

第8回 保護とセキュリティ(1)

入出力保護, アクセス制御

コンピュータシステムに対する脅威

- 災害: 天災(地震・洪水)、人災(テロ・戦争)
- 故障: 停電、ハードウェア故障、ソフトウェア故障(バグ等)
- 操作ミス(偶発的な人為災害)
- 故意の人為災害(特に、これが厄介)
 - 不法侵入、盗聴
 - 不法アクセス
 - 不正プログラム、不正トラフィック
- **保護**(protection): 誤り(内部的な脅威)への対処
 - 信頼性、可用性などOSの機能が重要な役割
- **セキュリティ**(security)^(注): 故意による安全性への脅威への対処
 - 運用方法やアプリケーションを含めた対応が必要

注: 機密保護とも訳されるが、意味が狭いため、近年は、カタカナで呼ばれる。
用法に注意(「セキュリティ対策」とは言わない)

安全性に関する特性

p.166,167

- 信頼性(reliability): システムが故障せずに動く
 - ハードウェア故障、ソフトウェア故障＝バグによる誤った動作
 - 信頼性向上: ハードウェア+OSを含めたソフトウェア
- 可用性(availability): システムが機能を維持し続ける
 - 冗長系による故障時の切り替え
 - 無停電電源装置(UPS)による停電時の動作維持
- セキュリティ(security): システムの安全を確保する(保安)
 - 侵入、不正使用、情報の窃盗・改ざん、破壊などへの対処
- 完全性(integrity): システムに欠陥が無く、意図どおりに機能する
 - セキュリティの問題を生じる安全性の欠陥: セキュリティホール

保護の目的と割り込み

- 多重プログラミング: 複数の利用者によるコンピュータの共用
 - コンピュータの使用率が改善される反面、
 - 1つのプログラムのバグが多くのプログラムに影響
 - 他人のカード(データ)を自分のものとして入力
 - 他のプログラムのデータを変更、OSのデータさえも変更
- 不正なプログラムから、OS自身、他のプログラム、データを保護
 - 他のプログラムの誤動作を引き起こさないことを保障
- プログラムの誤りの多くは、

割り込みが重要な役割

 - ハードウェアによって検出され、
 - OSによって処理される
- **外部割り込み**: **ハードウェアに起因**する割り込み
 - ハードウェアの故障・エラー、入出力完了、時計(タイマ)
- **内部割り込み**: **プログラムの実行が原因**で発生する割り込み
 - 不正命令、メモリ保護違反、システムコール

オペレーティングシステム(OS)の起動

基礎OSのスライド

- OS(正確にはカーネル)は**イベント駆動**^(注)プログラムである
 - 何かが起こるのを待つ
 - マウスのクリック、文字の入力、印刷の終了、メモリのエラー、...
- ハードウェアがイベントを検出し、**割り込み**によりOS(カーネル)を起動
 - そのとき実行していたプログラムを中断し、OS(カーネル)の特定番地にジャンプ
 - このように、**OS(カーネル)は、割り込みによってのみ起動される**
- 割り込みの種類
 - **外部割り込み**(external interrupt)
 - ハードウェア割り込み(hardware interrupt)とも呼ばれる
 - **内部割り込み**(internal interrupt)
 - ソフトウェア割り込み(software interrupt)とも呼ばれる
 - 外部割り込みを「割り込み」、内部割り込みを「**割り出し**(trap)」と言う人もいる
- 注: イベント(event: 事象)＝出来事

外部割り込み

基礎OSのスライド

- 直接的にはプログラムの実行に起因しない割り込み(**ハードウェアに起因**する割り込み)
- 外部割り込みの種類
 - マシンチェック割り込み
 - ハードウェアの故障
 - メモリの読み出しエラー(パリティチェックエラー)など
 - 入出力割り込み
 - 入出力装置からの**動作終了**通知
 - 異常通知など
 - 時計(タイマ)割り込み

基礎OSのスライド

内部割り込み

- プログラムの実行が原因で発生する割り込み
- 内部割り込みの種類
 - プログラムの誤り
 - 演算例外 (ゼロ除算, オーバフロー)
 - 不正命令違反 (定義されていない命令コードの使用)
 - メモリ保護違反 (許可されていないメモリ領域へのアクセス)
 - 仮想記憶におけるページフォルトもこの一種
 - システムによっては、ページフォルト専用の割り込み番号を持つもの有り
 - システムコール
 - その他 (デバッグ用、エラー解析用など)

実行モードとCPU保護

- 非特権モード (ユーザーモード)
 - 一般のAPを実行するモード。特権命令は実行不可
- 特権モード (カーネルモード)
 - OSのカーネルを実行するモード。特権命令も実行可能
- 特権命令
 - 入出力命令 (入出力保護に関連)
 - 記憶管理レジスタ変更命令 (記憶保護に関連)
 - タイマ起動、停止、タイマ値変更命令 (CPU保護に関連)
 - プログラムの実行制御のために用意された特別な命令
 - 割り込み禁止命令、割り込み禁止解除命令
 - 実行モード切替命令
 - HALT命令 (CPUを停止させる命令)
- CPU保護: 特定のAPIによるCPUの独占 (無限ループ) に対する保護
 - APを実行中とする時にタイマを設定 (タイマ値 > 量子時間)。
 - CPUバーストが続けば、無限ループと判断。

入出力保護

- 入出力保護: 入出力誤りに対する保護
 - 入出力誤りの例
 - 他人のデータを自分のものとして入力
 - 割り当てエリアをオーバーした出力
 - 保護の方法
 - 装置ドライバをOSが準備し、入出力要求の正当性を検査
- APのプログラムに対し、強制的に装置ドライバを使用させる必要がある
 - 入出力命令を特権命令とする (APは入出力命令を使用不可)
 - APが入出力命令を実行すると不正命令の内部割り込み
 - (APは非特権モードで実行するため)
 - 入出力要求のシステムコールを提供する
 - OS (装置ドライバ) が起動され、特権モードで入出力命令実行

重要: 入出力保護の実現(1)

入力装置

APのプロセス(P1)が特権命令を直接実行するとエラーとなる

内部割り込みによりOSに制御が渡る
割り込み分析の結果 (不正命令)、OSは利用者プログラムを終了させ、エラー処理 (その後、他のプログラムを実行させる)

● システムコール
● 特権命令

重要: 入出力保護の実現(2)

APのプロセス(P1)が入出力要求のシステムコールを発行

内部割り込みによりOSに制御が渡る
割り込み分析の結果 (システムコール)、OSはプロセスP1を待機中にし、特権命令を実行 (OSの実行は特権モードで行われるので、エラーとはならない)
入力が終わると、外部割り込み (入出力完了) によりOSに制御が渡る
割り込み分析の結果、プロセスP1をレディ状態にする (P2が終わればP1が実行)

主記憶保護

OSのデータやプログラムは極めて重要である

OSのプログラム、データを利用者プログラムから保護
誤動作してもOSを変更できないように

実行中のプロセスの前後の記憶空間を保護
上限レジスタ、下限レジスタ (OSが特権命令で設定)
実行中プロセスの上下限アドレスを設定

ジョブ1
ジョブ2
ジョブ3

上限レジスタ
下限レジスタ

