

仮想化講座

■ e-learningの目的

- ・ 講義・演習を始める前に、仮想化という概念や基礎的な用語について学ぶことを目的としています。演習を円滑かつ効果的に進めていくためにも、本e-learningで基礎知識をしっかりと構築していきましょう。

■ 講義・演習を始める前の基礎知識

- ・ 仮想化概要
- ・ 仮想化の構成要素

★第1章：仮想化概要

- 1-1 仮想化とはなにか
- 1-2 仮想化の種類
- 1-3 仮想化製品
- 1-4 サーバ仮想化
- 1-5 デスクトップ仮想化
- 1-6 仮想化とクラウド

★第2章：仮想化概要

- 2-1. ネットワークとは
- 2-2. LAN
- 2-3. WAN
- 2-4. IPアドレス
- 2-5. ネットワーク部とホスト部
- 2-6. IPアドレスのクラス

仮想環境の構成要素

- 2-1 仮想化のコンポーネント
- 2-2 仮想マシン
- 2-3 仮想CPU
- 2-4 仮想メモリ
- 2-5 仮想HBA、仮想ディスク
- 2-6 仮想NIC
- 2-7 仮想スイッチ、仮想ルータ

第1章：仮想化概要

- プロセッサやメモリ、ディスク、通信回線など、コンピュータシステムを構成する資源（リソース）を物理的構成に拠らず柔軟に分割したり統合したりすること
- 1台のサーバコンピュータをあたかも複数台のコンピュータであるかのように論理的に分割し、それぞれに別のOSやアプリケーションソフトを動作させる「サーバ仮想化」や、複数のディスクをあたかも1台のディスクであるかのように扱い、大容量のデータを一括して保存したり耐障害性を高めたりする「ストレージ仮想化」などの技術がある

IT用語辞典より転載

仮想化とは、物理的なハードウェアのリソースを論理的（ソフトウェア的）に分割したり、統合したりする技術全般を指します。

ハードウェアの進歩により、サーバをはじめ様々なハードウェアの持つリソースが高性能、大容量、高速になってきているため、そのリソースをひとつのシステムでは使い切れず、リソースが効率的に使用されている状態とはいえなくなっています。そこで、その物理的なリソースの未使用部分（余剰リソース）を有効活用するために、論理的にリソースを分割し、あたかも複数台のハードウェアを利用しているように見せたり、逆に複数台の物理的リソースを統合して、1台の高性能、大容量、高速なハードウェアを利用しているように見せる技術を指します。

代表的な仮想化技術としてサーバ仮想化があります。サーバ仮想化とは、物理的には1台のサーバの未使用リソースを利用して、あたかも複数台のサーバがあるように見せかけて、異なる複数のOSを走らせたり、ひとつのサーバに処理が集中することを避けるために、処理を分散させ、効率よく処理を進めたりする技術です。そのほか、ストレージ仮想化、デスクトップ仮想化、ネットワーク仮想化などの仮想化技術があります。それぞれの仮想化技術の概要をみていきましょう。

■ 仮想化は次の種類に分けられています。

- サーバ仮想化
- デスクトップ仮想化
- ネットワーク仮想化
- ストレージ仮想化

仮想化の技術は大きく 4 つの種類に分けられます。

[サーバ仮想化]

サーバ仮想化は、前ページでも触れたように 1 台の物理サーバを論理的に分割し、複数台のサーバがあるように見せかけて利用する技術です。論理的に分割された複数台の仮想サーバは、あたかもそれぞれ独立したサーバのように利用することができ、物理サーバに導入されている OS とは別の OS を走らせたり、別のアプリケーションを利用することができます。物理的なサーバの高性能化によってできた余剰リソースを利用して、複数台のサーバを運用していると同様の運用ができるようになります。これによって、メインの物理サーバでは対応できないアプリケーションの運用や、テストなどにも利用することが可能となります。また、論理的に構成されたサーバなので、バックアップを利用して物理的故障に対

しての保全も簡単に行うことができます。

[デスクトップ仮想化]

デスクトップ仮想化は、サーバにおかれたPC環境をPCの利用者が使用する端末に反映させて利用させる技術です。利用者が使用するPCには、アプリケーションやデータが置かれずに、PCからサーバにアクセスしてPCを利用する仕組みとなります。ネットワークに接続する環境があれば、認証を受けた利用者は、いつでも、どこでも、どのPCからでも、アプリケーションやデータを利用することが可能となります。運用サイドの視点からは、アプリケーションやデータがサーバ側にあるために、利用者や利用状況の管理が簡単になるとともに、データも利用者のPCに残らないので、データ流出を未然に防ぐセキュアな環境といえます。利用者サイドの視点からは、いつでも、どこでも、同じ環境でPCを利用できるメリットがあります。

[ネットワーク仮想化]

一般的にネットワーク仮想化とは、SDN (Software-Defined Networking)のことを指している場合が多いですが、正確な定義づけがされているわけではありません。ネットワーク仮想化とは、物理的に構成されたネットワークを分割して利用したり、複数のネットワークを統合することによって、仮想的なネットワークを構成する技術を指します。サーバやストレージなどをネットワーク上で利用する際に、専用のネットワーク仮想化ソフトウェアを利用してネットワークを構成することによって、従来の有線ネットワークや無線ネットワークのように物理的な作業をすることなくソフトウェア的にネットワークを管理できるようにする技術です。

[ストレージ仮想化]

急激に増加してきている大量のデータを記録するために、物理的な記憶媒体を追加するのではなく、既存の複数のストレージをソフトウェア的に統合し、あたかもひとつの巨大なストレージのように見せかけ、データを保存する技術です。複数のシステムで別個に利用されているそれぞれのストレージでは、容量の足りないものと、容量の余ってしまうものが出てきます。容量の足りなくなったストレージに対して、新たに物理的なストレージを増設するのではなく、ソフトウェア的に足りないストレージと余っているストレージを統合して、巨大なストレージを仮想的につくることによって、効率的にストレージを利用することができます。

■ 代表的な製品（ハイパーバイザ）

• サーバ仮想化 (Type-I)

VMware Sphere

Microsoft Hyper-V

Xen

• デスクトップ仮想化 (Type-II)

VMware Workstation, Player, Fusion

Microsoft Hyper-V

Virtual Box

ハイパーバイザとは、物理的なサーバやPCなどのハードウェア上に仮想化技術を実行させるための制御プログラム全般のことを指します。それに対して、スーパーバイザという言葉があります。ここでいうスーパーバイザとは、ハードウェアを制御するオペレーティング・システム（OS）のことを指します。

現在、ハイパーバイザは様々なベンダーから提供されていますが、このハイパーバイザには大きく分けて、サーバ仮想化（Type-I）とデスクトップ仮想化（Type-II）の2つのタイプがあります。スライドには、それぞれの代表的な製品を挙げています。サーバ仮想化（Type-I）とは、仮想化が実行されるハードウェア上で直接稼働するタイプの仮想化技術のことを指します。それに対して、デスクトップ仮想化（Type-II）とは、ハードウェアを制御しているOS上で稼働するタイプの仮想化技術を指します。

それぞれの特徴を次のページからみていきましょう。

■ Type-I型、ネイティブ型、ベアメタル型

- ハードウェア上で直接動作するハイパーバイザ
- OSはすべてハイパーバイザ上で動作し、ほぼネイティブ環境に近い動作速度が得られる



Type-Iのハイパーバイザの特徴は、ハードウェアに直接インストールし、仮想環境を稼働させるところにあります。ホストOSを介せずに直接仮想環境からハードウェアを制御することが可能なため、ハードウェアの能力を有効に利用することができます。狭義では、ハイパーバイザとはこのType-I型のハイパーバイザのことを指します。

■ Type-II型、ホストOS型

- ハードウェア上にまずOSが動作し、その上で1アプリケーションとしてハイパーバイザが動作



Type-II型のハイパーバイザは、ハードウェアを制御しているOS上のアプリケーションとしてハイパーバイザを稼働させるタイプを指します。ハードウェアを制御しているOSをホスト、ハイパーバイザ上で稼働している仮想環境上のOSをゲストと呼ぶこともあります。このタイプの特徴は、すでに稼働しているハードウェアとOSにインストールすることも可能なので、手軽に導入することができる反面、ゲストOSからのハードウェア制御には、ホストOSの経由が必要なため、余分な負荷がかかり、ハードウェアの持つ本来の性能を十分に利用できない場合があります。

■ クラウドサービスでは仮想化環境を提供

- ・ クラウドサービスはユーザが自由にリソースを変更可能。ニーズにマッチした仮想化環境が利用できる

	suse-sles-12-sp3-v20171212-hvm-ssd-x86_64 - ami-8368cefb SUSE Linux Enterprise Server 12 SP3 (HVM, 64-bit, SSD-Backed) ルートデバイスタイプ: ebs 仮想化タイプ: hvm ENA 有効: はい
	RHEL-7.4_HVM_GA-20170808-x86_64-2-Hourly2-GP2 - ami-9fa343e7 Provided by Red Hat, Inc. ルートデバイスタイプ: ebs 仮想化タイプ: hvm ENA 有効: はい
	ubuntu/images/hvm-ssd/ubuntu-xenial-16.04-amd64-server-20171121.1 - ami-0def3275 Canonical, Ubuntu, 16.04 LTS, amd64 xenial image build on 2017-11-21 ルートデバイスタイプ: ebs 仮想化タイプ: hvm ENA 有効: はい
	Windows_Server-2016-English-Full-Base-2017.11.29 - ami-f6d8008e Microsoft Windows Server 2016 with Desktop Experience Locale English AMI provided by Amazon ルートデバイスタイプ: ebs 仮想化タイプ: hvm ENA 有効: はい

クラウドサービスとは、利用者が手元の端末からネットワーク経由でデータやアプリケーションを利用するサービスの総称で、クラウドサービスを利用するための環境が整った端末があれば、いつでも、どこでも、クラウド上の様々なサービスを利用できるメリットがあります。クラウド側のリソースを、利用者が自由に使えるのでニーズにマッチした仮想化環境を構築できます。現時点では主に3つのサービスに分類されています。

SaaS (Software as a Service) : ネットワーク経由でソフトウェアの機能を提供するサービス

PaaS (Platform as a Service) : ネットワーク経由で仮想化されたアプリケーション実行用のプラットフォームを提供するサービス

IaaS (Infrastructure as a Service) : ネットワー

クラウド経由で仮想化されたハードウェアやインフラストラクチャを提供するサービス

図は、Amazonのクラウドサービス「Amazon EC2」でテンプレートとして用意されている仮想マシンの一例です。

第2章 ネットワークの基本

- 仮想化技術を習得する上で最低限の知識

2-1. ネットワークとは

- ネットワークとは、網という意味の英単語。複数の要素が互いに接続された網状の構造体のこと。ネットワークを構成する各要素のことを「ノード」(node)、ノード間の繋がりのことを「リンク」(link)あるいは「エッジ」(edge)と言う。

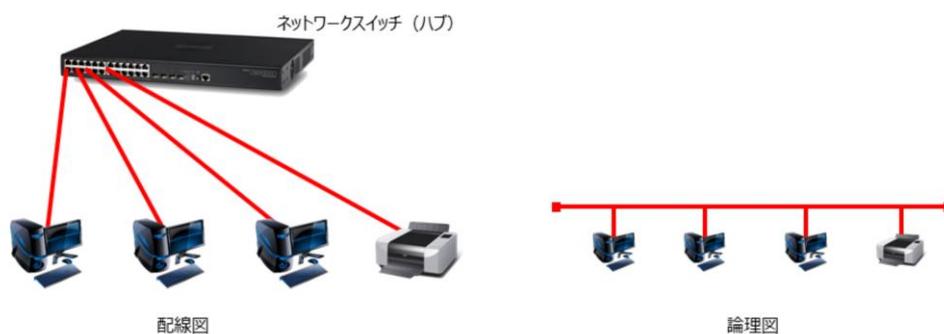
- 一般の外来語としては人間関係の広がりのことや、組織や集団の構造などを指すこともあるが、IT関連の分野で単にネットワークという場合は、複数のコンピュータや電子機器などを繋いで信号やデータ、情報をやりとりすることができるコンピュータネットワークあるいは通信ネットワークのことを意味することが多い。

■ IT用語辞典より転載

2-2. LAN

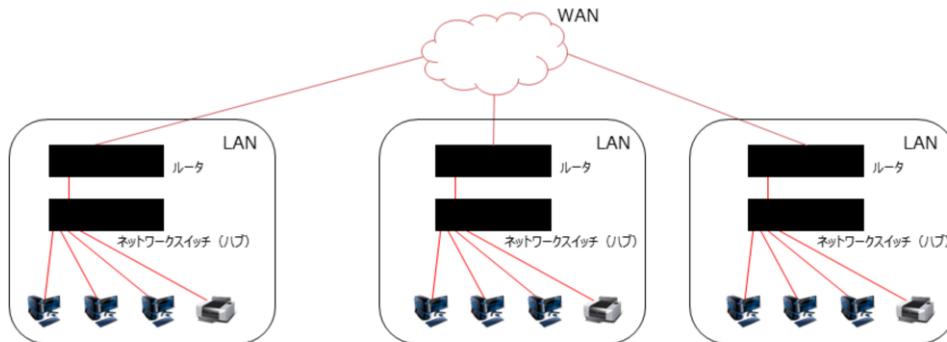
■ LAN (Local Area Network)

- 1つのフロア, 組織, 部署といった, 比較的狭い範囲でのネットワーク



■ WAN (Wide Area Network)

- 広域通信網 (Wide Area Network) の略。
LANとLANを結ぶ公衆網のことを指す場合が多い。
WANを世界規模で実現しているのがインターネット。



2-4. IPアドレス

- ネットワーク上で機器の識別をするための番号
- 32bit でIPアドレスを管理 (IPv4, Internet Protocol Version 4)
 - bit … 情報量の最小単位, 1 or 0
- ネットワーク部とホスト部の存在

192.168.1.10

10進 → 2進に変換

$$192_{(10)} = \boxed{1100\ 0000} \quad (2)$$

$$168_{(10)} = \boxed{1010\ 1000} \quad (2)$$

$$1_{(10)} = \boxed{0000\ 0001} \quad (2)$$

$$10_{(10)} = \boxed{0000\ 1010} \quad (2)$$

192.168.1.10

1100 0000 1010 1000 0000 0001 0000 1010

2進数の並びが $8 \times 4 = 32$ 桁



32bit

※ 8bitのかたまり = 1オクテットと呼ぶことも

octet

192.168.1.10/24

この例だと、IPアドレスのビット列の、

先頭から24bit = ネットワーク部

残りの8bit = ホスト部

1100 0000 1010 1000 0000 0001 0000 1010

24bit : ネットワーク部

8bit : ホスト部

ネットワークプレフィックスと言うことも、
network prefix

ネットワーク内の端末を
識別

端末がどのネットワークに所属しているのかを判別.

ひとつのネットワークに収容できるホスト数

ホスト部がすべて 0 ⇨ ネットワーク自身のことを表す

ホスト部がすべて 1 ⇨ そのネットワーク全体にデータを送る
ブロードキャストアドレスを表す

192.168.1.10 ならば…

ネットワーク自身 ⇨ 192.168.1.0

1100 0000 1010 1000 0000 0001 0000 0000

すべて 0

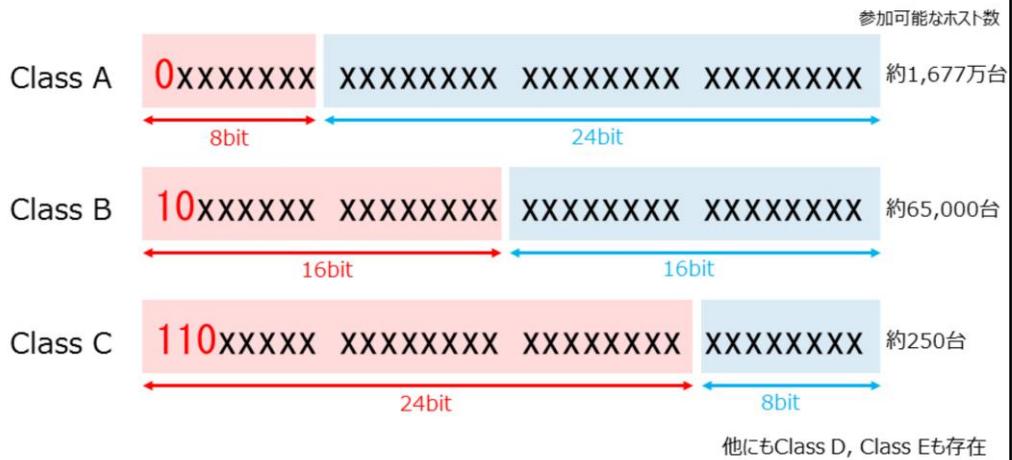
ブロードキャストアドレス ⇨ 192.168.1.255

1100 0000 1010 1000 0000 0001 1111 1111

すべて 1

2-6. IPアドレスのクラス

- 32bit中、「何bitがネットワーク部で、何bitがホスト部を表すか」
- ネットワークの規模を識別する



- (例題) 次のIPアドレスのクラス (ネットワークの規模) は？

172.16.0.1

10進 → 2進に変換

$$172_{(10)} = \boxed{1010\ 1100}_{(2)}$$

先頭ビットが 10… なので, 「クラスB」であることがわかる

第3章：仮想環境の構成要素

■ 主なコンポーネント

- 仮想マシン
- 仮想CPU
- 仮想メモリ
- 仮想HBA
- 仮想ディスク
- 仮想NIC
- 仮想スイッチ

仮想環境を実行するためには、その仮想環境を構成する仮想コンポーネントが必要です。ノートPCを動かすためには、ノートPCを構成しているCPUやメモリ、HDDやSSDのようなストレージ、各種物理スイッチなどのパーツが必要なように、仮想環境でもそれぞれの役割を担ったパーツが必要です。仮想環境を実行するために必要な主なコンポーネントは以下の通りです。

[仮想マシン]

サーバやデスクトップPC、ノートPC、タブレットなど、OSやアプリケーションソフトウェアを動かすために必要なハードウェアの環境を、仮想的にハイパーバイザ上で再現したマシンを指します。ソフトウェア的に再現されたPCと考えると分かりやすいかもしれません。

[仮想CPU]

実際に稼働しているハードウェアとしての物理CPUのリソースを分割し、ハイパーバイザ上で稼働している仮想マシンのCPUとして構成されたものを指します。

[仮想メモリ]

ここでいう仮想メモリとは、物理ハードウェア上で稼働しているOSが利用する物理メモリがリソース不足になった際に利用されるストレージのメモリ化とは異なり、ハイパーバイザが仮想マシンに割り当てて利用するメモリを指します。

[仮想HBA、仮想ディスク]

仮想マシンは、物理ハードウェア上に構成された仮想ディスクをストレージとして利用します。その仮想ディスクと仮想マシンを繋ぐ論理的な接続が仮想HBA（ホストバスアダプタ）です。

[仮想NIC、仮想スイッチ]

仮想マシンがネットワークを利用する場合は、物理ネットワーク機器と仮想マシンを間に仮想ネットワークを構成する必要があります。その仮想ネットワークを構成するには、論理的なNIC(ネットワークインターフェイスカード)が必要となり、論理的ルータ、論理的スイッチを利用します。

仮想マシン

- 物理的なPC、サーバをハイパーバイザによって仮想的な機械に置き換えたもの
- Virtual Machine : VM
- 構成ファイル、仮想ストレージなど構成される

Hyper-Vの例

■ ubuntu 14d	2017/11/29 22:41	ファイル フォルダ	
■ ubuntu 14-desktop.vhdx	2017/12/19 14:29	ハードディスク イメ...	9,441,280 KB

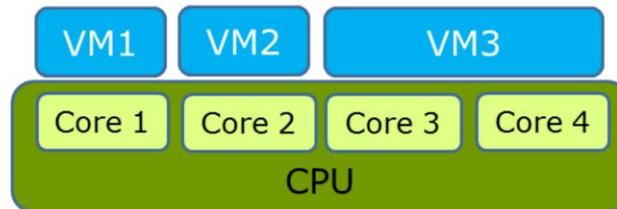


仮想マシン(ハードディスクイメージ)

仮想マシンとは物理的なハードウェア上に論理的に構成された仮想的なコンピュータを指します。一般的にはVirtual Machine（仮想機械）の頭文字をとって「VM」と表します。仮想マシンを構成するコンポーネントをひとまとめにして、ハイパーバイザ上にフォルダやディスクイメージとして保存、活用されます。

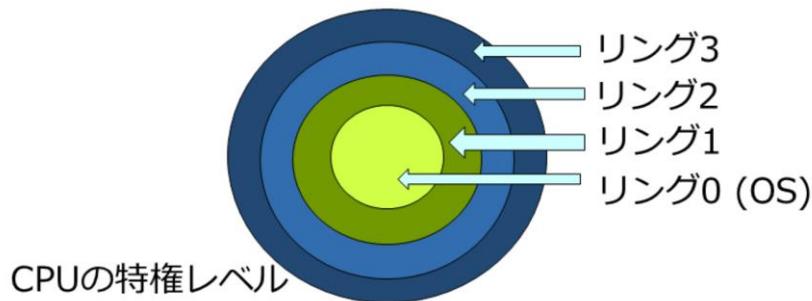
■ 仮想マシンからは仮想CPUが物理CPUとして見える

- 仮想マシン1つにつき1つのCPU、もしくは1つのコアを割り振るのが理想的
- 重い仮想マシン（VM3）には多くのコアを割り振り、軽い仮想マシン（VM1,VM2）には少ないコアを割り振る
- 商用のハイパーバイザの中には、CPUのコア数、仮想CPUの総コア数でライセンスが決まるものもある



CPU（Central Processing Unit：中央演算装置）は、コンピュータの機能を実行するための主装置のひとつで、演算を実行するパーツです。CPUにはコアと呼ばれる計算を実行する心臓部があり、現在の一般的なCPUは、ひとつのCPUのなかに複数のコア（マルチコア）を備え、一度に情報を並列処理できるようになっています。仮想マシンが利用する仮想CPUは、仮想マシン1台あたりに1つのCPU、もしくは1つのコアが割り振られることが理想的です。また、動作の重たい仮想マシンや複雑な処理をする仮想マシンには複数のコアを割り振り、仮想マシン上のリソースを確保する設定も可能なハイパーバイザもあります。

- 近年のCPUには、仮想CPUを物理CPUとほぼ同等に動作させる仮想化支援機能がある
 - Intel CPU: VT-x, AMD CPU:AMD-V
 - CPUの特権レベルが最も高いリング0にアクセスできるのはOSのみ
 - アプリケーションやハイパーバイザはリング3で動作
 - リング3からリング0へのアクセスは例外が発生する



CPUは、セキュリティやシステム保護の観点から、動作モードが設定されています。この動作モードは概念的にリング状になっており、中心のリング0（特権レベル）から外側に向かってリング1、リング2、リング3のように構成されています。リング0は、別名カーネルモードとも呼ばれ、CPUの全機能が無制限に利用することができますが、通常リング0にアクセスができるのはハードウェアを制御しているOSのみです。リング1からはカーネルモードに対して、ユーザーモードと呼ばれ、アプリケーションは通常リング3で動作しています。この仕組みは、アプリケーションによって出された不当な命令によって、ハードウェアやシステムを破壊してしまうこと未然に防ぐ保護機能として働いています。

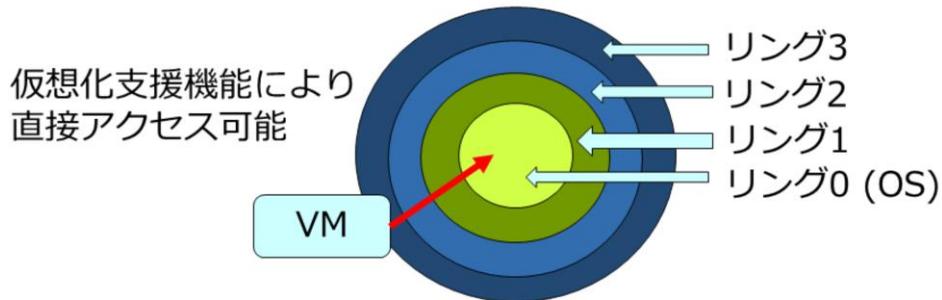
ハイパーバイザは、通常リング3で動作しています。つまり、リング3で仮想マシンによってOSが走ら

させているわけですが、そのOSが必要に応じて直接リング0へアクセスを試みると、命令矛盾が発生してしまいます。この命令矛盾を解決するために、仮想化支援機能としてCPUに新たな動作モードを搭載したCPUが開発されています。

仮想CPU

■ VT-xやAMD-Vに対応したハイパーバイザではVMからリング0へ例外なしにアクセス可能

- I/Oもほぼ直接アクセスできるため、物理環境に近い速度で動作
- デフォルトで仮想化支援機能が無効になっているPCがあるので注意



All Rights Reserved, Copyright© UHD2018

28

仮想化支援機能を利用すると、通常リング3で動作しているハイパーバイザからのリング0へのアクセスが可能となり、物理CPUを監視しているOSを介さずに直接CPUを動作させることができるようになります。その結果、オーバーヘッドを回避することができるようになり、物理CPUが持つ本来の性能を仮想マシンでも利用することが可能になります。

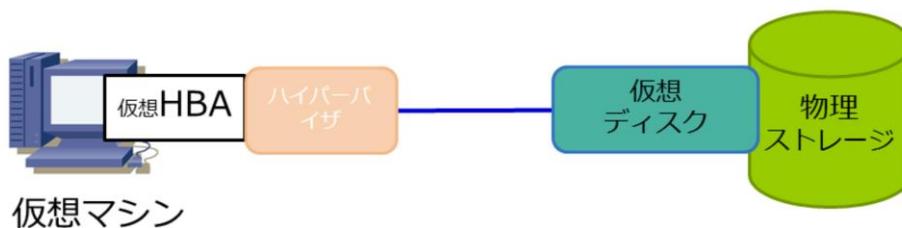
■ 仮想マシンの動作には当然メモリが必要

- ハイパーバイザによって最大メモリ量が異なる
- 仮想マシンへの仮想メモリとして割り当てる際に、完全固定として割り当てる方法（スタティック）と、最小容量と最大容量を定めておき、動的に変更できる方法がある
- Type-I ハイパーバイザ：仮想マシンがほぼすべてのメモリを使用可能
- Type-II ハイパーバイザ：他アプリケーションが使用するメモリ容量を考慮して仮想メモリを設計する

仮想マシンの動作に必要なメモリは、ハイパーバイザの種類によって利用できる領域が異なります。

Type-I ハイパーバイザの場合、ハイパーバイザから直接メモリへのアクセスが可能のため、ハードウェアの搭載されている物理メモリのほぼ全領域を利用することができます。しかし、Type-II ハイパーバイザの場合は、そのハイパーバイザを走らせているホストOSや、その他のアプリケーションが利用しているメモリ領域を考慮して、仮想マシンの仮想メモリ領域が決められます。どちらも場合も、物理メモリ内に固定された領域を仮想メモリとして仮想マシンに割り当てる方法（スタティック）と、必要に応じて、メモリ領域を変化させることが可能な設定があります。メモリ領域を動的に増減できるように設定した場合、物理ハードウェアのリブートが必要になることがあります。

- 仮想マシンは仮想ディスクをストレージとして使用する
- 仮想マシンには、ホストバスアダプタ (HBA) としてIDEやSCSIのインターフェイスが接続され、各方式の内蔵ディスクとして見える
- 仮想ディスクは動的構成を取ることができる
- 設定上120Gの仮想ディスクを使用しても、実際に使用しているサイズのみ物理ストレージ上では消費する



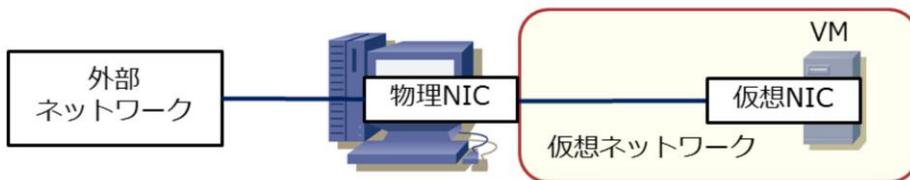
仮想マシンのストレージは、仮想HBAをインターフェースとした仮想ディスクを利用します。

仮想ディスクは物理ストレージと異なり、動的構成をとることができます。ここでいう動的構成とは、仮想ディスクのメリットののひとつであり、仮想マシンから見えている仮想ディスクのサイズと、実際に物理ディスクの上で消費されているストレージのサイズが異なるように構成することです。仮に120GBの仮想ディスクを繋いだ仮想マシンがあるとします。仮想マシンからみれば、そのストレージ領域として120GBが確保され、あたかも120GBの物理ディスクが繋がれているように構成されています。ストレージは、使用されている領域と未使用の領域がありますので、120GBの仮想ディスクも実際にデータが書き込まれ使用されている部分と、空いている部分があります。この実際には使用

していない部分は、仮想マシンからはストレージとして確保された領域として、物理ディスクからは空領域として構成できるということです。仮想ディスク上で使用されている部分のみが物理ディスク上でも使用されている領域として捉えられるので、リソースを効率よく利用することができます。

仮想NIC

- ハイパーバイザによって仮想的なインターフェイスである仮想NICが作成され、仮想ネットワークも作成される
- 物理NICと仮想NICを接続しないと、ホストOSと仮想OSは通信できない
- 物理NICと仮想NICの間に仮想ブリッジや仮想ルータを挟むことで、仮想ネットワーク形態が変わる



仮想NIC (Network Interface Card) は、仮想マシンを物理ネットワークやホストOSと通信を行うためのインターフェイスです。仮想マシンを構成する他の仮想コンポーネント同様に、論理的にネットワークインターフェイスを構成し、物理ハードウェア同様の役割をします。

- 仮想スイッチ：Virtual Switch (vSwitch)
 - 仮想ルータ：Virtual Router (vRouter)
- 仮想ネットワークにおいて、それぞれ物理機器と同じ役割を果たす
 - 仮想ネットワークをNATにする場合はvRouterが
 - VLANを作成する場合はvSwitchが必要



物理マシンをネットワークに接続する際に必要な仮想ネットワーク装置です。仮想マシンからは物理スイッチ、物理ルータとして見え、それぞれの役割も物理機器と同様です。インターネットプロトコルによって構成されているネットワークに接続する場合は、NAT（Network Address Translation：ネットワークアドレス変換）が必要なため、仮想ルータを利用します。また、VLAN（Virtual Local Area Network：仮想LAN）を構成する場合には仮想スイッチを利用してネットワークに接続します。