

# A Heavily Commented Linux Kernel Source Code

Zhao Jiong



# A Heavily Commented Linux Kernel Source Code

Kernel Version 0.12

(Chinese Revision 5)



Zhao Jiong  
Jiong. zhao@TongJi. edu. cn

WWW. OLDLINUX. ORG

2019-01-24

## Abstract

This book provides detailed and comprehensive comments and explanations on all source code of the early Linux kernel (V0.12), aiming to enable readers to gain a comprehensive and profound understanding of the working mechanism of Linux in a shortest possible time and to lay a solid foundation for further study of modern Linux systems. Although the version of the analysis is very low, the kernel has been able to compile and run, and it already includes the essence of the working principle of Linux.

The book first briefly introduced the development history of the Linux kernel, explained the main differences between the various kernel versions and improvements, and gave the reasons for choosing the 0.12 kernel source code as the study object. Then it gives the basic knowledge needed to read the source code, outlines the hardware structure of the PC running the Linux system, the assembly language used by the kernel, the extends of C language, and focuses on the 80X86 processor in protected mode. Then we introduced the kernel code overview, given the kernel source directory tree structure, and according to the organizational structure of all kernel, programs and files are described in detail. In order to deepen the reader's understanding of the working principle of the kernel, the last chapter gives a number of related operational debugging tests. All relevant information in the book can be downloaded from the website [www.oldlinux.org](http://www.oldlinux.org).

This book suits as the assistant and practical teaching material of university computer major student study operating system course, also suitable for self-study reference book of Linux lovers as learning kernel operating principle, also can be used as the reference book that the general technical personnel develops the embedded system.

## Copyright statement

The author retains all rights to modify and formally publish this book. Feedback from readers can be sent to me via e-mail: [jiong.zhao@tongji.edu.cn](mailto:jiong.zhao@tongji.edu.cn) or [gohigh@gmail.com](mailto:gohigh@gmail.com), or you can write directly to: School of Mechanical and Energy Engineering, Institute of Mechanical and Electronic Engineering, Tongji University, Address: Room B409, Machinery Building, 4800 Cao'an Road, Shanghai, China: 201804

*Dedicated to:*

*Sun Hongfang - my dear mother  
Zhao Bichen - my beloved father*

*In teaching me to grow up  
You have spent your hard life*

*Your son  
Zhao Jiong*

献给

孙洪芳 - 我亲爱的母亲  
赵碧臣 - 我敬爱的父亲

在教诲我成长过程中  
度过了你们艰辛一生

你们的儿子  
赵炯

"RTFSC - Read The F\*\*\*king Source Code :)"

-Linus Benedict Torvalds

# Table of Contents

<b>PREFACE.....</b>	<b>1</b>	LINUX KERNEL MEMORY MANAGEMENT .....	178
THE MAIN GOAL OF THIS BOOK .....	1	INTERRUPT MECHANISM .....	193
FEATURES OF THIS BOOK.....	1	LINUX SYSTEM CALLS.....	199
OTHER BENEFITS OF READING EARLY KERNEL CODE.....	2	SYSTEM TIME AND TIMING .....	201
THE IMPORTANCE AND NECESSITY OF READING THE COMPLETE CODE .....	3	LINUX PROCESS CONTROL.....	203
HOW TO SELECT THE KERNEL CODE VERSION TO READ	3	HOW TO USE THE STACK IN LINUX .....	215
THE BASIC KNOWLEDGE REQUIRED BY THE BOOK .....	4	FILE SYSTEM FOR LINUX 0.12 .....	219
IS READING AN EARLIER VERSION OUT OF DATE? .....	5	DIRECTORIES OF KERNEL SOURCE CODE .....	220
EXT FILE SYSTEM AND MINIX FILE SYSTEM.....	5	THE KERNEL CODE AND USER PROGRAMS .229	
<b>1   OVERVIEW .....</b>	<b>7</b>	5.12   LINUX/MAKEFILE .....	230
1.1   THE BIRTH AND DEVELOPMENT OF LINUX .....	7	5.13   SUMMARY .....	236
1.2   CONTENT REVIEW.....	15	<b>6   BOOTING SYSTEM.....</b>	<b>237</b>
1.3   SUMMARY.....	20	6.1   MAIN FUNCTIONS.....	237
<b>2   MICROCOMPUTER STRUCTURE .....</b>	<b>21</b>	6.2   BOOTSECT.S .....	239
2.1   THE MICROCOMPUTER COMPOSITION .....	22	6.3   SETUP.S.....	254
2.2   I/O PORT ADDRESSING & ACCESS CONTROL... 23		6.4   HEAD.S.....	286
2.3   MAIN MEMORY, BIOS AND CMOS MEMORY 26		6.5   SUMMARY .....	299
2.4   CONTROLLERS AND CONTROL CARDS .....	28	<b>7   INITIALIZATION PROGRAM (INIT) .....</b>	<b>301</b>
2.5   SUMMARY .....	38	7.1   MAIN.C .....	301
<b>3   KERNEL PROGRAMMING LANGUAGEAND ENVIRONMENT .....</b>	<b>39</b>	7.2   ENVIRONMENT INITIALIZATION .....	316
3.1   AS86 ASSEMBLER .....	39	7.3   SUMMARY .....	318
3.2   GNU AS ASSEMBLER .....	46	<b>8   KERNEL CODE (KERNEL).....</b>	<b>319</b>
3.3   C LANGUAGE PROGRAM .....	58	8.1   MAIN FUNCTIONS.....	319
3.4   INTERWORKING BETWEEN C AND ASSEMBLY LANGUAGE .....	67	8.2   ASM.S .....	322
3.5   LINUX 0.12 OBJECT FILE FORMAT.....	76	8.3   TRAPS.C .....	329
3.6   MAKE COMMAND AND MAKEFILE.....	87	8.4   SYS_CALL.S.....	335
3.7   SUMMARY .....	93	8.5   MKTIME.C .....	349
<b>4   80X86 PROTECTION MODE AND ITS PROGRAMMING.....</b>	<b>94</b>	8.6   SCHED.C .....	351
4.1   80X86 SYSTEM REGISTERS AND SYSTEM INSTRUCTIONS .....	94	8.7   SIGNAL.C.....	373
4.2   PROTECT MODE MEMORY MANAGEMENT....101		8.8   EXIT.C .....	391
4.3   SEGMENTATION MECHANISM.....106		8.9   FORK.C .....	404
4.4   PAGING.....119		8.10   SYS.C .....	413
4.5   PROTECTION .....	124	8.11   VSPRINTF.C.....	429
4.6   INTERRUPT AND EXCEPTION HANDLING.....136		8.12   PRINTK.C .....	438
4.7   TASK MANAGEMENT .....	147	8.13   PANIC.C .....	439
4.8   THE INITIALIZATION OF PROTECTED MODE 157		8.14   SUMMARY .....	440
4.9   A SIMPLE MULTITASK KERNEL EXAMPLE....161		<b>9   BLOCK DEVICE DRIVER .....</b>	<b>441</b>
4.10   SUMMARY .....	173	9.1   MAIN FUNCTIONS.....	442
<b>5   LINUX KERNEL ARCHITECTURE .....</b>	<b>175</b>	9.2   BLK.H .....	446
5.1   LINUX KERNEL MODE.....175		9.3   HD.C .....	451
5.2   LINUX KERNEL SYSTEM ARCHITECTURE .....	176	9.4   LL_RW_BLK.C .....	477
5.3		9.5   RAMDISK.C .....	485
		9.6   FLOPPY.C .....	491
		9.7   SUMMARY .....	521
<b>10   CHARACTER DEVICE DRIVER .....</b>	<b>523</b>		
10.1   MAIN FUNCTIONS.....	523		
10.2   KEYBOARD.S.....	535		

---

10.3	CONSOLE.C .....	555	14.11	TERMIO.S.H.....	947
10.4	SERIAL.C.....	594	14.12	TIME.H.....	954
10.5	RS_IO.S .....	603	14.13	UNISTD.H.....	956
10.6	TTY_IO.C .....	608	14.14	UTIME.H.....	963
10.7	TTY_IOCTL.C .....	626	14.15	FILES IN THE INCLUDE/ASM/ DIRECTORY .....	964
10.8	SUMMARY.....	635	14.16	IO.H .....	964
<b>11</b>	<b>MATH COPROCESSOR (MATH).....</b>	<b>637</b>	14.17	MEMORY.H.....	965
11.1	FUNCTION DESCRIPTION.....	637	14.18	SEGMENT.H.....	966
11.2	MATH-EMULATION.C.....	647	14.19	SYSTEM.H .....	968
11.3	ERROR.C .....	660	14.20	FILES IN THE DIRECTORY INCLUDE/LINUX/ ..	973
11.4	EA.C .....	661	14.21	CONFIG.H .....	973
11.5	CONVERT.C .....	665	14.22	FDREG.H .....	975
11.6	ADD.C .....	670	14.23	FS.H.....	977
11.7	COMPARE.C.....	673	14.24	HDREG.H .....	982
11.8	GET_PUT.C .....	675	14.25	HEAD.H .....	985
11.9	MUL.C .....	682	14.26	KERNEL.H .....	986
11.10	DIV.C .....	684	14.27	MATH_EMU.H .....	987
11.11	SUMMARY.....	686	14.28	MM.H .....	991
<b>12</b>	<b>FILE SYSTEM (FS).....</b>	<b>689</b>	14.29	SCHED.H .....	993
12.1	MAIN FUNCTIONS.....	689	14.30	SYS.H.....	1002
12.2	BUFFER.C .....	708	14.31	TTY.H.....	1004
12.3	BITMAP.C .....	728	14.32	HEADER FILES IN THE INCLUDE/SYS/ DIRECTORY.....	1008
12.4	TRUNCATE.C .....	735	14.33	PARAM.H .....	1008
12.5	INODE.C .....	738	14.34	RESOURCE.H .....	1009
12.6	SUPER.C .....	752	14.35	STAT.H .....	1011
12.7	NAMEI.C .....	763	14.36	TIME.H.....	1013
12.8	FILE_TABLE.C.....	793	14.37	TIMES.H .....	1014
12.9	BLOCK_DEV.C .....	793	14.38	TYPES.H .....	1015
12.10	FILE_DEV.C .....	798	14.39	UTSNAME.H .....	1016
12.11	PIPE.C .....	802	14.40	WAIT.H .....	1017
12.12	CHAR_DEV.C .....	807	14.41	SUMMARY.....	1018
12.13	READ_WRITE.C .....	810			
12.14	OPEN.C .....	817			
12.15	EXEC.C .....	826			
12.16	STAT.C .....	845			
12.17	FCNTL.C .....	848			
12.18	IOCTL.C .....	852			
12.19	SELECT.C .....	854			
12.20	SUMMARY.....	868			
<b>13</b>	<b>MEMORY MANAGEMENT (MM).....</b>	<b>869</b>			
13.1	MAIN FUNCTIONALITIES.....	869			
13.2	MEMORY.C .....	879			
13.3	PAGE.S .....	901			
13.4	SWAP.C .....	902			
13.5	SUMMARY.....	912			
<b>14</b>	<b>HEADER FILES (INCLUDE) .....</b>	<b>913</b>			
14.1	FILES IN THE INCLUDE/ DIRECTORY .....	914			
14.2	A.OUT.H .....	915			
14.3	CONST.H .....	926			
14.4	CTYPE.H .....	926			
14.5	ERRNO.H .....	928			
14.6	FCNTL.H .....	930			
14.7	SIGNAL.H .....	931			
14.8	STDARG.H .....	934			
14.9	STDDEF.H .....	936			
14.10	STRING.H .....	937			
			17.1	BOCHS SIMULATION SOFTWARE.....	1049
			17.2	RUNNING LINUX 0.1X SYSTEM IN BOCHS...	1054
			17.3	ACCESS INFORMATION IN A DISK IMAGE FILE	
				1059	
			17.4	COMPILING AND RUNNING THE SIMPLE KERNEL	
				1062	

17.5	USING BOCHS TO DEBUG THE KERNEL .....	1065
17.6	CREATING A DISK IMAGE FILE .....	1073
17.7	MAKING A ROOTFILE SYSTEM.....	1076
17.8	COMPILE KERNEL ON LINUX 0.12 SYSTEM	1084
17.9	COMPILE KERNEL UNDER REDHAT SYSTEM	1085
17.10	INTEGRATED BOOT DISK AND ROOT FS ....	1089
17.11	DEBUGGING KERNEL CODE WITH GDB AND BOCHS	1094
17.12	SUMMARY.....	1100
	<b>REFERENCES .....</b>	<b>1101</b>
	<b>APPENDIX.....</b>	<b>1103</b>
A1	ASCII CODE TABLE.....	1103
A2	COMMON C0, C1 CONTROL CHARACTERS	1104
A3	ESCAPE AND CONTROL SEQUENCES .....	1106
A4	THE FIRST SET OF KEYBOARD SCancode	1109

# Preface

モノづくりのインテリジェント化やネットワークによるモノの直接制御という一般的な流れの中で、Linuxオペレーティングシステムは、今日の組み込みシステムにおける動作制御のための最も重要な基本プラットフォームとなっています。本書は、Linuxオペレーティングシステムのカーネルの基本的な仕組みを解説した入門書です。

## この本の主な目的は

本書の主な目的は、最小限のスペース、あるいは限られたスペースの中で、完全なLinuxカーネルのソースコードを解剖し、オペレーティングシステムの基本機能と実際の実装を完全に理解することです。Linuxカーネルを完全かつ深く理解するために、Linuxオペレーティングシステムの基本的な動作原理の真の理解と導入を行います。

本書の読者層は、Linuxシステムの一般的な使い方を知っていたり、一定のプログラミングの基礎を持っているが、現在の新しいカーネルコードを読むための基礎知識が不足しており、一刻も早くUNIX OSのカーネルの動作原理と実際のコードを理解したいと考えている人に位置づけられる。

## この本の特徴

本書を執筆している時点では、Linuxカーネルを解説した書籍の中には、新しいLinuxカーネルのバージョン（Fedora8が採用しているバージョン2.6.24など）を使って、カーネルの動作メカニズムを説明しようとしているものがあります。しかし、カーネルのソースコードのサイズは既に非常に大きいため（例えば、2.2.20バージョンでは268万行！）、これらの書籍では、Linuxカーネルのソースコードを選択的に説明・解説することしかできず、多くのシステム実装の詳細は無視されています。そのため、Linuxカーネルについて明確かつ完全な説明をすることは困難です。

スコット・マクスウェル著「Linux Kernel Source Code Analysis」は、基本的にはLinuxの上級者向けの書籍です。この本を完全に理解するには、より包括的な基礎知識が必要です。また、スペースの都合上、Linuxカーネルのすべてのコードを解説しているわけではなく、カーネルで使用されている各種ヘッダファイル(\*.h)や、カーネルコードのイメージファイルを生成するツール、プログラムの役割、各makeファイルとその実装など、カーネルの実装に関する多くの情報が省略されています。そのため、入門レベルの読者にとって、本書を読むことは困難です。

ジョン・ライオンズ著の「レオンのUNIXソースコード解析」は、OSカーネルのUNIXソースコードを学ぶには良い本ですが、UNIXバージョンV6を使用しているため、システムコールのコードの一部が長く使われていないPDP-11シリーズのマシンのアセンブラー言語であるため、ハードウェア部分に関するソースコードを読んで

理解する場合には、実験を行うことが困難です。

Andrew S. Tanenbaum氏の著書「Operating Systems:Design and Implementation」は、オペレーティングシステムのカーネル実装に関する良い入門書ですが、この本で紹介されているMINIXシステムは、メッセージベースのカーネル実装の仕組みであり、Linuxカーネルの実装には違いがあります。そのため、本書を学んだ後に、より新しいLinuxカーネルのソースコードに着手するのは、あまり容易ではありません。

これらの本を学習に使うとき、「目の不自由な人は象のように感じる」という感覚があるでしょう。それは

Linuxカーネルシステムの特定の実装の全体的な概念を理解するために、特にLinuxシステムの初心者は、カーネルの原理を学ぶためにこれらの書籍を使用する場合、カーネルの全体的な動作構造。頭の中で明確に形成することはできません。これは、私が長年Linuxカーネルの学習に携わってきた中の深い経験です。1991年10月、Linuxの創始者であるリナス・トーバルズは、Linuxバージョン0.03の開発中に書いた記事の中で、同じ問題に言及しています。LINUX-a free unix-386 kernel "と題されたこの記事の中で、彼は次のように述べている。"Linuxの開発は、オペレーティングシステムの愛好家やコンピュータサイエンスを学ぶ学生たちの使用、学習、娯楽のためのものである。"現在の一般的なLinuxシステムは大規模化・複雑化しており、初心者がOSを学ぶ出発点としては適さなくなっている。

そこで本書では、最小限のスペースで、あるいは限られたスペースの中で、Linuxカーネルのソースコード全体を完全に分解し、OSの基本機能と実際の実装を完全に理解することを目指しています。Linuxカーネルを完全に深く理解するためには、Linuxオペレーティングシステムの基本的な動作原理の真の理解と導入が必要です。

## 初期のカーネルコードを読むことのその他の利点

現在では、DJJのx86オペレーティングシステムやUclinuxなど、Linuxの初期カーネルをベースに、組み込みシステム専用に開発されたカーネルバージョンが数多く存在しています。世界の多くの人々も、初期のLinuxカーネルのソースコードを通して学ぶことのメリットを実感しています。現在、中国ではすでに人間のアノテーションを整理して、この記事と同じような本を出版しています。したがって、初期の Linux カーネルバージョンのソースコードを読むことは、Linux システムを学ぶための効果的な方法であり、Linux 組み込みシステムの研究と応用にも非常に役立つものである。

初期のカーネルのソースコードについてコメントする中で、筆者は、初期のカーネルのソースコードは、現在使われている新しいカーネルをほとんど凝縮したようなものだと感じました。現在のバージョンの基本的な機能原理がすでにほぼすべて含まれているのです。System Software.An Introduction to System Programming」の著者であるLeland L. Beck氏は、このように紹介しています。An Introduction to System Programming "の著者であるLeland L. Beckは、システムプログラムとオペレーティングシステムの設計を紹介する際に、すべてのシステムプログラムの設計と実装を説明するために、極めて単純化されたSIC (Simple Instruction Computer) システムを導入しました。その原理は、実際のコンピュータシステムの複雑さを回避するだけでなく、問題を徹底的に記述したものである。ここでは、学習対象としてLinuxの初期のカーネ

ルバージョンを選択し、その指導思想はLelandと同じです。これは、Linuxカーネル学習の初心者にとって、最良の選択の一つです。Linuxカーネルの基本的な動作原理を、最短時間で深く理解することができます。

カーネルの動作原理をすでに知っている人にとっては、実際の作業でシステムの動作メカニズムを、空気中の城を感じさせないようにするためにには、カーネルのソースコードを読む必要があります。

もちろん、初期のカーネルを学習対象とすることにはデメリットもあります。選択したLinux初期カーネルバージョンには、仮想ファイルシステムVFSのサポート、ネットワークシステムのサポート、a.out実行ファイルのみのサポート、他の既存カーネルにある複雑なサブシステムの記述などが含まれていません。しかし、本書はLinuxカーネルの仕組みを学ぶための入門書ですから、この点はカーネルのバージョンが古いものを選択するメリットのひとつです。本書を学ぶことで、これらの高度な内容をさらに学ぶための基礎を固めることができます。

## 完全なコードを読むことの重要性と必要性

Linuxの創始者がニュースグループの投稿で述べたように、ソフトウェアシステムの真の動作メカニズムを理解するためには、必ずソースコードを読むようにしましょう (RTFSC - Read The F\*\*king Source Code)。システム自体は全体として完成されたものであり、一見重要でないような細部も多く含まれています。しかし、それを無視してしまうと、システム全体の理解が難しくなり、実際のシステムの実装方法や手段を真に理解することができません。

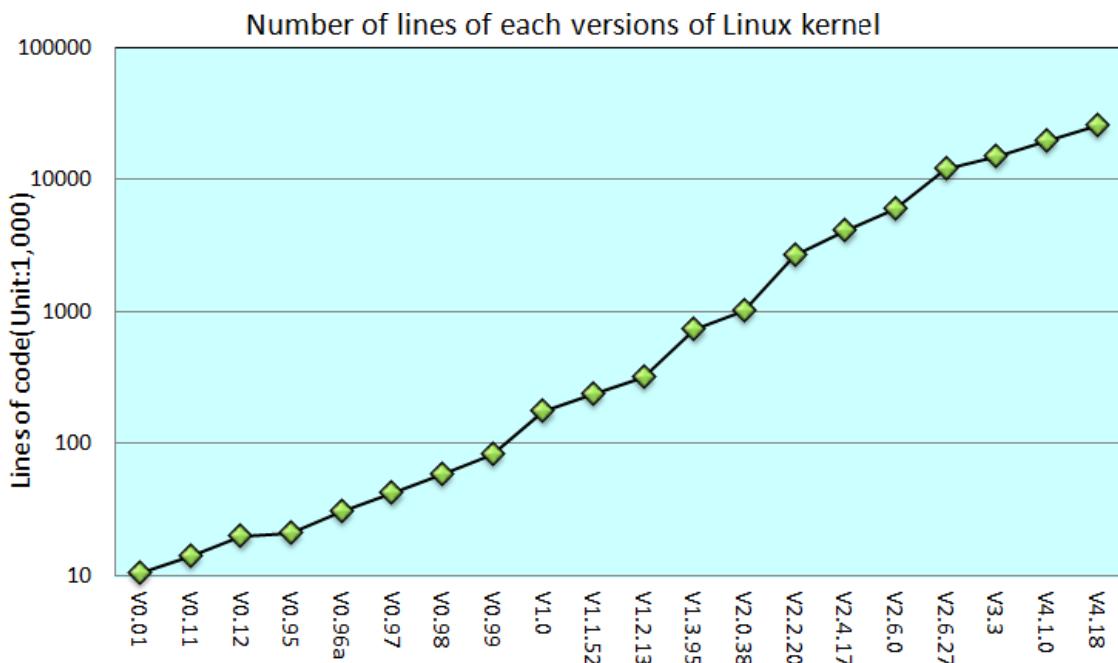
オペレーティングシステムの原理に関するいくつかの古典的な書籍 (MJBach氏の「UNIX Operating System Design」など) は、UNIX的なオペレーティングシステムの動作原理を理論的に導くために使用することができますが、実際のオペレーティングシステムの構成は

内部関係の実現についての理解はまだあまり明確ではありません。アンドリュー・S・タネンbaumが言ったように、"多くのオペレーティングシステムの教科書は理論的であり、軽い実践である。" ほとんどの本やコースは、スケジューリングアルゴリズムに多くの時間とスペースを消費し、I/Oを完全に無視しています。実際には、前者のコードは通常1ページにも満たない。後者はしばしばシステム全体のコードの3分の1を占めなければならない。"カーネルにおける多数の重要な詳細が言及されていません。そのため、本物のOSの真の美しさを理解することができません。完全なカーネルのソースコードを詳細に読んで初めて、システムに対する開放感が生まれ、システム全体の運用プロセスを深く理解することができます。後で学習するカーネルソースコードは、最新のものや新しいものを選ぶと、大きな問題は起こらず、基本的には新しいコードの内容をスムーズに理解することができます。

## 読み込むカーネルコードのバージョンの選択方法

では、多すぎる内容に惑わされることなく上記の要件を満たし、学習に適したLinuxカーネルのバージョンを選び、学習の効率を上げるにはどうすればよいのでしょうか。筆者は、多数のカーネルバージョンを比較・選択した結果、最終的に、現在のLinuxカーネルの基本機能に近く、かつ非常に

短い0.12カーネルを、入門に最適なバージョンとして選びました。次の図は、いくつかの主要なLinuxカーネルバージョンラインの統計を示しています。



現在のLinuxカーネルのソースコード量は数百万行に上り、2.6.0バージョンのカーネルコードラインは約592万行、4.18.Xバージョンのカーネルコードは非常に大きく、2,500万行を超えてます!ですから、これらのカーネルに完全に注釈をつけて詳しく説明することはほとんど不可能です。その0.12バージョンのカーネルは、コードの行数が2万行を超えていないので、本にしても説明やコメントがわかりやすくなっています。小さくても完成度は高い。研究対象のシステムを帰納的に理解し、実験を用いて原理の理解を深めるために、著者はこのカーネルをベースにしたLinux 0.12システムも特別に作り直しました。GNU

gccのコンパイル環境が入っているので、このシステムを使えば、簡単な開発作業もできます。

さらに、このバージョンを使用することで、さまざまなサブシステム（仮想ファイルシステムVFS、ext2、ext3ファイルシステム、ネットワークサブシステム、新しい複雑なメモリ管理メカニズムなど）の研究がますます複雑になっている既存の新しいカーネルバージョンを使用しないようにすることができます。

## 本で必要な基礎知識

この本を読むには、C言語の基礎知識とインテルCPUのアセンブリ言語の知識が必要です。C言語については、やはりBrain W. Kernighan氏とDennis M. Ritchie氏の著書「The C Programming Language」が一番の参考になります。アセンブリ言語のデータは、インテルCPUを解説したアセンブリ言語の教科書を参考にしてください。また、組み込み用のアセンブリ言語の情報も必要です。GNU gcc

コンパイラのマニュアルには、エンベデッド・アセンブリーに関する権威ある情報が掲載されています。また、インターネット上には、エンベデッド・アセンブリーに関する貴重なエッセイがあります

ので、そちらも参考にしてください。また、この本には、インライン・アセンブリの基本的な構文の説明があります(セクション5.5)。

また、読者の皆さんには、次のような基礎知識や関連する参考書をお持ちいただきたいと思います。ひとつは、80x86プロセッサのアーキテクチャやプログラミングに関する知識や情報です。例えば、80x86プログラミングマニュアル (INTEL 80386 Programmer's Reference Manual) は、インターネットからダウンロードできます。2つ目は、80x86のハードウェアアーキテクチャやインターフェースプログラミングに関する知識や情報です。この点については、多くの情報があります。3つ目は、Linuxシステムを使用する簡単なスキルも持っている必要があります。

を開始しました。

Linuxカーネルの実装は、「UNIX operating system design」という本の基本原則に沿って開発されたのが最初なので、ソースコード中の変数名や関数名の多くは、この本に由来しています。そのため、この本をきちんと読んでおけば、カーネルのソースコードを理解しやすくなります。

リーナスが初めてLinux OSを開発したとき、彼はMINIX OSを参考にした。たとえば、オリジナルのLinuxカーネルバージョンは、MINIX 1.0のファイルシステムを完全にコピーしています。そのため、本書を読む際には、A.S.タネンbaum氏の著書『Operating System:設計と実装』も大いに参考になります。

## 以前のバージョンを読むのは時代遅れ？

表面的には、Linuxの初期のカーネルバージョンの内容を、あたかもLinux OSがリリースされたばかりのように記しています。タネンbaumは、それが時代遅れ (Linux is obsolete) だと考えているのです。しかし、本書の内容を検討してみると、初期カーネルのソースコードの量が少なく、無駄がないため、本書を使ってLinuxカーネルを学ぶと、学習効率が非常に高く、少ない労力で多くのことができ、すぐに始められることがわかります。また、新しいカーネル部分のソースコードをさらに選択し続けるための強固な基礎を築くことができます。本書を読み終えると、システムがどのように動作するかについて、非常に完全で実用的なコンセプトを持つことになります。この完成された概念により、大量のコードを持つ新しいカーネルのソースコードを完全に読まなくても、新しいカーネルのソースコードの任意の部分をさらに選択して学習することが容易になります。

## ExtファイルシステムとMINIXファイルシステム

現在、Linuxシステムで使用されているExt3ファイルシステムは、カーネル1.x以降に開発されたもので、その機能は詳細で、性能も非常に完成度が高く安定しています。現在のLinux OSでは、デフォルトの標準ファイルシステムとなっています。しかし、Linuxオペレーティングシステムの完全な動作原理を入門的に学ぶ一環として、原理的には、より合理的であればあるほどよい。オペレーティングシステムの完全な理解を達成するために、様々なサブシステムの複雑で過剰な詳細に圧倒されることなく、学習用のカーネルバージョンを選択する原則は、システムコードが実際の動

作原理を説明できる限り、できるだけシンプルである。Linuxカーネルバージョン0.12には、当時最もシンプルなMINIX

1.0ファイルシステムしか含まれていませんでしたが、これはオペレーティングシステムにおけるファイルシステムの実際の構成と動作原理を理解するのに十分なものです。これが、学習用に初期のLinuxカーネルバージョンを選択する主な理由の1つです。

この本を一通り読んだ後、こんなため息を送ることになると思います。"Linuxカーネルシステムについては、ようやくスタートラインに立てた！"と。この時点では、最新のLinuxカーネルの各部分の動作原理やプロセスをさらに研究する自信があるはずです。

ザオ・ジオン博士

同濟大学 2019.1



# 1概要

本章ではまず、Linuxオペレーティングシステムの誕生、開発、成長の過程を振り返ります。このことは、本書が学習対象として初期バージョンのLinuxシステムを選んだ理由を理解するのに役立ちます。続いて、学習対象として初期バージョンのLinuxカーネルを選んだ場合のメリットとデメリット、さらに学習を始めるための方法を詳しく説明しています。最後に、各章の内容を簡単に紹介しました。

## 1.1 Linuxの誕生と発展

Linuxは、UNIXオペレーティングシステムのクローンシステムである。1991年10月5日に誕生しました（この日が最初の公式発表の日です）。以来、インターネットの普及に伴い、世界中のコンピュータ愛好家が協力して、現在では世界で最も広く使われているUNIX系OSとなり、現在もユーザー数が急増している。

Linuxオペレーティングシステムの誕生、発展、成長は、UNIXオペレーティングシステム、MINIXオペレーティングシステム、GNUプロジェクト、POSIX規格、インターネットネットワークという5つの柱に依存しています。この5つの基本的な手がかりをもとに、Linuxの開発史、醸成過程、初期開発を追っていく。まず、4つの基本要素を紹介し、Linuxの創始者であるリーナス・トーバルズ氏が、自身のコンピュータへの興味からコンピュータの知識を学び、自身のオペレーティングシステムの醸造を開始し、Linuxカーネルバージョン0.01の初期リリースまでリリースし、それがいかに困難なものであるかを追っていきます。そして、世界中のハッカーたちの協力を得て、一步一步前進し、ついにはより成熟したバージョン1.0の開発が導入されたのである。また、Linuxの初期開発の歴史についても詳しく書かれている。

もちろん、現在のLinuxカーネルのバージョンは4.18.xまで開発されているが、多くのLinuxシステムで使用されているカーネルは、安定した4.4.x~4.16.xのカーネルである（2桁目が奇数の場合は、開発中を意味し、システムの安定性を保証できない）。Linux開発の一般的な歴史については、多くの記事や書籍が紹介されていますので、ここでは繰り返しません。

### 1.1.1 オペレーティングシステム「UNIX」の誕生

Linuxオペレーティングシステムは、UNIXオペレーティングシステムのクローン版である。UNIXオペレーティングシステムは、1969年夏にベル研究所のKen.ThompsonとDennis RitchieがDEC PDP-7ミニコンピュータ上で開発したタイムシェアリングオペレーティングシステムです。ThompsonとDennis Ritchieが1969年夏にDEC PDP-7ミニコンピュータ上で開発したものです。

ケン・トンプソンは、お気に入りのスター・トラベル・ゲームを遊休中のPDP-7コンピュータで動かせるようにするために、1969年の夏、妻がカリフォルニアに帰省している間に、1カ月でUNIXのオペレーションを開発した。システムの原型となるもの。当時はBCPL言語（Basic Combination Programming

Language) が使われていた。1972年にデニス・リッチャーによって、移植性の高いC言語に書き換えられた後、UNIXシステムは大学やカレッジで普及していった。

### 1.1.2 MINIXオペレーティング・システム

MINIXシステムは、Andrew

S.

Tanenbaum (AST) によって開発されました。ASTは、オランダ・アムステルダムにあるヴリエ大学の数学・コンピュータサイエンスのシステムです。彼はACMとIEEEのシニアメンバーである（この2つの協会のシニアメンバーになっているのは世界でも数人しかいない）。合計100以上の論文と5冊のコンピュータ書籍を出版した。

ASTはニューヨークで生まれたが、それはオランダ人の駐在員であった（彼の祖父は1914年にアメリカに渡った）。ニューヨークの高校、M.I.T.の大学、そしてカリフォルニア大学バークレー校の博士課程で学んだ。博士号取得後の研究のため、故郷であるオランダに来た。それ以来、故郷との付き合いが続いている。その後、ヴリエ大学で教鞭をとり、大学院にも入学しました。オランダの首都アムステルダムは1年中雨の多い街ですが、ASTにとってはこれがベストで、この環境では家でパソコンをいじっていることが多いのです。

MINIXは1987年に誕生し、主に学生がオペレーティングシステムの原理を学ぶために使用されている。1991年にはバージョンが1.5になりました。現在、主に2つのバージョンが使われている。バージョン1.5とバージョン2.0です。当時、大学ではOSは無料でしたが、それ以外の用途では無料ではありませんでした。もちろん、現在のMINIXシステムは無料で、多くのFTPサイトからダウンロードすることができる。

Linuxシステムについては、後に開発者のリナス氏に賛辞を述べている。しかし、Linuxの開発は、MINIXを小さくするために、1学期で学習を終えてしまうために、世界中の多くの人からのMINIXの拡張要求を受け入れられなかつたことが大きな原因だと考えている。このような前提で、リナスはLinuxシステムを書くことになったわけです。もちろん、リナスもこのタイミングを逃さなかった。

オペレーティング・システムとしてのMINIXは優れたものではなく、C言語とアセンブリ言語で書かれたシステム・ソースコードも提供されている。プログラマーやハッカーを目指す人たちが、OSのソースコードを読むことができたのはこれが初めてのことです。当時、このソースコードはソフトウェアベンダーが大切に守ってきた秘密でした。

### 1.1.3 GNUプロジェクト

GNUプロジェクトとフリーソフトウェア財団は、1984年にリチャード・M・ストールマンによって設立され、UNIXに似た完全なオペレーティングシステムとフリーソフトウェア：GNUシステムを開発した（GNUは「GNU's Not」。Unixの再帰的な略語で、「guh-NEW」と発音します）。Linuxを中心としたさまざまなGNUオペレーティングシステムが広く使われている。これらのシステムはしばしば "Linux" と呼ばれます。ストールマンは厳密にはGNU/Linuxシステムと呼ばれるべきだと考えています。

1990年代初頭までに、GNUプロジェクトは、有名なemacs編集システム、bashシェルプログラム、gccシリーズコンパイラ、gdbデバッガなど、多くの高品質なフリーソフトウェアを開発しました。これらのソフトウェアは、Linuxオペレーティングシステムの開発に適した環境を作り出している。

これがLinux誕生の基盤のひとつとなり、現在では多くの人がLinux OSを「GNU/Linux」OSと呼んでいる。

### 1.1.4 POSIX規格

POSIX (Portable Operating System Interface for Computing Systems) は、IEEEとISO/IECが開発した規格群である。この規格は、既存のUNIXの慣習や経験に基づいており、オペレーティングシステムのコールサービスインターフェースを記述しています。コンパイルを確実に行うために使用されるアプリケーションは、ソースコードレベルで複数のオペレーティングシステムに移植して実行することができます。これは、1980年代前半に行われたUNIXユーザーグループ (usr/group) の初期の作業に基づいています。UNIXユーザーグループはもともと、AT&TのSystem Vオペレーティングシステムと、Berkeley CSRGのBSDオペレーティングシステムのコールインターフェースの違いを再統合しようとしていた。1984年にはusr/group規格をカスタマイズしました。

1985年、IEEE Operating System Technical Committee Standards Subcommittee (TCOS-SS) は、ANSIの庇護のもと、プログラムのソースコードの移植性オペレーティングシステムのサービスインターフェースの正式な規格を制定するようIEEE標準化委員会に指示を出し始めた。1986年4月には、IEEEが試験的に規格を策定した。1988年9月に最初の正式規格が承認され (IEEE 1003.1-1988) 、さらにPOSIX.1規格の

というのが後によく出てきます。

1989年までにPOSIXの作業はISO/IECコミュニティに移管され、15のワーキンググループがISO規格として開発を続けた。1990年になると、POSIX.1は、すでに採用されていたC言語規格と合わせて、IEEE 1003.1-1990 (ANSIでもある) およびISO/IEC 9945-1:1990規格として正式に承認された。

POSIX.1は、システムサービスのアプリケーション・プログラミング・インターフェース (API) を規定しているだけで、システムサービスの基本的な規格をまとめているに過ぎない。そのため、ワーキンググループでは、システムの他の機能に関する規格の策定を期待している。そこで、IEEE POSIXの作業が始まった。当初は10の承認計画が進行しており、四半期ごとの1週間の会議には300人近くが参加した。始まった作業は、コマンドとツールの規格 (POSIX.2) 、テスト方法の規格 (POSIX.3) 、リアルタイムAPI (POSIX.4) であった。1990年前半には、すでに25の計画が進行し、16のワーキンググループが参加した。同時に、X/Open、AT&T、OSFなど、同様の規格を開発している組織もある。

1990年代初頭、POSIX規格の策定は、1991年から1993年にかけて、最終段階の投票が行われていました。Linuxがまだ始まったばかりのこの時点で、このUNIX規格はLinuxにとって非常に重要な情報を提供し、Linuxが規格の指導のもとで開発され、ほとんどのUNIXオペレーティングシステムと互換性を持つことを可能にした。オリジナルのLinuxカーネルのソースコード (バージョン0.1、0.11、0.12) では、LinuxシステムはPOSIX規格との互換性を備えていました。Linuxバージョン0.01カーネルの/include/unistd.hファイルには、POSIX規格の要件に対応したいくつかのシンボリック定数が定義されており、リーナス氏はコメントにこう記している。"OK、これはジョークかもしれないが、私はそれに取り組んでいる。それはそうだ。"

1991年7月3日、リーナス氏はcomp.os.minixに投稿された記事の中で、POSIXのデータを収集していることに言及した。それによると、彼はOSの開発に取り組んでおり、開発当初はPOSIXとの互換性の問題を考えていたことが明らかになった。

### 1.1.5 OS 「Linux」 の誕生

1981年、IBMは世界的に有名なマイクロコンピューター「IBM PC」を発表した。1981年から1991年までの間、マイクロコンピューターのOSは常にMS-DOSが主役だった。この頃、コンピューターのハードウェアの価格は年々下がってきており、ソフトウェアの価格は高止まりしていた。その中で、アップル社の「MACs」というOSは、最高の性能を持っていると言えるが、その価格は誰も簡単には近づけないほどである。

また、当時のコンピューター技術の陣営には、UNIXの世界がありました。しかし、UNIXのOSは高価なだけの問題ではない。高い利益率を求めるために、UNIXの販売店は価格を極端に高くしてしまい、PCユーザーは近寄れないものである。また、かつてベル研究所から許可を得て、大学での教育に使用していたUNIXのソースコードも、漏洩しないように慎重に守られている。大多数のPCユーザーにとって、ソフトウェア業界の大手ベンダーがこの問題に有効な解決策を示したことはない。

この時、MINIXというOSが登場し、その設計と実装の原理を説明した本が同時に発行されたのである。ASTが書いたこの本は、非常に詳細でよくまとまっていたため、世界中のほとんどのコンピューター愛好家が、OSの仕組みを理解するためにこの本を読むようになったのである。その中には、Linuxシステムの創始者であるリーナス・ベネディクト・トーバルズも含まれている。当時（1991年）、彼はヘルシンキ大学のコンピュータサイエンス学科の2年生で、独学でコンピュータハッカーをしていた。21歳のフィンランド人青年は、自分のコンピュータをドラム缶に入れて、その性能や限界を試すのが好きだ。しかし、当時の彼に欠けていたのは、プロレベルのOSでした。

この年、GNUプログラムは数多くのソフトウェアツールを開発しました。最も期待されているのはGNU

Cコンパイラは登場したが、自由なGNUオペレーティングシステムはまだ開発されていない。教育現場で使われているMINIX

OSでさえ、著作権が発生し始めており、ソースコード入手するためには購入する必要があるのである。GNUオペレーティング・システムのHURDは開発中ではあるが、数年以内に完成するとは思えなかつた。

コンピュータの知識を身につけるために（興味本位かもしれないが）、ライナスはクリスマスの幸運なお金やローンを使って386互換機を購入し、米国からMINIXシステムのソフトウェアを郵送した。MINIXのソフトを待つ間、ライナスはインテル80386のハードウェアの知識を真剣に学んだ。モードによるダイアルアップで学校のメインフレームに接続できるようにするために、アセンブリ言語を使い、80386CPUのマルチタスク機能を利用して、ターミナル・エミュレーション・プログラムを作った。その後、古いパソコンに入っていた自分のソフトを新しいパソコンにコピーするために、フロッピーディスクドライブやキーボードなどのハードウェアデバイスのドライバーもコンパイルした。

プログラミングの練習を通して、また学習過程でMINIXシステムの多くの限界を認識したこと（MINIXは良いものだが、強力で実用的なオペレーティングシステムではなく、教育目的のシンプルなオペレーティングシステムに過ぎない）、リーナスはすでに似たようなものを持っていた。オペレーティングシステムのデバイスドライバのコードで、彼は新しいオペレーティングシステムのアイデアを持ち始めた。この時点で、GNUプロジェクトは多くのツールやソフトウェアを開発しており、

その中でも最も期待されているGNU

Cコンパイラが登場した。GNUの自由なオペレーティングシステムHURDは開発中ですが。しかし、リナスは急ぐことなく待っていた。

1991年4月からは、ターミナル・エミュレーション・プログラムやハードウェア・ドライバーを改造して、独自のOSを開発し始めた。当初の目的は、インテル386アーキテクチャの保護モード動作のプログラミング技術を習得するだけという単純なものだった。しかし、Linuxの開発は、当初の目的を完全に変えてしまった。comp.os.minixニュースグループでのリナス氏のニュースリリースによれば、彼がMINIXシステムの段階での学習から、独自のLinuxシステムの開発へと徐々に進化していくことがわかる。

リナスが初めてcomp.os.minixにメッセージを届けたのは1991年3月29日のこと。投稿された記事のタイトルは「gcc on minix-386 doesn't optimize」。これは、MINIX-386システムでgccコンパイラが最適化されて動作するというものです(MINIX-386は、Bruce EvansがIntel 386 features 32 Bit MINIX systemを使って改良したものです)。このことから、Linusは1991年初頭にすでにMINIXシステムを深く研究し始めており、その間にMINIXオペレーティングシステムの改良が行われていたことがわかります。MINIXシステムについてさらに学んだ後、このアイデアは、次第にインテル80386アーキテクチャをベースにした新しいオペレーティングシステムを再設計するというアイデアへと発展していった。

彼がMINIXについて誰かの質問に答えたとき、最初に言った文章は「Read the F\*\*ing Source Code :-」でした。)彼は、答えはソースプログラムの中にあると考えているのだ。このことからも、学習システムのソフトウェアでは、システムの基本的な動作原理を理解するだけでなく、実際のシステムを組み合わせて、実際のシステムの実装方法を学ぶ必要があることがわかります。結局のところ、理論は理論で、多くの枝が省略されています。このような枝葉の問題は、理論的な内容は少ないのですが、スズメに羽が生えているように、システムには必要なものなのです。

1991年4月以降、リナスはほとんどすべての時間をMINIX-386システムの研究(Hacking the kernel)と、GNUソフトウェアのMINIXへの移植(GNU gcc, bash, gdbなど)に費やした。そして、4月13日にcomp.os.minixで、bashのMINIXへの移植に成功し、シェルソフトを手放すことができなくなったと発表しました。

Linux関連のニュースが初めて公開されたのは、1991年7月3日のcomp.os.minixでした。(もちろん、当時はLinuxという名前はありませんでした。リナスは、その名前を「FREAK , FREAKX」ではないかと考えた。英語の意味は、グロテスク、モンスター、気まぐれ、など)。)これは、彼がLinuxシステムを開発していて、POSIXとの互換性の問題をすでに考えていたことを示している。

リナスの別の発表(comp.os.minix、1991年8月25日)では、すべてのMINIXユーザーに「MINIXシステムに最も見たいものは何ですか?("What would you like to see?" In minix?)と題して、(フリーの)386(486)オペレーティングシステムが開発されていることを初めて明かし、自分はそれにしか興味がないことを語った。コードは大きくなく、GNUのようなプロフェッショナルなものにはならないでしょう。MINIXシステムが好きな機能と嫌いな機能についてフィードバックしていただき、実用上の理由やその他の理由から、新しく開発されたシステムはMINIXに似ている(MINIXのファイルシステムを使っている)ことを説明していただければと思います。また、bash

(バージョン1.08) とgcc (バージョン1.40) を新システムに移植することに成功しており、数ヶ月後には実用化される予定です。

最後にリーナスは、自分が開発したOSはMINIXのソースコードを1行も使っていないと述べている。386のタスク切り替え機能のため、OSは移植性がなく（ノーポータビリティー）、ATのハードディスクしか使われていない。リーナスは、Linuxの移植性の問題を考えていなかった。しかし、現時点では、Linuxはほとんどの種類のハードウェアアーキテクチャで動作することができる。

1991年10月5日、リーナスはニュースグループcomp.os.minixにメッセージを掲載し、Linuxカーネルシステムの誕生を公式に発表した (Free minix-like kernel sources for 386-AT)。このニュースは、Linuxの誕生宣言ともいえるもので、広く流布している。そのため、10月5日はLinuxコミュニティにとって特別な日であり、その後の多くのLinuxバージョンがこの日を選んでいた。だから、RedHatがこの日を選んで新システムをリリースしたのは偶然ではない。

### 1.1.6 Linux OSのバージョン変更

Linux

OSが誕生してから1.0がリリースされるまでには、表1-

1のように多くのメジャーリリースが行われてきました。リーナスさんは、2003年9月にバージョン管理ツールBitKeeperの使い方を学び始めたときに、1.0の過去のバージョンをすべて見ました。実際にには、Linuxシステムにはこの0.00というバージョンは存在しないが、リーナスが自分の80386互換機で行った実験で、クロックの割り込み制御で2つのタスクを切り替えることに成功したため、自分のOS開発のアイデアをさらにある程度高めた。そのため、バージョンとしても記載しています。Linux版のカーネルバージョンが完成したのは、1991年9月17日のことである。しかし、リーナスには著作権意識が全くないので、このバージョンのinclude/string.hファイルには、著作権情報が1部だけ表示されています。このバージョンのカーネルのキーボードドライバは、フィンランド語のコードにのみハードコーディングされているため、フィンランド語のキーボードしかサポートしていません。また、8MBの物理メモリのみサポートしています。Linusのミスにより、その後の0.02, 0.03バージョンのカーネルのソースコードは破壊されて失われた。

Table 1-1 Earlier major versions of the kernel

Version No.	Release date	Description
0.00	1991.2.4	The two processes display 'AAA...' and 'BBB...' on the screen, respectively. (Note: No release)
0.01	1991.9.17	The first official release of the Linux kernel version. Multi-threaded file system, segmentation, and paging memory management. Does not include floppy disk drivers yet.
0.02	1991.10.5	This version and version 0.03 is an internal version that is currently unavailable. Features the same as above.
0.10	1991.10	The Linux kernel version released by Ted Ts'o. Added memory allocation library functions. The boot directory contains a script that converts as86 assembler syntax to gas assembler syntax.
0.11	1991.12.8	Basically functioning kernel. Supports hard disk and floppy drive devices as well as

		serial communications.
0.12	1992.1.15	The more stable version mainly increases the software simulation program of the math coprocessor. Added job control, virtual console, file symbolic links, and virtual memory swapping capabilities.
0.95.x (ie 0.13)	1992.3.8	Virtual file system support was added in this version, but it still contains only one MINIX file system. Added login functionality. Improves the performance of floppy disk drivers and file systems. Changed hard disk naming and numbering. The original naming method is the same as that of the MINIX system. At this time, it is the same as the current Linux system. Support CDROM.
0.96.x	1992.5.12	Began to add UNIX Socket support. Added ext file system alpha tester. SCSI drivers are officially added to the kernel. Floppy disk type is automatically recognized. Improved serial driver, cache, memory management performance, support for dynamic link libraries, and the ability to run X-Windows programs. The keyboard driver written in the original assembly language has been rewritten with C. Compared with the 0.95 kernel code, there are great changes.
0.97.x	1992.8.1	Added support for new SCSI drivers; dynamic caching; msdos and ext file system support; bus mouse drivers. The kernel is mapped to the beginning of the linear address 3GB.
0.98.x	1992.9.28	Improve support for TCP/IP (0.8.1) networks and correct extfs errors. Rewritten memory management section (mm), each process has 4GB of logical address space (the kernel occupies 1GB). Starting from 0.98.4, each process can open 256 files at the same time (originally 32), and the process's kernel stack uses a single memory page independently.
0.99.x	1992.12.13	Re-design the process of the use of memory allocation, each process has 4G linear space. Constantly improving the network code. NFS support.
1.0	1994.3.14	The first official version.

既存の0.10バージョンのカーネルコードは、当時保存されていたTed

Ts'oのバージョンで、Linus自身のものも失われています。このバージョンは、以前のバージョンに比べて大きく改善されています。このバージョンのカーネルシステムでは、GNU gccがカーネルのコンパイルに使われており、ファイルシステムのマウント/アンマウントの操作をサポートするようになりました。このカーネル・バージョンから、リナスは各ファイルの著作権情報を追加しました。"(C) 1991 Linus Torvalds"

です。その他の変更点としては、オリジナルのブートプログラム boot/boot.s が boot/bootsect.s と boot/setup.s の2つのプログラムに分割されたこと、1 最大 16MB の物理メモリをサポートしたこと、2 ドライバとメモリ管理プロシージャがそれぞれ別のサブディレクトリを作成したこと、3 フロッピードライバを追加したこと、4 ファイルの先読み操作をサポートしたこと、5 dev/port と dev/null デバイスをサポートしたこと、6 kernel/signal.c のコードを書き換え、sigaction() サポートを追加したこと、などが挙げられます。

カーネルの0.10バージョンと比較して、Linux

0.11バージョンの変更点は比較的小さい。しかし、このバージョンは、最初の安定版であり、他の人々は、カーネルの開発に参加し始めている。このバージョンの主な追加事項は次のとおりです。1 実行プログラムの要件をロードする、2 起動時に/etc/rc初期ファイルを実行する、3 数学コプロセッサの

シミュレーションプログラムのフレームプログラムの構造を構築する、4Ted

Ts'oは、スクリプトプログラムを追加する処理コード、5

Galen

Huntは、複数のディスプレイカードのサポートを追加する、6John

T

Kohlは、つぶやきとKILL文字をサポートするためにコンソールを有効にするためにカーネル/console.cプログラムを変更する、7は、多言語キーボードのサポートを提供します。

#### Linux

0.12は、Linusがより満足できるカーネルバージョンで、より安定したカーネルです。クリスマスの間に

1991年のシーズンには、gccのような「大規模な」ソフトウェアが2MBのメモリしか搭載されていないマシンでも使用できるように、仮想メモリ管理コードをコンパイルした。このバージョンを見て、リナスはカーネルのバージョン1.0をリリースすることが眼中にないことだと感じ、すぐに次のバージョン（バージョン0.13）をバージョン0.95にアップグレードした。リナスがこのようなことができる原因是、誰もがまだバージョン1.0には程遠いと感じないようにするという意味合いもある。しかし、0.95バージョンのリリースを急いだために、エラーも多く含まれており、0.95バージョンがリリースされたばかりの頃は、使用中に問題が発生するLinux愛好家が増えています。その時、リナス氏は「大惨事に遭遇した」と感じたという。しかし、それ以来、彼はこの教訓を受け入れた。その後、新しいカーネルバージョンがリリースされるたびに、彼はより慎重にテストを行い、公式に発表する前に数人の親友に試してもらうようにしています。カーネルの0.12バージョンの主な変更点は以下の通りです。1Ted

Ts'oによる端末信号処理のサポートの追加、2起動時に使用する画面ランクの変更が可能、3ファイルのIOによる競合状態の修正、4共有ライブラリのサポートの追加、メモリ使用量の節約、5シンボリックリンクの処理、6ディレクトリシステムコールの削除。7

ピーター・マクドナルドによる仮想端末のサポートの実装。これにより、Linuxは当時の特定の商用バージョンのUNIXよりもさらに優れたものとなった。関数のサポート。これは、何人かの人がMINIX用に提供したパッチをもとにピーター・マクドナルドが修正したものだが、MINIXはこれらのパッチを採用しなかった。9

再実行可能なシステムコール。10Linusによる数学コプロセッサのシミュレーションコードのコンパイル。

#### バージョン0.95は、GNU

GPLの著作権を使用した最初のLinuxカーネルバージョンです。このバージョンには、実際には3つのサブバージョンがあります。1992年3月8日に最初の0.95がリリースされたとき、いくつかの問題が発生したため、10日も経たないうちにすぐに別の0.95aがリリースされた（3月17日）。そして、1ヶ月後の4月9日には0.95c+がリリースされました。このバージョンの最大の改良点は、仮想ファイルシステムVFS構造の導入である。当時はMINIXファイルシステムしかサポートしていませんでしたが、複数のファイルシステムをサポートするために、プログラム構造を広範囲に調整しました。MINIXファイルシステム用のコードは、別のMINIXサブディレクトリに置かれています。0.95カーネルの他の変更点としては、以下のようなものがあります。1 ログインインターフェースの追加、2 Ross Biroによるデバッグコード(ptrace)の追加、3

フロッピーディスクドライブのトラックバッファリング、4

ノンブロッキングパイプラインファイル操作、5

システムの再起動(Ctrl-Alt-Del)、リアルタイムでスワップデバイスを選択するSwapon()システムコール、6

再帰的シンボリックリンクのサポート、7  
 ハードディスクパーティションのサポート、9  
 James Wiegandによる初期パラレルポートドライバのコンパイル、などなど。

また、0.95のリリースからは、カーネルの改良（パッチの提供）の多くが他社に独占され、リナスの主な仕事はカーネルのメンテナンスと、パッチを採用するかどうかの判断になっていきました。今まで、カーネルの最新バージョンは2018年6月にリリースされたバージョン4.16.16です。その使用しているgz圧縮のソースコードパッケージも約152MB!各メジャー安定版リリースの最新バージョンを表1-2に示す。表1-2

表1-2 新しいカーネルソースコードのサイズ

バージョン番号	発売日	サイズ(gz圧縮後)
2.0.40	2004.2.8	7.2 MB
2.2.26	2004.2.25	19 MB
2.6.25	2008.4.17	58 MB
3.0.10	2011.11.21	92MB
4.4.10	2016.5.11	127MB
4.16.16	2018.6.16	152MB

### 1.1.7 Linux名の由来

#### Linux

OSが誕生した当初は、Linuxとは呼ばれていませんでした。リナスは自分のオペレーティングシステムを

FREAK（フリーク）。英語の意味は、グロテスク、モンスター、気まぐれ。新しいOSをftp.funet.fiのサーバーにアップロードしたとき、管理者のアリ・レムケはこの名前をとても嫌がりました。彼は、リナスのオペレーティングシステムなので、その同音異義語であるLinuxをオペレーティングシステムのディレクトリとして使用することで、Linuxの名前が受け継がれるようになったと考えています。

リナスの自伝「Just for Fun」の中で、リナスはこう説明している。

「正直なところ、私はLinuxという名前ではリリースしたくありませんでした。それはあまりにも自己中心的だからです。最終的なリリースのために予約した名前は何でしたか？Freakです。（実際、初期のmakeファイル（ソースのコンパイル方法を記述したファイル）の中には、半年ほど「Freak」という言葉が含まれていました。でも、そんなことはどうでもいいことでした。その時点では、誰にも公開していなかったので、名前は必要ありませんでした）。

「そして、ftpサイトへの投稿を保証してくれたAri

LemkeはFreakという名前を嫌っていました。彼は、私が使っていたもう一つのワーキングネームであるLinuxを気に入り、私の投稿を「pub/OS/Linux」と名付けました。私があまり抵抗しなかったことは認めます。しかし、それは彼がやったことです。だから正直に言うと、私はエゴイストではなかったし、半分正直に言うと、エゴイストではなかったんです。でも、いい名前だと思ったし、いつでも誰かのせいにできると思ったから、今そうしているんだ」。

## 1.1.8 初期のLinuxシステムの開発に大きく貢献した

初期のLinuxのソースコードを見ればわかるように、リナス自身に加えて、Linuxシステムの最も有名な開発者の一人がセオドア・ツオ (Ted Ts'o) である。彼は1990年にMITコンピュータサイエンス学科を卒業した。大学時代には、学校で行われるさまざまな学生活動に積極的に参加した。趣味は、料理、サイクリング、そしてもちろんLinuxでのハッキング。その後、アマチュア無線の電報キャンペーンが好きになりました。現在は、IBMでシステムプログラミングなどの仕事をしています。また、International Network Design, Operations, Sales and Research Open GroupのIETFメンバーでもあります。

Linuxが世界的に普及したのも、彼の功績によるところが大きい。早くもLinux OSが登場したとき、彼はMaillistにLinuxの開発に大きな熱意を持って提供した。Linuxがリリースされて以来、彼はLinuxに貢献し続けている。また、Linuxカーネルに初めてプログラムを追加した人物でもある (Linuxカーネルバージョン0.10の仮想ディスクドライバ「ramdisk.c」、カーネルメモリ割り当てプログラム「kmalloc.c」など)。現在も、Linux関連の仕事に従事している。北米では、Linuxのftpサイト(tsx-11.mit.edu)を最初に立ち上げ、今でも大多数のLinuxユーザーにサービスを提供している。彼のLinuxへの最大の貢献は、ext2ファイルシステムの提案と実装です。このファイルシステムは、今ではLinuxの世界でデファクト・ファイルシステムの標準となっている。最近、彼はext3ファイルシステムを発表しました。このシステムは、ファイルシステムの安定性とアクセス効率を大幅に改善している。

彼への賞賛として、Linux Journal第97号（2002年5月）では、彼を表紙キャラクターに起用し、インタビューを行っている。現在は、IBM Linux Technology Centerに所属し、LSB (Linux Standard Base) の開発に取り組んでいる。

もう一人、Linuxコミュニティで有名なのがアラン・コックスだ。彼はもともと、ウェールズのスワンジー大学カレッジで働いていました。当初、彼はコンピュータゲームが好きで、特にMUD (Multi-User Dungeon or Dimension) を好んでプレイしていた。90年代前半の games.mud ニュースグループの投稿を見ると、彼が投稿したものがたくさんある。彼はMUD開発の歴史を書いたこともある (rec.games.mud news group, March 9, 1992, A history of MUD)。MUDゲームがインターネットと密接に関係していることから、彼は徐々にコンピュータネットワークに魅了されていきました。ゲームをプレイし、ゲームを実行しているコンピュータの速度やネットワークの伝送速度を向上させるためには、彼は最も満足のいくオペレーティング・プラットフォームを選択する必要がある。そこで、彼はさまざまな種類のOSに接触するようになった。お金がないので、MINIXシステムすら買えなかったのだ。Linux

0.1xや386BSDが発売された時には、386SXを購入するのに時間がかかった。386BSDは数学を必要とするので

コプロセッサに対応しており、CPUにインテル386SXを搭載したコンピューターには数学コプロセッサが搭載されていないことから、彼はLinuxシステムをインストールした。そこで彼は、無料のソースコードを使ってLinuxの学習を始め、Linuxシステム、特にネットワークに関して興味を持ち始めたのである。Linuxのシングルユーザーモードの動作についての議論では、「Linuxは美しく実装されている」と賞賛したほどである。

Linux

0.95のリリース後、彼はLinuxシステムのパッチ（修正プログラム）を書き始め（彼の最初の2つのパッチはLinusに採用されなかったことを覚えておいてください）、Linuxシステム上でTCP/IPネットワークコードの最初のユーザーになりました。

1人。その後、徐々にLinuxの開発チームに加わり、Linuxカーネルのソースコードを保守する主要な責任者の一人となった。また、Linuxコミュニティの中では、リーナスを中継した後の最も重要な人物とも言える。後にマイクロソフトからも誘われたが、あっさりと断っている。2001年からは、Linuxカーネル2.4.xのコードのメンテナンスを担当している。Linusは、主にカーネルの最新開発バージョン（2.5.xバージョンなどの奇数バージョン）の開発を担当している。

The Linux Kernel Hackers' Guide』の著者であるMichael K. Johnsonは、Linuxオペレーティングシステムに最初にコンタクトした人物のひとりでもあります（バージョン0.97から）。また、有名なLinux Document Project (LDP)の発起人のひとりでもある。かつては Linux Journal に勤務し、現在は RedHat に勤務している。

現在のように発展できるバックボーンは、Linuxシステムだけではありません。Linuxに多大な貢献をしたコンピュータの専門家はたくさんいます。ここではそれらをリストアップしません。主要な貢献者の具体的なリストは、Linuxカーネル内のCREDITSファイルに記載されており、Linuxに多大な貢献をした400人以上のリストがアルファベット順に記載されており、メールアドレスや送付先、ホームページ、主要な貢献内容などが記載されています。証書などがあります。

以上の説明を通して、Linuxの上記5つの柱をまとめると、以下のようになります。

#### ■ UNIXオペレーティングシステム--

UNIXは1969年にベル研究所で生まれた。LinuxはUNIXのクローンシステムです。UNIXの重要性は言うまでもありません。

#### ■ MINIXオペレーティングシステム--

MINIXオペレーティングシステムは、UNIXクローンシステムでもある。1987年に有名なコンピュータ教授アンドリュー・S・タネンbaumによって開発された。MINIXシステムの登場と、ソースコード（大学でのみ無償で使用可能）の提供により、世界中の大学でUNIXシステム学習の旋風が巻き起こった。Linuxは1991年に初めてMINIXシステムを参考にして開発を開始しました。

#### ■ GNUプロジェクト --

Linuxオペレーティングシステムの開発や、Linuxで使われているほとんどのソフトウェアは、基本的にGNUプログラムによるものです。LinuxはOSのカーネルに過ぎません。GNUソフトウェア環境（bashシェルなど）がなければ、Linuxは動きにくくなります。

#### ■ POSIX規格 -- この規格は、正式に開発された後のLinux OSの発展に重要な役割を果たした。Linuxの進歩の道標となっています。

#### ■ インターネット -

インターネットネットワークがなく、世界中の無数のコンピュータハッカーの無私の献身がなければ、Linuxは0.13（0.95）のレベルまでしか成長できません。

## 1.2 コンテンツレビュー

本書では、主に初期のLinuxカーネルバージョン0.12についての説明と解説を行う。Linux-0.12バージョンは1992年1月15日にリリースされました。出版の際には以下のファイルを含めてください。

---

bootimage-0.12.Z - 圧縮されたブートイメージファイルで、U.S. キーボードコードが含まれています。  
rootimage-0.12.Z - 1200kBの圧縮されたルートファイルシステムのイメージファイルです。

linux-0.12.tar.Z - カーネルのソースコードファイル。サイズは130KBで、展開後は463KBしかありません。as86.tar.Z - Bruce Evans氏によるバイナリ実行ファイルINSTALL-0.11- インストール情報ファイルを更新しました。

---

#### bootimage-0.12.Zとrootimage-

0.12.Zは、圧縮されたフロッピーアイメージファイルです。Bootimageはブートイメージファイルで、主にディスクのブートセクタコード、オペレーティングシステムのローダ、カーネルの実行コードが含まれています。PCが起動すると、ROM

BIOSのプログラムがデフォルトのブートドライブからブートセクタコードとデータをメモリに読み込み、ブートセクタコードがオペレーティングシステムローダーとカーネル実行コードをメモリに読み込んで制御します。

初期化のためにカーネルをさらに準備するのはオペレーティングシステムローダーであり、最終的にはローダーがカーネルコードに制御を与えます。カーネルコードが正しく機能するためには、ファイルシステムのサポートが必要です。Rootimageは、カーネルに最も基本的なサポートを提供するために使用されるルートファイルシステムで、オペレーティングシステムに少なくともいくつかの設定ファイルとコマンド実行手順を含む。Linuxシステムで使用されるUNIXベースのファイルシステムには、主にいくつかの指定されたディレクトリ、設定ファイル、デバイスドライバー、開発プログラム、その他すべてのユーザーデータやテキストファイルが含まれます。この2つのディスクの組み合わせは、起動可能なDOSオペレーティングシステムのディスクに相当する。

as86.tar.Z は 16 ビットのアセンブラー・リンクパッケージです。linux-0.12.tar.Z は Linux 0.12 カーネルのソースコードを圧縮したものです。INSTALL-0.11 は Linux 0.11 システム用の簡単なインストールドキュメントです。また、0.12 カーネルを使用している Linux システムにも適用されます。

現時点では、オリジナルの rootimage-0.12.Z ファイルに加えて、他の 4 つのファイルを見つけることができます。しかし、著者はインターネット上のリソースを利用して、Linux 0.12 用の完全に使用可能なrootimage-0.12ルートファイルシステムを再構築しました。0.12 環境で使用できる gcc 1.40 コンパイラを再コンパイルし、利用可能な実験的開発環境を設定しています。現在、これらのファイルは oldlinux.org

のウェブサイトからダウンロードできます。具体的なダウンロードディレクトリの場所は

- <http://oldlinux.org/Linux.old/images/>  
このディレクトリには、作成されたカーネルイメージファイル bootimage とルートファイルシステムイメージファイル rootimage があります。
- <http://oldlinux.org/Linux.old/kernels/> このディレクトリには、本書で紹介しているLinux 0.12 カーネルのソースコードプログラムを含む、カーネルのソースコードプログラムが格納されています。

- <http://oldlinux.org/Linux.old/bochs/>  
このディレクトリには、コンピュータ・シミュレーション・システムbochsで動作するよう  
に設定されたLinuxシステムが含まれています。
- <http://oldlinux.org/Linux.old/Linux-0.12/> このディレクトリには、Linux  
0.12システムで使用できるその他のツールや、オリジナルのインストール手順書などが含ま  
れています。

本書は、主にlinux-0.12

kernelに含まれるすべてのソースコードプログラムを詳細に解析し、各ソースプログラムファイルに  
対して、Makefileファイルのコメントを含めた詳細なコメントを付けています。解析作業は、主にコ  
ンピュータの起動プロセスに合わせて行われます。したがって、初期化カーネルの終了までの解析の  
一貫性は、シェルプログラムの呼び出しを開始します。それ以外のプログラムは、それぞれの解析の  
ためのもので、まとめはありませんので、それぞれの必要に応じて読んでください。ただし、解析  
中にいくつかの応用例を紹介しています。

すべてのプログラムを解析する過程で、筆者がその記述を理解するのが難しいと考えた場合には  
、関連する知識を詳しく説明します。例えば、割り込みコントローラへの入出力操作が発生した場合  
、インテルの割り込みコントローラ（8259A）チップの詳細な説明を行い、使用するコマンドやメソ  
ッドをリストアップします。これにより、コードの理解を深めるだけでなく、使用するハードウェア  
の使い方をより理解することができます。筆者は、ハードウェアなどの知識を全体的に紹介するため  
に別の章を設けるよりも、このような解釈方法の方がはるかに効率的だと考えています。

Linux 0.12のカーネルを "解剖" することで、Linuxの機能を理解する効率を高めることができます。  
オペレーティングメカニズム。全体のカーネルのソースコードのLinux  
0.12バージョンは、コンテンツを含むわずか約463Kバイトは、基本的にLinuxの本質です。最新のカ  
ーネルバージョン2.6.XXは非常に大きい、200メガバイトです。一生かけて読めるようになったとし  
ても、全部は読めないかもしれません。そこで、「せっかくJaneから始めるのだから、バージョン0.0  
1のLinuxカーネルのソースコードを小さくして分析してみたらどうだろう？約240Kバイトしかない  
んだから。」

とかね。主な理由は、0.01バージョンのカーネルコードには欠点が多すぎるからです。フロッピーデ  
ィスク用のドライバを含むだけでなく、数学コプロセッサの使用やログイン手順の指示にもうまく対  
応できていません。また、0.12の起動ブートプログラムの構造は、基本的に今のバージョンと同じで  
はありません。もうひとつの理由は、すでにコンパイルされているカーネルイメージファイル(booti  
mage-

0.12)の初期バージョン1.22が、ブートデモに使用できることです。簡単なルートファイルシステムイ  
メージ(rootimage-0.12)を追加すれば、普通に起動できるようになります。

また、Linux

0.12での学習には不備があります。たとえば、カーネルのバージョンには、特別なプロセスの待ち行  
列やTCP/IPネットワークなどに関する非常に重要なコードが含まれていません。また、メモリの割り  
当てや使用方法も現在のカーネルとは異なります。幸いなことに、Linuxのネットワークコードは基  
本的に自己完結型であり、カーネルの仕組みとの関係はそれほど大きくないので、Linuxの動作の基  
本原理を理解した上でコードを解析することができます。

本書は、Linuxカーネルのすべてのコードを解説しています。構造の整合性を保つために、コードの記述はカーネル内のソースコードの構造に基づいています。基本的には、各ソースコードの内容を1章としています。紹介するソースファイルの順番は、前回のファイルリストインデックスで確認できます。Linuxカーネルのソースコード全体のディレクトリ構造をリスト1-1に示します。すべてのディレクトリ構造は、Linuxをカレントディレクトリとした場合のものです。

List 1-1 Linux/ directory

Name	Size	Last modified date (GMT)	Desc.
boot/		1992-01-16 14:37:00	
fs/		1992-01-16 14:37:00	
include/		1992-01-16 14:37:00	
init/		1992-01-16 14:37:00	
kernel/		1992-01-16 14:37:00	
lib/		1992-01-16 14:37:00	
mm/		1992-01-16 14:37:00	
tools/		1992-01-16 14:37:00	
Makefile	3091 bytes	1992-01-13 03:48:56	

本書の内容は、5つのパートに分けられます。第1章から第4章までは基礎編。オペレーティングシステムは、実行されるハードウェア環境と密接に関係しています。オペレーティングシステムの全体的な動作を徹底的に理解したいのであれば、そのハードウェアの動作環境、特にプロセッサのマルチタスク動作の仕組みを理解する必要があります。このパートでは、マイクロコンピュータのハードウェア構成、Linuxカーネルプログラムをコンパイルするためのプログラミング言語、インテル80X86保護モード下でのプログラミング原理などをより詳しく紹介しています。第2パートには第5章から第7章までがあり、カーネルのブート起動と32ビット動作について説明しています。この方法の準備段階では、初心者がカーネルを学ぶために十分に読んでおく必要があります。第3部の第8章から第13章までは、カーネルコードの主要部分です。第8章の内容は、このセクションの後続の章を読むための主な手掛かりとすることができます。第14章から第16章までは

第4部の内容は、第3部のソースコードを読む際の参考になります。最後のパートには第17章のみが含まれており、PCシミュレーションソフトウェアシステム「Bochs」を使って、Linux 0.12カーネル上でさまざまな実験活動を行う方法が書かれています。

第2章では、従来のマイクロコンピュータシステムのハードウェアブロック図に基づいて説明しています。主にLinuxカーネルで動作するIBM

PC/AT386マイクロコンピュータの構成要素を紹介しています。各主要部の機能と関係を説明します。同時に、最新のマイクロコンピュータのブロック図とも比較しています。これにより、コンピュータの構成原理を学んでいない読者にも、十分な関連情報を提供することができる。

第3章では、Linux

0.12カーネルで使用されているプログラミング言語、オブジェクト・ファイル・フォーマット、およびコンパイル環境を紹介します。主な目的は、Linux  
カーネルのソースコードを読むために必要なアセンブリ言語と 0.12  
GNU C

言語拡張の知識を提供することです。本章では、まずas86とGNU asアセンブリの構文と使い方をより詳しく紹介し、次にGNU C言語のインライン・アセンブリ、ステートメント式、レジスタ変数、インライン関数などの一般的なC言語拡張を説明しました。また、C言語とアセンブリ関数の相互呼び出しの仕組みについても詳細に説明した。最後に、Makefileの使い方を簡単に説明する。

#### 第4章では、80X86

CPUのアーキテクチャと、プロテクトモードプログラミングの基礎知識について説明しています。この章では、80X86

CPUをベースにしたLinuxカーネルのソースコードを読むための準備として、しっかりとした基礎知識を身につけることができます。その内容は以下の通りです。80X86の基礎知識、プロテクトモードのメモリ管理、割込みと例外処理、タスク管理、そしてシンプルなマルチタスクカーネルの例です。

#### 第5章では、Linux

オペレーティングシステムのアーキテクチャ、カーネルのソースコードファイルの構成、各ファイルの一般的な機能について説明しています。また、Linuxでの物理的なメモリの割り当て、カーネルのいくつかのスタックとその使用方法、仮想リニアアドレスの使用についても紹介しています。最後に、カーネルパッケージのLinuxディレクトリにある最初のファイル、つまりカーネルコードの全体的なMakefileの内容について解説を始めます。このファイルは、すべてのカーネルソースプログラムのコンパイル管理用設定ファイルで、ビルド管理ツールソフトウェアmakeが使用します。

第6章では、bootディレクトリにある、ディスクブートプログラムのbootdisk.ss、BIOSのパラメータを取り込むsetup.sアセンブリ、32ビットランスタートコードプログラムのhead.sの3つのアセンブリプログラムについて詳しく説明します。この3つのアセンブリプログラムにより、ロックデバイスからメモリへのカーネルのブートロードとシステム構成パラメータの検出が完了し、32ビットプロテクトモードに入る前のすべての作業が完了します。カーネルシステムがさらに初期化作業を行うための準備を行う。

第7章では、主にinitディレクトリにあるカーネルシステムの初期化プログラムmain.cを紹介します。カーネルがすべての初期化作業を完了し、通常の動作に入るための重要なポイントとなります。システムの初期化がすべて完了すると、シェル用のプロセスが作成されます。プログラムの紹介では、それが呼び出す他のプログラムを見る必要があるので、後続の章の読み解きは、ここで呼ばれる順序で実行することができます。カーネルではメモリ管理プログラムの機能が広く使われているので、この章を最初に読むべきです。main.cまでのプログラムが本当に理解できるようになると、Linuxカーネルのことがある程度理解できるようになります。半分くらいは既に始まっていると言えますが、より深く読むためには、ファイルシステム、システムコール、各ドライバなども必要です。

第8章では、主にkernelディレクトリ内のすべてのプログラムを紹介しています。最も重要なのは、プロセススケジューラ()やsleep\_on()、プログラム関連のシステムコールです。この時点ですでに、重要なプログラムのいくつかを知っているはずです。この章の最初から、C言語プログラムに埋め込まれた多くのアセンブリ言語文に遭遇します。埋め込まれたアセンブリ文の基本的な構文は、第3章で説明します。

#### 第9章では、kernel/blk\_drv/

ディレクトリにあるロックデバイスプログラムについて説明します。本章では主にハードディスクやフロッピーディスクなどのロックデバイス用のドライバです。主にファイルシステムや高速バッファを扱うためのもので、よりハードウェアに関連した内容を含んでいます。そのた

め、この章を読む際には、いくつかのハードウェア情報を参照する必要があります。まず、ファイルシステムのセクションを見てみるのがよいでしょう。

第10章では、`kernel/chr_drv`/ディレクトリにあるキャラクターデバイスドライバについて注釈をつけています。本章では、主にシリアルラインドライバ、キーボードドライバ、モニタドライバを扱います。これらのドライバは、0.12カーネルでサポートされているシリアル端末やコンソール端末のデバイスを構成しています。そのため、本章ではハードウェア関連の内容も多くなっています。読む際には、関連するハードウェアの書籍を参考する必要があります。

第11章では、`kernel/math`/ディレクトリにある、数学コプロセッサのシミュレーションプログラムを紹介します。本書で注釈されているカーネルのバージョンでは、まだコプロセッサが本格的にサポートされ始めていないため、この章の内容は比較的小さく、比較的簡単なものになっています。一般的な理解をしておいてください。

第12章では、カーネルソースコードの`fs`/ディレクトリに格納されているファイルシステムプログラムを紹介します。本章を読む際には、しばらく立ち止まって、MINIXのファイルシステムについて、Andrew

S.Tanenbaum氏の著書「Operating System Design and Implementation」を参考にしました。チャプターは、オリジナルのLinuxシステムがMINIXファイルシステムしかサポートしていないため、Linux 0.12バージョンも例外ではありません。

第13章では、`mm`/ディレクトリ内のメモリ管理プログラムについて説明しています。この点を十分に理解するためには、インテル80X86マイクロプロセッサの保護モードの動作モードを十分に理解している必要があります。したがって、このプログラムのこの章を読むときには、この章の適切な場所に含まれる80X86の保護モードの動作モードの概要を参照することができます。また、この説明に加えて、第4章も同時に参照してください。この章では、ソースコード中の例題をオブジェクトとして使用することを説明していますので、メモリ管理の仕組みをより深く理解することができます。

既存のLinuxカーネル解析書では、一般的にカーネルヘッダファイルの記述が不足しており、初心者にとってはカーネルプログラムを読む上で多くの障害があります。本書の第14章では、`include`/ディレクトリにあるすべてのヘッダファイルを詳細に説明しています。基本的には、各定義、各定数、データ構造などが詳細にコメントされています。また、読書中の参照を容易にするために、本書では頻繁に使用される重要なデータ構造や変数を付録としてまとめていますが、これらの内容は実際に本章のヘッダーファイルに記載されています。本章の内容は、主に他の章の手順を読むためのものですが、カーネルの動作メカニズムを徹底的に理解したい場合には、やはりこれらのヘッダーファイルに書かれている内容の多くを理解する必要があります。

## 第15章では、Linux

0.12カーネルのソースコードの`lib`/ディレクトリにあるすべてのファイルについて説明しています。これらのライブラリ関数ファイルは、主にコンパイルシステムなどのシステムプログラムに対するインターフェース関数を提供しており、今後のシステムソフトウェアの理解に役立つものです。このようにバージョンが低いため、ここにはあまり何も書かれていませんので、すぐに読むことができます。これが、0.12を選んだ理由のひとつです。

第16章では、`tools`/ディレクトリにある`build.c`プログラムを紹介します。このプログラムは、コンパイルして生成したカーネルイメージファイルには含まれません。このプログラムは、カーネルのディスクブートブロックと他の主要なカーネルモジュールを接続して、完全なカーネルイメージファイルを作成するためにのみ使用されます。

第17章では、カーネルのソースコードを学ぶための実験環境と、実際に実験を行うための方法を紹介しています。主に、Bochsシミュレーション・システムでのLinuxカーネルの使用方法とコンパイル方法、ディスク・イメージ・ファイルの作成方法を紹介しています。また、Linux 0.12 のソースコードの構文を修正して、RedHat 9 システムで正しいカーネルをコンパイルできるようにする方法も紹介しています。

最後は、付録と索引です。付録では、Linuxカーネルにおける定数の定義や基本的なデータ構造の定義のほか、保護モードの動作メカニズムについて簡潔に説明しています。

また、参照を容易にするため、カーネルに使用されているPCハードウェアの情報は、本書の付録として別途掲載しています。参考文献では、以下のような書籍や論文などの情報のみを提供しました。

ソースコードを読むときに参考になるような、複雑な文献リストは用意しませんでした。私たちは、あらゆる種類の複雑で面倒な文献リストを提供しませんでした。たとえば、Linux Documentation ProjectのLDP (Linux Document Project) にあるファイルを参照する場合、LDPのウェブサイトのアドレスだけではなく、どのHOWTOの記事を参照する必要があるのかを明示的に記載します。

リーナスが初めてLinux OSのカーネルを開発したとき、主に3冊の本を参考にしました。ひとつはM.J.バッハの『UNIX Operating System Design』で、UNIX System Vカーネルの動作原理やデータ構造が書かれている。リーナスはこの本の中の多くの機能のアルゴリズムを使っている。また、Linuxカーネルのソースコードに含まれる多くの重要な関数の名前は、この本から引用されています。したがって、本書を読む際には、カーネルの動作原理についての必須の参考書となる。もう1つは、John H. Crawfordらが編集した『Programming the 80386』で、80x86のプロテクトモードのプログラミング方法を解説した良書です。また、Andrew S. Tanenbaumの『MINIX Operating System Design and Implementation』という本の初版もあります。リーナスはこの本に書かれているMINIXファイルシステムのバージョン1.0を主に使用しており、初期のLinuxカーネルでもこのファイルシステムのみをサポートしていますので、このファイルシステムの章を読むときには、ファイルシステムの動作原理 Tanenbaumの本から完全に入手できます。

各プログラムの説明では、まず、プログラムの主旨や目的、入出力パラメータ、他のプログラムとの関係などを簡単に説明した後、プログラムの完全なコードを列挙し、そのコードに詳細なコメントを付けていますが、オリジナルの

C言語は一種の英語であるため、プログラムのコードやテキストは一切変更・削除されていません。また、プログラムの元となる少量の英文コメントは、定数記号や変数名などの有用な情報を多く提供しています。コードの背後には、プログラムのより詳細な解剖図や、コードに登場する言語やハードウェア関連の知識の一部が記述されています。この情報を読んだ後にプログラムを見返すと、より深い理解が得られるでしょう。

本書を読むために必要な基本的な概念の知識の紹介は、各章の対応する部分に散りばめられています。これは主に検索の便宜を図るために、ソースコードの読み解きを組み合わせることで、いくつ

かの基本的な概念をより深く理解することができます。

最後に注意していただきたいのは、本書で説明されている内容を完全に理解したとしても、それはLinuxの専門家になったということではないということです。あなたは、Linuxカーネルマスターになるための初期知識を得て、Linuxの旅に出ただけです。この時点では、より多くのソースコードを、できればバージョン1.0から開発中の最新の奇数バージョンまで段階的に読むべきです。本書改訂時の最新Linuxカーネルはバージョン4.16.16です。これらの開発中の最新バージョンを素早く理解し、さらに自分で提案やパッチを考えられるようになったら、思い切って挑戦してみたいと思います。

## 1.3 概要

本章ではまず、Linuxの誕生と発展に欠かせない柱について詳しく説明しました。UNIXの初期のオープンソース版は、Linuxを実装するための基本原理とアルゴリズムを提供し、リチャード・ストールマンのGNUプログラムは、Linuxシステムのためのさまざまなフリーで実用的なユーティリティを提供しました。また、ツールやPOSIX標準の登場により、標準に準拠したシステムを実装するためのリファレンスガイドがLinuxに提供されています。AST社のMINIXオペレーティングシステムは、Linuxの誕生に欠かせない参考資料となり、インターネットは、Linuxが成長していくために必要な環境となっています。最後に、この章では本書の基本的な内容を紹介しています。

# 2マイクロコンピュータの構造

あらゆるシステムは、図2-

1に示すように、4つの基本部分からなるモデルとして見ることができます。入力部は、システムに入ってくる情報やデータを受け取るためのもので、処理センターで処理された後、出力部が送り出されます。エネルギー部は、システム全体の動作に必要なエネルギーの供給を行うもので、動作に必要なエネルギーの入力部と出力部を含む。

コンピュータ・システムの構成も例外ではなく、主にこの4つの部分で構成されています。しかし、内部的には、コンピュータシステムの処理センターと入出力部分との間のチャンネルやインターフェースは共通に使用できるので、図2-

1の(b)の方が、より適切にコンピュータシステムを抽象化して表すことができるはずである。もちろん、コンピュータや多くの複雑なシステムでは、それぞれが独立して完全なサブシステムとみなすことができ、このモデルを用いて記述することも可能であり、完全なコンピュータシステムはこれらのサブシステムによって構成されます。

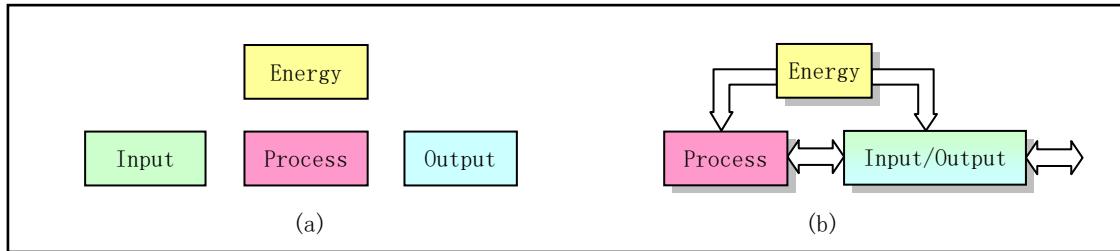


図2-1 システムの基本構成

コンピュータシステムは、ハードウェアとソフトウェアに分けられますが、これらは相互に依存しています。ハードウェア部分は、コンピュータシステムの目に見える部分であり、ソフトウェアの動作や保存のためのプラットフォームとなる。ソフトウェアは、ハードウェアの操作や動作を制御する命令の流れである。人間の脳に蓄積された情報や思考が人体の思考や行動を制御するように、ソフトウェアはコンピュータの「脳」の中の情報や思考と見ることができる。本書では、コンピュータシステムの動作メカニズムをテーマとしています。主に処理センターなど入出力部などのハードウェアの構成原理と、ソフトウェア制御の実現について解説しています。ハードウェア面では、Intel 80X86 CPU (Central Processing Unit) とその互換機をベースとしたIBM PCマイクロコンピュータのハードウェアシステムを概説します。コンピュータのCPUチップは、そのままシステムの処理センターと考えてよい。バスインターフェースは他の部品と接続されています。その上で動作するソフトウェアについては、Linuxオペレーティングシステムのカーネルの実装について具体的に説明します。

このように、OSは実行されるハードウェア環境と密接に関係していることがわかります。オペレーティングシステム全体を徹底的に理解するには、その動作するハードウェア環境を理解する必要があります。本章では、従来のマイクロコンピュータシステムのハードウェアブロック図をもとに、マイクロコンピュータの各主要部の機能を紹介しています。これらの内容は、基本的にLinux 0.12カーネルを読み解くためのハードウェアの基礎を確立しています。説明を容易にするために、PC/ATという用語は、80386以上のCPUを搭載したIBM PCおよびその互換マイクロコンピュータを指し、PCはIBM PC/XTおよびその互換マイクロコンピュータを含むすべてのマイクロコンピュータを総称して使用します。

## 2.1 マイクロコンピュータの構成

俯瞰的な視点から、80386以上のCPUを搭載したPCシステムの構造を説明する。従来のマイクロコンピュータのハードウェアの構造を図2-

2に示す。このうち、CPUはアドレス線、データ線、制御信号線で構成されるローカルバス（または内部バス）を介してシステムの他の部分と通信する。アドレスラインは、メモリやI/Oデバイスのアドレスを示すもので、データの読み書きが必要な特定の場所を示す。データラインは、CPUとメモリーやI/Oデバイスとの間のデータ転送経路となり、制御ラインは特定の読み書き動作を指示する役割を担う。80386のCPUを搭載したPCの場合、内部のアドレスラインとデータラインはそれぞれ32本あり、すべて32ビットである。したがって、アドレス空間は $2^{32}$ バイトで、0から4GBまである。

図では、通常、コンピュータのマザーボード上には、上位コントローラとメモリ・インターフェースが統合されている。これらのコントローラは、それぞれ大規模な集積回路チップを中心に構成された機能回路である。例えば、割り込みコントローラはインテル8259Aまたはその互換性のあるチップで構成され、DMAコントローラは通常インテル8237Aチップで構成され、タイミングカウンタはインテル8253/8254タイミングチップのコアであり、キーボードコントローラはキーボードと一緒にインテル8042チップを使用している。スキャン回路の通信を行う。

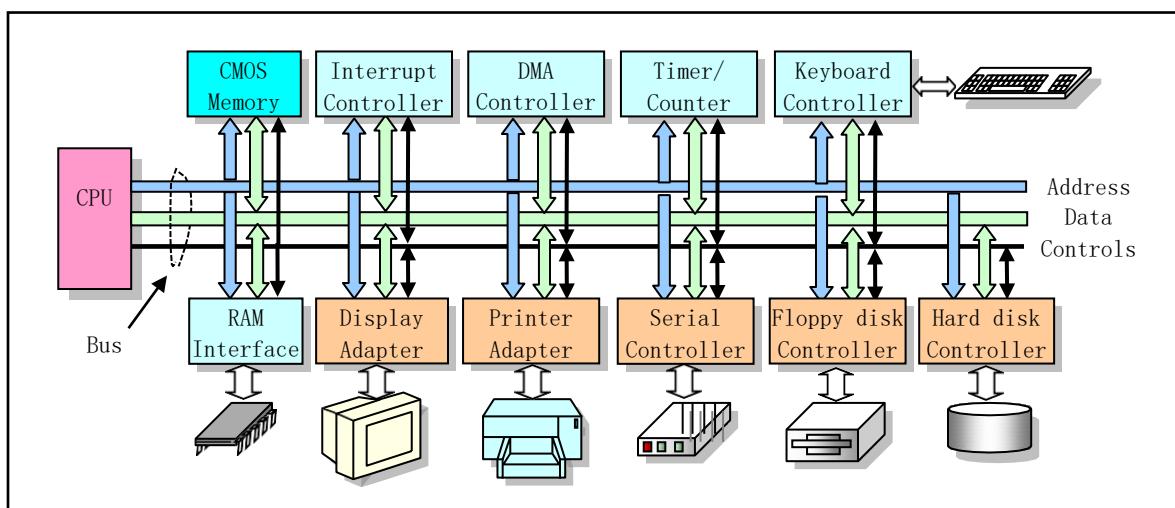


Figure 2-2 A block diagram of a traditional IBM PC and its compatibles

図の下側にあるコントロールカード（またはアダプター）は、拡張スロットを介してマザーボード上のシステムバスに接続されている。バススロットは、システムアドレスバス、データバス、コントロールラインの拡張デバイスコントローラへの標準的な接続インターフェースである。これらのバスインターフェース規格には、一般的に、ISA（Industry Standard Architecture）バス、EISA（Extended Industrial Standard Architecture）バス、PCI（Peripheral Component Interconnect）バス、AGP（Accelerated Graphics

Port）ビデオ。バスなどがあります。これらのバスインターフェースの主な違いは、データ転送速度と制御の柔軟性である。コンピュータのハードウェアの発展に伴い、シリアル通信のポイント・ツー・ポイント技術を用いた高速のPCIE（PCI

Express）バスなど、より高い転送速度と柔軟な制御が可能なバス・インターフェースが現在も登場し

ている。オリジナルの80386マシンにはISAバスしかないので、システムや外部のI/Oデバイスはデータ転送に16ビットのデータラインしか使えない。

コンピュータ技術の発展に伴い、従来はコントロールカードで実現していた多くの機能（ハードディスクのコントローラ機能など）が、コンピュータ本体に搭載された数個のVLSIチップに集約されている。

ボードに搭載されています。このようなチップが1つでもあれば、メインボードの主な特徴と機能が決定され、システムの各部分が最高の伝送速度を達成できるように、バス構造は大きく変化しています。現代のPCの構成は、しばしば図2-

3を使って説明することができます。最近のPCのマザーボードでは、CPUの他に、主に2つのチップセット、または超大型チップで構成されたチップセットが使用されています。ノースブリッジチップとサウスブリッジチップです。ノースブリッジチップは、CPU、メモリ、AGPビデオとのインターフェースに使われる。これらのインターフェースは非常に高い伝送速度を持っています。また、ノースブリッジチップは、メモリ制御の役割も担っています。そのため、インテルはこのチップをMCH (Memory Controller

Hub) チップと呼んでいます。サウスブリッジチップは、PCIバス、IDEハードディスクインターフェース、USBポートなどの低・中速コンポーネントの管理に使用される。そのため、サウスブリッジチップの名称はICH (I/O Controller

Hub) となっている。この2つのチップを総称して「サウスブリッジ」と「ノースブリッジ」と呼んでいるのは、インテル社が発行する一般的なPCマザーボードに搭載されているからである。メインバージョンの下端と上端（つまり地図の南と北）に配置されており、CPUとのチャネルブリッジの役割を果たしている。

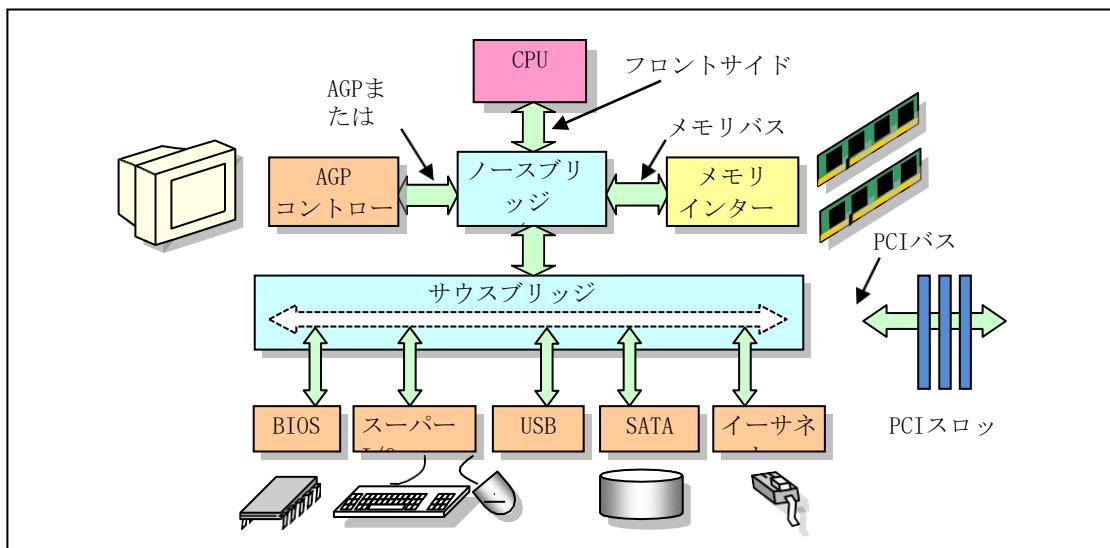


図2-3 最新のPCチップセットのブロック図

バスインターフェースは大きく変化し、将来的にはノースブリッジとサウスブリッジまでもが統合されますが、私たちプログラマーにとっては、これらの変化は従来のPCアーキテクチャとの互換性があります。したがって、従来のPCのハードウェア構造に対応したプログラムは、現在のPCでも動作

させることができます。これは、インテルの開発マニュアルでも確認できます。したがって、エンタリーラー学習を容易にするために、私たちは依然として伝統的なPCアーキテクチャの枠組みの中でPCの構成とプログラミング方法を議論し、研究しています。もちろん、これらの方法は現代のPCアーキテクチャにも適しています。以下では、図2-2の主なコントローラと制御カードのそれぞれの動作原理を概説し、それらの実際のプログラミング方法は、対応するカーネルのソースコードを読むまで延期します。

## 2.2 I/O ポートのアドレッシングとアクセスコントロール

CPUとI/Oアダプタ間のデータ転送を開始する前に、まず通信アダプタのI/O位置、つまりポートアドレスを決定する必要があります。CPUとI/Oインターフェイス間のデータ転送では、さまざまな転送制御モードが考えられます。一般的には、プログラムループ問い合わせ、割込み処理、DMA転送などが考えられます。

### 2.2.1 I/Oポートとアドレッシング

I/Oインターフェースコントローラーやコントロールカードのデータやステータス情報にアクセスするには、まずCPUがそれらのアドレスを指定する必要があります。このようなアドレスをI/Oポートアドレス、あるいは単にポートと呼ぶ。通常、I/Oコントローラには、データにアクセスするための「データポート」、コマンドを出力するための「コマンドポート」、コントローラの実行状況にアクセスするための「ステータスポート」がある。ポートのアドレスを設定するには、ユニファイドアドレッシングとインディペンデントアドレッシングの2つの方法がある。

ポートのユニファイドアドレッシングの原理は、I/Oコントローラ内のポートアドレスをメモリのアドレッシングアドレス空間に入れることである。したがって、このアドレッシング方法は、メモリ・イメージ・アドレッシングにもなる。CPUがポートにアクセスする動作は、メモリにアクセスする動作と同じであり、メモリにアクセスするための命令も使用される。ポート独立アドレスの方法は、I/Oコントローラとコントロールカードのアドレス空間を、I/Oアドレス空間と呼ばれる別のアドレス空間として扱うものである。各ポートにはそれに対応するI/Oアドレスがあり、ポートへのアクセスには専用のI/O命令を使用する。

#### IBM

PCとその互換マイクロコンピュータは、主に独立アドレスモードを採用しており、制御装置のレジスタをアドレス指定してアクセスするために、独立したI/Oアドレス空間を使用しています。ISAバスアーキテクチャを使用する従来のPCは、0x000から0x3FFまでのI/Oアドレス空間を持ち、1024個のI/Oポートアドレスが利用可能です。各コントローラやコントロールカードが使用するデフォルトのポートアドレス範囲を表2-1に示します。これらのポートの使用方法やプログラミング方法については、後に関連するハードウェアが具体的に登場したときに詳しく説明します。

#### また、IBM

PCではユニファイド・アドレッシング・モードを部分的に使用しています。例えば、CGAディスプレイメモリカードのディスプレイメモリのアドレスは、メモリアドレス空間0xB800～0xBC00の範囲を直接占めています。したがって、画面に文字を表示したい場合は、メモリ操作命令を使って、このメモリ領域に直接書き込み操作を行うことができます。

Table 2-1 I/O port address assignment

Address range	Allocation description
0x000 -- 0x01F	8237A DMA controller 1
0x020 -- 0x03F	8259A Programmable Interrupt Controller 1
0x040 -- 0x05F	8253/8254A Timer Counter
0x060 -- 0x06F	8042 Keyboard Controller
0x070 -- 0x07F	Access CMOS RAM/Real-Time Clock RTC Port
0x080 -- 0x09F	DMA page register access port
0x0A0 -- 0x0BF	8259A Programmable Interrupt Controller 2
0x0C0 -- 0x0DF	8237A DMA Controller 2
0x0F0 -- 0x0FF	Coprocessor access port
0x170 -- 0x177	IDE hard disk controller 1
0x1F0 -- 0x1F7	IDE hard disk controller 0
0x278 -- 0x27F	Parallel printer port 2
0x2F8 -- 0x2FF	Serial Controller 2
0x378 -- 0x37F	Parallel printer port 1
0x3B0 -- 0x3BF	Monochrome MDA display controller
0x3C0 -- 0x3CF	Color CGA display controller
0x3D0 -- 0x3DF	Color EGA/VGA display controller
0x3F0 -- 0x3F7	Floppy drive controller
0x3F8 -- 0x3FF	Serial Controller 1

EISAやPCIなどのバスアーキテクチャを採用している最近のPCでは、64KBのI/Oアドレス空間が利用可能です。関連するコントローラーや設定が使用するI/Oアドレスの範囲は、通常のLinuxシステムでは、/proc/ioportsファイルを見るなどで得ることができます。以下を参照してください。

---

```
[root@plinux root]# cat /proc/ioports
0000-001f : dma1
0020-003f : pic1
0040-005f : timer
0060-006f : keyboard
0070-007f : rtc
0080-008f : dma page reg
00a0-00bf : pic2
00c0-00df : dma2
00f0-00ff : fpu
0170-0177 : ide1
01f0-01f7 : ide0
02f8-02ff : serial(auto)
0376-0376 : ide1
03c0-03df : vga+
03f6-03f6 : ide0
03f8-03ff : serial(auto)
0500-051f : PCI device 8086:24d3 (Intel Corp.)
0cf8-0cff : PCI conf1
da00-daff : VIA Technologies, Inc. VT6102 [Rhine-II]
    da00-daff : via-rhine
e000-e01f : PCI device 8086:24d4 (Intel Corp.)
    e000-e01f : usb-uhci
e100-e11f : PCI device 8086:24d7 (Intel Corp.)
    e100-e11f : usb-uhci
e200-e21f : PCI device 8086:24de (Intel Corp.)
    e200-e21f : usb-uhci
e300-e31f : PCI device 8086:24d2 (Intel Corp.)
    e300-e31f : usb-uhci
f000-f00f : PCI device 8086:24db (Intel Corp.)
    f000-f007 : ide0
    f008-f00f : ide1
[root@plinux root]#
```

---

## 2.2.2 インターフェイスのアクセスコントロール

### PC

I/Oインターフェースのデータ転送制御モードは、一般的にプログラムのループ問い合わせモード、割り込み処理モード、DMA転送モードを採用することができます。周期問い合わせモードとは、その名の通り、CPUがプログラムをループさせて指定されたデバイスコントローラに状態を問い合わせることで、デバイスとのデータ交換が可能かどうかを判断するものです。この方法は、過剰なハードウェアサポートを必要とせず、使用方法やプログラムも比較的簡単ですが、貴重なCPU時間を消費します。そのため、マルチタスクOSでは、待ち時間が極端に短い場合や必要な場合を除いて、この方法は使用しない方が良いでしょう。Linux OSでは

システムでは、この方法は、デバイスやコントローラがすぐに情報を返すことができる一部の場所でのみ使用されます。

割り込み処理制御方式は、割り込みコントローラのサポートが必要です。この制御方式では、I/OデバイスがCPUに対して割り込みによる処理要求を行った場合のみ、CPUは現在実行中のプログラムを一時的に中断し、対応するI/O割り込み処理サービスプロセスを実行する。割り込み処理サービスプロセスの実行後、CPUは先ほど割り込まれたプログラムの実行を継続します。I/Oコントローラやデバイスが割り込み要求を発行すると、CPUは割り込みベクタテーブル（または割り込みディスクリプタテーブル）を用いて、対応する割り込み処理サービスプロセスのエントリーアドレスを指定します。したがって、割り込み制御モードを使用する場合は、まず割り込みベクタテーブルを設定し、対応する割り込み処理サービスプロセスをコンパイルする必要があります。Linux OSでは、ほとんどのデバイスI/O制御が割り込み処理を使用しています。

I/Oデバイスとシステムメモリー間の一括データ転送には、DMA（ダイレクトメモリアクセス）方式が採用されています。すべての動作プロセスは、CPUを介さずに専用のDMAコントローラを使用する必要があります。転送中にソフトウェアを介在させる必要がないため、非常に効率的に動作します。Linux

OSでは、フロッピーディスクドライバーが割り込みとDMA方式でデータ転送を実現している。

## 2.3 メインメモリ、BIOS、CMOSメモリ

一般的なPCには3種類のメモリが搭載されています。1つはプログラムの実行やデータの一時保存に使用されるメインメモリのRAM（Random Access Memory）、もう1つはシステムのブート診断やハードウェアプログラムの初期化に使用されるROM（Read Only Memory）メモリ、そして3つ目はコンピュータのリアルタイムクロック情報やシステムハードウェアの設定情報を保存する少量のCMOSメモリです。

### 2.3.1 メインメモリ

1981年にIBM

PCが登場したとき、システムには640KBのRAMメインメモリ（メモリと呼ばれる）しかなかった。使用されているCPUの8088/8086はアドレスラインが20本しかないため、メモリのアドレス範囲は最大で1024KB（1MB）である。オペレーティングシステム「DOS」が普及していた当時は、640Kや1MBのメモリ容量でも、基本的には通常のアプリケーションには十分だった。コンピュータのソフトウェアおよびハードウェア技術の急速な発展に伴い、現在のコンピュータは512MB以上の物理メモリ容量を持つ構成が一般的であり、すべてインテル社の32ビットCPU、つまりPC/ATコンピュータが使用されている。そのため、CPUの物理メモリのアドレス範囲は4GBまでとなっています（CPUの新機能を利用することで、64GBの物理メモリ容量をアドレス指定することも可能ですが）。しかし、ソフトウェア的にオリジナルのPCと互換性を持たせるために、システム1MB以下の物理メモリの割り当てはまだ基本的にはオリジナルのPCと同じままであるが、オリジナルシステムのROMのBIOSは常にCPUがアドレス可能なメモリの中で最も高い位置にありました。最後の場所では、BIOSの元の場所は、コンピュータの初期化時にBIOSのシャドウ領域として使用され、すなわち、BIOSコードは依然としてこの領域にコピーされます。図2-4をご覧ください。

コンピュータの電源を投入すると、物理メモリはアドレス0から始まる連続した領域に設定されます。0xA0000～0xFFFFF（384K～1Mの合計384K）と0xFFE0000～0xFFFFFFFF（4Gの最後の64K）のアドレス範囲を除くすべてのメモリがシステムメモリとして使用できます。この2つの特定の範囲は、I/OデバイスやBIOSプログラムに使用されます。コンピュータに16MBの物理メモリがある場合、Linux 0.1xシステムでは0～640Kがカーネルコードとデータの格納に使用されます。Linuxカーネルは、BIOSの機能を使用せず、BIOSが設定した割り込みベクターテーブルも使用しません。640Kと1Mの間の384Kは、まだ図に示した用途のために確保されています。このうち、アドレス0xA0000から始まる128Kはディスプレイメモリバッファとして使用され、その部分は他のコントロールカードのROM BIOSやそのマッピング領域に使用され、0xF0000から1Mの範囲は使用されます。

### は、ハイエンドシステムのROM

BIOSのマッピング領域として使用されます。1M～16Mは、カーネルが割り当て可能なメインメモリ領域として使用する。また、カーネルのコードやデータの背後には、高速バッファやメモリ仮想ディスクなどもメモリ領域の一部を占めている。この領域は通常640K～1Mにわたる。

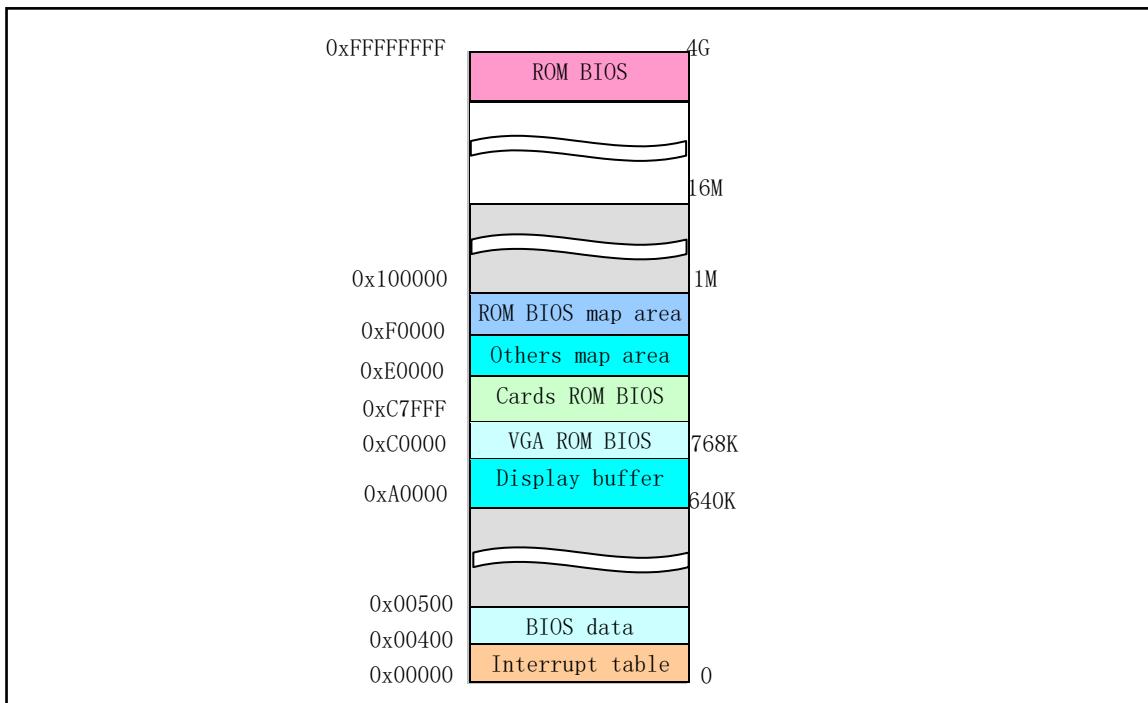


Figure 2-4 PC/AT machine memory area usage map

### 2.3.2 基本入出力プログラム BIOS

ROMに格納されているシステムBIOSプログラムは、主にコンピュータの電源投入時にシステム各部のセルフチェックを実行し、割り込みベクトルテーブルやハードディスクパラメータテーブルなど、OSが使用する必要のある各種設定テーブルを確立します。また、プロセッサやその他のシステムを既知の状態に初期化したり、DOSなどのOSにハードウェアデバイスのインターフェースサービスを提供したりする。しかし、BIOSが提供するこれらのサービスはリエントランシー（プログラムの同時実行ができないこと）ではないため、アクセス効率を考慮すると、初期化時にBIOSを使用して一部のシステムパラメータを提供することを除いて、Linux OSも同時に実行されます。BIOSの機能を使用しないでください。

コンピュータシステムの電源を入れたり、筐体のリセットボタンを押したりすると、CPUは自動的にコードセグメントレジスタCSを0xF000に設定し、セグメントベースアドレスを0xFFFFF0000に設定し、セグメント長を64KBに設定します。IPは0xFFFFF0に設定されているので、CPUのコードポインタは4G空間の最後の64Kの最後の16バイトである0xFFFFFFFF0を指していることになります。上の図から、ここにはシステムROMのBIOSが格納されています。そして、BIOSはここに、BIOSコードの64KB範囲内の命令にジャンプして実行を開始するためのジャンプ命令JMPを格納する。PC/ATマイコンのBIOS容量は1MB～2MBが主流で、フラッシュメモリROMに格納されているため、64KB以上の範囲のBIOSを実行・アクセスできるようにするために、0～1Mのアドレス空間からは離れています。その他のBIOSコードやデータは、まずBIOSプログラムが32ビットアクセスを使用して、データセグメントレジスタのアクセス範囲を（本来の64Kではなく）4Gに設定し、CPUが0～4Gの範囲のデータを実行・操作できるようにします。その後、BIOSがいくつかの列のハードウェア検出と初期化操作を行った後、元のPCと互換性のある64KBのBIOSコードとデータを64Kにコピーして

を1Mメモリのローエンドに設定し、ここにジャンプしてCPUをリアルにします。図2-5のようにリアルアドレスモードで実行します。最後に、BIOSはハードディスクやその他のブロックデバイスからOSのブートプログラムを0x7c00のメモリにロードし、この場所にジャンプしてブートプロセスを続行します。

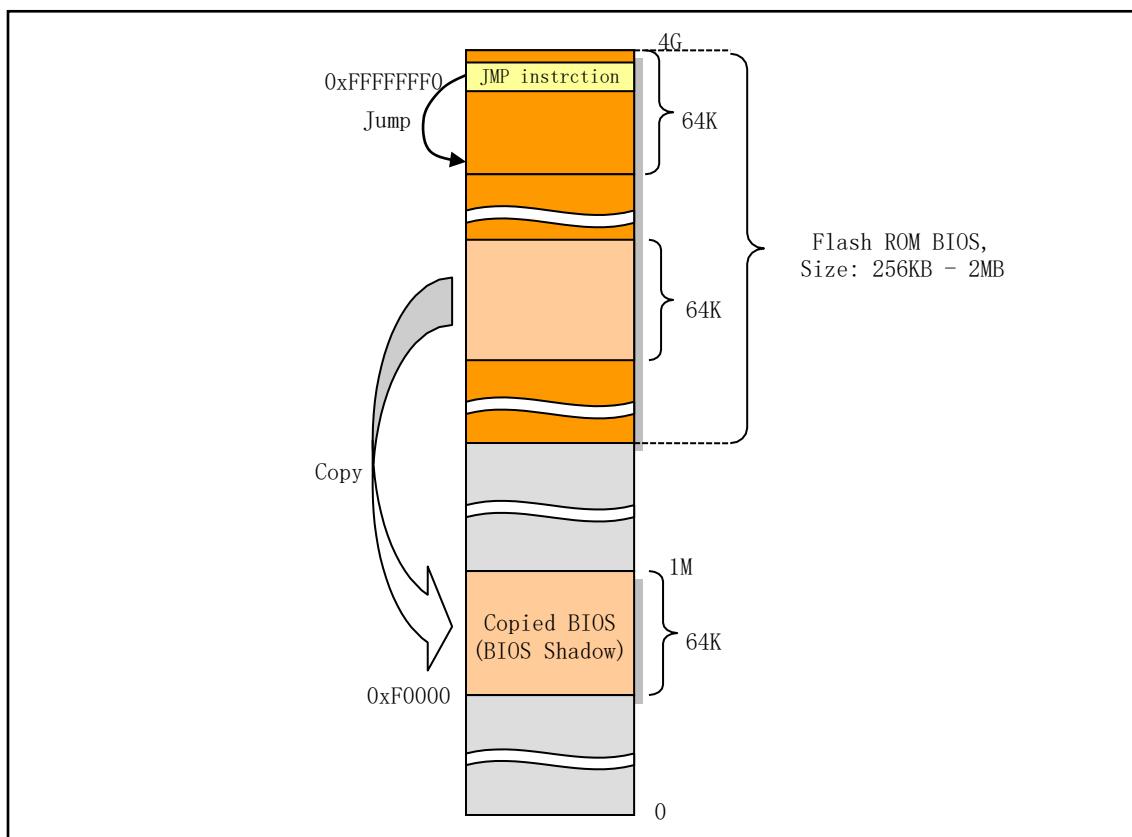


Figure 2-5 Flash ROM BIOS location and copy mapping area

### 2.3.3 CMOSメモリー

PC/AT機では、メモリやROM

BIOSを使用する必要があるほか、コンピュータのリアルタイムクロック情報やシステムハードウェアの構成情報を格納するために、記憶容量の少ない（64バイトまたは128バイト）CMOSメモリが使用されている。この部分のメモリは、通常、リアルタイムチップと一体化したブロックになっている。CMOSメモリのアドレス空間は基本メモリのアドレス空間の外にあるため、I/O命令を使ってアクセスする必要がある。

## 2.4 コントローラーとコントロールカード

図2-

2からわかるように、PCには、データの転送やコンピュータの動作を制御するためのさまざまな制御カードやコントローラが搭載されています。これらのコントローラやコントロールカードには、主に割り込みコントローラ、DMAコントローラ、キーボードコントローラ、フロッピー/ハードディスクコントロールカード、シリアル通信コントロールカード、ディスプレイコントロールカードなどがあります。ここで、「コントローラ」とは、コンピュータのマザーボード上に組み込まれた制御部品を指し、「コントロールカード」とは、拡張スロットからコンピュータに挿入される制御カード部品を指す。制御装置は、独立した制御カードの形で存在することもあれば、コンピュータの統合度の向上に伴ってメインボードに統合されることもあるため、コントローラと制御カードの間に実質的な違いはありません。以下、これらの制御装置について詳しく説明します。

### 2.4.1 割り込みコントローラ

IBM

PC/AT

80X86互換マイクロコンピュータでは、カスケード接続された2つの8259Aプログラマブル割込み制御チップを使用して、I/Oデバイス割込み制御データアクセスのための割込みコントローラを構成し、15個のデバイスに対して独立した割込みを提供することができます。その制御機能を図2-6に示す。コンピュータの初期起動時に、ROM

BIOSは2つの8259Aチップを初期化し、クロックタイマ、キーボード、シリアルポート、プリントポート、フロッピーディスクコントローラ、コプロセッサ、ハードディスクに15段階の割り込み優先順位を割り当てます。機器やコントローラを使用する。同時に、メモリ先頭の0x000-0xFFFFエリアに割り込みベクターテーブルが作成され、これらの割り込み要求は、表2-2に示すように、0x08から始まる割り込みベクタ一番号にマッピングされます。

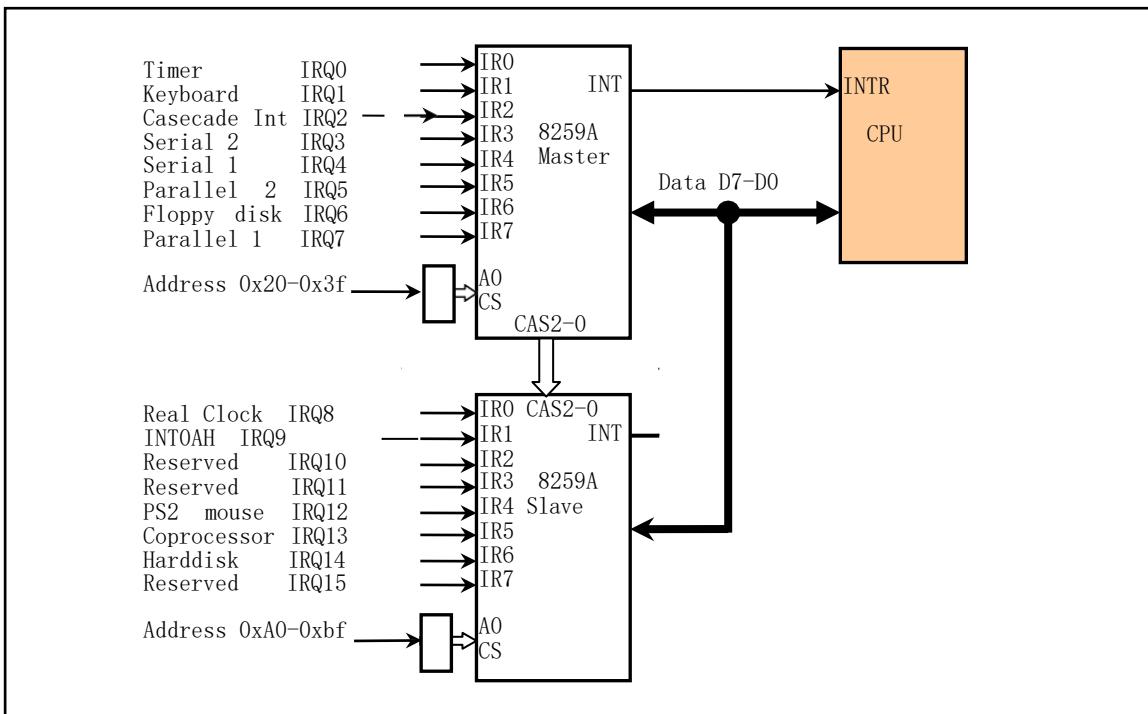


Figure 2-6 PC/AT microcomputer connected 8259 control system

し  
かし、0x00--  
0x1Fという割り込み番号は、CPU用に特別に確保されたインテルのものであるため、これらのBIOS設定はインテルの要求と相反することになります。この問題を解決するために、Linux OSはBIOSで設定されたこれらの割り込み番号を直接使用しません。パワーオン起動時、Linux OSはカーネルの初期化時に8259Aを再設定し、すべてのシステム・ハードウェア割り込み要求番号を0X20以上の割り込み番号にマッピングします。割り込みコントローラの動作やプログラム方法の詳細については、以降のセクションを参照してください。

Table 2-2 Hardware request interrupt number set by ROM BIOS at power on

IRQ number	Interrupt number Set by the BIOS	Usage description
IRQ0	0x08 (8)	8250 issued 100HZ clock interrupt
IRQ1	0x09 (9)	Keyboard interrupt
IRQ2	0x0A (10)	The slave chip's interrupt
IRQ3	0x0B (11)	Serial port 2
IRQ4	0x0C (12)	Serial port 1
IRQ5	0x0D (13)	Parallel port 2
IRQ6	0x0E (14)	Floppy disk drive
IRQ7	0x0F (15)	Parallel port 1
IRQ8	0x70 (112)	Real-time clock interrupt
IRQ9	0x71 (113)	Change to INT 0x0A
IRQ10	0x72 (114)	Reserved
IRQ11	0x73 (115)	Reserved (network interface)
IRQ12	0x74 (116)	PS/2 mouse port interrupt
IRQ13	0x75 (117)	Math coprocessor interrupt
IRQ14	0x76 (118)	Hard disk controller interrupt
IRQ15	0x77 (119)	Reserved

## 2.4.2 DMAコントローラ

前述したように、DMAコントローラーの主な機能は、外部デバイスがメモリに直接データを転送することで、システムのパフォーマンスを向上させることです。通常は、マシンに搭載されているインテル8237チップまたはその互換チップによって実装されています。DMAコントローラーをプログラムすることで、周辺機器とメモリー間のデータ転送をCPUの制御なしに行うことができます。そのため、データ転送の間、CPUは他の作業を行うことができます。

PC/AT機では、8237チップが2個使用されているので、DMAコントローラには8つの独立したチャネルが用意されています。そのうち最後の4つは16ビットチャネルです。フロッピーディスクコントローラは、特にDMAチャネル2を使用するように指定されています。チャネルを使用する前にまず設定する必要があります。これには、ページレジスタポート、（オフセット）アドレスレジスタポート、データカウントレジスタポートの3つのポートに対する操作が必要です。DMAレジスタは8ビット、アドレス値とカウント値は16ビットの値なので、それぞれを2回送信する必要があります。

## 2.4.3 タイマー/カウンター

インテル8253/8254は、コンピュータで正確な時間遅延を扱うために設計されたプログラマブル・インターバル・タイマー（PIT）チップです。このチップは、3つの独立した16ビットカウンターチャンネルを備えています。各チャネルは異なる動作モードで動作し、これらの動作モードはすべてソフトウェアで設定できます。ソフトウェアで遅延を行うには、ループ演算文を実行する方法がありますが、そのためにはCPU時間を消費します。機械に8253/8254チップが使用されている場合、プログラマ

は8253を独自の要件に合わせて設定し、カウンタ・チャネルの1つを使用して目的の遅延を実現することができます。遅延時間が経過すると、8253/8254はCPUに割り込み信号を送ります。

PC/ATおよびその互換マイクロコンピュータシステムには、8254チップが使用されています。3つのタイマ/カウンタチャネルは、時間帯別クロック割り込み、ダイナミックメモリのDRAMリフレッシュタイミング回路、ホストスピーカの音色合成に使用されています。Linux

0.12のOSでは、カウンタがモード3で動作するようにチャネル0のみをリセットし、10ミリ秒ごとに信号を送信して割り込み要求信号(IRQ0)を生成します。この間隔で発生する割り込み要求が、Linux 0.12カーネルのパルスとなります。現在実行中のタスクを定期的に切り替え、各タスクが使用するシステムリソース(時間)の量をカウントするために使用されます。

#### 2.4.4 キーボードコントローラー

私たちが今使っているキーボードは、1984年にIBMが発売したPC/AT互換機用のキーボードです。通常、AT-

PS/2互換キーボードと呼ばれ、101~104個のボタンが付いています。このキーボードにはプロセッサー(インテル8048またはその互換チップ)が搭載されている。

キーボードのエンコーダーと呼ばれるものです。これは、すべてのキーを押したり離したりしたときのステータス情報(すなわちスキャンコード)をスキャンして収集し、ホストコンピューターのメインボードにあるキーボードコントローラーに送信するためのものです。キーが押されたときにキーボードから送られてくるスキャンコードをMake code、または単にconnect codeと呼び、押されたキーが離されたときに送られてくるスキャンコードをdisconnectedと呼びます。ブレークコード、または単にブレークコードと呼ばれる。

ホストキーボードコントローラは、受信したキーボードのスキャンコードをデコードし、デコードしたデータをオペレーティングシステムのキーボードデータキューリーに送るように特別に設計されています。キーボードコントローラーは、各キーのオンとオフのコードが異なるため、スキャンコードに基づいて、ユーザーがどのキーを操作しているかを判断することができます。キーボード全体のすべてのキーのオンとオフのコードは、キーボードのスキャンコードセットを形成する。コンピュータの発展に伴い、現在では3つのスキャンコードセットが存在する。それらは

- 最初のスキャンコードセット--  
オリジナルのXTキーボードのスキャンコードセットです。現在のキーボードでは、このようなスキャンコードを送ることはほとんどありません。
- 2つ目のスキャンコード・・・最近のキーボードで使用されているデフォルトのスキャンコード・セットで、一般的にはATキーボードのスキャンコード・セットと呼ばれています。
- 3つ目のスキャンコードは、PS/2キーボードのスキャンコードセットです。IBMが発売した初代PS/2マイコンで使われたスキャンコードセットは、ほとんど使われていません。

ATキーボードは、デフォルトで2番目のスキャンコードを送信します。これにもかかわらず、ホスト・キーボード・コントローラは、図2-

7に示すように、PC/XTソフトウェアとの互換性のために、受信したすべてのセカンド・キーボード・スキャン・コードをファースト・スキャン・コードに変換します。そのため、キーボードコントローラをプログラミングする際には、通常、最初のスキャンコードのセットだけ知っていればよいのです

。これは、キーボードのプログラミングに関して、XTキーボードのスキャンコードセットのみが与えられている理由でもあります。

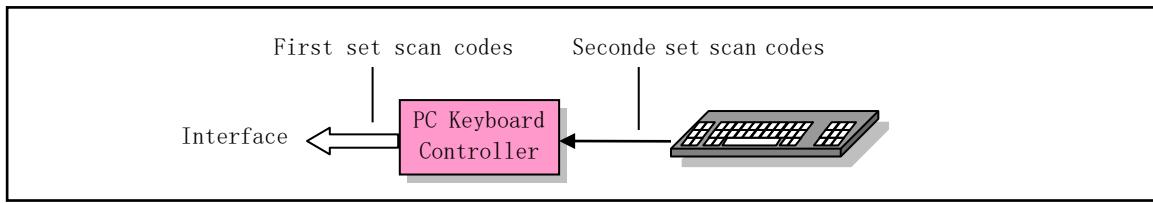


Figure 2-7 Keyboard controller conversion of scan code set

キーボードコントローラーには、一般的にインテル社のシングルチップ・マイクロプロセッサー・チップ「8042」またはその互換回路が使用されています。現在のPCでは、キーボードコントローラーはマザーボードのチップセットに組み込まれているが、機能的には8042チップを使用したコントローラーと互換性がある。キーボードコントローラーは、キーボードから送られてくる11ビットのシリアル形式のデータを受け取る。1ビット目はスタートビット、2-9ビット目は8ビットのキーボードスキャンコード、10ビット目はパリティチェックビット、11ビット目はストップビットです。次項のシリアルコントロールカードの説明を参照してください。11ビットのシリアルデータを受信したキーボードコントローラは、キーボードスキャンコードをPC/XT標準キーボード互換システムスキャンコードに変換した後、割り込みコントローラのIRQ1端子を介してCPUに割り込み要求を送信します。CPUが割り込み要求に応答すると、キーボード割り込みハンドラが呼び出され、コントローラ内のXTキーボードスキャンコードを読み取ります。

キーが押されると、キーボードコントローラポートからXTキーパッドのアクセスコードを受け取ることができます。このスキャンコードは、キーボード上のある場所のキーが押されたことを示すだけで、まだ文字コードにマッピングされていません。接続コードは通常1バイト幅です。例えば、キー「A」のキーオンコードは30 (0x1E) である。押したキーが離されると、キーボードコントローラポートからブレークコードが送られてきます。XTキーボードの場合（キーボードコントローラのプログラミングポートが受信するスキャンコード）、切断コードは

接続コードは、その接続コードに0x80を加えたもの、つまり最上位ビット（ビット7）がセットされているときに使用します。例えば、上記の「A」キーのブレークコードは、 $0x80 + 0x1E = 0x9E$ となります。

しかし、PC/XT標準の83キーKeyboardに新たに追加された（「拡張」された）ATキーボードキー（右のCtrlキーや右のAltキーなど）については、そのオン/オフのスキャンコードは通常2~4バイトで、1バイト目は0xE0でなければならない。例えば、拡張されていない左のCtrlキーを押すと、1バイトのパスコード0x1Dが生成され、右のCtrlキーを押すと、拡張された2バイトのパスコード0xE0, 0x1Dが生成される。対応するブレークコードは 0xE0, 0x9D です。表2-3は、スキャンコードのオン/オフを切り替えるいくつかの例を示しています。さらに、スキャンコードの完全な第1セットも付録として与えられています。

Table 2-3 Example of the first scan code set received on the keyboard controller port

Pressed key	Connect scan code	Break scan code	Description
A	0x1E	0x9E	Non-expanding ordinary keys
9	0x0A	0x8A	Non-expanding ordinary keys
Function key F9	0x43	0xC3	Non-expanding ordinary keys
Arrow key right	0xe0, 0x4D	0xe0, 0xCD	Extended keys
Right Ctrl key	0xe0, 0x1D	0xe0, 0x9D	Extended keys
Left Shift + G	0x2A, 0x22	0xAA, 0xA2	Press and release Shift first

また、キーボードコントローラ8042の出力ポートP2は、他の目的にも使用されます。P20端子は、CPU のリセット動作を実現するために使用され、P21 端子は、A20信号線のオープンを制御するために使用されます。出力ポートのビット1（P21）が1の時、A20信号線をオン（ゲート）にし、0の時、A20信号線をディスエーブルにします。今日のマザーボードでは、もはや個別の8042チップは搭載されていませんが、マザーボード上の他の集積回路は、互換性のために8042チップの機能をエミュレートします。そのため、現在ではキーボードのプログラミングは、まだ8042のプログラミング方法を使用しています。

## 2.4.5 シリアルコントロールカード

### 1. 非同期式シリアル通信の原理

2台のコンピューター/機器がデータを交換する、すなわち通信は、人が話すのと同じ言語を使わなければならない。コンピュータ通信の用語では、コンピュータ／機器とコンピュータ／機器の間の「言語」を通信プロトコルと呼んでいます。通信プロトコルは、有効なデータ長の単位を送信するためのフォーマットを規定しています。通常、このフォーマットを「フレーム」という言葉で表現します。また、通信当事者が送受信の順番を決定したり、一部のエラー検出動作を行うために、必要なデータに加えて、同期やエラー検出に使用する他の情報も、例えば、データ情報の送信開始前に、送信される1フレームの情報に含まれます。図2-8のように、最初に開始/同期または通信制御情報を送信し、必要なデータ情報を送信した後に、いくつかの検証情報を送信します。

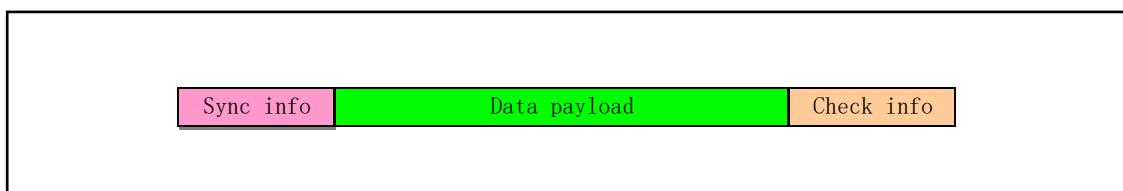


Figure 2-8 The general structure of communication frames

シリアル通信とは、ビット単位のデータストリームを1ビットずつ回線で伝送する通信方式のこと。シリアル通信は、非同期型シリアル通信と同期型シリアル通信に分類される。両者の主な違いは、送信時に同期させる通信単位（フレーム）の長さの違いである。非同期シリアル通信は、1文字を1通信単位または1フレームとして伝送し、同期シリアル通信は、複数の文字またはバイトの並びを1フレームのデータとして伝送する。人と人との対話に例えれば、非同期通信は2人の会話のスピードが遅いようなものだ。話すときは「語呂合わせ」で、一語一語話した後に任意の長さで一時停止することができる。一方、同期通信は、2者間の会話を一貫した文章で行うようなものです。実際に伝送単位を1ビット（文字で！）にしてみると、1文字の非同期シリアル通信も、同時送信のクロック信号の同期送信とみなすことができる。通信の方法。

## 2. 非同期式シリアル伝送フォーマット

非同期シリアル通信のフレームフォーマットを図2-9に示す。1文字の伝送は、スタートビット、データビット、パリティビット、ストップビットで構成されます。スタートビットは同期の役割を果たしており、値は常に0です。データビットは、実際に送信されるデータ、つまり1文字のコードです。データビットの長さは5~8ビットです。パリティビットはオプションで、プログラムによって設定されます。ストップビットは常に1で、プログラムによって1ビット、1.5ビット、2ビットに設定できます。通信が情報の送信を開始する前に、双方が同じフォーマットに設定されている必要があります。データビットとストップビットの数が同じであれば。非同期通信の仕様では、送信1をMARK、送信0をSPACEと呼んでいます。そのため、以下の説明ではこの2つの用語を使用します。

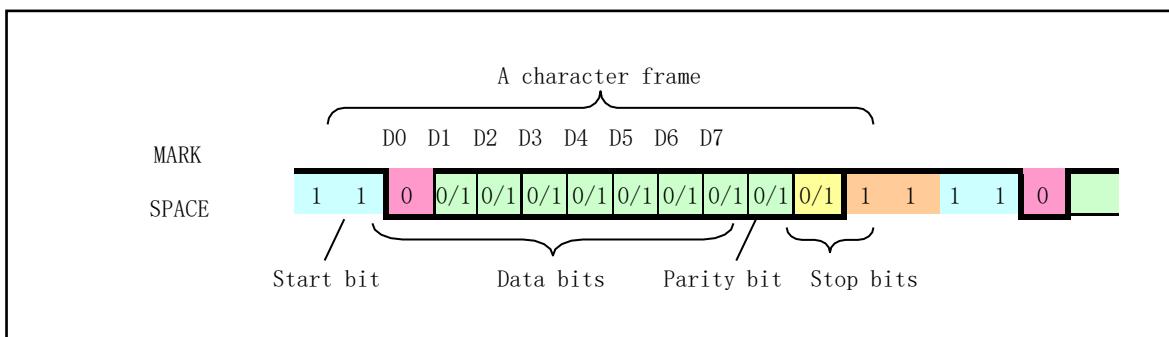


Figure 2-9 Asynchronous serial communication character transmission format

データ送信がない場合、送信者はMARK状態となり、連続して1を送信します。データを送信する必要がある場合、送信者はまず、ビット間隔のスペーススタートビットを送信する必要があります。スペース番号を受信した後、受信者は送信者との同期を開始し、その後のデータを受信します。プログラムでパリティビットが設定されている場合は、データ送信後にパリティビットを受信する必要があります。最後はストップビットです。文字フレームを送信した後、すぐに次の文字フレームを送信する場合と、パスワードを一時的に送信し、しばらくしてから文字フレームを送信する場合があります。

キャラクタフレームを受信する際、受信機は次の3つのエラーのいずれかを検出することができます。(1)パリティエラー。この時、プログラムは相手に文字の再送を依頼しなければなりません。この

エラーは、プログラムが受信速度よりも遅い速度で文字を取り込んでいるために発生します。この場合、プログラムを修正して、文字の周波数の取得を高速化する必要があります。 (3)

フレームフォーマットが正しくないこのエラーは、受信を要求されたフォーマット情報が正しくない場合に発生します。例えば、空の番号を受信した場合

ストップビットを受信すべき時に通常、このようなエラーは、回線の干渉を除く、両者のフレームフォーマットの違いによって発生します。

### 3. シリアルコントローラ

シリアル通信を実現するために、PCには通常、RS-232Cに準拠したシリアルインターフェースが2つ搭載されており、UART (Universal Asynchronous Receiver/Transmitter) で構成されたシリアルコントローラを用いて処理を行います。シリアルデータの送受信を行います。PCのシリアルインターフェースには、通常25ピンのDB-25または9ピンのDB-9コネクタが使用されており、主にMODEM機器を接続して動作させるために使用されています。そのため、RS-232C規格では多くのMODEM専用インターフェースピンが規定されています。

以前のPCは全てナショナルセミコンダクター社のNS8250またはNS16450のUARTチップを使用しています。現在のPCでは、16650Aとその互換チップを使用していますが、NS8250/16450チップとの互換性はあります。NS8250/16450と16650Aの主な違いは、16650AチップがFIFO転送もサポートしていることです。このモードでは、UARTは最大16文字の送受信を行った後にのみ割り込みを発生させることができます。システムやCPUの負担を軽減することができます。PCの電源を入れると、RESET信号がNS8250のMRピンを通過して、UARTの内部レジスタと制御ロジックをリセットします。その後、UARTを使用したい場合は、初期プログラミング操作を行い、UARTの動作ボーレート、データビット、動作モードを設定する必要があります。

## 2.4.6 ディスプレイ制御

IBM PC/ATおよびその互換機では、カラーおよびモノクロのビデオカードが使用できる。IBMの初期のPCビデオシステム規格には、モノクロのMDA規格やカラーのCGA規格のほか、EGAやVGA規格がある。後発の高機能グラフィックカード（現在のAGPグラフィックカードを含む）は、いずれもグラフィック処理速度やスマートアクセラレーション処理能力が極めて高いが、いずれもこれらの初期規格に対応している。Linux 0.1xのOSでは、これらの規格でサポートされているテキスト表示方法のみを採用しています。

### 1. MDAディスプレイ規格

モノクロディスプレイアダプタMDA (Monochrome Display Adapter) は、モノクロ表示のみ対応しています。また、独自のテキスト文字表示モード (BIOS表示モード7) にのみ対応しています。画面表示の仕様は、80列×25行（列番号x=0～79、行番号y=0～24）で、合計2000文字を表示することができます。1文字に1つの属性バイトが付いているので、1画面（1フレーム）を表示するのに4KBが必要となる。偶数アドレスバイトには文字コードが、奇数アドレスバイトには表示属性が格納される。MDAカードには8KBのディスプレイメモリが搭載されています。PCのメモリアドレス範囲には、0xb0000から始まる8KBの空間（0xb0000～0xb2000）が占有されます。ディスプレイの画面番号が video\_num\_lines = 25、列数が video\_num\_columns = 80 の場合、画面の列の行値 x, y に位置する文字や属性のメモリ上の位置は次のようにになります。

---

```
Character byte position = 0xb0000 + video_num_columns * 2 * y + x * 2;
Attribute byte position = Character byte position + 1;
```

---

MDAのモノクロ文字表示モードでは、各文字の属性バイトフォーマットを表2-4に示す。このうち、D7を1にすると文字が点滅し、D3を1にすると文字が強調表示される。基本的には、図2-10のカラー・テキスト文字の属性バイトと同じであるが、色は白（0x111）と黒（0x000）の2色のみである。それらを組み合わせた効果を表に示します。

2. Table 2-4 Monochrome display character attribute byte settings

Background color D6D5D4	Foreground color D2D1D0	Attribute value No flash low	display effect	example
0 0 0	0 0 0	0x00	Characters are not visible.	
0 0 0	1 1 1	0x07	White characters displayed on a black background (normal display).	Normal
0 0 0	0 0 1	0x01	White underlined characters displayed on a black background.	Underline
1 1 1	0 0 0	0x70	Black characters displayed on a white background (inverse).	Reverse
1 1 1	1 1 1	0x77	Show white squares.	■

### 3. CGAディスプレイ規格

カラーグラフィックアダプターCGA (Color Graphics Adapter) は、7種類のカラー・グラフィック表示に対応しています (BIOS表示0--6)。80カラム×25カラムのテキスト文字表示モードでは、モノクロ2種類、カラー16種類の表示モードがあります (BIOS表示モード2--3)。CGAカードには標準で16KBのディスプレイメモリ (メモリアドレス範囲0xb8000～0xbc000) が搭載されているので、合計4フレーム分の表示情報を保存することができます。同様に、1フレームあたり4KBの表示メモリには、偶数アドレスのバイトには文字コードが、奇数アドレスのバイトには文字の表示属性が格納されています。しかし、console.cプログラムでは、8KBの表示メモリ (0xb8000～0xba000) しか使用していません。CGAカラー・テキスト表示モードでは、各表示文字の属性バイトフォーマットの定義を図2-10に示す。

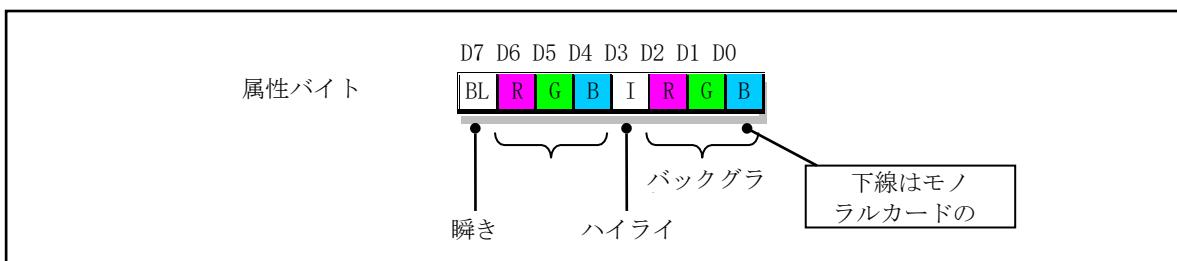


Figure 2-10 Character attribute format definition

モノクロ表示と同様に、D7を1にすると表示文字が点滅し、D3を1にすると文字が強調表示され、D6、D5、D4およびD2、D1、D0の各ビットを組み合わせることで8色の表示が可能となります。前景ビットと高輝度ビットの組み合わせで、残りの8色の文字色を表示することができます。これらの組み合わせの色を表2-5に示します。

4. Table 2-5 Foreground color and background color (left half)

I R G B	Value	Color name	I R G B	Value	Color name
0 0 0 0	0x00	Black	1 0 0 0	0x08	Dark grey
0 0 0 1	0x01	Blue	1 0 0 1	0x09	Light blue
0 0 1 0	0x02	Green	1 0 1 0	0x0a	Light green
0 0 1 1	0x03	Cyan	1 0 1 1	0x0b	Light cyan
0 1 0 0	0x04	Red	1 1 0 0	0x0c	Light red
0 1 0 1	0x05	Magenta	1 1 0 1	0x0d	Light magenta
0 1 1 0	0x05	Brown	1 1 1 0	0x0e	Yellow
0 1 1 1	0x07	Light grey	1 1 1 1	0x0f	White

## 5. EGA/VGAディスプレイ規格

EGA(Enhanced Graphics Adapters)やVGA(Video Graphics Adapters)では、MDAやCGA対応に加えて、グラフィックスの他の表示拡張にも対応しています。MDAやCGA対応の表示モードでは、占有するメモリアドレスの開始位置や範囲は同じである。ただし、EGA/VGAでは最低でも32KBの表示メモリが標準装備されている。0xa0000から始まる物理メモリのアドレス空間がグラフィカルに占有されます。

### 2.4.7 フロッピーディスクとハードディスクのコントローラー

PCのフロッピーディスク制御サブシステムは、フロッピーディスクとフロッピーディスクドライブで構成されています。フロッピーディスクはプログラムやデータを保存することができ、持ち運びも容易なため、フロッピーディスクドライブは古くからPCの標準的な構成機器の一つとなっている。ハードディスクもディスクとドライブで構成されているが、通常、ハードディスクの金属製ディスクはドライブに固定されており、取り外すことはできない。ハードディスクは記憶容量が大きく、読み書きの速度が非常に速いため、パソコンの中では最大の外部記憶装置であり、通常、外部ストレージとも呼ばれる。フロッピーディスクもハードディスクも、情報の保存には磁気媒体を使用しており、保存の動作も同様である。そこで、ここではハードディスクを例に挙げて、その仕組みを簡単に説明します。

ディスクにデータを保存する基本的な方法は、磁化した後にディスクの表面に磁気媒体の層を設けることである。フロッピーディスクではポリエステルフィルムを、ハードディスクでは金属アルミニウム合金を基板として使用している。フロッピーディスクには、ポリエステルフィルムのディスクが入っている。フロッピーディスクにはポリエステルフィルム製のディスクが入っており、上段と下段のヘッドでディスクの両面にデータを読み書きする。ディスクの回転速度は約300rpmである。容量1.44MBのフロッピーディスクの場合、ディスクの両面は80トラックに分かれており、各トラックには18セクタのデータが格納できるので、 $2 \times 80 \times 18 = 2880$ セクタあることになる。表2-6は、いくつかの一般的なタイプのフロッピーディスクの基本パラメータを示しています。

Table 2-6 Common floppy disk basic parameters

Disk type and capacity	tracks/face	Sectors/tracks	Total sectors	Rotate speed (r/min)	Data transmission rate (Kbps)
5¼ inch 360KB	40	9	720	300	250
3½ inch 720KB	80	9	1440	360	250
5¼ inch 1.2MB	80	15	2400	360	500
3½ inch 1.44MB	80	18	2880	360	500
3½ inch 2.88MB	80	36	5760	360	1000

ハードディスクは通常、少なくとも2枚以上のメタルディスクを含むため、2つ以上の読み書きヘッドを持つ。例えば、2枚のディスクを含むハードディスクには4つの物理ヘッドがあり、4枚のディスクを含むディスクには8つの読み取り/書き込みヘッドがあります。図2-

11参照。ハードディスクの回転速度は通常4500rpm～10000rpmと高速なので、ハードディスクのデータ転送速度は通常数メガビット/秒まで可能である。

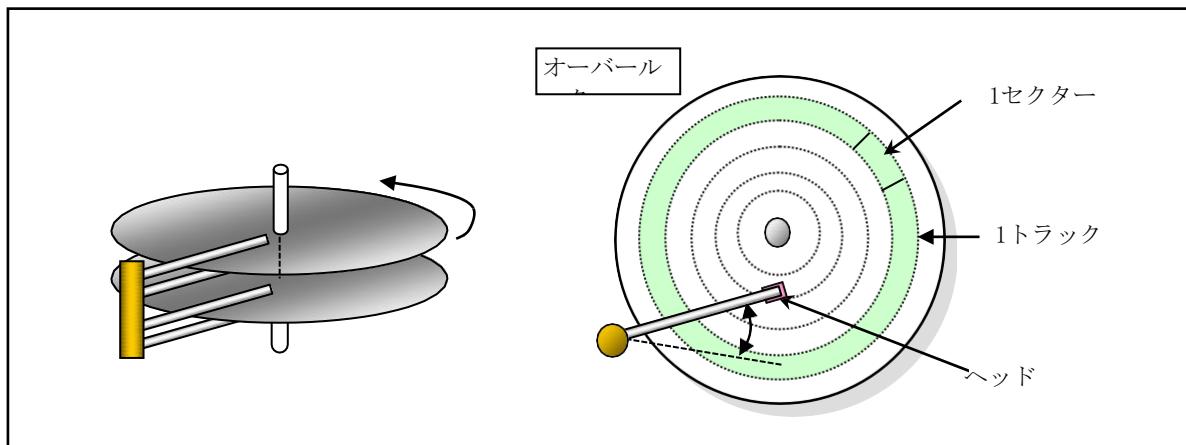


図2-11 2枚のディスクを持つ典型的なハードディスクの内部構造

ディスク面上の磁気ヘッドは、それぞれ読み出しコイルと書き込みコイルを持っている。データの読み取り動作では、まずヘッドが回転するディスク上のある位置に移動される。磁気ディスクが回転すると、磁気媒体は磁気ヘッドに対して一様な速度で移動するため、磁気ヘッドは実際に磁気媒体に磁力線を切る。その結果、誘導により読み取りコイルに電流が発生します。ディスク表面の残留状態の方向によって、コイルに誘導される電流の方向も異なるので、ディスクに記録されている0と1のデータが読み出され、ディスクからビットストリームを順次読み出すことができるようになります。ヘッドが読み取った各トラックは、情報を格納するための特定のフォーマットを持っているので、ディスク回路は、読み取ったビットストリームの中のフォーマットを認識することで、トラック上の各セクタのデータを判別して読み取ることができる。図2-

12を参照してください。その中で、GAPは分離に使われるインターバルフィールドである。通常、GAPは0の12バイトである。各セクタのアドレスフィールドには、該当するセクタのシリンド番号、ヘッド番号（面番号）、セクタ番号が格納されているので、アドレスフィールドのアドレス情報を読み取ることで、セクタを一意に判別することができる。

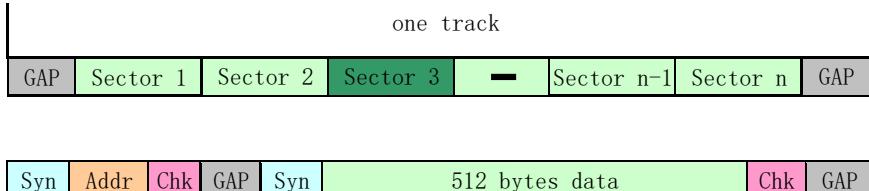


Figure 2-12 Disc track format

ディスクにデータを読み書きするには、ディスクコントローラを使う必要がある。ディスクコントローラは、CPUとドライバの間の論理的なインターフェース回路である。CPUからの要求コマンドを受け取り、シーク、リード/ライト、制御信号をドライバーに送り、データのフローパターンを制御・変換する。コントローラとドライバの間で転送されるデータには、図2-12のセクタのアドレス情報とタイミング・クロック情報が含まれています。コントローラは、これらのアドレス情報や一部のエンコード、デコードなどの制御情報を実際の読み書きデータから分離する必要があります。また、ドライバとのデータ転送はシリアルビットストリームなので、コントローラはパラレルバイトデータとシリアルビットストリームデータを変換する必要があります。

PC/AT機のFDC (Floppy Disk Controller) は、NECの「μPD765」またはその互換チップを使用しています。これは主に、図2-13に示すように、CPUから発行されたコマンドを受信し、コマンドの要求に応じて各種のハードウェア制御信号をドライバに出力するために使用されます。読み書き動作を行う際には、データ変換（ストリング・パラレル）、エンコード、ベリファイなどの動作を行い、ドライブの動作状態を常に監視する必要があります。

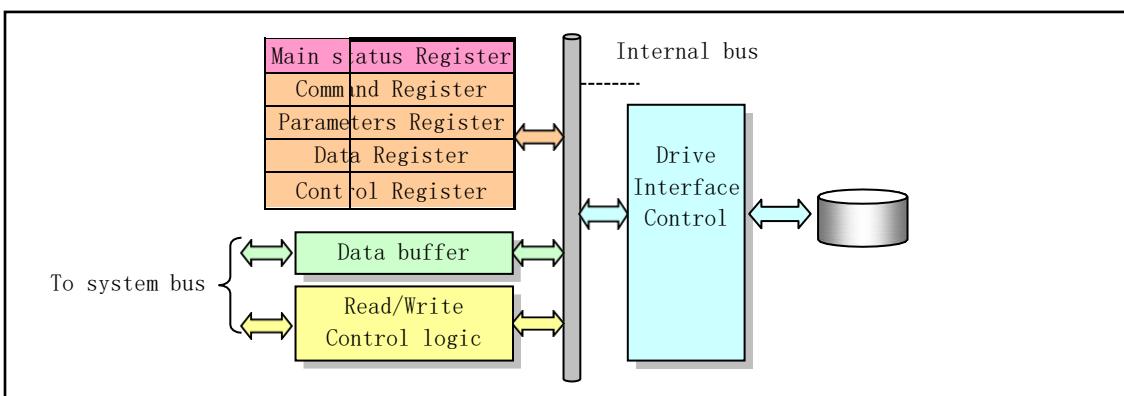


Figure 2-13 Disk controller internals

ディスクコントローラのプログラミングは、I/Oポートを介してコントローラ内の関連レジスタの内容を設定し、レジスタを介して動作の結果情報を得るというものである。セクターデータの転送に関しては、フロッピーディスクコントローラはPC/ATのハードディスクコントローラとは異なる。フロッピーディスクコントローラ回路はDMA信号を使用するため、データ転送にはDMAコントローラを使用

する必要があります。ATハードディスクコントローラでは、DMAコントローラを介さずに、高速データブロックを使って転送します。フロッピーディスクは比較的ダメージ（カビやキズ）に弱いため、現在ではフロッピーディスクドライブはコンピューターに配備されていない。代わりに、大容量で持ち運びに便利なUSBフラッシュドライブが使われている。

## 2.5 概要

ハードウェアは、オペレーティングシステムの基本的なプラットフォームです。オペレーティングシステムが動作するハードウェア環境を理解することは、その上で動作するオペレーティングシステムを深く理解するための必要条件です。本章では、従来のマイクロコンピュータのハードウェア構成をもとに、マイクロコンピュータの各主要部分を簡単に紹介します。次章では、Linuxカーネルが使用している2つのアセンブリ言語構文とそれに関連するコンパイラをソフトウェアの観点から説明するとともに、カーネルが使用しているGNU gcc構文拡張の内容を紹介する。

## 3カーネルのプログラミング言語と環境

言語コンパイル処理とは、人間が理解できる高級言語を、コンピューターのハードウェアが理解して実行できるバイナリの機械語命令に変換する処理である。この変換プロセスでは、通常、効率の悪いコードが生成されるため、高い動作効率が求められるコードや性能への影響が大きいコードの一部は、通常、低レベルのアセンブリ言語で直接記述するか、高級言語のコンパイルで生成されたアセンブラーを使用する。その後、手動で最適化のための修正を行います。本章では、Linuxで使用されているプログラミング言語、オブジェクトファイルフォーマット、コンパイル環境について説明します。

0.12 カーネルのソースコード主な目的は、Linux

0.12カーネルのソースコードを読むために必要なアセンブリ言語とGNU

C言語拡張の知識を提供することです。まず、as86とGNU

asアセンブラーの構文と使い方をより詳しく紹介します。次に、GNU

C言語のインラインアセンブリ、ステートメント式、レジスタ変数、インライン関数など、カーネルソースコードにおけるC言語拡張を使用します。導入し、C言語とアセンブリ関数の相互呼び出しの仕組みについて詳しく説明しています。オブジェクトファイルのフォーマットを理解することは、アセンブラーの動作を理解する上で最も重要な前提条件の一つであるため、2つのアセンブリ言語を紹介する際には、まずターゲットファイルの基本的なフォーマットを簡単に説明した上で、Linux

0.12については、この章の後半で詳しく説明します。システムで使用されているa.outオブジェクトファイルフォーマット。最後に、Makefileの使用方法について簡単に説明します。

本章の内容は、Linuxカーネルのソースコードを読む際の参考情報です。そのため、本章の内容をざっと見てから次の章を読み、問題が発生したときに本章を参照することができます。

### 3.1 as86 アセンブラー

Linux 0.1x では、2 種類のアセンブラーが使用されています。1 つは as86 アセンブラーで、コンパニオンの ld86 リンカを使って 16 ビットのコードを生成します。もう 1 つは GNU アセンブラー gas(as) で、GNU ld リンカを使って結果のオブジェクトファイルをリンクします。ここではまず as86 アセンブラーの使い方を説明し、アセンブラーの使い方は次のセクションで説明します。

as86 と ld86 は、MINIX-386 の主要開発者の一人である Bruce Evans 氏によって書かれた Intel 8086, 80386 アセンブラー用のコンパイラとリンカです。Linus が Linux カーネルの開発を始めたときに、すでに Linux システムに移植されています。80386 プロセッサ用の 32 ビットコードをコンパイルすることができるが、Linux システムでは、16 ビットのブートセクタプログラム boot/bootsect.s と、リアルモードの初期設定プログラム boot/setup.s のバイナリ設定コードを作成するためにのみ使用されている。このコンパイラは、高速かつコンパクトで、マクロやより多くのエラー検出方法など、GNU GAS にはない機能を備えています。しかし、このコンパイラの構文は、GNU

asのアセンブリコンパイラの構文とは互換性がなく、MicrosoftのMASM、BorlandのTurbo ASM、NASMなどのアセンブラの構文に近いものとなっています。これらのアセンブラはすべてインテルのアセンブリ言語構文を使用しています（例：オペランドの順序がGNU asと逆など）。

as86の構文は、MINIXシステムのアセンブリ言語構文をベースにしており、MINIXシステムのアセンブリ構文は、PC/IXシステムのアセンブラ構文をベースにしています。PC/IXは、昔、インテル8086のCPUで動いていたUN\*XのOSです。アンドリュー・S・タネンバウムは、PC/IXシステム上でMINIXシステムを開発した。

ブルース・エヴァンスは、32ビット版MINIXオペレーティングシステムの主要なリビジョンプログラマーの1人です。Linuxの創始者であるリナス・トーバルズの親しい友人でもある。Linuxカーネル開発の初期に、LinusはBruce EvansからUNIX系OSについて多くのことを学んだ。MINIX OSの不備も、仲良しの2人がお互いに議論した結果なのです。このようなMINIXの欠点は、リナス氏がインテル80386アーキテクチャ上で新しいコンセプトのOSを開発するきっかけとなった主な要因のひとつにすぎない。リナスはかつてこう言いました。"Bruce is my hero"という言葉があるように、Linux Evans氏との間にも密接な関係があると言えるだろう。

このコンパイラとリンクのソースコードは、FTP サーバ ftp.funet.fi または Web サイト www.oldlinux.org からダウンロードできます。最近の Linux システムでは、例えば dev86-0.16.3-8.i386.rpm のように、as86/ld86 を含む RPM パッケージを直接インストールすることができます。Linux システムでは as86 と ld86 は、前述の 2 つの 16 ビットアセンブラ bootsect.s と setup.s のコンパイルとリンクにのみ使用されるため、ここではこれら 2 つのプログラムで使用されるアセンブラの構文とアセンブラコマンド（アセンブラ）についてのみ説明します。indicator) の役割と使い方を説明します。）

### 3.1.1 as86のアセンブリ言語の構文

アセンブラは、低レベルのアセンブリ言語プログラムを、機械語を含むバイナリプログラムまたはオブジェクトファイルにコンパイルするように設計されています。アセンブラは、入力されたアセンブリ言語プログラム（srcfileなど）をオブジェクトファイル（objfile）にコンパイルします。アセンブラのコマンドラインの基本的な形式は次のとおりです。

---

```
as [options] -o objfile srcfile
```

---

オプションは、指定されたフォーマットと設定でターゲットファイルを作成するために、コンパイルプロセスを制御するために使用されます。入力されるアセンブリ言語プログラムsrcfileは、テキストファイルです。ファイルの内容は、改行文字で終わる一連のテキスト行で構成されていなければなりません。GNU

asはセミコロンを使用して1行に複数のステートメントを含めることができます。アセンブリ言語プログラムをプログラミングする際には、1行に1つのステートメントしか含めないのが一般的です。

ステートメントには、スペース、タブ、改行のみを含む空行のほか、代入ステートメント（または定義ステートメント）、擬似演算子ステートメント、機械語命令ステートメントなどがあります。代入文は、記号や識別子に値を割り当てるために使用する。識別子の後に等号を付け、その後に式を続けて構成されており、例えば"BOOTSEG = 0x07C0

"のように。疑似演算子文は、アセンブラーが使用する指標で、通常はコードを生成しません。疑似オペコードと 0 個以上のオペランドで構成されます。各オペコードは、ドット文字'!'で始まります。ドット文字'!'自体は、コンパイル時の位置カウンタを表す特別な記号です。その値は、ドット記号が現れる機械語命令の最初のバイトのアドレスです。

機械語命令文は、実行可能な機械語命令のニーモニックであり、操作コードと0個以上のオペランドで構成されます。また、ステートメントの前には、ラベルを付けることができます。ラベルとは、識別子の後にコロン「:」を付けたものです。アセンブラーはコンパイル時にラベルを見つけると、そのラベルに現在の位置カウンタの値を割り当てます。したがって、アセンブリステートメントは通常、ラベル（オプション）、命令ニーモニック（命令名）、オペランドの3つのフィールドで構成されています。ラベルは、命令の第1フィールドにあります。ラベルは命令の最初のフィールドにあり、その場所のアドレスを表し、通常はジャンプ命令の目的地を示します。最後に、コメントで始まるコメント欄を追うこともできます。

アセンブラーのコンパイルによって生成されるオブジェクトファイル objfile  
には、通常、テキストセグメント (.text) 、データセグメント (.data) 、および未初期化データセグメント (.bss) の少なくとも 3  
つのセグメントまたはセクションが含まれています。テキスト・セグメント（またはコード・セグメント）は初期化されたセグメントで、通常はプログラムの実行コードと読み取り専用のデータを含みます。データ・セグメントも初期化されたセグメントで、読み取り/書き込みデータを含みます。初期化されていないデータセグメントは

は初期化されていないセグメントです。通常、アセンブラーが生成する出力オブジェクトファイルでは、このセグメントのためのスペースは確保されませんが、オブジェクトファイルが実行プログラムにリンクされる際に、OSはセグメントの内容を0に初期化します。コンパイル時に、アセンブリ言語プログラムのコードやデータを生成するステートメントは、これら3つのセグメントのいずれかにコードやデータを生成します。コンパイルされたバイトは、「.text」セクションから順に格納されます。書き込まれたセグメントを変更するには、セグメント制御疑似演算子を使います。ターゲットファイルのフォーマットについては、後述の「Linux  
オブジェクトファイルフォーマット」の項で詳しく説明します。 0.12

### 3.1.2 as86のアセンブリプログラム

以下では、簡単なフレームワークのサンプルプログラムboot.sを使って、as86アセンブラーの構造とプログラム内のステートメントの構文を説明し、コンパイルリンクと実行方法を示します。最後にas86とld86の使用方法とコンパイルオプションを使用します。そのサンプルプログラムを以下に示します。このサンプルはbootsect.sのフレームワークプログラムで、ブートセクタコードをコンパイルして生成するものです。特定のステートメントの使用方法を示すために、意図的に無意味な20行のステートメントを追加しています。

---

```

1 !
2 ! boot.s -- bootsect.s framework program. Replace 1 character in the string msg1
3 ! with code 0x07 and display it on the first line of the screen.
4 .globl begtext, begdata, begbss, endtext, enddata, endbss ! Global id used for ld86 links
5 .text ! Text segment
6 begtext:
7 .data ! Data segment
8 begdata:
9 .bss ! Uninitialized data segment
10 begbss:
11 .text ! Text segment
12 BOOTSEG = 0x07c0 ! Original segment address for the loaded bootsect code.
13
14 entry start ! Inform the linker the program starts executing from here.
15 start:
16     jmpi    go,BOOTSEG ! Jump between segments. INITSEG indicates the jump
                           ! section address, the label go is the offset address.
17 go:      mov     ax,cs ! The value of the segment register cs -->ax is used
18         mov     ds,ax ! to initialize the data segment registers ds and es.
19         mov     es,ax
20         mov     [msg1+17],ah ! 0x07-> Replaces 1 dot in the string and beep once.
21         mov     cx,#20 ! 20 chars displayed, including cr & lf.
22         mov     dx,#0x1004 ! String displayed on screen at line 17, column 5.
23         mov     bx,#0x000c ! Character display attribute (red).
24         mov     bp,#msg1 ! Point to a string (required by interrupt call).
25         mov     ax,#0x1301 ! Write string and move cursor to the end of the string.
26         int    0x10 ! The BIOS interrupt call 0x10, function 0x13, subfunc 01.
27 loop1:   jmp    loop1 ! Dead cycle.
28 msg1:    .ascii "Loading system ..."! Message to be displayed, total of 20 ASCII characters.
29 .byte 13,10
30 .org 510 ! Indicates statement is stored from address 510 (0x1FE).
31     .word 0xAA55 ! Active boot sector flag, used by the BIOS.
32 .text
33 endtext:
34 .data
35 enddata:
36 .bss
37 endbss:

```

---

まず、プログラムの機能を紹介し、その後、各ステートメントの役割を詳しく説明します。このプログラムは、単純なブートセクタープログラムです。生成された実行プログラムをコンパイル、リンクすることで、コンピュータの起動に直接使用するフロッピーディスクの第1セクターに配置することができます。起動すると、画面の17行目と5列目に「Loading system ...」という赤い文字列が表示され、カーソルが1行下に移動します。その後、プログラムはコードライン27で無限にループします。

プログラムの最初の3行はコメント文です。as86のアセンブリ言語プログラムでは、感嘆符「！」またはセミコロン「;」で始まるステートメントの後にコメント文が続きます。コメント文は、任意の文の後に置くことも、新しい行から始めることもできます。

4行目の「.globl」は、アセンブリ指示子（またはアセンブリ指示子、疑似演算子）です。アセンブ

ラ指示文は一文字「・」で始まり、コンパイル時にはコードを生成しません。アセンブラー指示文は、疑似オペコードとそれに続く0個以上のオペランドで構成されます。例えば、4行目の「globl」は疑似オペコードで、それに続くラベル「begtext」begdata,  
 「begbss」などはそのオペランドです。ラベルは識別子の後にコロンを付けたもので、例えば6行目の'begtext:'のようになります。ただし、ラベルを参照する際にはコロンを取る必要はありません。

通常、アセンブラーは様々な疑似演算子をサポートしていますが、ここでは、Linuxシステムのbootsector.sとsetup.sのアセンブリ言語プログラムでよく使われるas86の疑似演算子についてのみ説明します。

`.globl` 疑似演算子は、後続のラベル識別子が外部またはグローバルであることを定義するために使用され、使用されない場合でも導入が必須となります。

5行目から11行目で定義された3つのラベルに加えて、「.text」、「.data」、「.bs」という3つの疑似演算子が定義されています。これらはそれぞれ、ターゲットファイルに3つのセグメント（テキストセグメント、データセグメント、未初期化データセグメント）を生成するアセンブラプログラムに対応しています。`.text` はテキスト・セグメントの開始位置を特定してテキスト・セグメントに切り替え、「.data」はデータ・セグメントの開始位置を特定して現在のセグメントをデータ・セグメントに切り替え、「.bs」は初期化されていないデータ・セグメントの開始位置を特定して現在のセグメントをbsセグメントに切り替えています。つまり5--

11行目は、各セグメントにラベルを定義し、テキストセグメントに切り替えて次のコードを書き始めるためのものです。ここでは、3つのセグメントがすべて同じ重複したアドレス範囲に定義されているので、サンプルプログラムは実際にはセグメント化されていません。

12行目では、代入文「BOOTSEG = 0x07c0」が定義されています。等号「=」（または記号「EQU」）を使って、識別子「BOOTSEG」が表す値を定義しているので、この識別子は記号定数と呼ぶことができる。この値は、C言語の文言と同様に、10進数、8進数、16進数で使用できます。

14行目の識別子'entry'は、リンク先が生成する実行ファイルに、それ以降に指定されたラベル'star'を強制的に含めるための予約キーです。通常、複数のオブジェクトファイルをリンクして実行ファイルを生成する際には、デバッグのためにキーワードentryでアセンブラーのエントリーラベルを指定する必要があります。しかし、今回の例やLinux カーネルの boot/bootsect.s、boot/setup.sアセンブラーでは、生成されるピュアバイナリの実行ファイルにシンボル情報を含めたくないで、このキーワードを省略することができます。

16行目にはセグメント間のファージャンプステートメントがあり、次の命令にジャンプします。BIOSが0x7c00の物理メモリにプログラムをロードしてそこにジャンプしたとき、CSを含むすべてのセグメントレジスタのデフォルト値は0、つまりCS:IP=0x0000:0x7c00です。そのため、ここではセグメント値0x7c0をCSに割り当てるために、セグメント間ジャンプステートメントを使用します。このステートメントが実行された後、CS:IP = 0x07C0:0x0005となります。次の2つのステートメントは、0x7c0セグメントを指すように、DSとESセグメントレジスタにそれぞれ値を割り当てます。これにより、プログラム内のデータ（文字列）のアドレス指定が容易になります。

20行目のMOV命令は、ahレジスタの0x7c0セグメント値の上位バイト（0x07）を、メモリ文字列msg1の最後の「・」の位置に格納するために使用します。この文字は、文字列が表示されたときに、BIOSの割り込みでビープ音を発生させます。この文は、主に間接オペランドの使い方を説明するために使われています。as86では、間接オペランドには角括弧のペアが必要です。他のアドレッシング方式では、次のようなものがあります。

---

```

! Direct register addressing. Jump to the address specified by bx, that is, copy bx to the IP.
    mov    bx, ax
    jmp    bx
! Indirect register addressing. The bx specifies the memory location as the address of the jump.
    mov    [bx], ax
    jmp    [bx]
! Put the immediate number 1234 into ax. Put the msg1 address value in ax.
    mov    ax, #1234
    mov    ax, #msg1
! Absolute addressing. Put the contents of the memory address 1234 (msg1) into ax.
    mov    ax, 1234
    mov    ax, msg1
    mov    ax, [msg1]
! Index addressing. Put the value at the memory location indicated by the second operand into ax.
    mov    ax, msg1[bx]
    mov    ax, msg1[bx*4+si]

```

---

21～25行目のステートメントは、即値データを適切なレジスタに入れるために使用されます。この#の前には即値の数字を置かなければならず、そうしないとメモリアドレスとして使用され、絶対アドレス指定のステートメントになってしまいます。上記の例を参照してください。また、ラベル（msg1など）のアドレス値をレジスタに入れるときは、前に「#」をつけないと、msg1のアドレスのレジスタになってしまいます！

26行目は、BIOSの画面表示割り込みコールint

0x10です。ここでは、その関数19、サブ関数1が使用されています。この割り込みの目的は、指定された位置のスクリーンに文字列（msg1）を書き込むことです。レジスタcxは文字列の長さの値、dxは表示位置の値、bxは表示使用文字属性、es:bpは文字列を指しています。

27行目は、現在の命令にジャンプするジャンプ文です。つまり、これは無限ループ文なのです。ここで無限ループ文を使うのは、表示された内容が削除されずに画面に残るようにするためです。デッドループ文は、アセンブラプログラムをデバッグするときによく使われます。

28-

29行目では、文字列msg1を定義しています。文字列を定義するには、疑似演算子「.ascii」を使い、文字列を二重引用符で囲む必要があります。また、疑似演算子「.asciiz」は、文字列の後に自動的にNUL L(0)文字を追加します。また、29行目では、キャリッジリターンとラインフィード（13, 10）の文字を定義しています。文字を定義するには、疑似演算子「.byte」を使用し、文字を一重引用符で囲む必要があります。例えば、以下のようになります。"D".もちろん、例のように文字のASCIIコードを直接書くこともできます。

30行目の疑似オペレータ文「.org」は、現在のアセンブラの位置を定義します。このステートメントは、アセンブラのコンパイル時に、現在のセグメントの位置カウンタの値を疑似オペレータステートメントで指定された値に調整します。この例のプログラムでは、このステートメントが位置カウンタを510に設定し、有効なブートセクタフラグワード0xAA55をここに配置します（31行目）。擬似演算子「.word」は、現在の位置にダブルバイトのメモリオブジェクト（変数）を定義するために使用され、その後に数値や式を続けることができます。コードもデータもないで、ここからboot.sでコンパイルされた実行ファイルはちょうど512バイトになるはずだと判断できます。

32行目--37行目は、3つのセグメントのそれぞれに、さらに3つのラベルを配置しています。3

つのセグメントの終了位置を示すために使用します。この設定は、次のような場合に、各モジュールの各セグメントの開始と終了を区別するために使用できます。

複数のターゲットモジュールをリンクすることができます。カーネル内の `bootsec.s` と `setup.s` はそれぞれ別個にコンパイル、リンクされているため、純粋なバイナリファイルの生成を期待しても、他のオブジェクトモジュールファイルとはリンクしません。そのため、サンプルプログラムでは、各セグメントの疑似プログラムを宣言しています。文字 (`.text`、`.data`、`.bss`) はすべて省略可能です。つまり、プログラムの4行目～11行目、32行目～37行目をすべて削除しても、リンクをコンパイルすれば正しい結果が得られます。

### 3.1.3 As86アセンブリ言語プログラムのコンパイルとリンク

次に、リンクサンプルプログラム `boot.s`

をコンパイルして、起動に必要なブートセクタプログラムを生成する方法を示します。上記のサンプルプログラムのコンパイルとリンクには、以下の最初の2つのコマンドが必要です。

---

```
[/root]# as86 -O -a -o boot.o boot.s           // Compile. Generate the target file.
[/root]# ld86 -O -s -o boot boot.o             // link. Remove symbol information.
[/root]# ls -l boot*
-rwx--x--x  1 root      root      544 May 17 00:44 boot
-rw-----  1 root      root      249 May 17 00:43 boot.o
-rw-----  1 root      root     767 May 16 23:27 boot.s
[/root]# dd bs=32 if=boot of=/dev/fd0 skip=1    // Write to a floppy disk or Image file.
16+0 records in
16+0 records out
[/root]# _
```

---

その中で、1つ目のコマンドはas86アセンブリを使ってboot.sプログラムをコンパイルし、boot.oオブジェクトファイルを生成します。2番目のコマンドはリンカーld86を使ってターゲットファイルにリンク操作を行い、最後にMINIX構造の実行ファイルbootを生成します。オプションの'-'は8086の16ビットターゲットプログラムを生成するために、'-a'はGNU asやldのバーツと互換性のあるコードを生成することを指定するために使われます。's' オプションは、最後に生成された実行ファイルからシンボル情報を削除するよう linkerに指示するために使用する。'-o'は、生成される実行ファイルの名前を指定します。

lsコマンドを使って上に挙げたファイル名を見ればわかるように、最後に生成されたブートプログラムは、先に述べたように正確に512バイトではなく、32バイトの長さです。この32バイトは、MINIX実行ファイルのヘッダの構造です（構造の詳細な説明は「カーネルコンポーネントの作成」の章を参照）。このプログラムを使ってマシンを起動するためには、この32バイトを手動で削除する必要があります。このヘッダー構造を削除するにはいくつかの方法があります。

- バイナリエディタでブートプログラムの最初の32バイトを削除して保存します。
- 現在のLinuxシステム（RedHat 9など）でas86コンパイルリンカーを使用する場合、MINIXヘッダー構造を含まない純粋なバイナリ実行ファイルを生成するオプションがありますが、該当システムのオンラインユーザーマニュアル（man as86）を参照してください。
- Linuxシステムのddコマンドを使用する。

上記の3番目のコマンドは、ddコマンドを使ってブートの最初の32バイトを削除し、その出力を直接フロッピーディスクのイメージファイルまたはBochsシミュレーションシステムに書き込みます。(Bochs PCアナログシステムを使用してください。前章を参照してください)。このプログラムをBochsシミュレーション・システムで実行すると、図3-1のような画面が得られます。

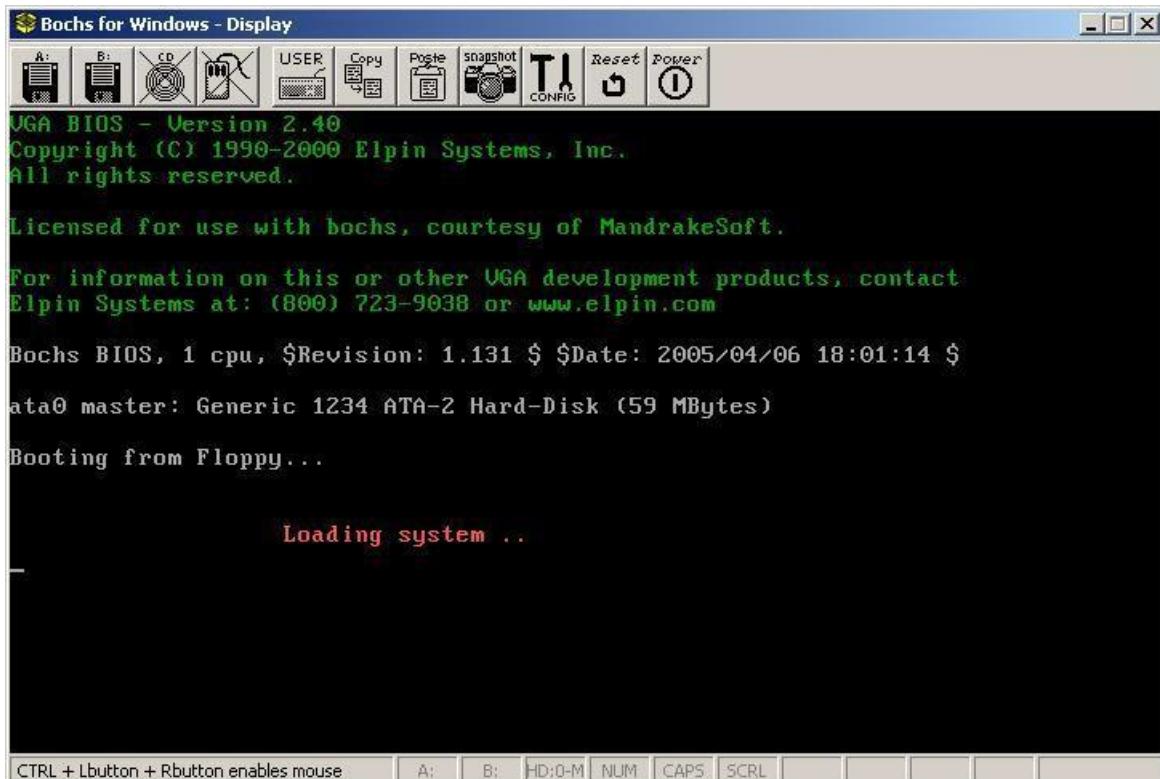


図3-1 Bochsシミュレーションシステムでのブートプログラムの実行

### 3.1.4 as86とld86の使用方法とオプション

as86とld86の使用方法とオプションは以下の通りです。

#### asの使い方とオプション

---

as [-O3agjuw] [-b [bin]]. [-lm [リスト]]。[-n 名前] [-o objfile] [-s sym] srcfile

デフォルト設定（以下のデフォルト以外のオプションのデフォルトはoffまたはnoneで、aフラグを指定しない場合は出力されません）。

-380386 の 32 ビット

出力を使用し、標準出力

に listDisplay します。

nameソースファイルの基本的な名前（つまり、「.」の後の拡張子は含まない）。

#### それぞれの選択肢の意味

-O16ビットのコードセグメントを使用する。

332ビットのコードセグメントを使用する。

-aGNU as, ldとの互換性オプションを開きます。

-bバイナリファイルを生成し、その後にファイル名を入力します。

-gグローバルシンボルのみをオブジェクトファイルに格納する。

-jすべてのジャンプ文をロングジャンプにします。

- 
- lリストファイルを生成し、その後にリストファイル名を入力します。
  - m リスト のマクロ定義を拡張します。
  - nモジュール名（ターゲットファイルへのソースファイル名の代わりに）が続きます。
  - oターゲットファイルを生成し、その後にターゲットファイル名（objfile）を入力します。
  - sシンボルファイルを作成し、その後にシンボルファイル名 を入力します。
  - u入力された未定義のセグメント のシンボルとして未定義のシンボルを使用する。
  - w警告メッセージは表示されません。
- 

### 1d リンカの使用構文とオプション。

Minixのa.outフォーマットを生成するバージョンについて。

```
1d [-03Mims[-]]... [-T textaddr] [-llib_extension] [-o outfile] infile...
```

GNU-Minixのa.outフォーマットを生成するバージョンです。

```
1d [-03Mimrs[-]]... [-T textaddr] [-llib_extension] [-o outfile] infile...
```

デフォルトの設定（以下のデフォルトを除き、他のオプションはデフォルトではオフまたはなし）。

    -0332ビット出力、  
outfilea.out形式出力。

    -016ビットのマジックナンバーを持つヘッダー構造を生成します。

    -1x オプションで i386 サブディレクトリを使用し、32 ビットのマジックナンバーを持つヘッダー構造を生成します。

    -MD リンクされたシンボルを標準出力デバイス に表示

    続けて、テキストベースのアドレス (strtoulに 適したフォーマットを使用) を入力します。

    -i命令とデータセグメント (I&D) を分離して出力。

    -1xリンクされたファイルリストにライブラリ /local/lib/subdir/libx.a を追加します。

    -mリンクされたモジュールを標準の出力デバイス に表示

    -o出力ファイル名 を指定します。

    -rさらなる再 配置に適した出力を生成します。

    -sターゲットファイル の全てのシンボルを削除します。

## 3.2 アセンブラーとしてのGNU

前節で紹介したas86アセンブラーは、カーネル内のboot/bootsect.sのブート・セクタ・プログラムと、リアル・モードのboot/setup.sのセットアップ・プログラムのコンパイルにのみ使用されます。カーネル内の他のすべてのアセンブリ言語プログラム（C言語で生成されたものも含む）は、ガスでコンパイルされ、C言語プログラムで生成されたモジュールとリンクされます。このセクションでは、80X86 CPUハードウェア・プラットフォームをベースにしたLinuxカーネルにおけるアセンブラー構文とGNU as assembler (以下、as assembler)の使用について説明します。まず、asのアセンブリ言語プログラムの構文を紹介し、次に一般的なアセンブリ指令（インジケータ）の意味と使い方を説明します。次の章の終わりには、詳細な命令を含むアセンブラ言語プログラムの例を示します。

オペレーティングシステムの主要なコード要件には、高い実行速度と効率性が求められるものが多いため、通常、オペレーティングシステムのソースコードには、主要なアセンブリ言語プログラムの約10%が含まれています。Linuxも例外ではありません。32ビットの初期化コード、すべての割り込みや例外処理のインターフェースプログラム、多くのマクロ定義など、すべてがアセンブリ言語プログラムまたは拡張エンベデッドアセンブリ文として使用されています。これらのアセンブリ言語プロ

グラムの機能を理解できるかどうかが、OSの具体的な実装を理解する上でのポイントになることは間違いません。

GNU gcc コンパイラは、C プログラムをコンパイルする際に、まず中間結果として as アセンブリ言語ファイルを出力し、次に gcc は as アセンブラを呼び出して、一時的なアセンブリ言語プログラムをターゲットファイルにコンパイルします。つまり、asアセンブラは本来、単体のアセンブラとして使われるよりも、gccが生成した中間のアセンブリ言語プログラムをアセンブルするために設計されたものです。そのため、asアセンブラは、文字や数字、定数の表現方法や表現形式など、C言語の多くの機能もサポートしています。

GNU as アセンブラは、もともと BSD 4.2 のアセンブラを踏襲して開発されました。現在の as アセンブラは、さまざまな形式のオブジェクトファイルを生成するように設定できます。しかし、コンパイルされたアセンブリは

言語プログラムは、使用または生成されるターゲットファイルの形式には関係ありませんが、以下の説明でターゲットファイルの形式が関係する場合は、Linux 0.12系で採用されているa.outターゲットファイルの形式について説明します。.

### 3.2.1 アセンブリプログラムとしてコンパイルする

as  
assemblerを使ってアセンブラプログラムをコンパイルする際の基本的なコマンドラインのフォーマットは以下の通りです。

---

```
as [ オプション ] [ -o objfile ] [ srcfile.s ... ]...
```

---

objfileはasのコンパイル出力のターゲットファイル名、srcfile.sはasの入力アセンブリ言語プログラム名です。出力ファイル名を使用しない場合、asはデフォルトの出力先ファイルであるa.outをコンパイルします。asプログラム名の後には、コマンドラインにコンパイルオプションやファイル名を入れることができます。すべてのオプションは自由に配置できますが、ファイル名のコンパイル結果は密接に関係しています。

プログラムのソースコードは、1つまたは複数のファイルに配置することができます。プログラムのソースコードがどのように複数のファイルに分割されても、プログラムのセマンティクスは変わりません。プログラムのソースコードは、これらすべてのファイルを順番に並べた結果をまとめたものです。asコンパイラを実行するたびに、1つのソースプログラムだけをコンパイルします。しかし、ソースプログラムは複数のテキストファイルで構成されることがあります（端末の標準入力もファイルの一つです）。

asのコマンドラインでは、0個以上の入力ファイル名を指定することができます。asは、これらの入力ファイルの内容を左から右へと読んでいきます。コマンドラインの任意の位置にあるパラメータが特定の意味を持たない場合、それらは入力ファイル名として扱われます。コマンドラインでファイル名が指定されていない場合、asはターミナルまたはコンソールの標準入力から入力ファイルの内容を読み取ろうとします。この場合、入力する内容がない場合は、手動で Ctrl-D キーの組み合わせを入力して as アセンブラに伝える必要があります。コマンドラインで入力ファイルとして標準入力を明示的に指定したい場合は、「--」というパラメータを使用する必要があります。

asの出力ファイルは、入力されたアセンブリ言語プログラムによってコンパイルされたバイナリデータファイル、すなわちターゲットファイルとなります。オプション「-o」で出力ファイルの名前を指定しない限り、asはa.outという名前の出力ファイルを作成します。ターゲットファイルは、主にリンカーldの入力ファイルとして使用されます。オブジェクトファイルには、コンパイルされたプログラムコード、実行可能なプログラムを生成する際にldを支援する情報、そして場合によってはデバッグシンボル情報が含まれています。Linux

0.12システムで使用されているa.outオブジェクトファイルフォーマットについては、本章で後述します。

`boot/head.s`アセンブラーを個別にコンパイルしたい場合は、コマンドラインで次のコマンドを入力します。

```
[/usr/src/linux/boot]#      as-o head.o head.s
[/usr/src/linux/boot]# ls -l head*.
-rw-rw-r-x1 rootroot26449 May 19 22:04 head.o
-rw-rw-r-x1
rootroot5938 Nov 18 1991 head.s [/usr/src/linux/boot]#.
```

### 3.2.2 アセンブリ構文として

gcc 出力アセンブラーとの互換性を保つために、AT&T System V アセンブラー構文（以下、AT&T 構文）を採用しています。この構文は、インテルのアセンブラーが使用している構文（略してインテル 構文）とは大きく異なり、いくつかの大きな違いがあります。

## 3.2.1 アセンブラーの前処理

アセンブラーは、アセンブリ言語プログラムの簡単な前処理機能を内蔵しています。この前処理機能では、余分なスペースやタブを調整・削除したり、コメント文を削除してスペースや改行文字に置き換えたり、文字定数を対応する値に変換したりします。ただし、マクロの定義やインクルードファイルの機能は処理しません。この機能が必要な場合は、アセンブリ言語プログラムに大文字の接尾辞「.S」を付けることで、ascにgcc CPPの前処理機能を使わせることができます。

Asのアセンブリ言語プログラムでは、C言語のコメント文（「/\*」と「\*/」）を使用しているため、1行のコメント開始文字としてハッシュ記号「#」も使用しており、アセンブリ前にプログラムを前処理しない場合は、プログラムに含まれるハッシュ記号「#」で始まるインジケータやコマンドはすべてコメントの一部として扱われます。

## 3.2.2 シンボル、ステートメント、および定数

シンボルは、文字で構成された識別子で、シンボルを構成する有効な文字は、大文字、小文字、数字、そして「\_.\$」の3つの文字から取られます。シンボルは、数字で始まることはできず、大文字と小文字も異なります。as assembler

では、シンボルの長さに制限はなく、シンボル内のすべての文字が有効です。シンボルは他の文字（スペース、改行など）やファイルの先頭を使用して開始点と終了点を定義します。

ステートメントの最後は、改行または改行文字（';」）で終わります。ファイルの最後のステートメントは、改行文字で終わらなければなりません。

行末にバックスラッシュ（改行の前）を使用すると、1つの文を複数行に分けて書くことができます。asがバックスラッシュと改行を読んだ場合、その2つの文字は無視されます。

ステートメントは、0個以上のラベルで始まり、その後にステートメントのタイプを決定するキー シンボルが続きます。ラベルは、シンボルの後にコロン（':」）を付けたものです。キー シンボルは、ステートメントの残りの部分のセマンティクスを決定します。キー シンボルが「...」で始まる場合は、現在のステートメントがアセンブリコマンド（またはディレクティブ、インジケータ）であることを示します。キー シンボルが文字で始まる場合、現在のステートメントはアセンブリ言語の命令ステートメントです。つまり、ステートメントの一般的な形式は

---

```
label: .directive    followed by optional some comments
another_label:      # This is an empty statement.
                   instruction    operand_1, operand_2, ...
```

---

定数とは、数字のことで、文字定数と数値定数に分けられます。文字

また、定数は文字列と一文字に分けられ、数値定数は整数、大数、浮動小数点数に分けられます。

文字列は二重引用符で囲む必要があり、バックスラッシュ「\」を使って特殊文字をエスケープすることができます。例えば、「\」はバックスラッシュ文字を表します。最初のバックスラッシュはエスケープインジケーターで、2番目の文字が通常のバックスラッシュ文字として扱われることを示しています。一般的なエスケープシーケンスを表3-

1に示します。バックスラッシュの後に別の文字が続くと、バックスラッシュは機能せず、アセンブラーは警告メッセージを表示します。

アセンブラーで1文字の定数を使用する場合、その文字の前に1つの引用符を書くことができます。例えば、"A"は値 65 を、"C""は値 67 を表します。表 3-1 のエスケープコードは、1

文字の定数にも使用できます。例えば、「\」はバックスラッシュ文字の定数を表します。

Table 3-1 As assembler supports escaped character sequences

Escape code	Description
\b	Backspace, value is 0x08
\f	Formfeed, value 0x0C
\n	Newline, value 0x0A
\r	Carriage-Return value is 0x0D
\NNN	Character code represented by 3 octal numbers
\xNN...	Hexadecimal number character code
\\"	Represents a backslash character
\"	Represents a double quote in a string ""

整数の数値定数は、「0b」または「0B」で始まる2進数（「0-1」）、「0」で始まる8進数（「0-7」）、0以外の桁（「0-9」）で始まる10進数、「0x」または「0X」で始まる16進数（「0-9a-fA-F」）の4通りで表されます。負の数を表すには、負の'-'を前につけねばよい。

### Bignum

は

32

ビット以上のビット数で、その方法は整数と同じです。アセンブラーにおける浮動小数点定数の表現は、基本的にC言語と同じです。カーネルコードでは浮動小数点数はほとんど使われないので、ここでは説明しません。

### 3.2.3 命令文、オペランド、アドレッシング

命令とは、CPUが行う操作のことです。通常、命令はオペコードとも呼ばれます。オペランドとは、命令操作の対象となるものです。アドレスとは、指定されたデータのメモリ上の位置のことです。命令文とは、プログラムの実行時に実行される文である。通常、4つの要素で構成されます。

- ラベル（オプション）です。
- Opcode（インストラクション・ニーモニック）の略。
- オペランド（特定の命令で指定されるもの）。
- コメント

命令文には、コンマで区切られた0個または3個までのオペランドを含めることができます。2つのオペランドを持つ命令文では、第1オペランドがソースオペランド、第2オペランドがデスティネーションオペランド、つまり命令操作の結果が第2オペランドに格納されます。

オペランドは、即値（つまり値が定数の式）、レジスタ（CPUのレジスタ内の値）、メモリ（メモリ内の値）のいずれかです。間接オペランド（Indirect operand）は、実際のオペランド値のアドレス値を含む。AT&Tの構文では、オペランドの前に'\*'の文字を付けて間接オペランドを指定します。間接オペランドは、リダイレクト／コール命令でのみ使用できます。後述のジャンプ命令の説明を参照してください。

- 即値オペランドの前には'\$'文字のプレフィックスが必要です。
- レジスター名の前に'%'文字のプレフィックスを付ける必要があります。
- メモリオペランドは、変数名または変数のアドレスを含むレジスタで指定します。変数名は

暗黙のうちに変数のアドレスを示し、そのアドレスのメモリの内容を参照するようにCPUに指示します。

### 3.2.3.1 命令のオペコード名

AT&T構文の命令オペコード名（命令ニーモニック）の最後の文字は、オペランドの幅を示すために使用されます。文字'b'、'w'、'l'は、それぞれバイト、ワード、ロングのオペランドを指定します。命令名にこのような文字の接尾辞がなく、命令文にメモリ・オペランドが含まれていない場合、asはデスティネーション・レジスタ・オペランドに基づいてオペランドの幅を決定しようとします。例えば、「`mov %ax, %bx`」という命令文は、「`movw %ax, %bx`」と同じです。同様に、「`mov $1, %bx`」という命令文は、「`movw $1, %bx`」と同じです。

AT&Tとインテルの構文では、ほとんどすべての命令オペコードの名前が同じですが、それでもいくつかの例外があります。シンボリック・エクステンションとゼロ・エクステンションの両命令では、ソース・オペランドとデスティネーション・オペランドに幅を指定する必要があることを示すために、2つの幅を必要とします。AT&Tの構文は、2つのオペコードサフィックスを使用して行われます。AT&T構文のシンボル拡張とゼロ拡張の基本的なオペコード名は、それぞれ「`movs...`」と「`movz...`」で、インテルではそれぞれ「`movsx`」と「`movzx`」です。オペコードの基本名には、2つのサフィックスが付きます。例えば、シンボリック拡張を使用して%alから%edxに移動するAT&Tのステートメントは'movsbl %al, %edx'であり、blはバイトからロングへ、bwはバイトからワードへ、wlはワードからロングへとなります。AT&Tの構文とインテルの構文の変換命令の対応を表3-2に示します。

表3-2 AT&Tシンタックスとインテルシンタックスの変換コマンドの対応関係

AT&T	インテル	説明
<code>cbtw</code>	<code>cbw</code>	al のバイト値を %ax に拡張します。
<code>cwtl</code>	<code>cwde</code>	記号を %eax に拡張します。
<code>cwtd</code>	<code>cwd</code>	max 記号を %dx:%ax に拡張します。
<code>cltd</code>	<code>cdq</code>	ex 符号を %edx:%eax に拡張します。

### 3.2.3.2 命令オペコードのプレフィックス

オペコードのプレフィックスは、後続のオペコードを変更するために使用されます。文字列命令の繰り返し、エリアオーバーライドの提供、バスロック操作の実行、オペランドやアドレス幅の指定などに使われます。通常、オペコードプレフィックスはオペランドを持たない命令の排他的な行として使用することができ、影響を受ける命令の直前に配置する必要がありますが、修正する命令と同じ行に配置するのがベストです。例えば、文字列スキャンコマンド「scas」は、繰り返し演算を行うためにプレフィックスを使用しています。

---

```
repne scas %es:(%edi), %al
```

---

オペランドの接頭辞の一部を表3-3に示す。

4 Table 3-3 Opcode prefix list

Opcode prefix	Description
cs, ds, ss, es, fs, gs	Section overrides the opcode prefix. Using the section:memory operands by specifying memory prefixes automatically adds this prefix.
data16, addr16	Operand/address width prefix. These two prefixes will change the 32-bit operand/address to a 16-bit operand/address. However, please note that as does not support 16-bit addressing.
lock	Bus latching prefix. Used to disable interrupts during instruction execution (only valid for some instructions, see the 80X86 manual).
wait	Coprocessor instruction prefix. Wait for the coprocessor to complete the execution of the current instruction. This prefix is not needed for the 80386/80387 combination.
rep, repe, repne	The prefix of the string instruction causes the string instruction to repeat the specified number of times in %ecx.

## 5

### 5.2.3.1 メモリの参照

インテル構文の間接メモリー参照形式： section:[base + index\*scale + disp] 次の AT&T 構文に対応しています： section:disp(base, index, scale)

baseとindexはオプションの32ビットベースレジスタとインデックスレジスタ、dispはオプションのオフセット値です。Scaleは、スケルファクターで、その範囲は1、2、4、8です。Scaleにindexを乗じてオペランドアドレスを算出します。Scaleが指定されない場合、スケールのデフォルトは1です。

Sectionは、メモリオペランドのオプションのセグメントレジスタを指定し、オペランドで使用されている現在のデフォルトのセグメントレジスタをオーバーライドします。指定されたセクションオーバーライトレジスタがデフォルトのオペレーションセクションレジスタと同じ場合、asはアセンブルされた命令に同じセクションプレフィックスを出力しないことに注意してください。以下は、いくつかのAT&Tおよびインテルの構文形式でのメモリ参照の例です。

```

movl var, %eax          # Put the contents at memory address var in the register %eax.
movl %cs:var, %eax      # Put the contents at var in the code segment into %eax.
movb $0x0a,%es:(%ebx)   # Save byte value 0x0a to offset specified by %ebx in es segment.
movl $var, %eax          # Put the address of var in %eax.
movl array(%esi), %eax  # Put contents at address determined by array+%esi into %eax.
movl (%ebx, %esi, 4), %eax # Put contents at address determined by %ebx+%esi*4 in %eax.
movl array(%ebx, %esi, 4), %eax # Put contents at address of array + %ebx+%esi*4 into %eax.
movl -4(%ebp), %eax      # Put contents at %ebp - 4 in %eax, using the default segment %%ss.
movl foo(%eax,4), %eax    # Put contents at foo+eax*4 intp %eax, using default seg %%ds.

```

### 5.2.3.2 ジャンプ命令

ジャンプ命令は、実行ポイントをプログラム内の別の場所に移動し、実行を継続するために使用されます。このジャンプ先は、通常、ラベルで表されます。オブジェクトコードファイルを生成する際、アセンブラーはタグ付けされたすべての命令のアドレスを決定し、ジャンプ命令のアドレスをジャンプ命令にエンコードします。ジャンプ命令は、無条件ジャンプと条件付きジャンプに分けられます

。条件付きジャンプ命令は、命令実行時にフラグレジスタ内の関連するフラグの状態に依存してジャンプするかどうかを決定し、無条件ジャンプはこれらのフラグに依存しない。

JMPは無条件のジャンプ命令で、直接ジャンプと間接ジャンプの2種類に分けられます。条件付きジャンプ命令は直接ジャンプの形式しかありません。直接ジャンプ命令では、ジャンプ先の命令のアドレスがジャンプ命令の一部として直接エンコードされ、間接ジャンプ命令では、ジャンプ先がレジスタやMemoryのロケーションから取得される。直接ジャンプ命令は、ジャンプ先のラベルを与えるように記述し、間接ジャンプ命令は、スター文字「\*」を演算指示子の先頭文字として記述し、演算指示子はmovl命令と同じ構文を使用します。以下に、直接ジャンプと間接ジャンプの例を示します。

---

```
jmp NewLoc      # Jump directly. Unconditionally jump to label NewLoc to continue execution.
jmp *%eax       # Indirect jump. The value of register %eax is the jump destination.
jmp *(%eax)     # Indirect jump. Read the jump destination from the address indicated by %eax.
```

---

同様に、命令カウンタPCに依存しない間接呼出オペランドにも、プレフィックス文字として「\*」を付ける必要があります。この文字を使用しない場合、asアセンブラーは命令カウンタPCに関連するジャンプラベルを選択します。また、メモリオペランドを持つその他の命令では、オペコードのサフィックス ('b'、'w'、'l') を使用して、オペランドのサイズ（バイト、ワード、ロング）を示す必要があります。

### 3.2.4 セクションとリロケーション

セクション（セグメントともいう）は、アドレス範囲を表すのに使われ、OSはそのアドレス範囲のデータ情報を同じように扱い、処理します。例えば、「読み取り専用」の領域があり、この領域からはデータを読み取ることしかできず、書き込むことはできません。ゾーンという概念は主に、コンパイラが生成するターゲットファイル（または実行プログラム）の中のテキスト領域やデータ領域など、異なる情報領域を示すために使われる。アセンブリ言語プログラムを正しく理解してコンパイルするためには、asが生成する出力オブジェクトファイルのフォーマットを理解する必要があります。Linux

0.12カーネルで使用されているa.out形式のオブジェクトファイルのフォーマットについては、本章の後半で詳しく説明します。ここでは、アセンブラーが生成するオブジェクトファイルの基本的な構造を理解するために、ゾーンの基本的な概念について簡単に紹介します。

リンクldは、入力されたオブジェクトファイルの内容を一定のルールに基づいて結合し、実行プログラムを生成します。asアセンブラーがターゲットファイルを出力する際、ターゲットファイル内のコードはデフォルトで0番地から始まるように設定されています。その後、ldはリンク処理の際に、異なるターゲットファイルの各部分に異なる最終アドレス位置を割り当てます。Ldは、プログラムのバイトブロックを、プログラムが実行されたアドレスに移動します。これらのブロックは固定された単位として移動されます。その長さやバイト順は変更されない。このような固定単位をゾーン（またはセグメント、パート）と呼ぶ。ゾーンにランタイムのアドレスを割り当てる操作を再配置操作といい、ターゲットファイルに記録されているアドレスが適切なランタイムのアドレスに対応するように調整することも含まれる。

as-  
assemblerは、text、data、bssエリアと呼ばれる少なくとも3つのフィールドを持つオブジェクトファイル

ルを作成し、出力します。各地区は空でもよい。アセンブラー命令で '.text' または '.data' 地区に出力を置かなかった場合、これらの地区は存在しますが、内容は空になります。ターゲットファイルでは、0番地からテキストエリア、データエリア、bssエリアの順に表示されます。

セクションが再配置されると、リンクer ldはどのデータがどのように変更されるのかを知るために、アセンブラーは必要な再配置情報をターゲットファイルに書き込みます。再配置の操作を行うためには、ldはターゲットファイルのアドレスが関係するたびに知る必要があります。

- ターゲットファイルのアドレスへの参照はどこから来たのか？
- 引用されたバイトの長さは？
- このアドレスで参照されるのはどのセクションでしょうか？(アドレス)-(セクションの開始アドレス)の値は何ですか？
- アドレスの参照は、プログラムカウンタPC (Program-Counter) に関連するものですか？

実際、asで使われるアドレスはすべて次のように表すことができます。(セクション) + (セクション内のオフセット)。また、asで評価される式のほとんどは、このようなゾーンに関連した特性を持っています。以下の説明では、ゾーンのsecname内のオフセットNを示すために、"{secname N}"という表記を使用する。

テキストエリア、データエリア、bssエリアに加えて、絶対アドレスエリア（アブソリュートエリア）についても理解しておく必要があります。リンクerがさまざまなオブジェクトファイルを結合するとき、絶対領域のアドレスは常に同じになります。例えば、ldは実行時に{absolute 0}というアドレスを0番地に「再配置」します。リンクerがリンク後に2つのターゲットファイルのデータ領域を重複したアドレスとして配置することはありませんが、ターゲットファイルの絶対領域は必ず重複して上書きされます。

また、Undefinedセクションがあります。アセンブリでは、このエリアの任意のアドレスが{undefined U}に設定されていると判断することはできません（Uは後で埋められます）。値は常に定義されているので、未定義のアドレスを表示するには、未定義のシンボルを使うしかありません。コモンブロックへの参照は、このようなシンボルです。その値はアセンブリ時には不明なので、未定義領域に入ります。

同様に、セクション名もリンク先のプログラムのセクション群を表すのに使われます。リンクer ldは、プログラムのすべてのオブジェクトファイルのテキストセクションを、隣接するアドレスに配置します。私たちが慣れ親しんでいるプログラムのテキスト・エリアとは、実際には、そのプログラムのすべてのオブジェクト・ファイルのテキスト・セクションの組み合わせによって形成されるアドレス・エリア全体を指しています。プログラムのデータ部やbss部の理解も同様です。

### 3.2.4.1 リンカの関与する部分

リンクer ldは、以下の4種類のセクションのみを対象としています。

- テキスト部、データ部・・・プログラムを保存するための2つの領域です。Asとldは、これらを独立して同等に扱います。テキストセクションの記述は、データセクションにも適しています。ただし、プログラムが実行されているときは、通常のテキストセクションは変更されません。テキストセクションは通常、プロセスで共有され、命令コードや定数などが書かれています。データセクションの内容は、通常、プログラムが実行されているときに変更されます。例えば、C言語の変数は通常、データセクションに格納されています。
- bssセクション

プログラムの実行開始時には、このエリアには0バイトが格納されています。初期化されていない変数を格納したり、共通の変数格納領域として使用される。プログラムの各ターゲットファイルのbssセクションの長さ情報は非常に重要であるが、このエリアにはゼロ値のバイトが格納されるため、ターゲットファイルにbssセクションを保存する必要はない。bss領域を設定する目的は、ゼロ値のバイトをターゲットファイルから明示的に除外することである。

### ■ 絶対セクション

この領域のアドレス0は、常にランタイムのアドレス0に「再配置」される。再配置の際に、ldが参照しているアドレスを変更したくない場合に、このセクションを使用します。この観点から、絶対アドレスを「再配置不可」と呼ぶことができます：再配置操作時に変更されません。

### ■ undefined

### section

前述の各セクションにないオブジェクトへの参照は、このセクションに属する。

理想的な3つのリロケータブル・セクションの例を図3-

2に示します。この例では、従来のセクション名である「.text」と「.data」を使用しています。横軸はメモリアドレスを示す。ldリンクの具体的な動作については、後ほど詳しく説明します。

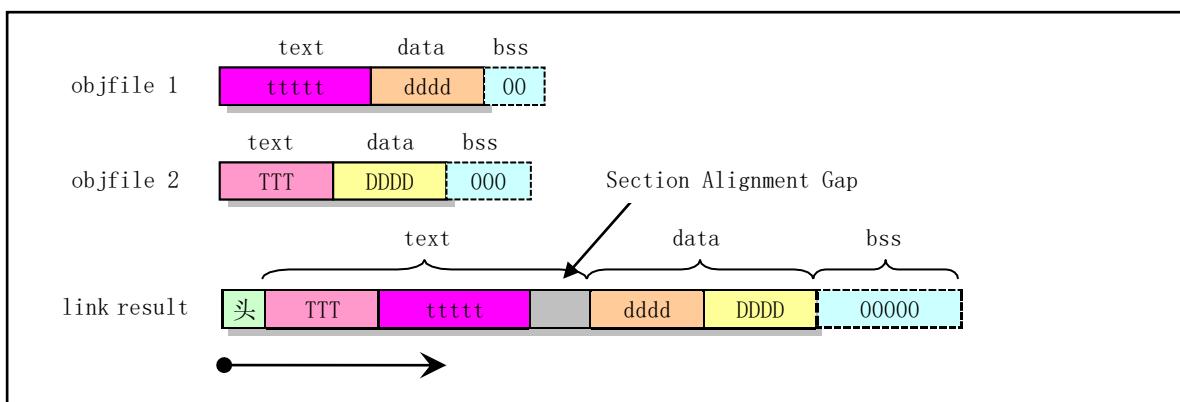


Figure 3-2 Example of linking two object files to generate a linked program

### 3.2.4.2 サブセクション

アセンブルされるバイトデータは、通常、テキスト部またはデータ部に配置されます。アセンブルのソースプログラムのある領域に、隣接していないデータ群が存在することがあります。アセンブル後にそれらをまとめて保存したい場合があります。Asアセンブラーでは、サブセクションを使用してこのような目的に使用できます。各セクションには、0~8192の番号が付いたサブエリアがあります。同じサブセクションでプログラムされたオブジェクトは、そのサブセクションの他のオブジェクトと一緒にターゲットファイルにまとめられます。例えば、コンパイラはテキストエリアに定数を格納したいが、これらの定数がアセンブルされるプログラム全体に散らばっていては困る場合があります。この場合、コンパイラは、出力される各コード領域の前に「.text 0」サブセクションを使用し、各定数セットの前に「.text 1」サブセクションを使用することができます。

サブセクションの使用は任意です。サブセクションを使用しない場合、すべてのオブジェクトはサブセクション0に配置されます。デスティネーションファイルにはサブセクションの番号順に表示されますが、デスティネーションファイルにはサブセクションを表す情報は含まれません。宛先ファイル

ルを処理するldなどのプログラムは、サブセクションの痕跡を見ることはできず、すべてのテキストサブセクションからなるテキストセクションと、すべてのデータサブセクションからなるデータセクションを見るだけです。後続のステートメントがどのサブセクション領域に組み立てられるかを指定するために、「.text expression」または「.data expression」に数値パラメータを使用することができます。式の結果は、絶対値でなければなりません。.text」のみを指定した場合は、デフォルトで「.text 0」が使用されます。同様に、「.data」を指定すると、「.data 0」が使用されます。

各セクションには、そのセクションにアセンブルされた各バイトをカウントするロケーションカウンタがあります。サブセクションはアセンブラーが使いやすいように設定されているだけなので、サブセクションカウンタはありません。位置カウンタを直接操作する方法はありませんが、アセンブリコマンド「.align」でその値を変更することができ、任意のラベル定義は位置カウンタの現在の値を取ります。ステートメントアセンブリ処理を実行しているゾーンの位置カウンタをカレントアクティビティカウンタと呼ぶ。

### 3.2.4.3 bssセクション

bssセクションは、ローカルのパブリック変数を格納するために使用されます。bssセクションにスペースを確保することはできますが、プログラムの実行前にデータを入れることはできません。なぜなら、プログラムの実行を開始すると、bssセクションのすべてのバイトがクリアされるからです。アセンブリコマンドの「.lcomm」はbssセクションのシンボルを定義するのに使われ、「.comm」はbssセクションのパブリックシンボルを宣言するのに使われる。

## 3.2.5 シンボル

プログラムのコンパイルやリンクの過程において、シンボルは重要な概念です。プログラマーはシンボルを使ってオブジェクトに名前を付け、 linker はシンボルを使ってリンク操作を行い、デバッガーはシンボルを使ってデバッグを行います。

ラベルは、シンボルの後にコロンを付けたものです。この時点では、シンボルはアクティブの現在の値を表しています。

位置カウンタで、例えば、命令のオペランドとして使用することができます。等号「=」を使って、シンボルに任意の値を割り当てることができます。

シンボル名は、アルファベットまたは「.\_」文字のいずれかで始まります。ローカルシンボルは、コンパイラやプログラマーが名前を一時的に使用するために使用されます。ローカルシンボルの名前は10個 ('0'...9) あり、プログラムの中で再利用することができます。ローカルシンボルを定義するには、「N:」(Nは任意の数字を表す) という形式のラベルを書くだけです。前に定義されたシンボルを参照する場合は'Nb'と書き、次に定義されたローカルラベルを参照する場合はNfと書く必要があります。ここで'b'は後方、'f'は前方を意味します。ローカルラベルの使用に制限はありませんが、いつでも、前方／後方の最も遠い10個のローカルラベルしか参照できません。

### 3.2.5.1 特別なポイント記号

特殊記号「.」は、アセンブリの現在のアドレスを示しています。つまり、「mylab: .long ...」という表現は、mylabが自分のアドレス値を含むように定義します。.に値を代入することは、アセンブリコマンド「.org」と同じです。つまり、「.=+4」という表現は、「.space 4」と全く同じである。

### 3.2.5.2 シンボルの属性

各シンボルは、名前に加えて、"value

"と

"type"

"の属性を持っています。出力のフォーマットによっては、シンボルが補助的な属性を持つこともあります。シンボルが定義されずに使用された場合、asはそのシンボルのすべての属性が0であるとみなします。

シンボルの値は通常32ビットです。テキスト、データ、bss、アブソリュートの各エリアの位置を示すシンボルの場合、エリアの先頭からラベルまでのアドレス値が値となります。テキストエリア、データエリア、bssエリアでは、通常、リンク処理中にエリアのベースアドレスの変更によりシンボルの値が変化しますが、アブソリュートエリアのシンボルの値は変化しません。このため、絶対記号と呼ばれている。

ldは、未定義のシンボルの値を扱います。未定義のシンボルの値が0の場合、そのシンボルがアセンブラーのソースプログラムで定義されていないことを意味します。ldは他のリンクされたファイルからその値を決定しようとします。シンボルは、プログラムがシンボルを使用しているが、シンボルを定義していない場合に生成されます。未定義のシンボルの値が0でない場合、シンボルの値は、.commパブリック宣言で必要とされるパブリックメモリ空間の長さを表します。シンボルは、このメモリ空間の最初のアドレスを指します。

シンボルのtype属性には、リンクやデバッガのための再配置情報、シンボルが外部にあることを示すフラグ、その他のオプション情報が含まれています。a.out形式のオブジェクトファイルでは、シンボルのtype属性は8ビットのフィールド（n\_typeバイト）に格納されます。その意味については、include/a.out.hファイルの説明を参照してください。

### 3.2.6 アセンブラーのディレクティブとして

アセンブラー指令とは、アセンブラーの動作方法を示す永続的な命令です。アセンブラー指令は、変数の領域確保、プログラムの開始アドレスの決定、現在のアセンブリセクションの指定、位置カウンタの値の変更などをアセンブラーに要求するために使用します。アセンブラー指令はすべて「.」で始まり、それ以外は文字で、大文字小文字は関係ありません。大文字小文字は関係ありませんが、一般的には小文字を使用します。以下では、一般的なアセンブラー命令について説明します。

#### 3.2.6.1 .align abs-expr1, abs-expr2, abs-expr3

.align

は、現在のサブセクションの次の指定されたメモリ境界に位置カウンタの値を設定（インクリメント）するストレージアラインアセンブラー指令です。最初の絶対値式abs-expr1（絶対値式）で、必要な境界アライメント値を指定します。a.out形式のオブジェクトファイルを使用する80X86システムでは、この式の値は、インクリメントされた後の位置カウンタの右端のバイナリ値のゼロ値のビット数、つまり2の累乗になります。例えば、「.align 3」は、位置カウンタの値を8の倍数にすることを意味します。位置カウンタの値自体が8の倍数である場合には、必要ありません。

を使って変更することができます。しかし、ELFフォーマットを使用する80X86システムでは、式の値がそのままそのために必要なバイト数になります。例えば、「.align 8」は、ポジションカウンタの値を8の倍数にすることです。

2つ目の式では、アライメントとパディングに使用するバイト値を指定します。この式とその前のコンマは省略可能です。省略された場合、パディングのバイト値は0になります。

3番目のオプションの式（abs-

expr3）は、アライメント操作によってパディングがスキップされることを許容する最大バイト数を示す

ために使用されます。アライメント操作によってスキップされたバイト数がこの最大値よりも大きい場合、アライメント操作はキャンセルされます。第2パラメータを省略したい場合は、第1パラメータと第3パラメータの間にカンマを2つ入れます。

### **3.26.1 .ascii "string"...**

位置カウンタの現在の位置から文字列用のスペースを割り当て、文字列を格納する。複数の文字列をカンマで区切って書くことができます。例えば、'.ascii "Hellow world!", "My assembler"'のようになります。アセンブラー命令では、これらの文字列を連続したアドレス位置に組み立て、各文字列の後に0 (NULL) バイトを追加しないようにします。

### **3.26.2 .asciz "string"...**

このアセンブラー指令は、「.ascii」と同じですが、各文字列の後にゼロ値のバイトが続きます。.asciz'の "z" は "ゼロ" を意味します。

### **3.26.3 .byte expressions**

このディレクティブは、カンマで区切られた  
個以上の式を想定しています。各式は次のバイトに結合されます。

### **3.26.4 .comm symbol, length**

bssセクションに名前付きのパブリックエリアを宣言します。ldのリンク時に、あるオブジェクトファイルの共通シンボルが、他のオブジェクトファイルの同名の共通シンボルにマージされます。ldがシンボル定義を見つけられず、1つ以上の共通シンボルだけを見つけた場合、ldは長さ length バイトの初期化されていないメモリを割り当てます。長さは絶対値表現でなければなりません。ldが、長さが同じで名前が異なる複数の共通シンボルを見つけた場合、ldは長さが最も大きいスペースを割り当てます。

### **3.26.5 .data subsection**

このアセンブラー指令は、次のステートメントをデータサブセクションの番号の付いたサブセクションにアセンブルするように指示します。番号を省略した場合、デフォルトでは番号  
が使用されます。数値は絶対値の表現でなければなりません。

### **3.26.6 .desc symbol, abs-expr**

このディレクティブは、シンボルの記述子を、絶対式の下位16ビットに設定します。a.outまたはb.outオブジェクト形式のみです。include/a.out.hファイルの説明を参照してください。

### **3.26.7 .fill repeat, size, value**

このアセンブラー指令は、サイズがNバイトのリピート（繰り返し）を生成します。sizeには  
0または何らかの値を指定しますが、sizeが8より大きい場合は8に制限されます。各リピートバイトのコネットは、8バイトの数値から取ります。最上位の4バイトは0、最下位の4バイトは数値となります。3つのパラメータ値は絶対値で、sizeとvalueはオプションです。2つ目のコンマとvalueが省略された場合、valueの値はデフォルトで0になり、2つ目のパラメータが省略された場合、sizeの値はデフォルトで1になります。

### **3.26.8 .global symbol ( .globl symbol )**

このアセンブラー命令により、リンクer ldにシンボルが表示されます。シンボルがオブジェクトファイルで定義されている場合、その値はリンクプロセスで他のオブジェクトファイルで使用されます。シンボルがオブジェクトファイルで定義されていない場合、その属性はリンクプロセスにおいて他のオブジェクトファイルの同名のシンボルから取得されます。これは、シンボルのシンボルタイプフィールドの外部ビットN\_EXTを設定することで行われます。include/a.out.hファイルの説明を参照してく

ださい。

### **3.26.9 .int expressions**

アセンブラーの指示により、ある領域に0個以上の整数値を設定します（80386系は4バイト、.longと同じ）。コンマで区切られた各式の値は、ランタイムの値です。例えば、.int 1234,567,0x89ABのようになります。

### **3.26.10 .lcomm symbol, length**

シンボルに指定されたローカルコモンエリアは、長さバイトの空間を確保します。確保された領域とシンボルの値は、新しいローカルコモンブロックの値となる。割り当てられたアドレスはbssセクションにあるため、これらのバイト値は実行時にクリアされます。シンボルはグローバル宣言されていないので、リンクのldは見えません。

### **3.26.11 .long expressions**

その意味は、.intと同じです。

### **3.26.12 .octa bignums**

このアセンブリ指示子は、コンマで区切られた16バイトのラージナンバー (.byte、.word、.long、.quad、.octaはそれぞれ1、2、4、8、16バイトに対応) を0個以上指定します。

### **3.26.13 .org new\_lc, fill**

このアセンブラー指令は、現在のセクションのロケーションカウンタに  
new\_lc  
という値を設定します。new\_lc  
は絶対値(式)、またはサブセクションと同じセクションを持つ式、つまりセクションをまたぐために  
.org  
を使用することはできません。new\_lcのセクションが正しくない場合、.orgは機能しません。ポジションカウンターはセクションベースであることに注意してください。つまり、各セクションがカウントの出発点として使われます。

位置カウンタの値が増加すると、スキップされたバイトは値のフィルで埋められます。この値は絶対値でなければなりません。カンマとfillを省略した場合、fillのデフォルトは0です。

### **3.26.14 .quad bignums**

コンマで区切られた8バイトのラージナンバーを0個以上指定するアセンブラー指令です。大数が8バイトに収まらない場合は、下位8バイトを取ります。

### **3.26.15 .short expressions ( same as .word expressions )**

コンマで区切られた	2	バイトの数値を	0
-----------	---	---------	---

個以上、セクション内で指定するアセンブラー指令です。各式には、実行時に16ビットの値が生成されます。

### **3.26.16 .space size, fill**

アセンブラー指令では、サイズバイトが生成され、それぞれのバイトにfillが入ります。このパラメータは絶対値です。カンマとfillが省略された場合、fillのデフォルト値は0です。

### **3.26.17 .string "string"**

カンマで区切られた1つまたは複数の文字列を定義します。文字列にはエスケープ文字を使用できます。各文字列には、自動的にヌル終端文字が付加されます。例えば、.string "\Starting", "other strings"などです。

### **3.26.18 .text subsection**

notification

asは、以下の記述を番号付きのサブセクションにまとめます。番号subsectionが省略された場合は、デ

フォルトの番号値0が使用されます。

### 3.2.6.19 .word expressions

32ビットマシンでは、このアセンブリ命令は.shortと同じ意味を持ちます。

## 3.2.7 16ビットコードの書き込み

GNU

asは通常、純粋な32ビットの80X86コードを記述するために使用されますが、1995年以降のリアルモードや16ビットプロテクトモードで動作するコードを記述するためのサポートも限られています。asのコンパイルで16ビットコードを生成するためには、16ビットモードで動作する命令文の前にアセンブリ命令「.code16」を追加し、asのアセンブラーを32ビットコードのアセンブリモードに戻すためにアセンブリ命令「.code32」を使用する必要があります。

asは、16ビットと32ビットのアセンブラー文を区別しません。16ビットモードと32ビットモードの各命令は、モードに関係なく全く同じように機能します。asは、16ビットモードと32ビットモードのどちらで実行されるかにかかわらず、アセンブラー文に対して常に32ビットの命令コードを生成します。アセンブリ命令　　'.code16'　　を使用して　　as　　を　　16　　ビットモードにすると、asはすべての命令に必要なオペランド幅のプレフィックスを自動的に追加し、16ビットモードで実行させます。なお、asはすべての命令にアドレスとオペランド幅のプレフィックスを追加するため、結果としてコード長やアセンブリのパフォーマンスに影響を与えます。

1991年のLinuxカーネル0.12の開発時には、アセンブラーが16ビットに対応していなかったため、前述のas86アセンブラーを使用して、ブート起動コードや初期化アセンブラーを記述・アセンブルしていました。

0.12カーネルリアルモード。

## 3.2.8 アセンブラーのコマンドラインオプションとして

- 4 -a Turn on program listings.
- 5 -f Fast operation, skip whitespace and comment preprocessing.
- 6 -o *objfile* Name the object-file output from as *objfile*
- 7 -R Fold the data section into the text section.
- 8 -W Suppress warning messages.

## 3.3 C言語プログラム

GNU

gccは、ISO標準C89に記載されているC言語をいくつか拡張しており、そのうちのいくつかはISO C99標準に含まれています。このセクションでは、カーネルで頻繁に使用されるgccの拡張機能のいくつかについて説明します。遭遇する拡張文の簡単な説明は、次のプログラムコメントのセクションでも隨時行われます。

### 3.3.1 Cプログラムのコンパイルとリンク

gccアセンブラーを使用してCプログラムをコンパイルする場合、通常は図3-3のように、前処理ステージ、コンパイルステージ、アセンブリステージ、リンクステージの4段階の

処理を行います。

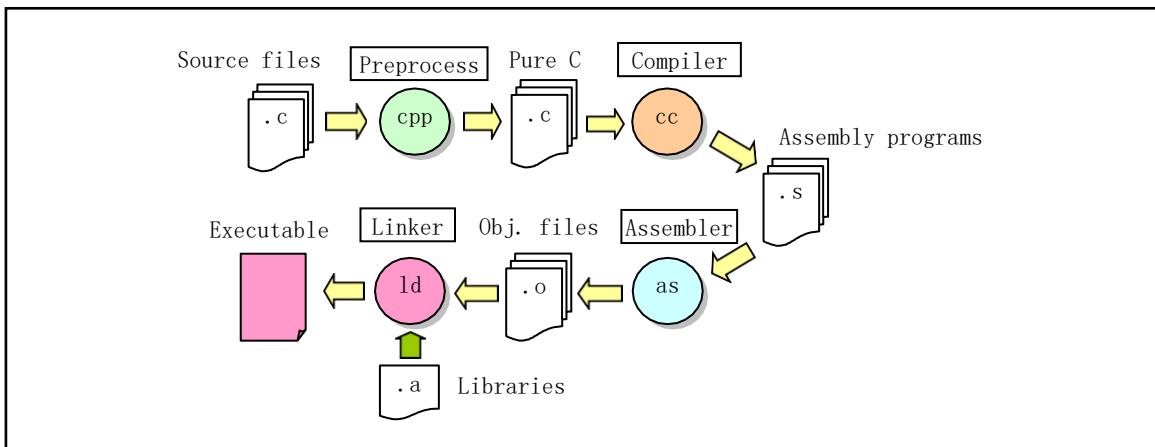


Figure 3-3 CC program compilation process

前処理段階では、gccはC言語プログラムをCプリプロセッサCPPに渡し、C言語プログラム中のインジケータやマクロを置き換えて、プレーンなC言語コードを出力する。コンパイル段階では、gccはC言語プログラムをコンパイルして、対応するMachine関連のアセンブリ言語コードを生成する。アセンブリ段階。

最後に、GNU

ld

リンクが、プログラムに関するターゲットファイルの組み合わせをリンクして、プログラムの実行イメージファイルが生成される。gccを呼び出すコマンドラインのフォーマットは、アセンブリ言語をコンパイルするときのフォーマットと似ています。

---

gcc [ オプション ] [ -o outfile ] infile ...

---

infileは入力C言語ファイル、outfileはコンパイル後の出力ファイルです。コンパイル処理では、4つの処理段階すべてを実行する必要はありません。コマンドラインオプションを使用することで、gccのコンパイル処理を特定の処理段階の後で実行を停止することができます。例えば、「-S」オプションを使用すると、C言語プログラムに対するアセンブリ言語プログラムを出力した後にgccを停止させることができ、「-c」オプションを使用すると、以下のようにリンク処理を行わずにターゲットファイルの生成のみを行うことができます。

---

gcc -o hello hello.c // Compile the hello.c to generate the execution file hello.  
gcc -S -o hello.s hello.c // Compile hello.c to generate corresponding assembly hello.s.  
gcc -c -o hello.o hello.c // Compile hello.c to generate target file hello.o without linking.

---

多数のソースプログラムファイルを含むLinuxカーネルのような大規模なプログラムをコンパイルする際には、通常、プログラム全体のコンパイルプロセスを自動的に管理するためにmakeツールが使用されます。以下の説明をご覧ください。

### 3.3.2 インライン・アセンブリ言語

ここでは、カーネルのC言語プログラムで公開されているインライン・アセンブリ文について説明します。通常、C言語のプログラムを作成する際にインラインアセンブリコードを使用することはほとんどありませんので、ここでは基本的な書式や使い方を説明する必要があります。`asm`を使ったアセンブリ命令では、命令のオペランドをC言語の式で指定することができます。つまり、使いたいデータが入っているレジスタやメモリの位置を推測する必要はなく、機械の説明書に記載されているようなアセンブリ命令のテンプレートを指定し、各オペランドに対してオペランド制約文字列を指定する必要があるのです。

---

```
asm( "Assembly language statement"
    : Output register operands
    : Input register operands
    : Registers of clobbered or modified);
```

---

1行目を除いて、後ろにコロンが付いている行は、使用しない場合は省略可能です。このうち、「`asm`」はインラインアセンブリ文のキーワード、「`assembly statement`」はアセンブリ命令を記述する場所、「`output register`」はこの組み込みアセンブリを実行した後の出力データを格納するためのレジスタを示す。ここでは、これらのレジスタは、それぞれCの式の値や、メモリのアドレスに対応しています。"入力レジスタ

"は、アセンブリコードの開始時に、ここで指定されたレジスタのいくつかに格納されるべき入力値を示します。また、それぞれCの変数や定数値にも対応しています。"Clobbered or Modified registers"は、ここに記載されているレジスタの値が変更され、gccコンパイラがこれらのレジスタに最初にロードした値に依存できなくなったことを意味します。gccは必要に応じてこれらのレジスタを再ロードする必要があります。したがって、出力/入力レジスタのセクションに記載されていないが、アセンブリステートメントで明示的に使用されている、または暗黙的に使用されているレジスタ名をリストアップする必要があります。

例えば、ここでは架空の「コンバイン」命令を紹介します。

---

```
asm("combine %1, %0" :"=r"(result) : "r"(length));
```

---

ここで`length`は入力オペランドのC式、`result`は出力オペランドのC式です。それぞれのオペランド制約には "r" があり、動的に割り当てられるジェネラルレジスタが必要であることを示しています。また、「`=r`」の「`=`」はオペランドが出力であることを示し、すべての出力オペランドの制約には「`=`」を使用しなければなりません。この制約は、gccのマニュアルに記載されているマシン記述で使用されているのと同じ言語を使用しています（第16章マシン記述のオペランド制約のセクション）。

上の例のように、各オペランドはオペランド制約文字列で記述され、その後にC式が括弧内に記述されます。アセンブリのテンプレートと最初の出力オペランドはコロンで区切られ、最後の出力オペランドと最初の入力がある場合はコロンで区切られます。カンマは各グループ内のオペランドを区切れます。オペランドの総数は10個まで、または機械の説明書に記載されている命令パターンの最大オペ

ランド数のどちらか多い方に制限されます。出力オペランドがなく、入力オペランドがある場合は、出力オペランドがある場所を囲むように2つの連続したコロンを置く必要があります。

以下では、より詳細な例を用いてオンラインアセンブリメントの使用方法を説明します。これは、`kernel/traps.c`ファイルの22行目から始まるコードブロックです。よりわかりやすくするために、このコードを並べ替えて番号を付けています。

```
01 #define get_seg_byte(seg,addr) \
02 ({ \
03     register char_ res; \
04     __asm__ ("push %%fs; \
05             mov %%ax,%%fs; \
06             movb %%fs:%2,%al; \
07             pop %%fs" \
08             : "=a" ( res) \
09             :"0" (seg), "m" (*(addr))); \
10     res;})
```

この10行のコードは、インラインアセンブラーのマクロ機能を定義するものです。アセンブラー文を使用するには、マクロの中に入れるのが最も便利です。括弧で囲まれた複合文（中括弧の文）。”({})”は式として使用でき、最終行の変数res(10行目)が式の出力値となります。次項で説明します。

マクロ文は1行で定義する必要があるため、ここではバックスラッシュを使って連結しています。このマクロ定義は、マクロ名が参照されるプログラムに代入されます。1行目では、マクロ関数名get\_seg\_byte(seg,addr)として、マクロの名前を定義しています。3行目では、レジスタ変数\_\_resを定義しています。この変数は、素早くアクセスして操作できるように、レジスタに保存されます。レジスタ(eaxなど)を指定したい場合は、「register char res asm ("ax");」のように記述しますが、「asm」は「sm」とも書くことができます。4行目の「asm」は、埋め込みアセンブリ文の先頭を示しています。4行目から7行目までの4つの文は、AT&T形式のアセンブリ文です。また、gccが生成するアセンブリ言語プログラムにおいて、レジスタ名の前にパーセント記号「%」を付けるためには、アセンブリ文のレジスタ名を埋め込む前にパーセント記号「%%」を2つ記述する必要があります。

8行目は出力レジスタです。この文の意味は、このコード実行の終了後、eaxで表されるレジスタの値を、この関数の出力値としてres変数に置くことです。"=a"の"a"はロードコードを呼び出し、"="はこれが出力レジスタであることを示し、そこにある値を出力の値を表します。ロードコードとは、CPUのレジスタやメモリのアドレス、一部の数値などを表す略式文字コードです。表3-

4は、私たちがよく使うレジスタのロードコードとその具体的な意味を示したものです。9行目は、このコードの実行開始時にeaxレジスタにsegが置かれることを表し、"0"は上記と同じレジスタが出力されることを表します。(\*addr)は、メモリオフセットのアドレス値を表す。このアドレス値を上記のアセンブラー文で使用するために、組み込みアセンブラプログラムでは、出力レジスタと入力レジスタに、それぞれ「%0」で始まる出力レジスタ列の左と右の上から順に番号を付けていくように指定しており、%0、%1、...%9と表記しています。したがって、出力レジスタの番号は%0（ここでは出力レジスタは1つだけ）、入力レジスタの最初の部分 ("0" (セグ) ) は番号%1

、後半の部分は番号%2となります。上記6行目の%2は、このメモリオフセットを(\*addr)表しています。

Table 3-4 Common register load code description

Code	Description	Code	Description
a	Use register eax	m	Use memory address, any memory operand is allowed.
b	Use register ebx	o	Use memory address, and can add offset value
c	Use register ecx	I	Use constants 0-31
d	Use register edx	J	Use constants 0-63
S	Use register esi	K	Use constants 0-255
D	Use register edi	L	Use constants 0-65535
q	Use dynamically allocated byte addressable registers (eax、ebx、ecx 或 edx)	M	Use constants 0-3
r	Use any dynamically allocated register	N	Use 1 byte constant (0-255)
g	Any general register, memory or immediate integer operand is allowed (eax、ebx、ecx、edx or memory variable)	O	Use constants 0-31
A	Combine eax with edx (64-bit)	=	Output operands. The output value will replace the previous value
+	Indicates that the operand is readable and writable	&	Early-clobber operands. Indicates that the content will be modified before the operands are used

では、4~7行目のコードの機能を見てみましょう。第1文では、fsセグメントレジスタの内容をスタックに置き、第2文では、eaxのセグメント値をfsセグメントレジスタに割り当て、第3文では、fs:(\*(addr))で指定されたバイトをalレジスタに入っています。.アセンブリ文を実行すると、出力レジスタeaxの値がマクロ関数(ブロック構造式)の戻り値としてresに入ります。簡単でしょう？

以上の分析から、マクロ名のsegは指定されたメモリセグメントの値を表し、addrはメモリオフセットのアドレス量を表していることがわかります。今まででは、このプログラムの機能について明確にしておく必要がありましたこのマクロ関数の機能は、指定されたセグメントとオフセット値のメモアドレスから1バイトをフェッチすることです。では、次の例を見てください。

---

```

01  asm("cld\n\t"
02      "rep\n\t"
03      "stos"
04      : /* No output register */
05      : "c"(count-1), "a"(fill_value), "D"(dest)
06      : "%ecx", "%edi");

```

---

1~3行目は、通常のアセンブリ文で、方向ビットをクリアして、値を繰り返し格納します。1~2行目にある「\」という文字は、gccのプリプロセッサの出力プログラムリストをきれいに設定するためのものです。この文字の意味は、C言語と同じです。つまり、C言語のプログラムに対応するアセンブリを生成し、そのアセンブリを呼び出してコンパイルし、ターゲットコードを生成するというのがgccの動作モードです。プログラムを書いたり、デバッグしたりするときに、C言語に対応したアセンブリ

を見たい場合は、プログラムを処理するアセンブラプログラムの前処理の出力を得る必要があります（これは、効率的なコードを書いたり、デバッグしたりするときによく使われます）。アセンブラの出力をきれいな形式で前処理するために、2つの「`^w^`」という形式記号を使うことができます。

4行目は、インラインアセンブラが出力レジスタを使用していないことを示しています。5行目の意味はcount-1の値をecxレジスタにロードし（ロードコードは "c"）、fill\_valueをeaxにロードし、destをedyに入っています。なぜ、このようなレジスタ値のロードを自分でやらずに、gccコンパイラにやらせなければならないのでしょうか？それは、gccが登録中にいくつかの最適化作業を行うことができるからです。たとえば、fill\_valueの値がすでにeaxに入っている場合があります。それがループ文の中にある場合、gccはループ処理全体でeaxを保持する可能性があるので、各ループの中でmovl文を使うことができます。

最後の行は、これらのレジスターの値が変更されたことをgccに伝えるためのものです。これらのレジスタで何をしているのかをgccが知った後は、gccの最適化に役立つことができます。次の例では、どの変数がどのレジスタを使うかを指定することはできず、gccに選択させています。

---

```
01  asm("leal (%1, %1, 4), %0")
02      : [=R] (Y)
03      : "0"(x);
```

---

実効アドレスの計算には「leal」という命令を使用しますが、ここでは簡単な計算に使用します。最初のアセンブラ文「leal (r1, r2, 4), r3」は、 $r1+r2*4 \Rightarrow r3$ を示しています。この例では、xを5倍することができます。このうち、「%0」と「%1」は、gccが自動的に割り当てるレジスタを意味します。ここでは、"%1"が入力値xを入れるレジスタを、"%0"が出力値のレジスタを表しています。レジスタのコードを出力する前に、必ず等号を付けてください。入力レジスタのコードが0または空の場合は、対応する出力と同じレジスタが使用されます。つまり、gccがrをeaxと指定した場合、上記のアセンブル文の意味は次のようになります。

---

```
"leal (eax, eax, 4), eax"
```

---

なお、コードを実行する際に、GCCの最適化によってアセンブリ文が変更されないようにするには、以下のようにasm記号の後にキーワードvolatileを追加する必要があります。この2つの宣言の違いは、プログラムの互換性の面にあります。後者の宣言方法を使用することをお勧めします。

---

```
asm volatile (....);
Or a more detailed explanation is:
__asm__ volatile__(....);
```

---

また、キーワード volatile を関数名の前に置くことで、その関数を装飾して gcc に知らせることができます。コンパイラに、その関数が返されないことを伝えます。これにより、gccはより良いコードを生成することができます。さらに、返さない関数については、このキーワードを使って、gccが誤った警告メッセージを生成するのを防ぐこともできます。たとえば、mm/memory.c の次の文は、関数 do\_exit() と oom() が呼び出し元のコードに戻らなくなったことを示しています。

---

```

31 volatile void do_exit(long code);
32
33 static inline volatile void oom(void)
34 {
35     printk("out of memory\n\r");
36     do_exit(SIGSEGV);
37 }。

```

---

ここにもっと長い例があります。これが読めれば、インラインアセンブリコードは基本的にOKということになります。このコードはinclude/string.hファイルから引用したもので、strncmp()の文字列比較関数の実装です。同様に、この各行の「\」は、gccプリプロセッサの出力リストが見栄え良くなるように設定されています。

---

```

//// String1 is compared with string2 in the first count characters.
// Paras: cs - Strings1, ct - String2, count - The number of characters to compare.
// %0 - eax(_res) return, %1 - edi(cs) String1 ptr, %2 - esi(ct)String2 ptr, %3 - ecx(count) .
// Return: If string1 > string2, ret 1; string1 == string2, ret 0; string1<string2, then ret -1.
extern inline int strcmp(const char * cs,const char * ct,int count)
{
register int __res ;           // _res is a register variable.
__asm__("cld\n"
        "1:\tdecl %3\n\t"      // Clear direction.
        "js 2f\n\t"             // count--.
        "lodsb\n\t"             // If count<0, go forward to label 2.
        "scasb\n\t"             // Take string 2 character ds:[esi]=>al, and esi++.
        "jne 3f\n\t"             // Compare char in al and in string1 es:[edi] and edi++.
        "testb %%al,%%al\n\t"    // If they are not equal, go forward to label 3.
        "jne 1b\n"               // Is this character a NULL character?
        "2:\txorl %%eax,%%eax\n\t" // No, go backward to label 1 and continue comparing.
        "jmp 4f\n"                // If it is a NULL char, eax is cleared (return value).
        "3:\tmovl $1,%%eax\n\t"   // Go forward to label 4 and end.
        "jl 4f\n\t"               // eax is set to 1.
        "negl %%eax\n\t"          // If the string2 chars <string1 chars, return 1 and end.
        "4:"                     // Otherwise eax = -eax returns a negative value, ends.
        :"=a" (_res):"D" (cs), "S" (ct), "c" (count):"si","di","cx");
return __res;                  // Return the comparison result.
}

```

---

### 3.3.3 括弧内のコンビネーション・ステートメント

中括弧「{...}」は、変数宣言やステートメントを複合ステートメント（コンビネーションステートメント）やステートメントブロックにまとめ、意的的に1つのステートメントと同等になるようにするために使用します。複合文の閉じ括弧の後にセミコロンを使用する必要はありません。括弧内の複合文、すなわち"(...)"

"形式の文は、GNU

Cでは式として使用することができます。これにより、ループ、switch文、ローカル変数を式の中で使用することができるため、この形式の文は、しばしば

文章表現です。文章表現は、以下のような例示形式になっています。

---

```
({ int y = foo(); int z;
  if (y > 0) z = y;
  else z = -y;
  3 + z; })
```

---

複合ステートメントの最後のステートメントは、セミコロンが続く式でなければなりません。この式の値（「3 + z」）は、全体の括弧で囲まれた値として使用されます。最後の文が式でない場合は、文の式全体がvoid型であるため、値はありません。また、このような式の中のステートメントで宣言されたローカル変数は、ブロックステートメント全体が終了した後に失効します。このサンプル文は、次のような形式の代入文のように使うことができます。

---

```
res = x + ({0mit...}) + b;
```

---

もちろん、普通の人は上記のような文を書かないので、通常はマクロの定義に使われます。例えば、カーネルのソースコードであるinit/main.cプログラムの中にあるCMOSクロック情報を読み取るためのマクロ定義です。

---

```
69 #define CMOS_READ(addr) ({ \
70     outb_p(0x80|addr, 0x70); \
71     inb_p(0x71); \
72 })
```

---

// First, output the addr to the I/O port 0x70.  
// Then read the value from port 0x71 as the return value.

ヘッダファイルinclude/asm/io.hのリードI/Oポートのマクロ定義をもう一度見てみると、最後の変数\_vの値がinb()の戻り値になっています。

---

```
05 #define inb(port) ({ \
06     unsigned char _v; \
07     __asm volatile ("inb %%dx, %%al": "=a" (_v): "d" (port)); \
08     _v; \
09 })
```

---

### 3.3.4 変数の登録

C言語に対するGNUのもう一つの拡張機能では、いくつかの変数の値をCPUのレジスタに入れるすることができます。いわゆるレジスタ変数です。この方法では、CPUは値を求めてメモリにアクセスするために長い時間を費やす必要がありません。レジスタ変数には、グローバルレジスタ変数とローカルレジスタ変数の2種類がある。グローバルレジスタ変数は、プログラムの動作中、複数のグローバル変数専用のレジスタを保持する。一方、ローカルレジスタ変数は、指定されたレジスタを保持せず、特別なレジスタはインラインasmアセンブリステートメントの入力または出力オペランドとしてのみ使用されます。gccコンパイラのデータフロー解析機能は、指定されたレジスタに使用中の値があるかどうか、他のフィールドをディスパッチできるかどうかを本質的に判断することができます。gccのデータフ

ロー解析機能は、ローカル・レジスタ変数の値が無駄になったときに格納されていると考えられる場合、その値を削除したり、ローカル・レジスタ変数への参照も削除、移動、簡略化したりすることができます。したがって、gccにこのような最適化の変更をさせたくない場合には、asm文にvolatileキーワードを追加するとよいでしょう。

アセンブラー命令の出力をインラインで指定したレジスタに直接書き込みたい場合はアセンブラー文では、このときにローカルレジスタ変数を使うと便利です。Linuxカーネルでは、通常、ローカルレジスタ変数しか使用しませんので、ここでは、ローカルレジスタ変数の使い方についてのみ説明します。GNU Cプログラムでは、次のように関数の中でローカルレジスタ変数を定義します。

---

register int res asm ("ax") です。

---

ここで ax は、変数 res が使用したいレジスタです。このようなレジスタ変数を定義しても、特にこのレジスタを他の目的のために確保するわけではありません。プログラムのコンパイル中に、gccのデータフロー制御によって、変数の値が使用されなくなったと判断された場合、そのレジスタは他の目的のためにディスパッチされたり、そのレジスタへの参照が削除されたり、移動されたり、簡略化されたりします。また、gccはコンパイルされたコードが変数を指定されたレジスタに保持することを保証しません。したがって、アセンブリに組み込まれる命令の部分では、このレジスタを明示的に参照しない方がよく、レジスタがこの変数の値を参照しなければならないと考えられます。ただし、この変数をasmのオペランドとして使用すると、指定されたレジスタがオペランドとして使用されることが保証されます。

### 3.3.5 インライン機能

プログラムの中で、関数をインライン関数として宣言することで、gccは関数のコードを関数を呼び出すコードに統合することができます。この処理により、関数呼び出し時の入出力のオーバーヘッドを取り除くことができ、実行速度を確実に向上させることができます。したがって、関数をインライン関数として宣言する主な目的は、関数本体ができるだけ早く実行できるようにすることにあります。また、インライン関数の中に定数値がある場合、gccはコンパイル時にその定数値を使って何らかの簡略化を行うことがありますので、すべてのインライン関数コードが埋め込まれるわけではありません。インライン関数方式は、プログラムコードの長さに明らかな影響はありません。インライン関数を使用してコンパイルされたプログラムは、状況に応じて長いまたは短いターゲットコードを生成します。

インライン関数を呼び出し側のコードに埋め込む操作は、最適化操作であるため、最適化されたコンパイルが行われた場合にのみコード埋め込み処理が行われます。コンパイル時に最適化オプション「-O」を使用しなかった場合、インライン関数のコードは実際には呼び出し元のコードには埋め込まれず、通常の関数呼び出しとしてのみ扱われます。関数をインライン関数として宣言するには、カーネルファイル fs/inode.c 内の以下の関数のように、関数宣言にキーワード "inline" を使用します。

---

```

01 inline int inc(int *a)
02 {
03     (*a)++;
04 }
```

---

関数内のいくつかのステートメントを使用すると、インライン関数の置き換えが正常に行われない場合や、置き換え操作に適していない場合があります。例えば、変数パラメータ、メモリ確保関数 `malloc()`、可変長データ型変数、ノンローカル goto 文、再帰関数などが使用されています。コンパイラは、オプション -Winline を使用することで、INLINEとマークされているのに置換できない関数について、その理由を含めた警告情報を `gcc` に与えることができます。

関数定義において、`inline`キーワードと`static`キーワードの両方を使用した場合、例えば以下のファイル `fs/inode.c` のインライン関数の定義では、インライン関数の呼び出しが置換された場合、すべての呼び出しが置換されます。呼び出し側のコードで、プログラムがインライン関数のアドレスを参照していない場合、インライン関数のアセンブリコード自体は参照されません。この場合、コンパイル時にオプション `-fkeep-inline-functions` を使用しない限り、`gcc` はインライン関数自体の実際のアセンブリコードを生成しなくなります。何らかの理由で、いくつかの

インライン関数の呼び出しを関数に統合することはできません。特に、インライン関数の定義の前にある呼び出し文は統合によって置き換えられず、再帰によって定義された関数にすることはできません。統合で置き換えられない呼び出しがあった場合、インライン関数は通常通りアセンブリコードにコンパイルされます。もちろん、プログラムにインライン関数のアドレスを参照するステートメントがあれば、インライン関数も通常通りアセンブリコードにコンパイルされます。インライン関数のアドレスへの参照は置き換えられないからです。

---

```

20 static inline void wait_on_inode(struct m_inode * inode)
21 {
22     cli();
23     while (inode->i_lock)
24         sleep_on(&inode->i_wait);
25     sti();
26 }
```

---

なお、ISO標準C99にはインライン関数の機能が盛り込まれていますが、この標準で定義されているインライン関数は、`gcc` で定義されているものとは全く異なります。ISO標準C99のインライン関数のセマンティックな定義は、キーワード `inline` と `static` の組み合わせの定義と同等であり、キーワード `static` を「排除」することを意味します。プログラムにC99規格のセマンティクスを使用する必要がある場合は、コンパイルオプション `-std=gnu99` を使用する必要があります。しかし、互換性を保つためには、この場合でもINLINEとスタティックの組み合わせを使うのがベストです。その後、`gcc` は最終的にC99の定義をデフォルトで使用するようになります。ここで定義されたセマンティクスをまだ使いたい場合は、オプション -

std=gnu89 を使って指定する必要があります。

インライン関数の定義にキーワード static が使われていない場合、gcc は他のプログラムファイルでもこの関数が呼び出されていると判断します。グローバルシンボルは一度しか定義できないため、他のソースファイルでその関数を定義することはできなくなります。したがって、インライン関数の呼び出しを、ここで統合で置き換えることはできません。したがって、非静的なインライン関数は、常に独自のアセンブリコードでコンパイルされます。この点、ISO 標準 C99 の static キーワードを使用しないインライン関数の定義は、ここで static キーワードの定義を使用することと同じです。

関数の定義時に inline と extern の両方のキーワードが指定されている場合、関数の定義は inline の統合にのみ使用され、関数が明示的に参照されていても、関数自身のアセンブリコードはいかなる場合でも個別に生成されません。また、アドレスも生成されません。このようなアドレスは、関数を定義せずに関数を宣言しただけの場合と同様に、外部参照となります。

inline と extern の組み合わせは、マクロ定義とほぼ同じです。この組み合わせ方法は、組み合わせキーワードを持つ関数定義を.h ヘッダーファイルに置き、キーワードを持たない同じ関数の定義をライブラリファイルに置くというものです。このとき、ヘッダーファイルに定義があると、その関数の呼び出しのほとんどが置換によって埋め込まれます。置換されていない関数の呼び出しがある場合は、プログラムファイルやライブラリのコピーが使用されます（参照されます）。Linux 0.1x カーネルのソースコードに含まれる include/string.h, lib/strings.c というファイルが、この使用例です。たとえば、string.h には次のような関数が定義されています。

---

```
// Copy the string (src) to another string (dest) until it encounters a NULL character.
// Paras: dest - dest string ptr, src - source string ptr. %0 - esi(src), %1 - edi(dest).
27 extern inline char * strcpy(char * dest, const char *src)
28 {
29     __asm__ ("cld\n"
30             "1: tlodsb\n"
31             "stosb\n"
32             "testb %%al, %%al\n"
33             "jne 1b"
34             :: "S" (src), "D" (dest): "si", "di", "ax");
35     return dest;
36 }
```

---

カーネルライブラリのディレクトリにある lib/strings.c ファイルでは、以下のようにインラインとエクステーンというキーワードが空しく定義されています。したがって、実際には、カーネルライブラリには、string.h ファイル内のこれらの関数のすべてのコピーが含まれており、それによって、これらの関数が一度再定義され、2つのキーワードの効果が「なくなる」のです。

---

```
11 #define extern // Defined as empty.
12 #define inline // Defined as empty.
13 #define _LIBRARY
14 #include <string.h>
15
```

---

上記で定義したライブラリ関数のstrcpy()は、次のようにになります。

---

```

27 char * strcpy(char * dest, const char *src) // Removed keywords inline and extern.
28 {
29     asm ("cld\n"
30          "1: |tlodsb|n|t"           // Clear direction.
31          "stosb|n|t"             // Load DS: [esi] 1 byte => al and update esi.
32          "testb %%al, %%al|n|t"   // Store byte al=>ES:[edi] and update edi.
33          "jne 1b"                // Just stored byte al is 0?
34          :: "S" (src), "D" (dest): "si", "di", "ax");
35 return dest;                                // Returns the destination string pointer.
36 }
```

---

## 3.4 C言語とアセンブリ言語のインターワーク

コードの実行効率を高めるために、カーネルのソースコードの一部ではアセンブリ言語を直接使用しています。その際、2つの言語プログラム間の呼び出し問題が発生します。ここでは、まずC言語の関数の呼び出しの仕組みを説明し、次に例を用いて2つの関数間の呼び出し方法を説明する。

### 3.4.1 Cファンクションコール機構

Linuxカーネルプログラムboot/head.sが基本的な初期化処理を行った後、init/main.cプログラムの実行にジャンプします。では、head.sプログラムは、どのようにしてinit/main.cプログラムに実行制御を移すのでしょうか？それは、アセンブリがC言語のプログラムを実行するためにどのように呼び出しているのか？ここでは、まずC言語の関数呼び出しの仕組み、制御転送モードを説明し、その後、head.sプログラムがCプログラムにジャンプすることを説明します。

関数呼び出しの操作には、あるコードから別のコードへの双方向のデータ転送と実行制御の転送があります。データの受け渡しは、関数のパラメータと戻り値によって行われます。また、関数に入るときには関数のローカル変数の記憶領域を確保し、関数を抜けるときにはこの領域を取り戻す必要があります。インテル80x86のCPUでは、制御の受け渡しには簡単な命令が用意されていますが、その一方で

データや、ローカル変数の記憶領域の確保と回復は、スタック操作によって実現されます。

### 3.4.1.1 スタックフレーム構造と制御伝達方法

ほとんどのプログラム実装では、関数呼び出し操作をサポートするためにスタックを使用します。スタックは、関数のパラメータを転送したり、リターン情報を保存したり、リカバリのためにレジスタの元の値を一時的に保存したり、ローカルデータを保存したりするために使用されます。1つの関数呼び出し操作で使用されるスタックの部分は、スタックフレーム構造と呼ばれます。その一般的な構造を図3-4に示します。スタックフレーム構造の両端は、2つのポインタで指定されます。レジスタebpは通常、フレームポインタとして使用され、espはスタックポインタとして使用されます。関数の実行中、スタックポインタespは、スタックに PUSHされるデータとともに移動します。したがって、関数内のほとんどのデータアクセスは、フレームポインタebpに基づいて行われます。

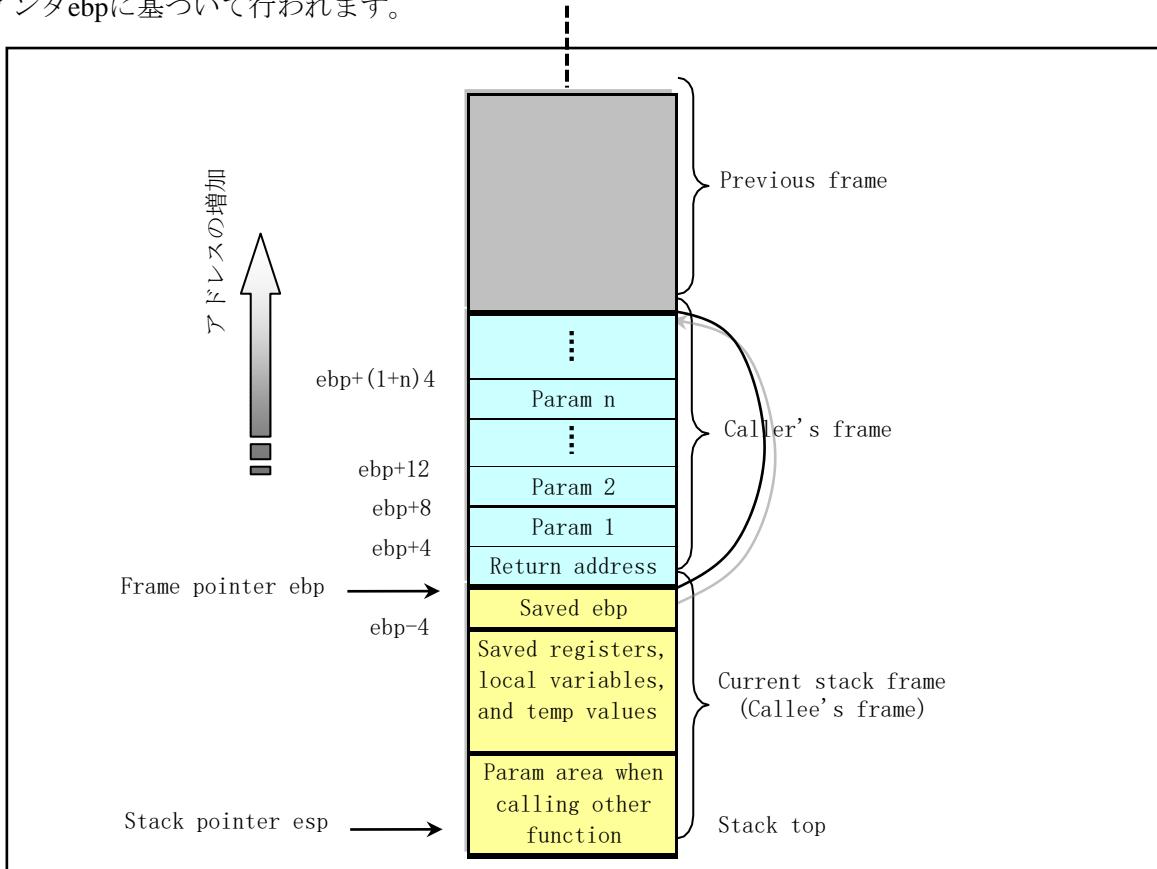


Figure 3-4 Frame structure in the stack

関数Aが関数Bを呼び出す場合、Bに渡されるパラメータはAのスタックフレームに含まれています。AがBを呼び出す際には、関数Aのリターンアドレス（呼び出しが返された後に実行を継続する命令のアドレス）がスタックに PUSHされます。また、このスタック上の位置は、Aのスタックフレームの終わりを明示的に示しています。Bのスタックフレームは、フレームポインタ（ebp）が格納されている後続のスタックセクションから始まります。その後、保存されたレジスタ値や関数の一時的な値を格納するために使用されます。

B関数は、レジスタに配置できないローカル変数の値を保持するためにもスタックを使用します。例えば、通常のCPUではレジスタの数が限られており、関数のローカルデータをすべて格納することができないとか、ローカル変数の中には配列や構造体のものがあるので、配列や構造体の参照を使つ

てアクセスしなければならないなどです。また、C言語のアドレス演算子「&」がローカル変数に適用された場合、変数のアドレスを生成する必要があり、変数のアドレスポインタのための空間が確保されます。最後に、B関数はスタックを使用して、他の関数を呼び出すパラメータを保存します。

スタックはロー（スマール）アドレスに向かって拡張され、espは現在のスタックのトップにある要素を指します。プッシュ命令とポップ命令を使うことで、データをスタックにプッシュしたり、スタックからポップしたりすることができます。初期データが指定されていない記憶領域では、スタックポインタを適切な値だけデクリメントすることでこれを行うことができます。同様に、スタックポインタの値を増やすことで、スタック上に割り当てられた空間を取り戻すことができます。

関数の呼び出しと戻りの操作には、CALLとRETという命令が使われる。CALL命令の効果は、リターンアドレスをスタックにプッシュし、呼び出された関数の先頭にジャンプすることである。リターンアドレスとは、プログラム内でCALL命令の直後にある命令のアドレスのことです。そのため、呼び出された関数が戻ってきたときには、その位置から続けて実行されます。リターン命令RETは、スタックの先頭のアドレスをポップアップし、そのアドレスにジャンプするために使用します。この命令を使用する前に、スタックの内容を正しく処理して、現在のスタックポインタが前のCALL命令で返されたものと同じになるようにしなければなりません。また、戻り値が整数またはポインタの場合は、戻り値を渡すためにレジスタeaxがデフォルトで使用されます。

一度に実行されるのは1つの関数だけですが、ある関数(caller)が別の関数(callee)を呼び出す際に、calleeがcallerが将来使用するレジスタの内容を変更したり上書きしたりしないようにする必要があります。そのため、インテルのCPUでは、すべての関数が遵守しなければならないレジスタの使用方法を統一しています。この規約では、レジスタeax、edx、ecxの内容は、呼び出し元自身が保持しなければならないことを示しています。関数BがAから呼び出されたとき、関数Bは、関数Aが必要とするデータを破壊することなく、これらのレジスタの内容を保存することなく、任意に使用することができます。さらに、レジスタebx、esi、およびediの内容は、呼び出し側Bによって保護されなければなりません。呼び出し側のA（または上位の関数）はこれらのレジスタの内容を保存する責任がないため、今後の操作で元の値を使用する必要があるかもしれません。また、2つ目の規約の使い方に従わなければならぬレジスタebpとespがあります。

### 3.4.1.2 機能呼び出しの例

例として、次のC言語プログラムexch.cの関数呼び出しの処理を見てみましょう。このプログラムは、2つの変数の値を交換し、その差を返します。

---

```

1 void swap(int * a, int *b)
2 {
3     int c;
4     c = *a; *a = *b; *b = c;
5 }
6
7 int main()
8 {
9     int a, b;
10    a = 16; b = 32;
11    swap(&a, &b);
12    return (a - b);
13 }
```

---

`swap()`という関数は、2つの変数の値を交換するために使われます。Cプログラムのメインプログラムである`main()`も関数である（後述）。`swap()`を呼び出した後、スワップされた結果を返します。これら2つの関数のスタックフレーム構造を図35に示します。ご覧のとおり、`swap()`関数は呼び出し元（`main()`）のスタックフレームからパラメータを取得しています。図中の位置情報は、レジスタ`ebp`内のフレームポインタからの相対値です。スタックフレームの左側にある数字は、フレームポインタに対するアドレスオフセット値を示しています。gdbなどのデバッガでは、これらの値は2の補数で表されます。例えば、「-4」は「0xFFFFFFF4」と表されます。

となり、「-12」は「0xFFFFFFFF4」と表現されます。

呼び出し元の`main()`のスタックフレーム構造には、フレームポインタに対して-4と-8のオフセットに位置するローカル変数`a`と`b`の格納スペースが含まれています。この2つのローカル変数のアドレスを生成する必要があるため、単にレジスタに格納するのではなく、スタックに格納する必要があります。

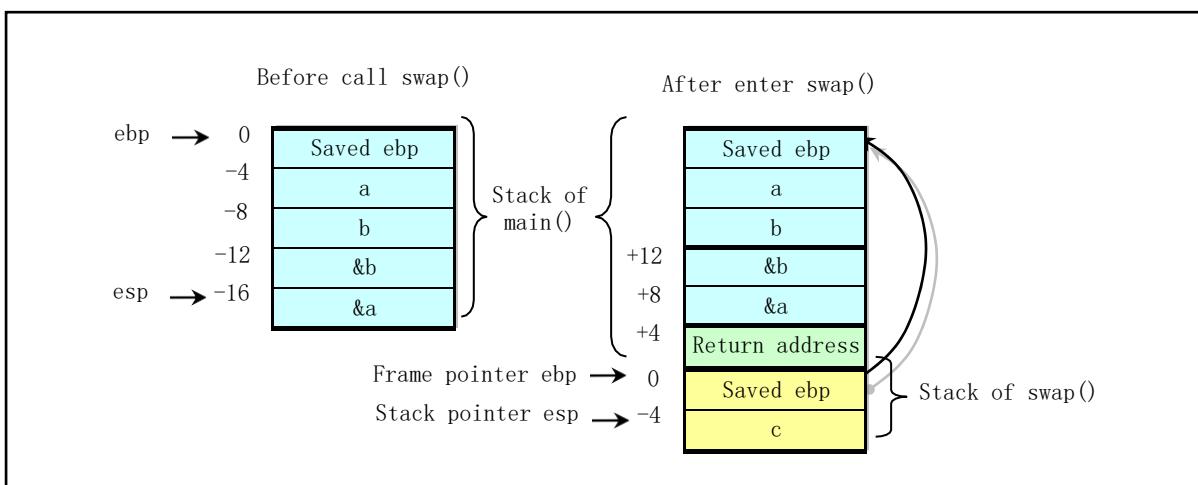


Figure 3-5 Stack frame structure when calling function main and swap

gcc -Wall -S -oexch.s  
`exch.c` コマンドを使用して、このC言語プログラムのアセンブリ`exch.s`コードを以下のように生成します（議論に関係のない数行の指示を削除します）。

```

1 .text
2 _swap:
3     pushl %ebp          # Save original ebp, set current function's frame pointer.
4     movl %esp,%ebp
5     subl $4,%esp         # Allocates space within the stack for the local variable c.
6     movl 8(%ebp),%eax    # Get 1st argument, which is a pointer to an integer value.
7     movl (%eax),%ecx     # Store value pointed by the pointer into variable c.
8     movl %ecx,-4(%ebp)   # Take 1st parameter again, and then take 2nd parameter.
9     movl 8(%ebp),%eax
10    movl 12(%ebp),%edx
11    movl (%edx),%ecx
12    movl %ecx,(%eax)
13    movl 12(%ebp),%eax
14    movl -4(%ebp),%ecx

```

---

```

15      movl %ecx, (%eax)
16      leave                      # Restore the original ebp and esp.
17      ret
18 _main:
19      pushl %ebp                  # Save original ebp, set current function's frame pointer.
20      movl %esp, %ebp
21      subl $8, %esp              # Allocates space in stack for local variables a and b.
22      movl $16, -4(%ebp)          # Assign initial values to variables (a=16, b=32).
23      movl $32, -8(%ebp)
24      leal -8(%ebp), %eax        # To call the swap(), push the address of variable b onto
25      pushl %eax                # stack. That is, push the second parameter first.
26      leal -4(%ebp), %eax        # Then push address of variable a as the first parameter.
27      pushl %eax
28      call _swap                # Call the function swap().
29      movl -4(%ebp), %eax        # Take the value of a - b.
30      subl -8(%ebp), %eax
31      leave                      # Restore the original ebp and esp.
32      ret

```

---

この2つの関数は、独立して3つの部分に分ることができます。スタックフレーム構造を初期化する "set"、関数の実際の計算を行う "body"、スタックの状態を復元して関数から戻る "end" です。swap()関数の場合、設定部分のコードは3~5行です。最初の2行は、呼び出し元のフレームポインタの設定と、関数のスタックフレームポインタの設定に使われます。5行目では、スタックポインタ espを4バイト下に移動させることで、ローカル変数cの領域を確保しています。6~15行目はswap関数のメイン部分です。6-

8行目は、呼び出し元の最初のパラメータである&aを取得し、このパラメータをアドレスとして、メモリの内容をecxレジスタにフェッチし、ローカル変数に割り当てられたスペース(-4(%ebp))に保存するために使用されます。9-

12行目は、2番目のパラメータである&bをフェッチし、そのパラメータ値をアドレスとして、その内容を1番目のパラメータで指定されたアドレスに取り込みます。13~15行目は、一時的なローカル変数cに格納された値を、第2パラメータで指定されたアドレスに格納しています。最後の16~17行目が関数の終了です。leave命令は、リターンに備えてスタックの内容を処理するために使用されます。その役割は、以下の2つの命令と同等です。

---

movl %ebp, %esp	# Restores original esp (to beginning of stack frame).
popl %ebp	# Restores original ebp (usually the caller's frame ptr).

---

この2行のコードは、swap()関数の入力時にレジスタespとebpの値を元に戻し、ret命令を実行するものです。

19-

21行目はmain()関数のセット部分です。フレームポインタの保存とリセットを行った後、main()はスタック上にローカル変数aとbの領域を確保します。22-

23行目では、この2つのローカル変数に値を割り当てています。24~28行目では、main()がswap()関数を呼び出していることがわかります。まず、leal命令（実効アドレスの取得）で変数bとaのアドレスを取得してスタックにプッシュしてから、swap()関数を呼び出しています。変数のアドレスがスタックにpushされる順番は、関数で宣言されたパラメータの順番とは全く逆になります。つまり、関数の最

後のパラメータが最初にスタックにプッシュされ、関数の最初のパラメータは、関数命令呼び出しの前にスタックにプッシュされます。29--

30行目では、すでに交換された2つの数値を引き算し、それを戻り値としてeaxレジスタに入っています。

以上の分析から、C言語は関数を呼び出す際に、転送された関数パラメータの値を一時的にスタックに格納することがわかります。つまり、C言語は値ベースの言語なのです。呼び出された関数の呼び出し側の変数を直接修正する方法はありません。

値を修正します。したがって、修正の目的を達成するためには、変数へのポインタ（つまり、変数のアドレス）を関数に渡す必要があります。

### 3.4.1.3 また、Main()は関数

上記のアセンブラーコードは、gcc

1.40を使ってコンパイルされています。数行の余分なコードがあることがわかります。これは、当時のgcc

コンパイラが最も効率的なコードを生成できなかったことを示しています。これが、いくつかの重要なコードを直接アセンブリ言語でコンパイルする必要がある理由の1つです。また、先ほどのC言語プログラムのメインプログラムも関数です。これは、リンクをコンパイルしたときに、crt0.sというアセンブラープログラムの関数として呼び出されるからです。crt "は "C run-time "の略です。このプログラムのターゲットファイルは、各ユーザーの実行プログラムの最初にリンクされ、主にいくつかの初期化グローバル変数を設定するために使用されます。Linux 0.12でのcrt0.sアセンブラープログラムを以下に示します。プログラム内の他のモジュールが使用するために、グローバル変数\_environが作成され、初期化されます。

---

```

1 .text
2 .globl _environ          # Declare the global variable _environ. (correspond to
3                                # the environ variable in C program).
4 __entry:                   # Code entry label.
5     movl 8(%esp), %eax   # Get environment variable pointer envp, save in _environ.
6     movl %eax, _environ   # envp is set by execve() when executable file is loaded.
7     call _main            # Call main program. Its return status is in eax register.
8     pushl %eax           # Push return value as an argument to exit() and call it.
9 1:    call _exit          # Control should not arrive here.
10    jmp 1b
11 .data
12 _environ:                # Define variable _environ and assign it a long word space.
13     .long 0

```

---

実行ファイルのコンパイルとリンクにgccを使用した場合、gccは自動的にcrt0.sのコードを実行プログラムの最初のモジュールとしてリンクします。コンパイル時にshow detailsオプション'-v'を使用すると、リンク処理を明確に確認することができます。

---

```

[/usr/root]# gcc -v -o exch exch.s
gccバージョン1.40
/usr/local/lib/gcc-as -o exch.o exch.s
/usr/local/lib/gcc-ld -o exch /usr/local/lib/crt0.o exch.o /usr/local/lib/gnulib -lc
/usr/local/lib/gnulib
[/usr/root]#

```

---

そのため、通常のコンパイルでは、スタブモジュールであるcrt0.oを指定する必要はありませんが、ld(gld)を使用して、上記で示したアセンブリプログラムから手動でexch.oモジュールから実行ファイルを生成する場合には　　コマンドラインでcrt0.oモジュールを指定し、リンク順序を　　"crt0.o,すべてのプログラムモジュール, ライブラリファイル"とする必要があります。

ELF形式のオブジェクトファイルを使用し、共有ライブラリのモジュールファイルを作成するために、現在のgccコンパイラ(2.x)では、このcrt0を複数のモジュールに拡張しています：crt1.o、crti.o、crtbegin.crt1.o、crti.o、crtbegin.o (crtbeginS.o), 全プログラムモジュール, crtend.o (crtendS.o), crtN.o, ライブラリモジュールファイル」の順にリンクされています。このリンク順序は、gccの設定ファイルspecfileで指定します。ここで、crt1.o, crtI.o, crtN.oは、Cプログラムの「起動」モジュールであるCライブラリから提供され、crtbegin.o, crtend.oは、コンパイラgccから提供されるC++言語の起動モジュールであり、crt1.o

これは、crt0.oの効果と同様に、主にmain()を呼び出す前の初期化作業に使用される。グローバル・シンボル\_startは、このモジュールで定義されています。

crtbegin.oとcrtend.oは、主にC++言語において、.ctorsセクションと.dtorsセクションにグローバルなコンストラクタとデストラクタの関数を実装するために使用されます。crtbeginS.oとcrtendS.oの役割は、最初の2つと同様ですが、共有モジュールを作成するために使用されます。crti.oは、.initセクションの初期化関数init()を実行するために使用されます。.initセクションには、プロセスの初期化コードが含まれています。つまり、プログラムの実行開始時に、システムはmain()を呼び出す前に.initのコードを実行します。CrtN.oは、.fini領域の処理関数fini()を終了させるためのプロセスの実行に使用されます。つまり、プログラムが正常に終了する(main()が戻る)ときに、システムは.finifのコードを実行するよう手配します。

カーネルでは、boot/head.sプログラムの136～140行目が、init/main.cのmain()関数にジャンプするための準備に使われています。139行目の命令はリターンアドレスをスタックにプッシュし、140行目はmain()関数コードのアドレスをプッシュしています。最終的にhead.sが218行目のret命令を実行すると、main()のアドレスがポップアップされ、init/main.cプログラムに制御が移ります。

### 3.4.2 アセンブリコードでC関数を呼び出す

アセンブリコードからC言語の関数を呼び出す方法は、実際に上記のように示されています。上のC言語の例のアセンブリコードでは、アセンブリ文がswap()関数を呼び出していることがわかります。ここで、呼び出し方法をまとめておきます。

C言語の関数をアセンブリコードで呼び出す場合、まず関数のパラメータを逆順にスタックにプッシュする必要があります。つまり、関数の最後（右端）のパラメータが最初にスタックにプッシュされ、最後の命令が呼ばれる前に左端の最初のパラメータがプッシュされるのである。図3-6をご覧ください。その後、CALL命令を実行して、呼び出された関数を実行する。呼び出した関数が戻ってきた後、プログラムは以前にスタックにプッシュされた関数パラメータをクリアする必要があります。

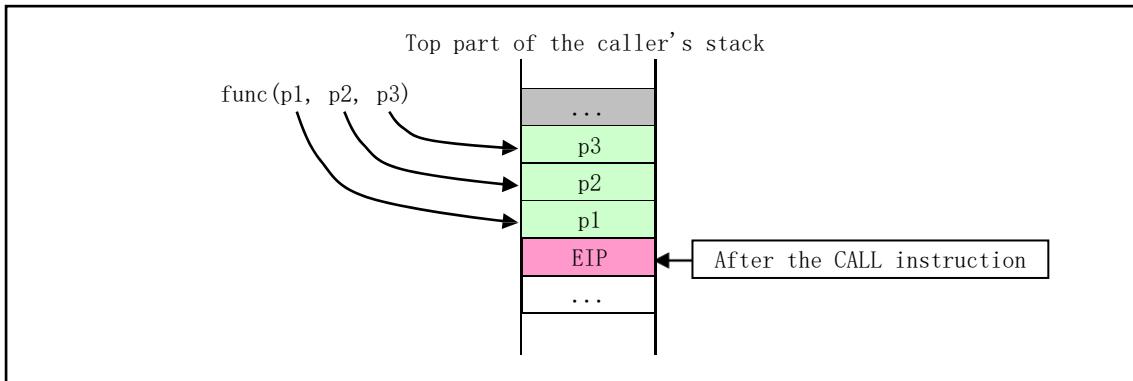


Figure 3-6 The parameters pushed into the stack when the function is called

CALL命令が実行されると、CPUはCALL命令の次の命令のアドレスをスタックにプッシュします（図のEIP参照）。呼び出しにコードの特権レベルの変更も伴う場合、CPUはスタックスイッチを行い、現在のスタックポインタ、セグメントディスクリプタ、呼び出しパラメータを新しいスタックにプッシュします。なお、Linuxカーネルでは、呼び出し時の特権レベル変更の処理には割り込みゲートとトラップドアのみを使用し、CALL命令は使用していないため、ここでは特権レベル変更時のCALL命令の使用について説明しない。

アセンブリでC関数を呼び出すことは、比較的自由です。スタック内の適切な場所にあれば、C関数のパラメータとして使用することができます。ここではまだ、図3-

6の3つのパラメータを持つ関数呼び出しを例にしています。func()で引数をプッシュして直接呼び出さなくても、func()関数はEIPの位置を保存します。スタックの残りの部分は、自分のパラメータとして使われます。もし、func()呼び出しのために、1番目と2番目のパラメータを明示的に押したとすると、func()関数の3番目のパラメータp3は、p2以前のスタックの内容を直接使用します。このLinux 0.1xのカーネルコードにはいくつかの箇所があります。例えば、copy\_process()関数(kernel/fork.cの68行目)は、kernel/sys\_call.sのアセンブリプログラムの231行目で呼び出されています。アセンブリ関数\_sys\_forkでは5つのパラメータしかスタックにプッシュされていませんが、copy\_process()では以下のように最大で17個のパラメータが設定されています。

```

226      push %gs
227      pushl %esi
228      pushl %edi
229      pushl %ebp
230      pushl %eax
231      call _copy_process      # Call the C function copy_process() (kernel/fork.c, 68).
232      addl $20,%esp          # Discard all the pushed content here.
233 1:     ret

```

---

```

// kernel/fork.c partial program.
68 int copy_process(int nr, long ebp, long edi, long esi, long gs, long none,
69             long ebx, long ecx, long edx, long orig_eax,
70             long fs, long es, long ds,
71             long eip, long cs, long eflags, long esp, long ss)

```

---

パラメータがスタックにpushされるのが遅ければ遅いほど、C関数のパラメータの左端に近いことがわかっています。したがって、copy\_process()が呼ばれる前に実際にpushされた5つのレジスタ値が、copy\_process()関数の5つの左端のパラメータとなります。順に、スタックされているeax(nr)、ebp、edi、esi、レジスタgsの値に対応しています。以下のパラメータの残りの部分は、実際にはすでにスタック上にあるものに直接対応しています。これらの内容は、システムコール割り込み処理プロセスが開始されてから、システムコールプロセスが呼び出されるまでの間に、スタックに徐々に追加される各種レジスタの値です。

パラメータnoneは、sys\_call.sプログラムの99行目のアドレスジャンプテーブルから\_sys\_forkが呼び出されたときの、次の命令のリターンアドレスです。アドレスジャンプテーブルsys\_call\_table[]は、ヘッダファイルinclude/linux/sys.hの93行目で定義されています。次のパラメータは、レジスタebx、ecx、edx、元のeax、そしてsystem\_call入力直後の85~91行目でスタックにpushされたセグメントレジスタfs、es、dsです。最後の5つのパラメータは、CPUの実行割り込み命令のpushリターンアドレスeiとcs、フラグレジスタeflags、ユーザースタックアドレスespとssです。システムコールはプログラムの特権レベルの変更を伴うため、CPUはフラグレジスタの値とユーザースタックアドレスをスタックにpushします。呼び出したC関数copy\_process()が戻ってきた後、\_sys\_forkは自分で押した5つのパラメータだけを破棄し、残りのスタックも保存します。上記の使い方をしている他の関数として、kernel/signal.cのdo\_signal()、fs/exec.cのdo\_execve()などがあります。ぜひ、ご自身で解析してみてください。

また、CALL命令を使わずに、JMP命令を使って関数を呼び出すのと同じ目的を達成できるので、アセンブリがC関数を呼び出すのは比較的自由だと言います。その方法は、パラメータをスタックにpushした後、次に実行する命令のアドレスを手動でスタックに入れ、直接JMP命令を使って呼び出された関数の開始アドレスにジャンプして関数を実行するというものです。その後、関数の実行が完了すると、RET命令が実行され、手動でスタックにpushした次の命令のアドレスを、関数から返されたアドレスとしてポップアップします。また、Linuxカーネルでは、kernel/asm.sプログラムの62行目でtraps.cのdo\_int3()関数を呼び出す場合など、様々な方法でこの関数を呼び出すことができます。

### 3.4.3 Cプログラムでアセンブリ関数を呼び出す

Cプログラムからアセンブリ関数を呼び出すことは、アセンブリでC関数を呼び出すことと同じですが、Linuxカーネルプログラムではありません。呼び出し方法の焦点は、やはり関数のパラメータのスタック内の位置の決定にあります。もちろん、呼び出し元のアセンブリ言語プログラムが比較的短ければ、上述のインラインアセンブリ文を使ってCプログラムに直接実装することもできます。以下、例を使ってこのようなプログラムの書き方を説明します。アセンブリは、2つを含むcalle.sの機能を以下に示します。

```
/*
 This assembly language program uses the system call sys_write() to implement the display
 function int mywrite(int fd, char * buf, int count).
 The function int myadd(int a, int b, int * res) is used to perform the a+b = res operation.
 If the function returns 0, it means overflow.
 Note: If you compile under the current Linux system (such as RedHat 9), remove the
 underscore '_' before the function name.*/
SYSWRITE = 4                                # Sys_write() system call number.
.globl _mywrite, _myadd
.text
_mywrite:
    pushl %ebp
    movl %esp, %ebp
    pushl %ebx
    movl 8(%ebp), %ebx      # Take the first argument of the caller: file descriptor fd.
    movl 12(%ebp), %ecx     # The second parameter: buffer pointer.
    movl 16(%ebp), %edx     # The third parameter: display character number.
    movl $SYSWRITE, %eax     # Put system call number 4 in %eax.
    int $0x80                # Execute the system call.
    popl %ebx
    movl %ebp, %esp
    popl %ebp
    ret

_myadd:
    pushl %ebp
    movl %esp, %ebp
    movl 8(%ebp), %eax      # Get the first parameter a.
    movl 12(%ebp), %edx      # Get the second parameter b.
    xorl %ecx, %ecx         # If %ecx is 0, the calculation overflows.
    addl %eax, %edx          # Perform additions.
    jo 1f                    # Jump if it overflows.
    movl 16(%ebp), %eax      # Take the third parameter pointer.
    movl %edx, (%eax)        # Put the result in the position of the pointer.
    incl %ecx                 # No overflow occurred, so set no overflow return value.
1:   movl %ecx, %eax          # %eax is the function return value.
    movl %ebp, %esp
    popl %ebp
    ret
```

---

アセンブリファイルの最初の関数mywrite()は、システム割り込み0x80を利用して、システムコールsys\_write(int fd, char \*buf, int count)を呼び出し、画面に情報を表示します。対応するシステムコールの関数番号は4です（include/unistd.h参照）。3つのパラメータは、ファイルディスクリプタ、表示バッファポインタ、表示文字数です。int 0x80を実行する前に、呼び出し元の関数番号(4)をレジスタ%eaxに入れ、呼び出し規則に従って、レジスタ%ebx、%ecx、%edxにそれぞれfd、buf、countを格納する必要があります。関数の引数であるmywrite()は、sys\_write()と全く同じ数のパラメータと用途を使用しています。

2番目の関数myadd(int a, int b, int \*res)は、足し算の演算を行います。パラメータresは演算の結果です。関数の戻り値は、オーバーフローが発生したかどうかを判断するために使用されます。戻り値が0の場合、計算がオーバーフローしており、結果は得られません。それ以外の場合は、計算の結果は、パラメータresを介して呼び出し側に返されます。

なお、現行のLinuxシステム（例：RedHat

9）でcallee.sをコンパイルする場合は、関数名の前のアンダースコア「\_」を削除してください。この2つの関数を呼び出すCプログラムcaller.cを以下に示します。

---

```

/*
Call assembly function mywrite(fd, buf, count) to display information;
Call myadd (a, b, result) to perform addition. If myadd() returns 0, it indicates
overflow. First, the start calculation information is displayed, and then the operation
result is displayed.

*/
01 int main()
02 {
03     char buf[1024];
04     int a, b, res;
05     char * mystr = "Calculating...\\n";
06     char * emsg = "Error in adding\\n";
07
08     a = 5; b = 10;
09     mywrite(1, mystr, strlen(mystr));
10    if (myadd(a, b, &res)) {
11        sprintf(buf, "The result is %d\\n", res);
12        mywrite(1, buf, strlen(buf));
13    } else {
14        mywrite(1, emsg, strlen(emsg)); 15
15
16    return 0;
17 }

```

---

このプログラムでは、まずアセンブリ関数のmywrite()を使って画面に「Calculating...」という情報を表示し、次に加算計算関数のmyadd()を呼び出して2つの数字aとbを演算し、3番目のパラメータresに計算結果を返します。最後に、mywrite()関数を使って、整形された結果情報文字列を画面に表示します。myadd()関数が0を返した場合は、overflow関数がオーバーフローして計算結果が無効になったことを意味します。この2つのファイルのコンパイル結果と実行結果を以下に示します。

---

```

[/usr/root]# as -o callee.o callee.s
[/usr/root]# gcc -o caller caller.c callee.o
[/usr/root]# ./caller
Calculating...
The result is 15
[/usr/root]#

```

---

## 3.5 Linux 0.12 オブジェクトファイルフォーマット

カーネルコードを生成するために、Linux 0.12は2つのコンパイラを使用しています。一つ目はアセンブリとそれに対応するリンク (またはリンク) ld86 ビットのカーネルブートセクタプログラムと、実アドレスモードで動作するセットアッププログラムのコンパイルとリンクにのみ使用されます。2つ目は、GNUアセンブリas(gas)、Cコンパイラgccとそれに対応するリンクgldです。このコンパイラは

ソースプログラムファイルに対応するバイナリコードとデータのオブジェクトファイルです。リンクは、関連するすべてのオブジェクトファイルを結合して、カーネルが読み込むことのできるターゲットファイル、すなわち実行ファイルを形成するために使用される。

このセクションでは、まず、コンパイラが生成するオブジェクトファイルの構造を簡単に説明し、次に、 linker が、リンクが必要なオブジェクトファイルのモジュールを組み合わせて、バイナリ実行可能なイメージファイルや大きなモジュールファイルを生成する方法を説明します。最後に、Linux 0.12 カーネルのバイナリコードファイル Image の生成原理とプロセスを説明しています。Linux 0.12 カーネルでサポートされている a.out

オブジェクト・ファイル・フォーマットに関する情報を提供しています。 As86 と ld86 は、 MINIX 固有のオブジェクトファイルフォーマットを生成しますが、このフォーマットを扱うカーネル作成ツールの章で紹介します。 MINIX オブジェクトファイルの構造は、 a.out オブジェクトファイルフォーマットと似ているので、ここでは説明しません。オブジェクト・ファイルと linker ・ プログラムの基本的な動作原理は、 John R. Levine の著書 「 Linkers & Loaders 」 に記載されています。

説明の便宜上、コンパイラによって生成されたオブジェクトファイルをオブジェクト・モジュール・ファイル（モジュールファイルと略す）と呼び、リンクプログラムによって生成された実行可能なオブジェクトファイルを実行ファイルと呼ぶ。また、これらを総称してオブジェクトファイルと呼びます。

### 3.5.1 オブジェクトのファイル形式

Linux 0.12 システムでは、 UNIX モジュールの伝統的な a.out 形式が、 GNU gcc または gas コンパイラの出力するオブジェクト・モジュール・ファイルと、 linker が生成する実行ファイルの両方で使用されています。これは、 Assembly & Linker Editor Output というオブジェクトファイル形式です。メモリのページング機構を持つシステムでは、これはシンプルで効果的なオブジェクトファイル形式です。 a.out 形式のファイルは、図 3-7 に示すように、ファイルヘッダとそれに続くコード部（テキスト部ともいう）、初期化データ部（データ部ともいう）、再配置情報部、シンボルテーブル、シンボル名の文字列構成で構成されています。コードセクションとデータセクションは、通常、それぞれテキストセグメント（コードセグメント）、データセグメントとも呼ばれる。

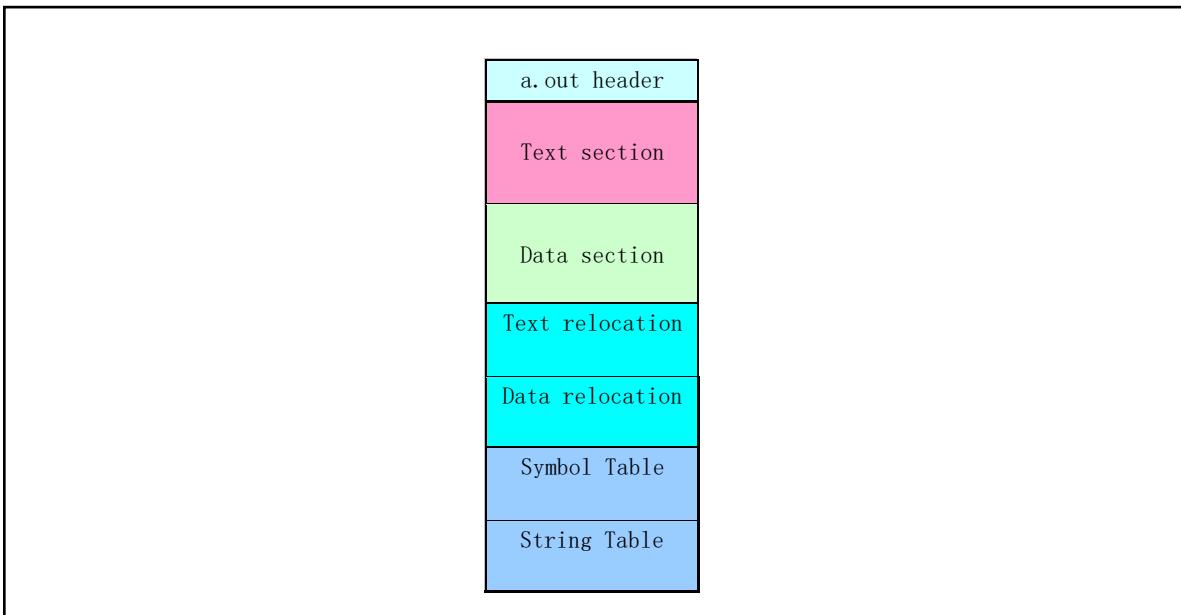


Figure 3-7 a.out format object file

a.outフォーマットの7つのセクションの基本的な定義と用途は以下の通りです。

- エクゼクティブヘッダ。エクゼクティブファイルのヘッダ部です。このセクションには、ターゲット・ファイルの全体的な構造情報である、いくつかのパラメータ (exec構造) が含まれています。例えば、コード領域とデータ領域の長さ、未初期化データ領域の長さ、対応するソースファイル名、ターゲットファイルの作成時刻などです。が含まれています。
- カーネルはこれらのパラメータを使って実行ファイルをメモリにロードして実行し、リンカー (ld) はこれらのパラメータを使ってモジュールファイルの一部を実行ファイルに結合します。対象文書の中で必要な部分はこれだけです。
- テキストセグメント。コンパイラやアセンブラーによって生成されたバイナリの命令コードとデータ情報で、プログラムの実行時にメモリにロードされる命令コードと関連データが含まれている。読み取り専用で読み込むことができる。
- データセグメント。コンパイラやアセンブラーが生成するバイナリ命令コードやデータ情報。このセクションには、すでに初期化されたデータが含まれており、常に読み書き可能なメモリにロードされる。
- テキストの再配置。リンカで使用するレコードデータを格納します。オブジェクト・モジュール・ファイルを結合する際に、コード・セグメント内のポインタやアドレスを特定するために使用します。リンカーがターゲット・コードのアドレスを変更する必要があるときに、修正とメンテナンスを行う必要がある。
- データの再配置。コード再配置セクションの役割と似ていますが、データセグメント内のポインタの再配置に使用されます。
- シンボルテーブルです。このセクションには、リンカーが使用するためのレコードデータも含まれています。これらのレコード・データには、モジュール・ファイルで定義されたグローバル・シンボルや、他のモジュール・ファイルから入力する必要のあるシンボル、あるいはリンカーが

定義したシンボルが格納されており、モジュール・ファイル間で名前付きの変数や関数（シンボル）を交差させるために使用されます。参考文献

- 文字列テーブル。シンボル名に対応する文字列が格納されています。リンクプロセスに關係なく、プログラムのデバッグターゲットコードをデバッグするために使用します。この情報には、ソースコードや行番号、ローカルシンボル、データ構造の記述情報などが含まれます。

あるターゲットファイルに対して、上記の情報のすべてが含まれているとは限りません。Linux 0.12では、インテル製CPUのメモリ管理機能を利用しているため、実行プログラムごとに64MBのアドレス空間（論理アドレス空間）が確保されています。この場合、リンカーが実行ファイルを固定のアドレスから開始するように処理しているため、当該実行ファイルには再配置情報が不要となる。以下、重要な部分を説明する。

### 3.5.1.1 エグゼクティブ・ヘッダー

ターゲットファイルのヘッダー部分には、32バイトのexecデータ構造があり、一般にファイルヘッダー構造や実行ヘッダー構造と呼ばれている。その定義は以下の通りです。a.out構造の詳細については、include/a.out.hファイルの後のイントロダクションを参照してください。

---

```
struct exec {
    unsigned long           a_magic; /* アクセスにはマクロ N_MAGIC
                                      などを使用 */
    unsigned                a_text;  /* テキストの長さ (バイト) */
    /* 符号なし */           a_data;  /* データの長さ (バイト単位) */ /* 符号あり */
    /* 符号なし */           a_bss;   /* ファイルの未初期化データ領域の長さ (バイト) */
    /* 符号なし */           a_syms;  /* ファイルのシンボルテーブルデータの長さ (バイト) */
    /* 符号なし */           a_entry; /* 開始アドレス */
    unsigned                a_trsize; /* テキスト の再配置情報の長さ (バイト)
                                       単位 */          a_drsize; /* データの再配置情報の長さ (バイト单
                                       位) */
};
```

---

a.outファイルのヘッダー構造のマジックナンバーフィールドの値によって、a.outファイルをいくつかのタイプに分けることができます。Linux

0.12系では、2つのタイプを使用しています。モジュール・オブジェクト・ファイルは、OMAGIC (Old Magic) タイプのa.outフォーマットを使用しており、このファイルがオブジェクト・ファイルまたは不純な実行ファイルであることを示しています。このタイプは

マジックナンバーは0x107 (8進数0407) です。実行ファイルは、ZMAGIC a.out形式を使用しており、このファイルがデマンドドリブン (demangling、つまり要求に応じてロードする) ロード用の実行ファイルであることを示しています。マジックナンバーは0x10b (8進数0413) です。この2つのフォーマットの主な違いは、各パートへのストレージの割り当て方である。構造体の全長は32バイトしかありませんが、ZMAGICタイプの実行ファイルの場合、ファイルの先頭部分にはヘッド構造体のために1024バイトのスペースが必要です。プログラムのテキスト・セグメントとデータ・セグメントは、この1024バイトの後にのみ配置されます。OGMIC タイプの.oモジュールファイルでは、ファイルの先頭にある32バイトのヘッダ構造の後に、コード領域とデータ領域が続きます。

実行ヘッダ構造体のa\_textフィールドとa\_dataフィールドは、それぞれ読み取り専用のコードセグ

メントと読み書き可能なデータセグメントのバイト長を示しています。a\_bssフィールドは、カーネルがターゲットファイルをロードする際に、データセグメントに続く未初期化データ領域（bssセクション）の長さを示す。Linuxではメモリを確保する際に自動的にゼロにするので、bssセクションはモジュールファイルや実行ファイルに含める必要はない。ターゲットファイルが論理的にbssセクションを持っていることを視覚的に表現するために、後述の図ではターゲットファイルのbssセクションを破線のボックスで表現している。

a\_entryフィールドは、プログラムコードが実行を開始するアドレスを指定し、a\_syms、a\_trsize、a\_drsizelfieldは、それぞれデータセグメント以降のシンボルテーブル、コード、データセグメントの再配置情報のサイズを記述します。シンボルテーブルと再配置情報は実行ファイルには必要ないで、リンカーがデバッグのためにシンボル情報を含めない限り、実行ファイルのフィールドは通常0である。

### 3.5.12 リロケーション情報欄

#### Linux

0.12システムのモジュールファイルや実行ファイルは、すべてa.out形式のオブジェクトファイルですが、コンパイラが生成したモジュールファイルのみ、プログラムをリンクするためのリロケーション情報が含まれています。コードセグメントとデータセグメントの再配置情報は、再配置レコード（アイテム）で構成される。各レコードの長さは8バイトである。その構造は以下の通りである。

---

```
struct relocation_info
{
    /* Address (within segment) to be relocated. */
    int r_address;
    /* The meaning of r_symbolnum depends on r_extern. */
    unsigned int r_symbolnum:24;
    /* Nonzero means value is a pc-relative offset
       and it should be relocated for changes in its own address
       as well as for changes in the symbol or section specified. */
    unsigned int r_pcrel:1;
    /* Length (as exponent of 2) of the field to be relocated.
       Thus, a value of 2 indicates 1<<2 bytes. */
    unsigned int r_length:2;
    /* 1 => relocate with value of symbol.
       r_symbolnum is the index of the symbol
       in file's the symbol table.
       0 => relocate with the address of a segment.
       R_symbolnum is N_TEXT, N_DATA, N_BSS or N_ABS
       (the N_EXT bit may be set also, but signifies nothing). */
    unsigned int r_extern:1;
    /* Four bits that aren't used, but when writing an object file
       it is desirable to clear them. */
    unsigned int r_pad:4;
};
```

---

再配置アイテムには2つの機能があります。1つは、コードセグメントが異なるベースアドレスに再配置されたときに、再配置アイテムを使用して修正が必要な場所を示すことです。2つ目は、モジュールファイルの中に未定義のシンボルへの参照がある場合、リンカーは対応する再配置アイテムを使って、未定義のシンボルが最終的に定義されたときにシンボルの値を修正することができる。上記の

再配置レコード・アイテムの構造からわかるように、各レコード・アイテムには、再配置が必要なモジュール・ファイルのコード・セクション（コード・セグメント）とデータ・セクション（データ・セグメント）のアドレスが4バイトの長さで含まれており、ポジショニング・オペレーション情報の計量方法が指定されている。アドレスフィールドr\_addressは、再配置可能なアイテムのコードセグメントやデータセグメントの先頭からのオフセット値を参照する。2ビットの長さフィールドr\_lengthは、再配置された項目の長さを示し、0～3はそれぞれ再配置された項目の幅が1バイト、2バイト、4バイト、8バイトであることを示す。フラグr\_pcrelは、再配置された項目が「PC関連」の項目であること、つまり命令の中で相対アドレスとして使用されることを示します。外部フラグr\_externは、r\_symbolnumの意味を制御し、再配置項目がセグメントを参照しているのか、シンボルを参照しているのかを示す。フラグの値が0であれば、再配置エントリは通常の再配置エントリであり、r\_symbolnumフィールドは、どのセグメントで位置決めが行われるかを指定する。フラグの値が1の場合は、再配置エントリは外部シンボルへの参照である。この場合、r\_symbolnumはターゲットファイルのシンボルテーブルのシンボルを指定し、そのシンボルの値を使って再配置する必要がある。

### 3.5.13 記号表と文字列部

ターゲットファイルの最後の部分は、シンボルテーブルと関連する文字列テーブルです。シンボルテーブルのエントリの構造は以下の通りです。

---

```
struct nlist {
    union {
        char      *n_name;           // String pointer,
        struct nlist *n_next;       // Or a pointer to another symbolic item structure,
        long       n_strx;          // Or the byte offset value of the symbol name in the table.
    } n_un;
    unsigned char n_type;         // This byte is divided into 3 fields. see a.out.h file.
    char       n_other;          // Usually not used.
    short      n_desc;           //
    unsigned long n_value;        // Symbol's value.
};
```

---

#### GNU

gccコンパイラでは、任意の長さの識別子を使用できるため、識別子の文字列は、シンボルテーブルの後にある文字列テーブルに配置されます。シンボルテーブルの各エントリは、12バイトの長さを持ち、最初のフィールドは、文字列テーブルからのシンボル名文字列（ヌル終端）のオフセットを与えます。タイプフィールド

n\_type  
は、シンボルのタイプを示します。このフィールドの最後のビットは、シンボルが外部（グローバル）であるかどうかを示すために使用されます。このビットが1であれば、シンボルはグローバルシンボルです。リンクはローカルシンボルの情報を必要としませんが、デバッガはそれを使用することができます。n\_typeフィールドの残りのビットは、シンボルタイプを示すために使用されます。a.out.hヘッダーファイルでは、これらのタイプの値の定数シンボルが定義されています。主なシンボルの種類には次のようなものがあります。

1 text, data,

bbsは、このモジュールファイルで定義されているシンボルを示す。このときのシンボルの値は、モジュール内のシンボルのリロケータブルアドレスである。

2 absは、シンボルが絶対的（固定的）に位置を変えられないシンボルであることを示します。

シンボルの値は、固定値です。

- 3 undefは、このモジュールファイルでは未定義のシンボルであることを示します。この時のシンボルの値は通常0です。

しかし、特殊なケースとして、コンパイラは未定義のシンボルを使って、リンカーに指定されたシンボリック名のためのメモリ空間を確保するように要求することができます。未定義の外部（グローバル）シンボルがゼロ以外の値を持つ場合、リンカーにとってその値は、プログラムがシンボリックアドレス用に指定したいメモリのサイズとなります。リンク処理中に、シンボルが本当に定義されていない場合、リンカーはシンボル名のためのメモリ空間をbssセクションに作成します。このスペースのサイズは、リンクされているすべてのモジュールにおけるシンボルの最大値となります。これがbs sセクションでのいわゆるコモンブロックの定義です。これは主に、初期化されていない外部（グローバル）データをサポートするために使用されます。例えば、プログラムで定義された初期化されていない配列などです。シンボルがいずれかのモジュールで既に定義されている場合、リンカーはこの定義を使用し、値を無視します。

### 3.5.2 Linuxにおけるターゲットファイル形式 0.12

#### Linux

0.12系では、objdumpコマンドを使って、モジュールファイルや実行ファイルに含まれるファイルのヘッダ構造の具体的な値を見ることができます。例えば、hello.oオブジェクトファイルとその実行ファイルに含まれるヘッダの具体的な値を以下に示します。

---

```

[~/usr/root]# gcc -c -o hello.o hello.c
[~/usr/root]# gcc -o hello hello.o
[~/usr/root]#
[~/usr/root]# hexdump -x hello.o
00000000 0107 0000 0028 0000 0000 0000 0000 0000
00000010 0024 0000 0000 0000 0010 0000 0000 0000
00000020 6548 6c6c 2c6f 7720 726f 646c 0a21 0000
00000030 8955 68e5 0000 0000 e3e8 ffff 31ff ebc0
00000040 0003 0000 c3c9 0000 0019 0000 0002 0d00
00000050 0014 0000 0004 0400 0004 0000 0004 0000
00000060 0000 0000 0012 0000 0005 0000 0010 0000
00000070 0018 0000 0001 0000 0000 0000 0020 0000
00000080 6367 5f63 6f63 706d 6c69 6465 002e 6d5f
00000090 6961 006e 705f 6972 746e 0066
0000009c

[~/usr/root]# objdump -h hello.o
hello.o:
magic: 0x107 (407) machine type: 0 flags: 0x0 text 0x28 data 0x0 bss 0x0
nsyms 3 entry 0x0 trsize 0x10 drsize 0x0
[~/usr/root]#
[~/usr/root]# hexdump -x hello | more
00000000 010b 0000 3000 0000 1000 0000 0000 0000
00000010 069c 0000 0000 0000 0000 0000 0000 0000
00000020 0000 0000 0000 0000 0000 0000 0000 0000
*
00000400 448b 0824 00a3 0030 e800 001a 0000 006a
00000410 dbe8 000d eb00 00f9 6548 6c6c 2c6f 7720
00000420 726f 646c 0a21 0000 8955 68e5 0018 0000
.....
--More--q
[~/usr/root]#
[~/usr/root]# objdump -h hello
hello:
magic: 0x10b (413) machine type: 0 flags: 0x0 text 0x3000 data 0x1000 bss 0x0
nsyms 141 entry 0x0 trsize 0x0 drsize 0x0
[~/usr/root]#

```

---

hello.oモジュールファイルのマジックナンバーは0407(OMAGIC)であり、ヘッダ構造の直後にコードセグメントがあることがわかります。ヘッダー構造に加えて、長さ0x28バイトのコードセグメントと、長さ0x10バイトの3つのシンボルアイテムとコードセグメントの再配置情報を持つシンボルテーブルが含まれています。それ以外のセグメントの長さは0である。対応する実行ファイルhelloのマジックナンバーは 0413 (ZMAGIC) で、コードセグメントはファイルオフセット位置 1024 バイトから格納されます。コードセグメントの長さは0x3000バイト、データセグメントの長さは0x1000バイトで、シンボルテーブルには141個のアイテムが格納されています。コマンドストリップを使って、実行ファイルのシンボルテーブル情報を削除することができます。例えば、以下では、helloの実行ファイルのシンボル情報を削除しています。これにより、hello実行ファイルのシンボルテーブルの長さが0になり、helloファイルの長さも元の20591バイトから17412バイトに短縮されたことがわかります。

```
[/usr/root]# ll hello
-rwx--x--x 1 root 4096 20591 Nov 14 18:30 hello
[/usr/root]# objdump -h hello
hello:
magic: 0x10b (413) machine type: 0flags: 0x0text 0x3000 data 0x1000 bss 0x0
nsyms 141 entry 0x0 trsize 0x0 drsize 0x0
[/usr/root]# strip hello
[/usr/root]# ll hello
-rwx--x--x 1 root 4096 17412 Nov 14 18:33 hello
[/usr/root]# objdump -h hello
hello:
magic: 0x10b (413) machine type: 0flags: 0x0text 0x3000 data 0x1000 bss 0x0
nsyms 0 entry 0x0 trsize 0x0 drsize 0x0
[/usr/root]#
```

図3-

8は、ディスク上のプロセス論理アドレス空間におけるa.out実行ファイルの領域の対応を示したもので  
す。Linux

0.12システムにおけるプロセスの論理空間サイズは64MBです。ZMAGICの実行ファイルであるa.outの  
コード領域は、メモリページサイズの整数倍となります。Linux 0.12  
カーネルでは、コードのページを実際に物理メモリページにロードするデマンドページング方式を採  
用しているため、ロード操作の fs/execve()  
関数にのみ設定されます。ページディレクトリエントリとページテーブルエントリのページングメカ  
ニズムなので、デマンドページ技術はロード処理を高速化することができます。

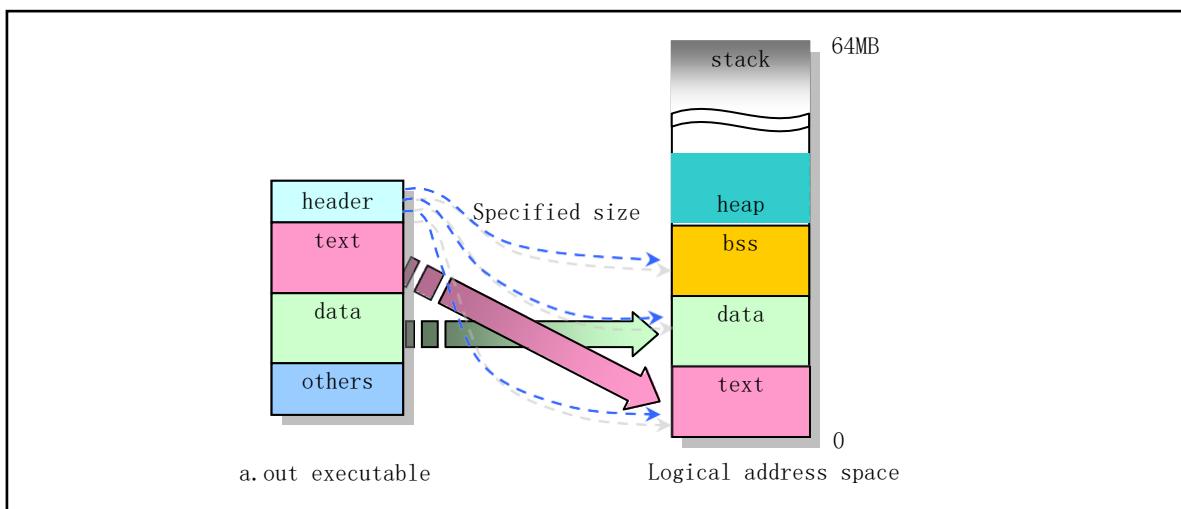


Figure 3-8 a.out execution file maps to process logical address space

図中、bssはプロセスの未初期化データ領域で、初期化されていない静的なデータを格納するため  
に使用されます。プログラムの実行開始時には、bssメモリの最初のページがすべて0に設定される。図  
中のヒープは、ヒープ空間領域であり、実行中のプロセスが動的に要求するメモリ空間を割り当てる  
ために使用される。

### 3.5.3 リンカー出力

リンカは、1つまたは複数の入力オブジェクトファイルと関連するライブラリ関数オブジェクトを処理し、最終的に対応するバイナリ実行ファイルまたはすべてのモジュールで構成される大きなモジュールファイルを生成する。この過程で、リンクプログラムが主な仕事は、実行ファイル（または出力モジュールファイル）の記憶領域の割り当て操作を行うことです。格納場所が決まれば、リンクプログラムは引き続きシンボル結合操作やコード修正操作を行うことができる。モジュール・ファイルに定義されているシンボルのほとんどは、ファイル内の格納位置に関連しているため、シンボルの対応位置が決定する前にシンボルを解決する方法はない。

各モジュール・ファイルには、いくつかのタイプのセグメントが含まれています。リンカの  
番目のタスクは、すべてのモジュールの同じタイプのセグメントを結合し、出力ファイルの指定されたセグメント・タイプの単一セグメントを形成することです。例えば、リンカはすべての入力モジュール・ファイルのコード・セグメントを  
1  
つのセグメントに結合し、それを出力実行ファイルに配置する必要があります。

a.out形式のモジュールファイルは、あらかじめセグメントの種類がわかっているので、リンカはa.out形式のモジュールファイルを簡単に格納・配置することができます。例えば、2つの入力モジュール・ファイルがあり、ライブラリ関数モジュールを接続する必要がある場合、その格納割り当ては図3-9のようになります。各モジュールファイルには、コード部、データ部、bss部があります。また、外部（グローバル）シンボルと思われる共通ブロックがある場合もあります。リンカは、任意のライブラリ機能モジュールのコード・セグメント、データ・セグメント、bss・セグメントを含む、各モジュール・ファイルのサイズを収集します。すべてのモジュールが読み込まれて処理された後、0以外の値を持つ未解決の外部シンボルはコモンブロックとして扱われ、その割り当てはbssセクションの最後に格納されます。

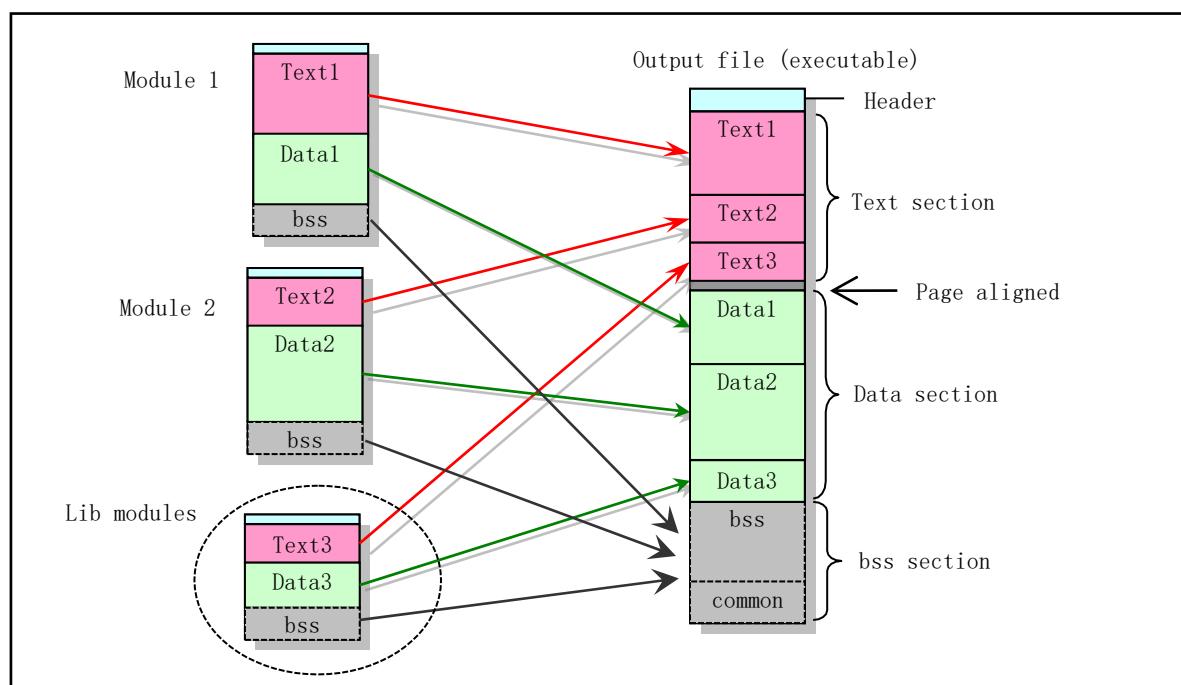


Figure 3-9 Object files link operation

これにより、リンカーはすべてのセグメントにアドレスを割り当てることができます。Linuxで使われ

ているZMAGICタイプのa.outフォーマットの場合は

0.12システムでは、出力ファイルのコードセグメントは固定アドレス0から始まるように設定されています。データセグメントは、コードセグメントの次のページ境界から始まります。データ・セグメントの直後には

bss

セクションがあります。各セグメント内では、リンカーは入力モジュール・ファイルのセグメントと同じ種類のセグメントを格納し、ワードごとに整列させます。

#### Linux

0.12カーネルが実行ファイルをロードする際には、まずファイルのヘッダ構造の情報に基づいて、そのファイルが適切な実行ファイルであるかどうかを判断します。つまり、マジックナンバータイプがZMAGICであれば、システムはユーザー モード スタックの最上位になります。プログラムは、コマンドラインで入力された環境パラメータやパラメータ情報ブロックを設定し、そのためのタスクデータ構造を構築します。そして、スタックリターンの手法を用いて、いくつかの関連するレジスタ値を設定した後、プログラムを実行します。実行プログラムイメージファイルのコードとデータは、実際に実行または使用されるときに、ロード・オン・デマンドを使用してメモリに動的にロードされます。

#### Linux

0.12カーネルのコンパイルプロセスでは、カーネル設定ファイルMakefileに基づいてコンパイラとリンクの動作を指令するmakeコマンドを使用しています。ビルドプロセスでは、toolsディレクトリにあるカーネルのソースコードに含まれるbuild.cプログラムも使用して、すべてのモジュールを結合するための一時的なツールプログラムbuildをコンパイルしてビルドします。カーネルはブートアッププログラムによってROM

BIOS割り込みコールを使ってメモリにロードされるため、コンパイルされたカーネルモジュール内の実行ヘッダー構造を削除する必要があります。ユーティリティプログラムビルドの主な機能は、bootsect、setup、systemの各ファイルの実行ヘッダ構造を削除し、順次結合してImageという名前のカーネルイメージファイルを作成することです。

### 3.5.4 リンカの定義済み変数

リンクの際、リンクld、ld86は変数を使って実行プログラムの各セグメントの論理アドレスを記録します。そのため、プログラム上では、外部変数にアクセスすることで、プログラムの中間セグメントの位置を取得することができます。リンクがあらかじめ定義している外部変数は、通常、少なくともetext、\_etext、edataです。

\_edata、end、\_end。

変数名\_etextとetextのアドレスはプログラムテキストセグメント終了後の最初のアドレス、\_edataとedataのアドレスは初期データ領域後の最初のアドレス、\_endとendのアドレスは未初期化データ領域(bss)後の最初のアドレスの位置です。名前の前にアンダースコア'\_'が付いているものは、下線が付いているものと同等です。両者の唯一の違いは、etext、edata、endという記号がANSI、POSIXなどの規格で定義されていないことです。

プログラムが実行され始めたばかりの時は、そのbrkの位置は\_endと同じ位置にあります。しかし、システムコールsys\_brk()や、メモリ割り当て関数malloc()、標準入出力の操作などによって、この位置は変わってしまいます。そのため、プログラムの現在のbrk位置はsbrk()を使って取得する必要があります。なお、これらの変数名はアドレスとして扱う必要があります。そのため、アクセスする際には

、&endのようにアドレスのプレフィックス「&」を使用する必要があります。例として

---

```
extern int _etext;
int et;

(int *) et = &_etext;           // et contains the address after the end of text segment.
```

---

The following program predef.c can be used to display the addresses of these variables. It can be seen that the address value is the same for the band and the underscore '\_' symbol.

---

```
/*
 Print the symbols predefined by linker.
*/
extern int end, etext, edata;
extern int _etext, _edata, _end;
int main()
{
    printf("&etext=%p, &edata=%p, &end=%p\n",
           &etext, &edata, &end);
    printf("&_etext=%p, &_edata=%p, &_end=%p\n",
           &_etext, &_edata, &_end);
    return 0;
}
```

---

### このプログラムをLinux

0.1Xシステムで実行すると、以下のような結果になります。なお、これらのアドレスは、プログラムのアドレス空間における論理的なアドレスであり、実行プログラムがメモリロケーションにロードされたときのアドレスであることに注意してください。

---

```
[/usr/root]# gcc -o predef predef.c
[/usr/root]# ./predef
&etext=4000, &edata=44c0, &end=48d8
&_etext=4000, &_edata=44c0, &_end=48d8
[/usr/root]#.
```

---

### このプログラムを最新の

Linux

システム(RedHat)

9

以降)で実行すると、次のような結果が得られます。Linuxシステムのプログラムコードは、現在、その論理アドレス0x08048000から格納されていることがわかっているので、プログラムのコードセグメント長は0x41bバイトであることがわかります。

---

```
[root@plinux]# ./predef
&etext=0x804841b, &edata=0x80495a8, &end=0x80495ac
&_etext=0x804841b, &_edata=0x80495a8, &_end=0x80495ac
[root@plinux]#
```

---

Linux 0.1x カーネルでは、ブロックデバイスキャッシュ(fs/buffer.c)を初期化する際に、変数名 \_end を用いて、メモリ上のカーネルイメージファイル

Image

の末尾の位置を取得し、この位置から高速設定を行っています。バッファを作成します。

### 3.5.5 System.map ファイル

GNU リンカ gld(l) を実行する際、「-M」オプションを使用した場合、または nm コマンドを使用した場合、リンクマップ情報が標準出力デバイス（通常はスクリーン）に出力されます。リンカが生成するターゲットプログラムのメモリアドレスマップ情報。メモリに読み込まれたプログラム・セグメントの位置情報が記載されている。具体的には以下のようないい情報がある。

- メモリ上にマッピングされたオブジェクトファイルやシンボル情報の位置。
- 公共のシンボルをどのように配置するか。
- リンクに含まれるすべてのファイルメンバーとその参照シンボル。

通常は、標準出力デバイスに送られてきたリンクイメージ情報を、ファイル（例：System.map）にリダイレクトします。カーネルをコンパイルする際、linux/Makefile ファイルで生成された System.map ファイルは、カーネルのシンボルテーブル情報を格納するために使用されます。シンボルテーブルとは、すべてのカーネルシンボルと、それに対応するアドレスのリストです。もちろん、上述の \_etext、\_edata、\_endなどのシンボルのアドレス情報も含まれています。カーネルをコンパイルするたびに、対応する System.map ファイルが新たに生成されます。カーネル内でエラーが発生した場合、System.map ファイルのシンボルテーブルを解析することで、アドレス値に対応する変数名を見つけることができ、またその逆も可能です。

System.map シンボルテーブルファイルを使用することで、カーネルや関連プログラムが故障したときに、より簡単に識別できる情報を得ることができます。シンボルテーブルの例は以下の通りです。

---

```
c03441a0 B dmi_broken
c03441a4 B is_sony_vaio_laptop
c03441c0 B dmi_ident
c0344200 b pci_bios_present
c0344204 b pirq_table
```

---

各行にはシンボルが記述されており、1列目はシンボルの値（アドレス）、2列目はシンボルの種類、シンボルがターゲットファイルのどのセクションにあるのか、またはその属性を示し、3列目は対応するシンボル名です。

2列目のシンボルタイプインジケータは、通常、表3-5に示すタイプがあるが、採用されているターゲットファイルフォーマットに関連するものもある。シンボルタイプが小文字の場合、そのシンボルはローカルであり、大文字の場合、そのシンボルはグローバル（外部）である。ファイル include/a.out.h (110-185行目) の nlist{}構造の n\_type フィールドの定義を参照してください。

Table 3-5 The symbol type in the target file symbol list file

Symbol type	Name	Description
-------------	------	-------------

A	アブソリュート	シンボルの値は絶対的なもので、今後も変更されることはありません。 をリンクしています。
B	BSS	シンボルは初期化されていないデータセクション、つまりBSSセクションにあります。
C	共通	シンボルはパブリックです。パブリックシンボルは初期化されていないデータです。リンクの際、複数のパブリック・シンボルが同じ名前になることがあります。シンボルが他の場所で定義されている場合はパブリックシンボルは未定義の参照として扱われます。
D	データ	シンボルは初期化されたデータ部にあります。
G	グローバル	シンボルはスマート・オブジェクトの初期化データ・セクションにあります。いくつかのオブジェクトファイルのフォーマットでは、スマートデータオブジェクトへのより効率的なアクセスを可能にする、グローバルな整数変数です。
I	不定形	シンボルは、他のシンボルを間接的に参照するものです。
N	デバッグ	このシンボルは、デバッグ用のシンボルです。
R	読み取り専用	シンボルは、読み取り専用のデータセクションにあります。
S	小型	シンボルを、スマートオブジェクトの未初期化データセクションに追加しました。
T	テキスト	コードセクションの記号
U	未定義	シンボルは外付けで、その値は0（未定義）です。
-	スタブ	このシンボルは、a.outオブジェクトファイル内のスタブシンボルであり、デバッグを保存するために使用されます。 の情報を提供します。
?	Unknwon	シンボルの種類は不明、または特定のファイル形式に関連しています。

dmi\_brokenという変数が、カーネルアドレス0xc03441a0にあることがわかります。

System.mapは、それを使用するソフトウェア（カーネルロギングデーモンklogdなど）が見つかる場所にあります。システム起動時に、klogdがSystem.mapの場所をパラメータの形で与えられない場合、klogdは以下の3箇所でSystem.mapを検索します。

---

```
/boot/System.map
/System.Map
/usr/src/linux/System.map
```

---

カーネル自体は実際にはSystem.mapを使用しませんが、klogd、lsof、psなどの他のプログラムや、dosemuなどのソフトウェアは、正しいSystem.mapファイルを必要とします。このファイルを使用することで、これらのプログラムは既知のメモリアドレスに基づいて対応するカーネル変数名を見つけることができ、カーネルのデバッグが容易になります。

## 3.6 MakeコマンドとMakefile

上記の例からわかるように、1つまたは数個のソースプログラムから生成される実行ファイルを作成する場合は、数行の簡単なコマンドを入力するだけで済みます。しかし、カーネルのように数百、数千のソースファイルから構成される大規模なプログラムの場合、すべてのコードファイルを手入力

でコンパイルするのは非常に煩雑です。`make`コマンドは、このような状況を自動的に処理するために設計された最高のツールです。`make`コマンドの主な目的は、多数のソースファイルを含む大規模なプロジェクトにおいて、どのファイルを再コンパイルする必要があるかを自動的に判断し、再コンパイルコマンドを発行することです。Makeの使い方を簡単に説明するために、コンパイル用のCプログラムを例に挙げますが、シェルコマンドを使ってコンパイルできるあらゆるプログラミング言語に適用することができます。詳しい使い方は、「GNU makeマニュアル」を参照してください。

`make`ツールを使用するためには、`make`実行用の`Makefile`（または`makefile`）という名前のテキストファイルを書く必要があります。

`Makefile`には主に、ファイル間の関係や、対応するターゲットファイルを生成するために必要なソースファイルのコンパイルやリンクの操作を`Make`に伝えるための実行ルールやコマンドが含まれています。

#### make

"がソースファイルを再コンパイルする際には、変更された各ソースファイルが再コンパイルされます。ヘッダーファイルが変更された場合は、そのヘッダーファイルを含む各ソースファイルが再コンパイルされます。各コンパイルでは、ソースファイルに対応するオブジェクトファイルが生成されます。最後に、すべてのソースファイルが再コンパイルされた場合、新しく作成されたものであれ、以前のコンパイルから保存されたものであれ、すべてのオブジェクトファイルがリンクされ、新しい実行ファイルが生成されます。

### 3.6.1 `Makefile`の内容

`Makefile`には、明示的なルール、暗黙のルール、変数定義、ディレクティブ、コメントの5つの要素があります。

- 明示的なルールは、ルールのターゲットと呼ばれる1つまたは複数のファイルを再コンパイルするタイミングと方法を指定するために使用されます。ルールには、前提条件（または依存関係）に依存するターゲット上の他のファイルと、ターゲットを作成または更新するためのコマンドが明示的に記載されています。
- 暗黙のルールは、ターゲットの名前とオブジェクトに基づいて、ルールのターゲットと呼ばれる1つまたは複数のファイルをいつ、どのように再コンパイルするかを決定します。このルールは、ターゲットがターゲット名に似たファイルに依存していることを説明し、そのようなターゲットファイルを作成または更新するために与えられます。
- 変数定義では、1行に変数のテキスト文字列を定義します。この変数は、後続のステートメントで置き換えることができます。例えば、以下の例の変数オブジェクトは、すべての`.o`ファイルのリストを定義しています。
- ディレクティブとは、`Makefile`を読み込む際に実行する特定の操作を示す`make`のコマンドです。これらの操作には、別の`Makefile`を読むこと、`Makefile`の一部を使用するか無視するかを決定すること、複数の行を含む文字列から変数を定義することなどが含まれる。
- コメントとは、`Makefile`のテキストの中で、「#」文字で始まる部分のことです。どうしても '#'文字を使いたい場合は、文字の前にバックスラッシュ（'\'）を付けてエスケープする必要があります。コメントは`Makefile`のどこにでも書くことができます。また、`Makefile`の中でTABで始まるコマンドラインスクリプトは、そのままシェルに渡され、シェルはそれがコマンドなのか、単なるコメントなのかを判断します。

適切なMakefileを書いておけば、ソースコードを修正するたびに「make」と入力するだけで、必要なプログラムの更新をすべて行うことができます。makeは、Makefileの内容とファイルの最終更新時刻から、更新（再コンパイル）が必要なファイルを判断します。更新が必要な各ファイルに対して、Makefileに記録されている関連コマンドを実行する。

### 3.6.2 Makefileファイルのルール

シンプルなMakefileには、以下のようなルールがいくつか含まれています。これらのルールは、主に操作対象（ソースファイルやオブジェクトファイル）の依存関係を記述するために使用されます。

---

```
ターゲット ...: 前提条件 ...
    コマンド
    ...
    ...
```

---

その中でも、ターゲット・オブジェクトは、通常、プログラムが生成するファイルの名前を指し、例えば、実行ファイルや「.o」で終わるオブジェクト・ファイルとなります。また、対象となるアクティビティの名前を指定することもできます。

は、例えば「clean」のように取られます。

前提条件とは、ターゲットを作成するために必要な一連のファイルや他のターゲットのことです。ターゲットは通常、このような複数の必要ファイルやターゲットファイルに依存します。

コマンド（command）とは、makeが実行する操作のことで、通常はターゲットを生成するシェルコマンドのことを指します。前提条件となる1つ以上のファイルの最終更新時刻がターゲットファイルの最終更新時刻よりも新しい場合、ルールのコマンドが実行されます。また、1つのルールに複数のコマンドが存在することもあり、各コマンドはルール内で1行を占めます。各コマンドを記述する前に、タブ文字を入力（Tabを押す）する必要があることに注意してください。

通常、コマンドは前提条件を持つルールの中に存在し、前提条件のいずれかが変更されたときにターゲットファイルを作成するために使用されます。ただし、ルールは必ずしも前提条件を持っていなければなりません。たとえば、ターゲット「clean」に関連する削除コマンドを含むルールには、前提条件が含まれていません。

ルールは、ある特定のルールのターゲットである特定のファイルを、いつ、どのように作り直すかを説明するものです。

makeは、ターゲットを作成または更新するための前提条件に基づいてコマンドを実行します。ルールは、ある操作をいつどのように行うかを説明することもできます。

Makefileには、ルールのほかにもさまざまなテキストを含めることができます。しかし、シンプルなMakefileであれば、通常、いくつかのルールを含めるだけで十分です。ルールの中には、先に挙げたものよりも複雑なものもありますが、基本的には似たようなものです。

### 3.6.3 シンプルなMakefile

ここでは、8つのCソースファイルと3つのヘッダーファイルからなるテキストエディタプログラムのコンパイルとリンクの方法を説明する簡単なMakefileについて説明します。

Makefileの内容に基づいてmakeがCファイルを再コンパイルする際には、変更されたCファイルのみが再コンパイルされます。もちろん、.hヘッダーファイルが変更された場合には、プログラムが正し

くコンパイルされるように、そのヘッダーファイルを含むすべてのCコードファイルが再コンパイルされる。各コンパイル作業により、ソースプログラムに対応するターゲットファイルが生成されます。正味のところ、修正されたソースコードファイルのいずれかがコンパイルされた場合、生成されるすべての.oオブジェクトファイル（ソースコードがコンパイルされる前にコンパイルされたばかりで修正されていないものを含む）をリンクして新しいものを生成する必要があるのです。実行可能なエディタプログラムです。

Makefileの例題ファイルの内容は、editという名前の実行ファイルが8つのオブジェクト・ファイルにどのように依存しているか、また8つのオブジェクト・ファイルが8つのCソース・ファイルと3つのヘッダ・ファイルにどのように依存しているかを説明しています。この例では、すべてのCファイルに "defs.h" というヘッダーファイルが含まれていますが、editコマンドを定義するCファイルには "command.h" が含まれており、editバッファを変更する下位のCファイルには "buffer.h" が含まれています。"のヘッダーファイルです。

---

```
edit : main.o kbd.o command.o display.o insert.o search.o files.o utils.o
      cc -o edit main.o kbd.o command.o display.o insert.o search.o files.o utils.o

main.o : main.c defs.h
        cc -c main.c
kbd.o : kbd.c defs.h command.h
        cc -c kbd.c
command.o : command.c defs.h command.h
        cc -c command.c
display.o : display.c defs.h buffer.h
        cc -c display.c
insert.o : insert.c defs.h buffer.h
        cc -c insert.c
search.o : search.c defs.h buffer.h
        cc -c search.c
files.o : files.c defs.h buffer.h command.h
        cc -c files.c
utils.o : utils.c defs.h
        cc -c utils.c
clean :
      rm edit main.o kbd.o command.o display.o insert.o search.o files.o utils.o
```

---

Makefileを使って "edit" の実行ファイルを作成するには、コマンドラインで "make" と入力するだけです。

Makefileを使ってコンパイル済みの実行ファイルとすべてのオブジェクトファイルをカレントディレクトリから削除するには、"make clean" と入力します。

Makefileでは、ルールの対象として、実行ファイル「edit」と、.oオブジェクトファイル「main.o」「kbd.o」などがあります。前提条件（または依存条件）となるファイルは、"main.c" や "defs.h"などのソースファイルです。実際、各「.o」ファイルは、ルールのゴールであると同時に、別のルールに必要な前提条件ファイルでもあることがわかります。コマンドには「cc -c main.c」と「cc -c kbd.c」があります。

ターゲットがファイルの場合、その前提条件にある依存ファイルが変更されると、再コンパイルやリンクが必要になります。もちろん、オブジェクトである前提条件のファイルを先に更新する必要

があります。この例では、"edit"は8つの.oターゲットファイルに依存しており、.oターゲットファイル"main.o"はソースファイル"main.c"とヘッダーファイル"defs.h"に依存しています。

Makefileの中のルールのターゲットと前提条件の次の行には、シェルコマンドがあります。これらのシェルコマンドは、前提条件に含まれるファイルを使用して、ターゲットのオブジェクトファイルを更新または生成する方法を示しています。なお、Makefileの中のコマンドラインと他の行を区別するために、各コマンドラインの前にタブを入力する必要があります。makeが行うことは、ターゲットを更新する必要があるときに、ルールの中のコマンドを実行することです。

対象となる「clean」は、ファイルではなく、単なる操作（アクティビティ）の名前です。一般的には、そのルールでこのアクションが実行されることを要求しないため、「clean」は他のルールの前提条件ではありません。その結果、makeはこのルールが明示されていない限り、このルールを実行しません。このルール（ターゲット）は、他のルールの前提条件であるだけでなく、前提条件を含んでおらず、また必要としていることに注意してください。つまり、このルールの唯一の目的は、指定されたコマンドを実行することです。このようなルールの場合、そのターゲットは他のファイルを参照したり依存したりせず、特定の操作を示すだけです。このターゲットをフォニーターゲットと呼びます。

### 3.6.4 makeがMakefileを扱う方法

デフォルトでは、makeはMakefileの中の最初のターゲット（'.'で始まるターゲットは含まない）からスタートします。この最初のゴールをMakefileのデフォルトゴールと呼びます。究極のゴールは、ターゲットの更新を試みる努力をすることです。

上の例では、実行プログラム「edit」を更新または作成することがデフォルトの最終目的なので、対応するルールをMakefileの先頭に置いています。コマンドラインでmakeコマンドを入力すると、makeはMakefileを読み、最初のルールの処理を開始する。この例では、最初のルールは再リンクして「edit」を生成することですが、makeがこのルールを完全に処理する前に、まず「edit」が依存しているファイルのルールを処理する必要があります。この例では、まずそれらの.oオブジェクトファイルを作成または更新する必要があります。それぞれの.oファイルは、それぞれのルールに従って処理されます。つまり、それぞれのソースファイルをコンパイルして、それぞれの.oオブジェクトファイルを生成します。ターゲットの前提条件となるソースファイルやヘッダーファイルが、.oオブジェクトファイルよりも新しい場合や、.oオブジェクトファイルが存在しない場合は、対応する.oオブジェクトファイルを更新または作成するために再コンパイルが必要です。.

Makefileに含まれる他のルールの中にも、そのゴール(ファイル)が最終目標の前提条件に現れていれば処理されます。最終目標（または任意の目標）が他のルールに依存していない場合は、私たちが積極的にmakeに処理を要求しない限り、makeはこれらのルールを処理しません。たとえば、makeを実行する際に、Makefileの中の特定のルールのターゲット名をコマンドラインで与えて、指定された更新操作を実行するよう

コマンド「make clean」。

.o オブジェクトを再コンパイルする前に、make  
はまず前提条件、ソースファイル、およびヘッダーファイルの更新を検討します。しかし、Makefileでは、ソースファイルとヘッダーファイルに対する処理が指定されていません。つまり、ソースファイルとヘッダーファイルは、どのルールの対象にもなっていないので、makeはこれらのソースファイル

に対して何の処理も行いません。

目的の.oオブジェクトファイルを再コンパイルした後、makeは、更新された編集プログラム "edit"を生成するために、再リンクを行うかどうかを決定します。これは、"edit"が存在しない場合や、対象となる.oオブジェクトファイルが "edit"よりも新しい場合にのみ行われます。リコンパイルされたばかりの.oオブジェクトファイルは、"edit"よりも新しいので、makeは再リンクして新しい"edit"を生成します。

したがって、ファイル "insert.c" を修正してmakeを実行すると、makeはソースファイルをコンパイルして対応する "insert.o" を更新した後、"edit" をリンクする。また、ヘッダファイル "command.h" を修正してmakeを実行すると、makeは対象ファイル "kbd.o", "command.o", "files.o" を再コンパイルしてからリンクし、新しい実行ファイル "edit" を生成します。

一般的に、make は Makefile の内容を使用して、更新が必要な .o オブジェクトファイルを判断し、その後、更新が必要なターゲットファイルを判断します。.oオブジェクトファイルがその関連ファイルのすべてよりも新しければ、.oオブジェクトはすでに最新の状態であり、それ以上の更新は必要ありません。もちろん、最初の最終ターゲットとしての入力条件（前提条件）にある必要なターゲットはすべて事前に更新されます。

### 3.6.5 Makefileに含まれる変数

上記の例では、「edit」ルールですべての.oターゲットファイルを2回リストアップする必要があります（下記参照）。

---

```
edit : main.o kbd.o command.o display.o insert.o search.o files.o utils.o
      cc -o edit main.o kbd.o command.o display.o insert.o search.o files.o utils.o
```

---

このように情報が重複していると、ミスが起こりやすくなります。プログラムに新しい.oオブジェクトファイルを追加した場合、.oオブジェクトファイル名をリストに追加しても、別の場所に追加するのを忘れてしまうことがあります。変数を使えば、このようなミスを減らすことができますし、Makefileをより簡潔に見せることもできます。変数を使うことで、一度定義したテキスト文字列を複数の場所で置き換えることができます。

Makefileでは、すべての.oオブジェクトファイルのリストを表すために、objectsまたはOBJECTSという名前の変数を定義するのが典型的なやり方です。通常、Makefileの中で次のような行を使って変数objectsを定義します。

---

```
objects = main.o kbd.o command.o display.o insert.o search.o files.o utils.o
```

---

その後、.oオブジェクトファイルをリストアップする必要があるすべての場所で、変数の値を「\$(objects)」と書くことで置き換えることができます。

### 3.6.6 makeが自動的にコマンドを推測するようにする

それぞれのCソースプログラムをコンパイルするために、ルールの中で関連するコマンドを与える必要はありません。なぜなら、make自身がそれを判断できるからです。makeには暗黙のルールがあり、ターゲットファイルの名前に応じて「cc

c」コマンドを使用し、対応する.cファイルに応じて対応する.oファイルを更新します。例えば、「cc -c main.c -o main.o」というコマンドを使って、「main.c」を「main.o」にコンパイルします。したがって、.oオブジェクトファイルのルールにあるコマンドを省略することができます。

このように.cファイルが自動的に使われると、前提条件(依存関係)に自動的に追加されます。そこで、ルールの前提条件で.c'ファイルを省略することができます  
---  
コマンドも省略したとします。以下は、この2つの変更を含み、変数を使用する完全なMakefileの例です。

---

```
objects = main.o kbd.o command.o display.o insert.o search.o files.o utils.o

edit : $(objects)
    cc -o edit $(objects)
main.o : defs.h
kbd.o : defs.h command.h
command.o : defs.h command.h
display.o : defs.h buffer.h
insert.o : defs.h buffer.h
search.o : defs.h buffer.h
files.o : defs.h buffer.h command.h
utils.o : defs.h

clean :
    -rm edit $(objects)
```

---

実際にMakefileファイルを書くときはこのようにします。暗黙のルールはとても便利なので、重要です。使っているのをよく見かけます。

### 3.6.7 自動変数の暗黙のルール

前提条件（依存オブジェクト）の一つがディレクトリを検索して別のディレクトリに見つかった場合、ルールのコマンドはスケジュール通りに実行されます。そのため、コマンドがこのディレクトリで必要な前提条件を検索できるように、慎重に設定する必要があります。これは、自動変数を使用することで実現できます。暗黙のルールである自動変数は、状況に応じてコマンドラインで自動的に置き換えることができる変数です。自動変数の値は、通常のコマンドが実行される前に設定されます。たとえば、自動変数「\$^」の値は、ルールの前提条件をすべて表し、それらが入っているディレクトリの名前も含まれています。「\$<」の値は、ルールの最初の前提条件を表し、「\$@」はターゲットオブジェクトを表します（他の自動変数については、makeのマニュアルを参照してください）。コマンドラインでヘッダーファイルを指定したくないときには、これらのヘッダーファイルを前提条件に含めることもあります。この時点では、自動変数「\$<」が最初の前提条件となります。

---

```
foo.o : foo.c defs.h hack.h
cc -c $(CFLAGS) $< -o $@
```

---

また、「\$<」はfoo.cに、「\$@」はfoo.oに自動的に置き換えられます。

makeがイディオムを使ってターゲットを更新するためには、コマンドを必要としないようにすれ

ばいいのである。コマンドを使わずにルールを書くか、ルールを書かないようにします。このとき、`make`はソースファイルの種類（ファイルサフィックス）に基づいて、どの暗黙のルールを使うかを判断します。

さらに、サフィックス・ルールと呼ばれる暗黙のルールがあります。これは、`make`の暗黙のルールを定義する昔ながらの方法です（現在では、このルールは使われず、代わりに、より一般的で明確なパターン・マッチング・ルールが使われています）。このルールはLinux 0.1xカーネルのMakefileで使われているので、ここでは簡単に説明します。次の例は、ダブルサフィックスルールを適用したもので、二重接尾辞ルールは、ソース接尾辞とターゲット接尾辞という接尾辞のペアで定義されます。対応する暗黙の前提条件は、ファイル名の中のターゲット接尾辞をソース接尾辞に置き換えることで得られます。したがって、このときの次の「\$<」の値は、「\*.c」のファイル名となる。正の`make`ルールの意味は、「\*.c」のプログラムを '\*.s' のコードにコンパイルすることである。

---

```
.c.s:
$(cc) $(cflags) && &
-nostdinc -Iinclude -S -o $*.s $<
```

---

通常、コマンドは前提条件（依存オブジェクト）を持つルールに属しており、前提条件のいずれかが変更されたときにターゲットファイルを生成するために使用されます。しかし、目標に対するコマンドを指定するルールは、必ずしも前提条件を持っていません。例えば、`delete`コマンドでターゲット「clean」に関連するルールは前提条件を必要としない。このとき、ルールは特定のファイルをいつどのようにして再作成するかを説明するものであり、特定のルールの対象となる。`Make`は前提条件に基づいてコマンドを実行し、ターゲットを作成または更新します。ルールは、ある操作をいつどのように行うかを説明することもできます。

`Makefile`にはルール以外のテキストを含めることもできますが、シンプルな`Makefile`には適切なルールだけを含める必要があります。

上記のテンプレートよりもはるかに複雑なルールに見えるかもしれません、基本的には統一されています。

#### Makefile

ファイルには、ファイル間で参照される依存関係を含めることができます。これらの依存関係は、ターゲットを再構築する必要があるかどうかを判断するために `make` が使用します。例えば、ヘッダファイルが変更された場合、`make` はそのヘッダファイルに関連するすべての「\*.c」ファイルをこれらの依存関係に基づいて再コンパイルします。依存関係の例としては、カーネルソースコードの`Makefile`を参照してください。

## 3.7 概要

本章では、いくつかの実行可能なアセンブリ言語プログラムを記述対象とし、アセンブリ言語としての`as86`とGNUの基本的な言語と使用方法について詳細に説明する。また、Linuxカーネルで使用されているC言語の拡張機能についても詳細に説明します。OSを学ぶ上で、システムがサポートするオブジェクトファイルの構造は非常に重要な役割を果たします。本章では、Linux 0.12で使用されている`a.out`オブジェクトファイル形式について詳しく説明します。

次の章では、保護モードで動作するIntel

80X86プロセッサの動作原理を詳しく説明します。保護モードのマルチタスクプログラムの例がありますが、この例を読むことで、オペレーティングシステムが最初にどのように「回転」するのかを基本的に理解することができ、Linux

0.12カーネルの全ソースコードを読み続けるための確かな基礎を築くことができます。

# 480X86のプロテクトモードとそのプログラミング

## 本書で紹介するLinux

OSは、インテル80X86プロセッサーと関連する周辺ハードウェアで構成されたPCシステムをベースにしています。80X86

CPUシステムのプログラミングについては、もちろんインテル社から発売されている全3巻の『IA-32 インテル・アーキテクチャー

ソフトウェア開発者マニュアル』、特に第3巻の「システム・プログラミング・ガイド」が最適です。特に第3巻の「システム・プログラミング・ガイド」は、80X86

CPUのシステム・プログラミングを理解する上で欠かせない資料です。80X86

CPUの動作原理を理解したり、システムプログラミングを行う上で欠かせない参考書です。これらの情報は、インテル社のホームページから無料でダウンロードできます。本章では、主に80X86

CPUのアーキテクチャと、プロテクトモードでのプログラミングの基礎知識について説明し、80X86

CPUをベースとしたLinuxカーネルのソースコードを読む準備をするための基礎固めを行います。主な内容は以下の通りです。1.80X86

CPUの基礎知識、2.プロテクトモードのメモリ管理、3.様々なCPU保護方法、4.割り込みと例外処理、5.タスク管理、6.プロテクトモードプログラミングの初期化、7.簡単なマルチタスクカーネルの例。

本章の最後のセクションで説明したシンプルなマルチタスクのカーネルプログラムは、Linux 0.12カーネルをベースにした簡略化された例です。この例では、メモリセグメンテーション管理とタスク管理の実装を説明しています。ページング機構の内容は含まれていません。しかし、この例題の動作メカニズムを十分に理解しておけば、後にLinuxカーネルのソースコードを読んだときに大きな問題が発生することはありません。この部分の内容に慣れている方は、本章の最後に掲載されている実行可能なカーネルのサンプルプログラムを直接読むことができます。もちろん、カーネルのソースコードを読むときには、いつでも本章を参照することができます。

## 4.1 80X86システムレジスタとシステム命令

80X86では、プロセッサの初期化や制御システムの動作を支援するために、フラグレジスタEFLAGSと、いくつかのシステムレジスタが用意されています。EFLAGSには、一般的なステータスフラグに加えて、いくつかのシステムフラグがあります。これらのシステムフラグは、タスクの切り替え、割り込み処理、命令の追跡、アクセス許可などの制御に使用されます。システムレジスタは、メモリ管理やプロセッサの動作制御に使用されます。

セグメント化やページング処理のためのシステムテーブルのベースアドレスや、プロセッサの動作を制御するビットフラグが含まれています。

### 4.1.1 フラグレジスタ

フラグレジスタEFLAGSのシステムフラグとIOPLフィールドは、図4-1に示すように、I/Oアクセス、マスク可能なハードウェア割り込み、デバッグ、タスク切り替え、仮想8086モードの制御に使用されます。通常、これらのフラグを変更できるのはオペレーティング・システム・コードのみです。EFLAGSの他のフラグは、いくつかの一般的なフラグ（キャリーCF、パリティPF、補助キャリーAF、ゼロフラグZF、ネガティブSF、方向DF、オーバーフローOF）です。ここでは、チームEFLAGSのシステムフラグについてのみ説明します。

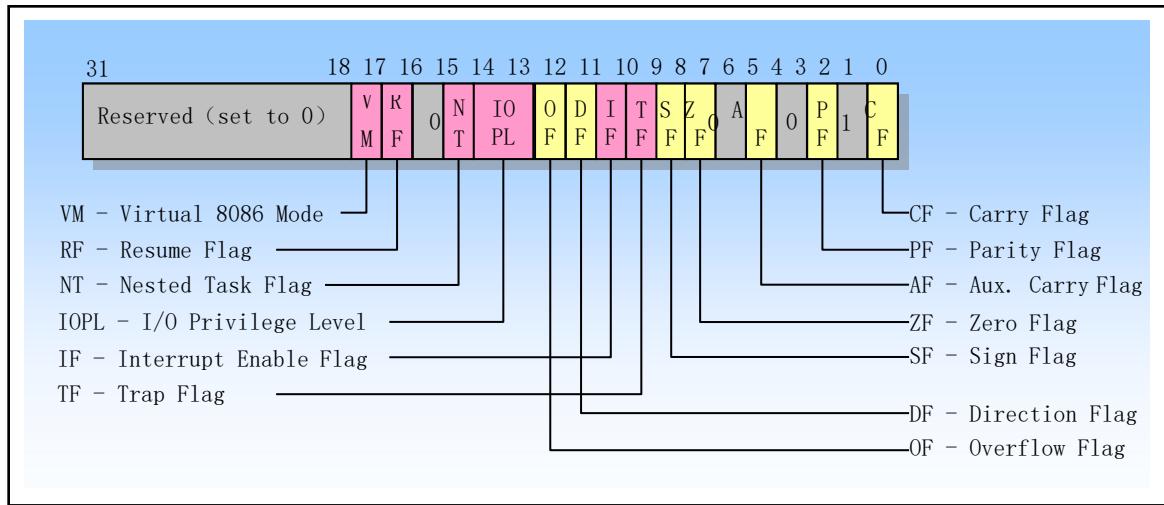


Figure 4-1 System Flags in EFLAGS

TFBit

8は、Trap

Flagですこのビットがセットされていると、デバッグ操作のためにステップ実行を開始することができます。リセットされるとシングルステップ実行が禁止されます。シングルステップ実行モードでは、命令を実行するたびにデバッグ例外が発生するので、各命令を実行した後の実行プログラムの状態を観察することができます。プログラムがPOPF、POPFD、またはIRET命令を使用してTFフラグを設定した

場合、プロセッサは後続の命令の後にデバッグ例外を生成します。

IOPLビット13~12は、I/O特権レベルフィールドです。このフィールドは、現在実行中のプログラムまたはタスクのI/O特権レベルIOPLを示します。現在プログラムやタスクを実行しているCPLがこのIOPL以下でないと、I/Oアドレス空間にアクセスできません。CPLが特権レベル0の場合のみ、プログラムはPOPF命令やIRET命令を使ってこのフィールドを変更することができます。IOPLは、IFロゴの変更を制御するメカニズムの1つでもある。

NTビット14は、入れ子になったタスクのフラグです。割り込まれたタスクと呼び出されたタスクの連鎖関係を制御します。プロセッサは、CALL命令、割込み、例外で開始されたタスクへの呼び出し時にこのフラグを設定します。IRET命令を使用してタスクから復帰する際、プロセッサはこのNTフラグをチェックして変更します。このフラグはPOPF/POPFD命令でも変更できますが、アプリケーションでこのフラグの状態を変更すると予期せぬ例外が発生する可能性があります。

RFビット16は、レジュームフラグですこのフラグは、ブレークポイント命令に対するプロセッサの応答を制御します。このフラグがセットされると、ブレークポイント命令によって生成されるデバッグ例外が一時的に無効になり、フラグがリセットされると、ブレークポイント命令によって例外が生成されます。RFフラグの主な機能は、例外をデバッグした後の命令の再実行を可能にすることです。デバッグソフトウェアがIRETD命令を使用して中断されたプログラムに戻る前に、スタック上のEFLAGSコンテンツのRFフラグを設定して、命令のブレークポイントが再び例外を発生させないようにする必要があります。命令が戻った後、プロセッサは自動的にフラグをクリアし、再び命令ブレークポイントによる例外処理を可能にします。

VMビット17は、Virtual-8086

Modeフラグです。このフラグがセットされていると、仮想8086モードがオンになり、リセットされるとプロテクトモードに戻ります。

### 4.1.2 メモリ管理レジスター

プロセッサには、4つのメモリ管理レジスタ（GDTR, LDTR, IDTR, TR）が用意されています。

図4-

2に示すように、メモリセグメントの管理に使用されるシステムテーブルのベースアドレスです。プロセッサは、これらのレジスタをロードおよびセーブするための特定の命令を提供します。システムテーブルの役割については、次項の「保護モードのメモリ管理」で詳しく説明しています。

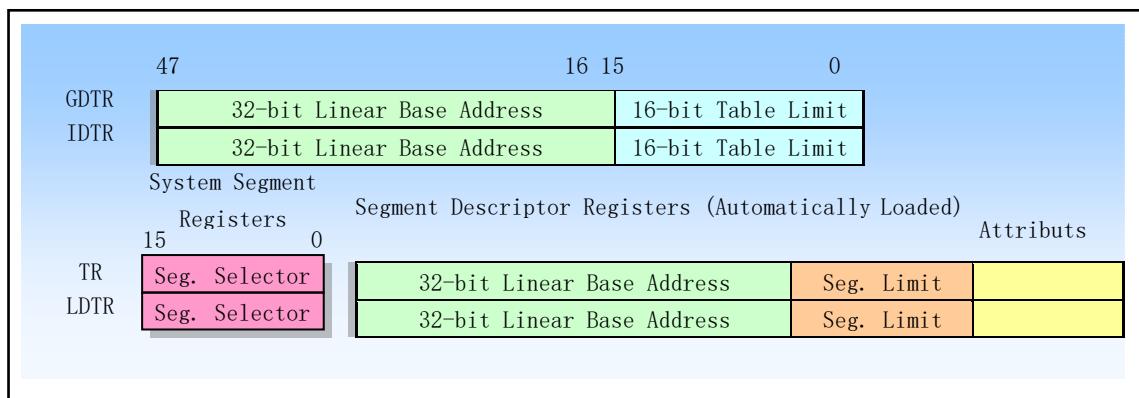


Figure 4-2 Memory management registers

GDTR、LDTR、IDTR、TRは、セグメント・ベース・レジスタで、セグメント・メカニズムのための重要な情報テーブルを含んでいます。GDTR、IDTR、LDTRは、ディスクリプターテーブルが格納されているセグメントのアドレスに使用されます。TRは、特別なタスクステートセグメントTSS（Task Segment）のアドレスに使用されます。TSSセグメントには、現在実行中のタスクに関する重要な情報が格納されています。ここでは、それらについて詳しく説明します。

#### 1. グローバルディスクリプターテーブルレジスタ(GDTR)

GDTRレジスタは、グローバルディスクリプターテーブルGDTの32ビットリニアベースアドレスと16ビットリミット値を保持しています。ベースアドレスは、リニアアドレス空間におけるGDTテーブルのバイト0のアドレスを指定し、テーブルレンジスはGDTテーブルのバイトレンジス値を示す。LGD T命令とSGDT命令は、それぞれGDTRレジスタの内容をロードおよびセットするために使用されます。マシンの電源投入直後やプロセッサのリセット後は、デフォルトでベース・アドレスが0に設定され、長さの値は0xFFFFに設定されています。保護モードの初期化時には、GDTRに新しい値をロードする必要があります。

#### 2. 割り込みディスクリプターテーブルレジスタ (IDTR)

IDTRレジスタは、GDTRと同様に、割り込みディスクリプターテーブルIDTの32ビットリニアベースアドレスと16ビットテーブル長の値を格納するために使用されます。LIDT命令とSIDT命令は、それぞれIDTRレジスタの内容をロードおよびセットするために使用されます。マシンの電源投入直後やP

ロセッサのリセット後は、デフォルトでベースアドレスが0に、長さの値が0xFFFFに設定されています。

### 3. ローカルディスクリプターテーブルレジスタ (LDTR)

LDTRレジスタは、ローカルディスクリプターテーブルLDTの16ビットセグメントセレクタ、32ビットリニアベースアドレス、16ビットセグメントリミット、およびディスクリプタ属性値を保持しています。LLDT命令とSLDT命令は、それぞれLDTRレジスタのセグメントセレクタ部分のロードとストアに使用されます。LDTテーブルを含むセグメントには、GDTテーブルにセグメントディスクリプターのエントリがなければなりません。LLDT命令を使用してLDTセグメントを含むセレクタをLDTRにロードする場合、LDTセグメント記述子のセグメントベースアドレス、セグメント長、記述子属性は自動的にLDTRにロードされます。タスクが切り替わると、プロセッサは新しいタスクのLDTのセグメントセレクタとセグメントディスクリプタを自動的にLDTRにロードします。マシンのパワー・アップまたはプロセッサのリセット後、セグメント・セレクタとベース・アドレスはデフォルトで0に設定され、セグメント長は0xFFFFに設定されます。

### 4. タスクレジスタ (TR)

TRレジスタは、16ビットのセグメントセレクタ、32ビットのベースアドレス、16ビットのセグメント長、ディスクリプタを保持しています。

現在のタスクTSSセグメントの属性値を表示します。GDTテーブル内のTSSタイプディスクリプターを参照します。LTR命令とSTR命令は、それぞれTRレジスタのセグメントセレクタ部分のロードとセーブに使用されます。LTR命令でセレクタをタスク・レジスタにロードすると、TSS記述子のセグメント・ベース・アドレス、セグメント長、記述子の属性が自動的にタスク・レジスタにロードされます。タスク・スイッチングが行われると、プロセッサは新しいタスクのTSSのセグメント・セレクタとセグメント・ディスクリプタを自動的にタスク・レジスタTRにロードします。

### 4.1.3 コントロールレジスター

制御レジスタ (CR0、CR1、CR2、CR3) は、図4-

3に示すように、プロセッサの動作モードや現在実行中のタスクの特性を制御・決定するために使用されます。CR0には、プロセッサの動作モードや状態を制御するシステム制御フラグが格納されており、CR1は使用予約されています。CR2には、ページフォルトを引き起こすリニアアドレスが格納されています。CR3にはページディレクトリテーブルの物理メモリベースアドレスが含まれているため、このレジスタはPDBR (Page-Directory Base Address Register) とも呼ばれます。

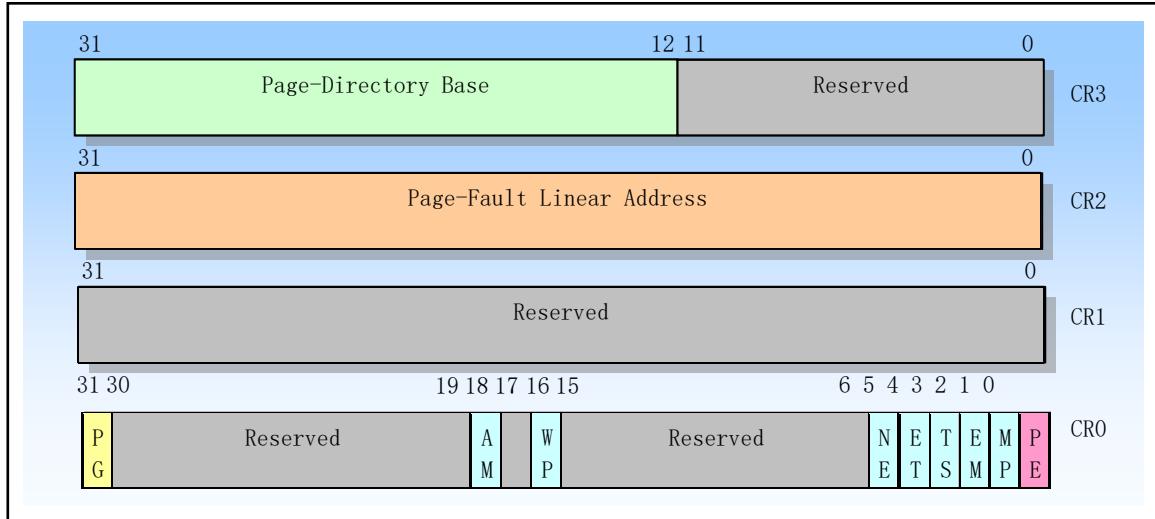


Figure 4-3 Control registers CR0--CR3

### 1. CR0のコプロセッサ制御ビット

CR0のET (Extended Type Bit) , TS (Task Switching Bit) , EM (Emulation Bit) , MP (Math Presence Bit) の4ビットは、80X86の浮動小数点 (Math) コプロセッサの動作を制御するために使用されます。コプロセッサとの通信に使用されるプロトコルを選択するために使用され、システムが80387と80287のどちらのコプロセッサを使用しているかを示します。TS、MP、EMビットは、フロート命令やWAIT命令でDevice

Not Available

例外を発生させるかどうかの判断に使用されます。この例外は、浮動小数点演算を使用するタスクでのみ、浮動小数点レジスタの保存と復元に使用できます。浮動小数点演算を使用しないタスクでは、そうすることで切り替えを高速化することができます。

#### CR0のETBit4は、Extension

Type フラグ

です。このフラグが1の場合、システムが80287コプロセッサを搭載し、32ビットのコプロセッサ・プロトコルを使用していることを示します。ET=0は80287コプロセッサの使用を示します。シミュレーションビットEM=1の場合、本ビットは無視されます。プロセッサのリセット操作時に、ETビットはシステムで使用されているコプロセッサの種類を示すために初期化されます。システムに80287がある場合はETが1に、80287がある場合やコプロセッサがない場合はETが0に設定されます。

#### CR0の

TSBit3は、タスク・スイッチ・フラグです。このフラグは、コプロセッサの内容を保存することを先延ばしにするために使用されます。

は、新しいタスクが実際にコプロセッサ命令を実行し始めるまでの間、タスクの切り替えを行います。このフラグは、タスクが切り替わるたびにプロセッサによって設定され、コプロセッサ命令が実行されるときにテストされます。

TSフラグが設定され、CR0のEMフラグが0の場合、コプロセッサ命令が実行される前にDevice

Not Available

例外が発生します。TSフラグが設定されていても、CR0のMP0フラグとEMフラグ

が設定されていない場合は、コプロセッサ命令WAIT/FWAITが実行されるまで、デバイス例外は発生しません。EMフラグがセットされている場合、TSフラグはコプロセッサ命令の実行に影響を与えません。表4-1参照。

タスクが切り替わると、プロセッサはコプロセッサのコンテキストを自動的に保存せず、TSフラグを設定します。このフラグは、新しいタスクのストリームを実行中に、いつでもコプロセッサの命令に遭遇したときに、プロセッサにデバイス実在性例外を発生させます。デバイス・エクシスタンント・ハンドラは、CLTS命令を使ってTSフラグをクリアし、コプロセッサのコンテキストを保存することができます。タスクがコプロセッサを使用したことがない場合、対応するコプロセッサのコンテキストを保存する必要はありません。

CR0のEMビット2は、EMulationフラグです。このビットがセットされていると、プロセッサに内部または外部のコプロセッサがないことを意味します。コプロセッサ命令を実行すると、device-not-

available例外が発生します。クリアすると、システムにコプロセッサがあることを意味します。このフラグを設定すると、すべての浮動小数点命令をソフトウェアでシミュレートすることになります。

MP CR0のビット1は、Monitor Present Coprocessor or Math  
Presentフラグです。WAIT/FWAIT命令とTSフラグの相互作用を制御するために使用します。MP=1、TS=1の場合、WAIT命令を実行するとdevice-not-available例外が発生します。MP=0の場合、TSフラグはWAITの実行には影響しません。

Table 4-1 Influence of EM, MP and TS Combinations in CR0 on Coprocessor Actions

CR0 Flags			Instruction Type	
EM	MP	TS	Floating-Point	WAIT/FWAIT
0	0	0	Execute	Execute
0	0	1	DNA Exception	Execute
0	1	0	Execute	Execute
0	1	1	DNA Exception	DNA Exception
1	0	0	DNA Exception	Execute
1	0	1	DNA Exception	Execute
1	1	0	DNA Exception	Execute
1	1	1	DNA Exception	DNA Exception

## 2. CR0の保護・制御ビット

CR0 の PEBit 0  
は、プロテクト・イネーブル・フラグですこのビットがセットされていると、プロテクトモードが有効になり、リセットされるとリアルアドレスモードになります。このフラグは、セグメントレベルのプロテクトを有効にするだけで、ページングを有効にするものではありません。ページング機構を有効にするには、PEとPGの両方のフラグを設定します。

PG

CR0のビット31は、ページングシグネチャです。このビットがセットされると、ページング機構が有効になり、リセットされると、ページング機構が無効になります。このとき、すべて

のリニアアドレスは物理アドレスと同等です。このフラグをオンにする前に、PEフラグをオンにする必要があります。つまり、ページング機構を有効にするには、PEフラグとPGフラグの両方をセットする必要があります。

WP	Intel	80486以上のCPUでは、CR0のビット16がWrite Protectフラグとなります。このフラグがセットされている場合、プロセッサはスーパーユーザープログラム（例：特権レベル0のプログラム）による書き込みを禁止します。
		このビットがリセットされると、逆にユーチューレベルの読み取り専用ページへの操作になります。このフラグは、UNIX系OSがプロセス作成時にCopy on Write技術を実装する際に有益です。

NE	Intel	80486以上のCPUの場合、CR0のビット5は、Numeric Errorフラグです。このフラグがセットされると、X87コプロセッサの内部エラー報告機構が有効になり、フラグがリセットされると、PCの形をしたX87コプロセッサのエラー報告機構が使われます。NEがリセット状態で、CPUのIGNNE入力端子に信号がある場合は、数学コプロセッサのX87エラーは無視されます。NEがリセット状態で、CPUのIGNNE入力端子に信号がない場合、マスクされていない数学コプロセッサのX87エラーが発生すると、プロセッサはFERR端子を介して外部に割り込みを発生させ、次の待機形式の浮動小数点命令直前に命令実行を停止するか、WAIT/FWAIT命令を実行します。CPUのFERR端子は、外部のコプロセッサ80387のERROR端子をエミュレートするため、通常は割り込みコントローラの入力要求端子に接続されています。NEフラグ、IGNNE端子、FERR端子は、外部ロジックによるPC形式の外部エラー報告機構を実現するためのものです。
----	-------	---

### PE (Enable Protected)

Protected ビット（ビット0）とPagingビット（ビット31）は、それぞれセグメンテーションとページングのメカニズムを制御するために使用されます。PEはセグメンテーション機構の制御に使用されます。PE=1の場合、プロセッサはオープン・セグメンテーション・メカニズムのコンテキストで動作します（すなわち、プロテクト・モードで動作します）。PE=0の場合、プロセッサはセグメンテーション機構をオフにし、8086のように実アドレスモードで動作します。PGはページング機構の制御に使用されます。PG=1の場合、ページング機構がオンになります。PG=0の場合、ページング機構は無効となり、リニアアドレスが物理アドレスとして直接使用されます。

PE=0, PG=0の場合、プロセッサは実アドレスモードで動作します。PG=0, PE=1の場合、プロセッサはページング機構なしの保護モードで動作します。PG=1, PE=0の場合、この保護モードではないため、ページング機構を有効にすることはできず、プロセッサは一般保護例外を生成します。このフラグの組み合わせは無効である。PG=1, PE=1の場合、プロセッサはページング機構を有効にした保護モードで動作する。.

PEビットとPGビットの変更には注意が必要です。PGビットの設定を変更できるのは、実行プログラムがリニアアドレス空間と物理アドレス空間のコードとデータの少なくとも一部が同一アドレスになっているときだけです。この時点では、この同一アドレスのコードの一部が、ページングされた世界と非ページングされた世界の橋渡しの役割を果たします。ページング機構がオンになっているかどうかにかかわらず、この部分のコードは同じアドレスになります。また、ページングが有効（PG=1）になる前に、ページキャッシュのTLBをリフレッシュする必要があります。

PEビットを変更した後、プログラムは直ちにジャンプ命令を使用して、プロセッサの実行パイプライン内で異なるモードを取得した命令をフラッシュしなければなりません。PEビットを設定する前に、プログラムはいくつかのシステムセグメントとコントロールレジスタを初期化する必要があります。電源投入時、プロセッサはPE=0、PG=0（リアルモード状態）にリセットされ、ブートコードがこれらのレジスタやデータ構造を初期化してから、セグメント化とページングのメカニズムを有効にします。

### 3. CR2とCR3

CR2とCR3はページング機構に使用されます。CR3には、ページディレクトリテーブルページの物理アドレスが格納されているため、CR3はPDBRとも呼ばれます。ページディレクトリテーブルページはページアラインされているため、このレジスタの上位20ビットのみが有効です。下位12ビットは、より高度なプロセッサで使用するために予約されているため、CR3に新しい値をロードする際には、下位12ビットを0に設定する必要があります。

CR2は、ページの例外が発生したときにエラーメッセージを報告するために使用されます。報告ページが異常な場合、プロセッサは例外が発生したリニア・アドレスをCR2に格納します。そのため、OSのページ例外ハンドラは、CR2の内容を確認することで、リニアアドレス空間のどのページで例外が発生したかを判断することができます。

CR3をロードするためにMOV命令を使用すると、ページキャッシュが無効になるという副作用があります。アドレス変換に必要なバスサイクル数を削減するために、最も最近アクセスされたページディレクトリとページテーブルは、TLB (Translation Lookaside Buffer) と呼ばれるプロセッサのページキャッシュに格納されます。ページテーブルエントリは、TLBに必要なページテーブルエントリが含まれていない場合に限り、余分なバスサイクルを使用してメモリから読み込まれます。

CR0 の PG ビットがリセット状態 (PG = 0) であっても、先に CR3 をロードすることで、ページング機構を初期化することができます。タスクを切り替えると、CR3 の内容も変化します。しかし、新しいタスクのCR3の値が元のタスクの値と同じであれば、プロセッサはページキャッシュをリフレッシュする必要はありません。これにより、ページテーブルを共有するタスクの実行速度が向上します。

#### 4.1.4 システム説明

システム命令は、システムレベルの機能を処理するために使用される。例えば、システムレジスタのロードや割り込みの管理などです。ほとんどのシステム命令は、特権レベル0のOSソフトウェアのみが実行できます。残りの命令は、アプリケーションが使用できるように、どの特権レベルでも実行することができます。表4-

2は、使用するシステム命令の一部を示しています。また、それらが保護されているかどうかも示しています。

Table 4-2 List of commonly used system instructions

Instruction	Description	Protected?	Description
LLDT	Load LDT Register	Yes	Load LDT segment selectors and segment descriptors from memory into the LDTR register.
SLDT	Store LDT Register	No	Save the LDT segment selector in LDTR to internal memory or general-purpose registers.
LGDT	Load GDT Register	Yes	Load the base address and length of the GDT table from memory into GDTR.
SGDT	Store GDT Register	No	Save the base address and length of the IDT table in GDTR to memory.
LTR	Load Task Register	Yes	Load TSS segment selectors (and segment descriptors) into the task register.
STR	Store Task Register	No	Save the current task TSS segment selector in TR to the memory or general register.
LIDT	Load IDT Register	Yes	The base address and length of the IDT table are loaded from memory into the IDTR.
SIDT	Store IDT Register	No	Store the base address and length of the IDT table in IDTR in memory.
MOV CRn	Move Control Registers	Yes	Load and save control registers CR0, CR1, CR2, or CR3.
LMSW	Load Machine State Word	Yes	Load the machine status word (corresponds to CR0 bit 15–0). This instruction is for compatibility with the 80286 processor.
SMSW	Store Machine State Word	No	Save the machine status word. This instruction is for compatibility with the 80286 processor.
CLTS	Clear TS flag	Yes	Clears the task switched flag TS in CR0. There are no exceptions for handling devices (coprocessors).
LSL	Load Segment Limit	No	Load Segment Limit
HLT	Halt Processor	Yes	Stop the processor execution.

## 4.2 プロテクトモードのメモリ管理

ここでは、メモリアドレッシングの定義、論理アドレス、リニアアドレス、物理アドレス間の変換原理に対するセグメンテーションとページングメカニズムの使用、タスクと特権レベル間の保護メカニズムについて簡単に紹介します。続くサブセクションでは、各パートの動作原理を詳しく説明します。

### 4.2.1 メモリアドレッシング

メモリとは、順番に並んだバイトの配列のことで、各バイトは固有のメモリアドレスを持つ。メモリアドレッシングとは、メモリに格納されている指定されたデータオブジェクトのアドレスを特定することです。ここでいうデータオブジェクトとは、メモリに格納されている指定されたデータタイプの数値や文字列のことである。80X86は複数のデータタイプをサポートしている。80X86では、1バイト、2バイト（ワード）、4バイト（ダブルワード、ロングワード）の符号なし整数や符号付き整数、マルチバイトの文字列など、複数のデータ型をサポートしています。通常、バイト内のあるビットの位置やアドレスは、バイト単位で指定できるため、最小のデータタイプのアドレス指定は、1バイト

データ（数値や文字）の位置指定となる。通常、メモリのアドレスは0から指定しますが、80X86 CPUの場合、アドレスバス幅が32ビットなので、物理アドレスは全部で $2^{32}$ 種類あります。つまり、メモリの物理アドレス空間は4Gあるので、合計4Gバイトの物理メモリをアドレス指定できます。マルチバイトのデータタイプ（2バイトの整数データタイプなど）の場合、このバイトはメモリに格納されます。80X86は、まず低値バイトを格納し、次に高値バイトをアドレスに格納します。したがって、80X86のCPUはスマートエンダムプロセッサです。

#### 80X86

CPUの場合、1つの命令は主にオペコードとオペラントで構成されています。オペラントは、レジスタまたはメモリ上に配置することができます。オペラントをメモリ上に置くためには、メモリアドレッシングが必要です。80X86では、メモリアドレッシングを伴う命令オペラントが多く、また、アドレッシングされるデータの種類に応じて、さまざまなアドレッシング方式があります。メモリアドレッシングには、80X86では「セグメント」と呼ばれるアドレッシング手法を採用しています。メモリ上のデータオブジェクトをアドレス指定するには、セグメントの開始アドレス（セグメントアドレス）と、セグメント内のオフセットアドレスが必要です。セグメントアドレスの部分は16ビットのセグメントセレクタで指定し、そのうち14ビットで $2^{14}$ 乗、つまり16384個のセグメントを選択できる。セグメントアドレス部は16ビットのセグメントセレクタで指定し、そのうち14ビットで $2^{14}$ 乗、つまり16384個のセグメントを選択できる。セグメント内オフセットアドレス部は32ビットで指定し、セグメント内アドレスは0～4Gとなる。つまり、1つのセグメントの最大長は4Gになります。このように、16ビットのセグメントセレクタと32ビットのセグメント内オフセットで構成される48ビットのアドレスまたはロングポインターが、論理アドレス（仮想アドレス）を形成します。これにより、データ・オブジェクトのセグメント・アドレスとセグメント・オフセット・アドレスが一意に決まります。32ビットのオフセットアドレスやポインターのみで指定されたアドレスは、現在のセグメントのオブジェクトアドレスに基づいています。また、セグメンテーション・メカニズムでは、セグメントをタイプ分けして、特定のタイプのセグメントで実行できる操作を制限することができます。

80X86には、セグメントセレクタを格納するための6つのセグメントレジスタが用意されています。CS,DS,ES,SS,FS,GSです。CSは常にコードセグメントのアドレスに使用され、スタックセグメントは特にSSセグメントレジスタを使用します。CSで指定されたセグメントを現在のコードセグメントと呼びます。このとき、EIPレジスタには、実行するカレントコードセグメント内のセグメント内のオフセットアドレスが格納されています。したがって、実行すべき命令のアドレスは、CS:[EIP]と表現できる。後述するセグメント間制御分岐命令を用いて、CSとEIPに新たな値を割り当てることで、実行位置を他のコードセグメントに変更することができ、異なるセグメントのプログラムの制御移行を実現することができます。

セグメント・レジスタSSで指定されたセグメントは、現在のスタック・セグメントと呼ばれます。スタックの最上位は、ESPレジスタの内容で指定されます。つまり、スタックの一番上のアドレスはSS:[ESP]です。他の4つのセグメント・レジスタは、一般的なセグメント・レジスタです。命令で演算するデータのセグメントが指定されていない場合は、DSがデフォルトのデータ・セグメント・レジスタになります。

メモリオペランドのセグメント内オフセットアドレスを指定するために、80X86命令ではオフセットの計算方法を多数規定しており、これを命令アドレッシングと呼ぶ。命令のオフセットは、ベースアドレスレジスタ、インデックスレジスタ、そしてオフセット定数の3つの部分から構成されています。というものです。

$$\text{オフセットアドレス} = \text{ベースアドレス} + (\text{インデックス} \times \text{スケールファクタ}) + \text{オフセット}$$

### 4.2.2 アドレス変換

完全なメモリ管理システムには、保護とアドレス変換という2つの重要な部分があります。プロテクションを提供することで、あるタスクが別のタスクやオペレーティングシステムのメモリ領域にアクセスすることを防ぎます。アドレス変換は、オペレーティングシステムが柔軟にタスクにメモリを割り当てることを可能にします。また、特定の物理アドレスを任意の論理アドレスでマッピングされないようにすることができるため、アドレス変換の際にメモリ保護が行われます。

前述したように、コンピュータ内の物理メモリはバイトの直線的な配列で、各バイトは固有の物理アドレスを持っています。プログラム内のアドレスは、セグメントセレクタとセグメント内のオフセットからなる論理アドレスです。このような論理アドレスは、直接物理メモリにアクセスすることはできず、アドレス変換機構を用いて物理メモリのアドレスに変換・マッピングする必要がある。この論理アドレスを物理メモリのアドレスに変換するのが、メモリ管理機構である。

アドレス変換の決定に必要な情報を減らすために、変換やマッピングは通常、メモリブロックを操作単位として使用します。アドレス変換の手法としては、セグメンテーション機構とページング機構が広く使われています。両者の違いは、論理アドレスをマップされたメモリブロックに整理する方法、変換情報の指定方法、プログラマの操作方法などです。フラグメントとページングは、それぞれの変換情報をメモリ上のテーブルで指定します。これらのテーブルは、アプリケーションによる不正な変更を防ぐために、OSからしかアクセスできないようになっている。

80X86では、図4-

4に示すように、論理アドレスから物理アドレスへの変換にセグメンテーションとページングを使用しています。第1段階では、セグメンテーション機構を用いて、論理アドレスをプロセッサのリニアアドレス空間のアドレスに変換します。第2段階では、ページング機構を用いてリニアアドレスを物理アドレスに変換します。アドレス変換処理では、第1段階のセグメンテーション機構は常に使用され、第2段階のページング機構はオプションです。ページング機構を使用しない場合、セグメンテーション機構で生成されたリニアアドレス空間は、プロセッサの物理アドレス空間に直接マッピングされます。物理アドレス空間とは、プロセッサがアドレスバス上に生成できるアドレス範囲のことです。

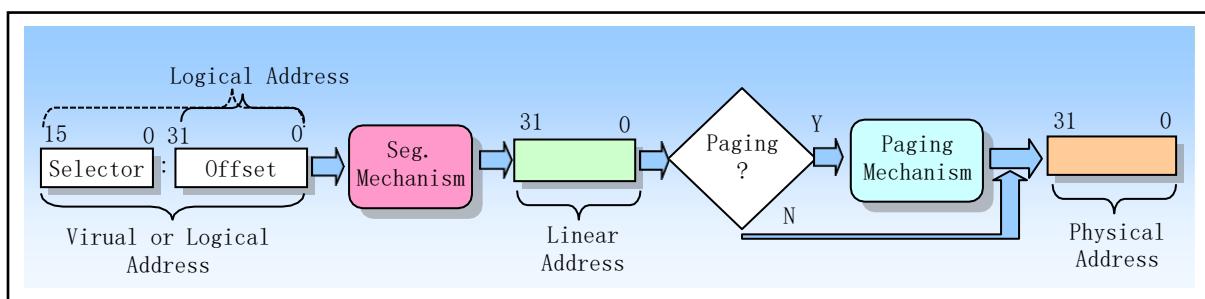


Figure 4-4 Logical address to physical address translation

## 1. セグメンテーション機構

セグメント化は、個々のコード、データ、スタック領域を分離するメカニズムであり、複数のプログラム（またはタスク）が互いに干渉することなく同じプロセッサ上で実行できるようにする。ページング機構は、従来のデマンドページと仮想メモリシステムの実装機構を提供する。仮想メモリーシステムは、プログラムコードが必要に応じて物理メモリーにマッピングされることを実現するために使用されます。ページングメカニズムはもちろん、複数のタスク間のアイソレーションを実現するためにも使用できます。

図4-

5に示すように、セグメンテーションは、プロセッサのアドレス可能なリニアアドレス空間を、セグメントと呼ばれる、より小さな保護されたアドレス空間領域に分割するメカニズムを提供します。セグメントは、プログラムコード、データ、スタック、またはシステムデータ構造（TSSやLDTなど）を格納するために使用できます。プロセッサ内で複数のプログラムやタスクが実行されている場合、各プログラムは独自のセグメントセットを割り当てることができます。このとき、プロセッサはこれらのセグメント間の境界を強制し、あるプログラムが他のプログラムのセグメントにアクセスすることで、そのプログラムの実行を妨害しないようにすることができます。セグメント化により、セグメントを分類することもできます。このようにして、特定の種類のセグメントに対する操作を制限することができます。

システム内のすべての使用済みセグメントは、プロセッサのリニアアドレス空間に含まれます。指定されたセグメント内のバイトを見つけるためには、プログラムは論理アドレスを指定する必要があります。論理アドレスには、セグメント・セレクタとオフセットが含まれます。セグメント・セレクタは、セグメントを一意に識別するためのものです。また、セグメント・セレクタは、セグメント・ディスクリプタ・テーブル（例：グローバル・ディスクリプタ・テーブルGDT）内のデータ構造（セグメント・ディスクリプタと呼ばれる）のオフセットを提供します。各セグメントには、セグメント記述子があります。セグメント記述子は、セグメントのサイズ、セグメントのアクセス権と特権レベル、セグメント・タイプ、リニア・アドレス空間におけるセグメントの1バイト目の位置（セグメントのベース・アドレスと呼ぶ）を指定する。論理アドレスのオフセットは、セグメントのベースアドレスに追加され、セグメント内のバイトを特定します。したがって、ベースアドレスにオフセットを加えたものが、プロセッサのリニアアドレス空間のアドレスとなります。

線形アドレス空間は、物理アドレス空間と同じ構造を持っています。2次元の論理アドレス空間に比べ、どちらも1次元のアドレス空間です。仮想アドレス（論理アドレス）空間は、最大16Kのセグメントを含むことができ、各セグメントは最大4GBとなり、仮想アドレス空間の容量は64TB（ $2^{46}$ ）となります。線形アドレス空間と物理アドレス空間はともに4GB（ $2^{32}$ ）です。実際、ページング機構を無効にした場合、リニアアドレス空間が物理アドレス空間となります。

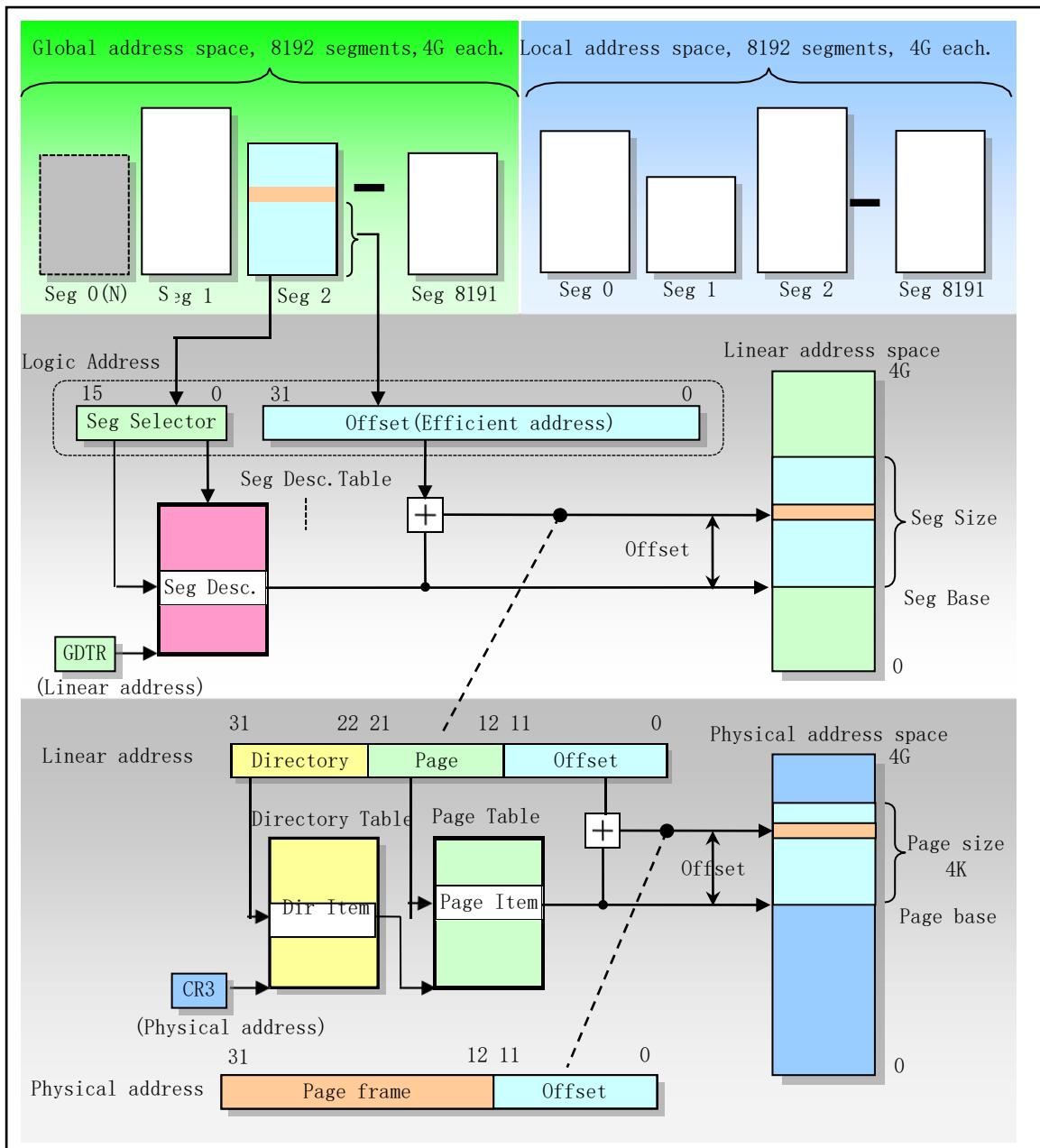


Figure 4-5 Logical, Linear, and Physical Addresses

## 2. ページング機構

マルチタスクシステムでは通常、含まれる物理メモリよりもはるかに大きなリニアアドレス空間を定義するため、何らかの「仮想化」されたリニアアドレス空間のアプローチ、つまり仮想ストレージ技術の使用が必要となる。仮想記憶は、プログラマーが、コンピュータの実際の物理的なメモリ容量よりもはるかに大きなメモリ空間があるように錯覚させるメモリ管理技術である。この錯覚を利用すれば、実際にどのくらいの物理メモリが存在するかを考慮することなく、大きなプログラムを自由にプログラミングすることができる。

ページング機構は、仮想記憶技術に対応しています。仮想記憶を使用する環境では、大容量のリニアアドレス空間を少量の物理メモリ (RAMやROM) と外部記憶領域 (大容量のハードディスクなど) でシミュレートする必要があります。ページングを用いる場合は、各セグメントをページ (通常1ペ

ージ4KB)に分割し、物理メモリまたはハードディスクに格納する。

オペレーティングシステムは、ページディレクトリといくつかのページテーブルを管理することで、これらのページに注意を払っています。プログラム(またはタスク)がリニアアドレス空間のアドレス位置にアクセスしようとすると、プロセッサはページディレクトリとページテーブルを使用してリニアアドレスを物理アドレスに変換し、そのメモリ位置で必要な操作(読み取りまたは書き込み)を行います。

現在訪問しているページが物理メモリにない場合、プロセッサはプログラムの実行を(ページfault例外を発生させることで)中断します。オペレーティングシステムは、その後、ハードディスクから物理メモリにページを読み込み、先ほど中断されたプログラムの実行を継続することができます。オペレーティングシステムがページングメカニズムを厳密に実装している場合、物理メモリとハードディスクの間のページの交換は、正しく実行されたプログラムには透過的に行われます。

80X86のページング機構は、仮想記憶技術のサポートに最も適している。ページング機構では固定サイズのメモリブロックを使用し、セグメント管理では可変サイズのブロックを使用してメモリを管理します。固定サイズのブロックを使ったページングは、物理メモリやハードディスク上のメモリを管理するのに適している。一方、セグメント管理では、可変サイズのブロックを使用するため、複雑なシステムの論理的なパーティションの処理に適しています。固定サイズのページに制約されることなく、論理ブロックサイズに収まるメモリセルを定義することができます。また、各セグメントを1つのユニットとして扱うことができるため、セグメントの保護や共有が容易になります。

セグメント化とページングは、2つの異なるアドレス変換メカニズムであり、いずれもアドレス変換操作全体に独立した処理ステージを提供する。どちらもメモリに格納された変換テーブルを使用するが、使用するテーブル構造が異なる。実際、セグメントテーブルはリニアアドレス空間に格納されており、ページテーブルは物理アドレス空間に格納されている。したがって、セグメント変換テーブルは、セグメント機構の情報や協力なしに、ページング機構によって再配置することができます。セグメント変換機構は、仮想アドレス(論理アドレス)をリニアアドレスに変換し、リニアアドレス空間にある自身のテーブルにアクセスしますが、ページング機構がこのリニアアドレスを物理アドレスに変換するプロセスを知りません。同様に、ページングメカニズムは、プログラムがアドレスを生成する仮想アドレス空間を知りません。ページングメカニズムは、単にリニアアドレスを物理アドレスに変換し、物理メモリ上の独自の変換テーブルにアクセスします。

### 4.2.3 保護

80X86では、2種類の保護方法をサポートしています。1つは、各タスクに異なる仮想アドレス(論理アドレス)空間を与えて、各タスクを完全に分離すること。実装の原則は、各タスクに異なる論理アドレスと物理アドレスのマッピングを与えることです。もう1つの保護機構は、タスク上で動作し、オペレーティングシステムのメモリセグメントやプロセッサの特殊システムレジスタがアプリケーションからアクセスされないように保護します。

#### 1. タスク間の保護

保護の重要なポイントとして、アプリケーションのタスク間の保護を行うことが挙げられます。80X86では、各タスクを異なる仮想アドレス空間に配置し、各タスクに論理アドレスと物理アドレスの異なるマッピングを与える方法が採用されている。各タスクのアドレス変換機能は、あるタスクの論理アドレスは物理メモリの一部にマッピングされ、別のタスクの論理アドレスは物理メモリの別の領域

にマッピングされるように定義されている。このようにすると、あるタスクは他のタスクの対応する論理アドレスにマッピングできる物理メモリの部分を生成できないので、すべてのタスクが分離されます。各タスクに個別のマッピングテーブルを与えると、各タスクは異なるアドレス変換機能を持つことになります。**80X86**では、各タスクはそれぞれセグメントテーブルとページテーブルを持っています。プロセッサが新しいタスクを実行するために切り替えるとき、タスク切り替えの重要な部分は、新しいタスクの変換テーブルに切り替えることです。

すべてのタスクに同一の仮想アドレスと物理アドレスのマッピング部分を配置し、オペレーティングシステムをこの共通の仮想アドレス空間部分に置くことで、OSをすべてのタスクで共有することができます。このすべてのタスクが持っている仮想アドレス空間の同じ部分をグローバルアドレス空間と呼びます。最近の**Linux OS**では、まさにこのように仮想アドレス空間が使われています。

仮想アドレス空間のうち、各タスクに固有の部分を「ローカルアドレス空間」と呼びます。ローカルアドレス空間には、システム内の他のタスクと区別する必要のあるプライベートコードとデータが含まれています。各タスクには異なるローカルアドレス空間が存在するため、2つの異なるタスクで同じ仮想アドレスを参照すると、異なる物理アドレスに変換されます。これにより、OSは各タスクのメモリに同じ仮想アドレスを与えつつ、各タスクを分離することができます。一方、グローバルアドレス空間では、すべてのタスクが同じ仮想アドレスを参照すると、同じ物理アドレスに変換されます。これにより、共通のコードやデータ（OSなど）の共有をサポートします。

## 2. 特権レベルの保護

タスクでは、セグメントに含まれるデータの機密性と、タスク内のプログラムの各部分の信頼度に基づいて、タスク内のセグメントへのアクセスを制限するために、4つの特権レベルが定義されています。最も機密性の高いデータには最高の特権レベルが与えられ、タスクの中で最も信頼されている部分からしかアクセスできません。機密性の低いデータには低い特権レベルが与えられ、タスク内より低い特権を持つコードがアクセスできます。

特権レベルは0～3の数字で表され、0が最も高い特権レベル、3が最も低い特権レベルとなります。各メモリセグメントには特権レベルが設定されています。この特権レベルによって、十分な特権レベルを持つプログラムがそのセグメントにアクセスすることが制限されます。プロセッサは、CSレジスタで指定されたセグメントから命令をフェッチして実行することがわかっています。現在の特権レベル、つまりCPLは、現在アクティブなコードセグメントの特権レベルであり、現在実行中のプログラムの特権レベルを定義しています。CPLは、プログラムがどのセグメントにアクセスできるかを決定します。

プログラムがセグメントにアクセスしようとするたびに、現在の特権レベルとセグメントの特権レベルが比較され、アクセス許可があるかどうかが判断されます。ある CPL レベルで実行されたプログラムは、同じレベルまたは下位レベルのデータ・セグメントへのアクセスを許可します。高レベルのセグメントへの参照は違法であり、オペレーティングシステムに通知する例外が発生します。

各特権レベルは、共有スタックの使用に伴う保護の問題を避けるために、独自のプログラムスタックを持っています。プログラムがある特権レベルから別の特権レベルに切り替わると、スタックセグメントも新しいレベルのスタックに変更されます。

## 4.3 セグメント化の仕組み

セグメント化のメカニズムは、さまざまなシステムデザインの実装に使用できます。例えば、プログラムを保護するために最低限の機能しか持たないフラットモデルから、複数のプログラム（またはタスク）を確実に実行できる堅牢な動作環境を構築するためにセグメント化されたマルチセグメントモデルまで、さまざまな設計が可能です。

システムの最もシンプルなメモリモデルは、基本的なフラットモデルです。このモデルでは、オペレーティングシステムやプログラムは、セグメント化されていない連続したアドレス空間にアクセスできます。この基本的なフラットモデルは、システム設計者やアプリケーションプログラマから、アーキテクチャのセグメント化の仕組みをほとんどの場合、隠すことができます。基本的なフラットメモリモデルを実装するには、少なくとも2つのセグメント記述子を作成する必要があります。1つは参照コードセグメント用、もう1つは参照データセグメント用です。ただし、どちらのセグメントもリニアアドレス空間全体にマッピングされます。つまり、2つのセグメント記述子は、同じベースアドレス値に対して、0と4GBという同じセグメント制限を持っています。

マルチセグメントモデルでは、セグメンテーションの仕組みを利用して、ハードウェアで強化されたコード、データ構造、プログラム、タスクを完全に保護することができます。一般的に、各プログラム（またはタスク）は、それぞれの

セグメント記述子テーブルと自分のセグメント。プログラムの場合、セグメントは完全にプライベートなものもあれば、プログラム間で共有されるものもあります。システム上のすべてのセグメントと各実行プログラムの実行環境へのアクセスは、ハードウェアによって制御されます。

アクセスチェックは、セグメントの境界外のアドレスへの参照を保護するためだけでなく、特定のセグメントで許されないアクションの実行を防ぐためにも使用できます。例えば、コードセグメントは読み取り専用に設計されているので、ハードウェアを使ってコードセグメントへの書き込みを防止することができます。また、セグメントのアクセス権情報を利用して、保護リングや保護レベルを設定することもできます。保護レベルは、アプリケーションによる不正なアクセスからオペレーティングシステムのプログラムを保護するために使用できます。

### 4.3.1 セグメントの定義

前節の概要で述べたように、80X86ではプロテクトモードで4GBの物理アドレス空間が用意されている。これは、プロセッサがアドレスバスでアドレス指定できるアドレス空間です。このアドレス空間はフラットで、アドレス範囲は0から0xFFFFFFFFまでです。この物理アドレス空間は、読み書き可能なメモリ、リードオンリーメモリ、メモリマップドI/Oにマッピングすることができます。セグメント化の仕組みは、仮想アドレス空間内の仮想メモリを、セグメントと呼ばれるいくつかの可変長のメモリブロック単位に整理することである。80X86の仮想アドレス空間における仮想アドレス（論理アドレス）は、セグメント部分とオフセット部分で構成されています。セグメントは、仮想アドレスからリニアアドレスへの変換メカニズムの基礎となります。各セグメントは3つのパラメータで定義されます。

1. ベースアドレスは、リニアアドレス空間におけるセグメントの開始アドレスを指定します。ベースアドレスはリニアアドレスで、セグメントのオフセット0に対応しています。
2. セグメントリミットは、仮想アドレス空間内のセグメント内で利用可能な最大のオフセットです。セグメントの長さを定義します。

3. 属性」は、セグメントの特性を指定します。例えば、セグメントが読み取り可能なのか、書き込み可能なのか、プログラムとして実行可能なのか、セグメントの特権レベルなどです。

セグメントの長さは、仮想アドレス空間におけるセグメントのサイズを定義します。セグメントベースのアドレスとセグメントリミットの長さは、セグメントがマッピングされるリニアアドレスの範囲または領域を定義します。セグメントの0からリミットまでのアドレス範囲は、リニアアドレスのベースからベース+リミットまでの範囲に相当します。セグメントリミットを超えるオフセットを持つ仮想アドレスは意味がなく、使用すると例外が発生する可能性があります。また、セグメント属性の許可を得ずにセグメントにアクセスした場合も例外が発生します。たとえば、読み取り専用のセグメントを書き込もうとすると、80X86は例外を発生させます。さらに、リニアアドレスにマッピングされた複数のセグメントの範囲は、図4-6のように部分的に重なったり、被ったり、あるいは完全に重なってしまうこともあります。本書で紹介するLinux 0.1xシステムでは、タスクのコードセグメントとデータセグメントのセグメントの長さは同じであり、リニアアドレスが同一で重なる領域にマッピングされています。

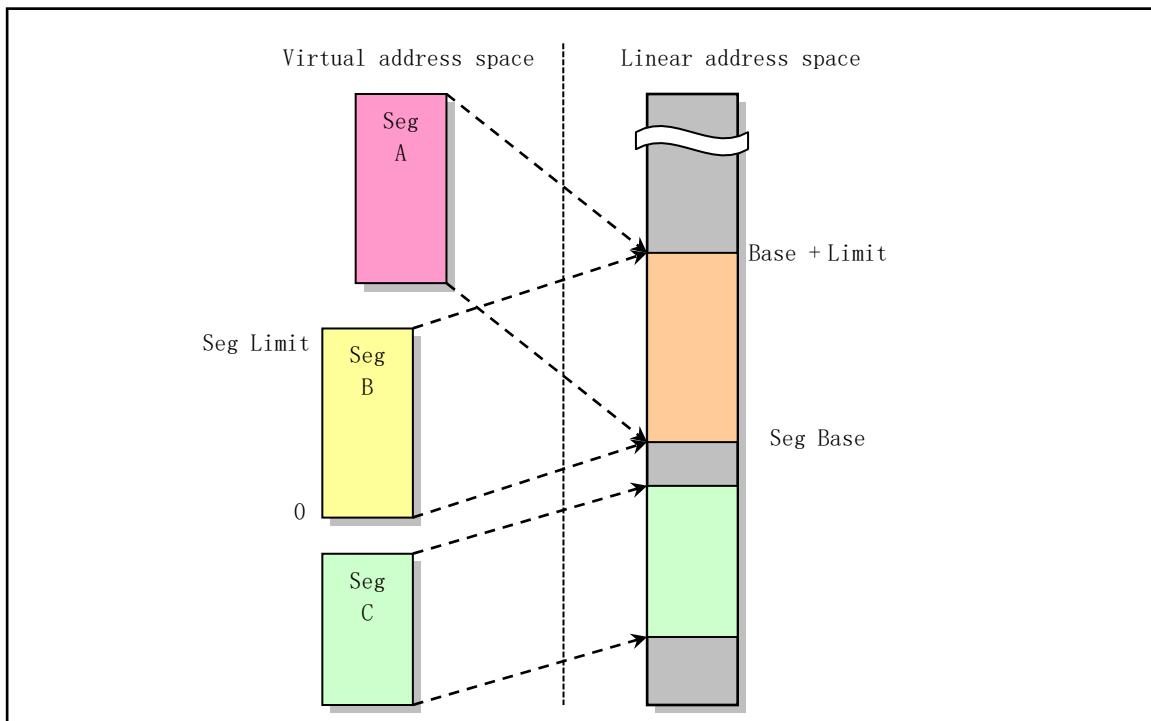


Figure 4-6 Segments in virtual map to linear address space

セグメントのベースアドレス、制限長、保護属性は、セグメント記述子と呼ばれる構造体に格納されます。このセグメント記述子は、論理アドレスから線形アドレスへの変換マッピングの際に使用されます。セグメント記述子は、記述子テーブルに格納されます。セグメント・ディスクリプター・テーブルは、セグメント・ディスクリプター・アイテムを含む単純な配列です。前述のセグメント・セレクタは、テーブル内のセグメント・ディスクリプタの位置を指定することで、対応するセグメントを指定します。

セグメントの機能を最小限にしても、論理アドレスを使ってプロセッサのアドレス空間の各バイトにアクセスできます。論理アドレスは、図4-

7に示すように、16ビットのセグメントセレクタと32ビットのオフセットで構成されます。セグメント

セレクタは、バイトが配置されているセグメントを指定し、オフセットはセグメントベースアドレスに対するセグメント内のバイトの位置を指定します。プロセッサは、各論理アドレスをリニアアドレスに変換します。リニアアドレスとは、プロセッサのリニアアドレス空間における32ビットのアドレスのことです。物理アドレス空間と同様に、リニアアドレス空間もまた、0から0xFFFFFFFFまでのアドレスを持つフラットな4GBのアドレス空間です。リニアアドレス空間には、システムで定義されたすべてのセグメントとシステムテーブルが含まれています。

論理アドレスをリニアアドレスに変換するために、プロセッサは以下の演算を行います。

1. セグメント・セレクタのオフセット値（セグメント・インデックス）を使用して、GDT または LDT テーブル内の対応するセグメント記述子を探します。（この手順は、新しいセグメント・セレクタをセグメント・レジスタにロードする場合にのみ必要です）。
2. セグメント記述子を調べて、セグメントのアクセス権と範囲をチェックし、セグメントがアクセス可能であること、オフセットがセグメントの制限内であることを確認します。
3. セグメント記述子で取得したセグメント・ベース・アドレスをオフセットに加え、最終的にリニア・アドレスを形成します。

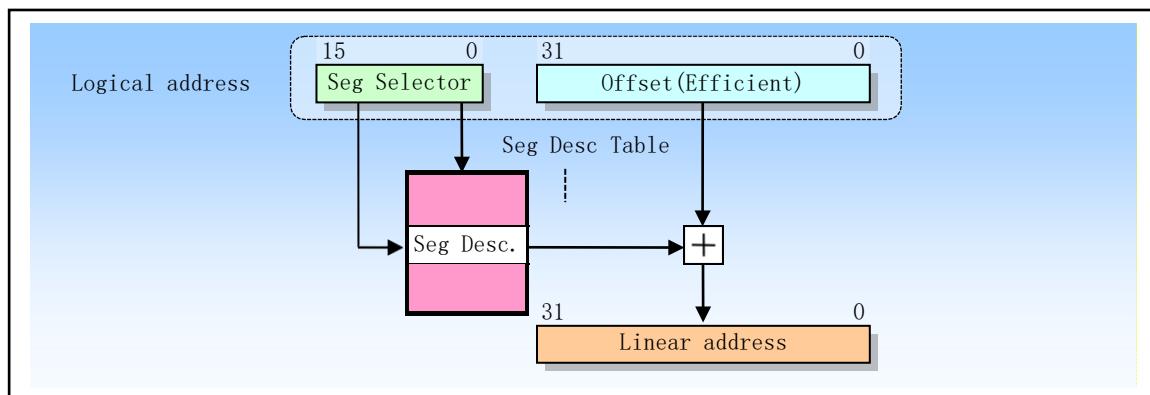


Figure 4-7 Logical address to linear address translation

ページングが有効でない場合、プロセッサはリニアアドレスを物理アドレスに直接マッピングします（つまり、リニアアドレスはプロセッサのアドレスバスに送られます）。リニアアドレス空間がページングされている場合は、第2レベルのアドレス変換を用いてリニアアドレスを物理アドレスに変換します。ページ変換については後で説明します。

### 4.3.2 セグメント記述子のテーブル

図4-

8に示すように、セグメントディスクリプターテーブルは、セグメントディスクリプターの配列です。ディスクリプターテーブルは可変長で、最大8192個の8バイトディスクリプターを格納できます。ディスクリプターテーブルには、グローバルディスクリプターテーブル（GDT）とローカルディスクリプターテーブル（LDT）の2つがあります。

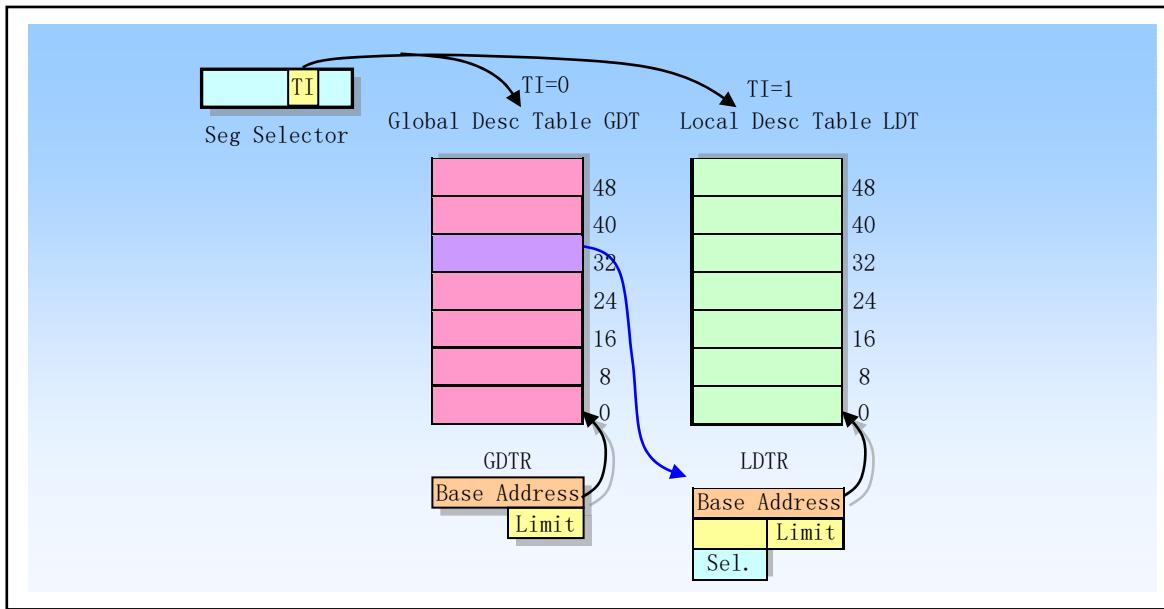


Figure 4-8 Global and Locat Descriptor Tables

各システムには、システム内のすべてのプログラムおよびタスクに使用できる1つのGDTが必要です。オプションとして、1つまたは複数のLDTを定義することができます。例えば、実行中の個々のタスクごとにLDTを定義したり、一部またはすべてのタスクで同じLDTを共有することができます。

GDT自体はセグメントではなく、リニアアドレス空間内のデータ構造である。GDTの基本リニアアドレスとリミットは、GDTRレジスタにロードする必要があります。また、GDTの基本アドレスはを8バイトごとに整列させることで、プロセッサの性能を最大限に引き出すことができます。GDTの制限値はバイト単位で表されます。セグメント化と同様に、リミット値はベースアドレスに追加され、最後の有効バイトのアドレスになります。リミット値が0の場合、有効なバイトは1つになります。セグメント記述子の長さは常に8バイトであるため、GDTリミットは常に8の整数倍（つまり $8N-1$ ）より小さくなければなりません。

LDTテーブルは、LDTタイプのシステムセグメントに格納されます。このとき、GDTにはLDTのセグメント記述子が含まれていなければなりません。システムが複数のLDTをサポートしている場合は、各LDTにセグメント記述子とセグメントセレクタがGDTに含まれていなければなりません。LDTセグメント記述子は、GDTテーブルのどこにでも格納できます。

LDTにアクセスするには、そのセグメントセレクタが必要です。LDTにアクセスする際のアドレス変換回数を減らすために、LDTのセグメントセレクタ、ベースアドレス、セグメント長、アクセス権

をLDTRレジスタに格納する必要があります。

SGDT命令でGDTRレジスタをストアすると、48ビットの「疑似ディスクリプタ」がメモリに格納される。ユーザー モード（特権レベル3）でのアライメントチェックエラーを回避するために、ダミー ディスクリプターは奇数ワードのアドレスに格納する必要があります（例：アドレスMOD4=2）。これにより、プロセッサは最初にアラインド・ワードを格納し、次にアラインド・ダブルワード（4バイト・アラインメント）を格納します。ユーザー モードのプログラムでは、通常、ダミーの記述子を保存しませんが、アライメントチェックエラーの可能性を避けるために、このアライメントを使用することができます。また、SIDT命令でIDTRレジスタの内容を保存する場合にも、同じアラインメントが使用されます。ただし、LDTRやタスクレジスタを保存する場合（それぞれSLTR命令、STR命令を使用）は、ダミー記述子をダブルワードアラインドのアドレス（すなわち、アドレスMOD4=0）に保存する必要があります。

記述子テーブルは、オペレーティングシステムが保持する特殊なデータ構造に格納され、プロセッサのメモリ管理ハードウェアによって参照されます。これらの特別な構造体は、アプリケーションがその中のアドレス変換情報を変更できないように、オペレーティングシステムソフトウェアのみがアクセスできる保護されたメモリ領域に格納する必要があります。仮想（論理）アドレス空間は、同じ大きさの2つのハーフに分けられます。半分はGDTによってリニアアドレスにマッピングされ、残りの半分はLDTによってマッピングされます。仮想アドレス空間全体には $2^{14}$ 個のセグメントがあり、その半分（つまり $2^{13}$ 個のセグメント）はGDTによってマッピングされたグローバル仮想アドレス空間であり、残りの半分はLDTによってマッピングされたローカル仮想アドレス空間である。記述子テーブル（GDTまたはLDT）とテーブル内の記述シンボルを指定することで、記述子の位置を特定することができます。

タスクの切り替えが発生すると、LDTは新しいタスクのLDTに置き換えられますが、GDTは変更されません。したがって、GDTによってマッピングされた仮想アドレス空間の半分はシステム内のすべてのタスクに共通ですが、残りの半分のLDTのマッピングはタスクが切り替わったときに変更されます。システム内のすべてのタスクが共有するセグメントは、GDTによってマッピングされます。このようなセグメントには、通常、オペレーティングシステムを含むセクションと、LDTを含む各タスクの特別なセクションがあります。LDTセグメントは、オペレーティングシステムに属するデータと考えることができます。

LDTには、1つのタスク専用のセグメントの記述子があります。複数のタスクが共通のLDTを共有することができます。この場合、これらのタスクはすべて同じLDTを持っているため、同じセグメントのセットを使用することができ、すべてのタスクは1つのGDTを共有します。また、両タスクはそれぞれのLDTでセグメント記述子を共有することができる、GDTに記述子を置くことなくセグメントを共有することができる、すべてのタスクで共有されます。この場合、共有セグメントは2つの異なるLDTに2つの記述子を持ち、一緒に更新しなければならないため、オペレーティングシステムが排他的に処理しなければなりません。

図4-

9は、GDTとLDTの間でタスクのセグメントがどのように分けられるかを示しています。この図では、2つのアプリケーション（AとB）とオペレーティング・システムに対して6つのセグメントがあります。システム内の各アプリケーションはタスクに対応しており、各タスクにはそれぞれLDTがあります。アプリケーションAはタスクAで実行され、セグメントCodeAとDataAをマップするLDTAを持っていて、同様

に、アプリケーションBはタスクBで実行され、LDTBを使ってCodeBとDataBのセグメントをマッピングします。オペレーティングシステムのカーネルを含む2つのセグメント、CodeOSとDataOSは、LDTを使用してマッピングされます。

GDTは、両方のタスクで共有できるようになっています。2つのLDTセグメントLDTAとLDTBもGDTでマッピングされています。

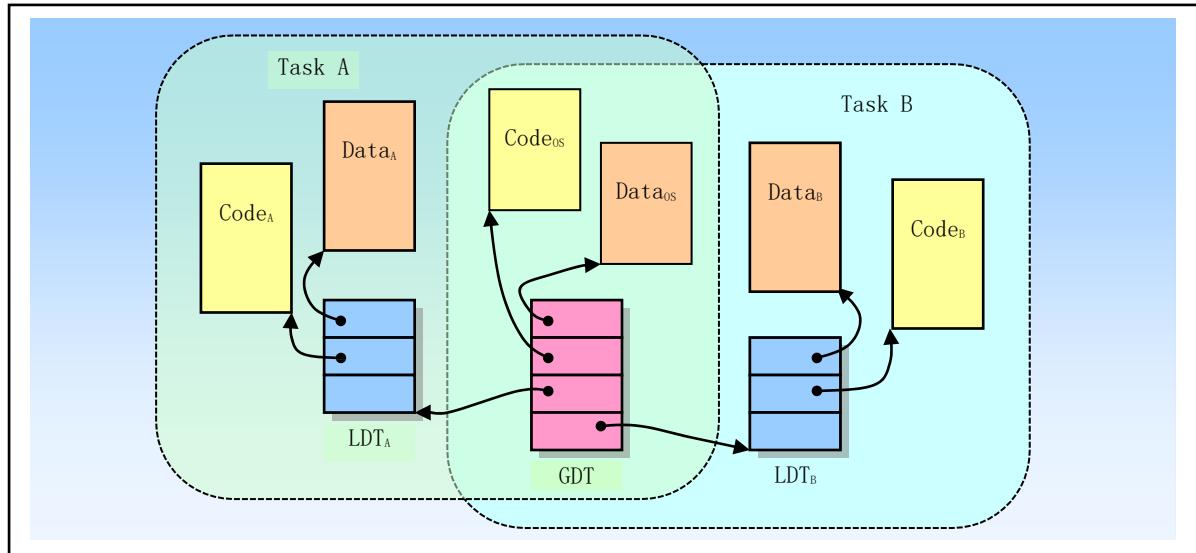


Figure 4-9 The segment types used by tasks

タスクAが実行されているとき、アクセス可能なセグメントには、LDTAマップのCodeAとDataAのセグメントに加え、GDTマップのオペレーティング・システムのCodeOSとDataOSのセグメントが含まれます。タスクBが実行中の場合、アクセス可能なセグメントには、LDTBマップのCodeBとDataBのセグメントに加え、GDTマップのセグメントが含まれます。

この例では、仮想アドレス空間を整理して、各タスクが異なるLDTを使用することで、各タスクを分離することができます。タスクAが実行中の場合、タスクBのセグメントは仮想アドレス空間に含まれないため、タスクAはタスクBのメモリにアクセスできません。同様に、タスクBが実行されているときは、タスクAのセグメントはアドレス指定できません。このように、LDTを使って各アプリケーションタスクを分離する方法は、重要な保護ニーズの一つです。

### 4.3.3 セグメントセレクター

セグメント・セレクタは、図4-

10に示すように、セグメントを表す16ビットの識別子です。セグメント・セレクタはセグメントを直接指すのではなく、セグメント・ディスクリプタ・テーブルの中のセグメントを定義するセグメント・ディスクリプタを指します。セグメント・セレクタは3つのフィールドで構成され、その内容は以下の通りです。

- Requested Privilege Level (RPL) の略。
- テーブルインデックス (TI)。
- インデックス

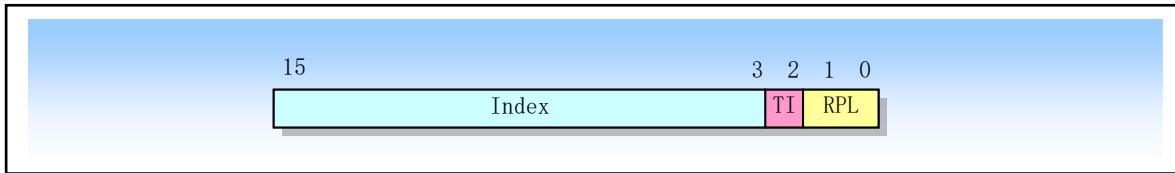


Figure 4-10 Segment selector structure

リクエスト・プリビレッジ・レベルRPLは、後に詳述するセグメント・プロテクション情報を提供する。テーブル・インデックス TI は、指定されたセグメントを含むセグメント記述子テーブル GDT または LDT を示すために使用されます。

セグメントの記述子です。TI=0はGDTに、TI=1はLDTに記述子があることを示す。インデックス・フィールドは、GDTまたはLDTテーブル内のディスクリプターのインデックス番号を示す。このように、セレクタはセグメント・テーブル内の記述子を探してセグメントを指定し、記述子にはセグメントのベース・アドレス、セグメントの長さ、セグメントの属性など、セグメントにアクセスするためのすべての情報が含まれていることがわかります。

例えば、図4-

11(a)のセレクタ(0x08)は、GDTでRPL=0のセグメント1を指定しています。インデックス・フィールドの値は1、TIビットは0で、GDTテーブルが指定されています。図4-

11(b)のセレクタ(0x10)は、GDTのRPL=0のセグメント2を指定しています。インデックス・フィールドの値は2、TIビットは0で、GDTテーブルが指定されています。図4-

11(c)のセレクタ(0x0f)は、LDTのLPL=3のセグメント1を指定しています。インデックス・フィールドの値は1、TIビットは1で、LDTテーブルが指定されています。図4-

11(d)のセレクタ(0x17)は、LPL=3のセグメント2をLDTで指定しています。インデックス・フィールドの値は2、TIビットは1で、LDTテーブルが指定されています。実際、図4-

11の最初の4つのセレクタ：(a)、(b)、(c)、(d)は、それぞれLinux

0.1xカーネルのカーネル・コード・スニペット、カーネル・データ・スニペット、タスク・コード・スニペット、タスクを表しています。データセグメントのセレクタ。図4-

11(e)のセレクタ(0xffff)は、LDTテーブルのRPL=3のセグメント8191を指定しています。インデックス・フィールドの値は0b111111111 (つまり8191)、TIビットは1で、LDTテーブルが指定されています。

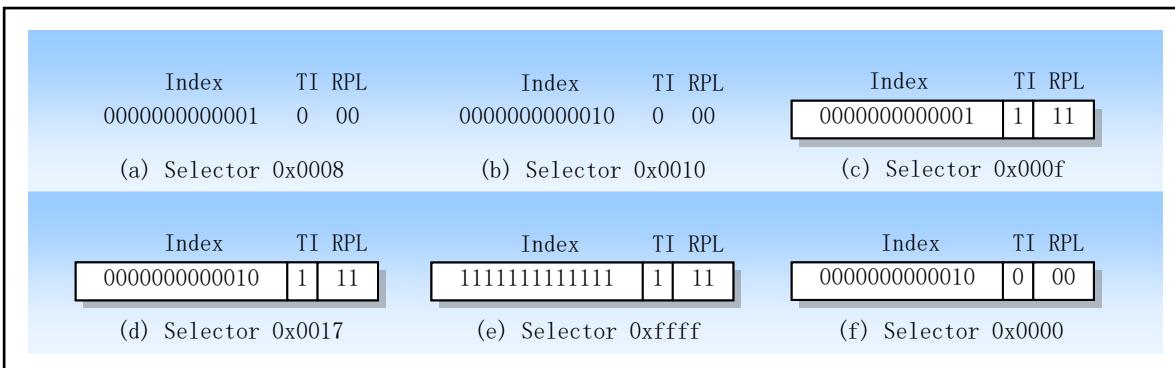


Figure 4-11 Segment selector examples

また、プロセッサはGDTテーブルの最初の項目を使用しません。図4-

11(f)に示すように、GDTエントリへのセレクタ(つまり、インデックス値が0でTIフラグが0のインデックス)は、「空セレクタ」として使用されます。空のセレクタをセグメント・レジスタ(CSとSS以外)にロードしても、プロセッサは例外を発生させません。しかし、空のセレクタを含むセグメント・レジスタを使ってメモリにアクセスすると例外が発生します。CSやSSのセグメント・レジスタに空のセレクタをロードすると例外が発生します。

セグメント・セレクタはポインタ変数の一部としてアプリケーションに表示されますが、セレクタの値は通常、アプリケーションではなく、リンク・エディタやリンク・ローダによって設定または変更されます。アドレス変換の時間とプログラミングの複雑さを軽減するために、プロセッサには最大6つのセグメントセレクタを保持するレジスタ(図4-12参照)、すなわちセグメントレジスタが用意されています。各セグメントレジスタは、特定の種類のメモリ参照(コード、データ、stack)をサポートします。原則として、各プログラムは少なくとも有効なセグメント・セレクタをコード・セグメント(CS)、データ・セグメント(DS)、stack・セグメント(SS)の各レジスタにロードする必要があります。また、プロセッサには3つの補助データセグメントレジスタ(ES、FS、GS)が用意されており、現在実行中のプログラム(またはタスク)が他の複数のデータセグメントにアクセスするために使用できます。

Visible Part		Hidden Part
Seg Selector	Base Address, Limit, Access Info	
		CS
		SS
		DS
		ES
		FS
		GS

Figure 4-12 Segment register structure

セグメントにアクセスするプログラムでは、セグメント・セレクタがセグメント・レジスタにロードされている必要があります。したがって、システムでは多くのセグメントを定義できますが、同時にすぐにアクセスできるのは  
6つのセグメントだけです。他のセグメントにアクセスするには、これらのセグメントのセレクタをロードする必要があります。

また、メモリにアクセスするたびに記述子テーブルを読まなくても済むように、セグメント記述子を読み込んでデコードするために、各セグメントレジスタには「可視部」と「隠部」があります(隠部は「記述子バッファ」または「シャドーレジスタ」とも呼ばれます)。セグメント・セレクタがセグメント・レジスタの可視部分にロードされると、プロセッサはセグメント・セレクタが指すセグメント・ディスクリプタのセグメント・アドレス、セグメント・レンジス、およびアクセス・コントロール情報をセグメント・レジスタの非表示部分にロードします。セグメント・レジスタ(可視部と非表示部)にバッファリングされた情報により、プロセッサはアドレス変換を行う際に、セグメント記述子からベース・アドレスとリミット値を読み取る時間を短縮することができます。

シャドウ・レジスタには、ディスクリプター情報のコピーが含まれているため、オペレーティング・システムは、ディスクリプター・テーブルの変更がシャドウ・レジスタに反映されるようにしな

ければなりません。そうしないと、記述子テーブルのセグメントのベース・アドレスまたはリミットが変更されても、その変更がシャドウ・レジスタに反映されません。このような問題に対処する最も簡単な方法は、ディスクリプター・テーブルのディスクリプターに変更を加えた直後に、6つのセグメント・レジスタをリロードすることです。これにより、ディスクリプター・テーブルの対応するセグメント情報がシャドー・レジスタに再ロードされます。

セグメントレジスタをロードするためのロード命令には、2種類あります。

1. MOV、POP、LDS、LES、LSS、LGS、LFSのような命令。これらの命令は、セグメントレジスタを明示的に直接参照します。
2. CALL、JMP、RET、IRET、INTn、INTO、INT3など、ロングポインタを使った命令が暗黙のうちにロードされる。これらの命令は、動作中にCSレジスタ（および他の一部のセグメントレジスタ）の内容の変更を伴います。

もちろん、MOV命令を使ってセグメントレジスタの可視部分の内容を汎用レジスタに格納することもできます。

#### 4.3.4 セグメントディスクリプタ

先ほど、セグメントセレクターを使って記述子テーブルの記述子を探すことを説明しました。セグメント記述子は、GDTおよびLDTテーブル内のデータ構造項目で、セグメントの位置やサイズ、アクセス制御の状態などの情報をプロセッサに提供するために使用されます。各セグメント記述子は8バイト長で、セグメントのベースアドレス、セグメントの長さ、セグメントの属性の3つのフィールドを含みます。セグメント・ディスクリプターは通常、コンパイラ、リンカー、ローダ、オペレーティング・システムによって作成されますが、決してアプリケーションではありません。図4-13は、すべてのタイプのセグメント記述子の一般的なフォーマットを示しています。

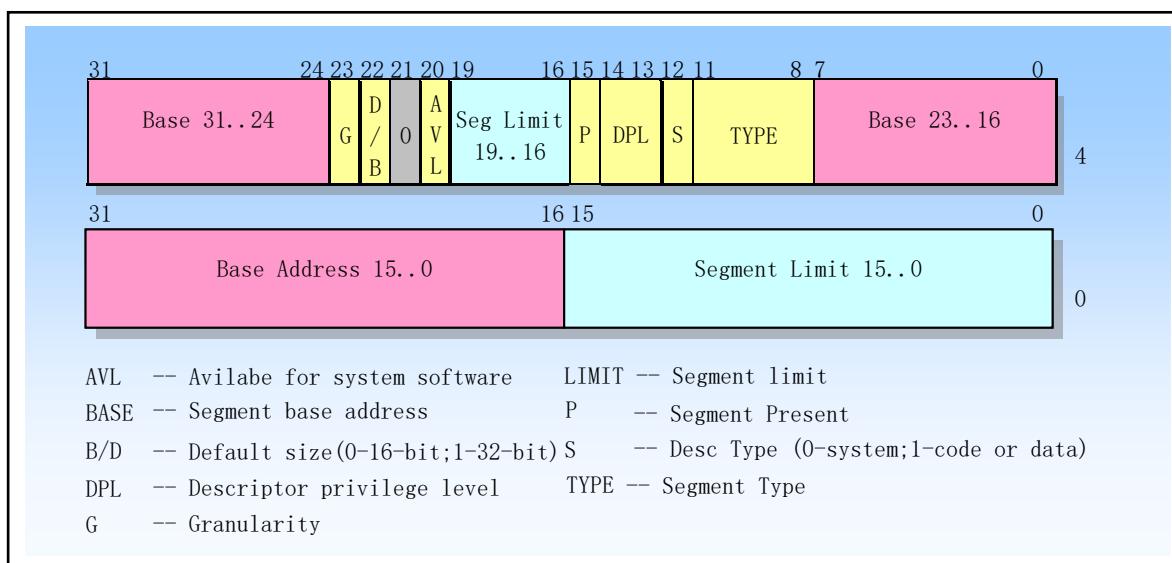


Figure 4-13 General format of segment descriptor

セグメントデスクリプタのフィールドとフラグの意味は以下の通りです。

#### ◆セグメントリミットフィールド (LIMIT)

セグメント・リミット・フィールドは、セグメントのサイズを指定するために使用される。

プロセッサは、セグメント記述子の2つのセグメント・リミット・フィールドを20ビットの値に結合し、セグメント・リミット長Limit値の実際の意味を粒度フラグGに応じて指定する。G=0の場合、セグメント長Limitの範囲は1バイトから1MBバイトまで、単位はバイトである。G=1の場合、セグメント長Limitの範囲は4KBから4GBまでで、単位は4KBとなります。

セグメントタイプのセグメント拡張方向フラグEに応じて、プロセッサはセグメントリミットLengthを2つの異なる方法で使用します。上方拡張セグメント（上方拡張セグメントと略す）の場合、論理アドレスのオフセット値は0からセグメント限界値Limitまでの範囲になります。限界長Limitより大きいオフセットは、一般的な保護例外を発生させます。下方に延長されているセグメント（下位セグメントと略す）では、セグメント限界値Limitの意味が逆になります。デフォルトのスタック・ポインタ・サイズ・フラグBの設定に応じて、オフセット値はセグメント限界長から0xFFFFFFFFまたは0xFFFFまでの範囲になります。オフセット値が制限長Limitより小さい場合、一般的な保護例外が発生します。次の拡張セグメントでは、セグメントリミットフィールドの値を減らすと、新しいメモリがセグメントアドレス空間の一番上ではなく、一番下に割り当てられます。80X86のスタックは常に縮小されているので、この実装はスタックを拡張するのに適しています。

#### ◆ベースアドレスフィールド (BASE)

このフィールドは、4GBのリニアアドレス空間におけるバイト0のセグメントの位置を定義します。プロセッサは、3つの異なるベースアドレスフィールドを組み合わせて32ビットの値を形成します。セグメントのベースアドレスは、16バイトの境界にアラインする必要があります。これは必須ではありませんが、プログラムのコードセグメントとデータセグメントを16バイト境界に揃えることで、プログラムの最高のパフォーマンスを得ることができます。

#### ◆タイプフィールド (TYPE)

タイプフィールドは、セグメントまたはゲートのタイプ、セグメントを記述するためのアクセスのタイプ、セグメントの拡張方向を指定する。このフィールドの解釈は、アプリケーション（コードまたはデータ）記述子であるか、システム記述子であるかを示す記述子タイプフラグSに依存する。のです。

TYPEフィールドのエンコーディングは、図4-

14に示すように、コード、データ、システムディスクリプターで異なります。

#### ◆ディスクリプタタイプフラグ (S)

記述子タイプフラグSは、セグメント記述子がシステムセグメント記述子であるか (S=0の場合)、コードまたはデータセグメント記述子であるか (S=1の場合) を示す。

#### ◆ディスクリプタ・プリビレッジ・レベル (DPL)

DPLフィールドは、ディスクリプターの特権レベルを示す。特権レベルの範囲は0から3までで、0が最も高く、3が最も低いレベルとなります。DPLはセグメントへのアクセスを制御するために使用されます。

#### ◆セグメントの存在 (P)

セグメント・プレゼンス・フラグPは、セグメントがメモリ内にある (P=1) か、メモリ内にない (P=0) かを示します。セグメント記述子のPフラグが0の場合、このセグメント記述子を

指すセレクタをセグメント・レジスタにロードすると、例外なくセグメントが生成されます。メモリ管理ソフトウェアはこのフラグを利用して、ある時点でのセグメントを実際にメモリにロードする必要性を制御することができます。この機能により、仮想ストレージはページングメカニズムを超えた制御が可能になります。図4-

15は、P=0の場合のセグメント記述子のフォーマットを示しています。Pフラグが0の場合、セグメントが実際には存在しない場所に関する情報など、フォーマット内でAvailableとマークされているフィールドを使って、オペレーティングシステムは独自のデータを自由に保存することができます。

#### ◆ 既定の演算サイズ／既定のスタックポインタサイズ／上限値（D/B）

このマークは、セグメント記述子が、実行コードセグメント、スプレッドデータセグメント、スタックセグメントのいずれであるかによって、機能が異なります。（32ビットのコードセグメントおよびデータセグメントでは、このフラグは常に1に設定されるべきであり、16ビットのコードセグメントおよびデータセグメントでは、このフラグは0に設定されます）。

- 実行可能なコードのセグメント。このフラグは、現時点ではDフラグと呼ばれ、このセグメントの命令が有効なアドレスとデフォルトの長さのオペランドを参照していることを示すために使用されます。フラグがセットされている場合、デフォルト値は32ビットのアドレスと32ビットまたは8ビットのオペランド、フラグが0の場合、デフォルト値は16ビットのアドレスと16ビットまたは8ビットのオペランドとなります。命令のプレフィックス0x66はデフォルト以外のオペランドサイズを選択するために、プレフィックス0x67はデフォルト以外のアドレスサイズを選択するために使用することができます。
- スタックセグメント（SSレジスターが指すデータセグメント）。このとき、このフラグはB（ビッグ）フラグと呼ばれ、暗黙のスタック操作（PUSH、POP、CALLなど）が発生したときのスタックポインタの大きさを示します。このフラグがセットされている場合、32ビットのスタックポインタが使用され、ESPレジスタに格納されます。フラグが0の場合、16ビットのスタックポインタが使用され、SPレジスタに格納されます。スタックセグメントが下位拡張データセグメントに設定されている場合、このBフラグはスタックセグメントの上限値も指定します。
- データセグメントを展開します。この時のフラグはBフラグと呼ばれ、セグメントの上限を示すのに使われます。このフラグがセットされている場合、スタックセグメントの上限は0xFFFFFFFF（4GB）、このフラグがセットされていない場合、スタックセグメントの上限は0xFFFF（64KB）となります。

#### ◆ グラニュラリティ（G）

このフィールドは、セグメント・リミット・フィールド値の単位を決定するために使用します。granularityフラグが0の場合、セグメント制限値の単位はバイトで、granularityフラグが設定されている場合、セグメント制限値は4KBの単位を使用します。（このフラグはセグメントのベースアドレスの粒度には影響しません。ベースアドレスの粒度は常にバイト単位です）。Gフラグが設定されていると、セグメント長を使ってオフセット値をチェックする際に、オフセット値の12ビットの最下位ビットをチェックしません。例えば、G=1の場合、セグメント制限長が 0 であれば、有効なオフセット値は 0 ~ 4095 であることを示します。

## ◆ 使用可能なビットと予約済みのビット

セグメント記述子の2つ目のダブルワードのビット20は、システム・ソフトウェアが使用可能であり、ビット

21は予約ビットで、常に0に設定する必要があります。

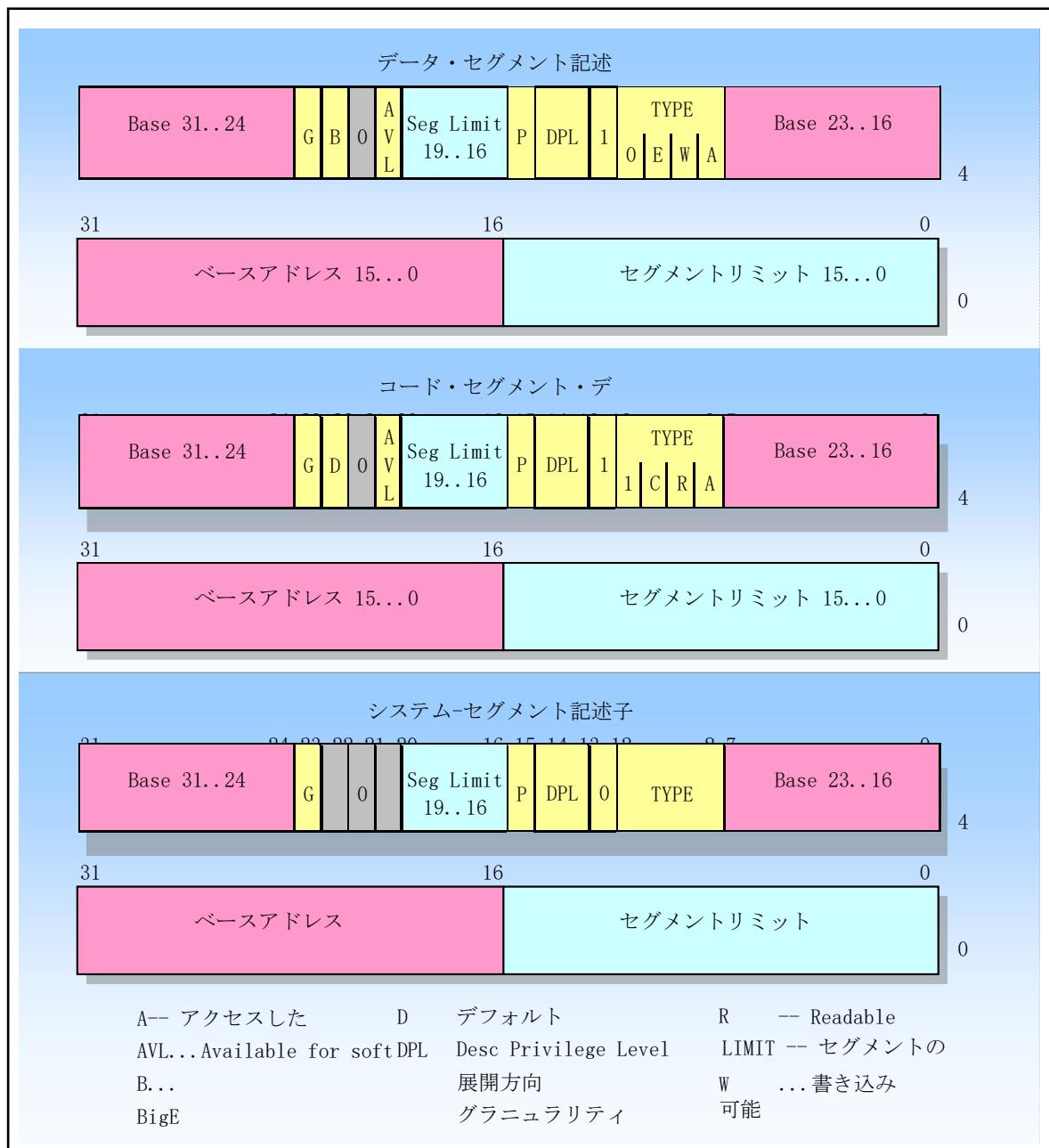


Figure 4-14 Code, data, and system segment descriptors formats

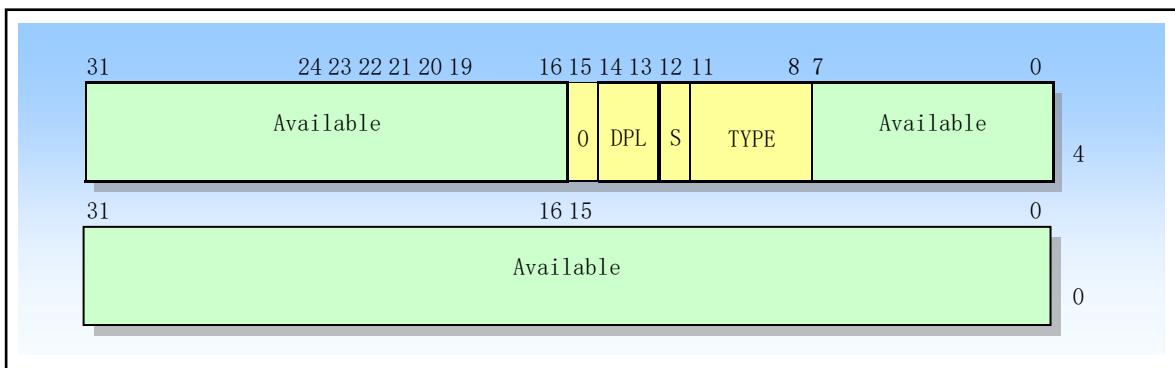


Figure 4-15 Segment Descriptor When bit P=0

### 4.3.5 コードとデータセグメントの記述子の種類

セグメント・ディスクリプターにS（ディスクリプター・タイプ）フラグが設定されている場合、そのディスクリプターはコード・セグメントまたはデータ・セグメントに使用されます。このとき、タイプ・フィールドの最上位ビット（2つ目のダブルワードのビット11）を使って、データ・セグメントの記述子（リセット）かコード・セグメントの記述子（セット）かを判断します。

データ・セグメントの場合、タイプ・フィールドの下位3ビット（ビット8、9、10）は、それぞれアクセス済み、書き込み可能、拡張方向を示すのに使用されます。コード・セグメントとデータ・セグメントのタイプ・フィールドのビット・フィールドの説明は、表4-3を参照してください。書き込み可能ビットWの設定により、データ・セグメントはリード・オンリー、またはリード・アンド・ライタブルになります。

Table 4-3 Code and Data Segment Descriptor Types

Decimal	TYPE Field					Descriptor Type	Description
	11	10	9	8			
		E	W	A			
0	0	0	0	0	Data	Read-Only	
1	0	0	0	1	Data	Read-Only, accessed	
2	0	0	1	0	Data	Read/Write	
3	0	0	1	1	Data	Read/Write, accessed	
4	0	1	0	0	Data	Expand-down, Read-Only.	
5	0	1	0	1	Data	Expand-down, Read-Only, accessed	
6	0	1	1	0	Data	Expand-down, Read/Write	
7	0	1	1	1	Data	Expand-down, Read/Write, accessed	
		C	R	A			
8	1	0	0	0	Code	Execute-Only	
9	1	0	0	1	Code	Execute-Only, accessed	
10	1	0	1	0	Code	Execute/Read	
11	1	0	1	1	Code	Execute/Read, accessed	
12	1	1	0	0	Code	Conforming, Execute-Only	
13	1	1	0	1	Code	Conforming, Execute-Only, accessed	
14	1	1	1	0	Code	Conforming, Execute/Read-Only	
15	1	1	1	1	Code	Conforming, Execute/Read-Only, accessed	

スタックセグメントは読み取り/書き込み可能なデータセグメントでなければなりません。書き換え不可能なデータセグメントセレクターが読み込まれると

SSレジスタを使用すると、一般保護例外が発生します。スタックセグメントの長さを動的に変更する必要がある場合、スタックセグメントは下方向に拡張されたデータセグメントとすることができます（拡張方向フラグが設定されています）。ここで、セグメントの上限を動的に変更すると、スタックスペースがスタックの最下部に追加されます。

アクセスされたビットは、オペレーティング・システムが最後にこのビットをリセットした後、セグメントがアクセスされたかどうかを示します。プロセッサがセグメントセレクタをセグメントレジスタにロードするたびに、このビットがセットされます。このビットは明示的にクリアする必要があります、クリアしないとセットされたままになります。このビットは、仮想メモリの管理やデバッグに使用できます。

コード・セグメントの場合、タイプ・フィールドの下位3ビットは、Accessed、Read-enable、Conformingと解釈されます。読み取り可能なRフラグの設定により、コード・セグメントは実行専用または実行/読み取りが可能です。実行/読み取り可能なコードセグメントは、定数などの静的データと命令コードをROMに配置する場合に使用できます。ここでは、CSオーバーライド・プレフィックスを持つ命令を使用するか、コード・セグメントのコード・セグメント・セレクタをデータ・セグメント・レジスタ (DS、ES、FS、GS) にロードすることで、コード・セグメントのデータを読み出すことができます。プロテクトモードでは、コードセグメントの書き込みはできません。

コードセグメントには、適合するものと適合しないものがあります。より高い特権レベルの適合セグメントに実行制御を移すと、プログラムは現在の特権レベルで実行を続けることができます。特

権レベルの異なる適合しないセグメントに転送すると、コールゲートやタスクゲートを使用しない限り、一般的な保護例外が発生します。

(適合するコードセグメントと適合しないコードセグメントの詳細については、「コードセグメントへの直接の呼び出しまだはジャンプ」を参照)。保護機能にアクセスしないシステムツールや、一部の例外タイプ(エラー、オーバーフローなど)は、整合性のあるセグメントに格納できます。低権限のプログラムやプロシージャによるアクセスを防止する必要があるツールは、非適合セグメントに格納する必要があります。なお、対象セグメントが適合コード・セグメントか不適合コード・セグメントかにかかわらず、コールやジャンプによって、より低い権限の(数値的に高い権限レベルの)コード・セグメントに実行を移すことはできません。

すべてのデータセグメントは、特権を持たないプログラムやプロシージャからはアクセスできないという意味で、不適合です。しかし、コード・セグメントとは異なり、データ・セグメントは、特別なアクセス・ゲートを使用せずに、より高い権限を持つプログラムやプロシージャからアクセスすることができます。

GDTやLDTのセグメント・ディスクリプターがROMに格納されている場合、ソフトウェアやプロセッサがROMのセグメント・ディスクリプターを更新(書き込み)しようとすると、プロセッサは無限ループに陥ります。この問題を防止するために、ROMに格納する必要のあるすべてのディスクリプターのアクセス済みビットをあらかじめ設定しておく必要があります。同時に、ROMのセグメントディスクリプターを変更しようとするOSのコードを削除する。

#### 4.3.6 システム記述子の種類

セグメント・ディスクリプターのSフラグ(ディスクリプター・タイプ)がリセット状態(0)のとき、そのディスクリプター・タイプはシステム・ディスクリプターです。プロセッサは以下のタイプのシステム記述子を認識できます。

- LDT(Local Descriptor Table) のセグメントディスクリプター。
- タスクステートセグメント(TSS)の記述子。
- コールゲートのディスクリプター。
- インタラプトゲートのディスクリプター。
- トランプゲートの記述子。
- タスクゲートの記述子。

これらの記述子は、大きく分けて「システムセグメント記述子」と「ゲート記述子」の2種類があります。システムセグメント記述子は、システムセグメント(LDTやTSSセグメントなど)を指します。ゲートディスクリプターは、「ゲート」を指します。コール、インタラプト、トランプゲートの場合は、コードセグメントのセレクタとそのセグメント内のプログラムエントリポイントのポインタを含み、タスクゲートの場合は、TSSセグメントのセレクタを含みます。表4-4

は、システムセグメント記述子とゲート記述子タイプフィールドのエンコーディングを示しています。

Table 4-4 System-Segment and Gate-Descriptor Types

Decimal	TYPE Field					Description
	11	10	9	8		
0	0	0	0	0		Reserved
1	0	0	0	1		16-Bit TSS (Available)
2	0	0	1	0		LDT
3	0	0	1	1		16-Bit TSS (Busy)
4	0	1	0	0		16-Bit Call Gate
5	0	1	0	1		Task Gate
6	0	1	1	0		16-Bit Interrupt Gate
7	0	1	1	1		16-Bit Trap Gate
8	1	0	0	0		Reserved
9	1	0	0	1		32-Bit TSS (Available)
10	1	0	1	0		Reserved
11	1	0	1	1		32-Bit TSS (Busy)
12	1	1	0	0		32-Bit Call gate
13	1	1	0	1		Reserved
14	1	1	1	0		32-Bit Interrupt Gate
15	1	1	1	1		32-Bit Trap Gate

TSSのステータス・セグメントとタスク・ゲートの使用については、「タスク管理」の項で説明します。コールゲートの使用については、保護のセクションで説明します。割り込みとトラップゲートの使用は、割り込みと例外処理で使用されます。セクションで説明します。

## 4.4 ページング

ページング機構は、80X86のメモリ管理機構の第2の部分である。ページング機構は、セグメンテーション機構に基づいて、仮想（論理）アドレスから物理アドレスへの変換処理を完成させます。セグメンテーション機構は、論理アドレスをリニアアドレスに変換し、ページングはリニアアドレスを物理アドレスに変換します。ページングは、あらゆる種類のセグメントモデルに使用できます。プロセッサのページングメカニズムは、セグメントがマッピングされたリニアアドレス空間を分割し、これらのリニアアドレス空間のページを物理アドレス空間のページにマッピングします。ページングメカニズムのいくつかのページレベルの保護手段は、セグメント保護メカニズムと組み合わせて使用したり、セグメントメカニズムの保護手段を置き換えることができます。例えば、読み取り/書き込みの保護は、ページ単位で強化することができます。さらに、ページ単位では、ページングメカニズムは、ユーザー・スーパーユーザーの2レベルの保護も提供します。

ページング機構は、コントロールレジスタCR0のPGビットを設定することで有効になります。PG=1の場合、ページングが有効になり、プロセッサはこのセクションで説明するメカニズムを使ってリニアアドレスを物理アドレスに変換します。PG=0の場合、ページングメカニズムは無効となり、セグメンテーションメカニズムによって生成されたリニアアドレスが物理アドレスとして直接使用されます。

前述のセグメンテーション機構は、さまざまな可変サイズのメモリ領域で動作します。フラグメントーションとは異なり、ページングメカニズムは固定サイズのメモリブロック（ページと呼びます）に対して動作します。ページングメカニズムでは、リニアアドレス空間と物理アドレス空間をページに分割します。線形アドレス空間のどのページも

物理アドレス空間の任意のページ。図4-

16は、ページング機構が線形アドレス空間と物理アドレス空間をページに分割し、これら2つの空間の間に任意のマッピングを行う様子を示しています。図中の矢印は、リニアアドレス空間のページと物理アドレス空間のページを対応させています。

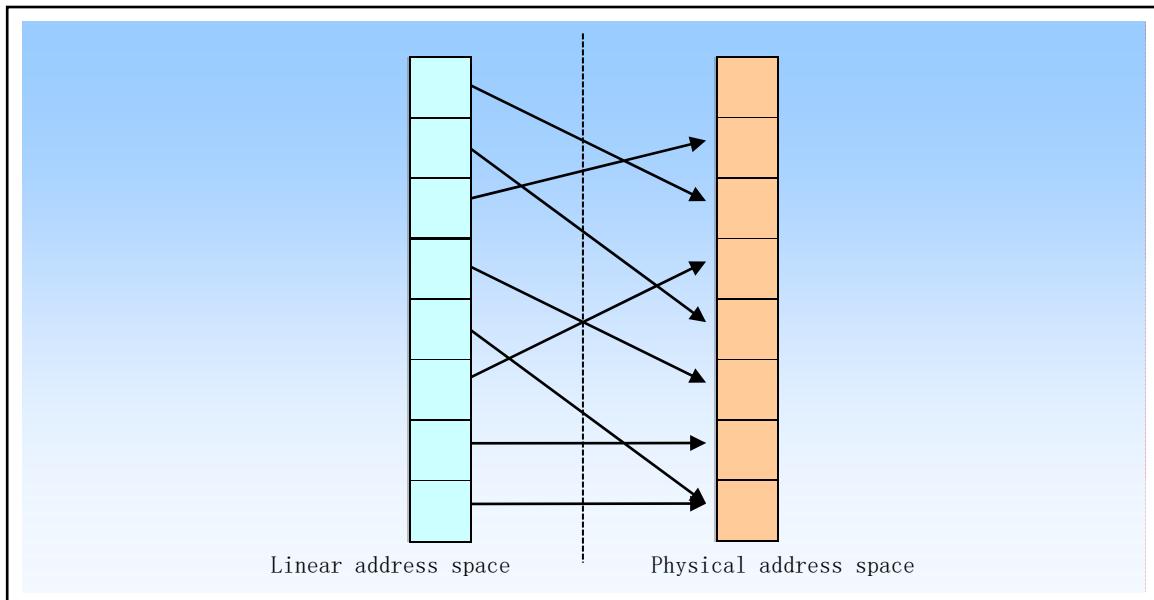


Figure 4-16 Illustration of correspondence between linear and physical address space pages

80X86では、4K ( $2^{12}$ ) バイトの固定サイズのページを使用し、4Kアドレス境界でアラインされています。つまり、ページングメカニズムは、 $2^{32}$ バイト (4GB) のリニアアドレス空間を $2^{20}$  (1M = 1048576) ページに分割します。ページングメカニズムは、リニアアドレス空間のページを物理アドレス空間に再配置することで動作します。4Kページは4K境界にアラインされた1つのユニットとしてマッピングされるため、リニアアドレスの下位12ビットは、物理アドレスの下位12ビットと同様にページ内オフセットとして直接使用することができます。ページング機構が行う再配置機能は、リニアアドレスの上位20ビットを、対応する物理アドレスの上位20ビットに変換することと考えられます。

ページングを使用すると、プロセッサはリニアアドレス空間を固定サイズのページ（長さ4KB）に分割して、物理メモリやディスクストレージにマッピングします。プログラム（またはタスク）がメモリ上の論理アドレスを参照すると、プロセッサはその論理アドレスをリニアアドレスに変換し、ページングメカニズムを使用してリニアアドレスを対応する物理アドレスに変換します。線形アドレスを含むページが物理メモリに存在しない場合、プロセッサはページフォルト例外を生成します。ページフォルト例外ハンドラは、通常、オペレーティングシステムに、対応するページをディスクから物理メモリにロードさせます（動作中に物理メモリの異なるページをディスクに書き込むこともあります）。ページが物理メモリにロードされた後、例外ハンドラからのリターンにより、例外の原因と

なった命令が再実行されます。プロセッサがリニアアドレスを物理アドレスに変換し、(必要に応じて) ページフォルト例外を生成するために使用する情報は、メモリに格納されているページディレクトリとページテーブルに含まれています。

ページングとセグメント化の最大の違いは、ページングでは固定長のページを使うことです。セグメント化されたアドレス変換のみを使用した場合、物理メモリに格納されたデータ構造には、そのすべての部分が含まれます。しかし、ページングを使用した場合、1つのデータ構造の一部を物理メモリに格納し、別の一部をディスクに格納することができます。

アドレス変換に必要なバスサイクル数を削減するために、直近にアクセスされたページディレクトリとページテーブルは、TLB (Translation Lookaside

Buffer) と呼ばれるプロセッサバッファに格納されます。TLBは

TLBは、バスサイクルを使わずに、ほとんどの読み取りページディレクトリとページテーブル要求を満たすことができます。TLBに必要なページテーブルエントリが含まれていない場合のみ、ページテーブルエントリをメモリから読み込むために余分なバスサイクルが使用されます。これは通常、ページテーブルエントリが長い間アクセスされていない場合に起こります。

#### 4.4.1 ページテーブル構造

ページング変換は、メモリ上に存在するテーブルによって記述されます。このテーブルはページテーブルと呼ばれ、物理的なアドレス空間に格納されています。ページテーブルは、 $2^{20}$ の項目を持つ単純な配列と見なすことができます。線形アドレスから物理アドレスへのマッピング機能は、簡単に言えば配列の検索と見なすことができます。リニアアドレスの上位20ビットは、この配列のインデックスを形成し、対応するページの物理(ベース)アドレスを選択するために使用されます。リニアアドレスの下位12ビットはページ内のオフセットを表し、これにページのベースアドレスが加わり、最終的に対応する物理アドレスが形成されます。ページベースアドレスは4Kバウンダリにアラインされているため、ページベースアドレスの下位12ビットは0でなければなりません。つまり、20ビットのページベースアドレスと12ビットのオフセット接続を組み合わせて、対応する物理アドレスを得ることができます。

ページテーブルの各エントリは、32ビットのサイズを持っています。ページの物理ベースアドレスを格納するのに必要なのは20ビットだけなので、残りの12ビットは、ページが存在するかどうかなどの属性情報を格納するのに使用できます。リニアアドレスインデックスページテーブルの項目が存在するとマークされていれば、その項目は有効であり、そのページの物理アドレスを取得することができます。アイテムが存在しないことを示している場合は、対応する物理ページにアクセスする際に例外が発生します。

##### 4.4.1.1 2階層のページテーブル構造

ページテーブルは $2^{20}$  (1M) 個のエントリを持ち、それぞれが4バイト (32ビット) を占める。これらが1つのテーブルとしてのみ格納されると、最大で4MBのメモリを占有することになる。そこで、80X86では、メモリ使用量を削減するために、2階層のテーブルを使用しています。このように、20ビットの上位リニアアドレスから物理アドレスへの変換も、1ステップあたり10ビットを使って2ステップで行われます。

第1階層のテーブルはページディレクトリと呼ばれる。1ページを4バイト長の $2^{10}$  (1K) 個のエントリで占めます。これらのエントリは、対応する2次テーブルを指しています。リニアアドレスの上位

10ビット（ビット31～22）は、1次テーブル（ページディレクトリ）のインデックス値として使用され、 $2^{10}$ 個の2次テーブルのいずれかを選択します。

第2レベルのテーブルはページテーブルと呼ばれる。ページテーブルの長さも1ページで、最大で1K個の4バイトエントリが含まれています。各4バイトのテーブルエントリには、関連するページの20ビットの物理ベースアドレスが含まれています。2次ページテーブルでは、リニアアドレスの中間10ビット（ビット21--

12）をエントリのインデックスとして使用し、ページの20ビット物理ベースアドレスを含むエントリを取得します。20ビットのページ物理ベースアドレスとリニアアドレスの下位12ビット（ページ内オフセット）が組み合わされ、ページ変換処理の出力値、すなわち対応する最終物理アドレスが得られます。

図4-

17は、2レベルのテーブルルックアップ処理を示しています。CR3レジスタは、ページディレクトリテーブルのベースアドレスを指定します。リニア・アドレスの上位10ビットは、このページ・ディレクトリ・テーブルのインデックスに使用され、関連する第2レベルのページ・テーブルへのポインタを取得します。線形アドレスの中央10ビットは、物理アドレスの上位20ビットを得るために、2次ページテーブルのインデックスに使用されます。線形アドレスの下位12ビットは、物理アドレスの下位12ビットとして直接使用され、完全な32ビットの物理アドレスを形成します。

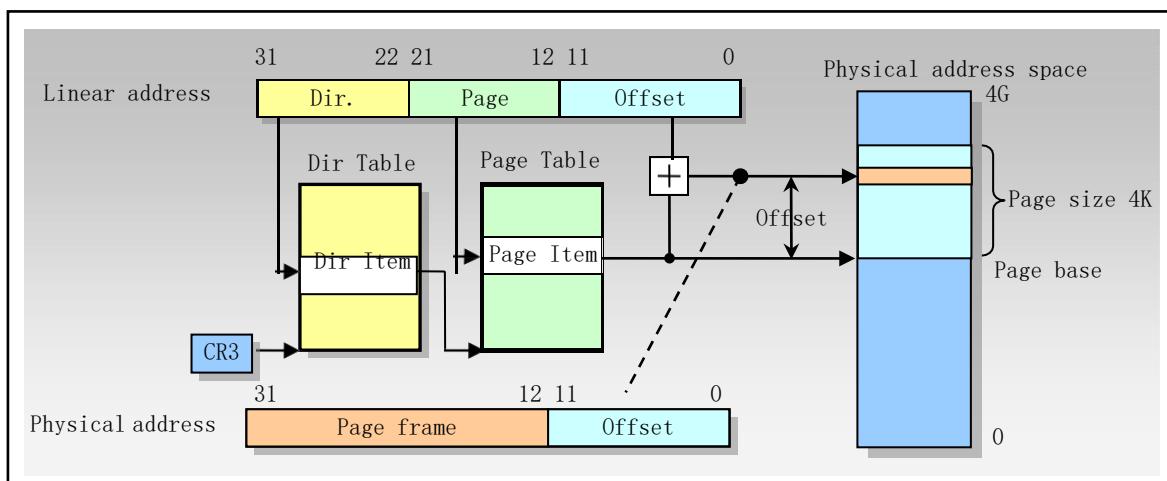


Figure 4-17 Linear Address Translation

#### 4.4.12 存在しないページテーブル

2階層のテーブル構造を採用することで、ページテーブルを連続した4MBのメモリブロックに格納することなく、メモリのページ間に分散させることができます。また、リニアアドレス空間に存在しない部分や未使用の部分に2次ページテーブルを割り当てる必要がないのです。ディレクトリページは常に物理メモリ上に存在しなければならないが、2次ページテーブルは必要に応じて再配置することができる。これにより、ページテーブル構造のサイズは、リニアアドレス空間のサイズの実際の使用に対応することになる。

ページ・ディレクトリ・テーブルの各テーブル・エントリは、ページ・テーブルのテーブル・エントリと同様に、存在属性も持っています。ページ・ディレクトリ・エントリのpresence属性は、対応するセカンダリ・ページ・テーブルが存在するかどうかを示す。ディレクトリエントリが、対応するセカンダリページテーブルが存在することを示している場合、セカンダリテーブルにアクセスするこ

とにより、テーブルルックアップ処理の第2ステップが上述のように継続される。対応する二次テーブルが存在しないことを示すビットがある場合、プロセッサは例外を生成してオペレーティングシステムに通知する。ページディレクトリエントリの存在属性により、オペレーティングシステムは、実際に使用されるリニアアドレス範囲に基づいて二次ページテーブルページを割り当てることができる。

ページディレクトリエントリのプレゼンスビットは、2次ページテーブルを仮想メモリに格納するためにも使用できます。これにより、二次ページテーブルの一部だけを物理メモリに格納し、残りはディスクに格納することができます。物理メモリ上のページテーブルに対応するページディレクトリエントリには、ページングが可能であることを示すために「存在」のマークが付けられます。ディスク上のページテーブルに対応するページディレクトリエントリは、存在しないとマークされます。二次ページテーブルが存在しないことによる例外は、ディスクから物理メモリに不足しているページテーブルをロードするようにオペレーティングシステムに通知します。ページテーブルを仮想メモリに保存することで、ページング変換テーブルの保存に必要な物理メモリの量を減らすことができます。

#### 4.4.2 ページ-ディレクトリとページ-テーブルのエントリ

ページディレクトリエントリとページテーブルエントリのフォーマットを図4-18に示します。31～12ビットは、物理アドレスの上位20ビットで、物理アドレス空間におけるページ（ページフレームとも呼ばれる）の物理ベースアドレスを特定するために使用されます。テーブルエントリの下位12ビットには、ページ属性情報が含まれています。存在属性についてはすでに説明しました。ここでは、残りの属性の機能と用途について簡単に説明します。

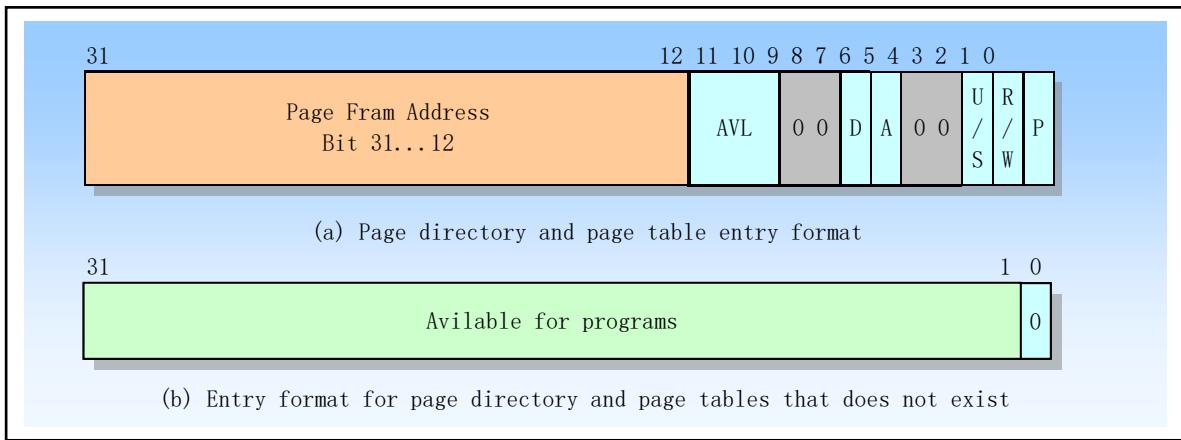


Figure 4-18 Page directory and page table entry format

### ■ P

ビット0はPresentフラグです。テーブルエントリが指示するページまたはページテーブルが、現在物理メモリにロードされているかどうかを示します。フラグがセットされると、そのページが物理メモリにあることを示し、アドレス変換を行います。フラグがクリアされると、そのページが物理メモリに存在しないことを意味します。プロセッサがそのページにアクセスしようとするとき、ページフォルト例外が発生します。この時点で、オペレーティングシステムはエントリの残りの部分を使用して、ディスクシステム内のページの位置などの情報を保存することができます。

### ■ R/W

ビット1は、Read/Writeフラグです。1に設定されている場合、そのページが読み取り、書き込み、または実行可能であることを意味します。0の場合、そのページは読み取り専用または実行可能です。R/Wビットは、プロセッサがスーパーユーザー特権レベル（レベル0、1または2）で実行されている場合には影響がありません。後述のU/Sフラグを参照してください。ページディレクトリエントリのR/Wビットは、それがマップするすべてのページに作用する。

### ■ U/S

ビット2はUser/Supervisorフラグです。1に設定されている場合、どのような特権レベルで実行されているプログラムでも、そのページにアクセスできます。0の場合、そのページは、スーパーユーザーの特権レベル（0、1、2）で実行されているプログラムのみがアクセスできます。ページディレクトリエントリのU/Sビットは、それがマッピングされているすべてのページに作用します。

### ■ A

ビット5はアクセス済みフラグです。ページテーブルエントリのこのフラグは、プロセッサがそのページテーブルエントリによってマッピングされたページにアクセスしたときに1に設定される。ページディレクトリエントリのこのフラグは、プロセッサがページディレクトリエントリによってマッピングされた任意のページにアクセスしたときに1に設定される。プロセッサはこのフラグを設定することにのみ責任があり、オペレーティングシステムは定期的にフラグをリセットすることで、ページの使用状況をカウントすることができます。

### ■ D

ビット6はページモディファイド(ダーティ)フラグ。プロセッサがページに書き込み操作を行うと、ページテーブルエントリに対応するDフラグがセットされます。プロセッサは、ページディレクトリエントリのDフラグを変更しません。

## ■ AVL

利用可能なフィールドです。このフィールドはプログラム用に予約されています。プロセッサがこれらのビットを変更することはありませんし、将来のアップグレード・プロセッサも同様です。

### 4.4.3 バーチャルメモリー

ページディレクトリおよびページテーブルのエントリにフラグPが存在することで、ページング技術を用いた仮想ストレージに必要なサポートが提供されます。リニアアドレス空間のページが物理メモリに存在する場合、対応するエントリにフラグP=1が設定され、対応する物理アドレスがエントリに含まれます。ページが物理メモリに存在しないテーブルは、そのフラグP=0となります。プログラムが物理メモリに存在しないページにアクセスした場合、プロセッサはページフォルト例外を生成します。このとき、オペレーティングシステムは、この例外処理プロセスを利用して、欠落しているページをディスクから物理メモリに転送し、対応する物理アドレスをテーブルのエントリに格納することができます。最後に、リターンプログラムが例外を引き起こした命令を再実行する前に、フラグP=1が設定される。

アクセスされたフラグAと修正されたフラグDは、仮想メモリ技術を効果的に実装するために使用することができます。すべてのAフラグを定期的にチェックしてリセットすることで、オペレーティングシステムは最近アクセスされていないページを判断することができます。これらのページは、ディスクに削除する候補となります。あるページがディスクからメモリに読み込まれたとき、そのダーティフラグD=0だったとすると、そのページが再びディスクに移されたとき、Dフラグがまだ0であれば、そのページはディスクに書き込む必要がない。この時にD=1であれば、ページの内容が変更されているので、そのページをディスクに書き込まなければなりません。

## 4.5 保護

プロテクトモードでは、80X86はセグメントおよびページレベルの保護機能を備えています。この保護機構は、特権レベル（4レベルの保護とレベル2のページ保護）に基づいて、特定のセグメントとページにアクセス制限を行います。例えば、オペレーティングシステムのコードやデータは、通常のアプリケーションよりも高い特権レベルのセグメントに格納されています。そして、プロセッサの保護機構は、アプリケーションがオペレーティングシステムのコードやデータにアクセスすることを、制御・規制して制限します。

信頼性の高いマルチタスク環境を実現するためには、保護メカニズムが必要です。個々のタスクを相互干渉から保護するために使用することができます。セグメントおよびページレベルの保護は、ソフトウェア開発のどの段階でも使用でき、設計上の問題やエラーの発見・検出を支援します。プログラムがエラーメモリ空間への望ましくない参照を実行した場合、保護メカニズムはそのような操作をブロックし、そのようなイベントを報告することができます。

保護機構としては、セグメント化やページング機構などがあります。プロセッサレジスタの2ビットは、現在実行中のプログラムの特権レベルを定義し、これをCurrent Privilege Level (CPL)と呼びます。セグメント化とページングのアドレス変換時に、プロセッサはCPLを検証します。

コントロールレジスタCR0のPEフラグ（ビット0）をセットすることで、プロセッサをプロテクトモードで動作させることができます。セグメンテーション保護機構をオンにすることができます。プロテクトモードに入ると、プロセッサには保護機構を停止または有効にするための明確な制御フラグはあ

りません。ただし、すべてのセグメント・セレクタとセグメント・ディスクリプタの特権レベルをレベル

0.この方法では、セグメント間の特権レベルの保護バリアを禁止することができますが、他のセグメント長やセグメントタイプのチェック、その他の保護メカニズムはまだ機能します。

コントロールレジスタCR0のPGフラグ（ビット31）をセットすると、ページング機構が有効になります。ページング保護も有効になります。同様に、ページングオープン状態でページレベル保護機構を無効化または有効化するための関連フラグはプロセッサにありません。しかし、各ページディレクトリエントリとページテーブルエントリにリード/ライト（R/W）フラグとユーザー/スーパーユーザー（U/S）フラグを設定することで、ページレベルの保護を無効にすることができます。この2つのフラグを設定することで、各ページを任意に読み書きできるようになり、実際にはページレベルの保護が無効になります。

セグメント・レベルの保護では、プロセッサはセグメント・レジスタのセレクタ（RPLおよびCPL）とセグメント・ディスクリプタのフィールドを使って保護検証を行います。ページング・メカニズムでは、ページ・ディレクトリおよびページ・テーブル・エントリのR/WおよびU/Sフラグが主に保護動作を実行するために使用されます。

## 4.5.1 セグメント保護

保護機構を使用する場合、各メモリ参照をチェックして、そのメモリ参照がさまざまな保護要件を満たしているかどうかを確認します。このチェック作業はアドレス変換と同時に行われるため、プロセッサのパフォーマンスに影響はありません。実行される保護チェックは、以下のカテゴリーに分けられます。

- セグメントリミットチェック
- セグメントタイプのチェック
- 特権レベルのチェック
- アドレス可能なドメインの制限
- プロシージャのエントリー・ポイントの制限
- 命令セットの制限。

プロテクトに違反すると、すべて例外が発生します。以下のセクションでは、プロテクトモードでの保護メカニズムについて説明します。

### 4.5.1.1 セグメント長リミットチェック

セグメント記述子のセグメント制限長フィールドは、プログラムやプロセスがセグメント外の場所にアドレッシングするのを防ぐために使用されます。セグメント長の有効値は、粒度Gフラグの設定状態に依存します。データ・セグメントの場合、セグメント長はフラグE（拡張方向）とフラグB（デフォルトのスタック・ポインタのサイズおよび上限）にも関係します。E

フラグは、データ・セグメント・タイプのセグメント記述子のタイプ・フィールドのビットです。

Gフラグがクリアされている場合（バイトグラニュラリティ）、有効なセグメント長は、20ビットのセグメント記述子の長さフィールドLimitの値となります。この場合、Limitは0から0xFFFFFFF（1MB）の範囲となります。Gフラグが設定されている場合（4KBページ・グラニュラリティ）、プロセッサはLimitフィールドの値に4Kの係数をかけます。この場合、有効なLimitの範囲は0xFFFFFFFから0xFFFFFFFF（4GB）となります。Gフラグが設定されている場合、セグメント・オフセット（アドレス）の下位12ビットはLimitと照合されないことに注意してください。例えば、セグメント長のLimitが0の場合、0～0xF

FFのオフセット値は有効です。

エクスパンデッド・データ・セグメントを除き、他のセグメント・タイプの有効範囲の値は、セグメント内でアクセスが許可されている最後のアドレスで、セグメント長よりも1バイト小さい値となります。セグメント長のフィールドを超えて有効なアドレス範囲を指定すると、一般的な保護例外が発生します。

エクスパンデッドダウンデータセグメントでは、セグメント長は同じ機能を持っていますが、その意味が異なります。ここでは、セグメント長はセグメント内のアクセスできない最後のアドレスを指定するので、Bフラグがセットされている場合、有効なオフセット値の範囲は（有効なセグメントオフセット+1）から0xFFFF

FFFFまでとなり、Bがクリアされている場合、有効なオフセット値の範囲は（有効なセグメントオフセット+1）から0xFFFFまでとなります。次の拡張セグメントのセグメント長が0の場合、そのセグメントは最大の長さになります。

セグメントの長さのチェックに加えて、プロセッサはディスクリプターテーブルの長さもチェックします。GDTR、IDTR、LDTRの各レジスタには、16ビットの限界値が含まれており、プログラムが記述子テーブルの外の記述子を選択するのを防ぐためにプロセッサが使用します。記述子テーブルの限界長値は、テーブル内の最後の有効バイトを示します。各記述子は8バイト長なので、N個の記述子エントリを含むテーブルは、 $8N-1$ の制限値を持つべきである。

セレクタの値はゼロでもよい。このようなセレクタは、GDTテーブルの最初の未使用ディスクリプタ項目を指します。このヌルのセレクタはセグメント・レジスタにロードできますが、このディスクリプタを使ってメモリを参照しようとすると、一般保護例外が発生します。

## 4.5.1.2 セグメントタイプチェック

セグメントディスクリプターには、ディスクリプターのSフラグとタイプフィールドのTYPEの2箇所にタイプ情報が含まれています。プロセッサはこの情報を使って、セグメントやゲートの不正使用によるプログラミング・エラーを検出します。

Sフラグは、記述子がシステムタイプかコードタイプかデータタイプかを示すために使用されます。TYPEフィールドには、コード、データ、システムの各タイプの記述子を定義するための4ビットが追加されています。前節の表は、コードおよびデータ記述子のTYPEフィールドのエンコーディングを示し、もう一つの表は、システム記述子のTYPEフィールドのエンコーディングを示しています。

セグメントセレクタやディスクリプタが操作されると、プロセッサはいつでもタイプ情報をチェックします。タイプ情報がチェックされるのは、主に次の2つのケースです。

1. セグメント・セレクタがセグメント・レジスタにロードされたとき。特定のセグメント・レジスタは、例えば、特定のディスクリプター・タイプのみを含むことができます。
  - CSレジスタは、実行コードセグメントのセレクタでのみロードできます。
  - 読めない実行可能セグメントのセレクタをデータセグメントレジスタにロードできない。
  - SSレジスタにロードできるのは、書き込み可能なデータセグメントのセレクタのみです。
2. セグメント・レジスタに記述子がすでにロードされているセグメントに命令がアクセスする場合。例えば、特定のセグメントは、あらかじめ定義された特定の方法でのみ命令によって使用することができます。
  - 実行可能なセグメントを書ける命令はありません。
  - 書き込み可能ビットが設定されていないデータセグメントには、どのような命令も書き込むことはできません。

- 実行可能フラグが設定されていない限り、どの命令も実行可能セグメントを読み取ることはできません。

### 4.5.13 特権レベル

プロセッサのセグメント保護機構は、0~3段階の4つの特権レベル（または特権層）を識別できます。数字が大きいほど、特権は少なくなります。図4-

19は、これらの特権レベルを保護リングの形態として解釈したものです。中央のリング（最先端のコード、データ、スタックを保持）は、最も重要なソフトウェアを含むセグメントに使用され、通常はオペレーティングシステムのコア部分に使用されます。中央の2つのリングは、より重要なソフトウェアに使用されます。2つの特権レベルのみを使用するシステムでは、特権レベル0と3を使用する必要があります。

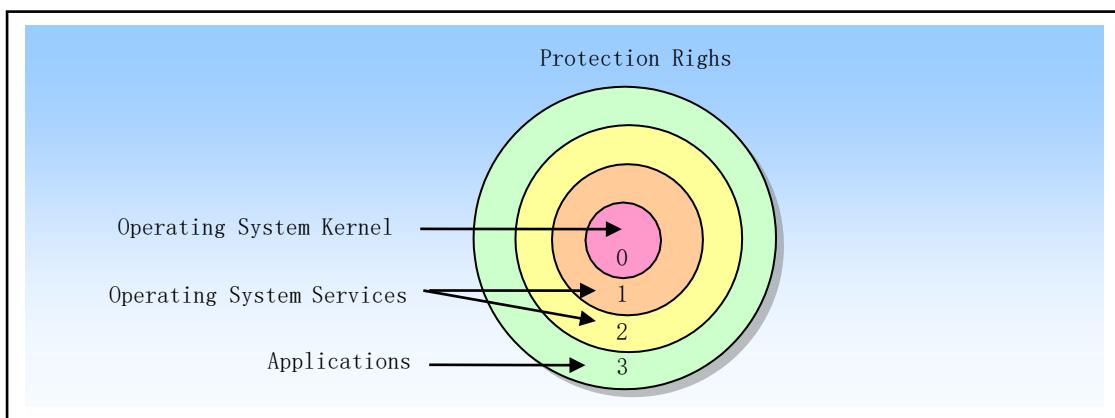


Figure 4-19 Protection Level Rings

プロセッサは特権レベルを利用して、制御された条件下でない限り、低い特権レベルで実行されているプログラムやタスクが高い特権レベルのセグメントにアクセスできないようにしています。プロセッサは、特権レベルに違反する操作を検出すると、一般保護例外を生成します。

個々のコードセグメントとデータセグメントの間で特権レベルのチェックを行うために、プロセッサは以下の3種類の特権レベルを認識することができます。

#### ■ Current

#### Privilege

**Level (CPL) の略。** CPLは、現在実行中のプログラムやタスクの特権レベルです。CPLはCSとSSセグメントレジスタのビット0と1に格納されています。通常、CPLは命令をフェッチしているコードセグメントの特権レベルと同じです。プログラムの制御が異なる特権レベルのコードセグメントに移されると、プロセッサはCPLを変更します。適合するコードセグメントにアクセスする場合は、CPL

の扱いが若干異なります。適合するコード・セグメントは、適合するコード・セグメントのDPLと同じか、それよりも数値的に大きい（少ない）特権レベルからアクセスすることができます。また、プロセッサがCPLと異なる特権レベルを持つ適合コードセグメントにアクセスしても、CPLは変更されません。

#### ■ Descriptor

#### Privilege

#### Level

#### (DPL)

**の略。** DPLは、セグメントまたはゲートの特権レベルです。セグメントやゲートの記述子のDPLフィールドに格納されています。現在実行中の

コード・セグメントがセグメントまたはゲートにアクセスしようとすると、セグメントまたはゲートのDPLが、（このセクションで後述する）セグメントまたはゲート・セレクタのCPLおよびRPLと比較されます。DPLは、アクセスするセグメントまたはゲートのタイプによって、異なる解釈がなされます。

#### ◆ データセグメント。DPL

は、プログラムやタスクがそのセグメントへのアクセスを許可されるために必要な最高の特権レベルを示します。例えば、データセグメントのDPLが1の場合、CPLが0または1のプログラムのみがそのセグメントにアクセスできます。

#### ◆ 不適合コードセグメント（コールゲートを使用しない場合）。DPLは、プログラムやタスクがセグメントにアクセスするために必要な特権レベルを示します。例えば、不適合コード・セグメントのDPLが0であれば、CPL 0で実行されているプログラムのみがこのセグメントにアクセスできます。

#### ◆ コールゲート。そのDPLは、コールゲートにアクセスしている現在の実行プログラムやタスクが可能な、数値的に最も高い特権レベルを示します。（これは、データセグメントのアクセスルールと同じです）。

#### ◆ コールゲートでアクセスされる適合コードセグメントと不適合コードセグメント。DPLは、プログラムやタスクがセグメントへのアクセスを許可されるために必要な、数値的に最も低い特権レベルを示します。例えば、適合コード・セグメントのDPLが2の場合、CPLが0または1で動作するプログラムはそのセグメントにアクセスできません。

#### ◆ タスクステータスセグメント

**TSS。** そのDPLは、TSSにアクセスしている現在の実行プログラムまたはタスクが可能な、番号的に最も高い特権レベルを示します。（これは、データセグメントのアクセスルールと同じです）。

### ■ リクエスト・プリビレッジ・レベル

**RPL。RPL**

はセグメント・セレクタに割り当てられたオーバーライド・プリビレッジ・レベルで、セレクタのビット 0 と 1

に格納されています。プロセッサはRPLとCPLの両方をチェックして、セグメントへのアクセスが許可されているかどうかを判断します。プログラムやタスクがセグメントにアクセスするのに十分な特権レベル（CPL）を持っていても、提供されたRPL特権レベルが不十分な場合、アクセスは拒否されます。つまり、セグメントセレクタのRPLがCPLよりも大きな値を持つ場合、RPLがCPLを上書きし（比較をチェックする際の特権レベルとしてRPLを使用する）、その逆も同様です。つまり、セグメントにアクセスする際には、RPL と CPL の値が最大の特権レベルが常に比較対象として扱われます。したがって、RPL を使用すると、アプリケーション自身がセグメントにアクセスしていない限り、高い特権を持つコードがアプリケーションに代わってセグメントにアクセスしないようにすることができます。

特権レベルチェック動作は、セグメント記述子のセグメント・セレクタがセグメント・レジスターにロードされたときに実行されますが、データ・アクセスのチェック方法は、コード・セグメント間のプログラム制御の転送をチェックする方法とは異なります。そのため、以下の2つのアクセス状況が考えられます。

### 4.5.2 データセグメントへのアクセス時の特権レベルチェック

データ・セグメントのオペランドにアクセスするには、データ・セグメントのセグメント・セレクタをデータ・セグメント・レジスタ (DS、ES、FS、GS) またはスタック・セグメント・レジスタ (SS) にロードする必要があります (セグメント・レジスタは、MOV、POP、LDS、LES、LFS、LGS、LSS命令でロードできます)。プロセッサはセグメント・セレクタをセグメント・レジスタにロードする前に、現在実行中のプログラムやタスクの特権レベル (CPL)、セグメント・セレクタのRPL、セグメントのセグメント記述子のDPLを比較して、特権チェックを行います (図4-

20を参照)。DPLがCPLとRPLの両方よりも数値的に大きいか等しい場合、プロセッサはセグメントセレクタをセグメントレジスタにロードします。それ以外の場合は、一般保護フォルトが生成され、セグメント・レジスタはロードされません。

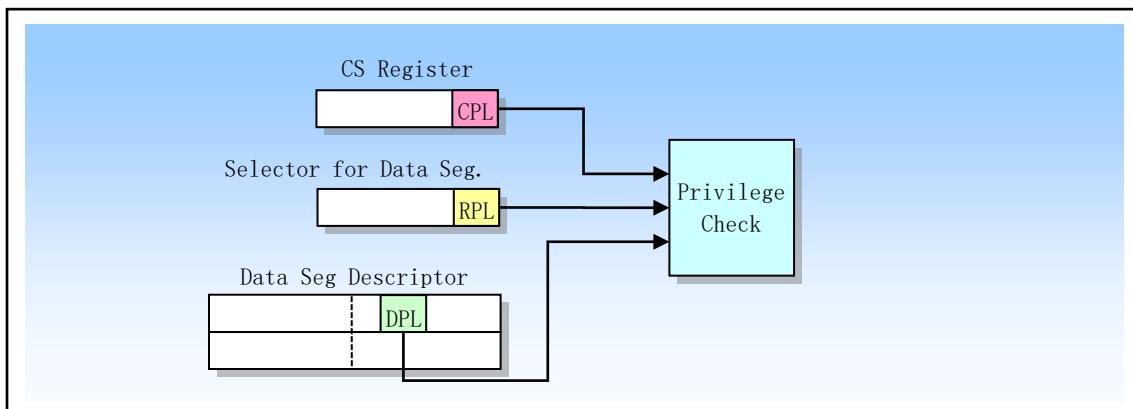


Figure 4-20 Privilege level check when accessing data segments

プログラムやタスクのアドレス可能領域は、CPLが変わると変化することがわかります。CPLが0のときは、この時点ですべての特権レベルのデータセグメントにアクセスでき、CPLが1のときは、特権レベル1～3のデータセグメントのみにアクセスでき、CPLが3のときは、特権レベル3のデータセグメントのみにアクセスできます。

また、コードとデータがROM化されている場合など、コードセグメントに含まれるデータ構造にアクセスすることが望ましい場合があります。そこで、時にはコードセグメント内のデータにアクセスする必要が出てきます。このとき、コードセグメント内のデータにアクセスするには、以下の方法があります。

1. 不適合で読み取り可能なコード・セグメントのセレクタをデータ・セグメント・レジスタにロードする。
2. 適合する読み取り可能なコード・セグメントのセレクタをデータ・セグメント・レジスタにロードします。
3. セレクタがすでにCSレジスタに入っている読み取り可能なコードセグメントを読み取るには、コードセグメントオーバーライドプレフィックス (CS) を使用します。

データ・セグメントへのアクセスに関する同じルールが方法1にも適用されます。方法2は、コード・セグメントのDPLにかかわらず、一貫したコード・セグメントの特権レベルがCPLと同等であるため、常に有効です。方法3も、CSレジスタで選択されたコード・セグメントのDPLがCPLと同じであるため、常に有効です。

また、スタックセグメントセレクタを使ってSSセグメントレジスタをロードする際にも、特権レ

ベルのチェックが行われます。ここでは、スタック・セグメントに関連するすべての特権レベルがCPLと一致する必要があります。つまり、CPL、スタック・セグメント・セレクタのRPL、スタック・セグメント・ディスクリプタのDPLのすべてが同じでなければなりません。RPL または DPL が CPL と異なる場合、プロセッサは一般保護例外を生成します。

### 4.5.3 プログラム制御を移す レベルチェック

際の特権

#### コードセグメント間

あるコード・セグメントから別のコード・セグメントにプログラム制御を移すには、対象となるコード・セグメントのセグメント・セレクタをコード・セグメント・レジスタ (CS) にロードする必要があります。このロード処理の一環として、プロセッサはターゲット・コード・セグメントのセグメント記述子を検出し、様々な制限、タイプ、および特権レベルのチェックを行います。これらのチェックに合格すると、ターゲット・コード・セグメント・セレクタがCSレジスタにロードされ、プログラムの制御が新しいコード・セグメントに移され、EIPレジスタが指す命令でプログラムの実行が開始されます。

プログラムの制御伝達は、JMP、RET、INT、IRETの各命令と、例外や割り込みの仕組みを使って実装される。例外と割り込みは、後述する特別な実装です。ここでは、JMP、CALL、RETSの各命令について説明します。JMPやCALL命令は

は、次の4つの方法で別のコードセグメントを参照することができます。

- ターゲット・オペランドには、ターゲット・コード・セグメントのセグメント・セレクタが含まれます。
- ターゲットオペランドは、ターゲットコードセグメントのセレクタを含むコールゲートディスクリプタを指します。
- ターゲットオペランドは、ターゲットコードセグメントのセレクタを含むTSSを指します。
- ターゲットオペランドは、ターゲットコードセグメントのセレクタを含むTSSを指すタスクゲートを指しています。

前者2つの参照タイプについては以下で説明し、後者2つの参照タイプについてはタスク管理のセクションで説明します。

#### 4.5.3.1 コードセグメントへのダイレクトコールまたはジャンプ

JMP、CALL、RET

命令の

near

フォームは、現在のコードセグメント内でプログラム制御の転送を行うだけなので、特権レベルのチェックは行われません。far形式のJMP、CALL、RET命令は、別のコードセグメントに制御を移すので、プロセッサは特権レベルのチェックを行う必要がある。

コールゲートを経由せずにプログラム制御を他のコードセグメントに移す場合、プロセッサは図4-21に示すように4種類の特権レベルとタイプの情報を確認します。

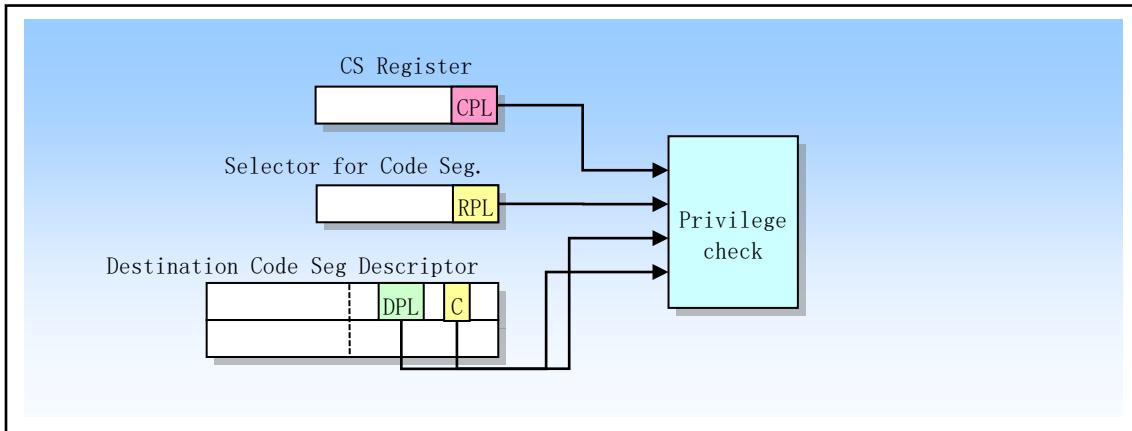


Figure 4-21 Privilege check when calling or jumping directly to another code segment

- 現在の特権レベルCPL。(ここで、CPLは呼び出しを実行するコードセグメントの特権レベル、つまり、呼び出しやジャンプを実行するコードセグメントの特権レベルです)
- 呼び出されたプロシージャを含むデスティネーション・コード・セグメント・ディスクリプターのディスクリプター・プリビレッジ・レベルDPLです。
- デスティネーションコードセグメントのセグメントセレクタで特権レベルRPLを要求する。
- デスティネーションコードセグメントディスクリプターのコンフォーミングフラグCです。コード・セグメントが非適合コード・セグメントであるか、整合性のあるコード・セグメントであるかを判断します。

プロセッサがCPL、RPL、およびDPLをチェックするルールは、フラグCの設定状態に依存します。不適合コード・セグメントにアクセスする場合(C=0)、呼び出し元(プログラム)のCPLは、宛先コード・セグメントのDPLと等しくなければならず、そうでない場合は一般保護例外が発生します。適合しないコード・セグメントを指すセグメント・セレクタのRPLは、チェックに限られた影響しか与えません。制御転送が正常に完了するためには、RPLは呼び出し側のCPL以下の数値でなければなりません。不適合コード・セグメントのセグメント・セレクタがCSレジスタにロードされても、特権レベル・フィールドは変更されず、すなわち呼び出し側のCPLのままでです。これは、セグメント・セレクタのRPLがCPLと異なっていても同様です。

#### 適合するコード・セグメント(C = 1)

1)にアクセスする場合、呼び出し側のCPLは、デスティネーション・コード・セグメントのDPLよりも数値的に大きくても小さくても構いません。プロセッサは、CPL < DPL の場合にのみ一般保護例外を生成します。適合するコード

セグメントへのアクセスでは、プロセッサは RPL のチェックを無視します。適合するコードセグメントの場合、DPL は呼び出し元がコードセグメントへの呼び出しを成功させることができる、数値的に最も低い特権レベルを表します。

プログラム制御が適合するコード・セグメントに移されたとき、デスティネーション・コード・セグメントのDPLがCPLよりも数値的に小さい場合でも、CPLは変更されません。これは、CPLが現在のコード・セグメントのDPLと同じでない場合がある唯一のケースです。また、CPLが変化していないので、スタックが切り替わることもありません。

ほとんどのコード・セグメントは非適合コード・セグメントです。これらのセグメントでは、P

ログラムの制御は、以下に説明するようにコールゲートを介した転送でない限り、同じ特権レベルのコードセグメントにしか転送できません。

### 4.5.2 ゲートディスクリプター

異なる権限レベルのコードセグメントへのアクセスを制御するために、プロセッサはゲートディスクリプタと呼ばれる特別なディスクリプタのセットを提供しています。ゲートディスクリプターには4つの種類があります。

- コールゲート (TYPE=12)。
- トラップゲート (TYPE=15)。
- 割り込みゲート (TYPE=14)。
- タスクゲート (TYPE=5)。

タスクゲートは、タスクの切り替えに使用され、後に「タスク管理」の項で説明します。トラップゲートとインタラプトゲートは、コールゲートのための特別なクラスで、次のセクションで説明するように、例外や割り込みのハンドラを呼び出すために使われます。このセクションでは、コールゲートの使い方のみを説明します。

コールゲートは、異なる特権レベル間で制御されたプログラム制御の転送を実現するために使用されます。コールゲートは通常、特権レベルの保護メカニズムを使用するオペレーティングシステムでのみ使用されます。図4-

22にコールゲート記述子のフォーマットを示します。コールゲート記述子は、GDTまたはLDTに格納できますが、割り込み記述子テーブルIDTには配置できません。コールゲートの主な機能は次のとおりです。

- アクセスするコードセグメントを指定します。
- 指定されたコードセグメント内のプロシージャ（プログラム）のエントリポイントを定義します。
- アクセスプロシージャの呼び出し側が必要とする特権レベルを指定します。
- スタック切り替えが発生した場合、スタック間でコピーする必要のあるオプションパラメータの数を指定します。
- コールゲート記述子が有効であるかどうかを示す。

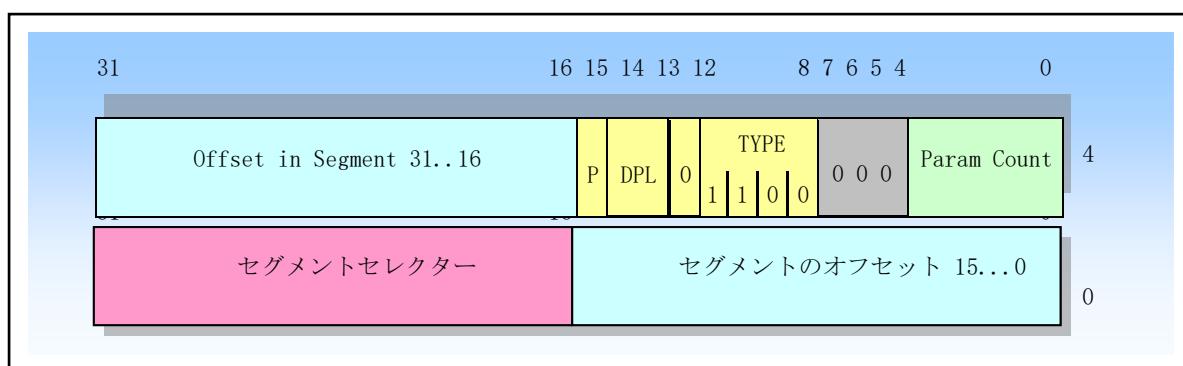


Figure 4-22 Call gate descriptor format

コールゲートのセグメント・セレクタ・フィールドでは、アクセスするコード・セグメントを指定します。オフセット値フィールドでは、セグメント内のエントリ・ポイントを指定します。このエントリ・ポイントは通常、指定されたプロセスの最初の命令です。DPLフィールドは、コールゲートの特権レベルを指定し、コールゲートを介して特定のプロシージャにアクセスするために必要な特権レベルを指定する。フラグPは、コールゲート記述子が有効であるかどうかを示す。パラメーター・カウント・フィールド (Param

Count) は、スタック・スイッチが発生したときに、呼び出し元のスタックから新しいスタックにコピーされたパラメーターの数を示します。

コールゲートは、Linuxカーネルでは使用されていません。コールゲートの説明は、次節の割込みや例外ゲートの処理に備えるためのものです。

#### 4.5.3.3 コールゲートからコードセグメントにアクセスする

コールゲートにアクセスするためには、CALLやJMP命令のオペランドのfarポインタを用意する必要があります。このポインタのセグメントセレクタは、コールゲートを指定するために使用されます。ポインタのオフセット値が必要ですが、プロセッサはこれを使用しません。このオフセット値は、任意の値に設定できます。図4-23を参照してください。

プロセッサがコールゲートにアクセスすると、コールゲート内のセグメントセレクタを使用して、宛先コードセグメントのセグメントディスクリプタを探します。次に、コード・セグメント記述子のベース・アドレスとコール・ゲートのオフセット値を組み合わせて、コード・セグメント内の指定されたプログラム・エントリ・ポイントのリニア・アドレスを形成します。

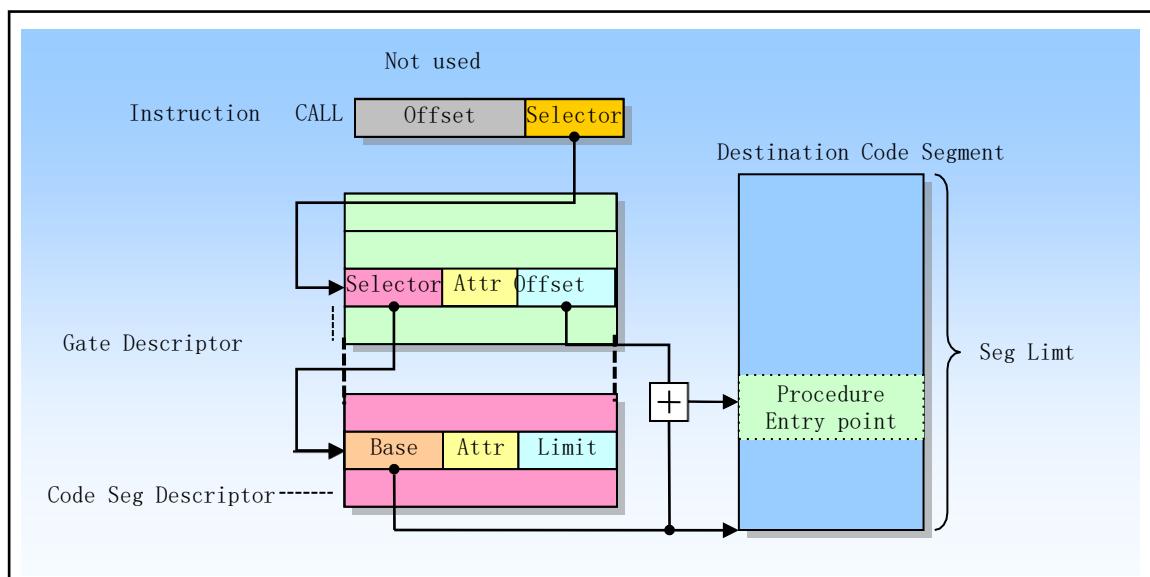


Figure 4-23 Call-gate operation process

コールゲートによってプログラムの制御権が移ると、CPUは図4-24のように4つの異なる特権レベルをチェックして制御権移譲の有効性を判断します。

- 現在の特権レベルCPLです。
- リクエスト者の権限レベル コールゲートのセレクタのRPL。
- コールゲートディスクリプターのディスクリプター特権レベルDPL。
- デスティネーションコードセグメントのセグメントディスクリプターのDPLです。

また、デスティネーションコードセグメント記述子の適合性フラグCもチェックされます。

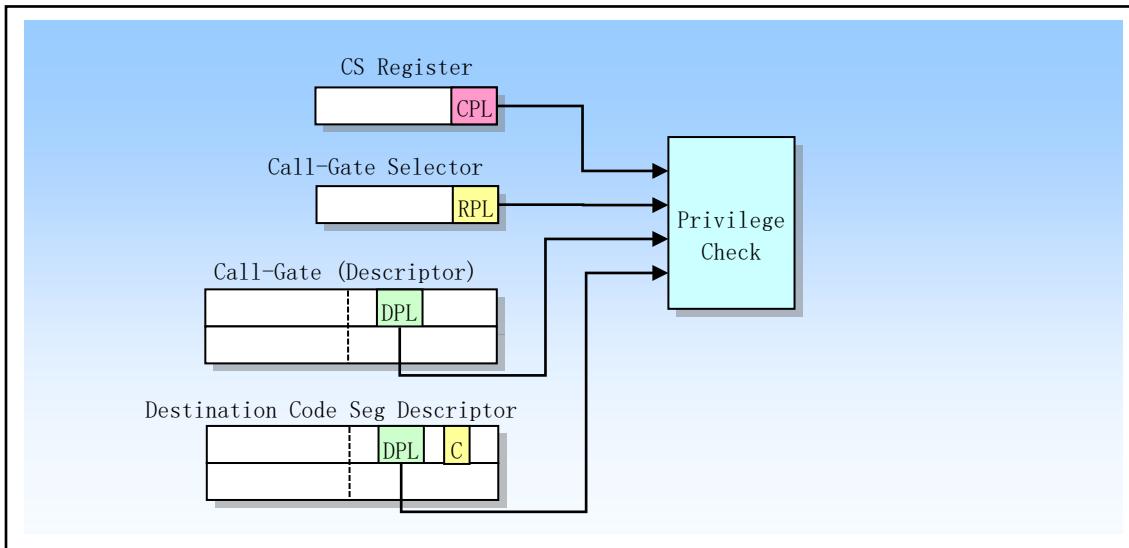


Figure 4-24 Privilege level check for control transfer with call-gate

表 4-5 に示すように、CALL 命令と JMP 命令

命令による制御転送では、特権レベルのチェックルールが異なる。コールゲートディスクリプタのDPLフィールドは、呼び出し側がコールゲートにアクセスできる最大の特権レベル（最低特権レベル）を数値で示す。つまり、コール・ゲートにアクセスするためには、呼び出し側プログラムの特権レベルCPLがコール・ゲートのDPL以下である必要があります。呼び出しゲートのセグメントセレクタのRPLも、これを起動するCPLと同じルールに従う必要があります。

Table 4-5 Privilege level check rules for CALL and JMP instructions

Instruction	Privilege Check Rules (numerically)
CALL	CPL<= Call gate DPL; RPL<= Call gate DPL Destination conforming & nonconforming code segments DPL<= CPL
JMP	CPL<= Call gate DPL; RPL<= Call gate DPL Destination conforming code segment DPL<= CPL; Destination nonconforming code segment DPL=CPL

呼び出し元とコールゲートの間の特権レベルチェックが成功すると、CPUは次に呼び出し元のCPLとコードセグメント記述子のDPLを比較する。この点で、CALL命令とJMP命令のチェックルールは異なる。CALL命令のみ、コールゲートを使用して、より特権的な（数値的に低い特権レベルの）不適合コードセグメントにプログラム制御を移すことができる、つまり、CPLよりも小さいDPLを持つ不適合コードセグメントに移すことができる。JMP命令は、CPLと等しいDPLを持つ不適合コード・セグメントにプログラム制御を移すためにのみ、コール・ゲートを使用することができる。ただし、CALL命令とJMP命令の両方とも、より高い特権レベルの適合コード・セグメント、つまりDPLがCPL以下の数値である適合コード・セグメントに制御を移すことができる。

コールがより高い特権レベルの非適合コード・セグメントに制御を移す場合、CPLは宛先コード・セグメントのDPL値に設定され、スタック・スイッチを引き起こします。しかし、コールやジャンプが

より高い特権レベルの適合コード・セグメントに制御を移す場合、CPLは変化せず、スタック・スイッチの原因とはなりません。

コールゲートは、コードセグメント内のプロシージャを、異なる特権レベルのプログラムがアクセスできるようにするものです。例えば、コードセグメントに配置されたオペレーティングシステムのコードは、オペレーティングシステム自身や

アプリケーションソフトがアクセスを許可しているコード（キャラクターI/Oを処理するコードなど）。このように、すべての特権レベルのコードがアクセスできるように、これらすべてのプロシージャにコールゲートを設定することができます。さらに、より高い特権レベルのコールゲートを、オペレーティングシステムでのみ使用されるコード専用に設定することもできます。

#### 4.5.3.4 スタックスイッチング

コールゲートを使用して、より特権的な不適合コードセグメントにプログラム制御を移すと、CPUは自動的に目的のコードセグメントの特権レベルのスタックに切り替わります。スタック切り替え動作の目的は、より特権的なプログラムがスタック容量不足でクラッシュするのを防ぐことと、低特権レベルのプログラムが共有スタックを介して意図的または非意図的に高特権レベルのプログラムを妨害するのを防ぐことがあります。

各タスクは最大4つのスタックを定義する必要があります。1つは特権レベル3で動作するアプリケーションコード用、もう1つは特権レベル2、1、0にそれぞれ使用されます。システム内で特権レベル3と0の2つだけを使用する場合は、各タスクには2つのスタックだけを設定する必要があります。各スタックは異なるセグメントにあり、セグメントセレクタとセグメント内のオフセット値を使って指定します。

特権レベル3のプログラムの実行時には、特権レベル3のスタックのセグメントセレクタとスタックポインタがそれぞれSSとESPに格納されており、スタックスイッチが発生すると呼び出されたプロシージャのスタックに保存されます。

特権レベル0、1、2のスタックの初期ポインタ値は、現在実行中のタスクのTSSセグメントに格納されています。TSSセグメント内のこれらのポインタは、読み取り専用の値です。タスクの実行中にCPUがこれらを変更することはありません。上位の特権レベルのプログラムが呼び出されると、CPUはこれらを使って新しいスタックを構築します。呼び出したプロシージャから戻るときには、対応するスタックは存在しません。次にプロシージャが呼ばれたとき、TSSの初期ポインタ値を使って再び新しいスタックが作られます。

オペレーティングシステムは、使用されるすべての特権レベルのスタックとスタックセグメント記述子を確立し、タスクのTSSに初期ポインタ値を設定する責任があります。各スタックは、読み取りと書き込みが可能で、以下の情報の一部を保持するのに十分なスペースが必要です。

- 呼び出したプロセスのSS、ESP、CS、EIPレジスタの内容。
- 呼び出されたプロシージャのパラメータと、一時的な変数のために必要なスペース。
- EFLAGSレジスタとエラーコードは、例外ハンドラや割込みハンドラを暗黙的に呼び出す場合に使用します。

1つのプロシージャが他のプロシージャを呼び出すことができ、オペレーティングシステムは複数の割り込みのネストをサポートすることができるので、各スタックは上記の情報の複数のフレームを収容するのに十分なスペースを持っていなければなりません。

ゲートへの呼び出しによって特権レベルが変更されると、CPUは以下の手順でスタックを切り替え、呼び出されたプロシージャを新しい特権レベルで実行し始めます（図4-25参照）。

1. デスティネーション・コード・セグメントのDPL（つまり新しいCPL）を使って、TSSから新しいスタックへのポインタを選択します。新しいスタックのセグメント・セレクタとスタック・ポインタは、現在のTSSから読み込まれます。セグメントバウンダリに違反するエラーが発生した場合、スタックセグメントセレクタ、スタックポインタ、スタックセグメントディスクリプタの読み取り処理中に、無効なTSS例外が発生します。
2. スタックセグメント記述子の特権レベルとタイプが有効かどうかをチェックします。無効な場合は、無効なTSSの例外も発生します。
3. SSレジスタとESPレジスタの現在の値を一時的に保存し、新しいスタックのセグメントセレクタとスタックポインタをSSとESPにロードします。そして、一時保存したSSとESPの内容を新しいスタックにプッシュします。
4. コールゲート記述子の中の指定された数のパラメータを、呼び出し元のプロシージャのスタックから新しいスタックにコピーします。コールゲート内のパラメータの値は31までです。0の場合は、パラメータがないことを意味し、コピーは必要ありません。
5. リターン命令ポインタ（つまり現在のCSとEIPの内容）を新しいスタックにプッシュします。新しい（デスティネーション）コードセグメントセレクタがCSにロードされ、コールゲートのオフセット値（新規命令ポインタ）がEIPにロードされます。そして、呼び出されたプロセスの実行が開始されます。

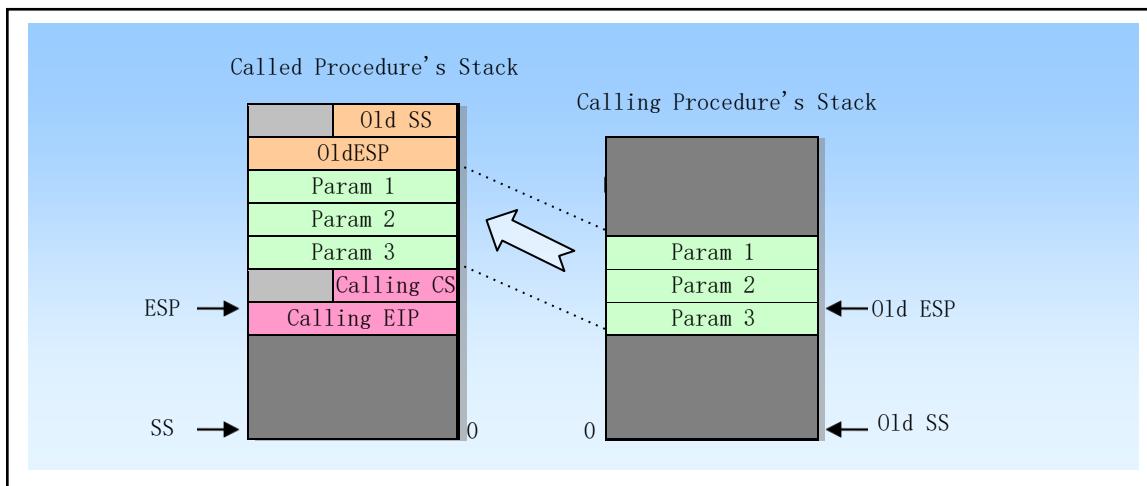


Figure 4-25 Stack switch when calling between different privilege levels

### 4.5.3.5 呼び出されたプロシージャからの復帰

RET 命令は near return、far return with privilege level、far return with different privilege level を実行するために使用されます。この命令は、CALL

命令で呼び出されたプロシージャから戻るために使用されます。ニアリターンでは、現在のコードセグメント内のプログラム制御を移すだけなので、CPUは境界チェックのみを行います。同じ権限レベルのファーリターンの場合、CPUはリターンコードセグメントのセレクタとリターン命令ポインタを同時にスタックからポップします。これらの2つのポインタは、通常CALL命令によってスタックにプッシュされるため、これによって有効となります。ただし、現在のプロセスがポインタの値を変更する可能性がある場合や、スタックに問題がある場合に対処するため、CPUは依然として特権レベルのチェックを行います。

クを行います。

特権レベルの変更となるファーリターンは、低特権レベルのプログラムに戻ることだけが許されます。すなわち、返されたコードセグメントDPLがCPLよりも数値的に大きい場合です。CPUはCSレジスタのセレクタのRPLフィールドを使用して、低特権レベルが必要かどうかを判断します。RPLの値がCPLよりも大きい場合、特権レベル間のリターン操作が実行されます。実行が呼び出したプロセスにマークに戻ると、CPUは以下のステップを実行します。

1. 保存されたCSレジスタのRPLフィールド値を確認し、復帰時に特権レベルを変更する必要があるかどうかを判断します。
2. 呼び出されたプロシージャ・スタック上の値を使用してCSレジスタとEIPレジスタをポップアップしてロードします。このとき、コード・セグメント・ディスクリプタとコード・セグメント・セレクタRPLの特権レベルとタイプのチェックが行われます。
3. RET命令にパラメータ・カウント・オペランドが含まれており、リターン操作によって特権レベルが変更された場合には、呼び出し側スタックのパラメータをスキップするために、ポップアップ・スタックのCS値とEIP値の後にパラメータ・カウント値がESPレジスタに追加されます。この時点でESPレジスタは、元々保存されていたコーラースタックのポインタSSとESPを指しています。
4. 保存したSS値とESP値をSSレジスタとESPレジスタにロードして、呼び出し側のスタックに切り替えます。このとき、呼び出し側スタックのSS値とESP値は破棄されます。
5. RET命令にパラメータ番号のオペランドが含まれている場合、ESPレジスタの値にパラメータ値が加算され、呼び出し側スタック上のパラメータがスキップ（破棄）されます。
6. セグメントレジスタ DS、ES、FS、GS の内容を確認します。新しいCPLよりも小さいDPLを指すセグメントがある場合（一貫性のあるコードセグメントを除く）、CPUはセグメント・レジスタにNULLセレクタをロードします。

#### 4.5.4 ページレベルの保護

ページディレクトリとページテーブルのエントリにある読み取り/書き込みフラグR/Wとユーザー/スーパーバイザーフラグU/Sは、セグメンテーションメカニズムの保護属性のサブセットを提供します。ページング・メカニズムでは、2つのレベルの権限しか認識しません。特権レベル0、1、2はスーパーユーザーレベルに分類され、特権レベル3は通常のユーザーレベルに分類されます。通常のユーザーレベルのページは、読み取り専用/実行可能、または読み取り可能/書き込み可能/実行可能としてマークすることができます。スーパーユーザーレベルのページは、表4-

6に示すように、スーパーユーザーにとっては常に読み取り可能/書き込み可能/実行可能ですが、一般ユーザーにとってはアクセスできません。

セグメント化の仕組みとしては、一番外側のユーザーレベルで実行されるプログラムは、ユーザーレベルのページにしかアクセスできませんが、任意のスーパーユーザーレベル（0、1、2）で実行されるプログラムは、ユーザーレイヤーのページにアクセスできるだけでなく、スーパーユーザーレイヤーのページにもアクセスできます。ユーザー層のページにもアクセスできます。セグメント化メカニズムとは異なり、内側のスーパーユーザーレベルで実行されたプログラムは、ユーザーレベルで読み取り専用/実行可能とマークされているものも含め、どのページに対しても読み取り/書き込み/実行可能な権限を持つ。

Table 4-6 Normal and super user access restrictions on the page

U/S	R/W	User Access Rights	Supervisor Access Rights
0	0	None	Read/Write/Execute
0	1	None	Read/Write/Execute
1	0	Read/Execute	Read/Write/Execute
1	1	Read/Write/Execute	Read/Write/Execute

80X86のアドレス変換機構全体の中で、ページング機構がセグメンテーション機構の後に実装されているように、ページレベルの保護もセグメンテーション機構の後の保護の役割を担っています。まず、すべてのセグメントレベルの保護がチェックされ、テストされます。そのチェックに合格すると、ページレベルの保護のチェックが行われます。例えば、メモリ上のバイトがレベル3のプログラムからアクセス可能なセグメント内にあり、かつユーザーレベルのページとしてマークされている場合にのみ、レベル3のプログラムからアクセスすることができます。ページへの書き込みは、セグメンテーションとページングの両方が許可されている場合にのみ実行できます。セグメントが読み取り/書き込みタイプであっても、そのアドレスに対応するページが読み取り専用/実行可能とマークされていれば、そのページへの書き込みはできません。セグメントのタイプが **read-only/executable** の場合、対応するページに与えられた保護属性にかかわらず、そのページは常に書き込みができません。このように、セグメンテーションやページングの保護機構は、電子回路のシリアルラインのようなもので、接続しないとスイッチが開かないようになっていることがわかります。

同様に、ページの保護属性は、表4-7に示すように、テーブルエントリの「シリアル」または「アンドオペレーション」と、ページテーブルのエントリで構成されています。ページ・テーブル・エントリのU/SフラグとR/Wフラグは、エントリ・マッピングの単一ページに適用される。ページ・ディレクトリ・エントリのU/SフラグとR/Wフラグは、そのディレクトリ・エントリにマッピングされたすべてのページに作用する。ページ・ディレクトリとページ・テーブルの複合保護属性は、2つの属性のAND演算で構成されているため、保護手段は非常に厳しいものとなります。

Table 4-7 Page directory and page table entries combined protection of the page

Dir Entry U/S	Page Entry U/S	Combined U/S	Dir Entry R/W	Page Entry R/W	Combined R/W
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	0
1	1	1	1	1	1

#### 4.5.4.1 ページテーブルのエントリを変更するためのソフトウェアの課題

メモリ参照のたびにメモリ上のページテーブルにアクセスしなくとも済むように、プロセッサ内のページ変換キャッシュには、直近に使用されたリニアアドレスから物理アドレスへの変換情報が格納されています。プロセッサは、メモリ上のページテーブルにアクセスする前に、まずバッファキャッシュの情報を使用します。プロセッサは、必要な変換情報がキャッシュ内にない場合にのみ、メモリ内のページディレクトリとページテーブルを検索します。ページ変換キャッシュの別称として、TLB

(Translation Lookaside Buffer) があります。

80X86プロセッサは、ページ変換キャッシュとページテーブルのデータの依存関係を維持するのではなく、それらの整合性を確保するためにオペレーティングシステムソフトウェアを必要とする。つまり、プロセッサは、ページテーブルがソフトウェアによって変更されたことを知りません。そのため、オペレーティングシステムは、ページテーブルを変更した後にキャッシュをリフレッシュして、両者の整合性を確保する必要があります。レジスタCR3をリロードするだけで、キャッシュのリフレッシュ動作を完了させることができます。

ページテーブルのエントリを変更しても、ページ変換キャッシュを更新する必要がない特別なケースがあります。すなわち、存在しないページのエントリを修正する際に、ページ変換に有効なエントリであることを示すためにPフラグを0から1に変更したとしても、キャッシュをリフレッシュする必要はないのである。無効なエントリはキャッシュに保存されないので、ディスクからメモリにページを呼び出してページを存在させるときも、ページ変換キャッシュをリフレッシュする必要はない。

#### 4.5.5 ページプロテクションとセグメントプロテクションの組み合わせ

ページングを有効にすると、CPUはまずセグメントレベルの保護を行ってから、ページレベルの保護を処理します。CPUはどのレベルでも保護違反のエラーを検出すると、メモリアクセスを破棄して例外を発生させます。それがセグメント機構で発生した例外であれば、それ以上のページ例外は発生しません。

ページレベルの保護機能は、セグメントレベルの保護機能を置き換えたり、上書きしたりするためには使えません。例えば、コードセグメントが書き込み不可能に設定されている場合、コードセグメントがページ化された後、ページのR/Wフラグが読み取り可能、書き込み可能に設定されていても、そのページは書き込み不可能になります。この時点で、セグメント保護のチェックにより、そのページに書き込もうとしてもブロックされます。ページレベルの保護は、セグメントレベルの保護を強化するために使用することができます。例えば、読み書き可能なデータセグメントがページ化されている場合、ページレベルの保護機能を使って個々のページを書き込み保護することができます。

## 4.6 割り込みと例外処理

割り込みや例外は、システム、プロセッサ、現在の実行者（またはタスク）のどこかで発生した、プロセッサで処理する必要のあるイベントです。多くの場合、このようなイベントによって、実行制御が現在実行中のプログラムから、割り込みハンドラや例外ハンドラと呼ばれる特別なソフトウェア関数やタスクに強制的に移されることがあります。割り込みや例外に対応してプロセッサが行う動作を、割り込み/例外サービス（処理）と呼びます。

通常、割り込みは、ハードウェアからの信号に応じて、プログラムの実行中のランダムなタイミングで発生します。システムのハードウェアは、外部機器へのサービス要求などの外部イベントを処理するために割込みを使用します。もちろん、ソフトウェアでもINT n命令を実行することで割り込みを発生させることができます。

例外は、プロセッサが命令を実行しているときに、以下のようなエラー条件が検出されたときに発生します。

のエラー状態をゼロで割ったものです。プロセッサは、保護機構の違反、ページフォルト、内部マシンエラーなど、さまざまなエラー状態を検出することができます。

アプリケーションやOSにとって、80X86の割り込み・例外処理機構は、発生した割り込みや例外を透過的に処理します。割り込みを受信したり、例外を検出したりすると、プロセッサは自動的に現在実行中のプログラムやタスクを中断し、割り込みや例外ハンドラの実行を開始します。ハンドラが完了すると、プロセッサは再開し、中断されたプログラムまたはタスクの実行を継続します。割り込まれたプログラムの復旧処理は、例外からの復旧が不可能な場合や、割り込みによって現在のプログラムが終了しない限り、プログラムの実行の継続性を失わない。ここでは、プロテクトモードにおけるプロセッサの割り込みと例外の処理機構について説明します。

### 4.6.1 割り込みの原因

プロセッサは、2つの場所から割り込みを受け取ります。

- 外部（ハードウェア生成）割り込み。
- ソフトウェアで生成された割り込み。

外部割り込みは、プロセッサチップ上の2つのピン（INTRとNMI）で受信します。ピンINTRが外部割り込み信号を受信すると、プロセッサは外部割り込みコントローラ（8259Aなど）から提供された割り込みベクタ番号をシステムバスから読み込みます。ピンNMIが信号を受信すると、ノンマスカブル割り込みを発生させます。プロセッサのINTR端子で受信する外部割り込みは、割り込みベクタ番号0～255を含めてマスカブルハードウェア割り込みと呼ばれます。フラグレジスタEFLAGSのIFフラグは、これらすべてのハードウェア割り込みをマスクするために使用できます。

#### INT

n命令は、命令オペランドに割り込みベクタ番号を指定することで、ソフトウェアからの割り込みを発生させることができます。例えば、INT

0x80という命令は、Linuxのシステム割り込みコールの割り込み0x80を実行します。この命令のパラメータには、0～255の任意のベクターを使用できます。ただし、プロセッサがあらかじめ定義したNMIベクターを使用した場合、それに対するプロセッサの応答は、通常に生成されるNMI割り込みとは異なります。INT命令にNMIベクタ番号2が使用された場合、NMI割り込みハンドラが呼び出されますが、この時、プロセッサのNMI処理ハードウェアは起動しません。

なお、INT命令を用いてソフトウェアで生成した割り込みは、EFLAGSレジスタのIFフラグではマスクできません。

### 4.6.2 例外の原因

また、プロセッサが受け取る例外のソースは2つあります。

- プロセッサが検出したプログラムエラーの例外。
- ソフトウェアで作られた例外です。

アプリケーションやオペレーティングシステムの実行中に、プロセッサがプログラムエラーを検出すると、1つまたは複数の例外が発生します。80X86プロセッサは、検出した各例外に対してベクターを定義します。例外はさらに、後述するように、フォールト、トラップ、アボートに分類されます。

#### INTO命令、INT

3命令、BOUND命令は、ソフトウェアから例外を生成するために使用できます。これらの命令は、命令ストリームの特定のポイントで実行される特別な例外条件をチェックします。例えば、INT

3命令はブレークポイント例外を発生させます。

#### INT

n命令は、指定された例外をソフトウェアでシミュレートするために使用できますが、1つの制限があります。INT命令のオペランドnが80X86の例外ベクター番号の一つである場合、プロセッサはベクターに関連した例外ハンドラを実行するベクター用の割り込みを生成します。しかし、これは実際には割り込みなので、ベクター関連の

ハードウェアで発生した割り込みは、通常、エラーコードを生成します。エラー・コードを生成する例外については、例外ハンドラは処理中にスタックからエラー・コードをポップ・オフしようとします。そのため、INT命令を使って例外発生をエミュレートすると、ハンドラはEIP（ちょうどエラーコードがない位置）をスタックにポップオフして捨ててしまい、リターン・ポジション・エラーが発生してしまいます。

### 4.6.3 例外的な分類

例外は、例外の報告方法や、例外の原因となった命令がプログラムやタスクの継続性を損なわずに再実行できるかどうかによって、Faults、Traps、Abortに細分化されます。

- フォルトとは、通常は修正可能な例外であり、修正後は継続して実行することができます。フォルトが発生すると、プロセッサはマシンの状態を、フォルトを発生させた命令を実行する前の状態に戻します。このとき、例外ハンドラのリターン・アドレスは、後続の命令ではなく、フォルトを発生させた命令を指すことになります。そのため、リターン後にフォルトを発生させた命令が再実行されます。
- Trapは、トラッピング命令の実行直後に報告される例外である。また、Trapはプログラムやタスクを連続性を失わずに実行することを可能にします。トラップハンドラのリターンアドレスは次の命令を指しているので、リターン後に次の命令が実行されます。
- Abortは、例外の原因となった命令の正確な位置を報告するとは限らず、例外の原因となったプログラムの実行を再開することもできない例外です。Abortは、ハードウェア・エラーやシステム・テーブルの不整合や不正な値などの深刻なエラーを報告するために使用されます。

### 4.6.4 エクセプションとインタラプトベクター

例外や割り込みを処理するために、プロセッサが特別な処理を必要とする定義された例外や割り込み条件には、ベクターと呼ばれる識別番号が与えられています。プロセッサは、ベクターをIDT (Interrrupt Descriptor Table) のインデックス番号として使用し、例外や割り込みハンドラのエントリポイントの位置を特定します。

許可されるベクター番号の範囲は0～255です。0～31は80X86プロセッサで定義されている例外や割り込みのために予約されていますが、現在この範囲のベクター番号は機能ごとに定義されておらず、未定義の機能のベクター番号は将来の使用のために予約されます。

ユーザー定義の割り込みには、32～255のベクター番号が使用されます。これらの割り込みは、通常、外部I/Oデバイスが外部のハードウェア割り込みメカニズムを介してプロセッサに割り込みを送信できるようにするために使用されます。

80X86 で定義されている例外および NMI 割り込みに割り当てられているベクターを表 4-8 に示します。それぞれの例外について、例外の種類、エラーコードの生成とスタックへの保存の有無を示しています。また、あらかじめ定義されている各例外およびNMI割り込みのソースも示しています。

す。

Table 4-8 Exceptions and interruptions in protected mode

Vector No.	Mnemonic	Description	Type	Error Code	Source
0	#DE	Divide Error	Fault	No	DIV and IDIV instructions.
1	#DB	Debug	Fault/Trap	No	Any code or data reference or the INT 1 instruction.
2	--	NMI Interrupt	Interrupt	No	Nonmaskable external interrupt.
3	#BP	Breakpoint	Trap	No	INT 3 instruction.
4	#OF	Overflow	Trap	No	INTO instruction.
5	#BR	BOUND Range Exceeded	Fault	No	BOUND instruction.
6	#UD	Invalid Opcode (Undefined)	Fault	No	UD2 instruction or reserved (new for P6)
7	#NM	Device Not Available (No Math Coprocessor)	Fault	No	Floating-point or WAIT/FWAIT instruction.
8	#DF	Double Fault	Abort	Yes(Zero)	Any instruction that can generate an exception, an NMI, or an INTR.
9	--	Coprocessor Segment Overrun (reserved)	Fault	No	Floating-point instruction (not for CPU after 386)
10	#TS	Invalid TSS	Fault	Yes	Task switch or TSS access.
11	#NP	Segment Not Present	Fault	Yes	Loading segment registers or accessing system segments.
12	#SS	Stack-Segment Fault	Fault	Yes	Stack operations and SS register loads.
13	#GP	General Protection	Fault	Yes	Any memory reference and other protection checks.
14	#PF	Page Fault	Fault	Yes	Any memory reference.
15	--	(Intel reserved. Do not use.)		No	
16	#MF	Floating-Point Error (Math Fault)	Fault	No	Floating-point or WAIT/FWAIT instruction.
17	#AC	Alignment Check	Fault	Yes(Zero)	Any data reference in memory.
18	#MC	Machine Check	Abort	No	Error codes (if any) and source are model dependent.
19	#XF	Streaming SIMD Extensions	Fault	No	SSE and SSE2 floating-point instructions. (for PIII cpu)
20-31	--	Intel reserved. Do not use.			
32-255	--	User Defined (Nonreserved) Interrupts	Interrupt		External interrupt or INT n instruction.

#### 4.6.5 プログラムまたはタスクの再起動

例外や割込みの処理後にプログラムやタスクが実行を再開するためには、Abortを除くすべての例外は正確な命令位置を報告でき、すべての割込み保証は命令境界上で発生します。

フォールトクラスの例外では、プロセッサが例外を発生させたときに保存された戻り命令ポインタは、フォールト命令を指します。そのため、フォールト・ハンドラの復帰後にプログラムやタスクが再起動されると、元のフォールト命令が再実行されます。フォルトの原因となった命令の再実行は、通常、アクセス命令のオペランドがロックされている場合の処理に使用されます。フォールトの最も一般的な例は、ページ・フォールト例外です。この例外は、プログラムがメモリ上のページないオペランドを参照したときに発生します。ページフォルト例外が発生すると、例外ハンドラはページをメモリにロードし、フォルト命令を再実行することでプログラムの実行を再開することができます。再実行が現在の実行プログラムにとって透過的であるように、プロセッサは必要なレジスタとスタック・ポインタの情報を保存して、フォールト命令を実行する前の状態に戻れるようになります。

Trapクラスの例外では、プロセッサが例外を発生させたときに保存されたリターンポインタは、トラップ動作の原因となった次の命令を指します。以下のような命令の実行中にTrapが検出された場合、Trapの原因となった次の命令を指します。

が制御の移行を行った場合、戻り命令ポインタは制御の移行を反映します。例えば、JMP命令の実行中にTrap例外が検出された場合、リターン命令ポインタはJMP命令の次の命令ではなく、JMP命令のターゲットロケーションを指します。

アボート・クラスの例外は、プログラムやタスクの確実な再起動をサポートしません。例外を中止するハンドラは、通常、例外が発生したときのプロセッサの状態に関する診断情報を収集し、可能な限り適切にプログラムやシステムを終了させるために使用されます。

割り込みは、中断したプログラムを継続性を失わずに再開することを厳密にサポートします。割り込みのために保存された戻り命令ポインタは、プロセッサが割り込みを取得したときに実行される次の命令境界を指します。実行されたばかりの命令に繰り返しのプレフィックスがある場合、現在の反復が終了し、次の反復のためにレジスタが設定されたときに割り込みが発生します。

## 4.6.6 割り込みの有効化と無効化

フラグレジスタEFLAGSのインタラプトイネーブルフラグ (IF) は、プロセッサのINTR端子で受信したマスカブルハードウェア割り込みの処理を無効にすることができます。 IF = 0の場合、プロセッサはINTRピンに送られる割り込みを無効にし、 IF = 1の場合、INTRピンに送られる割り込み信号はプロセッサによって処理されます。

IFフラグは、NMI端子に送られるノンマスキング割り込みや、プロセッサが発生させる例外には影響しません。EFLAGSの他のフラグと同様に、プロセッサはハードウェアリセット操作に応じてIFフラグをクリアする (IF=0)。

IFフラグは、STI命令とCLI命令を用いて設定または解除することができます。これらの2つの命令は、プログラムのCPL <= IOPLのときにのみ実行でき、そうでない場合は一般保護例外が発生する。また、IFフラグは以下の操作によっても影響を受ける。

- PUSHF命令は、EFLAGSの内容をスタック上に保存し、その内容を調べたり変更したりすることができます。POPF命令は、変更されたフラグの内容をEFLAGSレジスタに戻すために使用されます。
- タスクスイッチ、POPF、IRETの各命令はEFLAGSレジスタをロードします。したがって、これらの命令はIFフラグの設定を変更するために使用することができます。

- 割り込みゲートで割り込みが処理されると、IFフラグは自動的にクリア（リセット）され、マスク可能なハードウェア割り込みが無効になります。ただし、トラップゲートで割り込みが処理された場合は、IFフラグはリセットされません。

#### 4.6.7 例外や割り込みの優先順位

命令の境界で処理待ちの例外や割り込みが複数ある場合、プロセッサは指定された順序で処理します。表4-

9に、例外および割り込みソースクラスの優先順位を示します。プロセッサはまず、優先度の高いクラスの例外や割り込みを処理します。優先度の低い例外は破棄され、優先度の低い割り込みは待機します。割り込みハンドラが、例外や割り込みを発生させたプログラムやタスクに戻ると、破棄された例外が再び発生します。

Table 4-9 Priority of exceptions and interrupts

Priority	Description
1(Highest)	Hardware reset: RESET
2	Task switching trap: T flag is set in TSS
3	External hardware intervention
4	Previous instruction trap: breakpoint, debug trap exception
5	External interrupt: NMI interrupt, maskable hardware interrupt
6	Code breakpoint error
7	Take an instruction error: violation of code segment limit, code page error
8	The next instruction decode error: instruction length >15 bytes, invalid opcode, coprocessor does not exist
9(Lowest)	Execution instruction error: overflow, boundary check, invalid TSS, segment not present, stack error, general protection, data page, alignment check, floating point exception

## 4.6.8 割り込みディスクリプター テーブル(IDT)

割り込み記述子テーブル (IDT) は、各例外や割り込みベクターと、そのプロセスやタスクのゲート記述子を関連付け、関連する例外や割り込みを処理するために使用されます。GDTやLDTテーブルと同様に、IDTも8バイト長の記述子の配列です。GDTとは異なり、テーブルの最初の項目に記述子を含めることができます。IDTテーブルへのインデックスを形成するために、プロセッサは例外または割込みのベクタ番号を\*8に入れます。

割り込みや例外のベクターは最大でも256個なので、IDTには256個以上の記述子を含める必要はありません。記述子は例外や割り込みが発生したときにのみ必要なので、IDTは256個より少ない記述子を含むことができます。ただし、IDT内のすべての空の記述子エントリは、その存在ビット（フラグ）をゼロに設定する必要があります。

IDTテーブルはリニアアドレス空間のどこにでも存在することができますが、プロセッサはIDTRレジスタを使用してIDTテーブルの位置を特定します。このレジスタには、図4-26に示すように、IDTテーブルの32ビットのベースアドレスと16ビットの長さ（長さ制限）の値が含まれています。IDTテーブルのベースアドレスは、プロセッサのアクセス効率を高めるために、8バイト境界にアラインする必要があります。長さ制限値は、IDTテーブルの長さをバイト単位で表したものです。

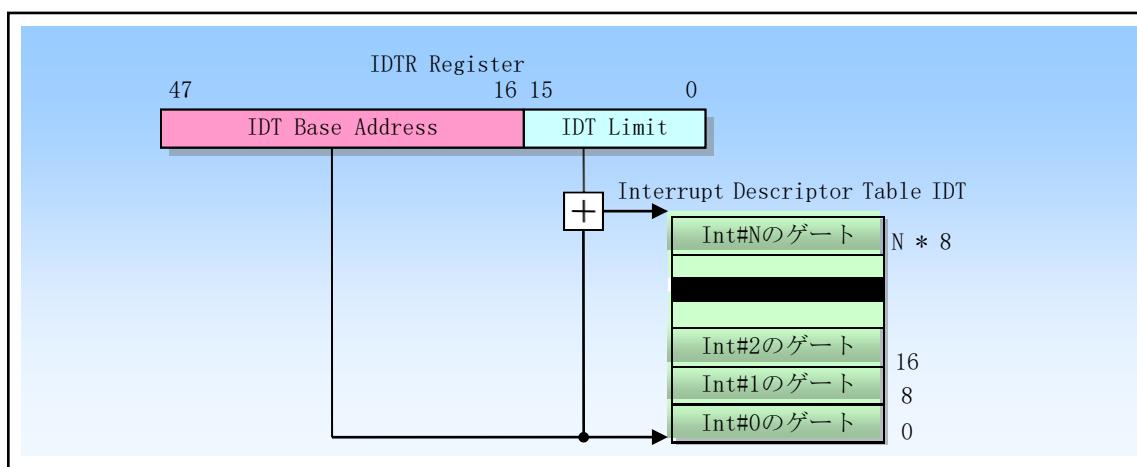


図4-26 インタラプトディスクリプター テーブルIDTとレジスタIDTR

LIDT命令とSIDT命令は、それぞれIDTRレジスタの内容をロードおよびストアするために使用されます。LIDT命令は、メモリ上のリミットとベースアドレスのオペランドをIDTRレジスタにロードします。この命令は、現在の特権レベルCPLが0のコードのみが実行可能で、通常、IDTの作成時にOSの初期化コードで使用されます。SIDT命令は、IDTR内のベースアドレスとリミットコンテンツをメモリにコピーするために使用されます。この命令はどの特権レベルでも実行可能です。割り込みや例外ベクターが参照するディスクリプターがIDTの境界を超えた場合、プロセッサは一般保護例外を生成します。

### 4.6.9 IDT記述子

IDTテーブルには、3種類のゲートディスクリプターを格納することができます。

- 割り込みゲートの記述子。
- トランプゲートの記述子。
- タスクゲートの記述子。

これら3つのゲート記述子のフォーマットを図4-27に示します。割り込みゲートとトランプゲートには、プロセッサがコードセグメント内の例外や割り込みに対してプログラムの実行権を移すために使用するロングポインタ（つまりセグメントセレクタとオフセット値）が含まれています。この2つのセグメントの主な違いは、プロセッサがEFLAGSレジスタのIFフラグを操作することです。IDTにおけるタスク・ゲート記述子のフォーマットは、GDTおよびLDTにおけるタスク・ゲートのフォーマットと同じです。タスクゲート記述子には、例外や割り込みの処理に使用されるタスクTSSセグメントのセレクタが含まれています。

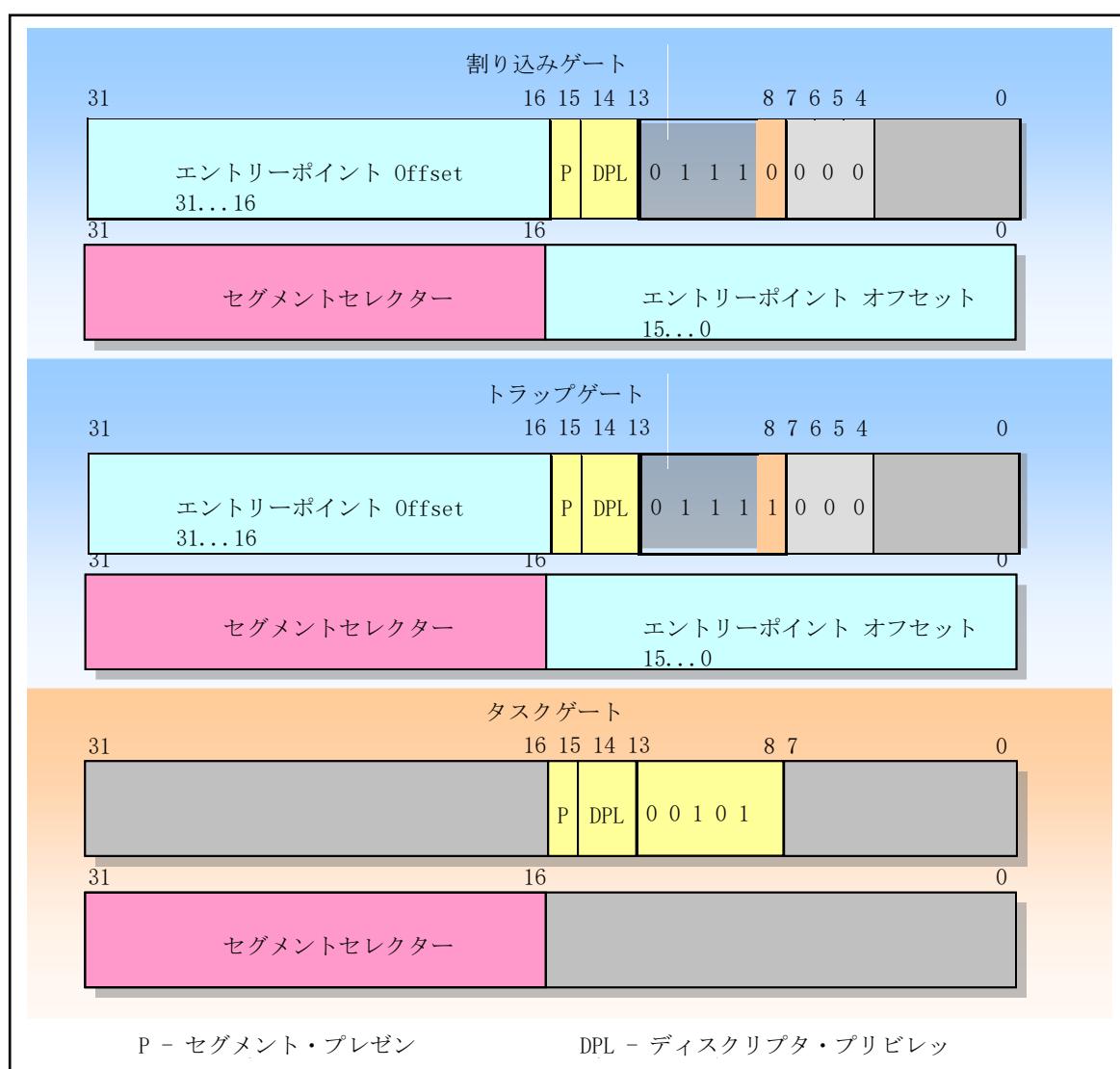


図4-27 インタラプトゲート、トランプゲート、タスクゲート記述子のフォーマット

### 4.6.10 例外と割り込みの処理

プロセッサが例外や割込みハンドラを呼び出す方法は、CALL命令を使ってプロシージャやタスクを呼び出すのと同じです。例外や割込みに応答する際、プロセッサは例外や割込みのベクターをIDTテーブルのインデックスとして使用します。インデックス値が割込みゲートまたはトラップゲートを指している場合、プロセッサはCALL命令の操作コールゲートと同様の方法で例外または割込みハンドラを呼び出します。インデックス値がタスクゲートを指している場合、プロセッサは、CALL命令操作のタスクゲートと同様の方法でタスクスイッチを行い、例外または割込み処理タスクを実行する。

図4-

28に示すように、例外・割込みゲートは、現在のタスクのコンテキストで実行される例外・割込みハンドラを参照します。ゲートのセグメント・セレクタは、GDTまたは現在のLDTの実行コード・セグメント・ディスクリプタを指します。ゲート記述子のオフセット・フィールドは、例外または割込み処理プロセスの開始点を指します。

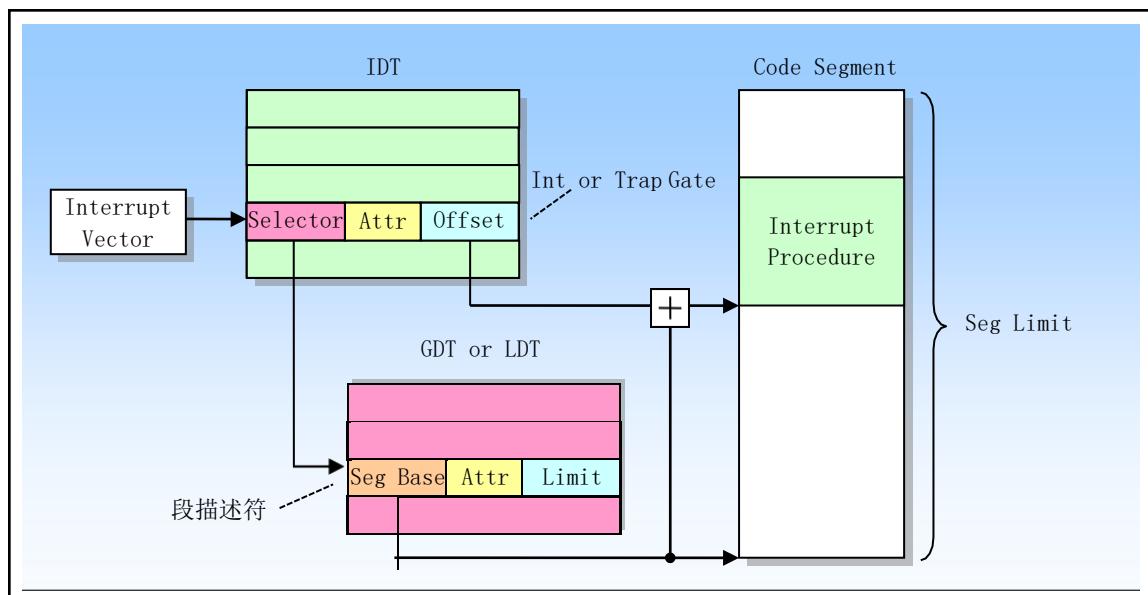


Figure 4-28 Interrupt Procedure Call

プロセッサが例外や割込みハンドラの呼び出しを実行すると、以下のような動作が行われます。

- ハンドラプロシージャが高い特権レベル（レベル0など）で実行される場合は、スタックスイッチ操作が発生します。スタック切り替えの手順は以下の通りです。

プロセッサは、現在実行中のタスクのTSSセグメント（例：tss.ss0、tss.esp0）から、割込みハンドラや例外ハンドラが使用するスタックのセグメントセレクタとスタックポインタを取得します。次にプロセッサは、図4-

29に示すように、中断されたプログラム（またはタスク）のスタック・セレクタとスタック・ポインタを新しいスタックにプッシュします。次に、プロセッサは

EFLAGS、CS、および

EIP

レジスタの現在の値を新しいスタックにプッシュします。例外によってエラーコードが

- 発生した場合は、そのエラーコードも新しいスタックにプッシュされます。
- ハンドラプロシージャが中断されたタスクと同じ特権レベルで実行される場合は  
プロセッサは EFLAGS、CS、EIP  
レジスタの現在の値を現在のスタックに保存します。例外によってエラーコードが発生した場合は、そのエラーコードも新しいスタックにプッシュされます。

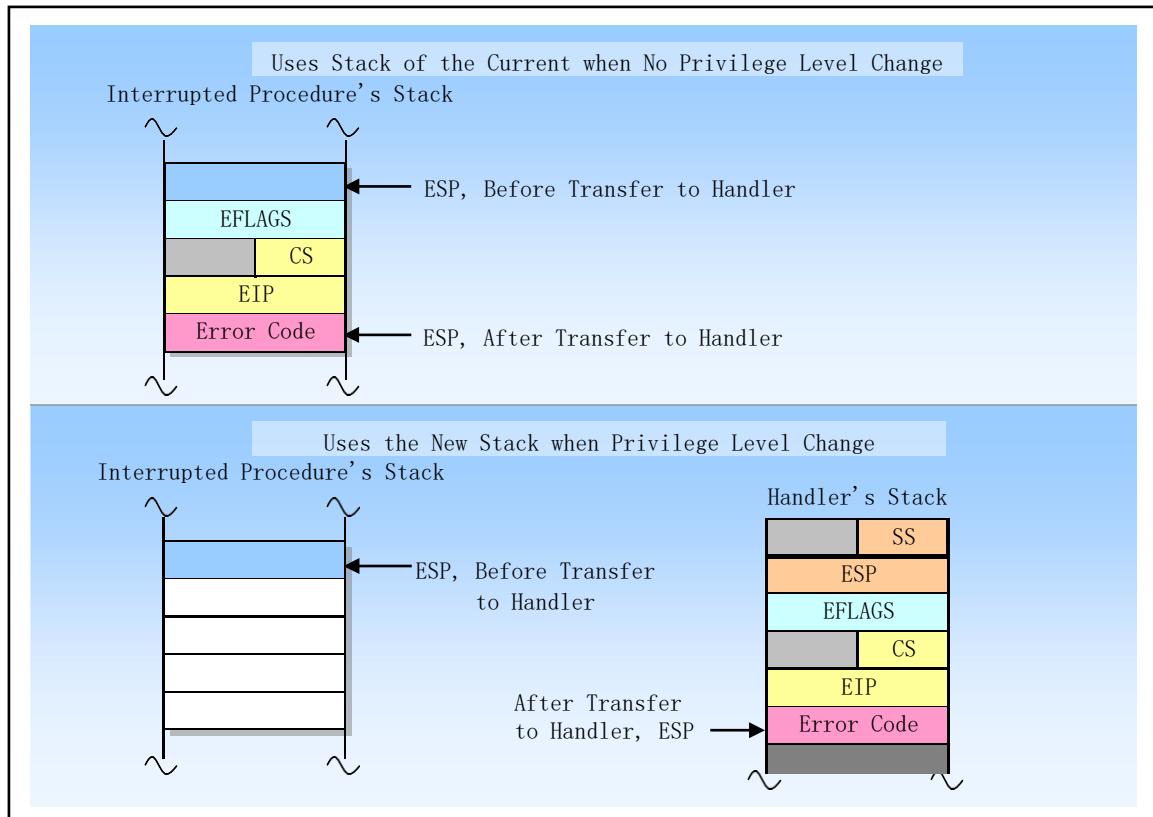


Figure 4-29 Stack usage method when transferring to interrupt processing

例外処理や割込み処理の手続きから戻るには、ハンドラはIRET（またはIRETD）命令を使用しなければなりません。IRET命令はRET命令と似ていますが、保存されているフラグをEFLAGSレジスタにリストアする点が異なります。EFLAGSレジスタのIOPLフィールドは、CPLが0の場合のみリストアされ、CPL  $\leq$  IOPLの場合のみIFフラグが変更されます。ハンドラプロシージャの呼び出し時にスタックスイッチが発生した場合、IRET命令はリターン時に中断されたプロシージャのスタックにスイッチバックします。

#### 4.6.10.1 例外の保護と割込みハンドラ手続き

例外処理や割込みハンドラプロシージャの特権レベル保護メカニズムは、コールゲートを介して通常のプロシージャを呼び出すのと同様です。プロセッサは、CPL特権コード・セグメントよりも下位の割込みハンドラ・プロシージャに制御を移すことを許可しません。そうしないと、一般保護例外が発生します。また、割込みや例外に対する保護機構は、以下の点で一般的なコールゲート手順とは異なります。

- 割り込みおよび例外ベクターにはRPLがないため、例外ハンドラおよび割り込みハンドラプロシージャが暗黙的に呼び出される際にRPLはチェックされません。
- プロセッサは、INT n、INT

3、またはINTO命令を使用して例外または割り込みが発生したときにのみ、割込みまたはトラップゲートのDPLをチェックします。このとき、CPLはゲートのDPL以下でなければなりません。この制限により、特権レベル3で実行されるアプリケーションがソフトウェア割り込みを使用してページフォルト処理などの重要な例外処理手順にアクセスすることができなくなります。これらの処理は、より高い特権レベルのコードセグメントに配置されていることを前提としています。ハードウェアで生成された割り込みやプロセッサが検出した例外に対しては、プロセッサは割り込みゲートやトラップゲートのDPLを無視します。

通常、例外や割り込みは定期的に発生するものではないので、特権レベルに関するこれらのルールは、例外処理や割り込みハンドラが実行できる特権レベルの制限を効果的に強化します。特権レベルの保護に違反しないように、以下のいずれかの手法を用いることができます。

■ 例外ハンドラや割り込みハンドラは、一貫したコードセグメントに格納することができます。

この手法は、スタック上で利用可能なデータにのみアクセスする必要があるハンドラーに使用できます（例えば、分割エラーの例外）。ハンドラがデータセグメントのデータを必要とする場合は、特権レベル3がこのデータセグメントにアクセスできなければなりません。しかし、保護は全くありません。

■ ハンドラは、特権レベル

0

の不適合コードセグメントに配置できます。このハンドラは、中断されたプログラムやタスクの現在の特権レベルCPLに関係なく、常に実行することができます。

#### 4.6.10.2 例外や割り込みハンドラのプロシージャによるフラグの使用

割り込みゲートやトラップゲートを経由して例外や割り込みハンドラにアクセスした場合、プロセッサはEFLAGSレジスタの内容をスタックに保存した後、EFLAGSのTFフラグをクリアします。TFフラグをクリアすることで、命令トレースが割り込み応答に影響を与えることを防ぎます。続くIRET命令は、スタックの内容でEFLAGSの元のTFフラグを復元します。

割り込みゲートとトラップゲートの唯一の違いは、プロセッサがEFLAGSレジスタのIFフラグを操作する方法です。割り込みゲートを介して例外や割り込みハンドラにアクセスすると、プロセッサはIFフラグをリセットして、他の割り込みが現在の割り込みハンドラに干渉しないようにします。後続のIRET命令は、スタックに格納された内容でEFLAGSレジスタのIFフラグを復元します。トラップ・ゲートからハンドラ・プロシージャにアクセスしても、IFフラグには影響しません。

#### 4.6.11 インタラプトハンドラータスク

タスクの切り替えは、IDTのタスクゲートを介して例外や割り込みハンドラにアクセスするときに発生します。例外や割り込みの処理を別々のタスクで行うことには、以下のようなメリットがあります。

- 中断されたプログラムやタスクの完全なコンテキストが自動的に保存されます。
- 新しいTSSでは、ハンドラが例外や割り込みを処理する際に、新しい特権レベル0のスタックを使用することができます。現在の特権レベル0のスタックが破壊された状態で例外や割り込みが発生した場合、タスク・ゲートを介してハンドラにアクセスすることで、ハンドラに新しい特権レベル0のスタックを提供し、システム・クラッシュを防ぐことができます。
- ハンドラは、独立したアドレス空間を与えることで、他のタスクからさらに分離することができます。これは、独立したLDTを与えることによって行われます。

例外処理や割り込み処理を別のタスクで行う場合、タスク切り替え時にマシンの状態を保存しな

ければならない分、割り込みゲートを使用するよりも遅くなり、結果的に割り込みのレイテンシーが増大するというデメリットがあります。

図4-

30に示すように、IDTのタスクゲートはGDTのTSS記述子を参照します。ハンドラタスクへの切り替え処理は、通常のタスク切り替え処理と同じです。割り込まれたタスクへのバックリンクは、ハンドラタスクTSSの前タスククリンクフィールドに保存されます。例外でエラーコードが発生した場合は、エラーコードが新しいタスクスタックにコピーされます。

オペレーティングシステムで例外ハンドラや割込みハンドラタスクを使用する場合、タスクをディスパッチするためのメカニズムは、実際には、オペレーティングシステムのソフトウェアスケジューラとプロセッサの割込み機構のハードウェアスケジューラの2つがあります。ソフトウェアスケジューラは、割り込みが有効なときにディスパッチされる可能性のある割り込みタスクに対応する必要があります。

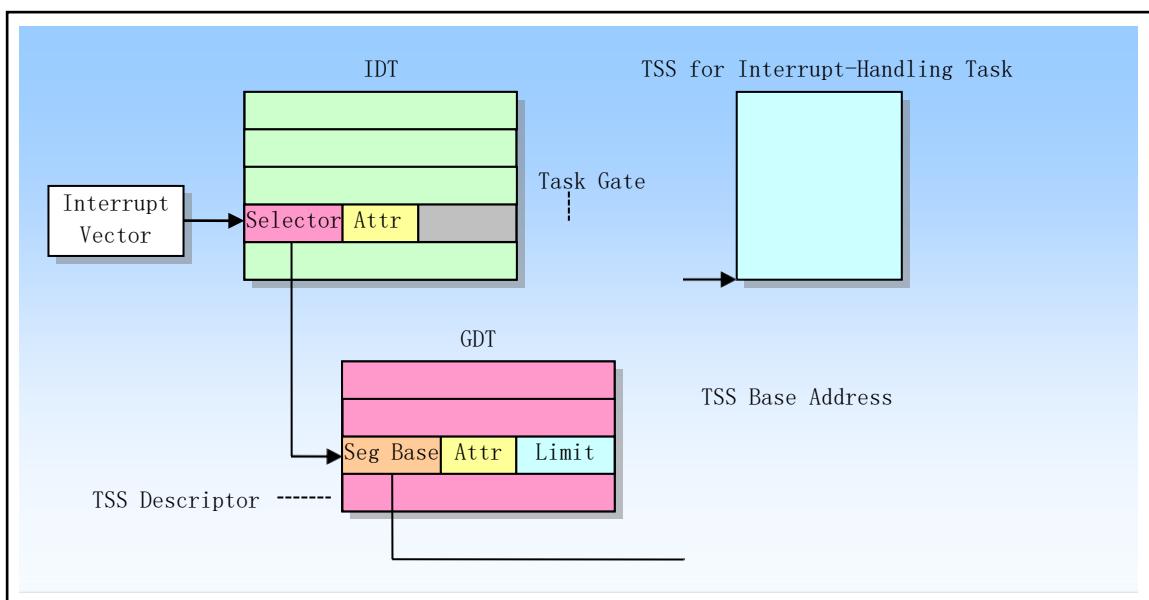


Figure 4-30 Interrupt Task Switch

#### 4.6.12 エラーコード

特定のセグメントに例外状態が発生した場合、プロセッサはエラーコードを例外ハンドラのスタックにプッシュします。エラー・コードのフォーマットを図4-

31に示します。エラーコードはセグメントセレクタとよく似ていますが、最下位3ビットはTIとRPLフィールドではなく、次の3つのフラグです。

- ビット0は、外部イベント (EXT) フラグです。セットされていると、プログラムの外部イベントによってハードウェア割り込みなどの例外が発生したことを示します。
- ビット1は、ディスクリプターロケーション (IDT) フラグです。本ビットがセットされている場合、エラーコードを示すインデックス部分がIDT内のゲートディスクリプタを指していることを示す。このビットがリセットされると、インデックスがGDTまたはLDT内の記述子を指していることを示します。

- ビット2は、GDT/LDTテーブルセレクトフラグTIです。IDT(ビット1)が0の時のみ有効です。TI=1の時は、エラーコードを示すインデックス部分がLDT内の記述子を指していることを示します。TI=0の場合、エラーコードを示すインデックス部がGDTテーブル内のディスクリプタを指していることを示す。

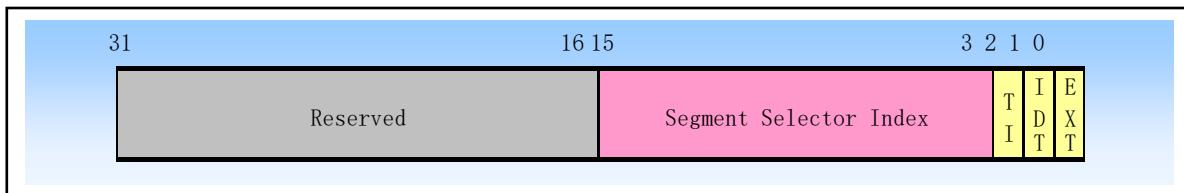


Figure 4-31 Error Code format

セグメント・セレクタ・インデックス・フィールドは、エラー・コードによって参照されるセグメントまたはゲート・セレクタのIDT、GDT、または現在のLDTへのインデックスを提供します。場合によっては、エラー・コードがヌル（下位16ビットがすべてクリア）になることがあります。ヌルのエラー・コードは、特定のセグメントを参照したことが原因でエラーが発生したのではないこと、または操作中にヌルのセグメント記述子を参照したことを示します。

ページフォルト例外のエラーコード形式は、図4-32に示すように、上記とは異なります。最下位3ビットのみが有効で、その名前はページテーブルエントリの最後の3ビットと同じです（U/S, W/R,

P). その意味と効果は

- ビット0(P)の場合、ページが存在しないか、アクセス権限に違反しているために発生する例外です。P=0は、ページが存在しないことを示し、P=1は、ページレベルの保護権限に違反していることを示します。
- ビット1 (W/R) 、メモリの読み出しありまたは書き込み操作により例外が発生したことを示す。W/R=0であれば、読み出し操作によるものであることを示し、W/R=1であれば、書き込み操作によるものであることを示す。
- ビット2 (U/S) , 例外発生時にCPUが実行するコードレベルを示す。U/S=0であれば、CPUがスーパーユーザコードを実行していることを示し、U/S=1であれば、CPUが一般ユーザコードを実行していることを示す。

さらに、プロセッサは、ページフォルト例外を発生させるために使用したリニアアドレスをCR2にも格納します。ページフォルト例外ハンドラは、このアドレスを使用して、関連するページディレクトリとページテーブルエントリを見つけることができます。



図4-32 ページフォルトのエラーコードのフォーマット

なお、エラーコードはIRET命令によって自動的にスタックからポップアウトされないので、割り込みハンドラはエラーコードをスタックにクリアしてからリターンする必要があります。また、プロセッサで発生した一部の例外はエラーコードを生成し、ハンドラプロシージャのスタックに自動的に保存されますが、外部ハードウェア割り込みやINT n命令を実行するプログラムで発生した例外は、エラーコードをスタックにpushしません。

## 4.7 タスク管理

タスクとは、プロセッサがスケジューリング、実行、サスペンドのために割り当てることのできる仕事の単位です。プログラム、タスクまたはプロセス、オペレーティングシステムサービス、割込みまたは例外処理手順、およびカーネルコードの実行に使用できます。タスクとは、実行中のプログラムや実行待ちのプログラムのことです。

80X86では、タスクの状態を保存したり、タスクをディスパッチしたり、あるタスクから別のタスクに切り替えたりするマルチタスクのハードウェアサポートを提供しています。プロジェクトモードで作業しているときは、プロセッサの操作はすべてタスクの中で行われます。単純なシステムでも、少なくとも1つのタスクを定義する必要があります。より複雑なシステムでは、プロセッサのタスク管理機能を利用して、マルチタスクアプリケーションをサポートすることができます。

ディスクリプターテーブルの指定されたエントリを用いて、割込み、例外、ジャンプ、コールなどでタスクを実行することができます。ディスクリプターテーブルのタスク関連記述子には、タスク状態セグメント記述子とタスクゲートの2種類がある。これらの記述子のいずれかに実行権が渡されると、タスクの切り替えが行われます。タスクスイッチングはプロシージャコールに似ていますが、タスクスイ

ッチングの方がより多くのプロセッサの状態情報を保存します。タスクスイッチングは、新しい実行環境、つまり新しいタスクの実行環境に制御を完全に移します。この転送操作では、フラグレジスタEFL AGSやすべてのセグメントレジスタなど、プロセッサ内のはぼすべてのレジスタの現在の内容を保存する必要があります。ただし、タスクはリエントラントにすることはできません。タスクの切り替えでは、スタックに情報をプッシュすることはありません。プロセッサの状態情報は、メモリ上のタスクステートセグメント（TSS）と呼ばれるデータ構造に格納されています。

#### 4.7.1 タスクの構造と状態

タスクは、タスク実行空間とタスクステートセグメント（TSS）の2つの部分で構成されています。図4-

33に示すように、タスク実行空間には、コードセグメント、スタックセグメント、および1つ以上のデータセグメントが含まれます。オペレーティングシステムがプロセッサの特権レベル保護メカニズムを使用している場合、タスク実行空間は、特権レベルごとに個別のスタック空間を提供する必要があります。TSSは、タスク実行空間を構成するセグメントを指定し、タスクの状態情報を格納します。マルチタスク環境では、TSSはタスク間のリンクを処理する手段にもなります。

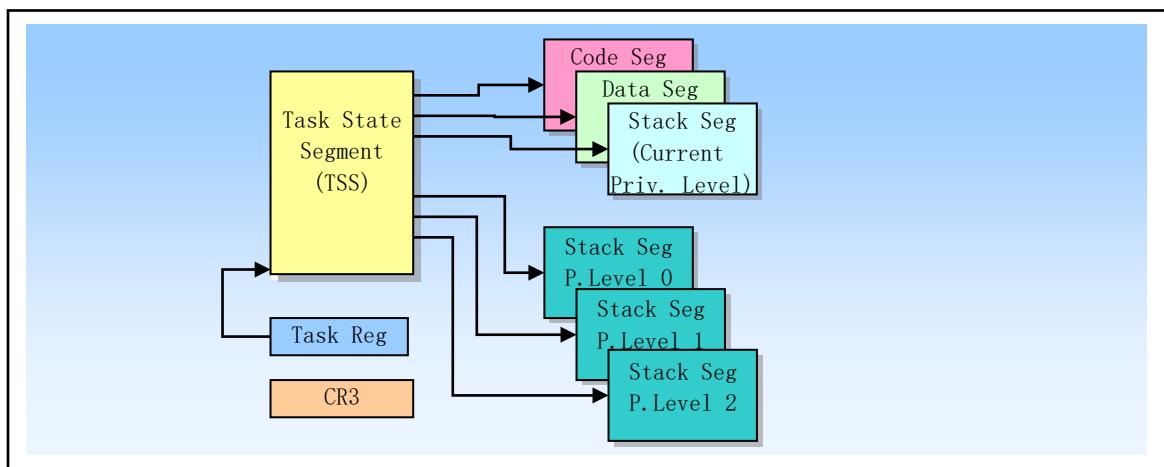


Figure 4-33 Structure of a Task

タスクは、TSSを指すセグメントセレクタで指定されます。タスクが実行のためにプロセッサにロードされると、タスクのセグメントセレクタ、ベースアドレス、セグメント長、TSSセグメント記述子の属性がタスクレジスタ（TR）にロードされます。ページング機構が使用されている場合は、タスクが使用するページディレクトリのベースアドレスがコントロールレジスタCR3にロードされます。現在実行中のタスクの状態は以下のように構成されています。

- セグメントレジスタ（CS、DS、SS、ES、FS、GS）のセグメントセレクタで定義されるタスクの現在の実行空間。
- 汎用レジスターの状態です。
- EFLAGS, EIP, コントロールレジスタCR3, タスクレジスタ, LDTRレジスタの状態です。
- I/OマップのベースアドレスとI/Oマップ（TSSに含まれています）。
- 特権0、1、2のスタックへのスタックポインタ（TSSに含まれる）。
- 以前に実行されたタスク（TSSに含まれる）へのリンク。

タスクを分配する前に、タスクのTSSには、タスクレジスタのステータスを除いて、これらの項目がすべて含まれています。また、LDTRレジスタの完全な内容はTSSには含まれず、LDTのセグメントセレクタのみが含まれます。

## 4.7.2 タスクの実行

ソフトウェアやプロセッサーは、以下のいずれかの方法でタスクを実行に移すことができます。

- CALL命令でタスクを明示的に呼び出すこと。
- JMP命令によるタスクへの明示的なジャンプ（Linuxカーネルが採用している方法）。
- 割り込みハンドラタスクに対する（プロセッサによる）暗黙の呼び出し。例外処理タスクへの暗黙の呼び出しです。
- EFLAGSレジスタのNTフラグがセットされている場合のリターン（IRET命令で開始）。

これらのタスク実行のスケジューリング方法は、いずれもタスクゲートやタスクのTSSセグメントを指し示すセレクタを使ってタスクを決定します。CALL命令やJMP命令でタスクをディスパッチする場合、命令内のセレクタは、タスクのTSSを直接選択する場合と、TSSのセレクタを保持するタスクゲートを選択する場合があります。割込みや例外を処理するためにタスクをディスパッチする場合、IDTの割込みや例外のエントリには、割込みや例外を処理するタスクのTSSのセレクタを保持するタスクゲートが含まれていなければなりません。

タスクがディスパッチされて実行されると、現在実行中のタスクとスケジュールされたタスクの間でタスクスイッチ動作が自動的に行われます。タスク切り替えの際には、現在タスクを実行している実行環境（タスクの状態またはコンテキストと呼ばれる）がTSSに保存され、タスクの実行が中断されます。その後、新たにスケジューリングされたタスクのコンテキストがプロセッサにロードされ、ロードされたEIPが指す命令から新しいタスクが実行されます。

現在実行中のタスク（caller）が、スケジュールされた新しいタスク（callee）を呼び出すと、callerのTSSセグメントセレクタがcalleeのTSSに格納され、callerへのリンクが提供されます。すべての80X86プロセッサでは、タスクは再帰的に呼び出されません。つまり、タスクは自己自身を呼び出したり、ジャンプしたりすることはできません。

割り込みや例外は、ハンドラタスクに切り替えて処理することができます。この場合、プロセッサは、割り込みや例外を処理するためのタスクスイッチを実行できるだけでなく、割り込みや例外のハンドラタスクが戻ってきたときに、自動的に割り込みタスクに戻ることができます。この機構により、割込みタスク中に発生した割込みを処理することができます。

タスク切り替え時には、別のLDTへの切り替えも行われるため、LDTベースのセグメントに対して、各タスクが異なる論理-

物理アドレスのマッピングを行うことができます。同時に、ページディレクトリレジスタCR3も切り替え時に再ロードされるため、各タスクは独自のページテーブルを持つことができます。これらの保護機能を利用して、個々のタスクを分離し、相互に干渉しないようにすることができます。

マルチタスクのアプリケーションを処理するために、プロセッサのタスク管理機能を使用することは任意です。また、ソフトウェアを使用してマルチタスクを実装し、ソフトウェアで定義された各タスクが単一の80X86アーキテクチャのタスクのコンテキストで実行されるようにすることもできます。

## 4.7.3 タスク管理のデータ構造

プロセッサには、マルチタスクをサポートする以下のレジスタとデータ構造が定義されています。

- タスク・ステート・セグメント (TSS)。
- TSS記述子。
- タスクレジスター (TR)。
- タスクゲートの記述子。
- EFLAGSレジスタのNTフラグ。

これらのデータ構造を利用することで、プロセッサは、元のタスクのコンテキストを保持したまま、あるタスクから別のタスクに切り替えて、そのタスクを再実行することができます。プロジェクトモードで動作する場合、少なくとも1つのタスクに対してTSSとTSS記述子を作成し、TSSのセグメントセレクタをタスクレジスタにロードする必要があります (LTR命令を使用)。

#### 4.7.3.1 タスク・ステート・セグメント (TSS)

タスクの実行を復元するためのプロセッサの状態情報は、タスクステートセグメントTSS (Task State Segment) と呼ばれるセグメントに保存されます。図4-34は、32ビットCPUで使用されるTSSのフォーマットです。TSSセグメントのフィールドは、ダイナミックフィールドとスタティックフィールドの2つに大別されます。

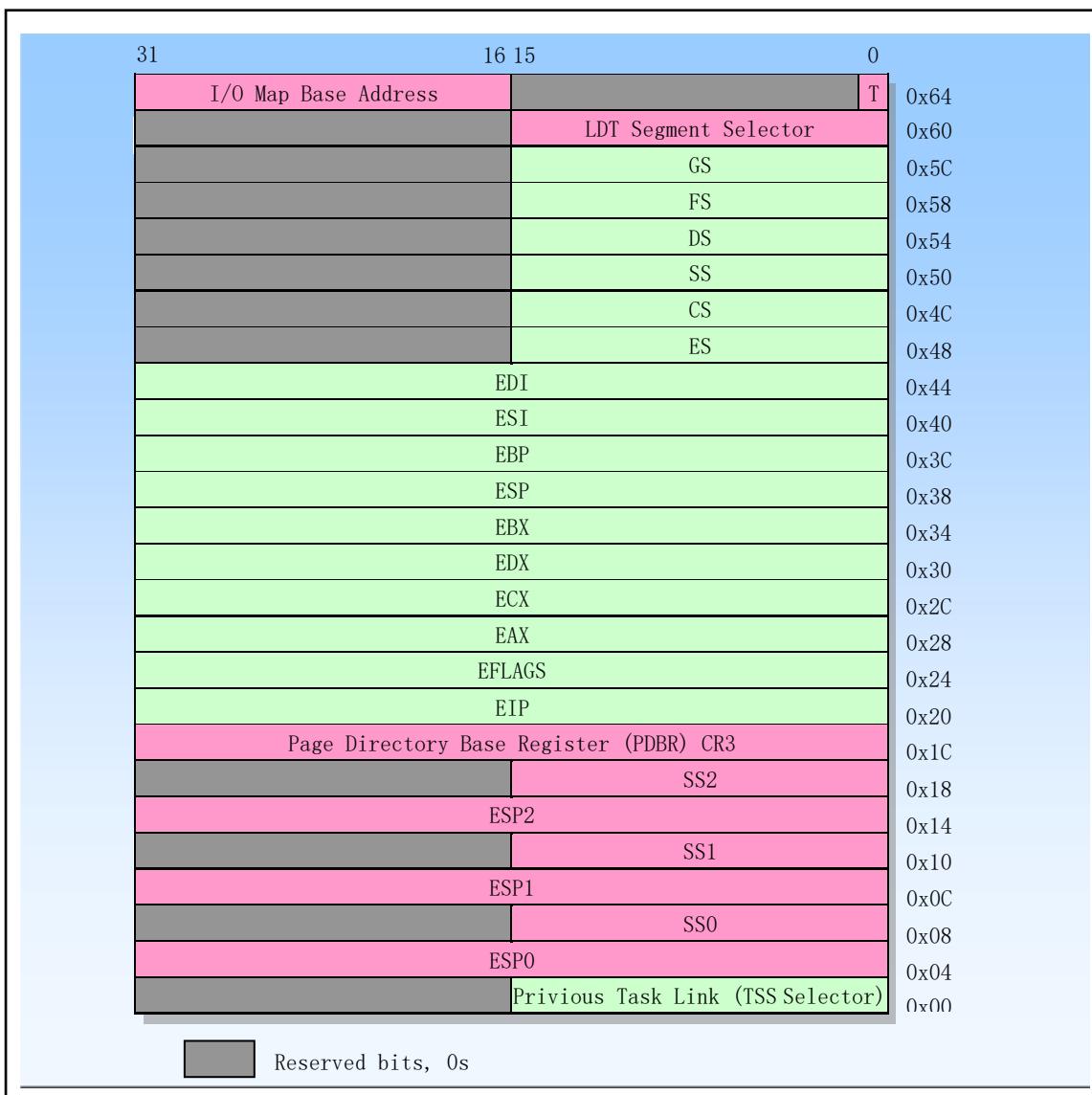


Figure 4-34 32-bit task status segment TSS format

1. ダイナミックフィールド。タスクが切り替えられて中断されると、プロセッサはダイナミックフィールドの内容を更新します。これらのフィールドには
  - 汎用のレジスタフィールドです。EAX, ECX, EDX, EBX, ESP, EBP, ESI, EDIの各レジスタの内容を保存するのに使用します。
  - セグメント・セレクター・フィールド。ES, CS, SS, DS, FS, GSの各セグメント・レジスタの内容を保存する際に使用します。
  - フラグレジスタ EFLAGS フィールド。EFLAGSを保存してから切り替えてください。
  - 命令ポインタEIPフィールド。切り替える前にEIPレジスタの内容を保存してください。
  - 前タスクリンクフィールド。前タスクのTSSセグメントセレクタを含む（コール、割り込み、例外発生のタスク切り替え時に更新される）。このフィールド（一般にバッククリンクフィールドとも呼ばれる）により、IRET命令を使ってタスクを前のタスクに切り替えることができます。
2. 静的フィールド。プロセッサは、スタティック・フィールドの内容を読みますが、通常は変更しません。これらのフィールドの内容は、タスクが作成されたときに設定されます。これらのフィールドは
  - LDT セグメントセレクタフィールド。タスクのLDTのセグメントセレクタを格納する。
  - CR3  
コントロール・レジスタ・フィールド。タスクが使用するページ・ディレクトリの物理ベース・アドレスを含む。  
コントロールレジスタCR3は、一般的にページディレクトリベースレジスタ (PDBR) とも呼ばれています。
  - 特権レベル0、1、2のスタックポインタフィールドです。これらのスタックポインタは、スタックセグメントセレクタ(SS0, SS1, SS2)とスタック内のオフセットポインタ(ESP0, ESP1, ESP2)で構成されています。これらのフィールドの値は、あるタスクでは一定であることに注意してください。したがって、タスクでスタックスイッチが発生した場合、レジスタSSとESPの内容は変化します。
  - デバッグトラップTフラグフィールド。このフィールドは、バイト 0x64 ビット 0 にあります。このビットがセットされていると、プロセッサがタスクに切り替わったときにデバッグ例外が発生します。
  - I/Oビットマップベースアドレスフィールド。このフィールドには、TSSセグメントの先頭からI/O許可ビットマップまでの16ビットのオフセット値が含まれています。これらのマップが存在する場合は、TSSの上位アドレスに格納されます。I/Oマッピングベースアドレスは、I/O許可ビットマップの先頭と、割り込みリダイレクトビットマップの末尾を指します。  
ページング機構が使用されている場合、タスク切り替え時のプロセッサ動作のTSS部分（最初の104バイト目）では、メモリページ境界を回避する必要があります。TSS部分にメモリページ境界がある場合は、境界の両側のページが物理メモリ上に同時にかつ連続して存在していなければなりません。また、ページング機構が使用されている場合、元のタスクTSSと新しいタスクTSSに関連するページ、およびそれに対応するディスクリプターテーブルのエントリは、読み取りと書き込みが可能である必要があります。

### 4.7.3.2 TSS記述子

他のセグメントと同様に、タスク・ステータス・セグメントTSSもセグメント記述子を使って定義します。図4-35にTSS記述子のフォーマットを示します。TSS記述子はGDTにのみ格納されます。

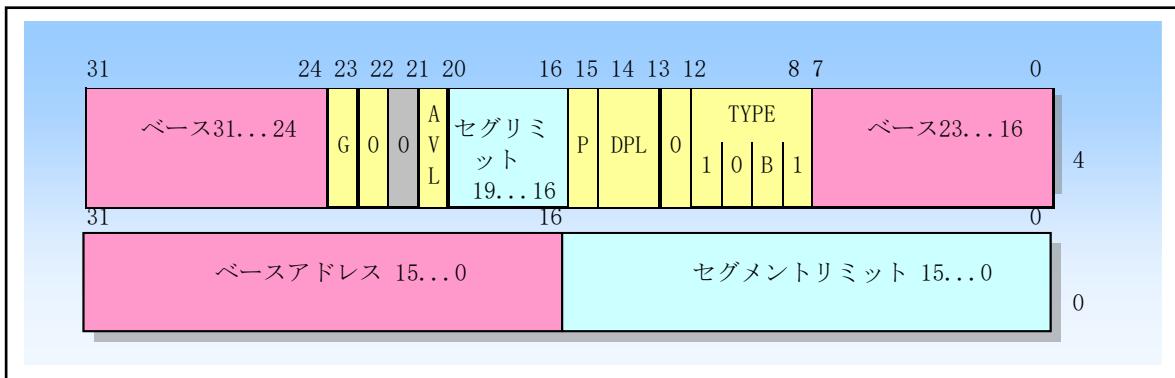


図4-35 TSSセグメント記述子のフォーマット

タイプフィールドTYPEのビジーフラグ(B)は、タスクがビジーであるかどうかを示すために使用されます。ビジーなタスクとは、現在実行中のタスクや、実行待ち(サスPEND)のタスクのことです。タイプフィールドの値が0b1001の場合は、タスクが非アクティブであることを示し、値が0b1011の場合は、タスクがビジーであることを示します。プロセッサはビジーフラグを使用して、実行が中断されたタスクを呼び出そうとしていることを検出します。1つのタスクに関連するビジー・フラグが1つだけであることを保証するために、各TSSはそれを指すTSS記述子を1つだけ持つべきです。

ベースアドレス、リミット、ディスクリプター特権レベルDPL、グラニュラリティG、現在のフラグは、データセグメントディスクリプターの対応するフィールドと同じ機能を持つ。G=0の場合、limitフィールドは103(0x67)以上の値でなければならず、TSSセグメントの最小長は104バイト以上となります。TSSセグメントにI/O許可ビットマップが含まれている場合、TSSセグメントの長さはより大きくする必要があります。また、OSが他の情報をTSSセグメントに格納したい場合は、TSSセグメントの長さを大きくする必要があります。

コール命令やジャンプ命令を使えば、TSS記述子にアクセスできるプログラムであれば、タスクスイッチを起こすことができます。

TSS記述子にアクセスできるプログラムは、TSS記述子のDPL以下の数値のCPLを持っている必要があります。ほとんどのシステムでは、TSS記述子のDPLフィールドを3以下に設定する必要があります。このようにして、特権的なソフトウェアのみがタスク切り替え操作を行うことができます。ただし、マルチタスク・アプリケーションでは、一部のTSSのDPLを3に設定することで、ユーザの特権レベルでもタスク切り替え操作を行うことができます。

TSSセグメント記述子にアクセスできるようになったからといって、プログラムに記述子の読み書きができるようになるわけではありません。TSSセグメント記述子を読み書きしたい場合は、メモリ上の同じ位置にマッピングされているデータセグメント記述子(つまりエイリアス記述子)を使用します。TSS記述子を任意のセグメントレジスタにロードすると、例外が発生します。また、TIフラグで設定されたセレクタ(現在のLDTのセレクタ)を使ってTSSセグメントにアクセスしようとすると、例外が発生します。

### 4.7.33 タスク登録

#### タスクレジスタTR(Task Register)

Register)には、16ビットのセグメントセレクタと、現在のタスクのTSSセグメントのディスクリプタ(不可視部分)全体が格納されています。この情報は、GDT内の現在のタスクのTSS記述子からコピーされます。プロセッサは、タスクレジスタTRの不可視部分を使用して、TSSセグメント記述子の内容をバッファリングします。

LTR命令とSTR命令は、それぞれタスクレジスタの可視部分、すなわちTSSセグメントのセレクタをロードおよびセーブするために使用されます。LTR命令は、特権レベル0のプログラムでのみ実行できます。LTR命令は、通常、システムの初期化時にTRレジスタの初期値（タスク0のTSSセグメントセレクタなど）をロードし、システム運用時には、タスク切り替え時にTRの内容を自動的に変更するために使用されます。

### 4.7.34 タスクゲート記述子

#### タスクゲート記述子は、図4-

27に示すように、タスクへの間接的な保護された参照を提供します。タスクゲート記述子は、GDT、LDT、またはIDTテーブルに格納することができます。

タスクゲート記述子のTSSセグメントセレクタフィールドは、GDT内のTSSセグメント記述子を指します。このTSSセグメントセレクタのRPLフィールドは使用されません。タスクゲート記述子のDPLは、タスク切り替え時のTSSセグメントへのアクセス制御に使用されます。プログラムがタスクゲートを介してタスクへの呼び出しやジャンプを行う場合、タスクゲートを指すゲートセレクタのCPLとRPLフィールドは、タスクゲートディスクリプタのDPL以下でなければなりません。なお、タスクゲートを使用する場合、ターゲットTSSセグメント記述子のDPLは無視されます。

プログラムは、タスクゲート記述子またはTSSセグメント記述子を介してタスクにアクセスできます。図4-

36は、LDT、GDT、IDTテーブルのタスクゲートがすべて同じタスクを指している様子を示しています。

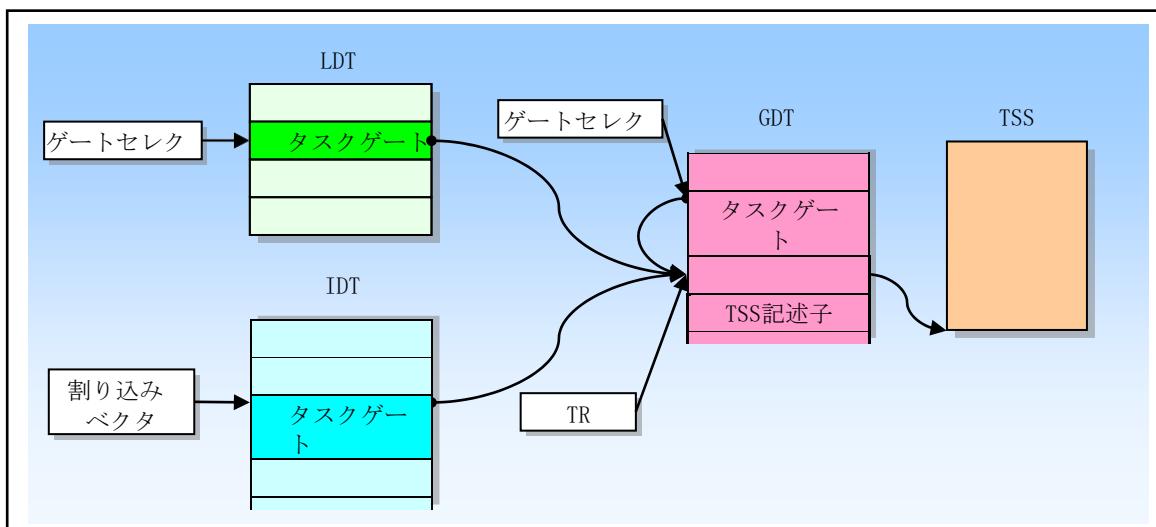


図4-36 同じタスクを参照するタスクゲート

#### 4.7.4 タスクの切り替え

プロセッサは、4つのケースのいずれかで、他のタスクに実行を移します。

1. 現在のプログラムまたはタスクが、GDT内のTSS記述子に対するJMPまたはCALL命令を実行します。
2. 現在のプログラムまたはタスクが、GDTまたは現在のLDT内のタスクゲート記述子へのJMPまたはCALL命令を実行する。
3. 割り込みや例外のベクターは、IDTテーブルのタスクゲート記述子を指します。
4. EFLAGSレジスタのNTフラグが設定されている場合、現在のタスクはIRET命令を実行します。

JMP命令、CALL命令、IRET命令、そして割り込みや例外などは、いずれもプログラムを切り替えるための一般的なメカニズムです。タスクスイッチが行われるかどうかは、TSS記述子やタスクゲートの参照(タスクへの呼び出しやジャンプ時)、NTフラグの状態(INET命令実行時)などによって決まります。

タスク切り替えは、JMP命令やCALL命令でTSS記述子やタスクゲートに制御を移すことができます。同じ2つの方法を使うと、図4-

37のように、プロセッサは指定されたタスクに制御を移すことになります。

割り込みや例外のベクタ・インデックスがIDTのタスク・ゲートである場合、割り込みや例外はタスク・スイッチを引き起こします。しかし、ベクターインデックスがIDT内の割込みまたはトラップゲートである場合、タスクスイッチは発生しません。

割り込みサービスハンドラプロシージャは、常に中断されたプログラムやプロシージャに実行権を返すので、中断されたプログラムが他のタスクにある場合もあります。NTフラグがリセット状態の場合は、一般的な復帰動作を行います。NTフラグがセットされている場合は、復帰操作によりタスクの切り替えが行われます。切り替え先の新しいタスクは、割込みサービス手順TSSのTSSセレクタ(前タスクリンクフィールド)で指定されます。

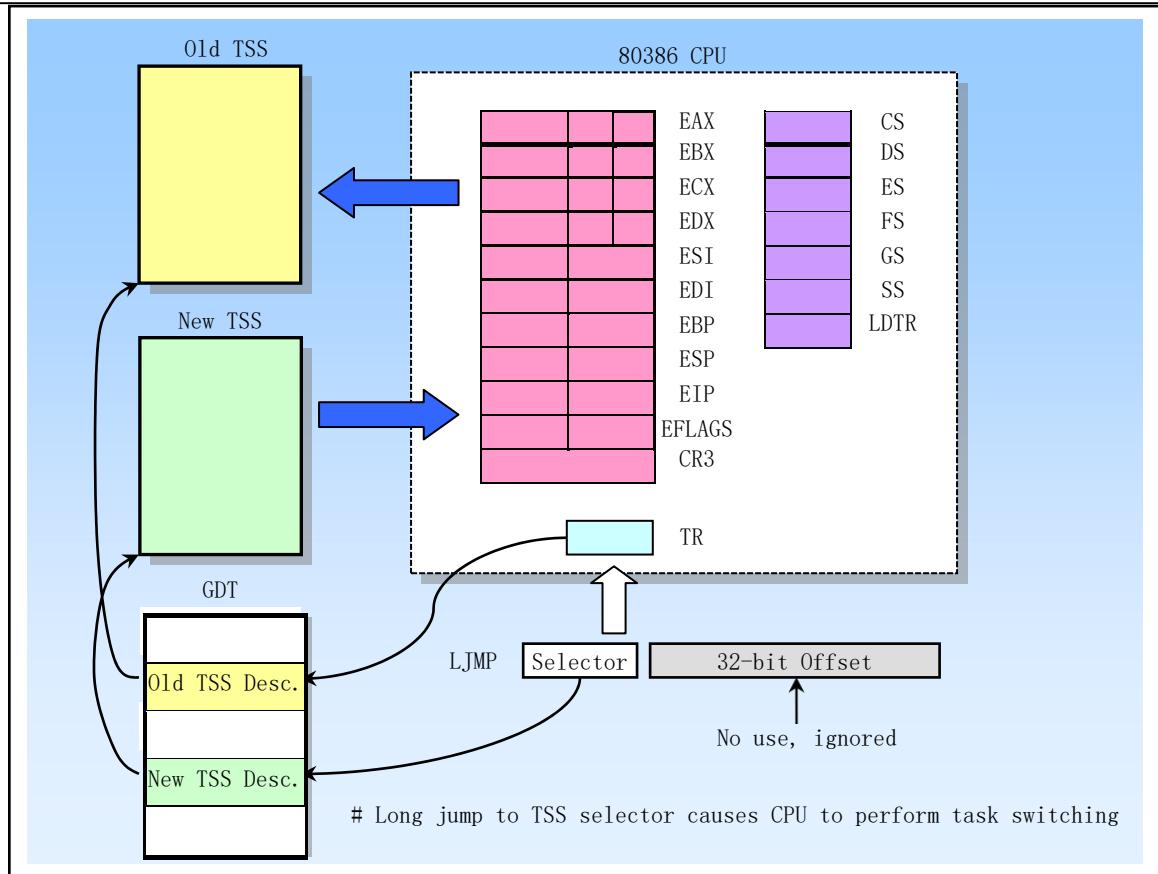


図4-37 タスク切り替え動作図

新しいタスクに切り替えるとき、プロセッサは次のような処理を行います。

1. 新しいタスクのTSSセグメントセレクタは、JMP命令やCALL命令のオペランド、タスクゲート、または現在のTSSの前タスクリンクフィールド（IRETによるタスク切り替えの場合）から取得します。
2. 現在のタスクが新しいタスクへの切り替えを許可されているかどうかをチェックします。JMP命令とCALL命令にデータ・アクセス・プリビレッジ・ルールを適用します。現在のタスクのCPL、および新しいタスクのセグメントセレクタのRPLは、参照されるTSS記述子またはタスクゲートのDPL以下でなければなりません。対象となるタスクゲートやTSS記述子のDPLに関わらず、例外、割り込み（INT n命令で生成される割り込みを除く）、IRET命令によってタスクの切り替えが可能です。INT n命令で生成された割り込みは、DPLを確認します。
3. 新しいタスクのTSS記述子が存在するとマークされていること（P=1）、制限が有効であること（0x67より大きいこと）を確認します。エラーを発生させる命令を実行しようとすると、プロセッサの状態に対するあらゆる変更が再開されます。これにより、例外ハンドラのリターン・アドレスは、エラー命令の次の命令ではなく、エラー命令を指すようになります。このため、例外ハンドラ・プロシージャは、エラー状態を処理して、タスクを再実行することができます。例外ハンドラ・プロシージャの介入は、アプリケーションからは完全に透過的です。
4. タスクスイッチがJMP命令やIRET命令で発生した場合、プロセッサは現在のタスク（旧タスク）のTSS記述子のビギーフラグBをリセットしますが、タスクスイッチがCALL命令や例外、割り込みで発生した場合、ビギーフラグBは変更されません。
5. タスクスイッチがIRET命令で開始された場合、プロセッサは一時的に保存されたEFLAGSイ

イメージ内のNTフラグをリセットします。タスクスイッチがCALL、JMP命令、または例外や割り込みで開始された場合、NTフラグは保存されたEFLAGSイメージ内で変更されません。

6. 現在の（古い）タスクの状態を、現在のタスクのTSSに保存します。プロセッサは、タスクレジスタから現在のタスクのTSSのベースアドレスを取得し、すべての汎用レジスタ、セグメントレジスタのセグメントセレクタ、フラグレジスタEFLAGS、命令ポインタEIPなどのレジスタの状態を現在のTSSにコピーします。
7. タスクの切り替えがCALL命令、例外、または割り込みで開始された場合、プロセッサは新しいタスクのTSSに格納されているEFLAGSイメージにNTフラグを設定し、IRET命令で開始された場合、プロセッサはスタックに格納されているEFLAGSイメージからNTフラグを復元します。JMP命令で開始された場合、NTフラグは変更されません。
8. タスクスイッチがCALL、JMP命令、または例外や割り込みによって開始された場合、プロセッサは新しいタスクTSS記述子にビギーフラグBを設定します。タスクスイッチがIRETによって生成された場合、Bフラグは変更されません。
9. 新しいタスクのTSSのセグメントセレクタとディスクリプタを使って、タスクレジスタTR（隠れた部分を含む）をロードする。新タスクのTSSに格納されているコントロールレジスタCR0の画像にTSフラグを設定する。
10. 新しいタスクのTSSステータスをプロセッサにロードします。これには、LDTRレジスタ、PDBR(CR3)レジスタ、EFLAGSレジスタ、EIPレジスタ、および汎用レジスタとセグメントセレクタが含まれます。この間に検出されたエラーは、新しいタスクのコンテキストに表示されます。
11. 新しいタスクの実行を開始します。(例外ハンドラには、新しいタスクの最初の命令が実行されていないように見える)

タスク切り替え動作が正常に行われると、現在実行中のタスクの状態が常に保存されます。タスクが実行を再開すると、保存されたEIPが指す命令から実行され、すべてのレジスタはタスクが中断されたときの値に復元されます。

タスクスイッチを行う際、新しいタスクの特権レベルは、元のタスクの特権レベルとは関係ありません。新しいタスクは、TSSからロードされたCSレジスタのCPLフィールドで指定された特権レベルで実行を開始します。各タスクは、独立したアドレス空間とTSSセグメントによって互いに分離されており、特権レベルのルールによってTSSへのアクセスがすでに制御されているため、ソフトウェアはタスク切り替え時に特権レベルのチェックを行う必要はありません。

コントロールレジスタCR0のタスク切り替えフラグTSは、タスクが切り替わるたびにセットされます。このフラグは、システムソフトウェアにとって非常に有用です。システム・ソフトウェアは、プロセッサと浮動小数点コプロセッサの間の操作を調整するために、TSフラグを使用することができます。TSフラグは、コプロセッサ内のコンテキストが現在のタスクのコンテキストとは異なる可能性があることを示します。

## 4.7.5 タスク連携

TSSの前タスクリンクフィールド(Backlink)とEFLAGSのNTフラグは、実行を前のタスクに戻すために使われます。NTフラグは、現在実行中のタスクが他のタスクの実行中に入れ子になっているかどうかを示し、現在のタスクの前タスクリンクフィールドには、入れ子の階層に上位のタスクがあれば

、そのタスクのTSSセレクタが保持されています（図4-38参照）。

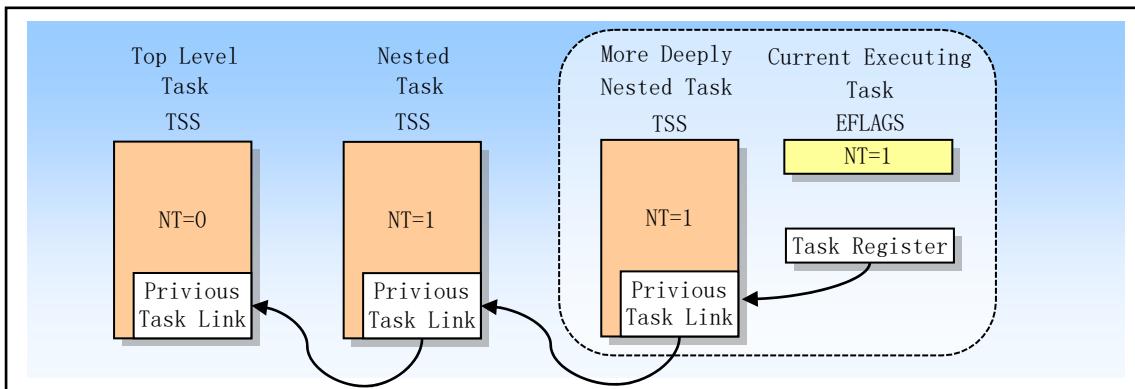


Figure 4-38 Nested Tasks

CALL命令や割込み、例外によってタスクスイッチが発生すると、プロセッサは現在のTSSセグメントのセレクタを新しいタスクTSSセグメントの前タスクリンクフィールドにコピーし、EFLAGSにNTフラグを設定します。NTフラグは、保存されたTSSセグメントのセレクタがTSSの前タスクリンクフィールドに保存されていることを示します。ソフトウェアがIRET命令を使って新しいタスクをサスペンドした場合、プロセッサは前タスクリンクフィールドの値とNTフラグを使って前のタスクに戻ります。つまり、NTフラグが設定されている場合、プロセッサは前タスクリンクフィールドで指定されたタスクに切り替えて実行します。

なお、JMP命令によるタスク切り替えの場合は、新しいタスクは入れ子になりません。つまり、NTフラグは0になり、前タスクのリンクフィールドは使用されません。JMP命令はネスティングが望まれないタスク切り替えに使用されます。

タスク切り替え時のビギーフラグB（TSSセグメントディスクリプター内）、NTフラグ、前タスクリンクフィールド、TSフラグ（CR0内）の使用方法を表4-10にまとめました。どのような特権レベルで実行されているプログラムでもNTフラグを変更することができるので、どのようなプログラムでもNTフラグを設定してIRET命令を実行することができることに注意してください。この方法では、プロセッサは現在のタスクTSSの前タスクリンクフィールドで指定されたタスクを実行することになります。このような偽造されたタスク切り替えの実行を成功させないために、オペレーティングシステムは、各TSSのこのフィールドを0に初期化する必要があります。

Table 4-10 Effects of a task switch on Busy flag, NT flag, previous task link field, and TS flag

Flag or Field	Effect of JMP	Effect of CALL or Interrupt	Effect of IRET
Busy (B) flag of new task.	Flag is set. Must have been clear before.	Flag is set. Must have been clear before.	No change. Must have been set.
Busy flag of old task.	Flag is cleared.	No change. Flag is currently set.	Flag is cleared.
NT flag of new task.	No change.	Flag is set.	Restored to value from TSS of new task.
NT flag of old task.	No change.	No change.	Flag is cleared.
Previous task link field of new task.	No change.	Loaded with selector for old task's TSS	No change.
Previous task link filed of old task.	No change.	No change.	No change.
TS flag in CR0	Flag is set.	Flag is set.	Flag is set.

## 4.7.6 タスクのアドレス空間

タスクのアドレス空間は、タスクがアクセスできるセグメントで構成されています。これらのセグメントには、TSS

で参照されるコード、データ、スタックとシステムセグメント、およびタスクコードがアクセスする他のセグメントが含まれます。これらのセグメントは、プロセッサのリニアアドレス空間にマッピングされた後、プロセッサの物理アドレス空間にマッピングされます（直接またはページングによって）。

TSSのLDTフィールドを使うと、各タスクに独自のLDTを与えることができます。あるタスクに対して、そのタスクに関連するすべてのセグメント記述子をLDTに入れることで、そのタスクのアドレス空間を他のタスクから分離することができます。もちろん、複数のタスクが同じLDTを使用することも可能です。これは、システム全体の保護バリアを捨てることなく、特定のタスクが相互に通信したり制御したりすることを可能にする、シンプルで効果的な方法です。すべてのタスクがGDTにアクセスできるため、このテーブルを介してアクセスされる共有セグメントを作成することも可能です。

ページング機構が有効な場合、TSSのCR3レジスタ（PDBR）フィールドにより、各タスクはリニアアドレスを物理アドレスにマッピングするための独自のページテーブルセットを持つこともできます。また、複数のタスクが同じページテーブルを共有することもできます。

### 4.7.6.1 リニアおよび物理アドレス空間へのタスクのマッピング

タスクをリニアアドレス空間と物理アドレス空間にマッピングするには2つの方法があります。

- すべてのタスクは、物理アドレス空間へのリニアなマッピングを共有しています。この方法は、ページング機構が有効になっていない場合にのみ使用できます。ページングがオンになっていないときは、すべてのリニアアドレスが同じ物理アドレスにマッピングされます。ページング機構がオンになっている場合、すべてのページが单一のページディレクトリを使用することで、リニアから物理アドレス空間へのこのマッピングを使用することができます。デマンドページ仮想記憶技術がサポートされていれば、リニアアドレス空間は既存の物理アドレス空間のサイズを超えることができます。
- 各タスクは独自のリニアアドレス空間を持ち、物理アドレス空間にマッピングされます。このマッピング形式を利用して、各タスクに異なるページディレクトリを使わせることができる。

DBR（制御レジスタCR3）はタスクが切り替わるたびにロードされるため、各タスクは異なるページディレクトリを持つことができます。

異なるタスクのリニアアドレス空間は、全く異なる物理アドレスにマッピングすることができます。異なるページディレクトリのエントリ（テーブルエントリ）が異なるページテーブルを指し、そのページテーブルが物理アドレスの異なるページを指している場合、各タスクは物理アドレスを共有することはありません。

タスクのリニアアドレス空間をマッピングするいずれの方法においても、すべてのタスクのTSSは共有の物理アドレス空間領域に格納されている必要があります、すべてのタスクはこの領域にアクセスすることができます。プロセッサがタスクスイッチングを行うためには

で、TSSの読み出しや更新時にTSSのアドレスマッピングが変わらない場合は、このマッピング方法が必要です。また、GDTによってマッピングされたリニアアドレス空間は、共有された物理アドレス空間にもマッピングされる必要があります。そうでないと、GDTの役割が失われてしまいます。

#### 4.7.6.2 タスクの論理的アドレス空間

タスク間でデータを共有するには、以下のいずれかの方法で、データセグメントの共有論理-物理アドレス空間マッピングを確立します。

- GDT 内のセグメント記述子を使用することで。すべてのタスクは、GDT 内のセグメント記述子にアクセスできなければなりません。GDT内のいくつかのセグメント記述子がリニアアドレス空間のセグメントを指しており、これらのセグメントがすべてのタスクが共有する物理アドレス空間にマッピングされている場合、すべてのタスクはそれらのセグメントのコードとデータを共有することができます。
- 共有の LDT を通じて。TSS の LDT フィールドが同じ LDT を指している場合、2 つ以上のタスクが同じ LDT を使用できます。共有 LDT の一部のセグメント記述子が物理アドレス空間の共通領域にマッピングされたセグメントを指している場合、LDT を共有するすべてのタスクは、それらのセグメントのすべてのコードとデータを共有できます。このような共有は、GDTによる共有よりも優れています。GDTによる共有では、共有対象が特定のタスクに限定されてしまうからです。システムには、これらの共有セグメントにアクセスできない他のタスクがあります。
- 異なるLDTのセグメント記述子は、リニアアドレス空間の共通アドレス領域にマッピングされます。このリニアアドレス空間の共通領域が、各タスクを物理アドレス空間の同じ領域にマッピングしている場合、これらのセグメント記述子によって、タスクはセグメントを共有することができます。このようなセグメント記述子は、しばしばエイリアスセグメントと呼ばれます。この共有方法は、LDT内の他のセグメント記述子が別々の共有されていないリニアアドレス領域を指し示すことができるため、上記の方法よりも優れています。

## 4.8 プロテクトモードの初期化

電源投入時やハードウェアリセット時には、プロセッサは8086互換の実アドレスモードで動作し、物理アドレス0xFFFFFFF0（通常はEPROM）から始まるソフトウェア初期化コードを実行します。ソフトウェア初期化コードでは、まず基本的なシステム機能の動作に必要なデータ構造情報を設定する必要があります。例えば、割り込みや例外を処理するリアルモードIDTテーブル（つまり、割り込みベ

クトルテーブル) などです。プロセッサがまだリアルモードで動作する場合、ソフトウェアはアプリケーションがリアルモードで確実に実行できるように、オペレーティング・システム・モジュールと対応するデータをロードしなければなりません。プロセッサがプロテクトモードで動作するのであれば、オペレーティング・システム・ソフトウェアは、モードの保護に必要なデータ構造情報をロードしてから、プロテクトモードに切り替える必要があります。

### 4.8.1 最初の命令が実行される

前述のとおり、ハードウェアリセット後に最初に取得・実行される命令は、物理アドレス0xFFFFF FF0にあります。このアドレスは、プロセッサの最上位物理アドレスの16バイト目にあたります。このアドレスは、通常、ソフトウェアの初期化コードを含むEPROMファームウェアが配置されているアドレス範囲です。

実アドレスモードでは、0xFFFFFFFF0というアドレスは、プロセッサの1MBアドレス可能範囲外です。プロセッサは以下の方法で開始アドレスに初期化します。CSレジスタには、目に見えるセグメントセレクタ部分と、目に見えないベース部分の2つの部分があります。実アドレスモードでは、ベースアドレスは通常、16ビットのセグメントセレクタの値を4ビット左にシフトして20ビットのベースアドレスを生成します。しかし、ハードウェアリセット時には、CSレジスタのセグメントセレクタは0xF000としてロードされ、ベースアドレスは0xFFFF0000としてロードされます。このため、開始アドレスはベースアドレスとEIPレジスタを足したものになります(つまり、0xFFFF0000 + 0xFFF0 = 0xFFFFFFFF0)。

ハードウェア・リセット後にCSレジスタが最初に新しい値をロードするとき、プロセッサは通常の実アドレスモードでのアドレス変換のルール(例:[CSベースアドレス=CSセグメントセレクタ\*16])を説明します。EPROMベースのソフトウェア初期化コードが完了するまで、CSレジスタのベースアドレスが変更されないようにするため、コードにファー・ホップやリモートコールを含めたり、割り込みを発生させたりしてはいけません(これによりCSセレクタの値が変化します)。

### 4.8.2 保護モード移行時の初期化動作

ハードウェアリセット後、プロセッサはリアルアドレスモードになります。一部の基本的なデータ構造とコードモジュールは、プロセッサのさらなる初期化をサポートするために、初期化中に物理メモリにロードする必要があります。プロテクトモードに必要なデータ構造の一部は、プロセッサのメモリ管理機能によって決定されます。プロセッサは、単一の統一されたアドレス空間のフラットモデルから、タスクごとに複数の保護されたアドレス空間を持つ高度に構造化されたマルチセグメントモデルまで使用可能なセグメントモデルをサポートしています。ページング機構は、一部がメモリ上にあり、一部がディスク上にある大規模なデータ構造情報を処理するために使用することができます。どちらの形式のアドレス変換でも、OSはメモリ管理ハードウェアに必要なデータ構造をメモリに設定する必要があります。したがって、プロセッサをプロテクトモードに切り替える前に、オペレーティング・システムのローディングおよび初期化ソフトウェア(bootsect.s, setup.s, head.s)は、まずプロテクトモードで使用するデータ構造の基本をメモリに設定する必要があります。これらのデータ構造には次のようなものがあります。

- プロテクトモードの割り込み記述子テーブルIDT。
- グローバルディスクリプター・テーブルGDTです。
- タスクステータスセグメントTSS。

- ローカルディスクリプターテーブルLDTのこと。
- ページングが有効な場合、少なくとも1つのページディレクトリと1つのページテーブルを設定する必要があります。
- プロセッサをプロテクトモードに切り替えるための実行コードを含むコードセグメント。
- 割り込みや例外ハンドラを含むモジュールをコード化する。

また、ソフトウェアの初期化コードで以下のシステムレジスタを設定しないと、プロテクトモードに切り替えることができません。

- グローバルディスクリプターテーブルベースアドレスレジスタ GDTR;
- インタラプトディスクリプターテーブルベースアドレスレジスタ IDTR。
- コントロールレジスタ CR1--CR3。

これらのデータ構造、コードモジュール、システムレジスタを初期化した後、CR0レジスタの保護モードフラグPE（ビット0）を設定することで、プロセッサを保護モードに切り替えることができます。

## 4.8.2.1 保護モードシステム構成表

ソフトウェアの初期化時にメモリに設定されるプロテクトモードのシステムテーブルは、主にオペレーティングシステムがサポートするメモリ管理のタイプに依存します（フラット、ページング付きフラット、セグメンテーション、ページング付きセグメンテーション）。

ページングのないフラットなメモリモデルを実装するためには、ソフトウェアの初期化コードで少なくとも1つのコードセグメントと1つのデータセグメントを持つGDTテーブルを設定する必要があります。もちろん、GDTテーブルの最初の項目には、ヌルデスクリプタも配置する必要があります。スタックは、通常の読み書き可能なデータセグメントに置くことができるので、特別なスタック記述子は必要ありません。また、ページング機構をサポートするフラットメモリモデルでは、ページディレクトリと少なくとも1つのページテーブルが必要です。GDTテーブルを使用する前に、LGDT命令を使用してGDTのベースアドレスとリミットをGDTRレジスタにロードする必要があります。

また、マルチセグメントモデルでは、OS用の追加セグメントのほか、アプリケーションごとのセグメントやLDTテーブルのセグメントが必要となります。LDTテーブルのセグメント記述子は、GDTテーブルに格納する必要があります。オペレーティングシステムの中には、アプリケーション用に新しいセグメントと新しいLDTセグメントを割り当てるものもあります。この方法は、Linuxのような動的なプログラミング環境に最大限の柔軟性をもたらします。

オペレーティング・システムを使用しています。プロセスコントローラーのような組み込みシステムでは、固定数のアプリケーション用に固定数のセグメントとLDTをあらかじめ割り当てておくことができ、リアルタイムシステムのソフトウェア環境構造を簡単かつ効率的に実現することができます。

## 4.8.2.2 プロテクトモードでの例外処理と割り込みの初期化

ソフトウェアの初期化コードでは、保護モードIDTを設定する必要があります。IDTには、少なくとも、プロセッサが生成する可能性のある各例外ベクターに対応するゲート記述子を含める必要があります。割り込みゲートやトラップゲートを使用する場合、ゲート記述子はすべて、割り込み処理や例外処理を含む同じコードセグメントを指すことができます。タスク・ゲートを使用する場合、タスク・ゲートを使用する各例外処理プロセスには、TSS

と関連するコード、データ、およびスタック・セグメントが必要です。ハードウェアが割込みを生成することを許可している場合、ゲート記述子は1つ以上の割込みハンドラのIDTに設定されなければなりません。

IDTテーブルのベースアドレスとリミットレンジスは、IDTを使用する前にLIDT命令でIDTRレジ

スタにロードする必要があります。

#### 4.8.23 ページングの初期化

ページング機構の設定は、コントロールレジスタCR0のPGフラグで行います。このフラグが0にクリアされると（ハードウェアリセット時の状態）、ページング機構はオフになります。PGフラグがセットされると、ページング機構はオンになります。PGフラグを設定する前に、以下のデータ構造およびレジスタを初期化する必要があります。

- ソフトウェアは、物理メモリ上に少なくとも1つのページディレクトリと1つのページテーブルを作成する必要があります。ページディレクトリテーブルに自分自身を指すエントリが含まれていれば、ページテーブルの使用をなくすることができます。この時点では、ページディレクトリテーブルとページテーブルは同じページに格納されています。
- ページディレクトリテーブルの物理ベースアドレスをCR3レジスタ（PDBRレジスタとも呼ばれる）にロードします。
- プロセッサはプロテクトモードになっています。他のすべての制限が満たされれば、PGフラグとPEフラグを同時に設定することができます。

互換性を保つために、PGフラグ（およびPEフラグ）を設定する際には、以下のルールを遵守する必要があります。

- PGフラグを設定する命令は、すぐにJMP命令に続くべきです。MOV CR0命令に続くJMP命令は、実行ストリームを変更するので、80X86プロセッサが取った命令やデコードした命令をクリアします。しかし、Pentium以上のプロセッサでは、分岐コードの向きにBTB（Branch Target Buffer）を使用しているため、分岐命令のキューを更新する必要がありません。
- ジャンプ命令JMPにPGフラグを設定するコードは、ピアマッピング上のページから来たものでなければなりません（つまり、ジャンプ前のリニアアドレスと、ページングをオンにした後の物理アドレスが同じであること）。

#### 4.8.24 マルチタスクの初期化

マルチタスク機構を使用する場合や、特権レベルの変更を許可する場合、ソフトウェアの初期化コードには、少なくとも1つのTSSと、それに対応するTSSセグメント記述子が必要です（特権レベル0、1、2のスタックセグメントポインタをTSSから取得する必要があるため）。TSS記述子にビジーのマークをつけない（ビジーフラグを立てない）。ビジーフラグは、タスクスイッチを行う際にプロセッサが設定するだけです。LDTセグメント記述子と同様に、TSS記述子もGDTに格納されています。

プロセッサがプロテクトモードに切り替わった後、LTR命令を使ってTSSセグメント記述子のセレクタをタスクレジスタTRにロードすることができます。この命令は、TSSをビジー（B = 1）としてマークしますが、タスクスイッチ操作は行いません。プロセッサはこのTSSを使って、特権レベル0、1、2のスタックを探すことができます。プロテクトモードでは、ソフトウェアが最初のタスクスイッチを実行する前に、TSSセグメントのセレクタを最初にロードする必要があります。

LTR命令の実行後、タスクレジスタに対する以降の操作は

タスクの切り替えを行います。他のセグメントやLDTと同様に、TSSやTSS記述子は事前に割り当てることも、必要に応じて割り当てることもできます。

### 4.8.3 モード切替

プロセッサをプロテクトモードで動作させるためには、実アドレスモードからのモード切り替え

を行う必要があります。いったんプロテクトモードに入ると、通常は実アドレスモードに戻る必要はありません。実アドレスモード用にプログラムされたプログラムを動作させるためには、通常、実モードに切り替えるよりも仮想8086モードで動作させた方が便利である。

### 4.8.3.1 プロテクトモードへの切り替え

プロテクトモードに切り替える前に、まず最低限のシステムデータ構造とコードモジュールをいくつかロードする必要があります。これらのシステムテーブルが作成されると、ソフトウェアの初期化コードをプロテクトモードに切り替えることができます。CR0レジスタのPEフラグをセットするMOV CR0命令を実行することで、プロテクトモードに入ることができます。(同じ命令で、CR0のPGフラグを使って、ページング機構を有効にすることができます)。プロテクトモードで動作しているとき、特権レベルCPLは0となります。

プログラムの互換性を確保するために、以下のように切り替え操作を行います。

1. 割り込みの無効化マスク可能なハードウェア割り込みはCLI命令で無効にできます。NMIはハードウェア回路によって無効化されます。同時に、ソフトウェアでは、モード切り替え動作中に例外や割り込みが発生しないようにする必要があります。
2. LGDT命令を実行し、GDTテーブルのベースアドレスをGDTRレジスタにロードする。
3. コントロールレジスタCR0にPEフラグ (PGフラグは任意設定) を設定するMOV CR0命令を実行します。
4. MOV CR0 命令の直後にファージャンプ JMP 命令またはファーコール CALL 命令を実行します。この操作は通常、命令ストリームの次の命令へのファージャンプ、または次の命令からのファーコールとなります。
5. ローカルディスクリプターテーブルを使用する場合は、LLDT命令を実行してLDTセグメントセレクタをLDTRレジスタにロードします。
6. LTR命令を実行して、タスクレジスタTRに初期プロテクトモードタスクのセグメントセレクタまたは書き込み可能なメモリ領域のセグメントディスクリプタをロードします。この書き込み可能なメモリ領域は、タスクの切り替え時にタスクのTSS情報を格納するために使用されます。
7. プロテクトモードに入っても、セグメントレジスタには実アドレスモードの内容が残っています。手順 4 の JMP または CALL 命令で CS レジスタがリセットされます。残りのセグメント・レジスタの内容を更新するには、以下のいずれかを行います。(1)レジスタDS、SS、ES、FS、GSをリロードします。ES、FS、GSレジスタを使用しない場合は、ヌルセレクタでロードします。(2)新規タスクでJMPやCALL命令を実行すると、自動的にセグメントレジスタの値がリセットされ、新規コードセグメントに分岐します。
8. LIDT命令を実行し、プロテクトモードIDTテーブルのベースアドレスとリミットをIDTRレジスタにロードする。
9. STI 命令を実行してマスク可能なハードウェア割り込みをオンにし、NMI 割り込みをオンにするために必要なハードウェア操作を行います。

さらに、MOV

CR0命令の直後にJMPまたはCALL命令を実行すると、実行の流れが変わります。ページング機構が有効な場合、MOV

CR0命令とJMPまたはCALL命令の間のコードは、ピアマッピング上のページからのものでなければなりません (つまり、ジャンプ前のリニアアドレスとページング後の物理アドレスは同じです)。JMPま

たはCALL命令がジャンプするターゲット命令は、ピアマッピングのページにある必要はありません。

### 4.8.3.2 リアルアドレスモードへの切り替え

実アドレスモードに戻したい場合は、MOV

CR0命令でコントロールレジスタCR0のPEフラグをクリアします。実アドレスモードに戻す処理は、以下の手順で行います。

1. 割り込みの無効化マスク可能なハードウェア割り込みはCLI命令で無効にできます。NMIはハードウェア回路によって無効化されます。同時に、ソフトウェアでは、モード切り替え動作中に例外や割り込みが発生しないようにする必要があります。
2. ページング機構が有効になっている場合は、実行する必要があります。
  - プログラム制御をピアマップのリニアアドレスに転送する（つまり、リニアアドレスは物理アドレスと等しい）。
  - GDTとIDTがピアマップされたページにいることを確認する。
  - CR0のPGフラグをクリアします。
  - CR3レジスタで0x00に設定すると、TLBバッファがリフレッシュされます。
3. プログラムの制御を長さ64KB（0xFFFF）の読み出し可能なセグメントに移す。このステップでは、リアルモードで要求されるセグメント制限を使用してCSレジスタをロードします。
4. SS、DS、ES、FS、GSの各セグメント・レジスタを、以下の設定値を持つディスクリプターを指すセレクタでロードします。
  - Limit = 64KBytes (0xFFFF)となります。
  - バイトグラニュラリティ (G=0)。
  - 拡大する (E=0)。
  - 書き込み可能 (W=1)。
  - 現在 (P=1)。
5. LIDT命令を実行して、1MBリアルモードアドレス範囲のリアルアドレスモード割り込みテーブルを指すようにします。
6. CR0のPEフラグをクリアして、リアルアドレスモードに切り替えます。
7. ファー・ジャンプ命令を実行し、リアル・モード・プログラムにジャンプする。このステップでは、命令キューが更新され、CSレジスタに適切なベースアドレスとアクセス値がロードされます。
8. SS、DS、ES、FS、GSの各レジスタは、実アドレスモードのコードに必要なだけロードされます。リアルアドレスモードで使用しないレジスタがある場合は、0を書き込んでください。
9. STI命令を実行してマスク可能なハードウェア割り込みをオンにし、NMI割り込みをオンにするために必要なハードウェア操作を行います。

## 4.9 シンプルなマルチタスク・カーネルの例

本章では、本章と前章のまとめとして、シンプルなマルチタスク・カーネルの設計と実装について完全に説明します。このカーネル例には、2つの特権レベル3のユーザータスクと、特権レベル0のシステムコール割り込み手続きが含まれています。まず、この単純なカーネルの基本構造とロード動作の基本原理を説明し、次にマシンのRAMメモリにロードする方法と、2つのタスクを切り替える方法を説

明します。最後に、この単純なカーネルを実装するためのソースコードとして、ブートと保護モードマルチタスクカーネルプログラム `head.s` を示します。

`boot.s``as`

### 4.9.1 マルチタスクプログラムの構造と動作原理

この章で紹介するカーネルの例は、2つのソースファイルから構成されています。一つはas86言語でコンパイルされたブートローダ`boot.s`で、コンピュータシステムの電源を入れたときに起動ディスクからカーネルコードをメモリにロードするのに使われます。もう一つはGNU assembly言語でコンパイルされたカーネルプログラム`head.s`です。これは

特権レベル3で動作する2つのタスクがクロック割り込みの制御下で相互に切り替わることを実装し、さらに画面に文字を表示するシステムコールを実装しています。

この2つのタスクをタスクAとタスクB（またはタスク0とタスク1）と呼ぶことにします。タスクAとタスクBは、それぞれシステムコールを呼び出して画面に文字「A」と「B」を表示し、10ミリ秒ごとに別のタスクに切り替わります。タスクAは常にシステムコールを呼び出して画面に文字'A'を表示し、タスクBは常に文字'B'を表示します。このカーネルインスタンスプログラムを終了させるには、マシンを再起動するか、実行中の模擬PC実行環境ソフトウェアを終了させる必要があります。

`boot.s`プログラムは、図4-39に示すように、フロッピーディスクやイメージファイルの第1セクターに格納される、合計512バイトのコードを生成します。PCの電源が入ると、ROM BIOSのプログラムは、ブートディスクの第1セクターを物理メモリ0x7c00（31KB）の位置の先頭にロードし、実行制御を0x7c00に移してブートコードの実行を開始します。

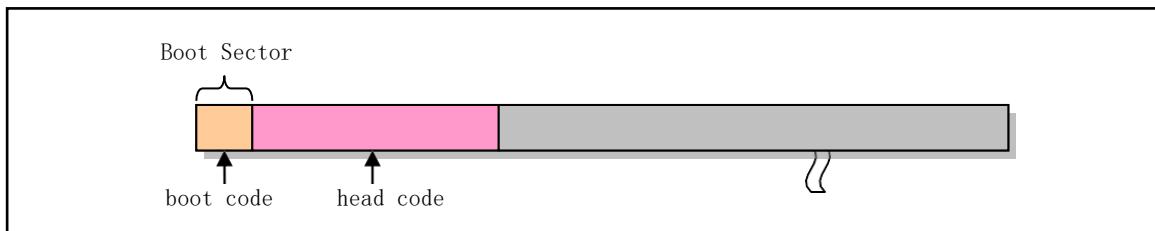


Figure 4-39 Floppy disk image file

ブートプログラムの主な機能は、フロッピーディスクやイメージファイル内のヘッドカーネルコードをメモリ内の指定された場所にロードすることです。一時的なGDTテーブルなどを設定した後、プロテクトモードで動作するようにプロセッサを設定します。その後、ヘッドコードにジャンプしてカーネルコードを実行します。実際には、`boot.s`プログラムは、まずROM BIOS割り込みint 0x13を利用して、フロッピーディスク内のヘッドコードをメモリ位置0x10000（64KB）の先頭に読み込んだ後、ヘッドコードをメモリ位置0の先頭に移動させ、最後にコントロールレジスタCR0の保護動作モード有効フラグをセットして、メモリ位置0にジャンプしてヘッドコードの実行を開始します。ブートコードがメモリ内のヘッドコードを移動する様子を図4-40に示します。

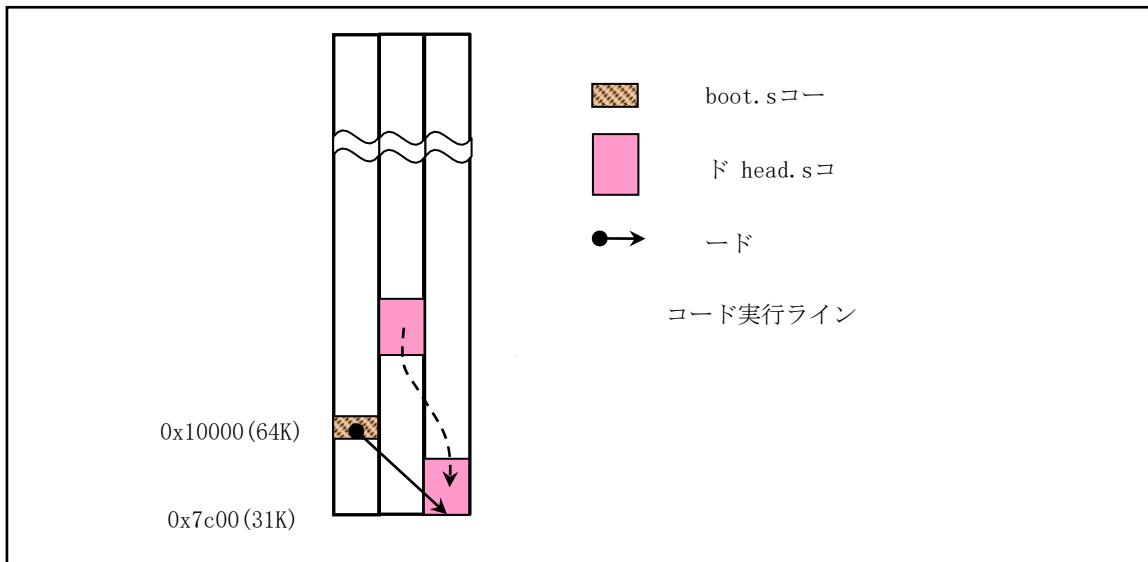


図4-40 物理メモリ上でのカーネルコードの移動・分散の様子

ヘッドのカーネルコードを物理メモリ0の先頭に移動させる主な理由は、GDTテーブルの設定が簡単なので、ヘッド.sのプログラムをできるだけ短くすることもできるからです。しかし、ブートプログラムでフロッピーやイメージファイルからメモリ0番地に直接ヘッドコードをロードさせることはできません。なぜなら、BIOSが使用する割り込みベクトルテーブルがメモリ0番地の先頭にあり、ロード操作にはROM BIOSが提供する割り込みプロセスを使用する必要があるからです。そのため、ヘッドコードをメモリ0に直接ロードすると、BIOSの割り込みベクターテーブルが破壊されてしまいます。

もちろん、ヘッドコードをメモリ0x10000にロードしてから、直接ヘッドコードを実行する場所にジャンプすることも可能です。この方法によるソースプログラムは、以下に説明するようにoldlinux.orgのサイトからダウンロードできます。

ヘッドプログラムは32ビットのプロテクトモードで動作し、主に初期設定のコード、クロック割り込みint0x08のプロセスコード、システムコール割り込みint0x80のプロセスコード、タスクAとタスクBのコードとデータが含まれています。(1)GDTテーブルのリセット、(2)システムタイマチップの設定、(3)IDTテーブルのリセットとクロックおよびシステムコール割り込みゲートの設定、(4)タスクAの実行への移行。仮想アドレス空間において、head.sプログラムのカーネルとタスクのコード割り当て図を図4-41に示す。実際には、このカーネルの例では、コードとデータのセグメントはすべて物理メモリの同じ領域、つまり物理メモリから始まる領域に対応しています。

location 0.

GDT内のグローバルコードセグメントとデータセグメントディスクリプターの内容は以下のように設定されています。

- ベースアドレスは0x0000です。
  - セグメントの制限値は0x07ffです。粒度は1なので、実際のセグメント長は8MBです。
- グローバル表示データセグメントの設定は以下の通りです。
- ベースアドレスは0xb8000です。
  - セグメントリミット長は0x0002なので、実際のセグメント長は表示メモリ領域に対応する8KBとなります。

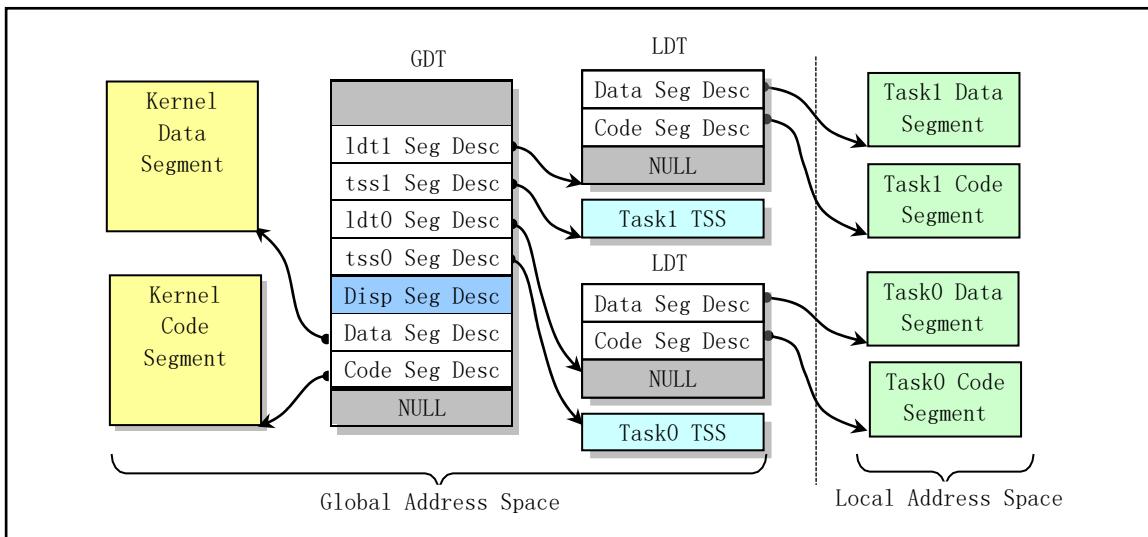


Figure 4-41 Diagram of the allocation of kernel and tasks in the virtual address space

また、両タスクのLDTにおけるコード・セグメントとデータ・セグメントの記述子の内容は、以下のように設定されています。

- ベースアドレスは0x0000です。
- セグメント長は0x03ffで、実際のセグメント長は4MBです。

したがって、リニアアドレス空間では、この「コア」のコードとデータのセグメント、およびタスクのコードとデータのセグメントは、リニアアドレス0から始まり、ページング機構を使用していないので、すべて物理アドレス0の先頭に直接対応しています。ヘッドプログラムがコンパイルしたオブジェクトファイルとその結果のフロッピーアイメージファイルでは、コードとデータの構成は図4-42のようになっています。

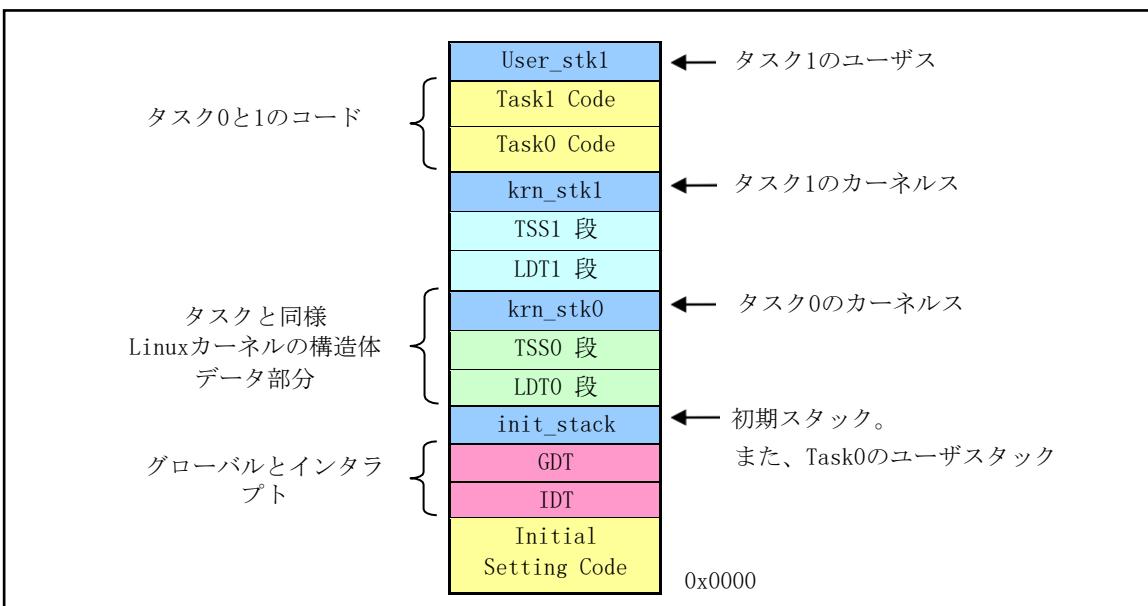


Figure 4-42 Kernel image file and in-memory head code and data diagram

特権レベル0のコードを特権レベル3のコードに直接転送することはできません。

が、制御の受け渡しは、割込み復帰命令を使うことで実現できます。そこで、GDT、IDT、タイミングチップが初期化されると、割り込み復帰命令IRETを使って最初のタスクを開始します。

具体的な実装方法としては、初期スタックのinit\_stackに手動でリターン環境を設定します。すなわち、タスク0のTSSセグメントセレクタをタスクレジスタLTRにロードし、LDTセグメントセレクタをLDTRにロードした後、タスク0のユーザースタックポインタ（0x17 : init\_stack）、コードポインタ（0x0f : task0））、フラグレジスタの値をスタックにpushし、割込み復帰命令IRETを実行します。

IRET命令は、スタック上のスタックポインタをタスク0ユーザースタックポインタとしてポップし、仮想タスク0フラグレジスタの内容を復元し、スタック内のコードポインタをCS:EIPレジスタにポップすることで、タスク0コードの実行を開始する。これで、特権レベル0のコードから特権レベル3のコードへの制御移行が完了します。

実行中のタスクを10ミリ秒ごとに切り替えるためには、10ミリ秒ごとにクロック割り込み要求信号を割り込み制御チップ8259Aに送るように、ヘッド.sプログラムでタイマチップ8253のチャネル0を設定しています。PCの電源投入時には、ROM BIOSプログラムによってクロック割り込み要求信号が8259Aの割り込みベクタ8に設定されているので、割り込み8ハンドラプロシージャでタスク切り替え操作を行う必要があります。タスク切り替えの方法は、変数currentの現在実行中のタスク番号を見て実行します。currentが0であれば、タスク1のTSSセレクタをオペランドにしてファージャンプ命令を実行することで、タスク1に切り替えて実行し、そうでなければその逆となります。

各タスクは、まず文字のASCIIコードをレジスタALに入れ、システム割り込みをかけてint 0x80を呼び出します。システムコールの処理プロセスでは、単純な文字書き込み画面のサブルーチンを呼び出し、レジスタALの文字を画面に表示し、文字を表示した画面の次の位置を次回の文字表示の画面位置として記録します。文字が表示された後、タスクコードはloop文を使って一定時間遅延させ、タスクコードの先頭にジャンプして、10ミリ秒の時限割り込みが発生するまでループを続けます。この時点でコードは別のタスクに切り替えて実行されます。タスクAの場合、文字'A'は常にレジスタALに格納され、タスクBの実行中は文字'B'が常にALに格納されます。したがって、プログラムが実行されているときには、図4-43のように、一連の文字'A'と一連の文字'B'が間隔をおいて連続的に画面に表示されることになります。

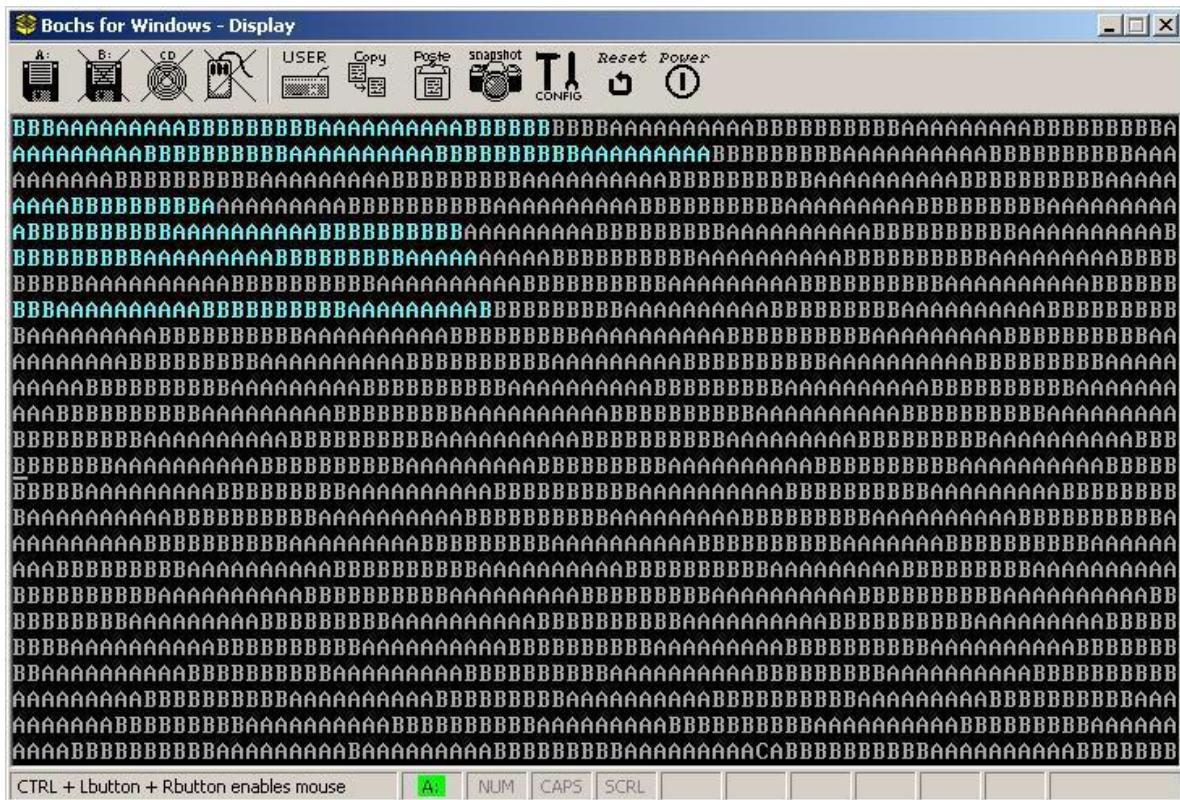


図 4-43 シンプルなカーネル実行画面の表示

図4-43は、この実行中のカーネルをBochsに表示した画面です。注意深い読者は、図の一番下の行に「C」という文字が表示されていることに気づくでしょう。これはPCが誤ってクロック割込みやシステムコール割込みではない別の割込みを発生させたためです。なぜなら、プログラムの中で他の割り込みに対してデフォルトの割り込みハンドラを設置しているからです。別の割り込みが発生すると、システムは文字'C'を表示するコードを含むデフォルトの割り込みハンドラを実行しますので、画面に文字'C'が表示され、割り込みが終了します。

boot.sプログラムとhead.sプログラムの詳細なコメントは以下の通りです。このシンプルなカーネルサンプルのコンパイルと動作については、本書の最終章にある「シンプルなカーネルサンプルプログラムのコンパイルと動作」の項を参照してください。

## 4.9.2 ブートスタートアッププログラム **boot.s**

プログラムができるだけシンプルにするために、このブートローダは16セクタ以下のヘッドコードしかロードできず、ROM BIOSが設定した割り込みベクタ番号を直接使用します。つまり、タイマー割り込み要求番号の割り込み番号は8のままでです。これは、Linuxシステムで使われているものとは異なります。Linuxシステムでは、カーネルの初期化時に8259A割り込み制御チップをリセットし、クロック割り込み要求信号を割り込み0x20にマッピングします。詳しくは「カーネルブートプログラム」の章をご覧ください。

---

```

01 ! boot.s program
02 ! First use BIOS interrupt to load head code into memory 0x10000, and then move it to memory 0.
03 ! Finally enter protected mode, jump to the beginning of head code at 0 to continue running.
04 BOOTSEG = 0x07c0           ! This program is loaded into memory at 0x7c00 by BIOS.
05 SYSSEG  = 0x1000           ! The head is first loaded to 0x10000 and moved to 0x0.
06 SYSLEN  = 17               ! Max num of disk sectors occupied by the kernel.
07 entry start
08 start:
09     jmpi    go, #BOOTSEG      ! Jump between segments to 0x7c0:go. All segment reg
10    go:     mov    ax, cs        ! are 0 when runs. This jump ins load CS with 0x7c0.
11    mov    ds, ax        ! Both DS and SS point to the 0x7c0 segment.
12    mov    ss, ax
13    mov    sp, #0x400       ! Set temp stack pointer. Its value needs to be larger
14                           ! than this program and has a certain space.
15 ! Load the kernel code to the beginning of memory at address 0x10000.
16 load_system:
17    mov    dx, #0x0000       ! Use BIOS int 0x13 func2 to load head code from bootdisk.
18    mov    cx, #0x0002       ! DH-head no; DL-drive no; CH-10 bit track no low 8 bits
19    mov    ax, #SYSSEG        ! CL-Bits7,6 track num high 2 bits ,bit 5-0 start sector
20    mov    es, ax        ! ES:BX - Read in buffer location (0x1000:0x0000).
21    xor    bx, bx        ! AH-read sector func num; AL- num of sectors read (17).
22    mov    ax, #0x200+SYSLEN
23    int    0x13
24    jnc    ok_load        ! If no error occurs, then continues, otherwise dead.
25 die:   jmp    die
26
27 ! Move kernel code to memory location 0. Total of 8KB bytes are moved (kernel code <8kb).
28 ok_load:
29    cli                  ! Disable interrupts.
30    mov    ax, #SYSSEG        ! Move from DS:SI(0x1000:0) to ES:DI(0:0).
31    mov    ds, ax
32    xor    ax, ax
33    mov    es, ax
34    mov    cx, #0x1000       ! Set the move 4K times, one word at a time.
35    sub    si, si
36    sub    di, di
37    rep    movw            ! Execute the repeat move instruction.
38 ! Load IDT and GDT base address registers IDTR and GDTR.
39    mov    ax, #BOOTSEG
40    mov    ds, ax        ! Let DS point to 0x7c0 segment again.
41    lidt   idt_48        ! Load IDTR. 2 byte table limit, 4 byte linear base addr.
42    lgdt   gdt_48        ! Load GDTR. 2 byte table limit, 4 byte linear base addr.
43
44 ! Set CR0 to enter protection mode. The seg selector value 8 refers to 2nd descriptor in GDT.
45    mov    ax, #0x0001       ! Set the protection mode flag PE (bit 0) in CR0.
46    lmsw   ax                  ! Jump to segment specified by the selector, offset 0.
47    jmpi   0, 8               ! Seg value is now a selector. The linear base addr is 0.
48
49 ! The following is the content of GDT. It has 3 seg descriptors. The first one is not used,
! the other two are code and data segment descriptors.
50 gdt:   .word  0, 0, 0, 0      ! First descriptor not used. Occupies 8 bytes.
51

```

---

```

52      .word 0x07FF          ! Descriptor 1. 8Mb - limit=2047 (2048*4096=8MB).
53      .word 0x0000          ! Segment base address = 0x00000.
54      .word 0x9A00          ! Code segment, readable/executable.
55      .word 0x00C0          ! Segment attribute granularity = 4KB, 80386.

56
57      .word 0x07FF          ! Descriptor 1. 8Mb - limit=2047 (2048*4096=8MB).
58      .word 0x0000          ! Segment base address = 0x00000.
59      .word 0x9200          ! Data segment, readable and writable.
60      .word 0x00C0          ! Segment attribute granularity = 4KB, 80386.

61 ! The following are the 6-byte operands of the LIDT and LGDT instructions, respectively.
62 idt_48: .word 0           ! The IDT table length is 0.
63      .word 0,0             ! The linear base address of IDT table is also zero.
64 gdt_48: .word 0x7ff        ! GDT limit is 2048 bytes, can hold 256 descriptors.
65      .word 0x7c00+gdt,0   ! Linear base of GDT is at offset gdt of seg 0x7c0.
66 .org 510
67      .word 0xAA55          ! Boot sector flag. Must be at last 2 bytes of boot sector.

```

---

### 4.9.3 マルチタスク・カーネル・プログラム・ヘッド.s

保護モードに入った後、head.sのプログラムがIDTテーブルとGDTテーブルを再設定して設定する主な理由は、プログラムの構造を明確にすることと、Linux 0.12カーネルのソースコードにある2つのテーブルの設定との整合性をとるためです。もちろん、このプログラムでは、boot.sで設定されたIDTテーブルとGDTテーブルの位置をそのまま利用して、適切なディスクリプター項目を記入することができます。

---

```

01 # Head.s contains code for 32-bit protected mode init, clock & system call interrupts, and two
02 # tasks code. After initialization, the program moves to task 0 to start execution, and the
# switching operation between tasks 0 and 1 is performed under the clock interrupt.
03 LATCH      = 11930          # Timer count, interrupt is sent every 10 ms.
04 SCRN_SEL   = 0x18           # The segment selector for the screen display memory.
05 TSS0_SEL   = 0x20           # TSS segment selector for task 0.
06 LDTO_SEL   = 0x28           # LDT segment selector for task 0.
07 TSS1_SEL   = 0X30           # TSS segment selector for task 1.
08 LDT1_SEL   = 0x38           # LDT segment selector for task 1.
09 .text
10 startup_32:
11 # First load DS, SS, and ESP. The linear base address of all segments is 0.
12     movl $0x10,%eax          # 0x10 is the data segment selector in the GDT.
13     mov %ax,%ds
14     lss init_stack,%esp
15 # Re-set the IDT and GDT tables at new location.
16     call setup_idt          # Setup IDT.
17     call setup_gdt          # Setup GDT.
18     movl $0x10,%eax          # Reload all segment registers after changing GDT.
19     mov %ax,%ds
20     mov %ax,%es
21     mov %ax,%fs
22     mov %ax,%gs
23     lss init_stack,%esp
24 # Set 8253 timing chip. Channel 0 is set to generate an interrupt request every 10 ms.
25     movb $0x36, %al          # Control word: Channel 0 in mode 3, Count in binary.

```

```

26      movl $0x43, %edx          # 0x43 is write port of control word register.
27      outb %al, %dx
28      movl $LATCH, %eax        # Init count set to LATCH (1193180/100), freq. 100HZ.
29      movl $0x40, %edx          # The port of channel 0.
30      outb %al, %dx          # Write initial count value to channel 0 in two steps.
31      movb %ah, %al
32      outb %al, %dx
33 # Set the timer interrupt gate descriptor at item 8 of the IDT table.
34      movl $0x00080000, %eax    # EAX high word set to kernel code seg selector 0x0008.
35      movw $timer_interrupt, %ax # Set timer int gate descriptor. Get handler address.
36      movw $0x8E00, %dx          # Interrupt gate type is 14, plevel is 0 or hardware used.
37      movl $0x08, %ecx          # Clock interrupt vector no. set by BIOS is 8.
38      lea idt(%ecx,8), %esi    # Put IDT Descriptor 0x08 address into ESI and set it.
39      movl %eax, (%esi)
40      movl %edx, 4(%esi)

# Set the system call trap gate descriptor at item 128 (0x80) of the IDT table.
41      movw $system_interrupt, %ax # Set system call gate descriptor. Get handler address.
42      movw $0xef00, %dx          # Trap gate type is 15, code of plevel 3 is executable.
43      movl $0x80, %ecx          # System call vector no. is 0x80.
44      lea idt(%ecx,8), %esi    # Put IDT Descriptor 0x80 address into ESI and set it.
45      movl %eax, (%esi)
46      movl %edx, 4(%esi)

47 # Now, to use IRET to move to task 0 (A), we manually prepare to setup the stack contents.
# See Figure4-29 for the stack contents we need to setup. Refer to include/asm/system.h.
48      pushfl                  # Reset NT flag in EFLAGS to disable task switch when
49      andl $0xfffffbfff, (%esp) # execute IRET instruction.
50      popfl
51      movl $TSS0_SEL, %eax      # Load task0's TSS seg selector into task register TR.
52      ltr %ax
53      movl $LDTO_SEL, %eax      # Load task0's LDT seg selector into LDTR.
54      lldt %ax                # TR and LDTR need only be manually loaded once.
55      movl $0, current          # Save current task num 0 into current variable.
56      sti                      # Enable int, build a scene on stack for int returns.
57      pushl $0x17                # Push task 0 data (stack) seg selector onto stack.
58      pushl $init_stack          # Push the stack pointer (same as push ESP).
59      pushfl                  # Push the EFLAGS.
60      pushl $0x0f                # Push current local space code seg selector.
61      pushl $task0                # Push task 0 code pointer onto stack.
62      iret                     # This causes execution moves to task0 in plevel 3.
63

64 # The following are the subroutines for setting descriptor items in GDT and IDT.
65 setup_gdt:                   # GDT table position & limit are set using
66     lgdt lgdt_opcode          # 6-byte operand lgdt_opcode.
67     ret

# The following code is used to temporarily set all 256 interrupt gate descriptors in the
# IDT table to the same default value. All use the default interrupt handler ignore_int.
# The specific method of setting is: first set the contents of 0-3 bytes and 4-7 bytes of
# the default interrupt gate descriptor into the eax and edx register pairs. Then, using
# this register pair, the interrupt descriptor is cyclically filled into the IDT table.
68 setup_idt:                   # Set all 256 int gate descriptors to use default handler.
69     lea ignore_int, %edx        # The same way as setting timer int gate descriptor.
70     movl $0x00080000, %eax      # The selector is 0x0008.
71     movw %dx, %ax
72     movw $0x8E00, %dx          # Interrupt gate type is 14, plevel is 0.

```

```

73      lea idt,%edi
74      mov $256,%ecx          # Loop through all 256 gate descriptor entries.
75 rp_idt: movl %eax,(%edi)
76      movl %edx,4(%edi)
77      addl $8,%edi
78      dec %ecx
79      jne rp_idt
80      lidt lidt_opcode      # IDTR register is loaded with a 6-byte operand.
81      ret
82
83 # Display characters subroutine. Get current cursor position & display char in AL.
# The entire screen can display 80 X 25 (2000) characters.
84 write_char:
85      push %gs               # First save the register to be used, EAX is
86      pushl %ebx             # saved by the caller.
87      mov $SCRN_SEL, %ebx     # Then let GS point to display mem seg (0xb8000).
88      mov %bx, %gs
89      movl scr_loc, %bx       # Get current char display position from scr_loc.
90      shl $1, %ebx           # Since each char has one attribute byte, so actual
91      movb %al, %gs:(%ebx)    # display memory offset should multiplied by 2.
92      shr $1, %ebx           # After putting char into display memory, divide the
93      incl %ebx              # position value by 2 plus 1 to get the next position.
94      cmpl $2000, %ebx       # If position is greater than 2000, it is reset to 0.
95      jb 1f
96      movl $0, %ebx
97 1:   movl %ebx, scr_loc      # Finally save this position value (scr_loc),
98      popl %ebx             # and pop up the contents of saved register, return.
99      pop %gs
100     ret
101
102 # The following are 3 interrupt handlers: default, timer, and system call interrupt.
103 # Ignore_int is default handler. If system generates other interrupts, it display char 'C'.
104 .align 2
105 ignore_int:
106     push %ds               # Let DS point to the kernel data segment because
107     pushl %eax             # the interrupt handler belongs to the kernel.
108     movl $0x10, %eax
109     mov %ax, %ds
110     movl $67, %eax          # Put 'C' in AL, call write_char to display on screen.
111     call write_char
112     popl %eax
113     pop %ds
114     iret
115
116 # This is the timer interrupt handler. The main function is to perform task switching operations.
117 .align 2
118 timer_interrupt:
119     push %ds
120     pushl %eax
121     movl $0x10, %eax          # First let DS point to the kernel data segment.
122     mov %ax, %ds
123     movb $0x20, %al           # Then send EOI to 8259A to allow other interrupts.
124     outb %al, $0x20
125     movl $1, %eax            # Then check current task to switch task 0 and 1.

```

```

126      cmpl %eax, current
127      je 1f
128      movl %eax, current
129      ljmp $TSS1_SEL, $0          # If current task is 0, save 1 in current and jump to
130      jmp 2f                      # task 1 to execute. The offset of jump is useless.
131 1:   movl $0, current           # If current task is 1, save 0 in current and jump to
132      ljmp $TSS0_SEL, $0          # task 0 to execute.
133 2:   popl %eax
134      pop %ds
135      iret
136
137 # The system call int 0x80 handler. This example has only one display char function.
138 .align 2
139 system_interrupt:
140     push %ds
141     pushl %edx
142     pushl %ecx
143     pushl %ebx
144     pushl %eax
145     movl $0x10, %edx           # First let DS point to the kernel data segment.
146     mov %dx, %ds
147     call write_char           # Then call routine write_char to display char in AL.
148     popl %eax
149     popl %ebx
150     popl %ecx
151     popl %edx
152     pop %ds
153     iret
154
155 /*****
156 current:.long 0                  # Store current task number (0 or 1).
157 scr_loc:.long 0                 # Store screen current display position.
158
159 .align 2
160 lidt_opcode:
161     .word 256*8-1             # 6-byte operand for set IDTR : table size & base.
162     .long idt
163 lgdt_opcode:
164     .word (end_gdt-gdt)-1      # 6-byte operand for set IDTR : table size & base.
165     .long gdt
166
167 .align 3
168 idt:    .fill 256,8,0          # IDT. 256 gate descriptors, each 8 bytes, total 2KB.
169 # The following is GDT table contents (of descriptors).
170 gdt:    .quad 0x0000000000000000 # [0] The first segment descriptor is not used.
171     .quad 0x0c09a00000007ff    # [1] Kernel code descriptor. Its selector is 0x08
172     .quad 0x00c09200000007ff    # [2] Kernel data descriptor. Its selector is 0x10
173     .quad 0x00c0920b80000002    # [3] Display mem descriptor. Its selector is 0x18
174     .word 0x68, tss0, 0xe900, 0x0 # [4] TSS0 descriptor. Its selector is 0x20.
175     .word 0x40, ldt0, 0xe200, 0x0 # [5] LDT0 descriptor. Its selector is 0x28
176     .word 0x68, tss1, 0xe900, 0x0 # [6] TSS1 descriptor. Its selector is 0x30
177     .word 0x40, ldt1, 0xe200, 0x0 # [7] LDT1 descriptor. Its selector is 0x38
178 end_gdt:
179     .fill 128,4,0              # Initial kernel stack space.

```

```

180 init_stack:          # Stack pointer when first enter protected mode.
181     .long init_stack    # Stack segment offset position.
182     .word 0x10           # Stack segment, same as kernel data seg (0x10).
183
184 # Below is the local segment descriptor in the LDT table segment of task 0.
185 .align 3
186 ldt0:    .quad 0x0000000000000000      # [0] The first descriptor is not used.
187     .quad 0x00c0fa00000003ff      # [1] The local code descriptor, its selector is 0x0f
188     .quad 0x00c0f200000003ff      # [2] The local data descriptor, its selector is 0x17
189 # Content of TSS seg for task 0. Note fields such as labels do not change when task switches.
190 tss0:   .long 0            /* back link */
191     .long krn_stk0, 0x10      /* esp0, ss0 */
192     .long 0, 0, 0, 0, 0       /* esp1, ss1, esp2, ss2, cr3 */
193     .long 0, 0, 0, 0, 0       /* eip, eflags, eax, ecx, edx */
194     .long 0, 0, 0, 0, 0       /* ebx esp, ebp, esi, edi */
195     .long 0, 0, 0, 0, 0       /* es, cs, ss, ds, fs, gs */
196     .long LDT0_SEL, 0x8000000 /* ldt, trace bitmap */
197
198     .fill 128,4,0          # This is the kernel stack space for task 0.
199 krn_stk0:
200
201 # Task 1 LDT table content and TSS segment content.
202 .align 3
203 ldt1:    .quad 0x0000000000000000      # [0] The first descriptor is not used.
204     .quad 0x00c0fa00000003ff      # [1] The selector is 0x0f, base = 0x00000.
205     .quad 0x00c0f200000003ff      # [2] The selector is 0x17, base = 0x00000.
206
207 tss1:   .long 0            /* back link */
208     .long krn_stk1, 0x10      /* esp0, ss0 */
209     .long 0, 0, 0, 0, 0       /* esp1, ss1, esp2, ss2, cr3 */
210     .long task1, 0x200        /* eip, eflags */
211     .long 0, 0, 0, 0          /* eax, ecx, edx, ebx */
212     .long usr_stk1, 0, 0, 0  /* esp, ebp, esi, edi */
213     .long 0x17,0x0f,0x17,0x17,0x17,0x17 /* es, cs, ss, ds, fs, gs */
214     .long LDT1_SEL, 0x8000000 /* ldt, trace bitmap */
215
216     .fill 128,4,0          # This is the kernel stack space for task 1. Its user
217 krn_stk1:                         # stack uses the initial kernel stack space directly.
218
219 # The programs of tasks 0 and 1, which cyclically display chars 'A' and 'B', respectively.
220 task0:
221     movl $0x17, %eax          # DS point to the local data segment of the task.
222     movw %ax, %ds             # No local data, these 2 instructions can be omitted.
223     movl $65, %al              # Put 'A' into the AL register.
224     int $0x80                 # Execute system call to display it.
225     movl $0xffff, %ecx          # Execute a loop, act as a delay.
226 1:    loop 1b
227     jmp task0                # Jump to start of task 0 to continue displaying.
228 task1:
229     movl $66, %al              # Put 'B' into the AL register.
230     int $0x80                 # Execute system call to display it.
231     movl $0xffff, %ecx          # Execute a loop, act as a delay.
232 1:    loop 1b

```

```
233      jmp task1
234
235      .fill 128,4,0          # This is user stack space for task 1.
236 usr_stk1:
```

---

## 4.10 概要

この章では、インテル80X86

CPUの保護モードのメモリ管理とプログラミングの原理について説明します。この章では、グローバル/ローカルディスクリプタテーブル、セグメントディスクリプタ、セグメントセレクタの具体的な意味を詳しく説明しています。また、プログラムの論理アドレス、CPUのリニアアドレス、物理メモリのアドレスの変換関係についても説明しています。最後に、簡単なカーネルのサンプルプログラムが与えられ、本章の最後に紹介されています。このサンプル・プログラムを理解することで、保護モード・プログラミングの習得度を大まかに説明することができます。

以下では、1つの章を使って、Linuxカーネルのハードウェア設定、メモリの割り当てと使用方法、タスクデータ構造の機能などを包括的に説明し、カーネルのソースツリーにあるすべてのソースコードを分類して、まず読者にカーネルコード全体のファイル構造を大まかに理解してもらいます。そして、次の章では、カーネル内のソースコードファイルを詳細に説明し、注釈を付けています。



## 5Linuxカーネルアーキテクチャ

本章は、カーネルのソースコードの概要を説明したもので、後続の章を読む際の参考にしていただけます。理解しづらい内容については、まず読み飛ばしてください。次の章で関連する内容を読むときには、この章を参照するよう戻ってください。本章を読む前に、80X86のプロテクトモード動作の仕組みを確認・学習してください。

本章では、まず

Linux

カーネルの構成モードとアーキテクチャの概要を説明した後、カーネルソースディレクトリ内のソースファイル構成、サブディレクトリ内の各種コードファイルの主な機能、基本コールの階層関係を詳細に説明しています。その後、直接トピックに切り込み、カーネルソースファイルLinuxディレクトリ内の最初のファイルMakefileから始めて、各行のコードを詳しく説明します。Linux 0.12カーネルのソースコードをもとに、基本的なアーキテクチャと主要なコンポーネントを簡単に説明します。また、ソースコードに登場するいくつかの重要なデータ構造についても説明します。最後に、Linux 0.12カーネルのコンパイル実験環境を構築する方法を説明します。

完全なオペレーティングシステムは、レイヤーの観点から見ると、図5-1に示すように、ハードウェア、オペレーティングシステムカーネル、オペレーティングシステムサービス、ユーザーアプリケーションの4つの部分から構成されます。ユーザーアプリケーションとは、ユーザー自身がコンパイルしたワードプロセッサやインターネットブラウザプログラムなどの各種アプリケーションのことであり、オペレーティングシステムサービスとは、ユーザーにサービスを提供するものであり、オペレーティングシステムの一部とみなされる。Linuxオペレーティングシステムでは、Xウィンドウシステム、シェルコマンド解釈システム、カーネルプログラミングインターフェイスなどのシステムプログラムがこれにあたる。オペレーティングシステムのカーネルは、本書の中で興味を引く部分である。主にハードウェアのリソースを抽象化し、すべてのシステムリソースの管理をスケジューリングするために使用されます。

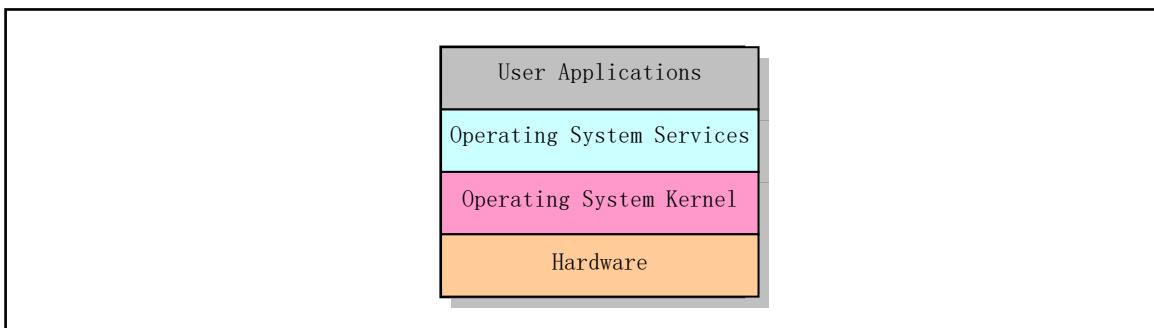


Figure 5-1 Operating system components

Linuxカーネルの主な目的は、コンピュータのハードウェアと相互作用し、コンポーネントのインターフェース操作やプログラムによる制御を実装し、ハードウェアリソースへのアクセスをスケジューリングし、コンピュータ上のユーザープログラムに使いやすい実行環境と共にハードウェア仮

想インターフェースを提供することです。.

## 5.1 Linuxカーネルモード

現在、オペレーティングシステムのカーネルの構造モードは、主にモノリシックなものと、それ以外のものに分けられます。

シングルコアモデルと階層型マイクロカーネルモデル、そして両者の混合モードがあります。本書で注釈を付けたLinux 0.12カーネルは、シングルコアモードを採用しています。

モノリシック・シングルコア・システム・モデルでは、オペレーティング・システムが提供するサービス・プロセスは、アプリケーション・プログラムが指定されたパラメーターでシステム・コール命令 (int

x80) を実行することで、CPUがユーザー・モードからコアの状態に切り替わります（カーネル・モデル）。システムコール命令を実行すると、OSは指定されたパラメータに従って特定のシステムコールサービスプロシージャを呼び出し、これらのサービスプロシージャは必要に応じて基礎となるサポート機能の一部を呼び出して特定の機能を完了します。アプリケーションが必要とするサービスが完了すると、OSはCPUをカーネルモードからユーザー・モードに戻し、アプリケーションに戻って次の命令の実行を継続します。つまり、シングルコアモードのカーネルは、サービスを呼び出すメインプログラム層、システムコールを実行するサービス層、システムコールをサポートする基盤機能の3つのレベルに大別することもできます。図5-

2をご覧ください。モノリシック・モデルの主な利点は、カーネル・コードがコンパクトで高速であることであり、欠点は主に階層が強固でないことです。

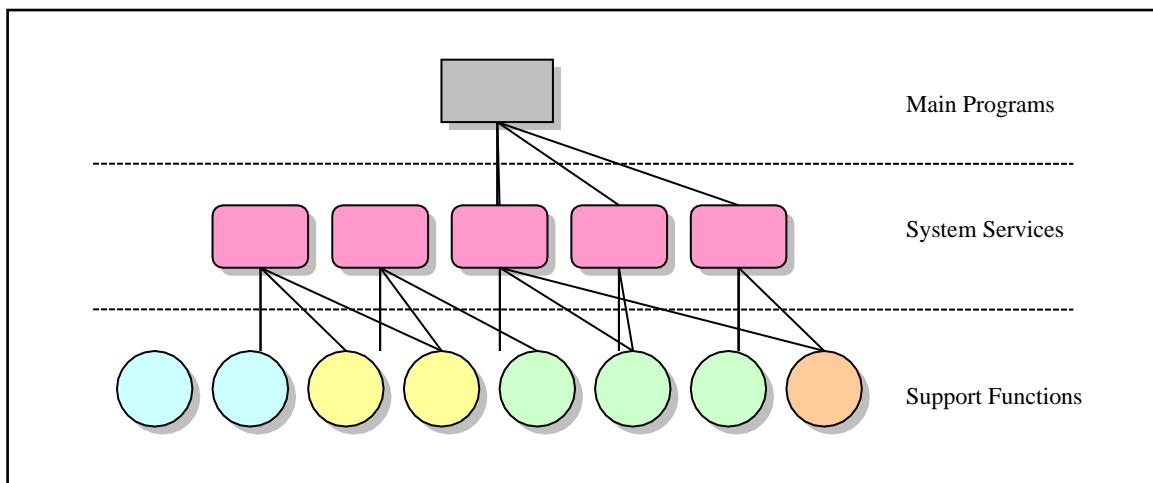


Figure 5-2 Simple structural of monolithic model

マイクロカーネルアーキテクチャモデルでは、機能のモジュール化と、サービススレッドまたはプロセス間のメッセージングが主な特徴です。システムコアは、基本的なハードウェア抽象化管理層と、主要なシステムサービス機能を提供します。これらの主要な機能とは、メインプロセス/スレッド間通信サービス、仮想メモリ管理、プロセススケジューリングなどです。オペレーティングシステムの残りの部分は、さまざまなモジュール形式でユーザースペースで機能します。したがって、マイクロカーネル構造の利点は、システムサービスの結合度が低いため、システムの改良、拡張、移植が

容易であることです。一方、主な欠点は、実行中にシステム・サービス・モジュール間で大量のメッセージ・パッシングや同期操作が必要となり、これらの操作が通信リソースの消費や時間の遅延を引き起こすことです。代表的なマイクロカーネル・アーキテクチャのシステムとしては、Machカーネルを搭載したMINIX OSやMac OSシステムなどがある。

## 5.2 Linuxカーネルシステムアーキテクチャ

Linuxカーネルは、図5-

3に示すように、プロセススケジューリングモジュール、メモリ管理モジュール、ファイルシステムモジュール、プロセス間通信モジュール、ネットワークインターフェースモジュールの5つのモジュールから構成されている。

プロセススケジューリングモジュールは、プロセスによるCPUリソースの使用を制御する役割を担っています。のです。

各プロセスが公平かつ合理的にCPUにアクセスできるようにする一方で、カーネルがタイムリーにハードウェア処理を実行できるようにするというスケジューリング戦略が採用されています。メモリ管理モジュールは、すべてのプロセスがマシンのメインメモリ領域を安全に共有できるようにするために使用されます。同時に、メモリ管理モジュールは仮想メモリ管理モードもサポートしており、Linuxサポートプロセスが実際のメモリ空間よりも多くのメモリ容量を使用するようになっています。ファイルシステムを使用して、未使用的メモリブロックを外部記憶装置にスワップし、必要に応じて交換することができます。ファイルシステムモジュールは、外部デバイスのドライブとストレージをサポートするために使用されます。仮想ファイルシステムモジュールは、すべての外部ストレージデバイスに共通のファイルインターフェースを提供することで、さまざまなハードウェアデバイスの異なる詳細を隠します。これは、他のオペレーティングシステムと互換性のある複数のファイルシステムフォーマットを提供し、サポートします。プロセス間通信モジュールは、複数のプロセス間の情報交換をサポートするために使用されます。ネットワークインターフェースモジュールは、様々なネットワーク通信規格へのアクセスを提供し、多くのネットワークハードウェアをサポートします。

これらのモジュール間の依存関係を図5-

3に示す。接続部は各モジュール間の依存関係を表し、破線と破線のボックスはLinux 0.12の未実装部分を表している（仮想ファイルシステムはLinux 0.95バージョンから徐々に実装されているが、ネットワークインターフェースのサポートはバージョン0.96以降でしか利用できない）。

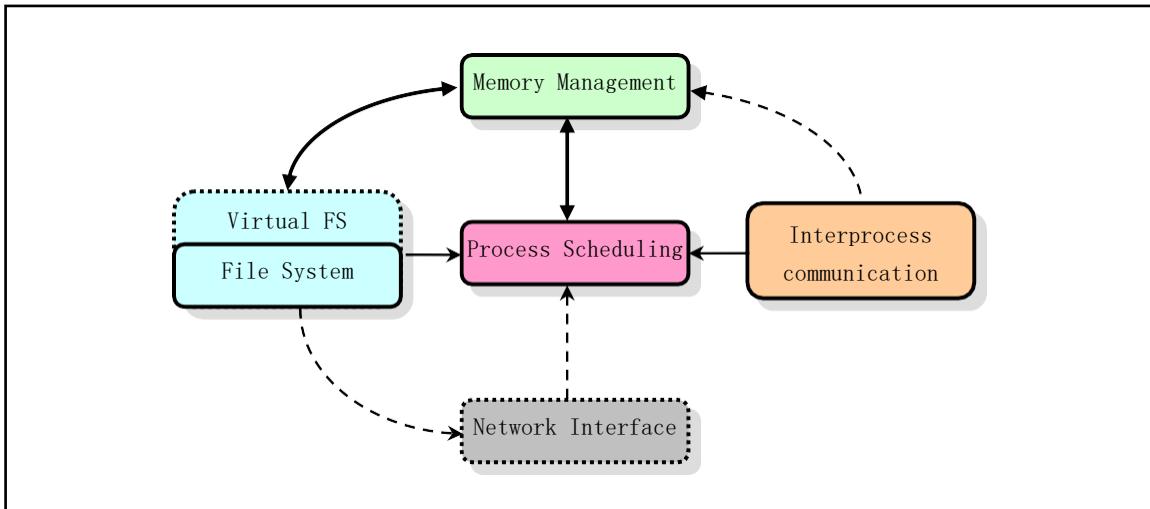


Figure 5-3 Linux kernel module structure and interdependence

図からわかるように、すべてのモジュールは、プロセススケジューリングモジュールに依存しています。なぜなら、すべてのモジュールはプロセススケジューラーに依存して、プロセスをサスペンド（一時停止）したり、再実行したりしているからです。一般的に、モジュールはハードウェアの操作を待っている間にサスペンドされ、操作が完了するまで実行され続けます。例えば、あるプロセスがデータのブロックをフロッピーディスクに書き込もうとしたとき、フロッピーディスクのドライバーは、ブートフロッピーディスクの回転中にプロセスをサスペンド待機状態にし、フロッピーディスクが通常の回転に入った後にプロセスを継続させることができます。他の3つのモジュールも同様の理由で、プロセススケジューリングモジュールに依存しています。

他のいくつかのモジュールの依存関係は、やや目立ちませんが、重要なものもあります。プロセススケジューリングサブシステムは、メモリ管理を使用して、特定のプロセスが使用する物理メモリ空間を調整する必要があります。プロセス間通信サブシステムは、メモリマネージャを使用して共有メモリ通信メカニズムをサポートします。この通信メカニズムでは、2つのプロセスがメモリの同じ領域にアクセスして、プロセス間で情報を交換することができます。また、仮想ファイルシステムでは

NFS (Network File System) をサポートするネットワークインターフェースと、メモリ・ラムディスク・デバイスを提供するメモリ管理サブシステムを備えています。また、メモリ管理サブシステムは、ファイルシステムを利用してメモリブロックのスワップをサポートします。

モノリシック構造モデルから、Linux 0.12カーネルのソースコードの構造に合わせて、カーネルのメインモジュールを図5-4のようなブロック図構造に描くこともできます。

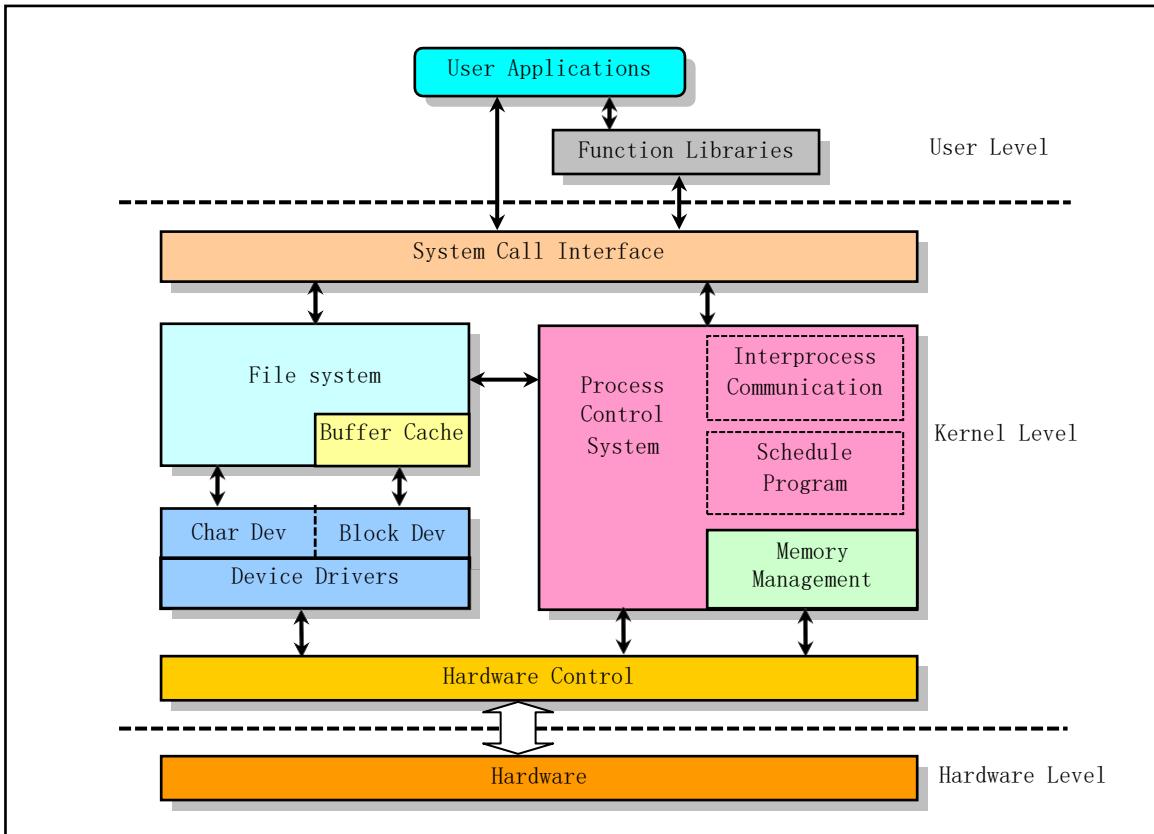


Figure 5-4 Kernel block diagram

カーネルレベルのいくつかのボックスでは、ハードウェア制御ブロック以外の太い線のボックスが、カーネルソースコードのディレクトリ構成に対応しています。これらの図に示されている依存関係に加えて、これらのモジュールはすべて、カーネル内の共通リソースにも依存しています。これらのリソースには、メモリの割り当てや再利用機能、警告やエラーメッセージを表示する機能、システムのデバッグ機能などがあります。

## 5.3 Linuxカーネルのメモリ管理

本節では、まず、Linux

0.12システムにおける比較的わかりやすい物理メモリの使い方を説明します。次に、Linux 0.12カーネルのアプリケーション状況と組み合わせて、メモリのセグメンテーションとページング管理のメカニズム、およびCPUのマルチタスク動作と保護モードについて概説します。最後に、Linux におけるカーネルコードとデータの対応関係を包括的に説明します。

0.12システムと、仮想・線形・物理アドレス空間における各タスクのコードとデータ。

この章での説明は、メモリ管理の概要やおさらいとも言えます。プロテクションモードでのメモリ管理の詳細については、第4章を参照してください。

### 5.3.1 物理的アドレス

Linux

0.12カーネルでは、マシン内の物理メモリを有効活用するため、図5-5に示すように、システムの初期化段階でメモリをいくつかの機能領域に分割しています。

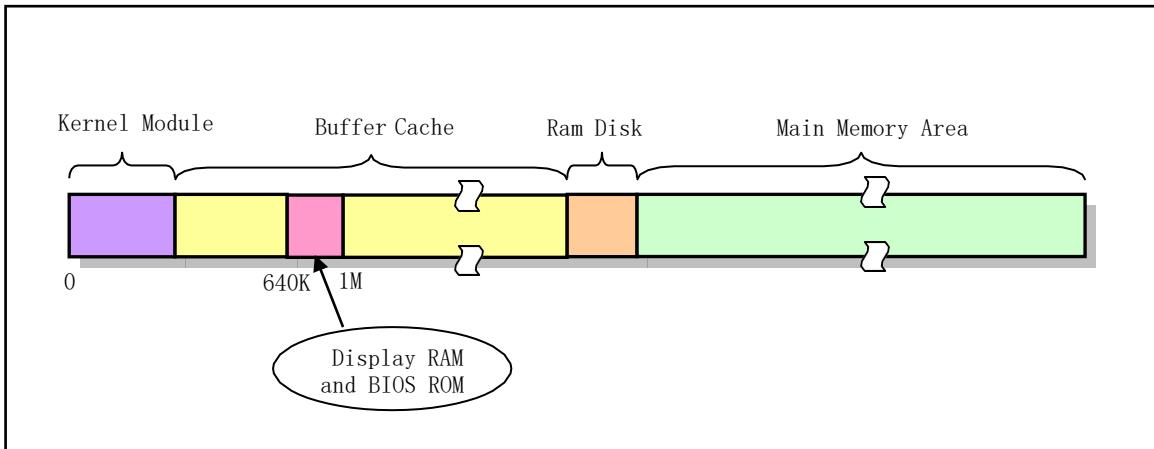


Figure 5-5 Functional distribution of physical memory usage

その中で、Linuxカーネルは物理メモリの先頭を占め、次にハードディスクやフロッピーディスクなどのブロックデバイス用の高速バッファ部分が続く（この中で、ディスプレイカードメモリやROM BIOSのメモリアドレス範囲は640K～1MB）。プロセスやタスクがブロックデバイスからデータを読み出す必要がある場合、システムはまずデータをキャッシュに読み込みます。また、ブロックデバイスに書き込むべきデータがある場合、システムはまずデータをキャッシュに入れ、次にブロックデバイスドライバが対応するデバイスに書き込みます。メモリの最後の部分は、すべてのプログラムがいつでも要求して使用できる主記憶領域である。カーネルプログラムがメインメモリ領域を使用する際にも、まずカーネルメモリ管理モジュールに申請する必要があります、申請が成功した後にメモリを使用することができるようになります。また、RAM仮想ディスクを搭載したシステムでは、仮想ディスクがデータを格納するために、主記憶領域のヘッダが部分的に削除される。

コンピュータシステムに含まれる実際の物理メモリの容量は限られているため、通常、CPUはシステム内のメモリを効率的に管理するためのメモリ管理機構を提供している。Intel 80386以降のCPUでは、「メモリセグメンテーション」と「ページング管理システム」という2つのメモリ管理（アドレス変換）機構が用意されている。ページング管理システムはオプションであり、採用するかどうかはシステムプログラマがプログラムします。Linuxシステムでは、物理的なメモリを有効に使うために、メモリセグメンテーションとページング管理の両方の仕組みを採用しています。

### 5.3.2 メモリアドレス空間の概念

Linux

0.12カーネルでは、アドレスマッピングを行う際に、まず、a)プログラム(プロセス)の仮想・論理アドレス、b)CPUのリニアアドレス、c)実際の物理メモリアドレスの3種類のアドレスと、それらの間の変換の概念を区別する必要がある。

仮想アドレスとは、プログラムが生成するアドレスのことで、セグメントセレクタとセグメント

内のオフセットアドレスの2つの部分から構成されています。この2つの部分は、物理メモリへのアクセスには直接使用されず、セグメントアドレス変換機構によって物理メモリのアドレスに対応するように処理またはマッピングされる必要があるため、このようなアドレスは仮想アドレスと呼ばれます。仮想アドレス空間は、GDTでマッピングされたグローバルアドレス空間と、LDTでマッピングされたローカルアドレス空間で構成されています。セレクタのインデックス部は13ビットで表現され、これに以下を区別する1ビットが加わります。

GDTとLDTの間にありますため、インテル80X86のCPUは合計16384個のセレクタをインデックスすることができます。各セグメントの長さが最大4Gの場合、最大の仮想アドレス空間は $16384 * 4G = 64T$ となる。

論理アドレスは、プログラムが生成するセクションに関連するオフセットアドレスの部分です。インテルのプロテクトモードでは、プログラム実行コードセクションの制限長内のオフセットアドレスを指します（コードセクションとデータセクションが同一であると仮定します）。アプリケーションプログラマは論理アドレスだけを扱えばよく、セグメンテーションやページングの仕組みは、システムプログラマにしか全く見えない。しかし、資料によっては、論理アドレスと仮想アドレスの概念を区別せず、総称して論理アドレスと呼んでいるものもある。

リニアアドレスは、仮想アドレスと物理アドレスの変換の中間層であり、プロセッサのアドレス可能なメモリ空間（リニアアドレス空間と呼ぶ）におけるアドレスである。プログラムコードは、論理アドレス、つまりセグメント内のオフセットアドレスに、対応するセグメントのベースアドレスを加えてリニアアドレスを生成します。ページング機構が有効な場合は、リニアアドレスを変換して物理アドレスを生成することができます。ページング機構が有効になっていない場合は、リニアアドレスがそのまま物理アドレスになります。Intel 80386のリニアアドレス空間は4Gである。

#### Physical

Addressは、CPUの外部アドレスバス上でアドレスされた物理メモリを示すアドレス信号で、アドレス変換の最終結果のアドレスとなります。ページング機構が有効な場合、リニアアドレスはページディレクトリとページテーブルの項目を用いて物理アドレスに変換されます。ページング機構が有効でない場合は、リニアアドレスがそのまま物理アドレスになります。

仮想記憶（または仮想メモリ）とは、コンピュータが実際に持っているメモリ量よりもはるかに大きなメモリを提示することである。そのため、プログラマーは実際のシステムが持っているよりもはるかに大きなサイズのプログラムをプログラミングして実行することができます。これにより、限られたメモリ資源のシステム上で、多くの大規模なプロジェクトを実行することができます。非常に適切な例えは、上海から北京まで列車を走らせるのに、長い線路は必要ないということです。このタスクを完了するのに十分な長さのレール（例えば10km）があればいいのです。方法としては、すぐに後部のレールを列車の前に敷くことです。操作が十分に速く、要件を満たすことができれば、列車は完全なトラックのように走ることができます。これが、仮想メモリ管理が達成すべきタスクです。Linux

0.12カーネルでは、各プログラム（プロセス）は、合計64MBの容量を持つ仮想メモリ空間に分割されています。そのため、プログラムの論理アドレス範囲は0x00000000～0x40000000となります。

前述のように、論理アドレスを仮想アドレスと呼ぶこともあります。なぜなら、論理アドレスは仮想メモリ空間の概念に似ており、実際の物理メモリの容量とは独立しているからである。

### 5.3.3 メモリ分割の仕組み

メモリセグメンテーションシステムでは、プログラムの論理アドレスは、セグメンテーション機構により、中間層の4GB ( $2^{32}$ ) リニアアドレス空間に自動的にマッピング（変換）される。プログラムがメモリを参照することは、メモリセグメント内のメモリを参照することになります。プログラムがメモリアドレスを参照すると、プログラマに見える論理アドレスに対応するセグメントベースアドレスを加えて、対応するリニアアドレスが形成されます。このとき、ページング機構が有効になつていなければ、リニアアドレスはCPUの外部アドレスバスに送られ、対応する物理メモリに直接アドレッシングされます。図5-6をご覧ください。

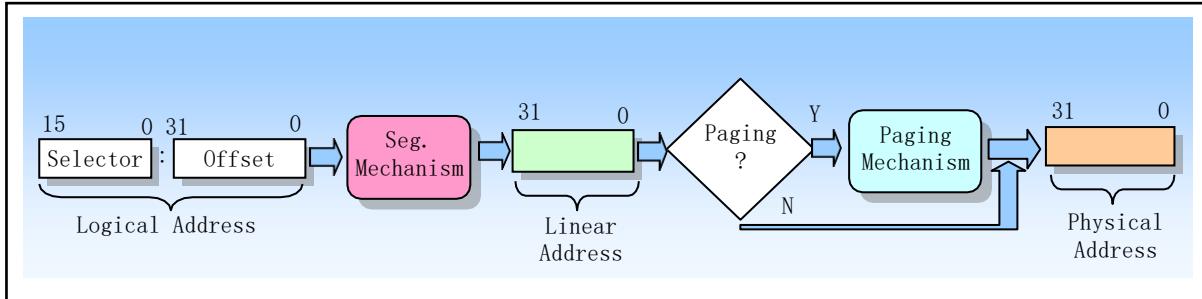


Figure 5-6 Logical address to physical address translation

CPUがアドレス変換（マッピング）を行う主な目的は、仮想メモリ空間から物理メモリ空間へのマッピング問題を解決することである。仮想記憶空間の意味は、二次記憶空間や外部記憶空間を利用して、実際の物理メモリの量に制限されることなくプログラムがメモリを使用できるようにする方法を指す。通常、仮想メモリ空間は実際の物理メモリよりもはるかに大きい。

では、仮想ストレージの管理はどのように行われるのでしょうか。その原理は、上記の列車運行のアナロジーに似ています。まず、プログラムが存在しないメモリを使用する必要がある場合（つまり、メモリページテーブルのエントリに対応するメモリページがメモリ内にない場合）、CPUはその状況を知る方法が必要です。これを実現するのが、80386のページフォルト例外割り込みです。プロセスが存在しないページのメモリアドレスを参照すると、CPUはページフォルト例外割り込みを発生させ、割り込みの原因となったリニアアドレスをCR2コントロールレジスタに入れます。したがって、割り込みを処理するプロセスは、ページ例外の正確なアドレスを知ることができるので、プロセスが要求するページを二次記憶空間（ハードディスクなど）から物理メモリにロードすることができます。このとき、物理メモリがすでに占有されている場合は、二次記憶空間の一部をスワップバッファ（Swapper）として使用し、二次バッファ内の一時的に使用されていないページを交換してから、要求されたページをメモリに転送することができます。

これは、メモリ管理のページフォルトローディング機構である。Linux 0.12カーネルのmm/memory.cというプログラムで実装されている。

インテルのCPUは、プログラムのアドレスにセグメントという概念を用いています。各セグメントには、メモリ上の領域やアクセスの優先順位などの情報が定義されている。ここでは、リアルモードでのメモリアドレッシングの原理は誰もが知っているとして、32ビットプロテクトモードの動作メカニズム下でのメモリアドレッシングの主な特徴を、リアルモードとプロテクトモードでのCPUのアドレッシングモードの違いに応じて、比較法を用いて簡単に説明する。

リアルモードでは、メモリアドレスのアドレッシングには主にセグメント値とオフセット値を使用します。セグメント値はセグメントレジスタ（DSなど）に格納され、セグメントの長さは64KBに

固定されています。セグメント内のオフセットアドレスは、アドレス指定に使用できる任意のレジスタ（例：SI）に格納されます。したがって、セグメント・レジスタとオフセット・レジスタの値に基づいて、図5-

7 (a) に示すように、実際のポインテッド・メモリ・アドレスを計算することができます。

プロテクトモードでは、セグメントレジスタは、アドレス指定されたセグメントのベースアドレスではなく、セグメントディスクリプターテーブルのディスクリプター項目のインデックス値となります。インデックス値で指定されたセグメントディスクリプター項目には、アドレスするメモリセグメントのベースアドレス、セグメントの限界長、セグメントのアクセス権レベルなどの情報が含まれています。指定されたメモリ・ロケーションは、セグメント記述子項目で指定されたセグメント・ベース・アドレスとセグメント内のオフセットの組み合わせです。セグメントの限界長は可変で、記述子の内容で指定されます。リアル・モードでのアドレス指定と比較して、セグメント・レジスタの値が次のようなインデックス値に置き換えられていることがわかります。

セグメントディスクリプターテーブルの対応するセグメントディスクリプターと、セグメントテーブル選択ビットと特権レベルを合わせて、セグメントセレクターと呼びますが

オフセット値は、やはりオリジナルモードでの概念を使用します。このように、プロテクトモードでメモリアドレスを指定するには、セグメントディスクリプターテーブルを使用するリアルモードに比べて、1つ多くの手順が必要になります。これは、プロテクトモードではメモリセグメントにアクセスするための情報が多く、16ビットのセグメントレジスタではこの内容をあまり保持できないためです。その回路図を図5-

7 (b) に示す。なお、セグメントディスクリプタでメモリリニアアドレス空間の領域を定義しないと、そのアドレス領域は全くアドレスされず、CPUはそのアドレス領域へのアクセスを拒否します。

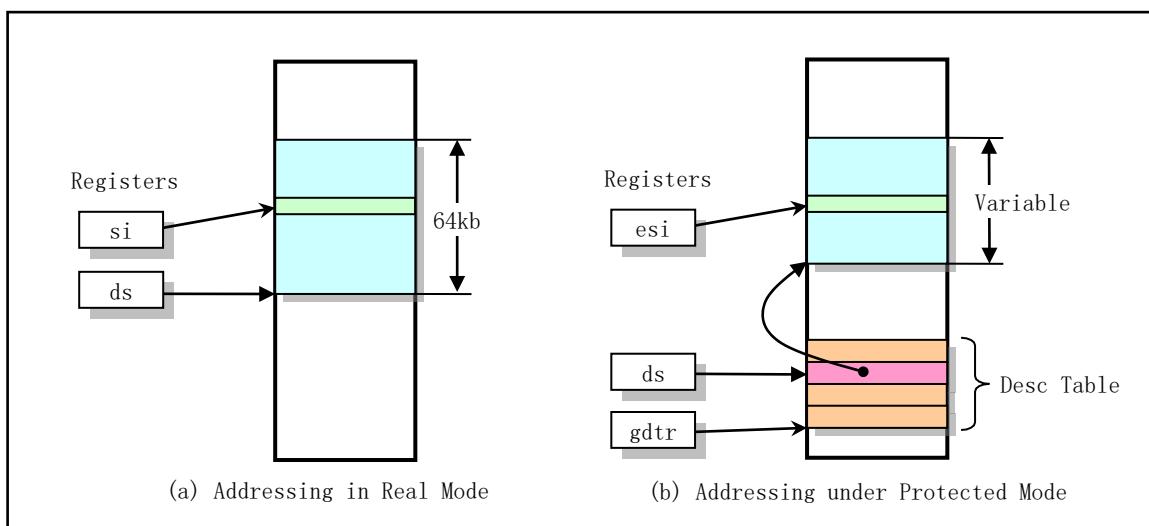


Figure 5-7 Comparison of addressing in real mode and protected mode

各記述子は8バイトで、リニアアドレス空間における記述されたセグメントの開始アドレス（ベースアドレス）、セグメントの限界長、セグメントの種類（コードセグメントやデータセグメントなど）、セグメントの特権レベル、その他の情報を含みます。1つのセグメントが定義できる最大の長さは4GBです。

ディスクリプタ項目を保存するディスクリプターテーブルには3種類あり、それぞれ目的が異なり

ます。グローバルディスクリプターテーブル (GDT) は、すべてのプログラムがメモリセグメントを参照するために使用できるメインベースのディスクリプターテーブルです。割り込み記述子テーブル (IDT) は、割り込みや例外処理のプロセスを定義するセグメント記述子を保持します。IDTテーブルは、8086システムの割り込みベクターテーブルを直接置き換えるものです。80X86のプロテクトモードで正常に動作させるためには、CPUにGDTテーブルとIDTテーブルを定義する必要があります。

最後のタイプのテーブルは、LDT (Local Descriptor Table) です。このテーブルは、マルチタスクシステムで使用され、通常はタスクごとに1つのLDTテーブルを使用します。GDTテーブルの拡張機能として、各LDTテーブルは対応するタスクに対してより多くの利用可能な記述子エントリを提供し、各タスクにアドレス可能なメモリ空間の範囲を提供します。

これらのテーブルは、リニアアドレス空間のどこにでも保存することができます。GDTテーブル、IDTテーブル、現在のLDTテーブルの位置をCPUが特定するために、GDTR、IDTR、LDTRの3つの特別なレジスタをCPUに設定する必要があります。これらのレジスタには、対応するテーブルの32ビットリニアベースアドレスと、テーブルの限界長バイト値が格納される。テーブルの長さ値は、テーブルの長さ値-1となります。

CPUがセグメントをアドレス指定する際には、16ビットのセグメントレジスタのセレクタを使ってセグメントディスクリプタを探します。80X86

CPUでは、セグメントレジスタの値を3ビット右にシフトした値が、ディスクリプターテーブルのディスクリプターのインデックス値となります。13ビットのインデックス値は、8192 (0--8191) までの位置を特定できます。

ディスクリプタのエントリです。セレクタビット2 (TI) は、どのテーブルを使用するかを指定するために使用されます。このビットが0の場合、セレクタはGDTテーブルの記述子を指定し、それ以外の場合はLDTテーブルの記述子を指定します。

各プログラムは、複数のメモリセグメントで構成されます。プログラムの論理アドレス（または仮想アドレス）は、これらのセグメントの特定のアドレス位置を指定するために使用されます。Linux

0.12では、プログラムの論理アドレスからリニアアドレスへの変換処理に、グローバルセグメント記述子テーブルGDTとローカルセグメント記述子テーブルLDTを使用しています。GDTでマッピングされたアドレス空間をグローバルアドレス空間、LDTでマッピングされたアドレス空間をローカルアドレス空間と呼び、両者で仮想アドレスの空間を構成している。具体的な使い方を図5-8に示す。

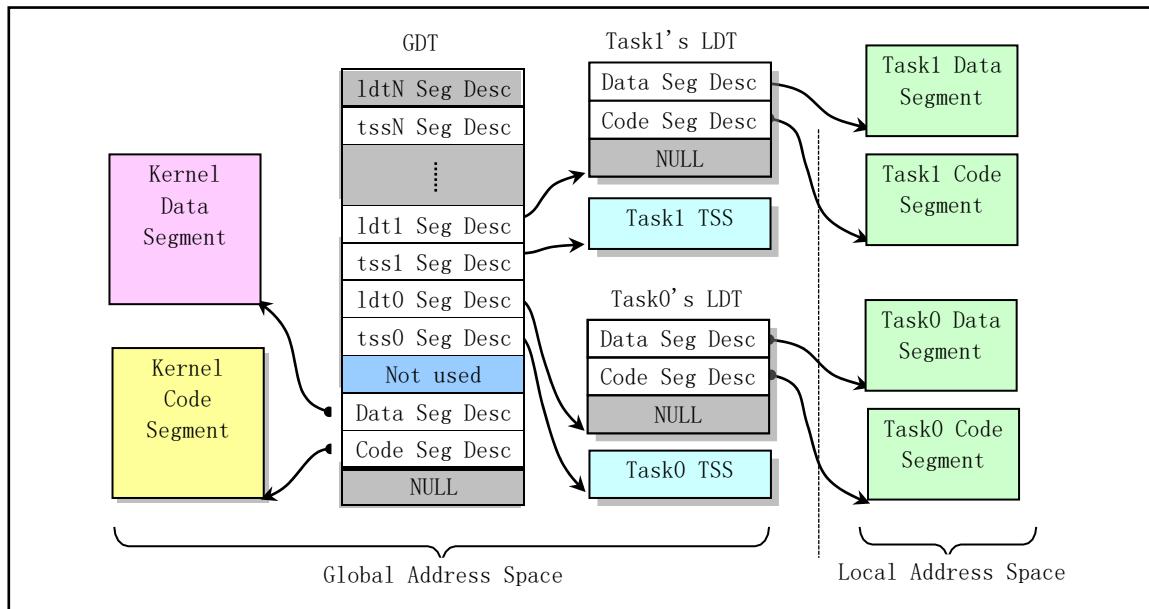


Figure 5-8 Virtual address space allocation map in Linux

図は、タスクが2つある場合の状況を示しています。各タスクのローカルディスクリプターテーブルLDTも、GDTのディスクリプターで定義されたメモリーセグメントであり、その中に対応するタスクのコードセグメントとデータセグメントのディスクリプターが格納されているため、LDTのセグメントは非常に短いことがわかります。セグメントの長さは通常、24バイトより大きければ良いとされています。同様に、各タスクのタスク・ステータス・セグメントTSSも、GDT内の記述子によって定義されるメモリ・セグメントであり、セグメント長の制限は、TSSのデータ構造を格納する能力を満足するものであれば十分である。

カーネルのコードセグメントに格納されています。Linux 0.12カーネルでは、カーネルと各タスクのコードセグメントとデータセグメントは、それぞれリニアアドレス空間の同じベースアドレスにマッピングされており、セグメント長も同じであるため、カーネルのコードセグメントとデータセグメントはオーバーラップしています。図5-10または図5-11に示すように、各タスクのコードセグメントとデータセグメントもそれぞれオーバーラップしている。タスクステートセグメント(TSS)は、タスクが切り替わったときに、関連するタスクの現在の実行コンテキスト(CPUの現在の状態)を自動的に保存または復元するためのものである。例えば、タスクが切り替わった場合、CPUはそのタスクのTSSセグメントにそのレジスタなどの情報を保存し、新たにタスクに切り替わったTSSセグメントの情報を用いて各レジスタを設定し、新たなタスクの実行環境を復元します。

### Linux

0.12では、各タスクのTSSセグメントの内容は、そのタスクのタスクデータ構造に保存されます。また、Linux

0.12のカーネルでは、GDTテーブルの4番目の記述子（図中のsyscall記述子のエントリ）は使用されていません。示されたinclude/linux/sched.hファイルの201行目のオリジナル英語コメントより

以下のことから、Linus氏がカーネルを設計する際に、システムコールのコードをこの特殊なセクションに配置するように設計したことが推測されます。

---

```
200 /*  
201 * 最初のTSSを探すためのgdtへの入力。0-nul, 1-cs, 2-ds, 3-syscall 202 *  
4-TSS0, 5-LDT0, 6-TSS1など ...  
203 */
```

---

### 5.3.4 メモリのページング管理

ページングを使用する場合、リニアアドレスは単なる中間結果であり、ページングメカニズムを使用して変換し、最終的に実際の物理メモリアドレスにマッピングする必要があります。セグメンテーションと同様に、ページング機構は各メモリ参照を特定の要求に合わせてリダイレクト（変換）することができます。最も一般的な使い方は、システムメモリが多くのブロックに分割されている場合に、ページングを行うことで、連続した大きなメモリ空間イメージを作成し、プログラムがこれらの散乱したメモリブロックを気にせずに管理できるようにすることです。ページング機構は、セグメンテーション機構の性能を高めます。また、ページアドレス変換はセグメント変換に基づいて行われます。ページング・メカニズムの保護手段は、セグメント変換の保護手段に取って代わるものではなく、さらなる確認作業を行なうだけです。

メモリページングの基本原理は、CPUのリニアメモリ領域全体を4096バイトのメモリページに分割することである。プログラムがメモリの使用を要求すると、システムはメモリページの単位でメモリを割り当てます。メモリページングは、セグメンテーション機構と同様の方法で実装されているが、セグメンテーションほど洗練されていない。ページングはセグメンテーションの上に実装されているため、システムのメモリを非常に柔軟に制御することができます。また、セグメンテーション機構のメモリ保護機能に加えて、ページング保護機能が追加されています。80X86のプロテクトモードでページングを使用するためには、コントロールレジスタCR0の最上位ビット（ビット31）を設定する必要があります。

このメモリページング方式を用いると、実行中の各プロセス（タスク）は、実際のメモリ容量よりもはるかに大きな連続したアドレス空間を使用することができる。80386では、ページングを利用して直線的なアドレスを比較的小さな物理メモリ空間にマッピングするために、ページディレクトリテーブルとページテーブルを利用している。ページディレクトリエントリは、基本的にはページテーブルエントリと同じフォーマットで、4バイトを占有し、各ページディレクトリテーブルまたはページテーブルには、1024個のページテーブルエントリしか含まれていません。したがって、1つのページディレクトリテーブルまたはページテーブルは、合計1ページ分のメモリを占有します。ページディレクトリエントリとページテーブルエントリの小さな違いは、ページテーブルエントリにはビットD（Dirty）が書き込まれているのに対し、ページディレクトリエントリにはそれがないことです。

リニアアドレスから物理アドレスへの転送プロセスを図5-9に示します。図中のコントロールレジスタCR3は、物理メモリ内の現在のページディレクトリテーブルのベースアドレスを保持しています（そのため、CR3はページディレクトリベースアドレスレジスタPDBRとも呼ばれています）。32ビットのリニアアドレスは、ページディレクトリテーブルとページテーブルの対応するエントリの位置を特定するための3つの部分に分割され、対応する物理メモ

リページ内のページ内オフセット位置を指定します。ページテーブルは1024個のエントリを持つことができるため、1つのページテーブルは最大1024 \* 4KB =

4MBのメモリをマッピングすることができ、ページディレクトリテーブルは1024個の2次ページテーブルに対応する最大1024個のエントリを持つため、1つのページディレクトリテーブルは最大マップ1024 \* 4MB =

4GBのメモリをマッピングすることができる。つまり、ページディレクトリテーブルは、リニアアドレス空間の全範囲をマッピングすることができるのです。

### Linux

0.1xシステムでは、カーネルとすべてのタスクが同じページディレクトリテーブルを共有しているため、プロセッサのリニアアドレス空間と物理アドレス空間のマッピング機能は、いつでも同じです。したがって、カーネルとすべてのタスクが重なって干渉しないようにするために、仮想アドレス空間から線形アドレス空間の異なる位置にマッピングする、つまり異なる線形アドレスを占有する必要があります。

スペースの範囲です。

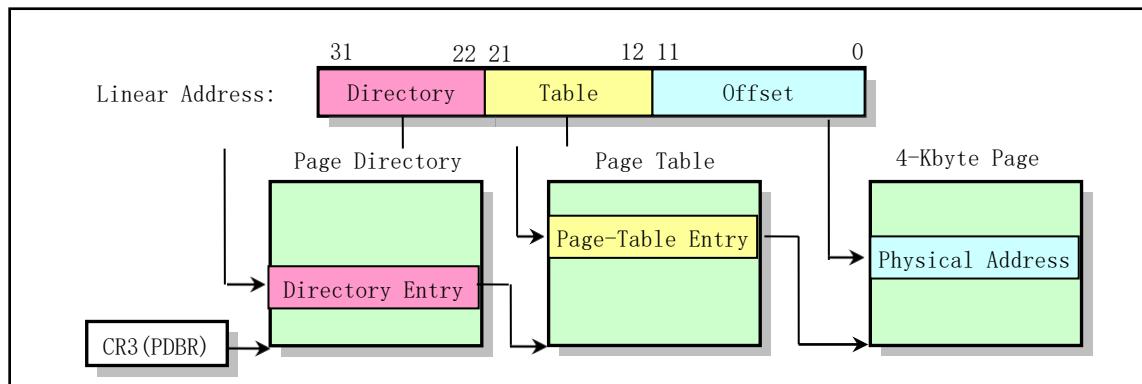


Figure 5-9 Diagram of linear address to physical address transformation

### Intel

80386システムでは、CPUは最大4Gのリニアアドレス空間を提供することができます。タスクの仮想アドレスは、まずローカルセグメント記述子によってCPUのリニアアドレス空間全体のアドレスに変換され、ページディレクトリテーブルPDT（プライマリページテーブル）とページテーブルPT（セカンダリページテーブル）を使って実際にマッピングされる必要がある。物理アドレスのページに実際の物理メモリを使用するために、各プロセスのリニアアドレスは、二次記憶ページテーブルによって主記憶領域の異なる物理メモリページに動的にマッピングされます。

### Linux

0.12では、1プロセスあたりの利用可能な仮想メモリ空間の最大値が64MBと定義されているため、各プロセスの論理アドレスは、(タスク番号) \* 64MBを加えることで線形空間上のアドレスに変換できる。ただし、本書のコードコメントでは、このようなプロセス内のアドレスを、混同しないように単に論理アドレスやリニアアドレスと呼ぶことがある。

### Linux

0.12カーネルでは、GDTに設定されているセグメントディスクリプターエントリの最大数は256です

。そのうち2つは使用されず、2つはシステムのエンルティであり、各プロセスやタスクは2つを使用する。したがって、この時点ではシステムは最大(256-

4)/2=126個のタスクを収容することができ、仮想アドレスの範囲は((256-

4)/2)\*64MBで約8Gに相当します。しかし、0.12カーネルで手動定義されているタスクの最大数はNR\_TASKS=64、各タスクの論理アドレス範囲は64M、リニアアドレス空間における各タスクの開始位置は(タスク番号)\*64MBです。したがって、すべてのタスクが使用するリニアアドレス空間は、図5-10に示すように、 $64MB \times 64 = 4G$ となります。

図は、システムに4つのタスクがある場合の状況を示しています。カーネルのコードセグメントとデータセグメントは、リニアアドレス空間の先頭の16MB部分にマッピングされており、コードセグメントとデータセグメントの両方が同じ領域にマッピングされており、完全にオーバーラップしています。最初のタスク(タスク0)は、カーネルが "手動"で起動します。コードとデータはカーネルのコードとデータの中に含まれているので、このタスクが使用するリニアアドレス空間はかなり特殊なものです。タスク0のコードセグメントとデータセグメントの長さは、リニアアドレス0から640KBの範囲であり、コードセグメントとデータセグメントも完全に重なり、カーネルのコードセグメントとデータセグメントと重なっています。実は、Linux 0.12では、すべてのタスクの命令空間I(Instruction)とデータ空間D(Data)は、1つのメモリを使っている。つまり、プロセスのコード部分、データ部分、スタック部分がすべて同じメモリセグメントに入っており、I&Dを分離せずに使用していることになります。

タスク1は、アドレス64MBから始まるリニアなアドレス空間を持ち、長さは640KBしかありません。両者の詳細な対応関係は後述します。タスク2とタスク3は、それぞれ128MBと192MBのリニアアドレスにマッピングされており、その論理アドレス範囲は64MBです。4Gのアドレス空間の範囲はは、まさに32ビットCPUのリニアアドレス空間の範囲であり、アドレス可能な最大の物理アドレス空間の範囲でもあります。また、タスク0とタスク1の論理アドレス範囲を64MBとみなすと、システムとしては

タスクの論理アドレス範囲も4GBとなるため、0.12カーネルでは3つのアドレス概念を混同しやすくなります。

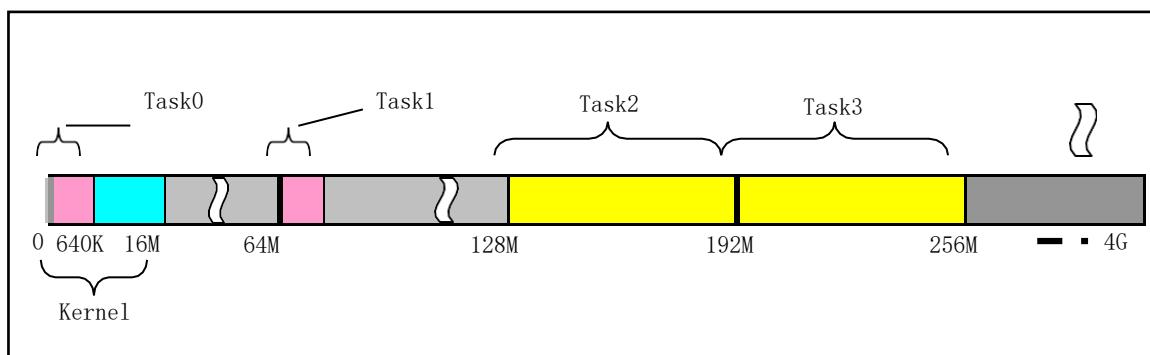


図5-10 Linux 0.12のリニアアドレス空間を利用した場合の図

仮想空間内のタスクも線形空間内のタスクの順番に合わせて配置すると、図5-11のようなシステムになります。仮想アドレス空間内のすべてのタスクの模式図ができ、仮想空間の範囲も4GBとなります。なお、仮想空間内のカーネルコードやデータの範囲は考慮していません。また、図では、タスク2とタスク3について、それぞれの論理空間におけるコードセグメントとデータセグメント（データとスタックの内容を含む）の位置も示されています。

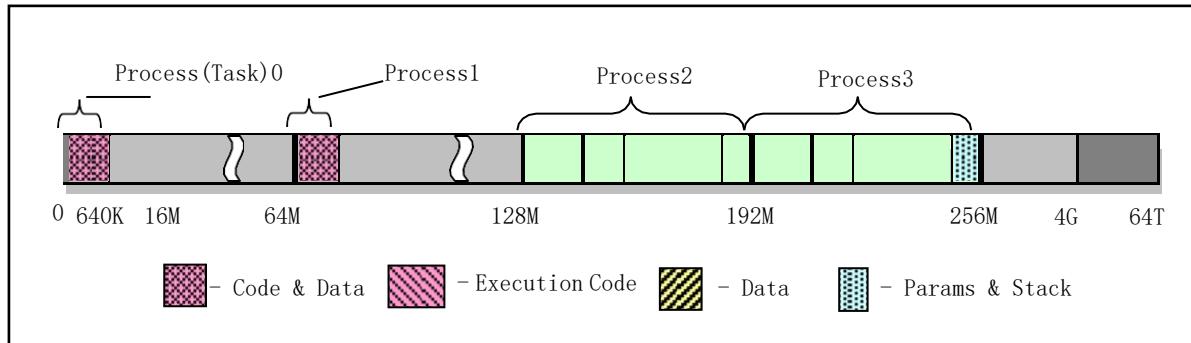


Figure 5-11 The spatial extent of tasks in virtual space in Linux 0.12

図 5-11 Linux 0.12 における仮想空間内のタスクの空間的広がり

また、タスクの論理アドレス空間におけるコード・セクションとデータ・セクションの概念は、CPUのセグメンテーション・メカニズムにおけるコード・セグメントとデータ・セグメントと同じ概念ではないことにも注意が必要です。CPUのセグメンテーションでは、セグメントの概念により、リニアアドレス空間におけるセグメントの目的や、強制的に行われる制約やアクセスを決定します。各セグメントは、4GBのリニアアドレス空間のどこにでも置くことができ、互いに独立していても構いません。また、完全にまたは部分的にオーバーラップすることもできます。タスクのコード部、データ部とは、コンパイラがプログラムをコンパイルする際、およびOSがプログラムをロードする際に指定するプロセスロジック空間内のコード領域、初期化・非初期化データ領域、スタック領域のことを指します。タスク論理アドレス空間のコードセグメントとデータセグメントの構造を図5-12に示します。図中のnrはプロセスまたはタスクの番号、start\_codeはリニアアドレス空間におけるプロセスの開始位置である。その他の変数はすべて、プロセス論理空間の値を含みます。

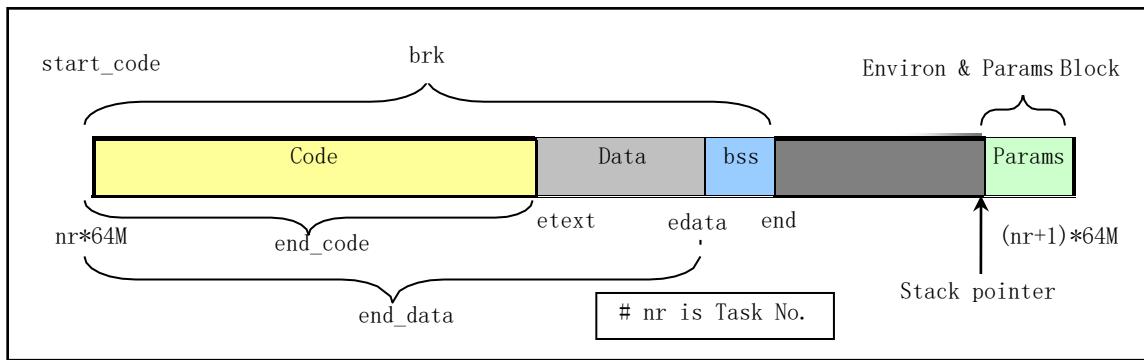


Figure 5-12 The distribution of task code and data in its logical address space

### 5.3.5 CPUのマルチタスク化と保護

80X86

CPUの保護機構には4つの保護レベルがあり、レベル0が最も優先度が高く、レベル3が最も優先度が低くなっています。OSのLinux

0.12では、CPUの保護レベルを0と3の2つにしています。各タスクには、コード領域とデータ領域があります。この2つの領域はローカルアドレス空間に格納されているため、システム内の他のタスクは不可視（アクセスできない）になっています。カーネルのコードとデータはすべてのタスクで共有されるので、グローバルアドレス空間に格納されます。この構造の模式図を図5-13に示します。図中の同心円は、CPUの保護レベル（保護層）を表しており、ここでは0と3のレベルのみを使用しています。放射状の光線は、システム内のタスクを区別するために使用されます。各放射状の光線は、各タスクの境界を示している。各タスクの仮想アドレス空間のグローバルアドレス領域を除いて、タスク1のアドレスはタスク2の同じアドレスとは独立している。

タスク（プロセス）がシステムコールを実行し、カーネルコードで実行されているとき、そのプロセスをカーネル動作中（または単にカーネルモード）と呼ぶ。この時点では、プロセッサは最高の特権レベル（レベル0）で実行されます。プロセスがカーネルモードの場合、実行されたカーネルコードは現在のプロセスのカーネルスタックを使用し、各プロセスは独自のカーネルスタックを持っています。プロセスがユーザー自身のコードを実行しているとき、そのプロセスはユーザーの実行状態（ユーザーモード）にあると言われます。つまり、プロセッサは現在、最も低い特権レベル（レベル3）のユーザーコードで実行されています。

ユーザープログラムが実行されているときに、割り込みハンドラプロシージャを実行するために突然中断された場合、ユーザープログラムは、プロセスのカーネル状態と象徴的に呼ぶこともできます。なぜなら、割込みハンドラは現在のプロセスのカーネルスタックを使用するからです。これは、カーネルモードのプロセスの状態と多少似ています。プロセスのカーネル状態とユーザーモードについては、後でプロセスの実行状態の項で詳しく説明します。

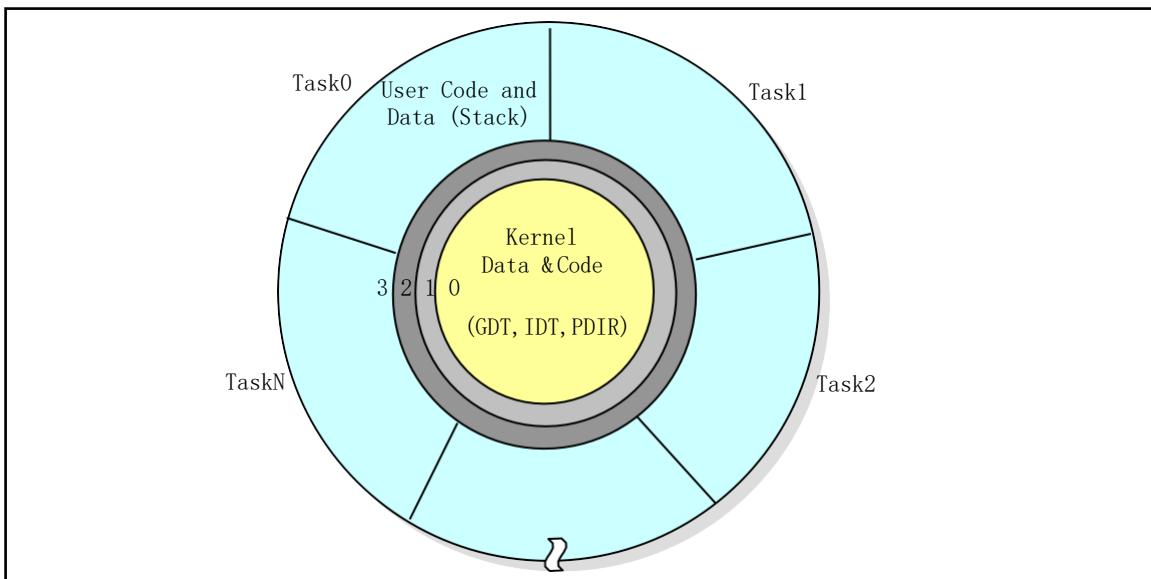


Figure 5-13 Multitasking protection system

### 5.3.6 仮想アドレス、リニアアドレス、物理アドレス

先に、メモリセグメンテーションとページングの仕組みによる、CPUのメモリ管理方法を説明しました。ここでは、Linux

0.12システムを例に、仮想アドレス空間、リニアアドレス空間、物理アドレス空間における、カーネルのコードとデータ、各タスクのコードとデータの対応を説明します。なお、タスク0とタスク1の生成・作成プロセスは特殊なので、別々に説明します。

#### カーネルコードとデータのアドレス

Linux

0.12では、`head.s`プログラムの初期化動作において、カーネルコードセグメントとデータセグメントの両方が16MBのセグメントに設定されています。この2つのセグメントの範囲は、リニアアドレス空間内で重複しており、リニアアドレス0からアドレス0xFFFFFFFまで、合計16MBのアドレス範囲となっています。この範囲には、すべてのカーネルコード、カーネルセグメントテーブル（GDT、IDT、TSS）、ページディレクトリテーブルとセカンダリページテーブル、カーネルローカルデータ、およびカーネル一時スタック（タスク0のユーザースタックとして使用される）が含まれます。そのページディレクトリテーブルと2次ページテーブルは、0～16MBのリニアアドレス空間を1つずつ物理アドレスにマッピングし、4つのディレクトリエントリ、つまり4つの2次ページテーブルを占有するよう設定されている。そのため、カーネルのコードやデータのアドレスについては、直接、物理メモリ上のアドレスと考えることができます。このとき、カーネルの仮想アドレス空間、リニアアドレス空間、物理アドレス空間の関係は、図5-14のように表すことができる。

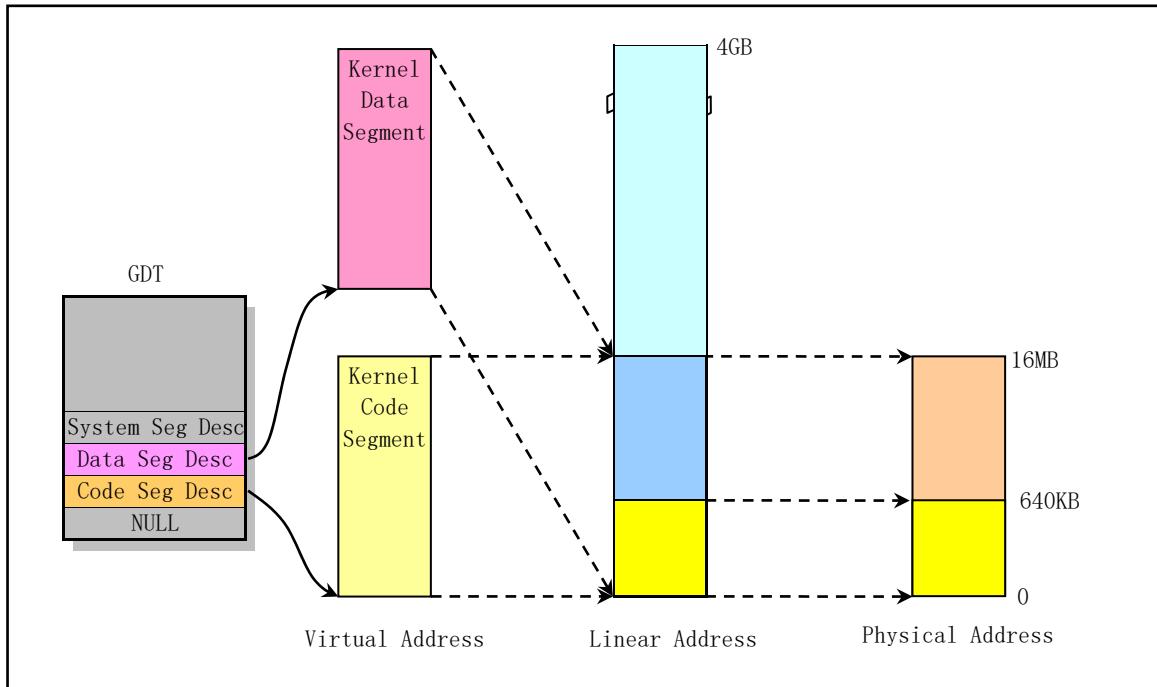


Figure 5-14 Kernel code and data segments in three address spaces

したがって、デフォルトでは、Linux

0.12カーネルは、最大16MBの物理メモリを管理することができ、4096の物理ページ（ページフレーム）、1ページあたり4KBを管理することができます。以上の分析を通して、次のことがわかります。

- ◆ カーネルコードとデータセグメント領域は、線形アドレス空間と物理アドレス空間で同じになります。この設定により、カーネルの初期化を大幅に簡略化することができます。
- ◆ GDTとIDTはカーネルデータセグメント内にあるため、そのリニアアドレスも物理アドレスと同じになります。リアルモードのsetup.sプログラムの初期化動作では、保護モードに入る前に設定しなければならない一時的なGDTとIDTを設定しました。この2つのテーブルは物理メモリ上の約0x90200の位置にあったため、プロテクトモードに入った後、カーネルシステムモジュールは物理メモリ0の開始位置にあり、0x90200のスペースは他の用途（キャッシング用）に使われてしまう。そこで、プロテクトモードに入った後、最初に実行しているプログラムのhead.sで2つのテーブルをリセットする必要があります。つまり、GDTRとIDTRを新しいGDTとIDTを指すように設定し、記述子も再読み込みする必要がある。しかし、ページング機構をオンにしても、2つのテーブルの位置は変わらないので、テーブルの位置を再設定したり、移動させたりする必要はないのです。
- ◆ タスク0以外のタスクが使用する物理メモリページは、少なくとも部分的にリニアアドレスのページとは異なるため、カーネルはメインメモリ領域で動的にマッピングして、ページディレクトリエントリやページテーブルエントリを動的に作成する必要があります。タスク1のコードとデータはカーネル内にもありますが、別途メモリを確保する必要があるため、独自のマッピングテーブルエントリも必要となります。

### Linux

0.12は、デフォルトで16MBの物理メモリを管理できますが、システムにそのような物理メモリを搭載する必要はありません。マシンに4MB（あるいは2MB）の物理メモリがあれば、Linux

0.12システムを動かすことができます。マシンに4MBの物理メモリしかない場合は、カーネルの4MB～16MBのアドレス範囲が存在しないアドレスにマッピングされます。しかし、これはシステムの動作を妨げるものではありません。なぜなら、カーネルメモリマネージャは、マシンの物理メモリの正確な量を

初期化時には、CPUのページング機構に、存在しない4MB～16MBへのリニアアドレスページのマッピングをさせません。カーネルのデフォルト設定は、主にシステムの物理メモリの拡張を容易にするためのもので、実際には存在しない物理メモリ領域を使用していません。システムが16MB以上の物理メモリを持っている場合、`init/main.c`プログラムの初期化で16MB以上のメモリの使用が制限されているため、ここではカーネルは0～16MBのメモリ範囲のみをマッピングします。そのため、16MB以上の物理メモリは使用されません。

もちろん、ここでカーネルにいくつかのページテーブルを追加し、`init/main.c`プログラムにマイナーな変更を加えることで、この制限を拡張することができます。例えば、システムに32MBの物理メモリがある場合、32MBのリニアアドレス範囲を物理メモリにマッピングするために、カーネルのコードとデータセグメント用に8つのセカンダリページテーブルエントリを作成する必要があります。

## タスク0のアドレス対応表

タスク0は、システムで手動で開始される最初のタスクです。コードとデータのセグメント長は640KBに設定されています。このタスクのコードとデータは、カーネルのコードとデータに直接含まれており、リニアアドレス0から始まる640KBの内容となっています。そのため、カーネルが設定したページディレクトリやページテーブルを直接利用して、ページングアドレス変換を行うことができます。同様に、そのコードとデータのセグメントは、リニアアドレス空間内で重なっています。対応するタスクステータスセグメントTSS0も手動で事前に設定され、タスク0のデータ構造情報の中に位置しています。`include/linux/sched.h`の156行目から始まるデータを参照してください。TSS0セグメントは、カーネルの`sched.c`ファイルのコード内にあり、長さは104バイトとなっています。詳細は、図5

- 24の「タスク0構造情報」の項目を参照してください。3つのアドレス空間におけるマッピングの対応を図5-15に示す。

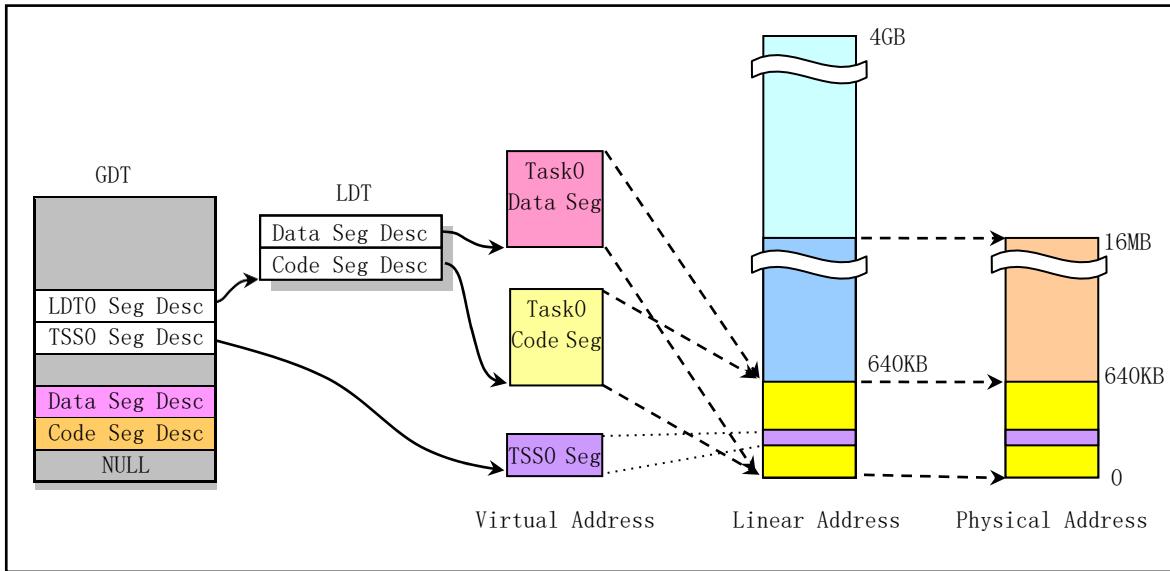


Figure 5-15 The relationship of task 0 in three address spaces

タスク0はカーネルコードに直接含まれているので、そのために追加のメモリページを割り当てる必要はありません。また、その動作に必要なカーネルモードのスタックとユーザーモードのスタック空間もカーネルコード領域にあり、カーネルページの初期化 (`head.s`) 以降、ページテーブルエントリのこれらのカーネルページのプロパティは`0b111`に設定されています。つまり、対応するページユーザーは読み書きができ、存在することができる。したがって、ユーザースタック `user_stack[]` 空間がカーネル空間にあるにもかかわらず、タスク0はそれに対して読み書きすることができます。

## タスク1 アドレス対応

タスク0と同様、タスク1も特別なタスクです。そのコードもカーネルコードエリアにあります。タスク0とは異なり、リニアアドレス空間では、`fork()`を使ってタスク（initプロセス）が生成されると、システムはタスク1の2次ページテーブルを格納するためのメモリページをメインメモリ領域に格納します。親プロセス（タスク0）のページディレクトリと2次ページテーブルのエントリはコピーされます。したがって、タスク1は独自のページディレクトリとページテーブルエントリを持ち、タスク1の線形空間の範囲である64MB～128MB（実際には64MB～64MB+640KB）を物理アドレス0～640KBにマッピングします。このとき、タスク1の長さも640KBで、コードセグメントとデータセグメントが重なり、1つのページディレクトリエントリと1つのセカンダリページテーブルしか占めていない。また、システムはタスク1に対して、タスクデータ構造とカーネルスタック空間を格納するためのメモリページを要求します。タスクデータ構造（プロセス制御ブロックPCBとも呼ばれる）情報には、タスク1のTSSセグメント構造情報が含まれています。図5-16を参照してください。

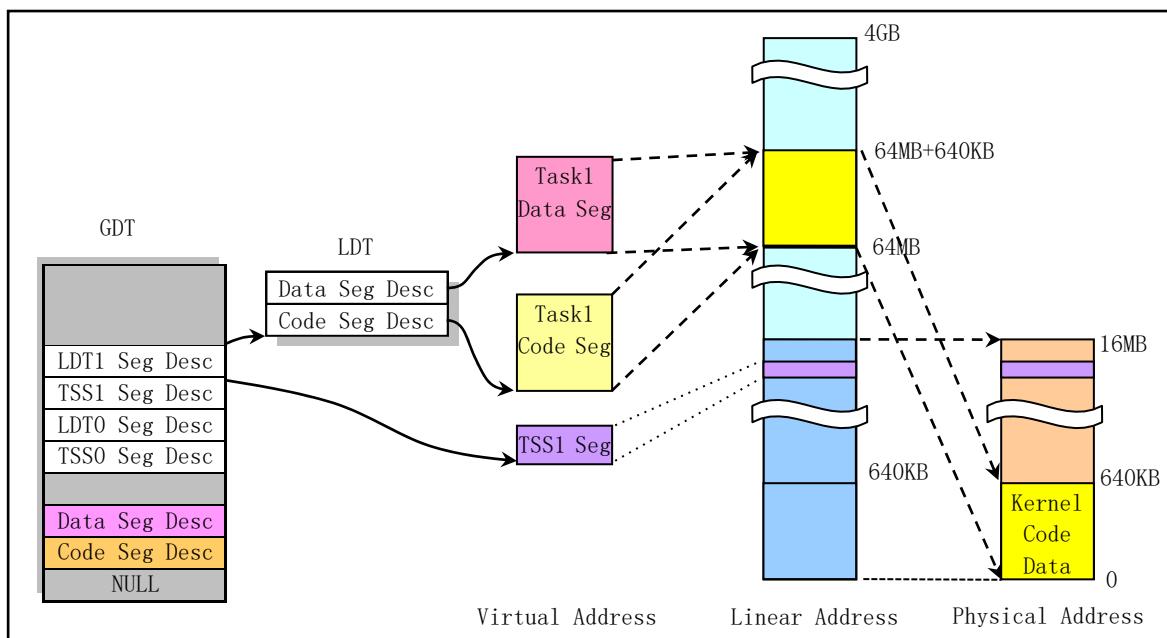


Figure 5-16 Task 1 relationship in three address spaces

タスク1のユーザモードスタック空間は、カーネルコード・データ領域（リニアアドレス0～640KB）にあるタスク0のユーザモードスタック空間`user_stack[]`を直接共有することになります（`kernel/sched.c`の82～87行目を参照）。そのため、タスク1のためにコピーされるスタックに無駄なデータが含まれないように、タスク1が実際に使用されるまで、このスタックは「クリーン」である必要があります。タスク1の生成開始時には、タスク0のユーザモードスタック`user_stack[]`がタスク1と共有されていますが、タスク1の実行開始時には、`user_stack[]`にマッピングされているページテーブルエントリは、読み取り専用に設定されています。これにより、タスク1がスタック操作を行うと書き込みページ例外が発生するため、カーネルは主記憶領域のページをユーザースタック空間として割り当てます。

## その他のタスクの対応

タスク2から作成された他のタスクについては、最終的な親プロセスはすべてinit（タスク1）プロセスです。Linux

0.12システムには、64個のプロセスがあることがすでにわかっています。以下では、タスク2を例にして、他のタスクによるアドレス空間の利用を説明します。

タスク2からは、タスク番号をnrとすると、リニアアドレス空間におけるタスクnrの開始位置は、 $nr * 64MB$ に設定されます。例えば、タスク2の開始位置 =  $nr * 64MB = 2 * 64MB =$

128MBです。タスクコードセグメントとデータセグメントの最大長は64MBに設定されているため、タスク2は128MBから192MBまでのリニアアドレス空間を占有し、合計で $64MB / 4MB = 16$ ページ分のディレクトリエントリを占有します。仮想空間内のタスクコードセグメントとデータセグメントは、同じ範囲のリニアアドレス空間にマッピングされているので、こちらも完全に重なっています。図5-17は、3つのアドレス空間におけるタスク2のコードセグメントとデータセグメントの対応関係を示しています。

タスク2が作成されると、その中でexecve()関数が実行され、シェルプログラムが実行されます。タスク1を複製してタスク2を作成したばかりのカーネルは、128MB--

128MB+640KBという直線的なアドレス空間を占有していることに加え、3つのアドレス空間におけるタスク2のコードとデータの関係はタスク1と同様である。タスク2のコード（init()）がexecve()システムコールを呼び出してシェルプログラムのロードと実行を開始すると、システムコールはタスク1からコピーしたページディレクトリとページテーブルのエントリと対応するメモリページを解放する。そして、新しい実行シェルのために、関連するページ・ディレクトリとページ・テーブル・エントリを再作成します。図5-

17は、タスク2がシェルプログラムの実行を開始したときの状況、つまり、タスク2のコードとデータがシェルプログラムのコードセグメントとデータセグメントによって元々コピーされていた場合を示しています。この図では、物理メモリの1ページ分がマッピングされている状況を示しています。ここで注意していただきたいのは、execve()関数を実行する際、システムはタスク2のためにリニアアドレス空間に64MBの空間範囲を割り当てていますが、カーネルはすぐにはタスク2のために物理メモリページを割り当ててマッピングしません。メモリマネージャは、タスク2の実行開始時に欠落ページフォールトによる例外が発生した場合にのみ、主記憶領域のリニアアドレス空間に物理メモリのページを割り当ててマッピングします。このように物理メモリのページを割り当ててマッピングする方法をロードオンデマンドといいます。メモリ管理」の章の関連説明を参照してください。

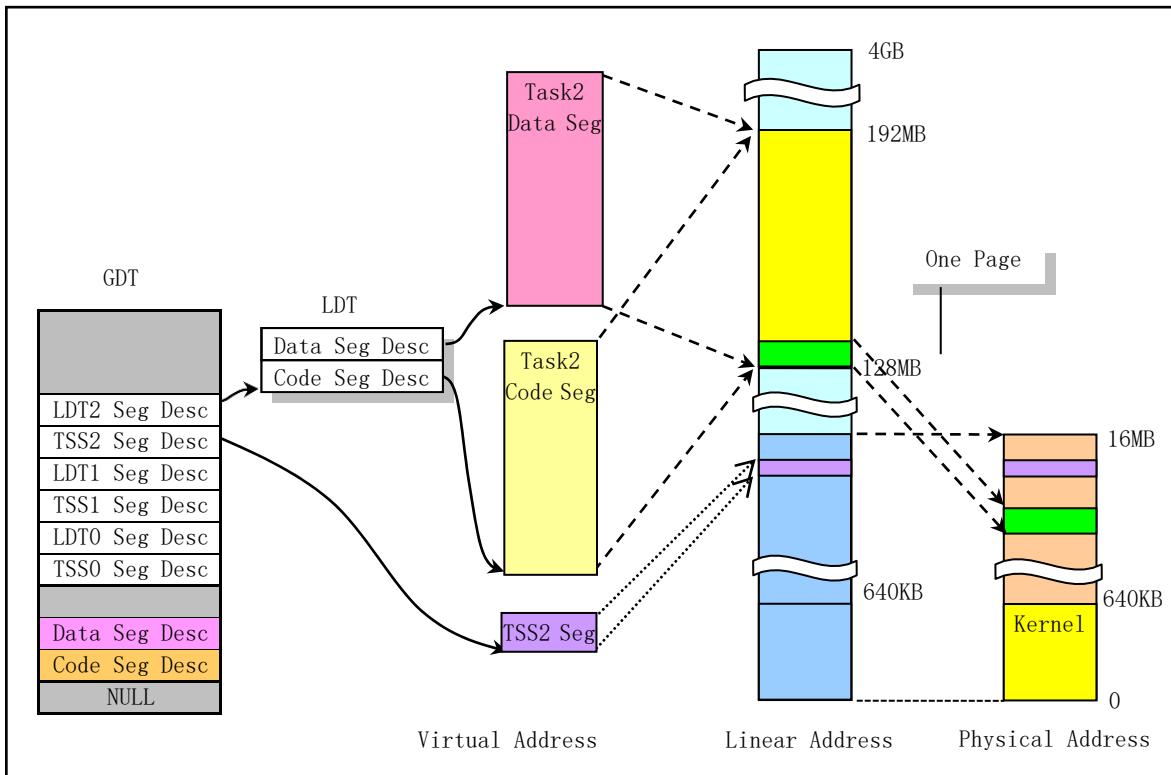


Figure 5-17 Correspondence in other task address spaces

Linuxカーネルのバージョン0.99以降、メモリ空間の使い方が変わりました。ページディレクトリテーブルを独立して使用することで、各プロセスは4Gアドレス空間の全範囲を楽しむことができます。を理解することができれば

本節で説明したメモリ管理の考え方を理解すれば、現在使われているLinux 2.xのカーネルで採用されているメモリ管理の原理がすぐに理解できます。紙面の都合上、ここでは説明を省略します。

### 5.3.7 メモリの動的割り当てのためのユーザーアプリケーション

ユーザープログラムがCライブラリのメモリ割り当て関数malloc()を使ってメモリを申請する場合、これらの動的アプリケーションのメモリ容量やサイズは、上位のCライブラリ関数malloc()が管理し、カーネル自身は介入しません。なぜなら、カーネルは、CPUの4Gリニアアドレス空間の中で、各プロセス（カーネルコードでメモリに常駐しているタスク0と1を除く）に64MBの領域を割り当てているからです。したがって、タスクやプロセスの実行範囲が64MBの範囲内であれば、カーネルも自動的に物理メモリページを割り当て、メモリページフォールト管理機構によって対応するページに対する操作をマッピングします。

しかし、カーネルは、プロセスが使用するコードとデータの空間のために、現在の位置の変数brkを保持しています。この変数値は、各プロセスのデータ構造に格納されています。これは、プロセス・アドレス空間におけるプロセス・コードおよびデータ（動的に割り当てられたデータ空間を含む）の終了位置を示す。malloc()関数は、プログラムにメモリを割り当てる際に、システムコールbrk()

によって、プログラムが要求する空間の長さをカーネルに通知します。カーネルコードは、`malloc()`から提供された情報に基づいて、`brk`の値を更新することができます。しかし、この時点では、新たに要求された空間のための物理メモリページはマッピングされていません。プログラムが対応する物理ページを持たないアドレスを指定した場合にのみ、カーネルは該当する物理メモリページに対してマッピング操作を行います。

あるデータがプロセスコードによってアドレス指定されているページが存在せず、そのページの位置がプロセスヒープスコープに属している場合、つまり実行ファイル・イメージファイルに対応するメモリ範囲に属していない場合、CPUはページフォルト例外を発生させる。そして、例外ハンドラで指定されたページの物理メモリページを割り当ててマッピングします。アプリケーションのメモリサイズと対応する物理ページの具体的な位置については、Cライブラリのメモリ割り当て関数`malloc()`が管理を行う。カーネルは物理メモリをページ単位で割り当て、マッピングする。この関数は、ユーザープログラムが何バイトのメモリを使用しているかを具体的に記録します。残りの容量は、プログラムがメモリを再申請したときに使えるように確保される。

ユーザープログラムが関数`free()`を使って要求されたメモリブロックを動的に解放すると、Cライブラリのメモリ管理関数は、プログラムが再度メモリを要求した場合に備えて、解放されたメモリブロックをフリーとマークします。カーネルがこのプロセスに割り当てた物理ページは、このプロセス中は解放されません。プロセスが終了して初めて、カーネルは、プロセスのアドレス空間に割り当てられマッピングされたすべての物理メモリページを完全に取り戻します。

ライブラリ関数`malloc()`と`free()`の具体的な実装コードは、カーネルライブラリ内の`lib/malloc.c`プログラムにあります。

## 5.4 インタラプトメカニズム

ここでは、割り込み機構の基本原理と、それに関連するプログラマブルコントローラのハードウェアロジック、およびLinuxシステムでの割り込みの使用方法について説明します。なお、プログラマブルコントローラの具体的なプログラミング方法については、次章の`setup.s`プログラム以降の記述を参照してください。

### 5.4.1 割り込み動作の原理

マイクロコンピュータシステムには、通常、入力デバイスと出力デバイスがあります。プロセッサが提供する一つの方法は

これらのデバイスにサービスを提供するには、ポーリングを使用します。この方法では、プロセッサがシステム内の各デバイスに順次問い合わせを行い、サービスが必要かどうかを「照会」します。この方法は、ソフトウェアのプログラミングが簡単なのが利点ですが、プロセッサのリソースを消費し、システムのパフォーマンスに影響を与えるのが欠点です。

デバイスにサービスを提供するもう一つの方法は、デバイスがサービスを必要とするときに、プロセッサ自身に要求を出すことです。また、プロセッサは、デバイスから要求された場合にのみ、デバイスにサービスを提供する。デバイスがプロセッサにサービス要求を行うと、プロセッサは、現在の命令が実行されるとすぐにデバイスの要求に応答し、デバイスの関連するサービスプログラムを実行します。サービスプログラムが実行されると、プロセッサは先ほど中断されたプログラムを続けて

実行します。このような処理を「割り込み方式」といい、デバイスがプロセッサに送るサービス要求を「IRQ Interrupt」といいます。

Request」といいます。その要求に応じてプロセッサが実行するデバイス関連のプログラムを「割り込みサービスルーチン」または「ISR」と呼びます。

PIC (Programmable Interrupt Controller) は、マイコンシステムにおいて、デバイスの割り込み要求を管理するアドミニストレータです。PICは、デバイスに接続された割り込み要求端子を介して、デバイスからターミナルサービスリクエスト信号を受け取ります。デバイスが割り込み要求IRQ信号をアクティブにすると、PICはすぐにそれを検出します。複数のデバイスから同時に割り込みサービス要求を受信した場合、PICはそれらを優先し、最も優先度の高い割り込み要求を選択して処理します。また、プロセッサがあるデバイスの割り込みサービスルーチンを実行中の場合、PICは選択された割り込み要求と処理中の割り込み要求の優先度を比較し、その比較に基づいてプロセッサに割り込みを発行するかどうかを判断する必要があります。PICがプロセッサのINT端子（図5-18のINTR端子）に割り込みを発行すると、プロセッサはその時点で行っていた処理を直ちに停止し、どの割り込みサービスリクエストを実行するかをPICに問い合わせます。PICは、割り込み要求に対応する割り込み番号をデータバスに送信することで、どの割り込みサービス処理を実行するかをプロセッサに通知します。プロセッサは、読み込んだ割り込み番号に応じて、割り込みベクタテーブル（32ビットプロテクトモードでは割り込みディスクリプタテーブルIDT）を問い合わせることにより、当該デバイスの割り込みベクタ（すなわち、割り込みサービスルーチンのアドレス）を取得し、割り込みサービスルーチンの実行を開始する。割り込みサービスルーチンの実行が終了すると、プロセッサは割り込み信号によって中断されたプログラムの実行を継続します。

これまで説明してきたのは、入出力デバイスの割り込みサービス処理です。しかし、割り込み方式は必ずしもハードウェアに依存するものではなく、ソフトウェアでも利用することができます。INT命令を使用し、そのオペランドで割り込み番号を示すことで、プロセッサを実行して対応する割り込み処理を行うことができます。PC/ATシリーズのマイクロコンピュータは256個の割り込みをサポートしていますが、そのほとんどがソフトウェア割り込みや例外に使用されています。例外とは、プロセッサが処理中にエラーを検出して発生する割り込みのことです。本機では、以下に挙げる割り込みのうち一部のみが使用されています。

#### 5.4.2 80X86 PCのインターラプトサブシステム

8259Aプログラマブル割り込みコントローラチップは、80X86で構成されるマイクロコンピュータシステムに使用されます。各8259Aチップは8つの割り込みソースを管理できます。マルチチップカスケードにより、8259Aは最大64個の割り込みベクタを管理するシステムを構成することができます。PC/ATシリーズ互換機では、2つの8259Aチップで15レベルの割り込みベクタを管理しています。カスケードの模式図を図5-18に示します。スレーブチップのINT端子は、マスターチップのIR2端子に接続されています。つまり、8259Aスレーブチップが送信する割り込み信号は、8259AマスターチップのIRQ2入力信号となります。マスターの8259Aチップのポートベースアドレスは0x20、スレーブのチップは0xA0です。IRQ9端子の機能は、PC/XTのIRQ2と同じです。つまり、PC/AT機では、IRQ2を使用しているデバイスのIRQ2端子をPICのIRQ9端子にリダイレクトするハードウェア回路を使用し、BIOSのソフトウェアを使用してIRQ9に割り込みをかけます。Int 71はIRQ2の割り込みにリダイレクトする int 0x0A

割り込みハンドラプロシージャです。これにより、IRQ2を使用するPC/XT搭載の8ビットカードが、PC/AT機の下で正しく機能するようになりました。PCシリーズの下位互換性を実現した。

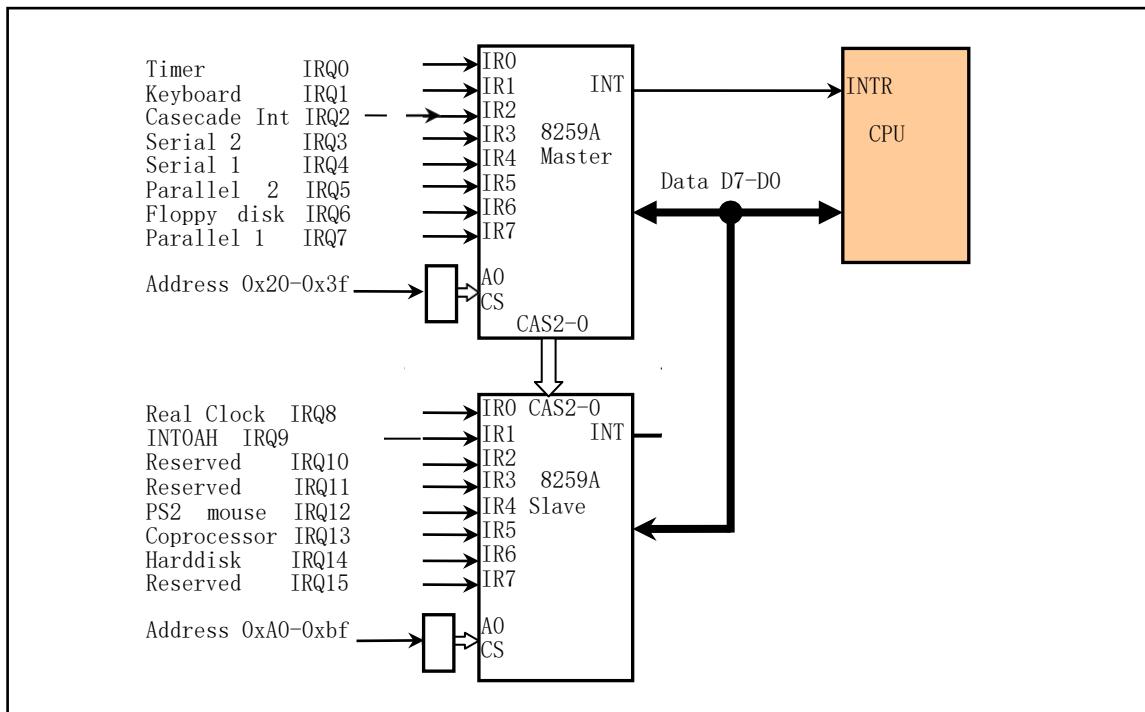


Figure 5-18 PC/AT microcomputer cascaded 8259 control system

バスコントローラの制御により、8259Aチップは、プログラミング状態と動作状態になります。プログラミング状態とは、CPUがIN命令やOUT命令を用いて8259Aチップを初期化している状態です。初期化のプログラミングが完了すると、チップは動作状態に入ります。この時、チップは外部デバイスから提案された割り込み要求(IRQ0～IRQ15)にいつでも応答することができ、また、システムは操作コマンドワードを使用して割り込み処理モードをいつでも変更することができます。割り込みアービトレーション選択機構により、チップは現在の最優先割り込み要求を割り込みサービスオブジェクトとして選択し、CPU端子INTによりCPUに割り込み要求を通知します。CPUが応答した後、チップはデータバスD7-D0から現在のサービスオブジェクトのプログラムされた割り込み番号を送信し、CPUは対応する割り込みベクタ値を取得し、割り込みサービスルーチンを実行します。

### 5.4.3 割り込みベクターテーブル

前節では、CPUは割込みサービスルーチンのエントリアドレス値に対応する割込み番号に基づいて割込みベクタ値をフェッチすることを示しました。したがって、CPUが割込み番号から対応する割込みベクターを見つけるためには、メモリ上にロックアップテーブル、すなわち割込みベクターテーブルを作成する必要があります（32ビット保護モードでは、このテーブルを割込みディスクリプターテーブルIDTと呼びます、後述します）。

80X86マイコンは256本の割り込みをサポートしており、割り込みごとに割り込みサービスルーチンが必要となります。80X86のリアルモードモードでは、各割り込みベクターは4バイトで構成されています。この4バイトは、割込みサービスルーチンのセグメント値とセグメント内オフセット値

を示します。このため、ベクターテーブル全体の長さは $4 \times 256 = 1024$ バイトとなります。80X86マイクロコンピュータの起動時には、ROM内のプログラムが

BIOSは、物理メモリの開始アドレス0x0000:0x0000に割り込みベクターテーブルを初期化して設定し、各割り込みに対するデフォルトの割り込みサービスルーチンをBIOSに与えます。割り込みベクターテーブルのベクタは割り込み番号の順に並んでいるので、割り込み番号Nが与えられた場合、対応する割り込みベクタのメモリ上の位置は0x0000 : N

\*

4、つまり対応する割り込みサービスプログラムのエントリアドレ스は物理メモリ0x0000 : N  
4の位置に格納されます。

\*

BIOSが初期化操作を行うと、2つの8259Aチップがサポートする16個のハードウェア割り込みベクターと、BIOSが提供する割り込み呼び出し機能に割り込み番号0x10-0x1Fを設定します。実際に使用されない割り込みについては、ベクターに一時的なダミーの割り込みサービスルーチンのアドレスが入力されます。その後、システムがOSを起動する際に、実際の必要性に応じていくつかの割り込みベクターの値が変更されます。例えば、DOSオペレーティングシステムの場合は、割り込み0x20-

0x2Fの割り込みベクター値をリセットして修正します。Linuxシステムの場合は、最初にカーネルをロードしたときにBIOSが提供するディスプレイとディスクリードの割り込みに加えて、新しい割り込みベクターテーブルが作成されます。つまり、setup.sプログラムで8259Aチップを再初期化し、head.sプログラムで割り込みベクターテーブル（割り込みディスクリプターテーブル）を再構築しています。そのため、カーネルが正常に動作した後のLinuxでは、BIOSの割り込みベクターテーブルを完全に放棄します。

インテルCPUが32ビットプロテクトモードで動作している場合、割り込みや例外を管理するためにInterrupt Descriptor Table (IDT)を使用する必要があります。IDTは、インテル8086～80186のCPUで使用されていた割り込みベクターテーブルをそのまま置き換えたものです。IDTの役割は、割り込みベクターテーブルと似ていますが、各割り込み記述子エントリには、割り込みサービスルーチンのアドレスに加えて、特権レベルと記述子クラスの情報が含まれています。Linux

OSは80X86プロテクトモードで動作するため、割り込みディスクリプターテーブルを使用して、各割り込みの「ベクター」情報を設定・保存します。

#### 5.4.4 Linuxカーネルの割り込み処理

Linuxカーネルの場合、割り込み信号は通常、ハードウェア割り込みとソフトウェア割り込み（または例外）の2つのカテゴリーに分けられます。各割込みは、割込み番号と呼ばれる0～255の数字で識別されます。割り込みINT0-INT31 (0x00-0x1f) については、表5-

1に示すように、各割り込みの機能がインテル社によって固定または予約されています。上の項からもわかるように、BIOSで設定された割り込み番号の範囲はそれと相反するものです。

Table 5-1 Exceptions and Interrupts reserved by Intel Co.

Vector No	Name	Type	Error Code	Signal	Source
0	Devide error	Fault (Error)	No	SIGFPE	DIV and IDIV instructions.
1	Debug	Fault/Trap	No	SIGTRAP	Any code or data reference or the INT instruction.
2	nmi	Interrupt	No		Non maskable external interrupt.
3	Breakpoint	Trap	No	SIGTRAP	INT 3 instruction.
4	Overflow	Trap	No	SIGSEGV	INTO instruction.
5	Bounds check	Fault	No	SIGSEGV	BOUND instruction.
6	Invalid Opcode	Fault	No	SIGILL	UD2 instruction or reserved opcode.
7	Device not available	Fault	No	SIGSEGV	Floating-point or WAIT/FWAIT instruction.
8	Double fault	Abort	Yes(0)	SIGSEGV	Any instruction that can generate an exception, NMI, or an INTR.
9	Coprocessor seg overrun	Abort	No	SIGFPE	Floating-point instruction.
10	Invalid TSS	Fault	Yes	SIGSEGV	Task switch or TSS access.
11	Segment not present	Fault	Yes	SIGBUS	Loading segment registers or accessing system segments.
12	Stack segment	Fault	Yes	SIGBUS	Stack operations and SS register loads.
13	General protection	Fault	Yes	SIGSEGV	Any memory reference and other protection checks.
14	Page fault	Fault	Yes	SIGSEGV	Any memory reference.
15	Intel reserved		No		
16	Coprocessor error	Fault	No	SIGFPE	Floating-point or WAIT/FWAIT
17	Alignment check	Fault	Yes(0)		Any data reference in memory.
20-31	Intel reserved.				
32-255	User Defined interrupts	Interrupt			External interrupt or INT n instruction.

これらの割り込みはソフト割り込みですが、インテルでは例外と呼んでいます。なぜなら、これらの割り込みは、CPUが命令を実行する際に検出された異常な状態によって引き起こされるからです。通常、フォールトとトラップの2つに分けられます。割り込みINT32--INT255 (0x20--0xff) は、ユーザーが設定・定義することができます。すべての割り込みの分類と、実行後のCPUの動作方法を表5-2に示します。

Table 5-2 Interrupt classification and how the CPU handles it

Interrupt	Name	CPU Check Method	Processing Method
Hardware	Maskable	CPU pin INTR	Clear the IF maskable interrupt flag of EFLAGS.
	Nonmaskable	CPU pin NMI	Non-Maskable Interrupts.
Software	Fault	Detected before error occurred	CPU re-executes the instruction that caused the error.
	Trap	Detected after error occurred	CPU continues to execute the following instruction.
	Abort	Detected after error occurred	Programs that caused this error should be terminated.

Linuxシステムでは、INT32--INT47（0x20--0x2f）が、8259A割り込み制御チップ（表5-3参照）が発行するハードウェア割り込み要求信号IRQ0--IRQ15に対応し、ユーザー・プログラムが発行するソフトウェア割り込みをINT128（0x80）に設定することを、システムコール（System Call）割り込みと呼びます。システムコール割り込みは、オペレーティング・システムのリソースを使用するユーザー・プログラムの唯一のインターフェースです。

Table 5-3 List of interrupt numbers for Linux system interrupt requests

Interrupt Request No.	Interrupt No.	Purpose
IRQ0	0x20 (32)	100HZ clock interrupt signal from 8253 chip
IRQ1	0x21 (33)	Keyboard interrupt
IRQ2	0x22 (34)	Cascade to slave chip
IRQ3	0x23 (35)	Serial port 2
IRQ4	0x24 (36)	Serial port 1
IRQ5	0x25 (37)	Parallel port 2
IRQ6	0x26 (38)	Floppy disk drive
IRQ7	0x27 (39)	Parallel port 1
IRQ8	0x28 (40)	Real clock
IRQ9	0x29 (41)	Reserved
IRQ10	0x2a (42)	Reserved
IRQ11	0x2b (43)	Reserved (Network interface)
IRQ12	0x2c (44)	PS/2 mouse
IRQ13	0x2d (45)	Coprocessor
IRQ14	0x2e (46)	Harddisk
IRQ15	0x2f (47)	Reserved

システムの初期化時、カーネルはまずダミーの割込みベクター（割込み記述子）を使用して、割込み記述子テーブル（IDT）の256個の記述子をすべてデフォルト設定にします。このダミーの割込みベクターは、デフォルトの「割込みなし」のハンドラプロシージャを指します。割り込みが発生し、割り込みベクターがリセットされていない場合、「Unknown interrupt」というメッセージが表示されます。システムで使用する必要がある一部の割り込みについては、カーネルは初期化を続ける過程でこれらの割り込みの割り込み記述子項目を再編集し、対応する実際のハンドラプロシージャを指すようにします。通常、例外割り込み処理（INT0～INT31）はtraps.cの初期化関数でリセットされ、システムコール割り込みint128はスケジューラの初期化関数でリセットされます。

また、Linuxカーネルは、割り込みディスクリプターテーブルIDTの設定時に、割り込みゲートとトラップゲートの両方のディスクリプターを使用します。両者の違いは、フラグレジスタEFLAGS内の割込みイネーブルフラグIFへの影響です。割り込みゲート記述子によって実行された割り込みは、IFフラグをリセットするので、他の割り込みが現在の割り込み処理を妨害することを防ぐことができる。続く割込み終了命令IRETは、スタックからIFフラグの元の値を復元します。トラップゲートを介して実行される割込みは、IFフラグに影響を与えません。

### 5.4.5 フラグレジスタのインタラプトフラグ

クリティカル・コード・エリアの競合と混乱を避けるために、Linux 0.12カーネル・コードの多くの場所でCLI命令とSTI命令が使用されています。CLI命令は、CPUフラグレジスタの割り込みフラグIFをリセットするために使用され、CLI命令を実行した後、システムが外部からの割り込みに反応しないようにします。STI命令は、CPUが外部機器からの割り込みを認識して応答できるように、フラグレジスタの割り込みフラグを設定するために使用されます。

競合状態を引き起こす可能性のあるコード領域に入る場合、カーネルはCLI命令を使用して外部割込みへの応答をオフにし、コンテンツコード領域を実行する際にSTI命令を実行してCPUの外部割込みへの応答を再度許可するようになります。例えば、ファイルスーパーblockのロックフラグの変更や、タスクの入退出待ちキューの操作を行う場合、まずCLI命令でCPUの外部割込みへの応答を禁止し、操作完了後にSTI命令で外部割込みへの応答を有効にする必要があります。CLI,STI命令のペアを使用しない場合、つまりCLIを使用して外部割込みへの応答を無効にせずにファイルのスーパーblockを修正する必要がある場合、修正前にスーパーblockロックフラグが設定されていないと判断され、このフラグを設定したい場合があります。ちょうどこのタイミングでシステムロックの割り込みが発生し、他のタスクの実行に切り替わり、たまたま他のタスクもスーパーblockを修正する必要があった場合、この他のタスクがまずスーパーblockのロックフラグを設定し、スーパーblockを修正します。システムが元のタスクに切り替わると、この時、タスクはロックフラグを判定せず、設定されたスーパーblockのロックフラグを実行し続けるため、2つのタスクが同時にクリティカルコード領域に対して複数の操作を行い、スーパーblockのデータを引き起こすことになります。不整合は、深刻な場合、カーネルシステムのクラッシュにつながる可能性があります。

## 5.5 Linuxシステムコール

### 5.5.1 システムコールインターフェース

システムコール（通称：シスコール）は、図5-4に示すように、Linuxカーネルが上流のアプリケーションと通信できる唯一のインターフェースである。割り込み機構の説明から、ユーザプログラムは、割り込みint 0x80を直接または（ライブラリ関数を介して）間接的に呼び出し、EAXレジスタにシステムコール関数番号を指定することで、システムハードウェアリソースを含むカーネルリソースを利用することができます。しかし、通常、アプリケーションは、図5-19に示すように、標準的なインターフェース定義を持つCライブラリの関数を使って間接的にカーネルのシステムコールを使用します。

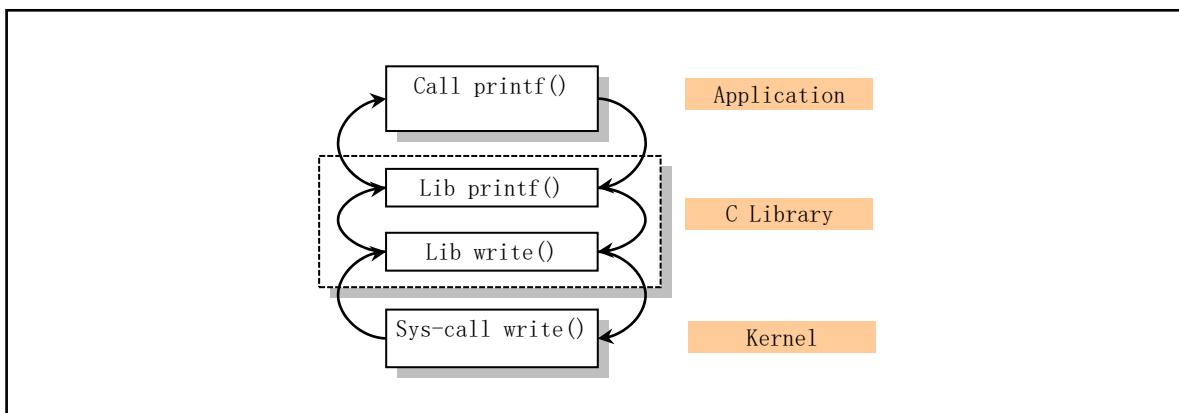


Figure 5-19 Relationship between user programs, library functions, and kernel system calls

通常、システムコールは関数形式で行われるため、1つ以上のパラメータを取ることができます。システムコールの実行結果は、戻り値で表されます。通常、負の値はエラーを、0は成功を表します。エラーの場合は、間違った型のコードがグローバル変数errnoに格納されます。ライブラリ関数の perror() を呼び出すことで、エラーコードに対応するエラー文字列情報を出力することができます。

Linuxカーネルでは、各システムコールに固有のシステムコール関数番号が設定されています。カーネル0.12には、合計87個のシステムコール機能（0～86）があります。これらの機能番号は、include/unistd.hというファイルの62行目の先頭で定義されています。例えば、writeシステムコールの機能番号は4で、シンボルである

NR\_writeです。これらのシステムコール関数番号は、実際にはinclude/linux/sys.hで定義されているシステムコールハンドラポインタの配列テーブルsys\_call\_table[]の項目のインデックスに対応しています。つまり、write()システムコールのハンドラポインタは配列の項目4にあります。

これらのシステムコールシンボルを自分のプログラムで直接使用したい場合は、以下のように、ファイル「<unistd.h>」をインクルードする前にシンボル「LIBRARY」を定義する必要があります。

---

```
#define LIBRARY
#include <unistd.h>
```

---

また、`sys_call_table[]`から、カーネル内のすべてのシステムコールハンドラの名前は基本的にシンボル「`sys_`」で始まっていることがわかります。例えば、カーネルのソースコードにおけるシステムコール`read()`の実装関数は`sys_read()`です。

### 5.5.2 システムコール処理

アプリケーションがライブラリ関数を介してカーネルに割込みINT 0x80を発行すると、システムコールが開始されます。システムコール番号はレジスタEAXに格納され、渡されたパラメータはレジスタEBX、ECX、EDXに順番に格納することができる。したがって、Linux

0.12カーネルのユーザープログラムは、最大3つのパラメータをカーネルに直接渡すことができる。もちろん、パラメータを受け取らないことも可能です。システムコール割り込みINT 0x80を処理する処理は、プログラム`kernel/system_call.s`の`system_call`です。

システムコールの実行を容易にするために、カーネルのソースコードにはマクロ関数である`include/unistd.h`ファイル内の`_syscalln()`（150～200行）で、`n`は運ばれるパラメータの数を表し、それぞれ0～3となります。したがって、最大3個のパラメータを直接渡すことができます。大きなチャփデータをカーネルに渡す必要がある場合は、チャփデータのポインタを渡すことができます。例えば、`read()`システムコールの場合、その定義は次の通りです。

```
int read(int fd, char *buf, int n);
```

対応するシステムコールをユーザープログラムで直接実行すると、そのシステムコールのマクロは

---

```
#define LIBRARY
#include <unistd.h>

_syscall3(int, read, int, fd, char *, buf, int, n)
```

---

つまり、Cライブラリを介さずに、ユーザープログラムで直接上記の`_syscall3()`を使って、システムコール`read()`を実行することができるのです。実際、C関数ライブラリでの関数呼び出しの形式は、ここで与えられたものと同じです。

`include/unistd.h`で指定された各システムコールマクロには、 $2+2*n$ 個のパラメータがあります。最初のパラメータは、システムコールの戻り値のタイプに対応し、2番目のパラメータは、システムコールの名前であり、その後にシステムコールによって運ばれるパラメータのタイプと名前が続く。このマクロを、以下のように、インラインのアセンブリ文を含むC関数に拡張します。

---

```

int read(int fd, char *buf, int n)
{
    long __res;
    __asm volatile
        ( "int $0x80"
        : "=a" (__res)
        : "0" (_NR_read), "b" ((long)(fd)), "c" ((long)(buf)), "d" ((long)(n)));
    if (__res >= 0)
        return __res;
    errno = -__res;
    return -1;
}

```

---

このマクロは、読み取りシステムコールの具体的な実装として展開されていることがわかります。埋め込みアセンブリステートメントを使用して、Linuxシステム割り込みコール0x80を、関数番号 NR\_read(3)です。この割り込みコールは、実際に読み込んだバイト数をEAX(res)レジスタに返します。返された値が0より小さい場合は、読み出し動作のエラーが発生したことを意味しますので、エラー番号を反転させて

グローバル変数errnoに格納され、-1の値が呼び出したプログラムに返されます。

システムコールが3つ以上のパラメータを必要とする場合、カーネルは通常、パラメータをパラメータバッファブロックとして使用し、バッファブロックのポインタをパラメータとしてカーネルに渡します。そのため、3つ以上のパラメータを持つシステムコールでは、1つの引数を持つマクロ\_sys\_call1()を使用するだけで、最初の引数のポインタをカーネルに渡すことができます。例えば、select()関数のシステムコールには5つの引数がありますが、その第一引数のポインタを渡すだけでよいのです。fs/select.cプログラムの説明をご覧ください。

カーネル内でカーネルコールハンドラkernel/sys\_call.sに入ると、system\_callコードは、まずEAXのシステムコール関数番号が有効なシステムコール番号の範囲内にあるかどうかをチェックします。そして、sys\_call\_table[]関数ポインタテーブルの呼び出しに従って、対応するシステムコールハンドラを実行します。

---

call _sys_call_table(%eax, 4)	// kernel/sys_call.s 第 99 行。
-------------------------------	------------------------------

---

このアセンブリステートメントのオペランドの意味は、\_sys\_call\_table + %eax \* 4の関数を間接的に呼び出すことです。

sys\_call\_table[]のポインタはそれぞれ4バイトなので、システムコール関数の番号を乗じる必要があります。

4.そして、その結果得られた値を使って、呼び出されたハンドラのアドレスをテーブルから取得します。

### 5.5.3 Linuxシステムコールのパラメータ受け渡し方法

Linuxのユーザプロセスがシステム割り込みコールプロシージャにパラメータを渡す場合、LinuxシステムではレジスタEBX、ECX、EDXなどの汎用的なレジスタ転送手段を使用します。このレジスタパッシング・パラメータを使用する方法の大きな利点は、システム割り込みサービスルーチンに入

ってレジスタ値を保存する際に、パラメータを渡したレジスタも自動的にカーネル状態のスタックに置かれることです。そのため、パラメータを渡したレジスタを特別に処理する必要はありません。これが、当時のリーナス氏が知っていた最もシンプルで高速なパラメータ転送方法である。また、インテルのCPUが提供するシステムコールゲートを利用したパラメータ転送方法もあり、これは渡されたパラメータをプロセスのユーザー状態スタックとカーネル状態スタックに自動的にコピーするものである。しかし、この方法で使われている方法はもっと複雑だ。

また、各システムコールハンドラでは、渡されたパラメータを検証し、すべてのパラメータが合法かつ有効であることを確認する必要があります。特に、ユーザーが提供したポインターは、ポインターが指すメモリ領域の範囲が有効であり、適切な読み取り権限と書き込み権限を持っていることを厳密に確認する必要があります。

## 5.6 システムの時間とタイミング

### 5.6.1 システム時間

オペレーティングシステムが自動的に正確な現在の時刻と日付の情報を提供できるようにするために、PC/ATマイクロコンピュータシステムでは、バッテリー駆動のリアルタイムRT（Real Time）回路のサポートが提供されています。通常、この回路部分は、システム情報を保持する少量のCMOS RAMと一緒に1チップに集積されているので、この部分はRT/CMOS RAM回路と呼ばれる。モトローラ社のMC146818チップは、PC/ATマイクロコンピュータまたはその互換機に使用されている。

#### 初期化時、Linux

0.12カーネルは、チップに格納されている現在の時刻と日付の情報を読み取り、1970年1月1日0:00からの秒単位の現在時刻に変換します。これをUNIXカレンダータイムと呼んでいます。この時刻は、システムが動作を開始する暦上の時刻を決定し、グローバル変数`startup_time`に保存され、すべてのカーネルコードが使用できるようになります。ユーザープログラムは、システムコールの`time()`を使って、この時刻の値を読み取ります。

`startup_time`、一方、スーパーユーザーは`stime()`を呼び出してシステム時間の値を変更することができます。

また、プログラムは、システムスタートからカウントされた以下のシステムチック値のjiffiによって、現在の実行時間を一意に決定することができます。各目盛りは後述のタイマーによって生成されます。各目盛りのタイミング値は10ミリ秒であるため、現在時刻のコードへのアクセスを容易にするために、カーネルコードにマクロが定義されています。このマクロは`include/linux/sched.h`ファイルの192行目に定義されており、以下のような形式になっています。

---

```
#define CURRENT_TIME (startup_time + jiffies/HZ)
```

---

中でも`HZ=100`は、コアシステムのクロック周波数です。現在時刻マクロ`CURRENT_TIME`は、システムの起動時間`startup_time`に、起動後にシステムが動作している時間`jiffies/100`を加えたものと定義されています。このマクロは、ファイルがアクセスされたときや、その`i-node`が変更されたときの時間を修正するときに使用されます。

## 5.6.2 システムタイミング

システムの基本的なタイミングビートは、タイミングチップによって生成されます。Linuxの初期化時に

0.12カーネルの場合、PCのプログラマブル・タイミング・チップIntel

8253 (8254) のカウンタ・チャネル0はモード3で動作するように設定され、初期カウント値LATCHは10ミリ秒ごとに出力OUTに矩形波の立ち上がりエッジを発するように設定されています。8254チップのクロック入力周波数は1.193180MHzなので、初期カウント値LATCH=1193180/100は約11931となります。OUT端子はプログラマブルな割り込み制御チップのレベル0に接続されているため、システムは10ミリ秒ごとにクロック割り込み要求 (IRQ0) を発行します。このタイムビートがOSのパルスであり、これをシステムチックあるいはシステムクロックサイクルと呼んでいます。したがって、1ティックの時間が経過するたびに、システムはクロック割り込みハンドラ (timer\_interrupt) を呼び出します。

クロック割り込みハンドラ	timer_interrupt
--------------	-----------------

は、主にシステムが起動してから経過したクロックティックの数を	jiffies
--------------------------------	---------

変数で累積するために使用されます。jiffiesの値は、クロック割込みが発生するたびに1ずつ増加します。その後、C言語の関数do\_timer()を呼び出して処理を進めます。呼び出し時のパラメータCPLは、割り込みプログラムのセグメントセレクタ（スタックに格納されているCSセグメントレジスタの値）から、現在のコード特権レベルCPLを取得します。

do\_timer()関数は、特権レベルに基づいて、現在のプロセスの実行時間を蓄積する。CPL=0の場合、プロセスがカーネルモードで実行されているときに中断されていることを意味するので、カーネルはプロセスのカーネル状態の実行時間stimeを1つ増やし、そうでなければプロセスのユーザ状態の実行値を1つ増やします。フロッピーディスクプログラムfloppy.cが動作中にタイマーを追加した場合、タイマーリストが処理されます。タイマーが期限切れ（デクリメント後に0になる）になると、そのタイマーのハンドラが呼び出されます。その後、現在のプロセス実行時間が処理され、現在のプロセス実行タイムスライスが1つデクリメントされます。タイムスライスとは、プロセスが切り替わる前に実行し続けることができるCPU時間のことです。単位は、上記で定義したティック数です。プロセスのタイムスライスの値がデクリメントされ、まだ0より大きい場合は、そのタイムスライスが使い切られていないことを意味するので、do\_timer()を終了し、現在のプロセスの実行を継続する。この時、プロセスのタイムスライスがデクリメントされて0になってしまえば、そのプロセスがCPUのタイムスライスを使い切ったことを意味し、プログラムは中断されたプログラムのレベルに応じて、さらなる処理方法を決定する。中断された現在のプロセスがユーザーモードで動作している(特権レベルが0より大きい)場合、do\_timer()はスケジューラのschedule()を呼び出し、実行する別のプロセスに切り替えます。中断された現在のプロセスがカーネルモードで動作している場合、つまり、カーネルプログラムで実行中に中断された場合、do\_timer()は直ちに終了します。したがって、この処理方法は、Linuxシステムプロセスがカーネルモードで動作しているときに、スケジューラによって切り替えられないことを決定します。つまり、カーネルモードで動作しているときは、プロセスはノンプリエンプティブである

のプログラムである。

上記のタイマーコードは、フロッピーモーターのオンとオフのタイミング操作に特化していることに注意してください。この

この種のタイマーは、最新のLinuxシステムに搭載されているダイナミックタイマーと同様に、カーネルのみで使用されます。このようなタイマーは、必要に応じて動的に作成し、タイミングが切れたら動的に取り消すことができます。Linuxでは

0.12カーネルでは、最大64個のタイマーが同時に動作します。タイマーの処理コードは、`sched.c` プログラム283--368行目にあります。

## 5.7 Linuxプロセスコントロール

プログラムとは、実行可能なファイルのこと、プロセスとは、実行中のプログラムのインスタンスのことです。Linuxでは、複数のプロセスを同時に実行できるタイムシェアリング技術を採用しています。タイムシェアリング技術の基本原理は、CPUの動作時間を一定の長さのタイムスライスに分割し、各プロセスが1つのタイムスライスで動作することである。プロセスのタイムスライスがなくなると、システムはスケジューラーを使って別のプロセスの実行に切り替えます。そのため、実際には、1つのCPUを搭載したマシンの場合、一度に実行できるプロセスは1つだけです。しかし、各プロセスは短いタイムスライスを実行するので（例えば、15システムチック=150ミリ秒）、すべてのプロセスが同時に実行されているように見えます。

### Linux

0.12カーネルの場合、システムは同時に最大64のプロセスを持つことができます。手動で作成された最初のプロセスを除いて、残りのプロセスはシステムコール`fork`を使用して既存のプロセスによって作成された新しいプロセスです。作成されたプロセスは子プロセスと呼ばれ、作成者は親プロセスと呼ばれます。

カーネルプログラムは、各プロセスを識別するためにプロセスID（Process ID、pid）を使用します。プロセスは、実行可能な命令コード、データ、スタックセクションで構成されています。プロセス内のコード部とデータ部は、それぞれ1つの実行ファイル内のコードセグメントとデータセクションに対応しています。各プロセスは、自分自身のコードを実行し、自分自身のデータとスタック領域にアクセスすることしかできません。プロセス間の通信は、システムコールを介して行う必要がある。CPUが1つしかないシステムでは、一度に実行できるプロセスは1つだけである。カーネルは、スケジューラーを介して各プロセスをタイムシェアリング方式で実行するようにスケジュールします。

Linuxシステムのプロセスは、カーネルモードとユーザーモードで実行され、それぞれが独立したカーネル状態スタックとユーザー状態スタックを使用することは既にご存知の通りです。ユーザー状態スタックは、プロセスが呼び出した関数のパラメータやローカル変数などを一時的に保存するために使用され、カーネル状態スタックには、カーネルプログラムが関数呼び出しを実行する際の情報が格納されています。

また、Linuxカーネルでは、プロセスを「タスク」と呼ぶことが多く、ユーザー空間で動作するプログラムを「プロセス」と呼びます。本書では、この2つの用語を混在させながら、このデフォルトルールに従うようにしています。

### 5.7.1 タスクのデータ構造

カーネルプログラムは、プロセステーブルを介してプロセスを管理し、各プロセスはプロセス

ーブルの1項目を占有します。Linuxシステムでは、プロセステーブルの項目はtask\_structタスク構造体のポインタである。PCB (Process Control Block) やPD (Process Descriptor) と表記している書籍もあります。プロセスを制御・管理するためのすべての情報を保持しています。主な内容は、プロセスの現在の実行状況、シグナル、プロセス番号、親プロセス番号、実行時間の累積値、使用中のファイル、タスクのローカルディスクリプタ、タスクのステータスセグメント情報などです。タスクデータ構造は、ヘッダファイルinclude/linux/sched.hで定義されており、構造体の各フィールドの具体的な意味は以下の通りです。

---

```
struct task_struct {
    long state;                      // -1 unrunnable, 0 runnable (ready), > 0 stopped.
    long counter;                     // Task run time tick (decrement), run time slice.
    long priority;                   // Priority. When task starts running, counter=priority.
    long signal;                     // Signal bitmap, each bit is a signal( = bit offset + 1).
    struct sigaction sigaction[32];   // Signal attribute struct. Signal operation and flags.
    long blocked;                    // Process signal mask (Bitmap of masked signal).
    int exit_code;                   // Exit code after task stops, its parent will get it.
    unsigned long start_code;        // Code start location in linear address space.
    unsigned long end_code;          // Code length or size (bytes).
    unsigned long end_data;          // Code size + data size (bytes).
    unsigned long brk;              // Total size (number of bytes).
    unsigned long start_stack;       // Stack bottom location.
    long pid;                        // Process identifier.
    long pgrp;                       // Process group number.
    long session;                   // Process session number.
    long leader;                     // Leader session number.
    int groups[NGROUPS];            // Group numbers. A process can belong to more groups.
    task_struct *p_pptr;             // Pointer to parent process.
    task_struct *p_cptr;             // Pointer to youngest child process.
    task_struct *p_ysptr;             // Pointer to younger sibling process created afterwards.
    task_struct *p_osptr;             // Pointer to older sibling process created earlier.
    unsigned short uid;              // User id.
    unsigned short euid;             // Effective user id.
    unsigned short suid;             // Saved user id.
    unsigned short gid;              // Group id.
    unsigned short egid;             // Effective group id.
    unsigned short sgid;             // Saved group id.
    long timeout;                   // Kernel timing timeout value.
    long alarm;                      // Alarm timing value (ticks).
    long utime;                      // User state running time (ticks).
    long stime;                      // System state runtime (ticks).
    long cutime;                     // Child process user state runtime.
    long cstime;                     // Child process system state runtime.
    long start_time;                 // Time the process started running.
    struct rlimit rlim[RLIM_NLIMITS]; // Resource usage statistics array.
    unsigned int flags;               // per process flags.
    unsigned short used_math;        // Flag: Whether a coprocessor is used.
    int tty;                          // The tty subdevice number used. -1 means no use.
    unsigned short umask;             // The mask bit of the file creation attribute.
    struct m_inode *pwd;              // Current working directory i-node structure pointer.
    struct m_inode *root;              // Root i-node structure pointer.
    struct m_inode *executable;       // The pointer to i-node structure of the executable file.
```

---

```

    struct m_inode * library; // The loaded library i-node structure pointer.
    unsigned long close_on_exec; // A bitmap flags that close file handles on execution.
    struct file * filp[NR_OPEN]; // File structure pointer table, up to 32 items.
                                // The index is the value of file descriptor.
    struct desc_struct ldt[3]; // LDT. 0=empty, 1=code seg cs, 2=data & stack seg ds & ss.
    struct tss_struct tss; // The task status segment structure TSS of the process.
};


```

---

**◆ long state**

--

**state** フィールドには、プロセスの現在の状態が格納されています。Linuxのプロセスは、ある時点で5つの状態のいずれかになり、カーネルのスケジューラの操作により、これらの状態間を移行することができます。5つの状態とは、実行中の状態 (TASK\_RUNNING) 、割り込み可能なスリープ状態 (TASK\_INTERRUPTIBLE) 、割り込み不可能なスリープ状態 (TASK\_UNINTERRUPTIBLE) 、ゾンビ状態 (TASK\_ZOMBIE) 、停止状態 (TASK\_STOPPED) です。カーネルがプロセスの状態を変更する方法については、次のセクションで説明します。

**◆ long counter -- counter**

**counter** フィールドは、プロセスが実行可能な時間刻みの数を保持します。を一時的に停止します。つまり、他のプロセスに切り替わるには、通常、数システムクロックサイクルかかります。スケジューラはプロセスのカウンタ値を使って次に実行するプロセスを選択するので、カウンタはプロセスの動的な機能と考えることができます。カウンタの初期値は、プロセスが作成されたばかりのときの優先度と同じです。

**◆ long priority -- priority**

priorityはカウンタの初期値を決めるのに使われる。Linux

0.12では、この初期値は15システムクロックサイクルタイム(15ティック)です。必要に応じて、スケジューラは**priority**の値を使用してカウンタに初期値を割り当てます。sched.cおよびfork.cプログラムを参照してください。sched.cやfork.cを参照してください。もちろん、優先度の単位も時間刻みの数です。

**◆ long signal**

--

**signal** フィールドは、プロセスが現在受信しているシグナルのビットマップである。ビットマップは32ビットで、各ビットがシグナルを表し、シグナルの値=ビットオフセット値+1となります。つまり、Linuxカーネルは最大で32個のシグナルを持っています。各システムコールプロセスの終了時に、シグナルビットマップを用いてシグナルの前処理が行われます。

**◆ struct sigaction sigaction[32]**

--

**sigaction**構造体の配列は、各信号の処理に使用される操作と属性を格納するために使用されます。配列の各項目は、1つのシグナルに対応しています。

**◆ long blocked**

--

**blocked** フィールドは、プロセスが現在処理したくないシグナルのブロッキングビットマップです。signal フィールドと同様に、各ビットがブロックされたシグナルを表します。

**◆ int exit**

--

**exit** フィールドは、プログラムが終了するときの終了コードを保存するために使用されます。子プロセスが終了した後、親プロセスはその終了コードを問い合わせることができます。

**◆ unsigned long start\_code**

--

**start\_code** フィールドは、CPUのリニアアドレス空間におけるプロセスコードの開始アドレスである。Linux 0.1xカーネルでは、64MBの整数倍の値となります。

**◆ unsigned long end\_code -- end\_code**

--

**end\_code** フィールドには、プロセスコードのバイト長値が格納される。

◆ unsigned long end\_data --

end\_dataフィールドには、プロセスのコード長+データ長の総バイト数の値が格納される。

◆ unsigned long brk -- brkフィールドは、図5-

12に示すように、プロセスコードとデータの合計バイト長値（ポインタ値）でもあります、未初期化データ領域bssも含まれています。これがプロセスの実行開始時のbrkの初期値です。このポインタを変更することで、カーネルはプロセスに動的に割り当てられたメモリを追加・解放することができます。これは通常、カーネルがmalloc()関数を呼び出したり、brkシステムコールを呼び出したりして行います。

◆ unsigned long start\_stack --

start\_stackフィールドの値は、プロセスの論理アドレス空間にあるスタックの先頭を指します。図5-12のスタックポインタの位置も参照してください。

◆ long pid -- Pidは、プロセスの識別番号です。プロセスを一意に識別するために使用されます。

◆ long pgrp -- Pgrpとは、そのプロセスが属するプロセスグループ番号のことです。

◆ long session -- Sessionはプロセスのセッション番号で、セッションのプロセスIDとなります。

◆ long leader --

leaderは、セッションの最初のプロセス番号です。プロセスグループとセッションの概念については、第7章「プログラムリスト」に続く説明を参照してください。

◆ int groups[NGROUPS] --

Groupsは、プロセスが属する各グループのグループ番号の配列である。1つのプロセスは、複数のグループに属することができます。

◆ task\_struct \*p\_pptr -- p\_pptr は親プロセスのタスク構造体へのポインタです。

◆ task\_struct \*p\_cptr -- p\_cptr は、最新のサブプロセスのタスク構造へのポインタです。つまり、一番下の子のタスク構造です。図5-20を参照してください。

◆ task\_struct \*p\_ysptr --

p\_ysptrは、自分よりも後に作られた隣接プロセスへのポインタである。つまり、弟分のプロセスへのポインタです。

◆ task\_struct \*p\_osptr --

\*p\_osptrは、自分よりも前に作られた隣接プロセスへのポインタである。つまり、古い兄弟プロセスへのポインタです。以上の4つのポインタの関係は、図5-20を参照してください。Linux

0.11カーネルのタスクデータ構造には、親プロセス番号フィールドfatherがありますが、これは

0.12 カーネルを使っています。この時点で、プロセスのpptr->pidを使って、親プロセスのプロセス番号を知ることができます。

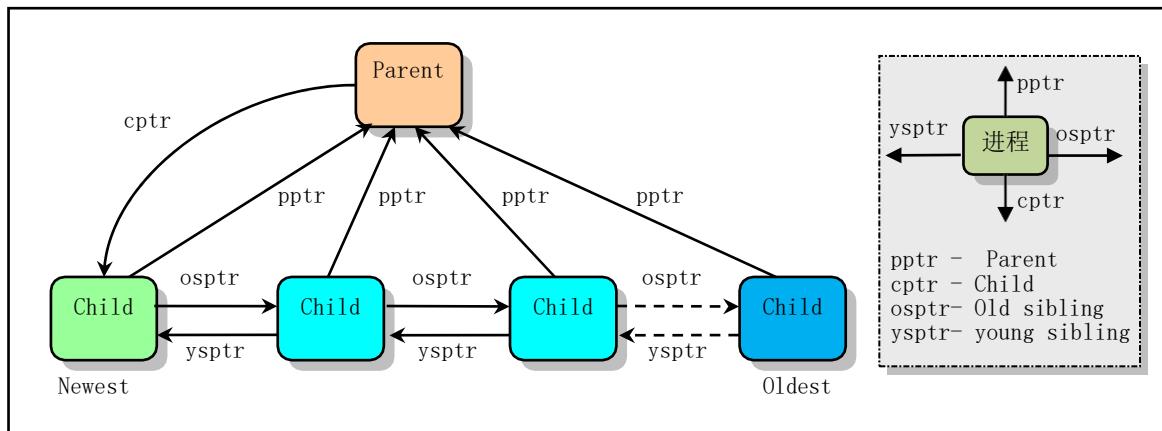


Figure 5-20 Relationship between process pointers

- ◆ unsigned short uid -- Uidは、プロセスを所有するユーザーの識別番号（ユーザーID）です。
- ◆ unsigned short euid -- Euidは、ファイルへのアクセス権限を示す有効なユーザー識別番号です。
- ◆ unsigned short suid -- Suidは保存されたユーザ識別番号である。実行ファイルの set-user-ID フラグが設定されている場合は、実行ファイルの suid が保存される。それ以外の場合、suid はプロセスの euid と等しい。

◆ unsigned short gid -- Gidは、ユーザーが所属するグループの識別番号（グループID）です。プロセスを所有するユーザーグループを識別します。

◆ unsigned short egid -- Egidは、ファイルにアクセスするユーザーのグループの権限を示す有効なグループ識別番号です。

◆ unsigned short sgid -- Sgidは、保存されているユーザグループの識別番号である。実行ファイルの set-group-ID フラグが設定されている場合は、実行ファイルの gid が sgid に保存される。それ以外の場合、sgidはプロセスのegidと等しくなります。これらのユーザIDとグループIDの説明は、第5章のsys.cプログラムの概要を参照してください。

◆ long timeout -- カーネルのタイミングのタイムアウト値。

◆ long alarm -- Alarmは、プロセスのアラームタイミング値(ティック数)です。プロセスがシステムコールalarm()を使ってフィールド値を設定した場合、システム時間の刻み値がアラームフィールド値を超えると、カーネルはプロセスにSIGALRMシグナルを送ります。デフォルトでは、このシグナルによってプログラムの実行が終了します。もちろん、シグナルキャプチャ関数 (signal) ()またはsigaction ()を使って、指定した操作のシグナルをキャプチャすることもできます。関数alarm()は、kernel/sched.cの370行目から始まっています。カーネルは、秒単位の関数値を目盛り値に変換して、システムの現在時刻の目盛り値の後のフィールドに格納します。

◆ long utime -- Uttimeは、プロセスがユーザーの状態で実行される累積時間（ティック）です。

◆ long stime -- Stimeは、システムの状態でプロセスが実行される累積時間（tick）です。

◆ long cutime -- Cutimeは、子プロセスがユーザー状態で動作する累積時間（ティック）です。

◆ long cstime -- Cstimeは、子プロセスがシステム状態で動作する累積時間（ティック）です。

◆ long start\_time -- Start\_timeは、プロセスが生成され、実行が開始される時間です。

◆ struct rlimit rlim[RLIM\_NLIMITS] -- プロセスのリソース使用統計配列。

◆ unsigned int flags -- そのプロセスごとのフラグで、0.12カーネルはまだ使用されていません。

- ◆ unsigned short used\_math -- プロセスがコプロセッサを使用しているかどうかを示すフラグである。
  - ◆ int tty --  
tty端末を使用しているプロセスのサブデバイス番号です。1は使用していないことを意味します。

◆ unsigned short umask --  
セスが新規ファイルを作成する際に使用する16ビットの属性マスクワード（各ビットはファイル  
です），つまり，新規ファイルで設定されるアクセス属性である。マスクワードのビットがセット  
している場合は、対応する属性が無効（マスクされている）ことを意味する。この属性マスクワー  
ド，ファイル作成時に与えられた属性値（mode

`&~umask)`とともに、新しく作成されたファイルの実際のアクセス属性として使用される。マスクワードとファイル属性の具体的な意味については、`include/fcntl.h`および`include/sys/stat.h`ファイルを参照のこと。

- ◆ struct m\_inode \* pwd -- Pwdは、プロセスのカレントワーキングディレクトリのinode構造へのポインタである。各プロセスは、相対パス名を解決するカレントワーキングディレクトリを持ち、システムコールchdirを使って変更することができます。

- ◆ struct m\_inode \* root -- Rootはプロセス自身のルートinode構造です。各プロセスは、絶対パス名を解析するために、独自に指定されたルートディレクトリを持つことができます。chrootを呼び出してこのルートディレクトリを変更できるのはスーパーユーザだけです。

- ◆ struct m\_inode \* executable -- Executableは、プロセスの実行ファイルのメモリ内のinode構造へのポインタです。システムはこのフィールドを使って、システム内に同じ実行ファイルを実行している別のプロセスがあるかどうかを判断することができます。もしそうであれば、executable->i\_countのメモリ内i-

node参照カウント値は1より大きくなります。プロセスが作成されると、このフィールドには親プロセスの同じフィールドと同じ値が与えられ、親プロセスと同じプログラムが実行されていることを意味しています。指定された新しい実行ファイルを実行するために、一種のexec()関数が呼び出されると、フィールドの値は、exec()関数によって実行される新しいプログラムのメモリi-nodeポインタに置き換えられます。プロセスがexit()関数を呼び出して終了処理を行うと、このフィールドが指すメモリi-nodeの参照カウントが1だけデクリメントされ、フィールドは空白になります。このフィールドの主な役割は、memory.cプログラムのshare\_page()関数に反映されています。この関数コードは、プロセスの実行によって指されたノードの参照カウントに従って、現在実行中のプログラムのコピーがシステム内に複数（少なくとも2つ）あるかどうかを判断することができます。もしそうであれば、それらの間でページ共有操作を試みます。

システムの初期化時には、システムで作成されたすべてのタスクの実行度は、`execve()`関数を実行する最初の呼び出しの前に0になっています。つまり、カーネルコードに直接含まれているすべてのタスクの実行可能フィールドは0です。タスク0のコードはカーネルコードに含まれているため、システムがファイルシステムから読み込むことはありません。そのため、カーネルコード内の実行可能コードは0という固定値になっています。また、新しいプロセスを作成する際、`fork()`は親プロセスのタスクデータ構造をコピーするため、タスク1の実行可能コードも0となります。しかし、`execve()`を実行した後、実行可能コードには、実行されるファイルのメモリノードへのポインタが与えられます。それ以降は、すべてのタスクのこの値が0になることはありません。

- ◆ unsigned m\_inode \* library  
Library は、プログラム実行時にロードされるライブラリファイルのインメモリ構造体ポインタです。

## ◆ unsigned

long

close\_on\_exec

--

プロセスのファイル記述子（ファイルハンドル）のビットマップフラグです。各ビットは1つのファイル記述子を表し、システムコールexecve()が呼ばれたときにクローズする必要のあるファイル記述子を決定するために使用されます（include/fcntl.h参照）。プログラムがfork()を使って子プロセスを作成すると、通常、子プロセス内でexecve()関数を呼び出し、別の新しいプログラムをロードします。この時点で、子プロセスは新しいプログラムに完全に置き換わり、新しいプログラムが子プロセス内で実行を開始します。close\_on\_execのファイルディスクリプターの対応するビットがセットされていれば、子プロセスがexecve()を実行したときに、開いているファイルに対応するファイルディスクリプターが閉じられます。つまり、新しいプログラムではファイルディスクリプターが閉じられますが、そうでなければファイルディスクリプターは常に開いたままです。

## ◆ struct

file

\*

filp[NR\_OPEN]

--

プロセスが使用しているすべてのオープンファイルのファイル構造ポインタのテーブルで、最大32エントリまであります。ファイル記述子の値は、構造体テーブルのインデックス値です。それぞれのこれらは、ファイル記述子がファイルポインタの位置を特定し、ファイルにアクセスするために使用されます。

## ◆ struct

desc\_struct

ldt[3]

--

プロセスローカルディスクリプターテーブル構造体LDTである。仮想アドレス空間内のタスクのコードセグメントとデータセグメントを定義している。配列の項目0はNULL項目、項目1はコードセグメントの記述子、項目2はデータセグメント（データとスタックを含む）の記述子である。

## ◆ struct

tss\_struct

tss

--

プロセスのタスクステートセグメントTSS情報構造体である。tss\_struct構造体は、タスクが実行から切り替えられたときの現在のプロセッサのすべてのレジスタ値を保持します。タスクが再実行されると、CPUはこれらの値を使ってタスクが切り替わったときの状態に戻し、実行を開始します。

プロセスが実行されているとき、CPUのすべてのレジスタの値、プロセスの状態、スタックの内容などをプロセスのコンテキストと呼びます。カーネルは、別のプロセスに切り替える必要があるときには、現在のプロセスの状態をすべて保存する、つまり、現在のプロセスのコンテキストを保存して、再びプロセスを実行するときに、切り替える前の状態に戻すことができるようになります。Linuxでは、現在のプロセスのコンテキストは、タスクのタスクデータ構造に保存されています。割り込みが発生すると、カーネルは割り込みプロセスのコンテキストで、カーネルステート内の割り込みサービスルーチンを実行します。同時に、使用する必要のあるすべてのリソースを保持し、割り込みサービスが終了したときに、割り込みプロセスの実行を再開できるようにします。

## 5.7.2 プロセスの動作状態

図5-

21に示すように、プロセスはその寿命の間、プロセス・ステートと呼ばれる異なるステートのセットに入ることができます。図の中で数字が異なる円は、それぞれ異なる状態を表しています。前述のように、プロセス状態はプロセスタスク構造の状態フィールドに保存されます。

プロセスがCPUの使用を待っている場合や実行中の場合は、準備完了状態や実行中状態と言います。このとき、プロセス状態フィールドの値はTASK\_RUNNINGとなります。プロセスがシステム・リソースやイベントの発生を待っている間にスリープ状態になっている場合は、割り込み可能なスリープ状態、または割り込み不可能なスリープ状態と言われます。このとき、プロセスの状態フィール

ドは、それぞれTASK\_INTERRUPTIBLEまたはTASK\_UNINTERRUPTIBLEとなります。プロセスが終了したものの、カーネルリソースを完全に解放していない場合、そのプロセスはデッドステートにあると言われます。この時点では、プロセスの状態フィールド値はTASK\_ZOMBIEです。プロセスが一時的に停止している場合は、サスペンド状態といいます。この時点で、プロセスの状態フィールド値はTASK\_STOPPEDです。

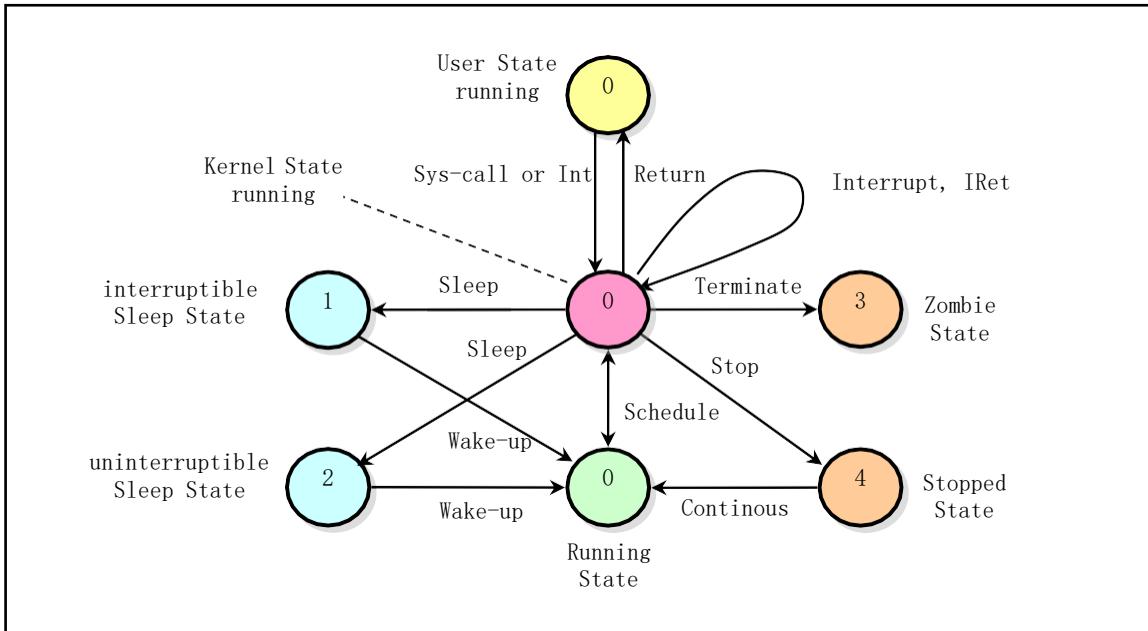


Figure 5-21 Process status and conversion relationship

Linuxプロセスの5つの状態を表す定数シンボル名を以下に示します。これらは、include/linux/sched.hの46～50行目で定義されています。

---

```

// This defines the state of a process.
46 #define TASK_RUNNING          0 // is running or ready to run
47 #define TASK_INTERRUPTIBLE     1 // is in an interruptible wait state.
48 #define TASK_UNINTERRUPTIBLE   2 // uninterruptible wait state for wait I/O operation.
49 #define TASK_ZOMBIE            3 // is in a zombie state and has been terminated.
50 #define TASK_STOPPED           4 // The process has stopped.
  
```

---

#### ◆ 実行中の状態 (0, TASK\_RUNNING)

プロセスがCPUによって実行されているとき、またはスケジューラによっていつでも実行できる状態にあるとき、そのプロセスは実行状態と呼ばれます。また、図5-21のように、現時点でCPUが実行していない場合は、実行準備状態といいます。図では、上から下までの真ん中の3つの円には同じ値0が含まれており、すべて準備完了状態または実行状態であることを意味している。プロセスには、カーネルモードとユーザーモードの2種類があります。

プロセスがカーネルコードを実行している状態をカーネル実行状態、または単にカーネルモードと呼び、プロセスが自分のコードを実行している状態をユーザー実行状態（ユーザーモード）と呼びます。システムリソースが利用可能になると、プロセスはウェイクアップし、実行可能な状態になります。これを準備状態と呼びます。これらの状態（図の中段）は、カーネルでは同じ方

式を表し、TASK\_RUNNING状態と言われています。新しいプロセスが作られたばかりの時は、この状態（下の0）になっています。

#### ◆割り込み可能なスリープ状態 (1, TASK\_INTERRUPTIBLE)

プロセスが割り込み可能な待機（スリープ）状態にあるとき、システムはプロセスの実行をスケジューリングしません。システムが割り込みを発生させたり、プロセスが待機しているリソースを解放したり、プロセスが信号を受信したりすると、プロセスを起こして準備状態（つまり実行状態）に変更することができます。

#### ◆無瞬断のスリープ状態 (2, TASK\_UNINTERRUPTIBLE)

この状態は、信号を受信しても起こされないことを除けば、割り込み可能なスリープ状態と同様です。しかし、この状態のプロセスは、`wake_up()`関数を使って明示的にアウェイクしたときにのみ、実行可能なレディ状態に変換することができます。この状態は一般的に、プロセスが邪魔されずに待つ必要がある場合や、待機イベントがすぐに発生する場合に使用されます。

#### ◆ゾンビ状態 (3, TASK\_ZOMBIE)

あるプロセスが実行を停止したにもかかわらず、その親プロセスが`wait()`を呼び出して状態を問い合わせていない場合、そのプロセスは死んだ状態にあると言われています。親プロセスが実行を停止したという情報を得るために、子プロセスのタスクデータ構造の情報を保持する必要があります。親プロセスが`wait()`を呼び出して子プロセスの情報を取得すると、その状態にあるプロセスのタスクデータ構造が解放されます。

#### ◆停止状態 (4, TASK\_STOPPED)

プロセスが信号SIGSTOP、SIGTSTP、SIGTTIN、SIGTTOUを受信すると、停止状態になります。SIGCONT信号をプロセスに送ると、実行可能な状態に移行します。デバッグ中にプロセスが受信した信号は、この状態に入る。Linux

0.12では、この状態への変換処理は実装されていません。この状態のプロセスは、プロセス終了として処理されます。

プロセスが時間切れになると、システムはスケジューラーを使って、実行するプロセスを別のプロセスに強制的に切り替えます。また、プロセスがカーネルモードで実行する際に、システムの特定のリソースを待つ必要がある場合、プロセスは`sleep_on()`または`interruptible_sleep_on()`を呼び出してCPUの使用権を自発的に放棄し、スケジューラに他のプロセスを実行させます。プロセスはスリープ状態（TASK\_UNINTERRUPTIBLEまたはTASK\_INTERRUPTIBLE）になります。

カーネルは、プロセスが「カーネル実行状態」から「スリープ状態」に移行したときにのみ、プロセスの切り替え操作を行います。カーネルモードで動作しているプロセスは、他のプロセスからブリエンプトされることなく、また、あるプロセスが他のプロセスの状態を変更することもできません。プロセス切り替え時のカーネルのデータエラーを避けるために、カーネルはクリティカルエリアコードの実行時にすべての割り込みを無効にします。

### 5.7.3 プロセスの初期化

bootディレクトリでは、ブートローダがディスクからカーネルをメモリにロードし、システムをプロテクトモードにした後、システム初期化プログラム`init/main.c`を起動する。メインプログラムは、まずシステムの物理メモリの割り当てと使用方法を決定し、次にカーネルの各部の初期化関数を呼び出して、メモリ管理、割込み処理、ロックデバイス、キャラクタデバイス、プロセス管理、ハー

ドディスクやフロッピーディスクのハードウェアを初期化する。これらの操作が完了すると、システムの各部分が動作可能になる。その後、プログラムの制御は「手動」でタスク0（プロセス0）に移され、`fork()`コールを使って初めてプロセス1が生成されます。プロセス1では、プログラムは引き続きアプリケーション環境の初期化とシェル・ログイン・プログラムの実行を行います。元のプロセス0は、システムがアイドル状態のときに実行されるようにスケジュールされます。この時点では、タスク0は`pause()`システムコールを実行するだけで、その結果、スケジューラ関数が実行されます。

タスク0の実行に移す」という処理は、マクロ `move_to_user_mode` (include/asm/system.h)によって行われます。これは、main.cプログラムの実行フローを、カーネルモード(特権レベル0)からユーザーモード(特権レベル3)のタスク0に移動させるものです。移動の前に、システムはまず、スケジューラーの初期化処理 (`sched_init()`) でタスク0の実行環境を設定します。これには、タスク0のデータ構造 (include/linux/sched.h) のフィールドの値を手動で事前に設定したり、タスク0のタスク・ステート・セグメント (TSS) ディスクリプターやグローバル・ディスクリプター・テーブルのローカル・ディスクリプター・テーブル (LDT) を追加したりします。セグメント記述子は、それぞれタスクレジスタtrとローカル記述子テーブルレジスタldtrにロードされます。

ここで強調しておきたいのは、カーネルの初期化は特殊な処理であり、カーネルの初期化コードはタスク0のコードでもあるということです。タスク0のデータ構造の初期データセットから、コードのベースアドレスである

タスク0のコードセグメントおよびデータセグメントのベースアドレスは0で、セグメント長は640KBです。カーネルコードセグメントとデータセグメントのベースアドレスは0で、セグメント長は16MBです。したがって、タスク0のコード・セグメントとデータ・セグメントは、それぞれカーネル・コード・セグメントとデータ・セグメントに含まれます。カーネル初期化プログラムmain.cはタスク0のコードですが、タスク0に移行する前にシステムがカーネルモードの特権レベル0でメインコードを実行している点が異なります。マクロ`move_to_user_mode`の機能は、実行特権レベルをカーネル状態のレベル0からユーザーモードのレベル3に移動させても、元のコードの命令ストリームを継続して実行するために使用されます。

タスク0への移行時には、マクロ`move_to_user_mode`は、割込み復帰命令を使用して、特権レベルの変更を引き起こします。制御転送にこの方法を使用するのは、CPUの保護機構が原因です。CPUは、ゲートや割り込み、トラップゲートを呼び出すことで、低レベル（特権レベル3など）のコードを呼び出したり、高レベルのコードに転送したりすることはできますが、その逆はできません。そこでカーネルは、低レベルのコードを返すために、IRETを模したメソッドを使います。この方法の主な考え方は、割り込みリターン命令の内容をスタックに構築し、リターンアドレスのセグメントセレクタを、特権レベル3のタスク0コードセグメントセレクタに設定します。

その後、割り込みリターン命令IRETを実行すると、システムCPUは特権レベル0から外層の特権レベル3にジャンプします。特権レベル変更時の割込み復帰スタック構造図は図5-22を参照してください。

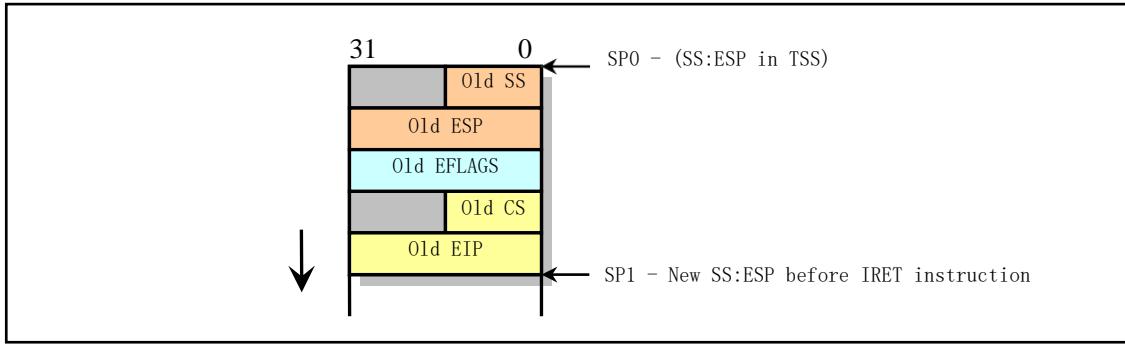


図 5-22 特権レベル変更時のインタラプト・リターン・スタック構造

マクロ`move_to_user_mode`は、まずタスク0のスタックセグメント（つまりデータセグメント）のセレクタとカーネルスタックポインタをカーネルスタックにプッシュします。次に、フラグレジスターの内容をプッシュします。最後に、タスク0コードセグメントセレクタと、「割込み復帰」後に次に実行される命令のオフセットを押し込みます。

IRET命令が実行されると、CPUはCS:EIPにリターンアドレスを送信し、スタックのフラグレジスターの内容をポップアップします。このとき、CPUは送信先コードセグメントの特権レベルを3と判断しているため、現在のカーネル状態のレベル0とは異なります。その後、CPUはスタック内のスタックセグメントセレクタとスタックポインタをSS:ESPにポップします。特権レベルの変更に伴い、セグメント・レジスタDS、ES、FS、GSの値が無効になり、CPUはこれらのセグメント・レジスタをクリアします。そのため、IRET命令を実行した後、これらのセグメント・レジスタを再ロードする必要があります。その後、システムはタスク0のコードに対して特権レベル3で実行を開始します。この時点では、移動前に使用していたオリジナルのスタックがタスク0の加入者局スタックとして使用されます。カーネル状態のスタックは、タスク0のTSSの内容で指定され、タスクデータ構造があるページの先頭(PAGE\_SIZE + (long) & init\_task)から指定されます。タスク0のタスクデータ構造（ユーザースタックポインタを含む）は、後で新しいプロセスを作成する際にコピーする必要があるため、タスク1（プロセス1）が作成されるまで、タスク0のユーザモードスタックは「クリーン」な状態を保つ必要があります。

#### 5.7.4 新しいプロセスの創造

Linuxシステムで新しいプロセスを作成するには、`fork()`システムコールを使用する必要があります。初期化後に作成されるプロセスは、すべてプロセス0の子プロセスを起点としています。

新しいプロセスを作成する過程で、システムはまず、タスクデータ構造の配列の中から、どのプロセスにも使われていない空のアイテム（空のスロット）を見つけます。システムがすでに64のプロセスを実行している場合、タスク配列テーブルに利用可能な空のアイテムがないため、`fork()`システムコールはエラーを返します。そうでなければ、システムは新しいプロセスがタスク・データ構造情報を保存するためにメイン・メモリ・エリアにメモリのページを申請し、新しいプロセスのタスク・データ構造のテンプレートとして現在のプロセスのタスク・データ構造のすべての内容をコピーします。処理されていないこの新しいプロセスがスケジューラーによって実行されるのを防ぐために、新しいプロセスの状態を直ちに中断不可能な待機状態（`TASK_UNINTERRUPTIBLE`）に設定する必要があります。

その後、コピーされたタスクデータ構造が変更されます。現在のプロセスを新しいプロセスの親

に設定し、シグナルビットマップをクリアして新しいプロセスの統計情報をリセットし、ランタイムスライスの初期値を15システムティック（150ミリ秒）に設定します。次に、タスクステータスセグメント(TSS)のレジスタの値を現在のプロセスに応じて設定します。プロセスの生成時には、新しいプロセスの戻り値は0でなければならぬため、tss.eax

≡

0を設定する必要があります。新しいプロセスのカーネル状態スタック・ポインタtss.esp0は、新しいプロセス・タスク・データ構造が配置されているメモリ・ページの先頭に設定され、スタック・セグメントtss.ss0はカーネル・データ・セグメント・セレクタに設定されます。Tss.ldtには、GDT内のローカルテーブル記述子のインデックス値が設定されます。現在のプロセスがコプロセッサを使用している場合は、コプロセッサの完全な状態を新しいプロセスのtss.i387構造体に保存する必要もあります。

その後、新しいタスクのコードおよびデータセグメントのベースアドレスと制限長を設定し、現在のプロセスのメモリページテーブルをコピーします。なお、この時点では新プロセスに実際の物理メモリページを割り当てず、親プロセスのメモリページを共有させています。親プロセスと新プロセスのいずれかにメモリの書き込み操作があった場合にのみ、システムは書き込み操作に関連するメモリページを割り当てます。このような処理をCopy

On

Write技術といいます。この技術の詳細については、「メモリ管理」の章の「Write-Only Replication」のメカニズムを参照してください。

その後、親プロセスに開いているファイルがあれば、対応するファイルの開封回数を1回増やしてください。続いて、新しいタスクのTSSおよびLDT記述子のエントリがGDTに設定され、ベース・アドレス情報が新しいプロセス・タスク構造のtssおよびldtを指すようになります。最後に、新しいタスクを実行可能な状態に設定し、新しいプロセス番号を返します。

また、新規に子プロセスを作成することと、実行ファイルを読み込むことは別の概念であることに注意してください。子プロセスが作成されると、親プロセスのコードとデータ領域を完全にコピーし、そこに子プロセス部分のコードを実行する。ロックデバイスでプログラムを実行する場合、一般的にはexec()システムコールを実行して子プロセスで実行される。exec()に入ると、子プロセスの元のコードやデータ領域はクリア(解放)されます。子プロセスが新しいプログラムの実行を開始すると、この時点ではカーネルがロックデバイスからプログラムのコードをロードしていないので、CPUは直ちにページが存在しないという例外を発生させます。ここで、メモリマネージャがロックデバイスから対応するコードページをロードし、CPUは例外発生の原因となった命令を再実行します。ここまでで、新しいプログラムのコードが実際に実行され始めます。

## 5.7.5 プロセススケジューリング

カーネル内のスケジューラーは、システム内で次に実行するプロセスを選択するために使用されます。この選択的運用

のメカニズムは、マルチタスクOSの基礎となるものです。スケジューラは、実行中のすべてのプロセス間でCPUランタイムを割り当てる管理コードと考えることができます。前述の説明からわかるように、Linuxプロセスはプリエンプティブですが、プリエンプティブされたプロセスはTASK\_RUNNING状態のままであるが、CPUによって一時的に実行されているわけではありません。プロセスのプリエンプションは、プロセスがユーザー状態の実行フェーズにあるときに発生し、カーネル状態で実行されているときはプリエンプションできません。

プロセスがシステムリソースを有効に利用し、プロセスの応答速度を速くするためには、プロセ

ス切り替えのスケジューリングに一定のスケジューリング戦略を採用する必要があります。Linux 0.12では、優先キューイングによるスケジューリング方式を採用しています。

### スケジューラー

`schedule()`関数は、まずタスク配列をスキヤンします。準備状態(TASK\_RUNNING)のタスクごとに、ランタイムカウントカウンタの値を比較して、現在どのプロセスの実行時間が最も短いかを判断します。どの値が大きいかは、実行時間が長くないことを意味するので、そのプロセスを選択し、タスク切り替えマクロ関数を使って、そのプロセスに切り替えます。

このとき、TASK\_RUNNING状態のプロセスのタイムスライスをすべて使い切っていた場合、システムは各プロセスの優先度の値に応じて、システム内の各プロセス（スリープ中のプロセスを含む）に必要なタイムスライス（カウンタ）を再計算します。その計算式は

$$counter = \frac{counter}{2} + priority$$

したがって、スリープ状態のプロセスについては、起床時のタイムスライスカウンタの値が大きくなります。次に、`schedule()`関数は、task配列のTASK\_RUNNING状態の全プロセスを再スキヤンし、プロセスが選択されるまで処理を繰り返します。最後に`switch_to()`が呼ばれ、実際のプロセス切り替え操作が行われます。

この時、他に実行できるプロセスがなければ、システムはプロセス0を選択して実行します。Linux

0.12の場合、プロセス0は`pause()`を呼び出して自分を割り込み可能なスリープ状態にし、再び`schedule()`を呼び出します。しかし、プロセスをスケジューリングする際、`schedule()`はプロセス0の状態を気にしません。システムがアイドル状態である限り、プロセス0の実行がスケジューリングされます。

### プロセス切り替え

新しい実行可能なプロセスが選択されるたびに、`schedule()`関数は`switch_to()`マクロを呼び出し、実際のプロセス切り替え操作を行います。`switch_to()`は、`include/asm/system.h`で定義されています。このマクロは、CPUの現在のプロセスの状態(コンテキスト)を、新しいプロセスの状態に置き換えます。`switch_to()`は切り替えを行う前に、まず切り替え先のプロセスが現在のプロセスであるかどうかを確認し、そうであれば何もせずにそのまま終了します。そうでない場合は、まずカーネルのグローバル変数`current`に新しいタスクのポインタが設定され、次に新しいタスクのタスクステートセグメントTSSのアドレスにジャンプして、CPUにタスク切り替え動作を行わせます。このとき、CPUはすべてのレジスタの状態を、カレントタスクレジスタTRのTSSセグメントセレクタが指すカレントプロセススクデータ構造のtss構造に保存します。その後、新しいタスク状態セグメントセレクタが指す新しいタスクスクデータ構造のtss構造のレジスタ情報がCPUに復元されます。その後、システムは新しいスイッチを実行するタスクを正式に開始しました。この処理を図5-23に示します。

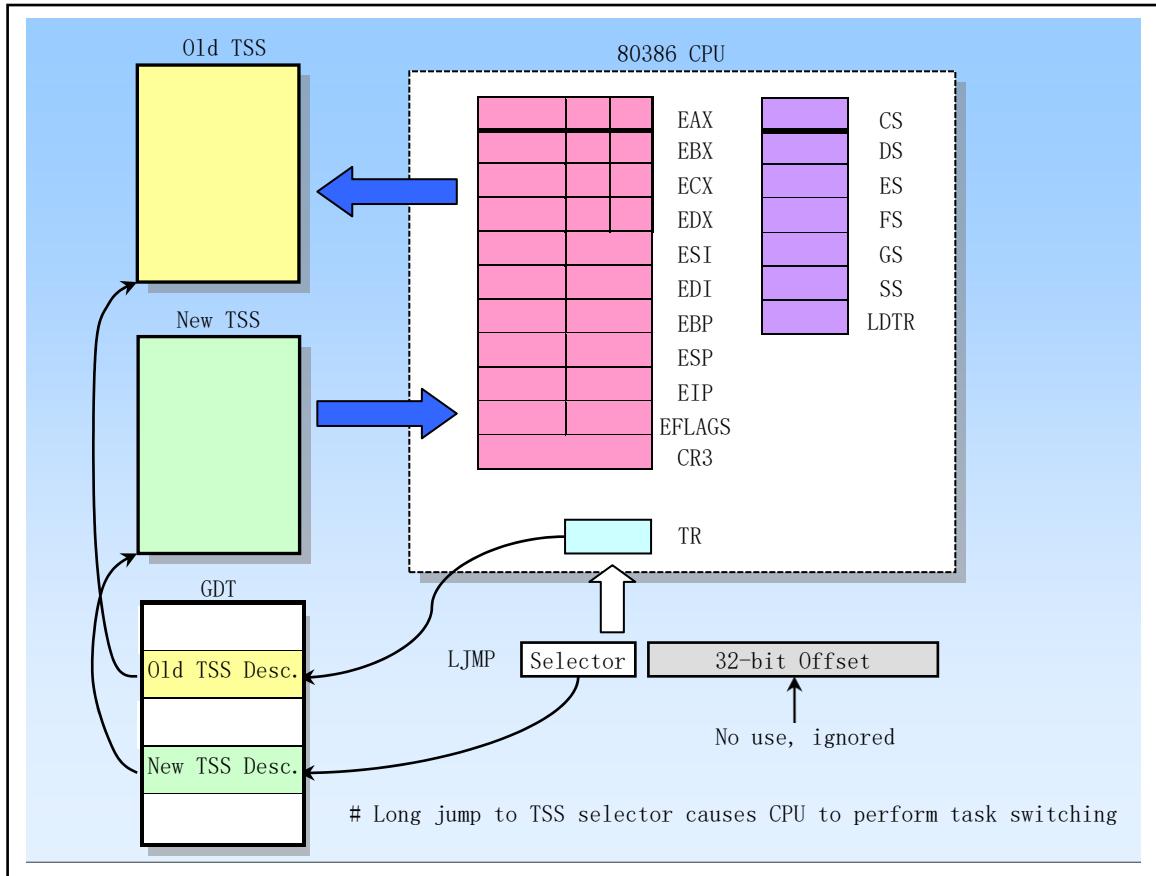


Figure 5-23 Task switching operation diagram

### 5.7.6 プロセスの終了

プロセスの実行が終了したり、実行が途中で終了したりすると、カーネルはプロセスが占有していたシステムリソースを解放する必要があります。これには、プロセスの実行中に開いたファイルや使用したメモリなどが含まれます。

ユーザープログラムがexit()システムコールを呼び出すと、カーネル関数do\_exit()が実行される。この関数はまず、プロセスのコードセグメントとデータセグメントが占有していたメモリページを解放し、プロセスが開いていたすべてのファイルを閉じ、現在の作業ディレクトリ、ルートディレクトリ、プロセスが使用しているプログラムを実行しているinodeを同期させます。プロセスが子プロセスを持つ場合は、initプロセスをそのすべての子プロセスの親とします。プロセスがセッションヘッダプロセスであり、制御端末を持っている場合は、制御端末を解放し、ハングアップ信号SIGHUPをセッションに属するすべてのプロセスに送信します。これにより、通常はセッションの全プロセスが終了します。そして、プロセスの状態をTASK\_ZOMBIEに設定します。そして、元の親プロセスにSIGCHLDシグナルを送り、子プロセスの一部が終了したことを知らせます。最後にdo\_exit()は、他のプロセスを実行するためにスケジューラを呼び出します。プロセスが終了しても、親プロセスもその情報を使用する必要があるため、タスクデータ構造は残っていることがわかります。

子プロセスの実行中、親プロセスは通常、wait()またはwaitpid()関数を使用して子プロセスが終

了するのを待ちます。待機中の子プロセスが終了してゾンビ状態になると、親プロセスは子プロセスが費やした時間を自分のプロセスに蓄積します。最終的には、子プロセスのタスクデータ構造が占有していたメモリページが解放され、タスク配列で子プロセスが占有していたポインタ項目が空になります。

## 5.8 Linuxでのスタックの使い方

このセクションでは、起動からシステムアップタイムまで、Linuxカーネルがどのようにスタックを使用するかの概要を説明します。この部分の説明は、カーネルコードと密接に関連しているので、最初は飛ばしても構いません。関連するコードを読むときに戻ってきて勉強することができます。

### Linux

0.12システムでは、4種類のスタックが使用されています。1つはシステムブートの初期化時に一時的に使用されるスタック、もう1つはプロジェクトモードに入った後にカーネルを初期化するために使用されるスタックで、カーネルコードのアドレス空間の固定された場所にあります。このスタックは、後にタスク0が使用するユーザモードスタックでもあります。次に、各タスクがシステムコールを通じてカーネルコードを実行する際に使用するスタックで、タスクのカーネルレベルスタックと呼んでいます。各タスクは独立したカーネルモードスタックを持っています。最後は、タスクがユーザモードで実行するスタックで、タスク（プロセス）の論理アドレス空間の端の方にあります。

複数のスタックを使用したり、状況に応じて異なるスタックを使用する理由は主に2つあります。一つ目は、リアルモードがプロテクションモードに入ってから、CPUのメモリアクセスマードが変更されたため、セットアップスタック領域を再調整する必要があること。また、CPUの異なる権限レベルによるスタックの使用による保護問題を解決するために、レベル0のカーネルコードとレベル3のユーザーコードの実行には、異なるスタックを使用する必要があります。タスクがカーネルモードに入ると、そのTSSセクションに与えられた特権レベル0であるスタックポインタtss.ss0, tss.esp0を使用し、これがカーネルスタックとなります。元のユーザースタックポインタはカーネルスタックに保存されます。ユーザーモードからカーネルモードに戻る際には、ユーザーモードのスタックが復元されます。以下、別々に説明します。

### 5.8.1 初期化フェーズ

#### ブートの初期化 (bootsect.s, setup.s)

##### ブートセクトコードがROM

BIOSによって物理メモリ0x7c00にロードされると、スタックセグメントが設定されません。もちろん、プログラムはスタックを使用しません。bootsectが0x9000:0に移動した後、スタックセグメントレジスタSSが0x9000に設定され、スタックポインタespレジスタが0xff00に設定されます。つまり、スタックの先頭は 0x9000:0xff00 になります。boot/bootsect.s の 61 行目をご覧ください。bootsectで設定されたスタックセクションは、setup.s

プログラムでも使用されます。これは、システムの初期化時に一時的に使用されるスタックです。

#### プロジェクトモード (head.s) 突入時

head.sプログラムから、システムが正式にプロジェクトモードで動作していることがわかります。この時点で、スタックセグメントはカーネルデータセグメント (0x10) に設定され、スタックポイン

タ`esp`は`user_stack`配列の先頭を指すように設定され（`head.s`の31行目を参照）、1ページ（4K）のメモリがスタックとして使用するために予約されています。`user_stack`配列は`sched.c`の67～72行目で定義されており、合計1024個のロングワードを含んでいます。この配列の物理メモリ上の位置は図5-24のとおりです。この時点では、カーネル自身が使用するスタックです。図中のアドレスは概算値であり、コンパイル時の実際の設定パラメータに関連しています。これらのアドレスの位置は、カーネルのコンパイル時に生成される`system.map`ファイルに記載されています。

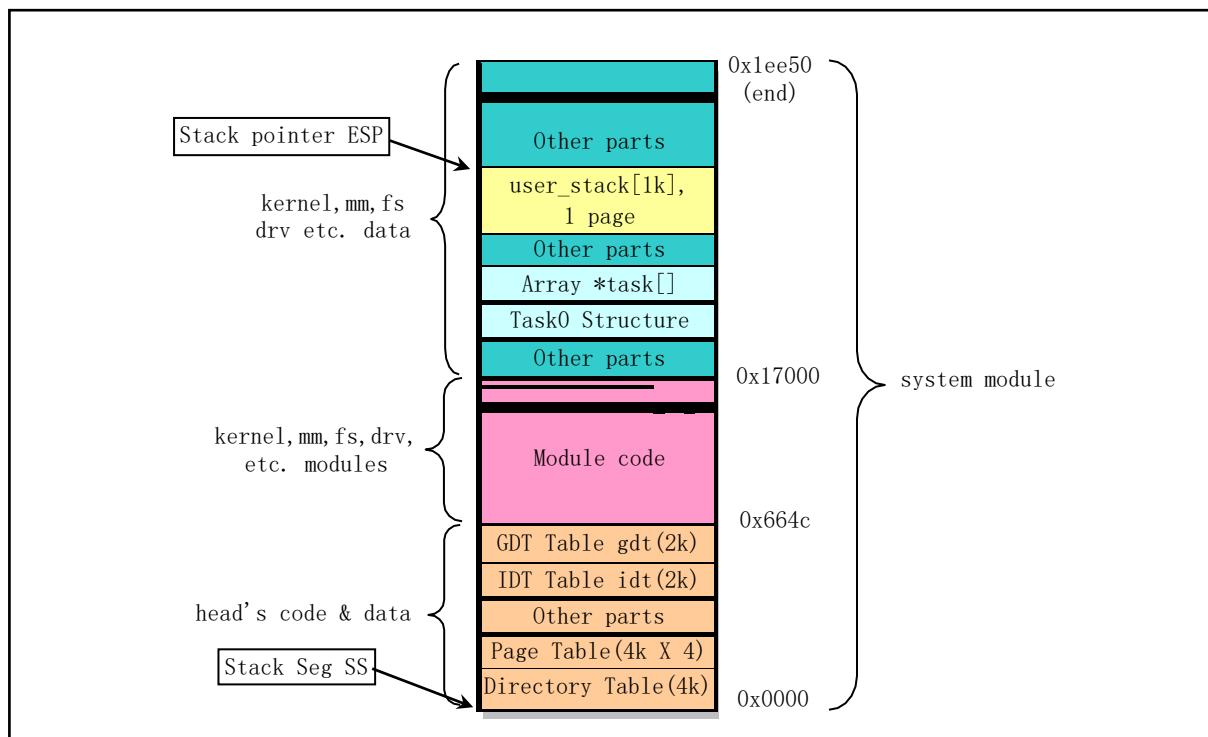


Figure 5-24 Stack diagram used by the kernel when entering protection mode

## 初期化 (main.c)

`init/main.c`プログラムでは、タスク0に制御を移す`move_to_user_mode()`コードを実行する前に、システムは常に上記のスタックを使用します。`move_to_user_mode()`が実行された後、`main.c`のコードはタスク0に「スイッチ」されます。`fork()`システムコールを実行することで、`main.c`の`init()`はタスク1で実行され、タスク1のスタックを使用します。タスク0に "切り替わった" "main()"は、タスク0のユーザモードスタックとして、カーネル自身のスタックを使い続けます。タスク0が使用するスタックの詳細な説明は後述します。

### 5.8.2 タスクの積み重ね

各タスクには、ユーザモードとカーネルモードのプログラムを実行するための2つのスタックがあり、それぞれユーザモードスタック、カーネルステートスタックと呼ばれています。この2つのスタックの主な違いは、CPUの特権レベルが異なることに加えて、タスクのカーネルモードスタックは小さく、保存できるデータ量は（4096バイト）約3Kバイトを超えることはできません。タスクのユーザモードのスタックは、ユーザーの64MBのスペース内に拡張することができます。

## ユーザー モードでの動作時

各タスク（タスク0、1を除く）は、それぞれ64MBのアドレス空間を持っています。タスク（プロセス）が生成されたばかりのとき、そのユーザ状態スタックポインタは、そのアドレス空間のほぼ最後(64MB先頭)に設定されます。実際には、図5-

25に示すように、末尾部分には実行プログラムのパラメータや環境変数なども含まれており、その後にユーザースタック空間があります。アプリケーションがユーザモードで実行されているときは、常にこのスタックを使用します。スタックが実際に使用する物理メモリは、CPUのページング機構によって決定されます。Linuxはcopy-on-writeを実装しているので、プロセスが生成された後、プロセスとその親プロセスがスタックを使用しない場合、両者は同じスタックに対応する物理メモリページを共有します。カーネルメモリマネージャは、いずれかのプロセスがスタックの書き込み操作（プッシュ操作など）を行った場合にのみ、書き込みプロセスのために新しいメモリページを割り当てます。タスク0とタスク1のユーザースタックは、以下に説明するように特別なものです。

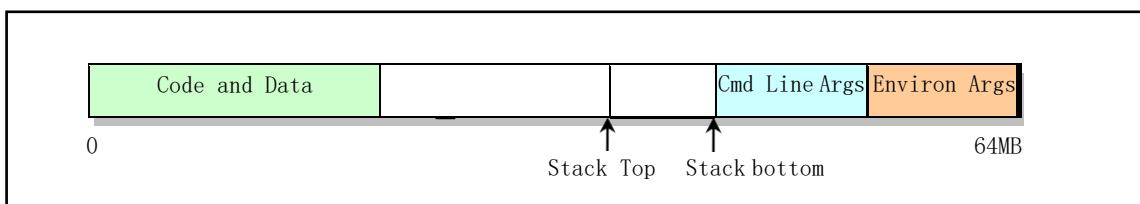


Figure 5-25 User state stack in logical space

## カーネルモードでの動作時

各タスクは、カーネルコードの実行中にタスクが実行するための独自のカーネルモードスタックを持っています。そのリニアアドレスの位置は、タスクTSSセグメントのss0とesp0フィールドで指定されます。ss0はタスクのカーネル状態スタックのセグメントセレクタで、esp0はスタックのロープインタです。そのため、タスクがユーザーコードからカーネルコードに転送されるときには、タスクのカーネル状態スタックは常に空です。タスクのカーネル状態スタックは、そのタスクデータ構造が配置されているページの最後、つまりタスクのタスクデータ構造（task\_struct）と同じページに配置されます。これは、新しいタスクが作成されたときに、fork()プログラムがタスクtssセグメントのカーネルレベルのスタックフィールド(tss.esp0とtss.ss0)に設定されることを意味します。kernel/fork.cの92行目を参照してください。

---

```
p->tss.esp0 = PAGE_SIZE + (long)p;
p->tss.ss0 = 0x10;
```

---

ここで、pは新しいタスクのタスクデータ構造ポインタ、tssはタスクステートセグメント構造です。カーネルは新しいタスクに対して、task\_struct構造のデータを保持するためのメモリを要求し、ts構造（セグメント）はtask\_structのフィールドとなります。このタスクのカーネルスタックセグメント値tss.ss0も0x10（つまりカーネルデータセグメントセレクタ）に設定されており、tss.esp0は図5-26のようにtask\_struct構造体が保存されているページの終わりを指しています。実際には、tss.esp0はページの先頭バイト（外側）を指すように設定されています（図ではスタックの一番下にあります）。これは、インテルCPUがスタック操作を行う際に、まずスタックポインタのesp値をデクリメントしてから、スタックの内容をespポインタに保存するためです。

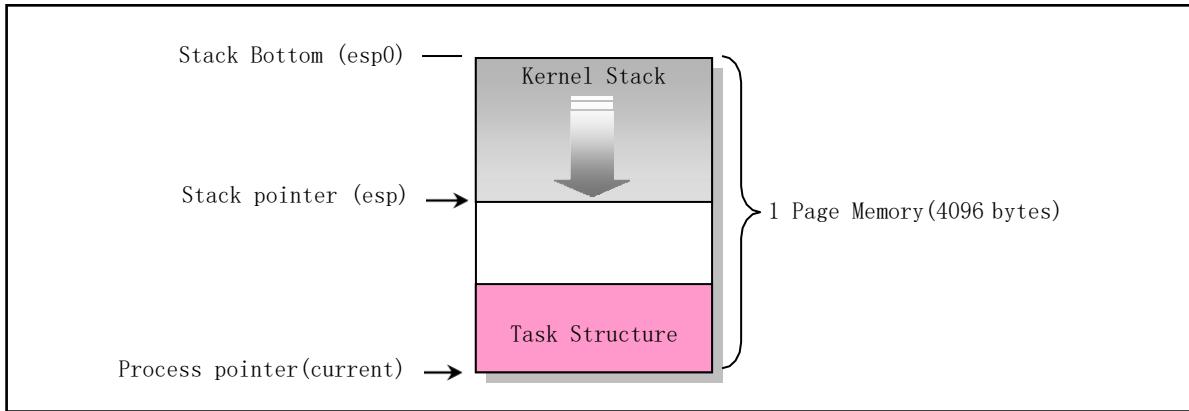


Figure 5-26 Kernel state stack diagram of a process

主記憶領域のタスクデータ構造を保存するためのメモリページを、なぜカーネルデータセグメントのデータに設定できるのでしょうか。つまり、なぜtss.ss0を0x10に設定できるのでしょうか。これは、ユーザーのカーネル状態スタックがまだカーネルデータ空間に属しているからです。このことは、カーネルコードセグメントの長さから説明することができます。head.sプログラムの最後に、カーネルコードとデータセグメントのディスクリプターがそれぞれ設定され、セグメント長はすべて16MBに設定されています。このセグメントの長さは、Head.sプログラムが使用できる最大の物理メモリの長さです。

## Linux

0.12のカーネルがサポートしています (head.s、110行目からのメモを参照)。そのため、カーネルコードは、主記憶領域を含む物理記憶領域全体のどこにでもアドレスを設定することができます。タスクがカーネルコードを実行し、そのカーネルスタックを使用する必要がある場合、CPUはTSS構造体を使用して、そのカーネル状態スタックをtss.ss0とtss.esp0の2つの値で構成されるように設定します。タスクが切り替わると、旧タスクのカーネルスタックポインタesp0は保存されません。CPUにとって、この2つの値はリードオンリーです。そのため、タスクがカーネルモード実行に入るたびに、そのカーネル状態スタックは常に空になります。

## タスク0とタスク1のスタック

タスク0(アイドルプロセス)とタスク1(initプロセス)のスタックは特殊なので、特に説明が必要です。タスク0とタスク1のコードセグメントとタスクセグメントは同じで、制限長も640KBですが、異なるリニアアドレス範囲にマッピングされています。タスク0のセグメントベースアドレスはリニアアドレス0から始まり、タスク1のセグメントベースアドレスは64MBから始まりますが、いずれも物理アドレス0~640KBの範囲にマッピングされます。このアドレス範囲には、カーネルコードや基本データが格納される。move\_to\_user\_mode()が実行されると、タスク0とタスク1のカーネル状態スタックは、それぞれのタスクデータ構造が配置されているページの末尾に配置され、タスク0のユーザ状態スタックは、プロテクトモードに入る前に使用されていたスタックで、sched.cのuser\_stack[]配列の位置に配置されます。しかし、タスク1が実行を開始すると、タスク1がuser\_stack[]にマッピングしたページテーブルエントリが読み取り専用に設定されているため、タスク1がスタック操作を行うと書き込みページ例外が発生します。そのため、カーネルはコピー온ライトのメカニズムを使って、タスク1用のメインメモリ領域ページをスタック空間として割り当てます。そうして初めて、タスク1は独自の別のユーザースタックメモリページの使用を開始します。したがって、タスク1が実際に使用

を開始するまで、タスク0のスタックは「クリーン」に保たれる必要があります。つまり、コピーされたスタックページにタスク0のデータが含まれていないことを保証するために、現時点ではタスク0はスタックを使用できません。

タスク0のカーネル状態スタックは、手動で設定された初期化タスクデータ構造で指定されます。そのユーザモードスタックは、図5-

22に示すように、`move_to_user_mode()`を実行したときの模擬的なreturnの前のスタックに設定されています。特権レベルの変更が発生すると、宛先コードは新しい特権レベルのスタックを使用し、元の特権レベルコードのスタックポインタは新しいスタックに保存されることがわかっています。そのため、まずタスク0のユーザースタックポインタが現在の特権レベル0のスタックにプッシュされ、コードポインタもスタックにプッシュされます。この手動設定されたスタックでは、元のesp値はuser\_stac kの元の位置のままであり、元のssセグメントセレクタはユーザローカルテーブルLDTのデータセグメントセレクタに設定されている0x17に設定されています。そして、タスク0のコードセグメントセレクタ0x0fが、スタック内の元のCSセグメントのセレクタとしてスタックにプッシュされ、次の命令のポインタが元のEIPとしてスタックにプッシュされます。このようにして、IRET命令を実行することで、タスク0のコードに「リターン」して実行を継続することができます。

### 5.8.3 カーネルスタックとユーザースタックの切り替え

Linux

0.12

では、すべての割込みサービスルーチンはカーネルコードに属しています。タスクがユーザーコードで実行されているときに割り込みが発生すると、割り込みによってCPUの特権レベルがレベル3からレベル0に変更され、その時点でCPUはユーザー状態のスタックとカーネル状態のスタックを切り替えることになります。CPUは新しいスタックのセグメントセレクタとオフセット値を、現在のタスクのTSSから取得します。割り込みサービスルーチンはカーネル内にあり、レベル0の特権レベルコードに属しているため、48ビットのカーネル状態スタックポインタはTSSのss0とesp0フィールドから取得します。新しいスタック（カーネル状態スタック）の位置を特定した後、CPUはまず元のユーザ状態スタックポインタssとespをカーネル状態スタックにプッシュし、次にフラグレジスタeflagsの内容とリターンポジションcsとeipをカーネル状態スタックにプッシュします。

システムコールはソフトウェア割り込みなので、タスクがシステムコールを呼び出すと、カーネルに入り、カーネル内の割り込みサービスコードを実行します。この時、カーネルコードはタスクのカーネルモードスタックを使って動作します。同様に、カーネルに入る際、特権レベルが変わると（ユーザーモードからカーネルモードへ）、ユーザーモードのスタックセグメントとスタックポインタ、およびeflagがタスクのカーネル状態のスタックに格納されます。カーネルを終了してユーザープログラムに戻るためにIRET命令が実行されると、ユーザー状態のスタックとeflagが復元されます。このプロセスを図5-27に示します。

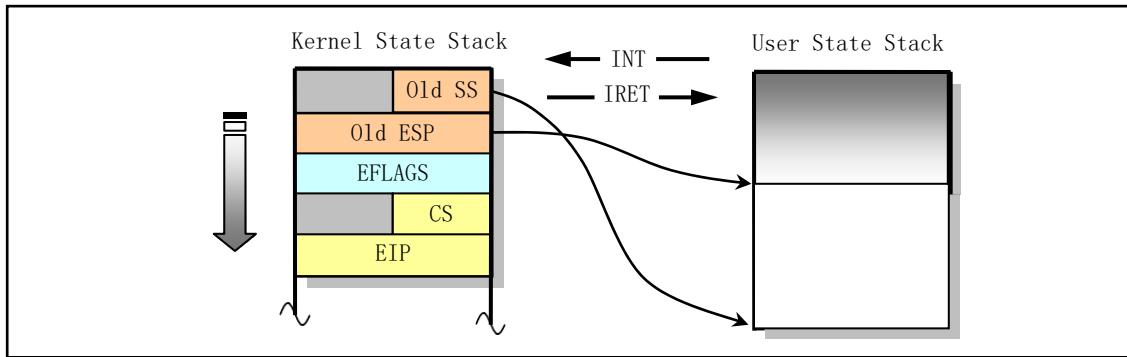


図5-27 カーネルの状態とユーザーの状態のスタック切り替え

タ

スクがカーネルモードで動作している場合、CPUが割り込みに応答すれば、スタックスイッチの操作は不要になります。なぜなら、このときタスクが実行しているカーネルコードは、すでにカーネルの状態スタックを使用しており、優先レベルの変更を伴わないからです。そのため、CPUはeflagsと割込みリターンポインタcsとeipを現在のカーネル状態スタックにpushするだけで、割込みサービスプロセスを実行します。

## 5.9 Linux用ファイルシステム 0.12

カーネルが正しく機能するためには、ファイルシステムのサポートが必要です。ルートファイルシステムは、カーネルに最も基本的な情報とサポートを提供するために使用されます。つまり、Linuxシステムが起動して開始すると、デフォルトのファイルシステムはルートファイルシステムとなります。これには、OSの最低限の設定ファイルやコマンド実行プログラムの一部が含まれる。Linuxシステムで使用されているUNIX系のファイルシステムでは、主にいくつかの指定されたディレクトリ、設定ファイル、デバイスドライバー、実行プログラム、ユーザーアプリケーション、データまたはテキストファイルが含まれます。これらには、一般的に以下のようなサブディレクトリやファイルが含まれる。

---

etc/	The directory mainly contains some system configuration files;
dev/	Contains device special files for file operation statement on devices;
bin/	Store system execution programs. Such as sh, mkfs, fdisk, etc.;
usr/	This directory stores library functions, manuals, and other files;
usr/bin	These directories store commands commonly used by users;
var/	This directory is used to store system runtime data or log information.

---

そのファイルシステムを保持する装置がファイルシステムデバイスです。例えば、一般的に使用されているWindows

10のOSでは、ハードディスクCがファイルシステムデバイスであり、ハードディスクに一定のルールに従って格納されているファイルがファイルシステムを構成しています。Windows 10では、NTFS、FAT32などのファイルシステムの

の異なるフォーマットがあります。Linuxには、EXT2やEXT3など、さまざまな形式のファイルシステムが用意されている。Linux

0.12カーネルでサポートされているファイルシステムは、MINIXオペレーションシステムの作者であるAndrew Tanenbaum氏が作成したMINIX

1.0です。しかし、現在のLinuxシステムで最も広く使われているのは、ext3またはext4ファイルシステムです。

第1章で説明したフロッピーディスク上で動作するLinux

0.12システムの場合、ブートイメージディスクとルートイメージディスクという2つの単純なフロッピーディスクから構成されています。Bootimage

はブートイメージファイルで、主にディスクのブートセクタコード、オペレーティング・システム・ローダ、カーネルのバイナリコードなどが含まれています。ルートイメージは、カーネルに最も基本的なサポートを提供するためのルートファイルシステムです。これらの2つのディスクは、起動可能なDOSオペレーティングシステムのディスクに相当します。

Linuxの起動ディスクがルートファイルシステムをロードする際には、ディスクの起動セクタの509バイト目と510バイト目にあるワード (ROOT\_DEV) のデバイス番号に従って、指定されたデバイスからルートファイルシステムがロードされる。デバイス番号が0の場合、ルートファイルシステムは起動ディスクがある現在のドライブからロードされる必要があることを意味します。デバイス番号がハードディスク・パーティション・デバイス番号の場合、ルート・ファイル・システムは指定されたハードディスク・パーティションからロードされます。

現在、その仕様ファイルとなっているのが、Linux Foundation (LF) が管理している「Filesystem Hierarchy Standard」です。FHS仕様は、オリジナルのUNIXファイルシステムの組織構造と内容をベースに、1994年からLinuxディストリビューションシステムのファイルシステムの構造と内容の標準化を検討してきました。FHSは現在、Linux Standard Library ( LSB) が提唱するISO

LSBの正式規格の一部となっています。

## 5.10 カーネルのソースコードのディレクトリ

Linuxカーネルはシングルコアモードのシステムなので、カーネル内のほとんどすべてのコードが密接に関連しています。それらの間のデータの依存関係や呼び出し関係は非常に密接です。そのため、ソースコードのファイルを読むときには、他のファイルを参照する必要があることが多いのです。そのため、カーネルのソースコードを読み始める前に、ソースコードファイルのディレクトリ構造や配置に慣れておく必要があります。

ここではまず、カーネルのソース・ディレクトリを、そのサブ・ディレクトリも含めてすべて列举します。そして、各ディレクトリに含まれるプログラムの主な機能を1つずつ紹介し、カーネルのソースコードの配置全体が頭の中で大まかに整理できるようにして、次の章でのソースコードの読み込み作業を容易にします。

linux-

0.12.tar.gzファイルをtarコマンドで解凍すると、カーネルのソースファイルがlinux/ディレクトリに配置されます。そのディレクトリ構造を図5-28に示します。

```

linux
├── boot      System boot assembly programs
├── fs        File system files
├── include   Header files (*.h)
│   ├── asm    Files related to the CPU architecture
│   ├── linux   Linux kernel specific header files
│   └── sys    System data structures
├── init     Kernel initialization program
├── kernel   Kernel process scheduling, signal, system-calls, etc.
│   ├── blk_drv Block device driver
│   ├── chr_drv Character device driver
│   └── math    Math coprocessor simulation programs
├── lib      Kernel specific library
└── mm      Memory management programs
└── tools   Tool program for generating kernel image file

```

Figure 5-28 Linux kernel source code directory structure

このバージョンのカーネルのソースコードディレクトリーには、14のサブディレクトリーがあり、合計102のコードファイルが含まれています。以下では、これらのサブディレクトリの内容を1つずつ説明します。

### 5.10.1 カーネルのホームディレクトリ `linux`

`linux`ディレクトリは、ソースコードのメインディレクトリです。ホームディレクトリには、14個のサブディレクトリがすべて含まれているのに加えて、固有のMakefileが含まれています。このファイルは、コンパイル支援ソフトmakeのパラメータ設定ファイルです。makeツールの主な目的は、複数のソースファイルが存在するシステムにおいて、どのファイルが変更されたかを識別して、再コンパイルが必要なファイルを自動的に判断することである。したがって、makeツールは、プログラムプロジェクトの管理ソフトウェアである。

`linux`ディレクトリのMakefileは、すべてのサブディレクトリに含まれるMakefileもネストします。このようにして、makeは`linux`ディレクトリ（サブディレクトリを含む）内で変更されたすべてのファイルを再コンパイルします。つまり、カーネル全体のすべてのソースコードファイルをコンパイルするには、`linux`ディレクトリでmakeソフトウェアを一度実行するだけです。

### 5.10.2 ブートプログラムのディレクトリ

`boot`ディレクトリには、カーネルのソースコードファイルをコンパイルした最初のプログラムである3つのアセンブリ言語ファイルが含まれています。これら3つのプログラムの主な機能は、コンピュータの電源投入時にカーネルを起動し、カーネルコードをメモリにロードし、32ビット保護モードに入る前にシステムの初期化を行うことである。

- `bootsect.s`プログラムは、コンパイル後のディスクの第1セクタ（ブートセクタ、0トラック（シリンド）、0ヘッド、第1セクタ）に常駐するディスクブートブロックプログラムです。PCの電源を入れ、ROM BIOSのセルフテストを行った後、メモリ0x7C00にロードされて実行されます。
- `setup.s`プログラムは、主にマシンのハードウェア構成パラメータを読み取り、カーネルモジ

ュールシステムを適切なメモリ位置に移動させるために使用されます。

- head.sのプログラムはコンパイルされ、カーネルシステムモジュールの最前部に接続され、主にハードウェアデバイスのプローブ設定や、メモリ管理ページの初期設定を行います。

bootsect.sとsetup.sのプログラムは、as86ソフトウェアを使って、as86アセンブリ言語形式（Microsoftのものと同様）でコンパイルする必要があります。Head.s は GNU as を使って、AT&T 形式のアセンブリ言語を使ってコンパイルする必要があります。これらの2つのアセンブリ言語については、次章のコードコメントと、コードリストに続く説明で簡単に説明します。

### 5.10.3 ファイルシステムディレクトリ fs

#### Linux

0.12カーネルのファイルシステムは、バージョン1.0のMINIXファイルシステムを使用していますが、これはLinuxがMINIXシステム上で開発されたためです。MINIXファイルシステムはクロスコンパイルが容易であり、LinuxのパーティションはMINIXからロードすることができます。MINIXファイルシステムが使用されていますが、LinuxはMINIXシステムとは異なる方法で処理します。主な違いは、MINIXではファイルシステムにシングルスレッドのアプローチを採用しているのに対し、Linuxではマルチスレッドのアプローチを採用していることです。マルチスレッド処理方式のため、Linuxのプログラムは、マルチスレッドによるレースコンディションやデッドロックに対処しなければなりません。そのため、Linuxのファイルシステムのコードは、MINIXのシステムよりもはるかに複雑になっています。競合状態の発生を回避するために、Linuxシステムではリソースの割り当てを厳密にチェックしています。また、カーネルモードで動作しているとき、タスクが能動的にスリープ（sleep()を呼び出す）しなければ、カーネルはタスクの切り替えを許可しないようになっている。

fs/ディレクトリは、ファイルシステム実装のディレクトリで、合計18個のCプログラムが含まれている。これらのプログラム間の主な参照関係と依存関係を図5-29に示す。図中の各ボックスはファイルを表し、基本的な参照関係で上から下に配置されている。ファイル名には接尾辞.cが省略されており、仮想ボックス内のプログラムファイルはファイルシステムの一部ではない。矢印付きの線は参照関係を、太い線は相互参照関係を示す。

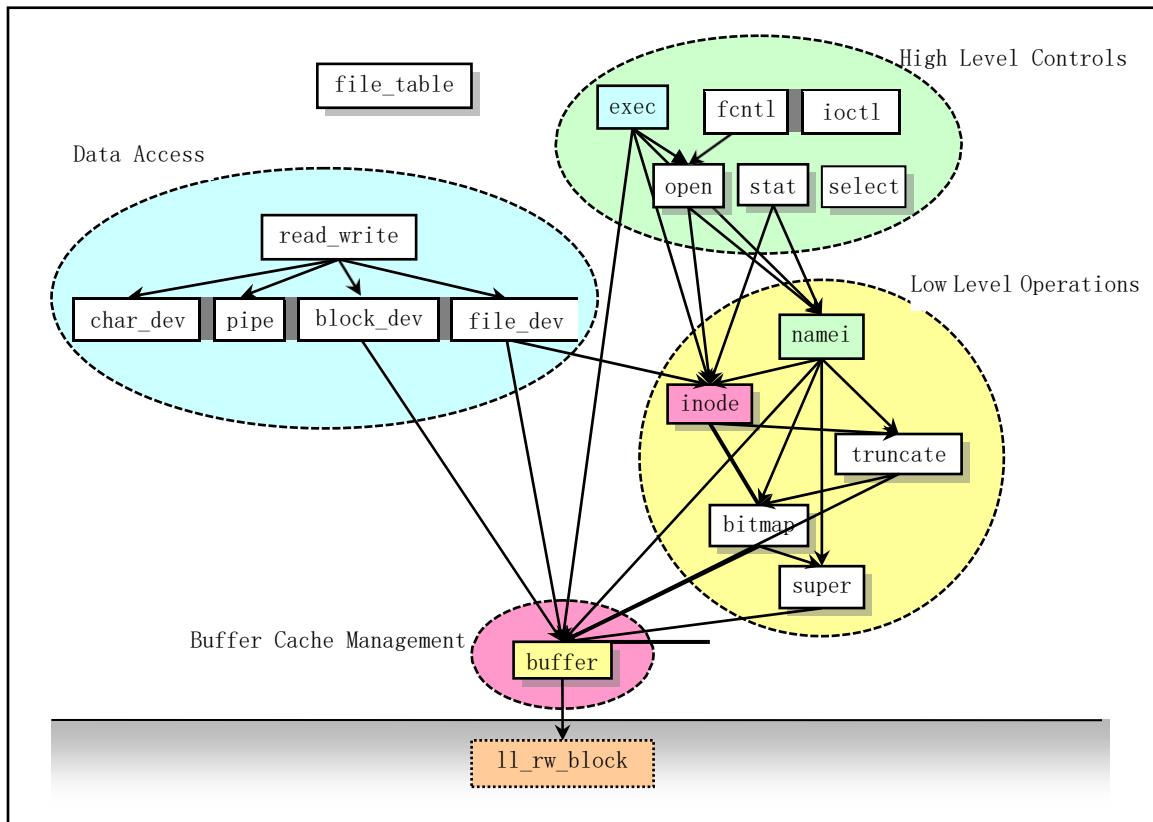


Figure 5-29 The relationship of each program in the fs directory.

図5-29 fsディレクトリ内の各プログラムの関係。

図からわかるように、このディレクトリのプログラムは、キャッシュ管理、ファイルの低レベル操作、ファイルのデータアクセス、ファイルの高レベル関数の4つの部分に分けられます。このディレクトリのファイルにアノテーションを付ける際にも、4つの部分に分けて記述します。

ファイルシステムは、メモリキャッシュの延長線上にあると考えることができます。ファイルシステムのデータにアクセスするには、まずキャッシュに読み込まれる必要があります。このディレクトリにあるプログラムは、主にファイルシステムの管理に使用されます。

キャッシュ内のバッファブロックの割り当てと、ブロックデバイス上のファイルシステムの割り当てを行います。キャッシュを管理するプログラムはbuffer.cで、その他のプログラムは主にファイルシステムの管理に使われる。

- file\_table.cファイルでは、現在、ファイルハンドル（ディスクリプター）構造の配列が1つだけ定義されています。
- ioctl.cファイルは、kernel/chr\_drv/tty.cの関数を参照して、キャラクターデバイスのio制御機能を実装します。
- exec.cファイルには、主に実行関数do\_execve()が含まれており、これはすべてのexec()関数群の中でメインとなる関数です。
- fcntl.cプログラムは、ファイルのi/o制御のためのシステムコール機能を実装するために使用されます。

- `read_write.c` プログラムは、ファイルの読み取り/書き込みを実装し、3つのシステムコール関数を見つけるために使用されます。
- `stat.c` プログラムは、ファイルの状態情報を取得する2つのシステムコールを実装しています。
- `open.c` プログラムは、ファイル属性の変更やファイルの作成・クローズを行うシステムコール関数を中心に構成されています。
- `char_dev.c` には、主にキャラクターデバイスの読み書き関数 `rw_char()` が含まれています。
- `pipe.c` プログラムには、パイプの読み取りと書き込みの関数と、パイプを作成するためのシステムコールが含まれています。
- `file_dev.c` プログラムは、`i-node` と `descriptor` 構造に基づいたファイルの読み取りと書き込みの関数を含んでいます。
- `namei.c` プログラムは、主にファイルシステムのディレクトリ名やファイル名に関する操作関数やシステムコールを含んでいます。
- `block_dev.c` には、ブロックデータの読み書き関数が含まれています。
- `inode.c` プログラムには、ファイルシステムの `i-node` を操作するための関数が含まれています。
- `truncate.c` は、ファイルを削除する際に、ファイルが占有していたデバイスのデータ領域を解放するためのプログラムです。
- `bitmap.c` ファイルは、ファイルシステム内の `i-node` や論理ブロックのビットマップを処理するために使用されます。
- `super.c` プログラムは、ファイルシステムのスーパーブロックのハンドラを含んでいます。
- `buffer.c` プログラムは、主にメモリキャッシュの処理に使用されます。
- `select.c` プログラムは、主に複数のファイルに対する同時I/O操作の問題を効果的に処理するために使用されます。

バーチャルボックス内の `ll_rw_block` は、ブロックデバイスの基本的な読み取り機能です。fs ディレクトリではなく、`kernel/blk_drv/ll_rw_block.c` にあるブロックデバイスのリード・ライトドライバ関数です。ここに置くことで、ファイルシステムが高速バッファキャッシュとブロックデバイスのドライバ(`ll_rw_block()`)を経由して、ブロックデバイスのデータを読み書きする必要があることが明確になります。ファイルシステムのプログラム自体は、ブロックデバイスのドライバと直接やりとりすることはない。

プログラムのアノテーションを行う際には、これらのファイル内の主要な関数間の呼び出し階層を追加します。

#### 5.10.4 ヘッダーファイルのディレクトリのインクルード

ヘッダーファイルのディレクトリには、合計36個の.h ヘッダーファイルがあります。メインディレクトリに13個、asmサブディレクトリに4個、Linuxサブディレクトリに11個、sysサブディレクトリに8個あります。これらのヘッダーファイルのそれぞれの機能について、以下に簡単に説明します。具体的な動作や情報については、「ヘッダーに関する注意事項」を参照してください。

- `<a.out.h>`  
`a.out` ヘッダーファイルは、`a.out` 実行ファイルのフォーマットといくつかのマクロを定義しています。
- `<const.h>` 定数シンボルファイルでは、現在、`i-node` の `i_mode` フィールドのフラグのみが定義されています。
- `<ctype.h>` 文字型のヘッダーファイルです。文字型変換のためのマクロを定義しています。
- `<errno.h>`

エラー番号のヘッダファイルです。システムの様々なエラー番号を含んでいます。(Linus は minix から導入されました)。

- <fcntl.h>  
ファイル制御のヘッダファイルです。に使用されている演算制御定数記号の定義は、以下の通りです。  
ファイルとそのディスクリプターを表示します。
- <signal.h>  
シグナルのヘッダーファイルです。シグナルシンボルの定数、シグナル構造、シグナル操作関数のプロトタイプを定義します。
- <stdarg.h>  
標準パラメータのヘッダファイルです。変数パラメータのリストをマクロの形で定義する。主に、vsprintf、vprintf、vfprintf関数用の1つの型(va\_list)と3つのマクロ(va\_start、va\_arg、va\_end)が記述されています。
- <stddef.h> 標準定義のヘッダファイルです。NULL, offsetof(TYPE, MEMBER)が定義されています。
- <string.h>  
文字列のヘッダーファイルです。主に、文字列操作に関するいくつかの組み込み関数を定義しています。
- <termios.h>  
端末入出力機能のヘッダーファイルです。主に非同期通信ポートを制御する端末インターフェースを定義しています。
- <time.h>  
時間型のヘッダーファイル。この中で最も重要なのは、tm構造体の定義と、timeに関連するいくつかの関数プロトタイプです。
- <unistd.h>  
Linux標準のヘッダーファイルです。様々なシンボル定数や型が定義され、様々な関数が宣言されています。LIBRARYが定義されている場合は、システムコール番号とインライニアセンブリ\_syscall0()も含まれます。
- <utime.h>  
ユーザータイムのヘッダーファイルです。アクセスタイム、修正タイムの構造体とutime()プロトタイプが定義されています。

### **include/asm -- アーキテクチャ関連ヘッダーファイルのサブディレクトリ**

これらのヘッダーファイルは、主にCPUアーキテクチャに密接に関連するデータ構造、マクロ関数、変数などを定義しています。

- <asm/io.h> Io  
のヘッダーファイルです。ioポートを操作する関数を、マクロの組み込みアセンブリの形で定義する。
- <asm/memory.h> メモリコピーのヘッダーファイルです。memcpy()  
の組み込みアセンブリマクロ関数を含みます。
- <asm/segment.h>  
セグメント操作作用のヘッダーファイルです。セグメント・レジスタ操作のための組み込みアセンブリ関数が定義されています。
- <asm/system.h>  
システムのヘッダーファイルです。ディスクリプタ／割込みゲートなどを定義・変更する組み

込みアセンブリマクロが定義されています。

### **include/linux -- Linuxカーネル専用ヘッダーファイルのサブディレクトリ**

- <linux/config.h>  
カーネル設定用のヘッダーファイルです。キーボード言語やハードディスクタイプ (HD\_TYPE) のオプションを定義します。
- <linux/fdreg.h>  
フロッピーディスク用のファイルです。フロッピーディスクコントローラのパラメータの定義が含まれています。
- <linux/fs.h>  
ファイルシステムのヘッダーファイルです。ファイルテーブルの構造 (file、buffer\_head、m\_inodeなど) を定義します。
- <linux/hdreg.h>  
ハードディスクパラメータのヘッダーファイル。ハードディスクのレジスタポート、ステータスコード、パーティションテーブルなどの情報へのアクセスを定義します。
- <linux/head.h>  
頭部のヘッダーファイルです。セグメントディスクリプターの簡単な構造と、いくつかのセレクタ定数が定義されています。
- <linux/kernel.h>  
カーネルのヘッダーファイルです。カーネルでよく使われる機能のプロトタイプ定義が含まれています。
- <linux/math\_emu.h>  
コプロセッサのエミュレーション用ヘッダーファイルです。コプロセッサのデータ構造と浮動小数点表現構造が定義されています。
- <linux/mm.h>  
メモリ管理用のヘッダーファイルです。ページサイズの定義と、いくつかのページリリース関数のプロトタイプが含まれています。
- <linux/sched.h> スケジューラーのヘッダーファイルでは、タスク構造体task\_structと、初期のタスク0、および記述子のパラメータ設定と取得に関するいくつかの組み込みアセンブリ関数マクロの記述。
- <linux/sys.h>  
システムコール用のヘッダーファイルです。sys\_で始まる72個のシステムコールC関数ハンドラを含みます。
- <linux/tty.h>  
ttyヘッダーファイルは、tty\_ioというシリアル通信のためのパラメータや定数を定義しています。

### **include/sys -- システム固有のデータ構造サブディレクトリ**

- <sys/param.h>  
パラメータファイルです。いくつかのハードウェア関連のパラメータ値が与えられています。
- <sys/resource.h>  
リソースファイル。プロセスが使用するシステムリソースの制限と利用に関する情報が含まれる。
- <sys/stat.h>  
ファイル状態のヘッダーファイルです。ファイルやファイルシステムの状態を表す構造体 stat{} と定数を含む。
- <sys/time.h> timeval構造体とitimerval構造体が定義されています。

- <sys/times.h> プロセス中の実行時間構造tmsとtimes()関数プロトタイプを定義します。
- <sys/types.h> 型のヘッダファイル。基本的なシステムデータ型が定義されている。
- <sys/utsname.h> システム名構造のヘッダファイル。
- <sys/wait.h>  
Waitのヘッダファイル。システムコールのwait()コアのwaitpid()と関連する定数シンボルを定義しています。

### 5.10.5 init -- カーネル初期化プログラムのディレクトリ

このディレクトリには、main.cというファイルが1つだけあり、カーネルの初期化作業を行います。その後、制御はユーザー モードに移り、新しいプロセスを作成し、コンソールデバイス上でシェルプログラムを実行します。

プログラムはまず、マシンに搭載されている物理メモリの量に基づいてバッファメモリの容量を割り当てます。システムが使用する仮想ディスクも設定している場合は、バッファメモリの後ろにもスペースを残します。その後、最初のタスク（タスク0）を手動で作成したり、割り込み可能フラグを設定するなど、ハードウェアの初期化がすべて行われる。制御がカーネルの状態からユーザーの状態に移ると、システムはまずプロセス作成関数fork()を呼び出し、init()を実行するためのプロセスを作成します。この子プロセスの中で、システムはコンソール環境を設定し、シェルプログラムを実行するための子プロセスを生成します。

### 5.10.6 kernel -- カーネルプログラムのメインディレクトリ

linux/kernelディレクトリには、合計32のファイルと3つのサブディレクトリ（blk\_drv, chr\_drv, math）が含まれています。kernelディレクトリには12個のコードファイルとMakefileがあり、サブディレクトリのkernel/blk\_drvには5個のファイル、kernel/chr\_drvには6個のファイル、kernel/mathには9個のファイルがあります。

タスクを処理するすべてのプログラムは、kernel/ディレクトリに格納されており、フォーク、イグジット、スケジューラ、一部のシステムコーラーなどが含まれます。また、割込み例外やトラップを処理する手続きサービスも含まれています。サブディレクトリには、get\_hd\_block や tty\_writeなどの低レベルデバイスドライバが含まれています。これらのファイルに含まれるコードの呼び出し関係は複雑であるため、ここではファイル間の参照関係図を詳しく説明しません。しかし、図5-30に示すように、およその分類を行うことは可能です。

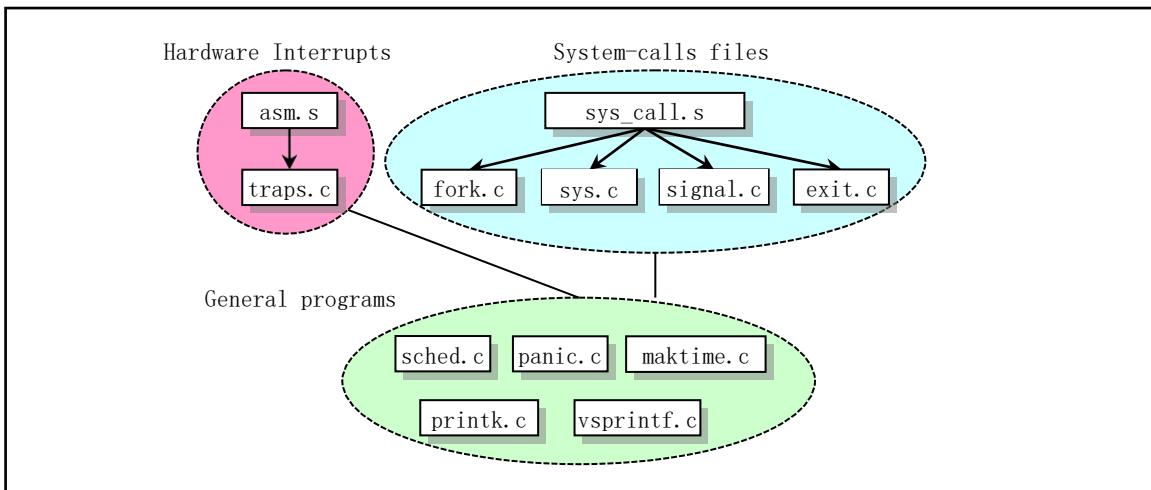


Figure 5-30 Call hierarchy of each file

図5-30 各ファイルの呼び出し階層

- `asm.s`は、システムのハードウェア例外による割り込みを処理するためのプログラムです。
- ハードウェア例外の実際の処理には、`traps.c`ファイルを使用します。各割り込み処理では、`traps.c`内の対応するC言語処理関数が個別に呼び出されます。
- `exit.c`プログラムには、プロセスの解放、セッション（プロセスグループ）の終了、プログラムの終了処理機能など、プロセスの終了処理を行うためのシステムコールや、プロセスのキル、プロセスの終了、プロセスのサスペンドなどのシステムコール機能が主に含まれています。
- `fork.c`プログラムは、`sys_fork()`システムコールで使用される2つのC言語関数、`find_empty_process()`と`copy_process()`を提供します。
- `mkttime.c`プログラムには、カーネルが1970年1月1日0:00から起動日までの秒数を計算するために使用する時刻関数`mkttime()`が含まれています。この関数は`init/main.c`で一度だけ呼び出されます。
- `panic.c`ファイルには、カーネルのエラーメッセージを表示して停止する関数`panic()`が含まれています。
- `printk.c`プログラムには、カーネル固有の情報表示関数である`printk()`が含まれています。
- `sched.c`プログラムには、スケジューリングのための基本的な関数（`sleep_on`、`wakeup`、`schedule`など）と、いくつかの簡単なシステムコール関数が含まれています。また、タイミングに関連したいくつかのフロッピーディスク操作関数もあります。
- `signal.c`プログラムには、信号処理のための4つのシステムコールと、対応する割込みハンドラで信号を処理する関数`do_signal()`が含まれています。
- `sys.c`プログラムには、多くのシステムコール関数が含まれており、その中にはまだ実装されていないものもあります。
- `system_call.s`プログラムは、Linuxのシステムコール（int 0x80）のインターフェース処理を実装しています。実際の処理は、各システムコールに対応するC言語の関数に含まれています。これらの処理関数は、Linuxカーネルコード全体に分散して配置されています。
- `vsprintf.c`プログラムは、標準ライブラリ関数に含まれるようになった文字列フォーマット関

数を実装しています。

### **kernel/blk\_drv -- ブロックデバイスドライバのサブディレクトリ**

通常、ユーザはファイルシステムを介してデバイスにアクセスし、デバイスドライバはファイルシステムへのアクセスインターフェースを実装します。ブロックデバイスを使用する場合、データのスループットが大きいブロックデバイス上のデータを効率的に利用するために、ユーザー・プロセスとブロックデバイスの間にキャッシング機構が使用されます。ブロック・デバイス上のデータにアクセスする際、システムはまずブロック・デバイス上のデータをデータ・ブロックの形でキャッシングに読み込んだ後、ユーザーのバッファ空間にデータをコピーする。

blk\_drvサブディレクトリには、合計4つのcファイルと1つのヘッダーファイルが含まれています。ヘッダーファイルblk.hは、以下を目的としています。

は、ブロックデバイスプログラムのため、Cファイルと一緒に置かれています。これらのドキュメントのおおよその関係を図5-31に示します。

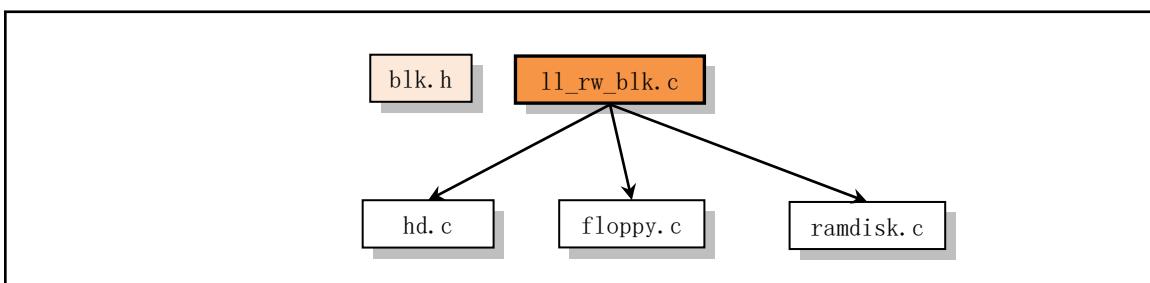


図5-31 blk\_drvディレクトリ内のファイルの階層関係。

#### ■ blk.h

ブロック・デバイス・スペシャル・ヘッダー・ファイル。複数のCプログラムで共有されるブロック・デバイス構造とデータ・ブロック・リクエスト構造が定義されています。

#### ■ hd.c

プログラムは、ハードディスクのデータブロックを読み書きするための基本的なドライバー機能、主にdo\_hd\_request()関数を実装しています。

#### ■ floppy.c

プログラムは、主にdo\_fd\_request()関数を中心に、フロッピーデータブロックの読み書きドライブ機能を実装しています。

#### ■ ramdisk.c

プログラムは、メモリ仮想ディスクドライバです。メインの関数はdo\_rd\_request()です。仮想ディスクデバイスとは、物理メモリを使って実際のディスク記憶媒体をシミュレートする技術です。その主な利点は、データアクセス操作の速度を大幅に向上させることができます。

#### ■ ll\_rw\_blk.c

プログラムは、低レベルのブロックデバイスデータ読み書き関数ll\_rw\_block()を実装しています。カーネル内の他のすべてのプログラムは、ブロックデバイスからのデータアクセスにこの関数を使用します。この関数は、ブロックデバイスのデータにアクセスする多くの場所、特にキャッシングファイル  
fs/buffer.c  
の中で呼び出されていることがわかります。

### **kernel/chr\_drv -- キャラクターデバイスドライバのサブディレクトリ**

「キャラクタ・デバイス」サブディレクトリには、4つのC言語プログラムと2つのアセンブラー・ファイルが含まれています。これらのファイルは、シリアル・ポートのrs-

232、シリアル・ターミナル、キーボード、コンソール・ターミナルのドライバを実現します。図5-32は、これらのファイル間のおおよその呼び出し階層です。

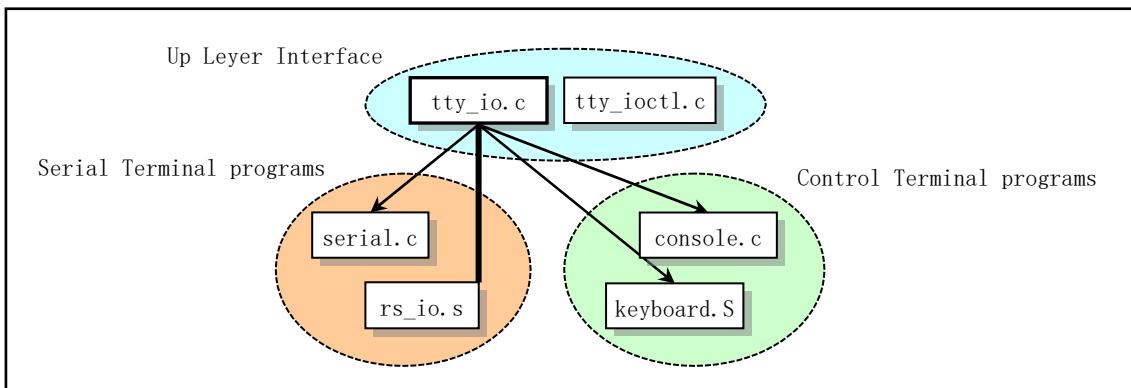


Figure 5-32 Schematic diagram of the relationship between character device programs

- `tty_io.c` プログラムには、`tty` キャラクターデバイスのリード関数 `tty_read()` とライト関数 `tty_write()` が含まれており、ファイルシステムの上位層アクセスインターフェースを提供しています。また、このプログラムには、C 関数 `do_tty_interrupt()` は、シリアル割り込み処理中に呼び出されます。この関数は、割り込みタイプがリードキャラクタの場合に呼び出されます。
- `console.c` ファイルには、主にコンソールの初期化プログラムと、`tty` デバイスで使用されるコンソール書き込み関数 `con_write()` が含まれています。また、画面表示やキーボード割り込みのための初期化設定プログラム `con_init()` も含まれています。
- `rs_io.s` プログラムは、2つのシリアルインターフェースの割り込みハンドラを実装するため使用されます。割り込みハンドラは、割り込み識別子レジスタ（ポート `0x3fa` または `0x2fa`）から取得した4つの割り込みタイプのそれぞれを処理し、割り込みタイプをリードキャラクタとして処理するコードで `do_tty_interrupt()` を呼び出します。
- `Serial.c` は、非同期シリアル通信チップであるUARTの初期化と、2つの通信ポートの割り込みベクターの設定に使用されます。また、`tty` がシリアルポートへの出力に使用する `rs_write()` 関数も含まれています。
- `tty_ioctl.c` プログラムは、`tty` の io 制御インターフェース関数 `tty_ioctl()` を実装し、`termio(s)` 端末の `i`o 構造体への読み書きを行うもので、システムコール `sys_ioctl()` を実装した `fs/iotcl.c` プログラムの中で呼ばれている。
- `keyboard.S` プログラムは、主にキーボード割り込みハンドラプロシージャ `keyboard_interrupt` を実装しています。

### **kernel/math -- コプロセッサエミュレータのサブディレクトリ**

このサブディレクトリには、数学コプロセッサのエミュレーションハンドラファイルがあり、合計9個のCファイルがあります。マシンに数学コプロセッサが存在しない場合、CPUがコプロセッサ命令を実行すると、デバイスが存在しないという割り込みINT7が発生します。そのため、この割り込みを利用して、コプロセッサの機能をソフトウェアでシミュレートすることができます。これらのプログラムは、CPUのハードウェアと密接に関係していますが、それ以外のカーネルの実装とはほとんど関係ありません。プログラムに含まれる関連知識は、マルチプロセッサのプログラミングやア

サンプル・ディスアサンプルなどのシステムレベルのプログラムを実装する際に非常に役立ちます。

- `math_emulate.c` プログラムは、コプロセッサエミュレーションのメインプログラムで、デバイスが存在しない例外ハンドラ、浮動小数点命令エミュレーションのメイン関数`do_emu()`、他の補助関数を実装しています。
- `error.c` は、コプロセッサから送られてくるエラー信号を処理するためのプログラムです。その主な関数は`math_error()`です。
- `ea.c` プログラムは、浮動小数点命令をシミュレーションする際に、命令内のオペランドが使用する実効アドレスを計算するために使用されます。
- `convert.c` は、シミュレーションの計算過程において、ユーザーデータ形式と一時的な実数形式との間のデータ型変換操作を行うためのプログラムです。
- `add.c` プログラムは、シミュレーションプロセスにおける加算を実装し、仮数部の記号化と非記号化の間の変換を行います。
- `compare.c` プログラムは、コプロセッサのコンペア・アキュムレータにおける2つの一時的な実数のサイズをシミュレートするために使用されます。
- `get_put.c` プログラムは、ユーザーのメモリ上のデータへのアクセスを実装しています。
- `mul.c` プログラムは、コプロセッサの乗算命令をシミュレートするために使用されます。
- `div.c` プログラムは、コプロセッサの分割をシミュレートするために使用されます。

## 5.10.7 lib -- カーネル・ライブラリ・ディレクトリ

通常のユーザープログラムとは異なり、カーネルコードは標準Cライブラリやその他のライブラリコードを使用することができません。また、メイン

その理由は、完全なC関数ライブラリは大きく、実装が複雑だからです。そのため、カーネルソースには特別なlib/ディレクトリがあり、カーネルが使用する必要のあるいくつかの関数を提供しています。カーネル関数ライブラリは、ユーザー mode (プロセス0、1) で実行されるカーネル初期化プログラム`init/main.c`のコールサポートに使用されます。これは、通常の静的ライブラリの実装とまったく同じです。読者は一般的な`libc`ライブラリの基本構造を学ぶことができます。

`lib/ディレクトリ`には12個のC言語ファイルがあります。`tytso`氏が作成した`malloc.c`を除き、他のファイルは非常に短く、1~2行のコードしかないものもあります。これらのファイルは、いくつかのシステムコールのインターフェース関数を実装しています。これらのファイルには主に、終了関数`_exit()`、ファイルクローズ関数`close(fd)`、ファイル記述子コピー関数`dup()`、ファイルオープン関数`open()`、ファイルライト関数`write()`、プログラム実行関数`execve()`などがある。メモリ確保関数`malloc()`、子プロセスの状態を待つ関数`wait()`、セッションを作成するシステムコール`setsid()`、`include/string.h`で実装されているすべての文字列操作関数。

## 5.10.8 mm -- メモリ管理ディレクトリ

このディレクトリには、3つのコードファイルが含まれています。主にアプリケーションのメインメモリ領域の使用を管理するために使用され、論理アドレスからリニアアドレス、リニアアドレスから物理メモリアアドレスへのマッピング操作を実装しています。また、メモリページング機構により、主記憶領域の仮想メモリページと物理メモリページの間に対応関係が確立される。同時に、仮想記憶技術も実現している。

Linux カーネルは、フラグメント方式とページング方式の両方でメモリを扱います。1つ目は、80X86 4G の仮想アドレス空間を 64 セグメント (1 セグメントあたり 64MB) に分割する方法です。カーネルプログラムは最初のセグメントを占有し、その物理アドレスはセグメントのリニアアドレスと同じになります。その後、各タスクに使用するセグメントが割り当てられます。ページング機構を用いて、指定された物理メモリページをセグメントにマッピングし、フォークで作成された重複コピーを検出し、コピー・オン・ライト機構を実行する。

page.sファイルには、メモリページアポート (int

14) ハンドラが含まれており、主にページフォールトによるページ例外や不正なアドレスへのアクセスによるページ保護の処理に使用されます。

memory.cプログラムには、メモリを初期化するmem\_init()関数と、page.sのメモリ割り込み手続きから呼び出されるdo\_no\_page()関数とdo\_wp\_page()関数が含まれています。新規プロセスの作成やプロセスのコピー操作を行う際には、メモリハンドラを使用して管理用メモリ空間を確保します。

swap.cプログラムは、メインメモリーの物理ページと高速二次記憶装置（ハードディスク）の空間との間のページスワップを管理するために使用されます。メインメモリーの空き容量が足りない場合、一時的に使用していないメモリーページをハードディスクに保存することができます。ページフォールト例外が発生すると、まず要求されたページがハードディスクのスワップスペースにあるかどうかを確認します。存在していれば、そのページはスワップスペースから直接メモリに読み込まれます。

## 5.10.9 tools -- カーネル・ツール・ディレクトリ

このディレクトリにある

build.c

プログラムは、完全なカーネルモジュールを構築するために使用されます。このプログラムは、Linuxディレクトリでコンパイルされたオブジェクトを、実行可能なカーネル・イメージ・ファイル・イメージに結合します。具体的な機能については、次の章で説明します。

## 5.11 カーネルコードとユーザープログラム

Linuxシステムでは、カーネルは2つの方法でユーザープログラムのサービスサポートを行うことができます。1つはシステムコールインターフェース、つまりint 0x80を呼び出す割り込みで、もう1つは開発の

環境ライブラリ関数、またはカーネルライブラリ関数です。ただし、カーネルライブラリ関数は、カーネルで作られたタスク0やタスク1でしか使われません。最終的にはシステムコールを呼び出すことに変わりはありません。したがって、実際には、カーネルは、すべてのユーザープログラムやプロセスに対して、システムコールの統一的なサービスインターフェースを提供しているにすぎません。lib / ディレクトリにあるカーネル・ライブラリ関数コードの実装方法は、基本的に C 関数ライブラリ libc と同じです。カーネルのリソースを使用するため、図5-4に示すように、最終的にはインラインのアセンブリコードによってカーネルのシステムコールが呼び出されます。

システムコールは、主にシステムソフトウェアのプログラミングや、ライブラリ機能の実装に用いられる。一般的のユーザーが開発したプログラムは、libcなどのライブラリの関数を呼び出してカーネルリソースにアクセスする。これらのライブラリに含まれる関数やリソースは、しばしばアプリケ

ーション・プログラミング・インターフェース（API）と呼ばれます。これは、アプリケーションが使用する標準的なプログラミング・インターフェースのセットを定義するものである。これらのライブラリの関数を呼び出すことにより、アプリケーションコードは、ファイルやデバイスへのアクセスの開閉、科学的計算の実行、エラー処理、グループやユーザーID番号などのシステム情報へのアクセスなど、さまざまな共通タスクを実行することができる。

UNIX系OSでは、POSIX規格に基づいたAPIインターフェースが最もよく使われており、Linuxも例外ではない。APIとシステムコールの違いは、POSIXなどのアプリケーション・インターフェース規格を実装するために、APIがシステムコールに対応している場合と、複数のシステムコール関数によって実装されている場合があることだ。もちろん、API関数の中には、システムコールを使う必要のないもの、つまり、カーネルが提供するサービスを使わないものもある。したがって、関数ライブラリは、POSIX規格を実装したメインのインターフェイスとみなすことができます。アプリケーションは、システムコールとの関係を気にしません。2つのOSが提供するシステムコールにどれだけの違いがあるても、同じAPI規格への準拠を提供していれば、アプリケーションはこれらのOS間で移植可能です。

システムコールは、カーネルと外界との間のインターフェースの最上位に位置します。カーネルでは、各システムコールはマクロとして実装されていることが多く、シリアル番号を持っています（`include/unistd.h`ヘッダファイルで定義されています）。アプリケーションは、システムコールを直接使用してはいけません。そうしないと、プログラムの移植性が悪くなります。そのため、現在のLinux Standard

Base (LSB) をはじめとする多くの標準規格では、アプリケーションがシステムコールのマクロに直接アクセスすることを推奨していません。システムコールに関するドキュメントは、Linuxオペレーティングシステムのオンラインマニュアルのパート2に記載されています。

ライブラリファイルには一般的に、高度な機能を実行するためにC言語では提供されていない入出力関数や文字列操作関数などのユーザーレベルの関数が含まれている。ライブラリ関数の中には、システムコールを拡張しただけのものもあります。例えば、標準I/Oライブラリ関数の`fopen`と`fclose`は、システムコールの`open`と`close`と同様の機能を、より高いレベルで提供しています。この場合、通常はシステムコールの方がライブラリ関数よりも若干性能が良いのですが、ライブラリ関数の方がより多くの機能を提供し、より多くのエラーを検出することができます。システムが提供するライブラリ関数は、オペレーティングシステムのオンラインマニュアルのセクション3に記載されています。

## 5.12 linux/Makefile

このセクションから、カーネルのソースコードファイルのアノテーションを開始します。まず、Linuxディレクトリで最初に出会うMakefileというファイルについてコメントします。以降のセクションも同様の記述構造で注釈をつけていきます。

### 5.12.1 機能説明

Makefileは、プログラムのコンパイル時のバッチファイルに相当します。これは、デフォルトのコンパイル設定

は、実行時にユーティリティプログラムmakeの入力ファイルとなります。Makefileのあるディレクトリでmakeコマンドを入力するだけで、Makefileの設定に従って、コンパイラやリンクを呼び出し、ソースコードやターゲットコードファイルをコンパイル、リンク、インストールします。

makeユーティリティーは、複数のソースファイルを含むプログラムパッケージの中で、どのファイルを再コンパイルする必要があるかを自動的に判断し、それらのプログラムファイルをコンパイルするコマンドを発行する。そこで、makeを使う前に、Makefileというテキストファイルを書いておく必要がある。このファイルには、パッケージ全体のプログラムの関係を記述し、更新が必要なファイルごとに具体的な制御コマンドを与える。一般的に、実行可能なターゲットは、コンパイラによって作成されたオブジェクトファイルに基づいて更新されます。適切なMakefileを書いておけば、プログラムパッケージ内のいくつかのソースコードファイルを変更するたびに、必要なすべての再コンパイル作業を行うことができます。makeツールは、Makefileファイルとコードファイルの最終修正時刻を使って、どのファイルを更新する必要があるかを判断します。更新が必要な各ファイルに対して、Makefileの情報に基づいて適切なコマンドを発行します。Makefileの中で「#」で始まる行はコメント行です。ファイルの先頭にある「=」代入文は、いくつかのパラメータやコマンドの略語を定義しています。

カーネルディレクトリにあるこのMakefileの主な機能は、独立してコンパイルされたツール/ディレクトリ内のビルド実行ファイルを使って、最終的にすべてのカーネルのコンパイル済みコードを接続し、実行可能なカーネルイメージファイルにマージするよう、makeプログラムに指示することです。具体的なプロセスは(1)

8086アセンブラーを使って、boot/にあるbootsect.sとsetup.sをコンパイルし、それぞれのオブジェクトを生成します。(2)

他のプログラムをGNUコンパイラgcc/gasを用いてソースコードをコンパイルし、リンクしてモジュールシステムを生成する。(3)

最後に、ビルドツールを使って、3つのパートをカーネルイメージファイルのイメージにまとめます。

ビルドツールは、tools/build.cソースファイルからコンパイルされたスタンドアローンの実行ファイルです。カーネルコードにはコンパイル、リンクされません。カーネルイメージファイルを構築する過程でのツールとしてのみ使用されます。基本的なコンパイル・リンク・組み合わせの構造を図5-33に示します。

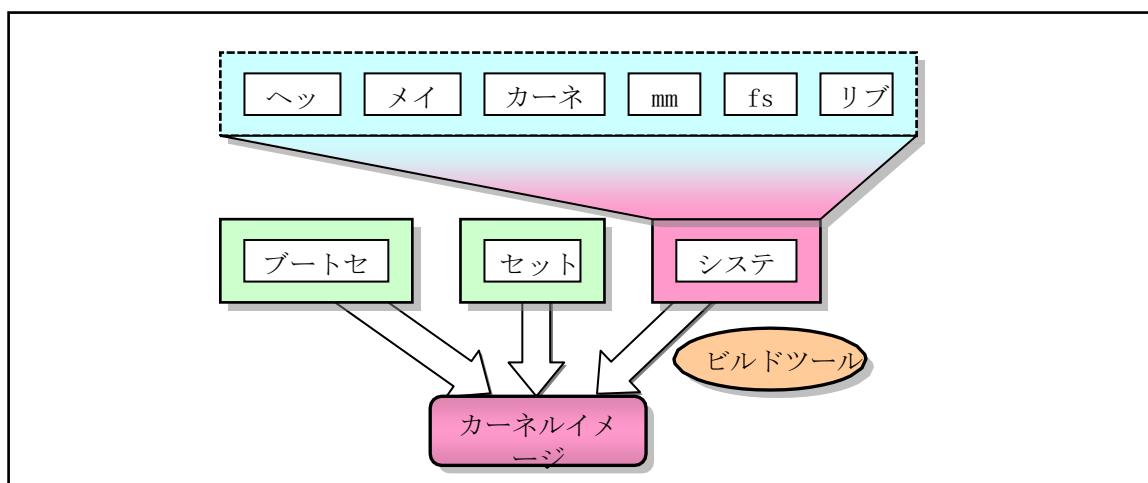


図 5-33 カーネルのコンパイルリンク/結合構造

Linuxカーネルのソースコードでは、tools/、init/、boot/の各ディレクトリを除いて、それぞれのサブディレクトリに対応するMakefileが含まれており、その構造は同一です。紙面の都合上、本書ではMakefileの注釈は1つだけとなっています。プログラム5-1は、このファイルの詳細なコメントです。

なお、ソースファイル中の行番号のある文がオリジナルの文、行番号のない文が本書の著者のコメントです。

## 5.12.2 プログラムアノテーション

Program 5-1 linux/Makefile

```

1 #
2 # if you want the ram-disk device, define this to be the
3 # size in blocks.
4 #
# Define the size of the block if you want to use a RAM disk device. The default RAMDISK
# is not defined here (commented out), otherwise gcc will be compiled with the option
# '-DRAMDISK=512', see line 13 below.
5 RAMDISK = #-DRAMDISK=512
6
7 AS86    =as86 -O -a      # 8086 assembly and linker. The meaning of parameter is: -O
8 LD86    =ld86 -O        # generates 8086 object; -a code compatible with gas and gld.
9
10 AS     =gas           # GNU assembler and linker. see chapter 3 for more information.
11 LD     =gld
# gld options: -s all symbolic info omitted in output file; -x removes all local symbols;
# -M indicates that a link map is required, which is a memory address map generated by the
# linker, which lists the location information that the code block is loaded into memory.
12 LDFLAGS =-s -x -M

# gcc is the GNU compiler. For UNIX-like scripts, when you reference an identifier, you
$ need to precede it with a sign and enclose the identifier in parentheses.
13 CC     =gcc $(RAMDISK)

# gcc options: -Wall prints all warnings; -O optimizes code. '-f flag' specifies flag.
# Where, -fstrength-reduce is used to optimize loop statements; -fomit-frame-pointer
# indicates that do not leave frame pointer in register for functions that do not require
# frame pointer. This avoids operation and maintenance of frame pointer in the function.
# -fcombine-reg is used to indicate that the compiler combines instructions that copy
# one register to another. -mstring-insns is an option that Linus adds to gcc. It is used
# by gcc-1.40 to copy string structures using 386 CPU string instructions and can be removed.
14 CFLAGS =-Wall -O -fstrength-reduce -fomit-frame-pointer \
15 -fcombine-reg -mstring-insns

# cpp is gcc's preprocessor, used for macro substitution, conditional compilation, and
# inclusion files specified with '#include'. All lines starting with '#' need to be
# processed by preprocessor. All macros defined by '#define' will be replaced with their
# definitions. All conditional lines such as '#if', '#ifdef', '#ifndef', and '#endif' are
# used to determine whether to include statements in their specified range.
# The option '-nostdinc -Iinclude' means not searching standard header file directory,
# ie not using files in /usr/include/, but using directory specified by the '-I' option
# or searching in the current directory.
16 CPP    =cpp -nostdinc -Iinclude

```

```

17
18 #
19 # ROOT_DEV specifies the default root-device when making the image.
20 # This can be either FLOPPY, /dev/xxxx or empty, in which case the_
21 # default of /dev/hd6 is used by 'build'.
22 #
23 # Here /dev/hd6 corresponds to first partition of the second hard disk. This is the
24 # location where the root file system is located when Linus develops the Linux kernel.
25 # /dev/hd2 represents 2nd partition of 1st hard disk and is used as a swap partition.
26 ROOT_DEV=/dev/hd6
27 SWAP_DEV=/dev/hd2
28
29 # Below are the object files generated in the kernel, mm, and fs directories. For ease of
30 # reference, they are represented here by the ARCHIVES identifier.
31 ARCHIVES=kernel/kernel.o mm/mm.o fs/fs.o

# Block and character device library files. '.a' indicates that the file is an archive
# file, that is, a library file containing a collection of executable binary code
# subroutines, usually generated by GNU's ar program. Ar is a GNU binary file tool for
# creating, modifying, and extracting files from archive files.
32 DRIVERS =kernel/blk_drv/blk_drv.a kernel/chr_drv/chr_drv.a
33 MATH =kernel/math/math.a
34 LIBS =lib/lib.a           # A generic library compiled from files in lib/ dir.
35
36 # Here is the old-fashioned implicit suffix rule for make. This line instructs make to
37 # compile all '.c' files into '.s' assembly using the commands of rule after ':'. The
38 # whole sentence means that gcc uses the option specified by the CFLAGS and only uses the
39 # header file in include/ dir, and stops (-S) compiling, thereby generating an assembly
40 # file corresponding to each input C file. By default, the resulting assembly file is the
41 # original C file with suffix '.c' replaced with '.s'. '-o' indicates the output file.
42 # Where '$*.s' (or '$@') is automatic object variable, and '$<' represents the first
43 # prerequisite, here is the file that meets the condition '*.c'.
44 # The following three rules are used for different requirements. If the target is .s
45 # file and the source is a .c file, the first rule will be used; if target is .o and the
46 # original is .s, the second rule will be used; if the target is a .o file, the original
47 # is a c file, then the third rule is used.
48 .c.s:
49     $(CC) $(CFLAGS) \
50         -nostdinc -Iinclude -S -o $*.s $<
51 .s.o:
52     $(AS) -c -o $*.o $<
53 .c.o:
54     $(CC) $(CFLAGS) \
55         -nostdinc -Iinclude -c -o $*.o $<
56
57 # The following 'all' means to create the topmost target of the Makefile, here is the
58 # Image file. It is the boot disk image file. If you write it to a floppy disk, you can
59 # use the floppy disk to boot the Linux system. See the line 46 for commands to write an
60 # Image to a floppy disk under Linux. The software rawrite.exe can be used under DOS.
61 all:    Image
62
63 # The target (Image) is generated by 4 elements behind the colon, which are the bootsect
64 # and setup files in boot/, the system and build files in tools/. Lines 43--44 are commands

```

```

# executed. Line 43 indicates that the bootsect, setup, and system files are assembled
# to be kernel image file, with $(ROOT_DEV) device using build utility in tools directory.
# The sync cmd on line 45 forces buffer to immediately write disk and update super block.
42 Image: boot/bootsect boot/setup tools/system tools/build
43         tools/build boot/bootsect boot/setup tools/system $(ROOT_DEV) \
44             $(SWAP_DEV) > Image
45         sync
46
47 # Indicates that the disk target is created from Image. dd is a standard cmd: copy a file,
48 # convert and format it according to the options. bs= the number of bytes read/written at
49 # a time. If= the input file, and of= the file to be output. Here /dev/PS0 refers to first
50 # floppy disk drive (device file). Use /dev/fd0 under current linux system.
51 disk: Image
52     dd bs=8192 if=Image of=/dev/PS0
53
54 tools/build: tools/build.c          # Create executable build tool.
55     $(CC) $(CFLAGS) \
56     -o tools/build tools/build.c
57
58 boot/head.o: boot/head.s          # Generate head.o object using the .s.o rule.
59
60 # Indicates that the tools/system is to be generated by the elements to the right of the
61 # colon. Line 57--62 is cmds to generate system object. The last '> System.map' means that
62 # gld needs to redirect the link info into the System.map file.
63 tools/system: boot/head.o init/main.o \
64     $(ARCHIVES) $(DRIVERS) $(MATH) $(LIBS)
65     $(LD) $(LDFLAGS) boot/head.o init/main.o \
66     $(ARCHIVES) \
67     $(DRIVERS) \
68     $(MATH) \
69     $(LIBS) \
70     -o tools/system > System.map
71
72 # The archive file math.a is built by cmds on line 64: cd into kernel/math/; run make.
73 kernel/math/math.a:
74     (cd kernel/math; make)
75
76 kernel/blk_drv/blk_drv.a:          # Create block driver archive file.
77     (cd kernel/blk_drv; make)
78
79 kernel/chr_drv/chr_drv.a:          # Character driver archive file.
80     (cd kernel/chr_drv; make)
81
82 kernel/kernel.o:                  # kernel object file.
83     (cd kernel; make)
84
85 mm/mm.o:                          # Memory management object file.
86     (cd mm; make)
87
88 fs/fs.o:                           # File system object file.
89     (cd fs; make)
90
91 lib/lib.a:                         # Internal lib.a
92     (cd lib; make)

```

```

85 # Compile setup.s file to generate setup.o using the 8086 assembler and linker. The option
# -s indicates that the symbol information in the target file need to be removed.
86 boot/setup: boot/setup.s
87         $(AS86) -o boot/setup.o boot/setup.s
88         $(LD86) -s -o boot/setup boot/setup.o
89
90 # Execute preprocessor, replace macro in *.S file to generate the corresponding *.s file.
91 boot/setup.s:    boot/setup.S include/linux/config.h
92         $(CPP) -traditional boot/setup.S -o boot/setup.s
93
94 boot/bootsect.s:      boot/bootsect.S include/linux/config.h
95         $(CPP) -traditional boot/bootsect.S -o boot/bootsect.s
96
97 boot/bootsect:  boot/bootsect.s
98         $(AS86) -o boot/bootsect.o boot/bootsect.s
99         $(LD86) -s -o boot/bootsect boot/bootsect.o
100
101 # When 'make clean' is executed, the commands on lines 101--107 are executed, and all
102 # files generated are removed. 'rm' is a file deletion cmd, and the option -f means to
103 # ignore files that do not exist and does not display deletion messages.
104 clean:
105     rm -f Image System.map tmp_make core boot/bootsect boot/setup \
106             boot/bootsect.s boot/setup.s
107     rm -f init/*.o tools/system tools/build boot/*.o
108     (cd mm;make clean)
109     (cd fs;make clean)
110     (cd kernel;make clean)
111     (cd lib;make clean)
112
113 backup: clean
114     (cd .. ; tar cf - linux | compress - > backup.Z)
115     sync
116
117 dep:
118 # This goal or rule is used to generate dependencies between files. These dependencies are
119 # created to let the make command use them to determine if a target object needs to be rebuilt.
120 # For example, when a header file has been changed, make can recompile all *.c files related
121 # to it through the generated dependencies. The specific method is as follows:
122 # Use the string editor sed to process the Makefile (here, this file), the output is to
123 # delete all the lines after the '## Dependencies' line in the Makefile, that is, delete
124 # all lines from 122 to the end of the file, and generate a temporary file tmp_make (also
125 # known as 114 lines). # Then perform a gcc preprocessing operation on each C file (in fact,
126 # only one file main.c) in the specified directory (init/). The flag '-M' tells the preprocessor
127 # cpp to output rules describing the relevance of each object file, and these rules conform
128 # to the make syntax. For each source file, the preprocessor outputs a rule whose result
129 # is the target file name of the corresponding source file plus its dependencies, that is,
130 # a list of all the header files contained in the source file. Then add the pre-processing
131 # results to the temporary file tmp_make, and finally copy the temporary file into a new Makefile.

```

---

```

# The '$$i' on line 115 is actually '$($i)'. Here '$i' is the value of the shell variable
# 'i' in front of this sentence.
114      sed '/#\#\#\ Dependencies/q' < Makefile > tmp_make
115      (for i in init/*.c;do echo -n "init/";$(CPP) -M $$i;done) >> tmp_make
116      cp tmp_make Makefile
117      (cd fs; make dep)
118      (cd kernel; make dep)
119      (cd mm; make dep)
120
121 #### Dependencies:
122 init/main.o : init/main.c include/unistd.h include/sys/stat.h \
123   include/sys/types.h include/sys/time.h include/time.h include/sys/times.h \
124   include/sys/utsname.h include/sys/param.h include/sys/resource.h \
125   include/utime.h include/linux/tty.h include/termios.h include/linux/sched.h \
126   include/linux/head.h include/linux/fs.h include/linux/mm.h \
127   include/linux/kernel.h include/signal.h include/asm/system.h \
128   include/asm/io.h include/stddef.h include/stdarg.h include/fcntl.h \
129   include/string.h

```

---

## 5.13 概要

本章では、初期のLinux

OSのカーネルモードとアーキテクチャについて概観します。まず、Linux

0.12のカーネルの使用方法と管理メモリの方法、カーネル・ステート・スタックとユーザ・ステート・スタックの設定と使用方法、割り込みの仕組み、システム・ロックのタイミング、プロセスの生成・スケジューリング・終了の方法について説明します。そして、ソースコードのディレクトリ構造に沿って、各サブディレクトリ内のコードファイルの基本機能や階層関係を詳しく紹介しています。

また、Linux

0.12で使用されているターゲット・ファイル・フォーマットについても説明しています。最後に、Linuxカーネルのホームディレクトリにあるmakefileから始めて、カーネルのソースコードにコメントを付け始めました。

本章は、Linux

0.12カーネルに関する重要な情報をまとめたものと言えますので、後続の章を読む際の参考にしてください。次章のブートローダからは、正式にカーネルのソースコードのアノテーションを開始しました。