

仮想という考え方

総合科目「ネットワーク社会を支える情報技術入門 II」、2015年12月07日

筑波大学システム情報系
新城 靖
<yas @ cs.tsukuba.ac.jp>

このページは、次の URL にあります。

<http://www.softlab.cs.tsukuba.ac.jp/~yas/gen/it-2015-12-07>

あるいは、次のページから手繰っていくこともできます。

<http://www.softlab.cs.tsukuba.ac.jp/~yas/gen/>

<http://www.cs.tsukuba.ac.jp/~yas/>

印刷配布資料 <http://www.softlab.cs.tsukuba.ac.jp/~yas/gen/it-2015-12-07/it-2015-12-07.pdf>

■今日の重要な話

- 「仮想(virtual)」という考え方は、コンピュータとネットワークの技術に伴い生じた考え方である。
- 「仮想」の一義的な意味は、「現物と置き換え可能なもの」の意味である。「実体がない」という意味ではない。日本語訳、漢字の語感に感わされな ないこと。
- 重要な「仮想」がつく概念
 - 仮想記憶(virtual memory)
 - 仮想計算機(virtual machine)
 - 仮想専用線(virtual private network)
- 仮想計算機には、様々な利用方法がある。
- オペレーティング・システムの誕生と「プロセス」の考え方の発明で、仮想化が始まった。

■仮想とは

◆コンピュータ由来の「仮想」の意味

英語では、virtual。

- ソフトウェアの働きで作られている。
- 現実のもの(ハードウェア)と置き換え可能である。仮に取り替えても、(ある範囲では)利用している側には気がつかれない。

類語：抽象(abstract)、論理(logical) (←→物理(physical))

反語：実(real)

◆英語のvirtualの説明

virtual (adjective)

almost or nearly as described, but not completely or according to strict definition : *the virtual absence of border controls.*

- **Computing** not physically existing as such but made by software to appear to do so : a virtual computer. See also virtual reality .
- **Optics** relating to the points at which rays would meet if produced backward.
- **Physics** denoting particles or interactions with extremely short lifetimes and (owing to the uncertainty principle) indefinitely great energies, postulated as intermediates in some processes.

Thesaurus (類語)

1. *a virtual guarantee* effective, in effect, near, near enough, essential, practical, to all intents and purposes.
2. *a virtual shopping environment* simulated, artificial, imitation, make-believe; computer-generated, online, virtual reality.

MacOSX付属 New Oxford American Dictionary, New Oxford Writers Thesaurus より。

◆英和辞典

virtual (形容詞)

《表面的にはまたは名目上はそうでないが》事実上の、実質上の、実際(上)の; 仮想の、バーチャルな;

- 【光】 虚像の (opp. real)
- 【理】 仮想の《遷移の中間状態として現われ直接検出にかからない; opp. real》
- 【電算】 仮想記憶 (virtual memory) の[を用いる];
- 《古》 実効のある。

リーダーズ英和辞典第2版より。

◆日本語の辞書に現れる「仮想」

この講義で中心的に扱う「仮想の考え方」とは、適合しない。virtual の訳語に「仮想」を当てたのは、失敗だった。「事実上の」と訳せば良かった。

仮想 (広辞苑)

仮に考えること。仮に想定すること。例：仮想敵国。

仮想敵国の英語は、[hypothetical、imagined、potential] enemy。virtual enemy とは言わない。

■仮想記憶 (virtual storage,仮想メモリ,virtual memory)

コンピュータのメモリをうまくつかうための仕組み。

◆(物理的な)メモリ

コンピュータには、2種類の記憶のためのハードウェア部品が含まれている。

メモリ(メインメモリ)、RAM(Random Access Memory)

実行中のプログラムを保持する。加工するデータを一時的に保持する。

IC (Integrated Circuit、シリコンという元素による半導体で作られた電気回路)で作られているので、速い。容量は、ハードディスクよりは小さい。値段が高い。(揮発的(電源を切ると消えてしまう)。)

ハード・ディスク (HD(Hard Disk), HDD(Hard Disk Drive))

プログラムやデータをデータを保持する。容量は、メモリより大きい。値段が安い。(永続的である(電源を切っても残っている)。)

メモリには、数字で番地(アドレス)が付いている。番地を指定して、データを保存する。番地を指定すると、データが取り出せる。

◆仮想記憶(仮想メモリ)

仮想記憶(仮想メモリ、virtual memory)とは、[オペレーティングシステム\(後述\)](#)の動きにより、実際に備えているメモリ容量よりも大きなプログラムを動かすための仕組みである。

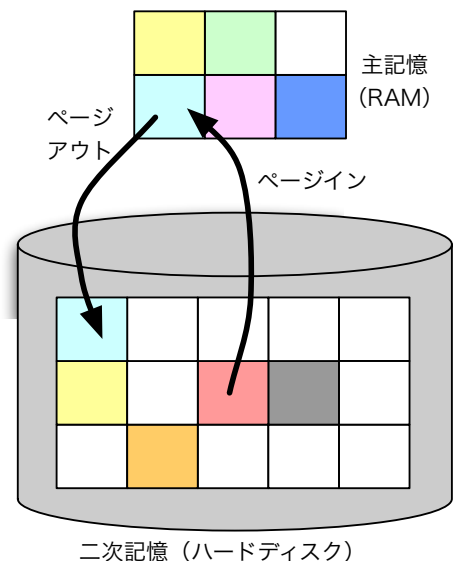


図 仮想記憶による主記憶容量の拡大。主記憶よりも、「事実上」多くのメモリがあるように見せかける。

主記憶 (main memory, primary storage)

RAMで作る。小容量、高価。

二次記憶(secondary storage)

ハードディスクで作る。大容量、安価。

ページ

主記憶と二次記憶(ハードディスク)を固定長のブロックに分けたもの。大きさは、4Kバイト-8Kバイトが一般的。

ページアウト

主記憶にある(当分使いそうにない)ページを、二次記憶へコピーする。

ページイン

二次記憶にある(現在必要とされている)ページを、主記憶へコピーする。

仮想記憶の基本的なアイデアは、高価なRAMの容量を、安価なハードディスクを使って、「事実上」拡大する。すぐに使うところだけを速いメモリ(IC)に、当分使わない所を、遅いハードディスクに置き、ディスクとメモリの内容を入れ替えながら仕事を進める。この時、速いメモリを主記憶、遅いハードディスクを二次記憶とす。

仮想記憶を使うと、メモリが1000Mバイトしかないコンピュータで、2000Mバイトのメモリを使うプログラムを実行することができるようになる。

もともとは、1つのプログラムで実際のメモリ容量以上のものを使うための仕組みである。最近では、複数のプログラムが使うメモリの総量で考えることもある。

◆要求ページング

要求ページング(demand paging)は、仮想記憶を実現するための技術。

- 主記憶には、最初は何にも入れない
- プログラムが実行して、あるページをアクセスした時に、主記憶になければ、プログラムの実行を一旦中断する。目的のページを、二次記憶から主記憶へページインして、実行を再開する。

特徴

- アクセスされないページは、主記憶には入らない。
- 無駄な二次記憶から主記憶へのコピーは発生しない。
- 存在しないページをアクセスした時に「中断」と「再開」が行われるので、その分遅くなることもある。

◆ページ置き換えアルゴリズム

ページインしようとした時に、全部の主記憶が利用中ということがある。この時には、利用中のページの中から、犠牲となるページを選択してページアウトし、空きを確保する。

犠牲となるページを選択する方法(アルゴリズム)には、次のようなものがある。

- OPT(Optimal)アルゴリズム。最も遠い将来まで利用されない部分を二次記憶へ。
- FIFO (First-In First-Out) アルゴリズム。最も早い時刻に読み込まれた部分を二次記憶へ。
- Randomアルゴリズム。ランダムに選んで二次記憶へ。
- LRU((Least Recently Used))アルゴリズム。最も長い時間参照されていない部分を二次記憶へ。

一番よいアルゴリズムは、OPTアルゴリズムだが、実現不可能である。未来の情報を使うので。LRUは、過去の情報を使って未来を予測する方法。

アルゴリズム(手法、算法)とは、問題を解くためのあらかじめ記述された定義の明確な規則、あるいは、指示の集まり。日本語などで書くこともできる。直接的にはコンピュータでは実行できない。なんらかの方法で実行できるようになったものは、プログラムである。

◆「超整理法」押し出しファイリング

野口悠紀雄(のぐち ゆきお)氏が提唱した、紙のファイルを整理する方法[1]。この手法は、LRUアルゴリズムと同じ。

- 書類を、紙のファイル(封筒)に入れ、整理棚に並べる。木構造で分類しない。
- ファイルは、最後に利用した日時に並べる。

- ファイルを探す時には、最後に利用したものから順に見る。(木構造で分類するより速く見つかる。)
- ファイルを戻す時には、左端に戻す。(元の場所に戻さない。)
- 整理棚があふれたら、右端(Last Recently Used)のファイルを、棚から外に出す。

[1] 野口 悠紀雄: "「超」整理法 -- 情報検索と発想の新システム", 中央公論社 (1993).

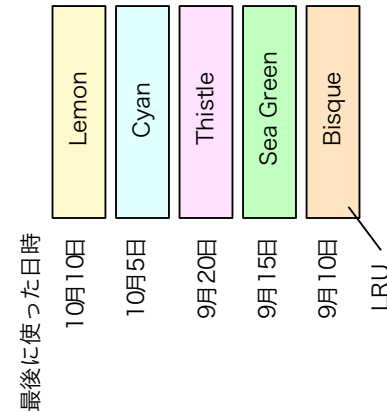


図 超整理法の棚(1): 探す時には、左から見る。

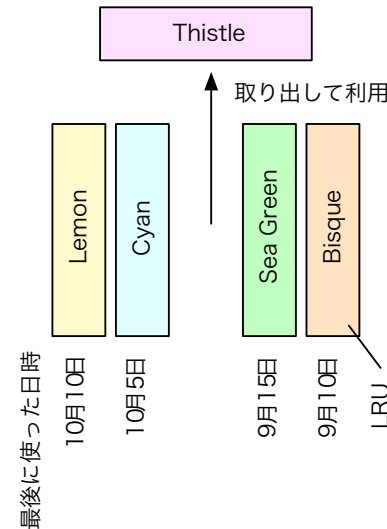


図 超整理法の棚(2): 見つかったファイルを取り出して利用する。

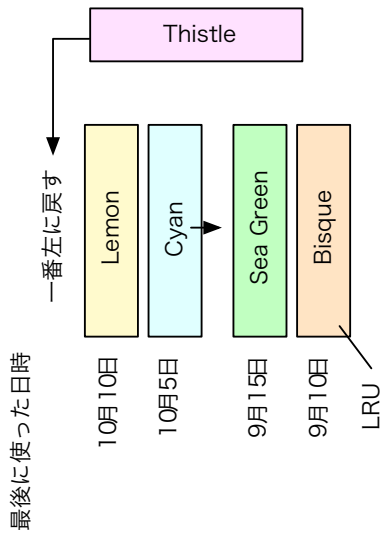


図 超整理法の棚(3): ファイルを棚に戻す時には、左端に戻す。元の場所に戻さない。

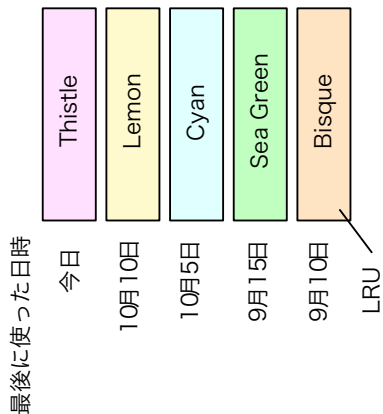


図 超整理法の棚(4): 探す時には、左から見る。

■仮想計算機(virtual machine)

あるいは、仮想マシン、仮想コンピュータ。計算機(専門用語)とは、コンピュータのこと。電卓ではない。

◆コンピュータの構成

- 1セットのハードウェア(実計算機)を1つのオペレーティング・システム(OS)が操作する。
- OS上で複数のアプリケーション・プログラムが動作する。
- ハードウェアには、次のようなものが含まれる。
 - CPU
 - メモリ
 - 周辺装置(ハードディスク、ディスプレイ、キーボード、ネットワーク・カード)

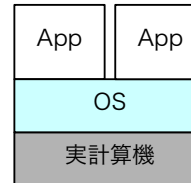


図 単純化したコンピュータの構成

◆仮想計算機

仮想計算機とは、仮想計算機モニタと呼ばれるソフトウェアの働きにより作り出された、事実上のハードウェア。オペレーティング・システムから見ると、実際のハードウェアとは区別がつかない。

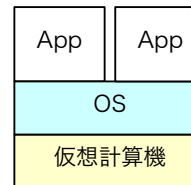


図 仮想計算機上でのオペレーティング・システムの実行

仮想計算機は、仮想計算機モニタ(virtual machine monitor, VMM)という小さなソフトウェアにより実現される。仮想計算機モニタは、ハイパーバイザ(hypervisor)と呼ばれることもある。

仮想計算機モニタは1個でも、複数の仮想計算機を作ることができる。

◆仮想計算機の利用方法

- もともと複数のコンピュータで行っていた仕事を1台の物理的なコンピュータでこなすために集約する。
- 1台のコンピュータで、複数のオペレーティング・システム用の **アプリケーション・プロ**

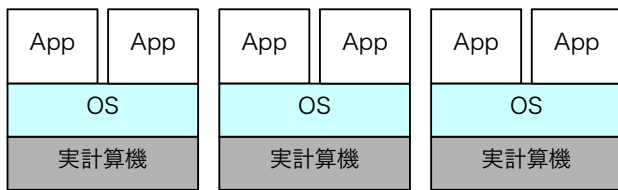
グラムを同時に利用する。

- ハードウェアが故障した時に、簡単に交換できるようにする。
- データのバックアップや、ソフトウェアのインストールを簡単にする。
- クラッシュに強くする。(書き込みを取り消すことができるハードディスクを使う。)
- オペレーティング・システムの開発環境として利用する。
- セキュリティを高める。

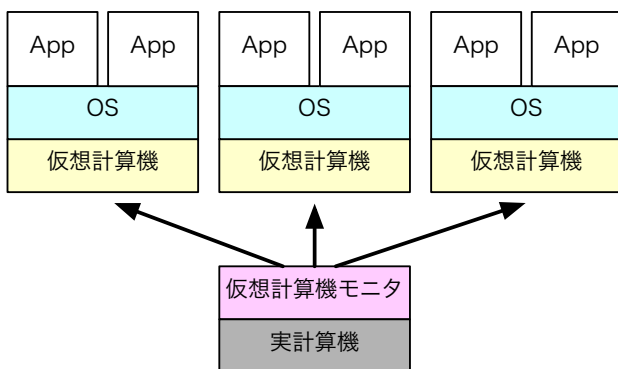
◆コンピュータの集約

目的

- 1970年代: ハードウェアの価格が高い。1つのハードウェアで複数のOSが走れば、ハードウェアを買うお金が節約できる。
- 現在: コンピュータの高速化で、性能が余ってきた。もともとハードウェアn台でやっていた仕事を、ハードウェアとしては1台でこなせるようになってきた。並列処理の逆。



図? 仮想計算機によるサーバの集約(集約前)



図? 仮想計算機によるサーバの集約(集約後)

◆ハイパーバイザ型とホスト型

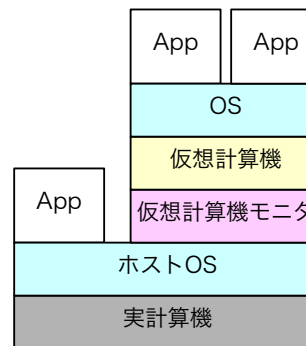
仮想計算機モニタの分類

ハイパーバイザ型

実計算機上で仮想計算機モニタが動作する。

ホスト型

実計算機上では普通のオペレーティング・システムが動作する。仮想計算機モニタは、そのオペレーティング・システムの1つのアプリケーションとして動作する。



図? ホスト型仮想計算機モニタ

◆仮想計算機モニタの実例紹介

VMware Fusionは、MacOSX上で動くホスト型の仮想計算機モニタ製品。デモでは、次のOSを実行する。

- Windows
- Linux
- MacOSX

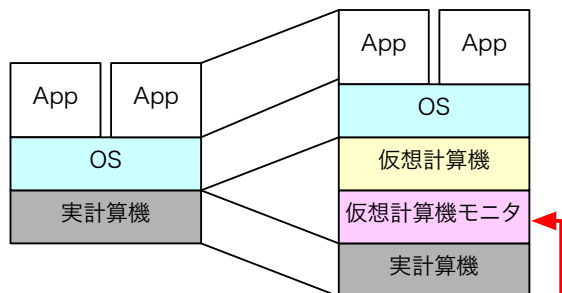
◆セキュアVM/BitVisor

日本政府が決定した「セキュア・ジャパン2006」の項目の1つ。内閣官房情報セキュリティセンターが推進する。文部科学省2006年度科学技術振興調整費「高セキュリティ機能を実現する次世代OS環境の開発」による支援を受ける。筑波大学がとりまとめ。電気通信大学、東京工業大学、慶應義塾大学、奈良先端科学技術大学院大学、豊田高専、富士通、NEC、日立製作所、NTT、NTTデータ、ソフトイサーの技術者が参加。インテルが技術協力。2009年3月開発プロジェクト終了。

目標: オペレーティング・システムやアプリケーションに依存しない形でセキュリティ機能を付加する。

- ICカードがないと、オペレーティング・システムが起動しない。盗難にあっても、他人には使われない。
- ハードディスクが自動的に暗号化される。ハードディスクのが取り出されても、情報漏えいが発生しない。
- 強制的に [仮想プライベート・ネットワーク \(後述\)](#) に参加させ、ネットワーク通信を暗号化すると共に、利用可能なネットワークを制限する。

既存のオペレーティング・システム(Windows, Linux 等)を変更しないで実行する。このために、仮想計算機 (モニタ) で、セキュリティ機能を追加する。



セキュリティ機能の追加

- ICカードによる利用者認証と起動制御
- ハードディスクの暗号化
- ネットワーク通信の暗号化

図? BitVisor の機能



図? BitVisor の起動画面

<http://www.bitvisor.org/> <http://www.securevm.org/>

◆エミュレータとシミュレータ

エミュレータ

別のシステムで、本物のシステムと同じ動きを真似するソフトウェア。本物は、必ずしもコンピュータ全体 (計算機) でなくてもよい。

- Wine: Unix 上で Windows 用のプログラムを実行するためのプログラム。Wine は、Windows のソフトウェア部分(システム・コールと実行時プログラム)をエミュレートする。
- 端末エミュレータ: [文字端末](#) の機能を全部、または、部分的にエミュレートする。
- 仮想計算機: コンピュータ全体のエミュレータ。

シミュレータ

現実世界の予測に使うもの。数式でモデル化して計算で予測する。実際にやるとコストがかかるもの、取り返しがつかないものをコンピュータの中で実行する。現実の代わりにはならない。(エミュレータは、本物の代わりに使える。シミュレータは、本物の代わりには使えない。)

- フライト・シミュレータ
- 地球シミュレータ

(文字)端末

1 台の (高価な) 中央のコンピュータを、複数人で TSS (Time Sharing System) で使う時に使う (安価な) コンピュータ。キーボードから打ち込まれた文字を中央のコンピュータに送る機能と、中央のコンピュータから送られてきた文字を画面に表示する機能がある。

◆Java仮想計算機

Java 言語で書かれたプログラム (バイトコードと呼ばれる機械語の一種に変換されたもの) を実行する。

Java仮想計算機を使うと、さまざまな種類ハードウェア(CPU)やオペレーティング・システムで共通にバイトコードという機械語が使えるようになる。バイト・コードに変換されたアプリケーションは、どの CPUやオペレーティング・システムでも動作する。

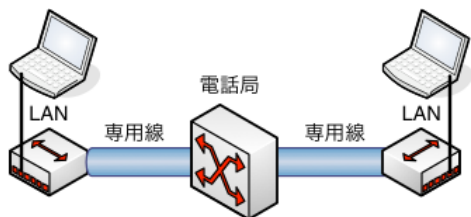
バイトコード	バイトコード	バイトコード	バイトコード
Java仮想計算機	Java仮想計算機	Java仮想計算機	Java仮想計算機
Linux	MacOSX	Windows	Solaris
x86	PowerPC	x86	SPARC

図? 共通のバイトコードが使える

■仮想専用線

◆専用線(Private Network)

(仮想がつかない)専用線サービスとは、NTT等の通信事業者から自分専用の通信回線を借りること。料金は、通信帯域と距離で決まる。(普通の電話の料金は、時間で決まる。)他の人が入り込むことはないので、安全である(通信を傍受するには、電話並に難しい。)



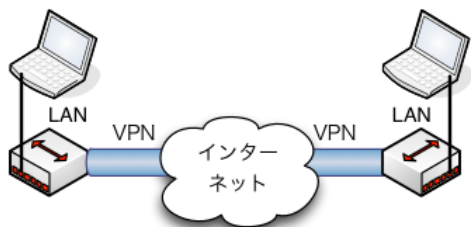
図? 専用線

専用線サービスは、非常に高価。例。

- NTT デジタルアクセス 64 K bit/s, 15km 以内, 月額 28,000円～
- NTT デジタルアクセス 1.6 M bit/s, 15km 以内, 月額 152,000円～

◆VPN(Virtual Private Network)

本当は、インターネットという、誰もがアクセスできるネットワークを通っているが、あたかも専用線(private network)で結ばれているように見せかける。



図? VPN

VPNを実現する技術:

- PPTP
- L2PT over IPsec

- SoftEther VPN <http://www.softether.org/>, Packetix VPN, UT-VPN <http://utvpn.tsukuba.ac.jp/>
- OpenVPN
- MS-SSTP

筑波大学では、学外から学内(IPアドレスで制限)のサービスを利用するために使える。

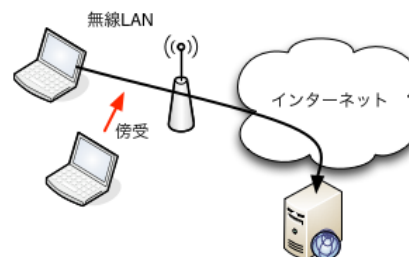
- 学術情報メディアセンター VPN サービス <http://campus-vpn.cc.tsukuba.ac.jp/ja/>
- 情報科学類 <http://www.coins.tsukuba.ac.jp/ce/> (手引きの中)

◆VPNと無線LAN

無線LANを使う時、電波で発せられたデータは、周りのPCで受信可能である。無線LAN部分の暗号化の有無に注意する。

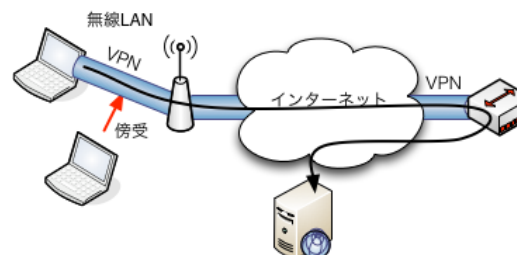
- 暗号化なし。接続する時に、パスワードを聞かれないもの。
- 標準的な暗号化あり。WPA, WPA2 など。
- 弱い暗号化。WEP など。

暗号化なし(パスワードなし)のものは、電波が届く範囲で通信内容を傍受される。



図? 無線LANの通信傍受

無線LANの通信内容の傍受を防ぐには、VPNを使って暗号化すると良い。傍受している人は、暗号化されたデータと、VPNの接続先を知ることができる。暗号化前のデータを入手することは難しい。



図? 無線LANの通信傍受

注意1: VPNの接続先を隠すことはできない。

注意2: VPN の接続先で、暗号化された通信内容は、復号される（元にもどされる）。VPN の接続先と、本来の接続先間の通信にも気を使う必要がある。

◆無線LAN利用時のHTTPSとDNS

Web ページの URL で、http: で始まるものは、通信路が暗号化されていない。https: で始まるものは、通信路が暗号化されている。https: の通信は、暗号化されていない無線 LAN であったとしても、通信内容の傍受は難しい。

しかし、https: の通信の前に、[DNS](#) のアクセスがなされる。DNS のアクセスは、暗号化されていない。無線 LAN が暗号化されていなければ、アクセスしたサーバの名前が傍受される。

VPN を使えば、(設定により) DNS の部分も暗号化できる。

■その他の仮想技術

◆仮想ディスク(virtual disk)

1つの大きなファイルを、1つのハードディスクと同じように扱えるようにしたもの。仮想ディスクを使うと、次のようなことができる。

- データを暗号化して保存する。
- 複数のファイルからなるソフトウェアを1まとめにする。
- CD-R などに書き込むためのファイルを一時的に蓄える。

◆仮想ホスト(virtual host)

ネットワークに接続されたコンピュータをホストという。ホストは、サービスを提供するプログラム(サーバ)を動作とせるという意味もある。

仮想ホストは、本来なら複数のコンピュータが必要であったものを、1台に集約する。ただし、ネットワークを超えて向こう側を見た時には、1台に集約されていることには気がつかせない。

仮想ホストの実現方法

- 仮想計算機を使う
- 個々のプログラムで対応する。1台のコンピュータで動いている1つのプログラムで、複数のドメイン名に対してサービスを提供する。
 - Web サーバ
 - メール・サーバ

◆仮想現実感(virtual reality)

高度なコンピュータ・グラフィックスやサウンドの技術を使って、実在しないものを(コンピュータの中に)実在しているかのごとく見せかける。

人間が働き掛けると、現実と同じように**応答する**。感覚のフィードバックがある。

◆世俗的な「仮想」

最近の日本語では、コンピュータによる原義を離れて、「現実には存在しない」という意味が使われることがある。以前は、空間(と時間)の制約で実現できなかったことが、コンピュータとネットワークの発達により、現実に近いレベルにまで達してきた(部分的に現実のものと同じ置き換え可能になってきた)という意味も生じてきている。

- 仮想都市、仮想社会
- 仮想大学、仮想教官、仮想学生
- . . .

■オペレーティング・システム

◆オペレーティング・システム (Operating System,OS) とは

- 基本ソフトウェア(プログラム)。
- 電源を入れて、使えるようになった時に動いているプログラム。(オペレーティング・システム以外のプログラムは、すべてオペレーティング・システムの働きで実行される。)
- コンピュータの「顔」を作る。基本的な考え方と操作方法とを決める。同じハードウェアでも、違うオペレーティング・システムが動くと、考え方も操作方法も違う。
- ソフトウェアにより、基本的なもの(幻影、オブジェクト)を提供する。
 - ファイルとディレクトリ
 - プロセス
 - ウィンドウ、アイコン
- 管理職。ハードウェアを管理する。メモリ管理、CPU管理。

◆オペレーティング・システムのメモリへの読み込みと実行

徒然草(つれづれぐさ)。八になりし年。最初の仏問題。

OSは、他のプログラムを実行するプログラムである。他のプログラムは、OSの力を借りてはじめて実行される。

ではOSは、誰が実行するか？

BIOSがブートローダをメモリに読み込み、ブートローダを実行する。

ブートローダがOSをメモリに読み込み、OSを実行する。

BIOS(Basic Input Output System)、ROM Monitor。OSをハードディスクからメモリにコピーして、OSに制御を渡すプログラム。ROM (Read-Only Memory) という、少容量の不揮発的なメモリに入っている。古いシステムでは、(フロッピーディスクへの) 基本的な入出力の機能が含まれていた。

◆オペレーティング・システムの種類

- Unix, Linux
- MacOS 9/X
- Microsoft Windows 95/98/2000/NT/XP/Vista/7/8
- MS-DOS
- iOS, Android, Symbian OS, iTron

ソフトウェアを買う時、自分のパソコンのOSで動作するものを買う。(CPUの種類も大事。同じOSでもCPUの種類がプログラムは違うと動作しない。)

自分が使いたいソフトウェアが動作するようなOSとCPUを積んだパソコンを買う。

◆歴史

- ローダ(Loader)
- モニタ(Monitor)
- バッチ処理OS
- TSS (Time Sharing System)OS
- ワークステーション用OS
- パソコン用OS
- ネットワークOS, 分散OS, 実時間OS

「パーソナル・コンピュータ」の考え方は、比較的新しい。昔は、コンピュータが高価だったので、1台のコンピュータを複数人(時には数百人)で同時に使うことが一般的だった。

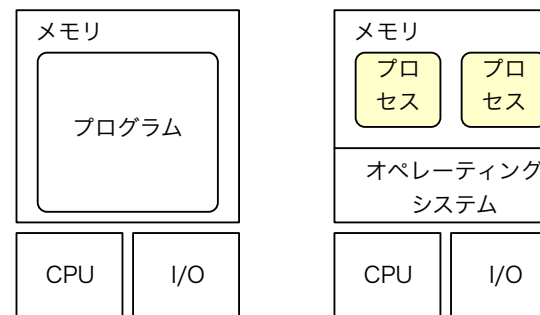
TSS (Time Sharing System)では、1台のコンピュータを大勢の人で同時に使う、一人ひとり、自分で占有しているかのように見える。

◆プロセス

プログラムとプロセス。

プロセスとは、オペレーティング・システムの働きにより、二次記憶に保存されていたプログラムがメモリ(主記憶)に読み込まれ、実行可能になったもの。

単にファイル(ハードディスク)に入っても、プログラムはプログラムである。1つのプログラムを同時に2個動かすことを考えると、プログラムとプロセスの違いがわかる。



1つのプログラムだけが動作しているコンピュータ

複数のプロセスが動作しているコンピュータ

図? オペレーティング・システムの構成要素

1つのプロセスから見ると、普段は自分一人で全部のコンピュータのハードウェアを利用しているように見える。コンピュータの仮想化の最初。

プロセスは、時々、他のプロセスからデータを受け取る(プロセス間通信)。

Last updated: 2015/12/04 16:34:32

[Yasushi Shinjo](mailto:yasushi@cs.tsukuba.ac.jp) / <yas@cs.tsukuba.ac.jp>