

計算機方式論

第12章 記憶保護

1

記憶保護(memory protection)

◆複数のユーザが同時使用するシステム

多数のユーザプログラム+管理の制御プログラム

↓ ユーザのプログラムの誤り

他のユーザプログラムや制御プログラムの破壊、誤使用

↓ これを避ける

•保護機能

ファイル保護機能(file protection)

ファイルの保護

記憶保護機能(memory protection)

主記憶上のプログラムやデータの保護

2

モード制御機能

• モード制御機能

実行モードを設け、各モード下で、異なるアクセス制御を行う。

実行モード:

特権モード

制御プログラムが動作するモード。

ハードウェアの全機能の制御。

非特権モード

ユーザプログラムが動作するモード。

ハードウェアの一部の機能の制御。

一部の命令(特権命令)を実行できない。

• モード指定インディケータ

プログラム状態語(PSW)中(IBM:15ビット目)

各セグメントごとにモード指定(MULTICS)

中央処理装置に設置(NEAC2200)

3

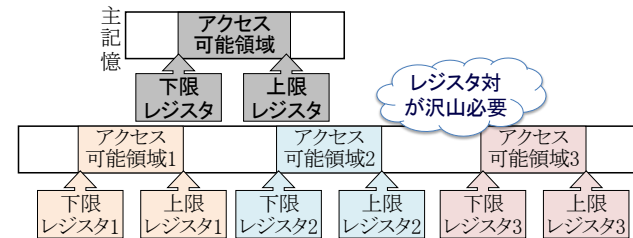
アクセス制御機能-限界レジスタ方式

• アクセス制御機能

他のプログラムを誤ってアクセスすることを防止するための
チェックを行なう機能-非特権モード下でチェック

①限界レジスタ方式

主記憶の領域を上限レジスタと下限レジスタで指定し、
その領域以外のアクセスを禁止する方式。

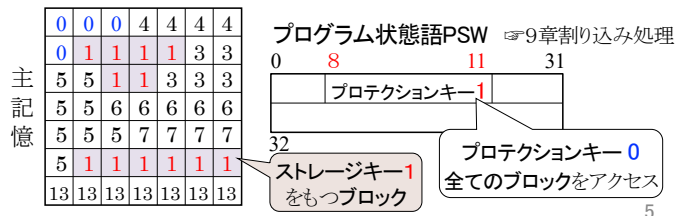


4

アクセス制御機能-キー方式

②キー方式

- 主記憶を一定の大きさ(主記憶ブロック)に区切り、
ストレージキー(5ビット)を設ける
4ビット…キー番号(0~15)
1ビット…アクセス指定インディケータ
0: 書き込み時のみに保護
1: 読み出し／書き込み時に保護
- プログラム…**プロテクションキー**(4ビット)
キーの一致するブロックだけアクセスできる⇒ブロック単位の保護



リング保護方式による記憶保護

- MULTICS**で採用された方式で、セグメント単位で保護
- インテルのマイクロプロセッサ80386以降にも採用
- システムの動作モードが**特権モード**と**非特権モード**だけでは不十分:
TSS等の業務をやりながら、制御プログラムの機能の追加や修正。
制御プログラムの全てが完全にデバッグされているとは限らない。
このため、制御プログラムもいくつかのレベルに分け、そのレベルに応じてアクセス権限を規定する。
- リング番号**: 各セグメントがもち、保護の度合を表す
リング番号0: 制御プログラム中で最も保護された領域
リング番号1: それより重要でないもの
リング番号2: ……
リング番号3: ユーザプログラム

6

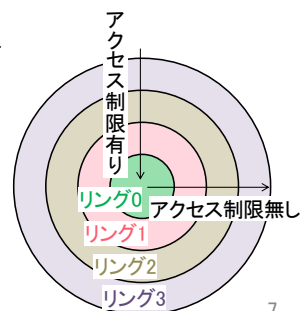
リング保護方式による記憶保護

・カレントリングレジスタ

中央処理装置上にあり、現在実行中のプロセッサセグメントのリング番号を保持。

◆カレントリングレジスタ

アクセス先セグメントのリング番号
制限子(R,W,E,A)
を使って、リング保護を行う。



リング保護方式による記憶保護

制限子	コード	内容
Read	R	データ/プロセッサセグメントの内容の読取り
Execute	E	プロセッサセグメントの実行
Write	W	データ/プロセッサセグメントの内容の書換え
Append	A	データセグメントに内容の追加

カレントリングレジスタ

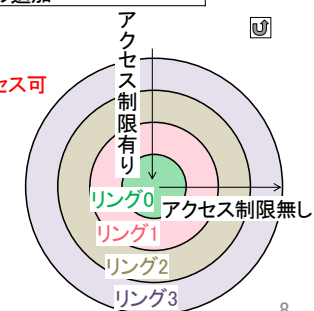
< アクセス先のセグメントのリング番号
…R, W, E, Aの制限をうけずに、**アクセス可**

カレントリングレジスタ

= アクセス先のセグメントのリング番号
…**R, W, E, A許可**の制限に従う

カレントリングレジスタ

> アクセス先のセグメントのリング番号
…**R許可**がある場合だけ、読める。



多重仮想記憶方式(MVS)および セグメンテーション方式での記憶保護


- 各プログラム(ユーザ)の仮想記憶空間は**独立**。



ある仮想記憶空間で実行されているプログラムから
他の仮想記憶空間のプログラムやデータは直接アクセスできない。

9

アクセスマトリックスによる記憶保護

- プログラム、データ、ファイルをアクセスする際に、
アクセス側のプログラム…**主体(subject)**
アクセスされる側のプログラム、データ、ファイル…**客体(object)**
- 主体が客体をアクセスする際の参照**R**・更新**W**・実行**E**の権限を表にしてプログラム、データおよびファイルを保護
- この表を**アクセスマトリックス(access matrix)**、**アクセスリスト(access list)**、**資格リスト(capability list)**とよぶ。 

	o1	o2	o3	o4
s1	R		RW	E
s2			RW	
s3		RW		
s4			R	

si : 主体(アクセス側のプログラム)

oi : 客体(アクセスされる側のプログラム、データまたはファイル)

R: 読出権限

W: 書込権限

E: 実行権限

空白: 禁止

10

演習-記憶保護

- 記憶保護方式に関し、次の問に答えよ。
 - キー方式による記憶保護を説明せよ。
 - リング保護方式による記憶保護を説明せよ。
- モード制御機能による記憶保護では、
2つのモードをとる。それらを説明せよ。

11