

目次

1 章 サーバー設計	2
1.1. サーバーフォームファクターの機能と役割	2
1.1.1 ラックマウント型	2
1.1.2 タワー型	4
1.1.3 ブレードテクノロジー	5
1.2. サーバーコンポーネントの設置、設定、管理	7
1.2.1. CPU	7
1.2.2. RAM	14
1.2.3. 拡張スロット	19
1.2.4. NIC	20
1.2.5. ハードディスク	20
1.2.6. ライザーカード	21
1.2.7. RAID コントローラー	21
1.2.8. ファームウェア	22
1.2.9. BIOS/UEFI	22
1.2.10. USB インターフェース/ポート	23
1.2.11. ホットスワップ対応コンポーネントとホットスワップ非対応コンポーネントの違い	23
1.3. 電力と冷却のコンポーネント	24
1.3.1. 電源	24
1.3.2. 冷却	33
第 1 章サーバー設計(12%出題)章末問題	35
第 1 章サーバー設計(12%出題)章末問題 解説	39
2 章 サーバー管理	45
2.1 サーバー用 OS のインストールと設定	45
2.1.1. サーバーの役割と目的の決定	45
2.1.2. ファームウェアのアップデート	45
2.1.3. BIOS/UEFI の設定	45
2.1.4. ディスクの準備	47
2.1.5. ホスト名の設定	53
2.1.6. ローカルアカウントのセットアップ	53
2.1.7. ネットワークへの接続	54
2.1.8. ドメイン/ディレクトリの構成	54

2.1.9. セキュリティ対策.....	55
2.1.10. サービスの有効化.....	56
2.1.11. 機能/ロール/アプリケーション/ドライバーのインストール.....	56
2.1.12. パフォーマンスベースライン	57
2.1.13. 無人/リモートからのインストール.....	58
2.2. サーバーの役割と必要条件.....	60
2.2.1. アプリケーションサーバー	60
2.2.2. ディレクトリサーバー	60
2.2.3. データベースサーバー	60
2.2.4. ファイルサーバー.....	61
2.2.5. プリントサーバー.....	61
2.2.6. メッセージングサーバー.....	62
2.2.7. メールサーバー	63
2.2.8. ルーティング/リモートアクセスサーバー	63
2.2.9. ネットワークサービスサーバー.....	63
2.3. サーバーを管理するためのアクセスとコントロールの使用	65
2.3.1. ローカルハードウェア管理	65
2.3.2. ネットワークベースのハードウェア管理	66
2.3.3. ネットワークベースのオペレーティングシステム管理	68
2.4.適切なサーバー管理手法の実施	72
2.4.1. 変更管理	72
2.4.2. パッチ管理.....	72
2.4.3. 停電と SLA(サービスレベルアグリーメント)	74
2.4.4. パフォーマンスの監視	76
2.4.5. ハードウェアメンテナンス	79
2.4.6. フォールトトレランスと高可用性の手法	80
2.5. 資産管理と文書化の重要性.....	83
2.5.1. 資産管理	83
2.6. 仮想化コンポーネントの目的と運用方法	85
2.6.1. 仮想マシンのホストとゲスト	85
2.6.2. ハイパーバイザ	85
2.6.3. 仮想マシン用の管理インターフェース	86
2.6.4. ハードウェアの互換性リスト	87
2.6.5. ホストとゲスト間のリソース配分	88
第2章サーバー管理(24%出題)章末問題	90
第2章サーバー管理(24%出題)章末問題 解説	98

3 章 ストレージ.....	110
3.1. 特定の仕様とインターフェースを使用しプライマリストレージデバイスをインストールする	110
3.1.1 ディスクの仕様	110
3.1.2. インターフェース.....	112
3.1.3. ハードディスクと SSD の違い	113
3.2. 最適な方法を使用して RAID を設定する.....	114
3.2.1.RAID レベルとパフォーマンスの考慮.....	114
3.2.2. ソフトウェア RAID とハードウェア RAID の違い	115
3.2.3. RAID の設定上の要件(Configuration specifications)	116
3.2.4. ホットスワップのサポートと波及効果(Hotswap support and ramifications)	116
3.2.5. ホットスペアとコールドスペアの違い.....	117
3.2.6. アレイコントローラー(RAID コントローラー).....	117
3.3. ハードウェアと様々なストレージテクノロジーの特性	119
3.3.1. DAS.....	119
3.3.2. NAS.....	119
3.3.3. SAN.....	121
3.3.4. JBOD	124
3.3.5. テープ	125
3.3.6. 光学ドライブ	125
3.3.7. フラッシュ/コンパクトフラッシュ/USB ドライブ	126
3.4. 将来的な成長を見越した適切なストレージ容量の計画と算出	127
3.4.1. 10 進数と 2 進数のディスクサイズの計算(1000 と 1024 の違い).....	127
3.4.2. ディスククオータ	127
3.4.3. 圧縮	127
3.4.4. 容量計画の考慮	127
第3章ストレージ(12%出題)章末問題	130
第3章ストレージ(12%出題)章末問題 解説	134
4 章 セキュリティ	141
4.1. 物理セキュリティの方法と概念.....	141
4.1.1. セキュリティの概念	141
4.1.2. 多要素認証(認証の要素)	143
4.2. サーバー要塞化の手法	149
4.2.1. ハードウェアの要塞化	149
4.2.2. OS の要塞化	150

4.2.3. アプリケーションの要塞化	150
4.2.4. エンドポイントセキュリティ	150
4.2.5. ゼロ弱性スキャンを基にセキュリティの問題を修正する	151
4.3. 基本的なネットワークセキュリティシステムとプロトコル	153
4.3.1. ファイアウォール	153
4.3.2. ポートセキュリティ/802.1x / NAC	155
4.3.3. ルーターアクセリスト	156
4.3.5. 認証プロトコル	157
4.3.6. PKI	159
4.3.7. VPN	164
4.3.8. IPsec	165
4.3.9. セキュリティゾーン	168
4.4. 企業のポリシーに基づいた、論理的なアクセス制御の方法	172
4.4.2. パーミッション(アクセス許可)	174
4.5. データセキュリティの方法とセキュアストレージの処分方法	180
4.5.1. ストレージの暗号化	180
4.5.2. ストレージメディアの処分	180
4.6. 適切な環境管理策および環境管理技術の実装	182
4.6.1. 電源装置のコンセプトと最適な手法(ベストプラクティス)	182
4.6.2. 安全性	185
4.6.3. HVAC/CRAC	188
第4章セキュリティ(13%出題)章末問題	190
第4章セキュリティ(13%出題)章末問題 解説	195
5章 ネットワーク	203
5.1. IP アドレッシングとネットワークインフラストラクチャサービスを利用してサーバーを設定する	203
5.1.1. IPv4 と IPv6	203
5.1.2. デフォルトゲートウェイ	204
5.1.3. CIDR 表記とサブネットティング	204
5.1.4. パブリック IP アドレスとプライベート IP アドレス	205
5.1.5. 静的 IP 割り当てと DHCP の違い	205
5.1.6. DNS	206
5.1.7. NetBIOS	208
5.1.8. WINS	208
5.1.9. NAT/PAT	209
5.1.10. MAC アドレス	211

5.1.11. ネットワークインターフェースカードの設定	211
5.2. 様々なポートとプロトコル	213
5.2.1. TCP と UDP の違い	213
5.2.2. サーバーのサービスで使用されるプロトコルとポート	213
5.3. 適切なケーブル管理手順の実施	224
5.3.1. カッパー・ケーブル(銅線)	224
5.3.2. ファイバーケーブル	225
5.3.3. コネクター	226
5.3.4. ケーブルの設置とルーティング(配線経路)	228
第 5 章ネットワーク(10%出題)章末問題	229
第 5 章ネットワーク(10%出題)章末問題 解説	234
6 章 災害復旧	241
6.1. 災害復旧原則の重要性	241
6.1.1. 運用の継続	241
6.1.2. サイトの種類	242
6.1.3. 複製(レプリケーション)の方法	243
6.2. 適切なバックアップの手法	244
6.2.1. バックアップ手法	244
6.2.2. バックアップメディア	247
6.2.3. メディアと復元の最適手法(ベストプラクティス)	247
6.2.4. メディアの保管場所	249
第 6 章災害復旧(9%出題)章末問題	251
第 6 章災害復旧(9%出題)章末問題 解説	254
7 章 トラブルシューティング	259
7.1. トラブルシューティングの理論と方法	259
7.1.1. 問題を特定し、影響範囲を判断する	259
7.1.2. 明確な質問により、可能性の高い原因の仮説を立てる	259
7.1.3. 原因を判断する理論をテストする	260
7.1.4. 問題を解決するための対応計画を策定し、影響のあるユーザーに通知する	260
7.1.5. 解決策を実行し、必要に応じてエスカレーションする	260
7.2. 適切なツールと方法を選択し、ハードウェアに関連する問題のトラブルシューティングを実施する	262
7.2.1. 一般的なハードウェア障害	262
7.2.2. ハードウェア障害に共通する原因	264
7.2.3. 環境の問題	265
7.2.4. ハードウェアツール	266

7.3. 適切なツールと方法を選択し、ソフトウェアに関連する障害を効果的にトラブルシューティングする.....	268
7.3.1. 一般的なソフトウェア障害	268
7.3.2. 一般的なソフトウェア障害の原因	272
7.3.3. ソフトウェアツール	275
7.4. 適切なツールと方法を選択し、ネットワークに関連する障害を効果的に診断する.....	280
7.4.1. 一般的なネットワーク障害	280
7.4.2. 一般的なネットワーク障害の原因	283
7.4.3. ネットワークツール	286
7.5. 適切なツールと方法を選択し、ストレージに関連する障害を効果的にトラブルシューティングする	295
7.5.1. 一般的なストレージ障害.....	295
7.5.2 一般的なストレージ障害の原因.....	298
7.5.3. ストレージツール	303
7.6. 適切なツールと方法を選択し、セキュリティに関連するトラブルを効果的に診断する	308
7.6.1. 一般的なセキュリティトラブルの診断.....	308
7.6.2 一般的なセキュリティトラブルの原因.....	309
7.6.3. セキュリティツール	314
第7章トラブルシューティング(20%出題)章末問題	318
第7章トラブルシューティング(20%出題)章末問題 解説	326

Windows はマイクロソフト社の登録商標です。

また本文内の各商標、製品名は各社の登録商標です。

1章 サーバー設計

学習のポイント

この章では、サーバーのハードウェア、ファームウェアについて学習します。サーバーの筐体、ラック、CPU、メモリ、外部機器の接続インターフェース、機能拡張スロット、BIOS、電源、冷却など、サーバーを構成する要素について学習します。

1.1. サーバーフォームファクターの機能と役割

フォームファクターとは、マザーボードのサイズ、ケースへ固定するネジ穴の位置、I/O パネルの位置と大きさ、拡張スロットの位置、ラックサイズ、バックアップ用のテープ媒体などを規定した規格です。複数のベンダで製造される PC/AT 互換機では、フォームファクターを標準化して互換性を確保しています。

マザーボード(システムボード)は、コンピューターの中心となるプリント基板で CPU、メモリ、グラフィックス、ネットワークなどを制御する LSI(チップセット)、CPU やメモリを差し込むソケット、拡張カードを差し込む拡張スロット、ハードディスク、CD/DVD などのドライブとケーブルの接続コネクター、BIOS(ROM)、電源コネクタ、CMOS バッテリーなどが搭載されています。

ケースに固定され、CPU、メモリ、機能拡張カードなどを装着し、電源ケーブル、ディスクケーブルなどを装着します。

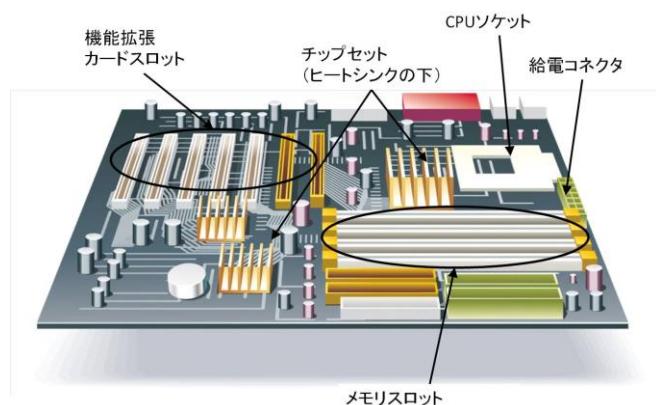


図 1.1. マザーボード

1.1.1 ラックマウント型

ラックマウント型は標準化された幅 19 インチのラックにサーバーを積み重ねるように集中配置できる形状にしたもので、サーバーの高密度化を図ることができます。

ラックマウント型は、ISP、データセンター、大企業など、狭い面積に多数のサーバーを設置する高密度化の必要性に応じて普及しています。



図 1.2.ラックマウント型サーバー

ラックマウント型のメリット/デメリット	
メリット	ラック対応機器を縦に集中配置できること。一般的なサーバーラックは、高さ 40U 程度で 1U のラックマウントサーバー40 台を設置可能。 管理運用面でケーブルを短くして整理しやすい。 ラック幅、マシンの高さなどの標準規格がある
デメリット	ラックコストがかかる。 ラックマウント型マシンのケースが小さいので、内部冷却に高出力空冷ファンが必要となり、騒音が大きくなる可能性がある。(最近の 1U のサーバーは静謐性が高い)

表 1.1. ラックマウント型のメリット/デメリット

1.1.1.1 寸法

EIA(米国電子工業会)の定めた幅 19 インチ(482.6mm)で標準化されています。ラックに装着される機器の高さは U(ラックユニット/rack Unit)という単位で標準化されています。

- **1U=1.75 インチ(44.45mm)**

例：2U=3.5 インチ、4U=7 インチ、8U=14 インチ

1.1.1.2 ケーブルマネジメントアーム

ケーブルマネジメントアームは、ラックマウントサーバーの後ろ側のケーブルをまとめるために、左右のレールキット間を指し渡すように装着するパーツです。



図 1.3. ケーブルマネジメントアーム

http://www.rtk.jp/images/img_16/ophpc365403b21_3.jpg

1.1.1.3 レールキット

レールキットは、ラックの前後の支柱にレールを装着しサーバー本体にラック搭載用ブラケットを装着して、レールに合わせて奥に送り込み、前に飛び出さないように前面(フロントベゼル)の固定用のつまみで押さえます。

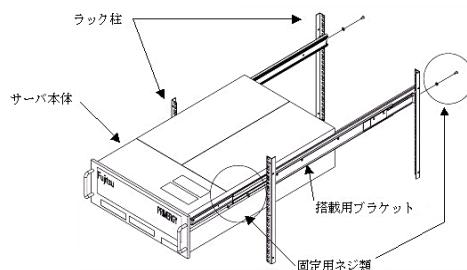


図 1.4. レールキット

<http://jp.fujitsu.com/platform/server/primergy/peripheral/rack/image/image01.gif>

レールキットは、前に伸ばした時にどれだけの幅の物が必要かを、ラック設置とサーバー購入前に測っておきます。

1.1.2 タワー型

タワー型(ペデスタル型)は高さにより、[フルタワー]、[ミドルタワー]、[ミニタワー]などに分類されます。

タワー型のメリット/デメリット	
メリット	目的に応じたサイズを選ぶことができる 配置が容易
デメリット	複数のサーバーを集中配置すると、ケースサイズが不揃いになり、隙間なく配置することが難しい 重ねて積めないため、設置面積が増える

表 1.2.タワー型のメリット/デメリット

サイズが豊富でエントリ用サーバーではデスクトップPCと同程度、ミッドレンジ用は、内蔵ドライブ用のベイを多くそなえた幅広(40cm以上)のものが選ばれます。エンタープライズ用は、約2mの高さの大型ケースの製品もあります。



図1.5. タワー型サーバー

正面は施錠可能なフロントベゼルを装着し、USBインターフェースや電源ボタンへのアクセスを禁止します。

1.1.3 ブレードテクノロジー

ブレードテクノロジーは、複数のサーバーを集約して使用することを前提とする技術です。このためサーバーの核となる「ブレード(刃の意味)」と、複数のブレードを格納するブレードエンクロージャー(ブレードシャシー)から構成されます。

1.1.3.1 ブレードエンクロージャー(ブロードシャーシ)

ブレードエンクロージャー(ブレードシャシー)は、ブレードを接続し格納する筐体です。ブレードの差込口が並び、ブレードを差し込むだけでサーバーとして稼動させることができます。

ブレードエンクロージャーのメリットとデメリット	
メリット	背面に複数の電源ユニット、冷却ファン、LANやSANのスイッチなど複数のブレードで共用する装置を冗長化して装着可能 前面に挿入するブレード単体の構成を簡素化させ小型化できる ブレードとエンクロージャー間の接続は配線不要(差し込むだけ) ホットスワップ機能が提供される場合は、システム全体を稼動させたまま故障したブレードの切り離しと新しいブレードの装着が可能。
デメリット	ブレードとブレードエンクロージャー間の規格は、標準化されていない。(ブレードエンクロージャーを選択すると、装着可能なブレードはエンクロージャーと同じベンダの製品で装着可能なブレードに限定される。)

表1.3.ブレードエンクロージャーのメリットとデメリット

ブレードエンクロージャーの電源容量やI/O技術が将来の技術革新を考慮して設計されているかも調べておく必要があります。

例えば、サーバーの消費電力は CPU クロック周波数に比例して増大するため、後からブレードエンクロージャーに最新のブレードを追加しようとして、消費電力がブレードの許容電源容量を超えててしまうので搭載できないという場合が考えられます。

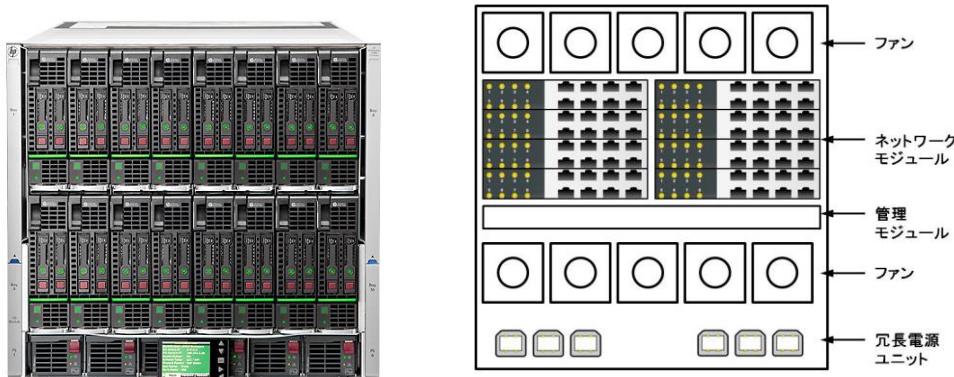


図 1.6. ブレードエンクロージャー

http://h50146.www5.hp.com/products/servers/bladesystem/c/component/enc_c7000/
(HP カタログ写真)

構成要素	説明
バックプレーン/ミッドプレーン	バックプレーン/ミッドプレーンは、ブレードエンクロージャー内で、前面のブレード装着部と背面のエンクロージャー管理モジュール、ネットワークモジュール、冷却ファン、ネットワークモジュール/スイッチなどの装着部の間で、これらの要素を配線により接続する。 ラックマウントサーバーでも使用され、前面のディスクユニット、DVD ユニットなどと、背面のマザーボード部分の間でこれらの要素を接続する。
(冗長)電源ユニット	ブレード上には電源は無く、背面の(冗長)電源ユニットに装着される。
ネットワークモジュール/スイッチ	ネットワークカードは各ブレードに搭載され、バックプレーン/ミッドプレーンを介してエンクロージャー背面の LAN スイッチと接続する
管理モジュール	エンクロージャー内のシステムの温度や電力の状況、ハードウェア構成、ネットワーク構成などを監視、制御する管理コントローラモジュールを背面に装着可能。エンクロージャー内の電源容量の上限設定、設定値内でサーバーの電力消費の制御機能、管理モジュールの二重化なども可能。

表 1.4.ブレードエンクロージャーの構成要素

1.1.3.2. ブレードサーバー

ブレードサーバーは、1U 未満の厚さでディスクを 2 台程度まで搭載し、1U ラックマウント型サーバーを複数使用するよりも、さらに高密度化と省エネルギーを実現できます。ブレードのサイズはフルハイイト、ハーフハイイト、クオーターハイイトブレードがあります。

ブレードはエンクロージャーに縦に装着したため幅をハイト(height/高さ)と表現します。(現在は横に装着するものもあります。)

種類	特徴
フルハイトブレード	幅(高さ)14 インチ(約 36cm)のブレード。
ハーフハイトブレード	幅(高さ)7 インチ(約 18cm)のブレード。フルハイトブレードのスロットに 2 枚装着でき、高密度化を実現できる。 エンクロージャーによっては、設置スロットが限定される場合もある。
クオーターハイトブレード	幅約(高さ)約 3.5 インチ(約 9cm)のブレード。フルハイトブレードの 1/4 幅(高さ)で、さらに高密度化可能。

表 1.5.ブレードの種類

例えば、高さ 10U のブレードエンクロージャーに 16 枚のハーフハイトブレードを装着すると、1U のラックマウント型サーバー 10 台よりも 6U 分の密度が高くなります。また LAN スイッチも 10U エンクロージャーの背面に収まるので、スイッチの設置分もラックに余裕ができます。

1.2. サーバーコンポーネントの設置、設定、管理

1.2.1. CPU

CPU(Central Processing Unit)は、プログラムによって指示された演算や周辺機器の制御を高速に処理します。

シリコンウェハーから製造された CPU は半導体そのもので、この状態の CPU を、CPU チップ、ダイなどと呼びます。この CPU チップを小さい基板の上に実装しカバーで覆い保護したものを、CPU パッケージと呼びます。

□ プロセスとスレッド

プログラムは実行時に OS が「プロセス」として管理します。CPU は OS が実行する「プロセス」を「スレッド」という単位に分けて実行します。CPU から見るとプログラムの実行単位(最小実行単位)は「スレッド」です。複数のスレッドを同時に実行する CPU の能力をマルチスレッドと呼びます。

1.2.1.1. CPU の設計

CPU の代表的なアーキテクチャには CISC、RISC、ARM があります。

種類	説明
CISC	複合命令セットコンピュータ (Complex Instruction Set Computer)。CPU の命令を高級言語に近づけ、複雑な処理を実行できるようにして処理能力を向上させる Intel 系の一般的な CPU は CISC アーキテクチャ。例 : x86、x64 Windows Server は CISC アーキテクチャの CPU のみをサポートする
RISC	縮小命令セットコンピュータ (Reduced Instruction Set Computer)。CPU の命令を簡略化しパイプライン処理(並行処理)の効率を高め処理能力を向上させる Linux/UNIX などの OS は RISC 型の CPU アーキテクチャもサポートする
ARM	RISC を進化させたアーキテクチャ。ARM Ltd が開発 スマートフォン、タブレット用に消費電力を抑えている 32 ビット版/64 ビット版がある

表 1.6. CPU アーキテクチャ

CISC アーキテクチャを持つ Intel 系の代表的な CPU の種類には x86 と x64 があります。

□ x86 と x64(Intel 系 CPU)の違い

種類	説明
x86	8086 以降 80486までの Intel プロセッサ(及び互換プロセッサ)の呼称。32 ビット CPU。 IA-32 は、80386 以降の 32 ビット単位でデータ処理を行う命令セットアーキテクチャを持つ Intel 系 CPU の呼称だが、x86 は IA-32 と同義語として 32 ビット CPU(32 ビット単位の命令セットアーキテクチャを持つ CPU)指して使用されることが多い。i386 の表記も x86 と同様の意味で使用される。 データバス、アドレスバス共に 32 ビットであり、アドレッシング可能なメモリの最大は 4GB
x64	x86 命令セットアーキテクチャ(32 ビット単位のデータ処理)を 64 ビット単位に拡張した命令セットアーキテクチャ、および CPU の呼称。IA-64 とも呼ばれる 64 ビット CPU。 Intel の発表した IA-64 は当初 IA-32 と互換性が無かったが AMD が x86 を拡張し上位互換性を持つ x86-64 を発表したため、Intel も IA-32 と互換性を持つ Intel64 を発表した。現在は全て x64 と呼ばれる。 Windows Server 2008R2 以降は x64 アーキテクチャのみをサポートする 注：ソフトウェアパッケージに「x86-64 用」の表記がある場合は x64(64 ビット)CPU 用で x86(32 ビット)CPU では動作しない。

表 1.7. x86 と x64 の違い

1.2.1.2. マルチコアとマルチプロセッサ

□ マルチコア

CPU の中心部分をコアと呼びます。マルチコアは、1 つの CPU パッケージ内に内蔵される複数のコアのことです、このような CPU はマルチコア CPU です。コア 1 つの CPU はシングルコア CPU です。

マルチコア CPU には、2 つのコアを内蔵するデュアルコア、4 つのコアを内蔵するクアッドコア、6 コア(ヘキサコア)、8 コア(オクタコア)、10 コア(デカコア)、12 コア(ドデカコア)、16 コア(ヘキサデカコア)などがあります。

サーバーマシンで使用される CPU、Xeon、Opteron の特徴を挙げておきます。Xeon などのマルチコア CPU を搭載したマシンをハード的に「マルチコアサーバー」と呼ぶこともあります。

CPU	特徴
Xeon	Intel 社のプロセッサ Xeon(ジーオン) x86 と x64 命令セットを持つサーバー用 CPU コア数 : 1, 2, 4, 6, 8, 10, 12 E7, 7000 系 : 4 ソケット、8 ソケットのマルチプロセッサマシン向け E5, 5000 系 : 2 ソケットを中心とするマルチプロセッサマシン向け E3, 3000 系 : 1 ソケットのエントリサーバー、ワークステーション向け
Opteron	AMD 社のプロセッサ Opteron(オプテロン) x86 と AMD64 命令セットを持つ CPU コア数 : (1,) 2, 4, 6, 8, 12, 16 Opteron 6300 : 12, 16 コア中心のハイエンドサーバー向け Opteron 4300 : 4, 6, 8 コアのミドルレンジサーバー向け Opteron 3300 : 4, 8 コアのエントリサーバー向け

表 1.8. Xeon と Opteron(参考)

□ ハイパースレッディング

ハイパースレッディングは 1 つのコアで 2 つのスレッドの同時実行メカニズムを搭載し、1 つのコアを 2 つのコアのように見せて処理速度を向上させる技術です。ハイパースレッディング技術により CPU クロックあたりの性能は 20%程度向上すると言われています。

□ マルチプロセッサ

マルチプロセッサとは、マザーボード上の複数の CPU ソケットにそれぞれ CPU を装着した状態のことです。各 CPU はマルチコア CPU でもかまいません。マルチプロセッサの制御方式には SMP と ASMP(AMP)があります。特徴は次の表の通りです。

方式	特徴
SMP	Symmetric MultiProcessing(シンメトリックマルチプロセッシング) 対称型マルチプロセッシング 各 CPU を等しく扱い並列処理を行わせる(同時スレッド性が向上する) 複数の CPU は 1 つの同じメモリ空間を使用し情報を共有するため、それぞれ他の CPU と同じ処理を行うことができ、処理能力と耐障害性の向上を図ることができる CPU は同じ型式、同じステッピング(後述)のものを使用する
ASMP (AMP)	ASymmetric MultiProcessing(アシンメトリックマルチプロセッシング) 非対称型マルチプロセッシング 複数の CPU それぞれに別々の処理を分担させて実行する SMP に比べ制御が難しく、高価

表 1.9. マルチプロセッサの制御方式



図 1.7. マルチプロセッサ(デュアルプロセッサ)

1.2.1.3. キャッシュレベル：L1、L2、L3

CPU はメモリ(主記憶装置)へのアクセスを頻繁に繰り返し命令を実行しますが、CPU の処理速度に比べるとメモリのアクセス速度は遅いため、CPU に待ち時間が生じます。

「キャッシュメモリ」は、CPU とメモリとのアクセス時間のギャップを埋めるために CPU とメモリの間に配置されるメモリよりも高速にアクセス可能な小さな記憶域です。次に使用される可能性が高いと予測される情報から、1 次(レベル 1/L1)キャッシュ、2 次(L2)キャッシュ、3 次(L3)キャッシュの順に格納されます。

CPU は命令の実行時に、最初にプロセッサ内のデータレジスタを探し、データが見つからなければ L1、次に L2、さらに L3 キャッシュを探します。

キャッシュメモリは CPU の能力向上に伴い、一時期 SRAM を用いて CPU の外に、より大きい外部キャッシュを配置し、CPU 内蔵の 1 次(L1)キャッシュ、外部の 2 次(L2)キャッシュとして利用した時期がありました。現在では、2 次(L2)キャッシュ、さらに大きい 3 次(L3)キャッシュまで CPU に内蔵され、CPU キャッシュは全て内蔵となっています。

1.2.1.4. スピード(CPU スピード)

CPU のスピードに関連する要素は、クロック速度、バス幅、コア数です。

□ クロック速度と CPU スピードの関係

コンピューターは一定間隔でパルスを生成する水晶発信器からクロック信号(14.31818MHz)を作成します。この信号を、コンピューターの様々な回路で必要とされる周波数に変調する PLL(Phase Locked Loop)回路を含むクロックジェネレータを通し、コンピューターは必要なクロック周波数を得ます。

□ バスと CPU スピードの関係

バスはコンピューター内で各回路がデータをやり取りする伝送経路です。CPU の外側にあるバスはシステムバスと電源バスです。システムバスには、アドレスバス、データバス、制御バスが含まれます。

バスの種類		特徴
システム バス	アドレスバス	メモリアドレスを指定する経路(CPU からメモリへの一方行) アドレスバスのビット数(幅)で CPU が直接扱えるメモリ容量が決まる
	データバス	データの送受信用の双方向の経路
	制御バス	アドレスやデータの送受信タイミング制御信号の経路
電源バス		電力供給経路

表 1.10. バスの種類

システムバスは、CPU とチップセット、CPU とメモリ、チップセットとメモリ、IO インターフェースなどを接続します。

Core i7/i5 などの Nehalem(ネハレム：開発コード名)マイクロアーキテクチャを採用する Intel 社の CPU は、メモリコントローラを CPU に内蔵するため、CPU とメモリ間は複数チャンネルのメモリ専用システムバス(メモリバス)で直接接続します。CPU と PCI-Express スロットも PCI-Express バスで直接接続しています。

CPU とチップセット(IOH/Input Output Hub)間は QPI(クイックパスインターフェクト /QuickPath Interconnect)システムバスを使用します。QPI は CPU と CPU 間の接続にも使用します。

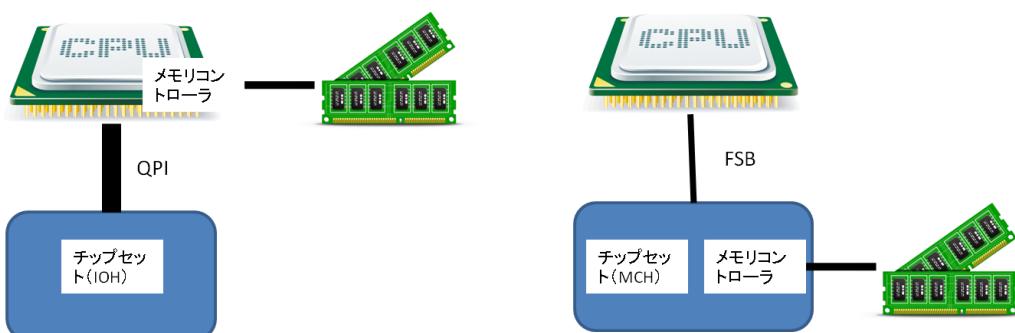


図 1.8. QPI と FSB バスの比較

QPI は片方向で実効 16 ビット(2 バイト)転送となるため、最速で片方向 6.4GT/s=12.8GB/s の帯域幅(転送スピード)となり、双方で 25.6GB/s になります。(片方向 4.8GT/s の場合は、9.6GB/s、双方で 19.2GB/s になります。)

T/s(Transfers per second)は、1秒間に何回データ転送するかの単位です。この例では G(Giga)の補助単位付きで GT/s と表現されています。

QPI 以前は FSB(フロントサイドバス/Front Side Bus)というパラレル転送バスが使用されていました。

種類	特徴
QPI	<p>QuickPath Interconnect。FSB に変わるバス。</p> <p>片方向のポイントツーポイントリンクの「シリアル転送」バスで、相互接続の場合は 2 系統必要。</p> <p>転送レート: 4.8GT/s または 6.4GT/s (GT/s : GigaTransfers per second) 片方向</p> <p>実質 16 ビットの転送となるため帯域幅は双方向で 19.2GB/s または 25.6GB/s</p> <p>クロック信号線を持つ。</p> <p>クロックあたりの伝送効率は FSB より高い。(より高速)</p>
FSB	<p>フロントサイドバス。Intel 社製の CPU(Pentium II)などで採用されたバスで、外部 2 次キャッシュ以外の伝送経路用のバス。</p> <p>双方向の共有バスでパラレル転送。</p> <p>当初は CPU のベースクロックと同じ周波数で動作。Pentium4 以降は、ベースクロックの 4 倍の周波数で転送が可能になった(Quad Pumped 技術)</p> <p>BSB(バックサイドバス)は、FSB とペアで採用されたバスで、CPU と部 2 次キャッシュを接続する専用バス。</p> <p>転送速度: FSB 1600MHz 転送で 12.8GB/s</p>
HT	<p>Hyper Transport。AMD 社の汎用 Point to Point 接続技術</p> <p>FSB の置換えだけでなく CPU と CPU の接続などにも利用可能。</p> <p>バージョン 1.x, 2.0, 3.0, 3.1 がある</p> <p>3.2GHz のクロック信号に DDR(ダブルデータレート)で同期して動作する</p> <p>双方向のシリアル/パラレルラインで、接続は 2 ビットのラインから、2 つの 32 ビットのラインで接続可能でビット幅は自動調整される。</p> <p>双方向 32 ビット接続を 3.2GHz で動作させると最大で 51.2 GB/s の転送が可能</p>

表 1.11. QPI と FSB と HT

□ バスチャネル

チャネル(channel)は、データの論理的な伝送経路を表す言葉です。バスチャネルは CPU と周辺機器間でのデータ伝送路を指しています。現在では CPU とメモリ間には複数のバスチャネル(メモリチャネル)が構成され、メモリ転送を高速化しています。

□ コアと CPU スピードの関係

マルチコア CPU では、1 つの CPU で同時に複数のスレッドの実行(同時スレッド処理/マルチスレッド)が可能となるため、「マルチスレッド対応のプログラム」の処理速度が向上します。

□ Intel ターボブーストテクノロジ

Intel ターボブーストテクノロジは、プロセッサが TDP (熱設計電力:Thermal Design Power) の限界未満で稼働している場合に、自動的に定格の動作周波数よりも早く動かす

(オーバークロック)技術です。マルチスレッド対応のプログラムもマルチスレッド未対応のプログラムも共に処理速度が向上します。

1.2.1.5. CPU ステッピング

Intel 社の CPU の「B-2」、「C-1」などの表示で CPU の内部のバージョンの違いを表わしたものと「ステッピング」と呼びます。同じ CPU で同じクロックの製品でも製造ロットによりステッピングが異なり、後期ロットでは不具合が修正されたり、命令が増減したりします。

CPUID 命令を使い、数値でステッピングを確認することができます。(i386 後期以降)。例えば Pentium4 のステッピング B-2 は CPUID [7]、C-1 は CPUID [10] と表されます。

SMP 方式のマルチプロセッサを装着する場合は、同一形式、同一ステッピングのものを選択します。

1.2.1.6. ソケットの種類

CPU ソケットは、マザーボード上に設置された CPU を装着し電気的な接続を確立する接続点を提供する部品です。

CPU 底面の PGA(ピージェー/Pin Grid Array)構造のピンを穴に差し込む形状で、レバーを使い CPU パッケージをソケットに圧着して固定します。

CPU ソケットは、CPU の種類やメーカーにより異なります。どの CPU が装着可能かは、CPU ソケットの形式を確認する必要があります。代表的な CPU ソケットを次の表に列挙します。

名称	ピン数	サポート CPU	バス
Socket B/ LGA1366	1366	インテル Core i7 900 シリーズ	QPI
Socket LS/ LGA1567	1567	インテル Xeon 6500/7500 系, E7 系用	QPI
Socket R/ LGA 2011	2011	インテル Core i7 3800/3900, 4800/4900 系 Xeon E5, E5-v2 1600/2600/4600 系 Xeon E7 2800/4800 系, E7-v2 2800/4800/8800 系等	QPI
Socket R3/ LGA 2011-v3	2011	インテル Core i7 5800/5900 系 Socket R と互換性はない	QPI
Socket G34	1974	AMD Opteron 6000 系	HT
Socket AM3+	942	AMD Phenom II (AM3 用), Athlon II, Sempron, Opteron 138x DDR2 メモリを非サポート	HT
Socket AM3	941	AMD Phenom II (AM3 用), Athlon II, Sempron, Opteron 138x	HT

表 1.12. 代表的な CPU ソケット

1.2.2. RAM

RAM(ラム/Random Access Memory)は、読み書きを自由に行える揮発性の半導体メモリで、IT 機器の一時記憶装置として一般的に利用されています。

1.2.2.1. SRAM と DRAM の違い

RAM(Random Access Memory)には SRAM(スタティック RAM/Static RAM)と DRAM(ダイナミック RAM/Dynamic RAM)があります。

種類	特徴
SRAM	半導体記憶素子にデータの書き込み後、通電中は内容が失われない。 アクセスは DRAM に比べ速い 構造が複雑で高価 集積度も DRAM ほど高くない CPU の外部キャッシュとして利用されていた。 CPU のキャッシュメモリ、ルーターやハードディスクのバッファなどに利用される
DRAM	半導体記憶素子にデータの書き込み後、記憶内容が消えないように一定時間ごとに電流を流す 「リフレッシュ」を実行する 構造が簡素で低価格、集積度を上げることが可能 コンピューターの大容量の一時記憶として利用される

表 1.13. SRAM と DRAM の相違

1.2.2.2. モジュールの設定

メモリは、通常 1 枚のメモリ基板上に複数のメモリチップが実装されたメモリモジュールで提供されます。

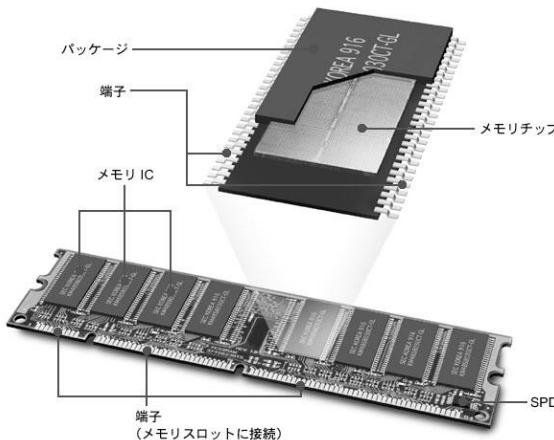


図 1.9. メモリモジュールの構造

例えば、256MB のメモリモジュールは、128M ビットのメモリチップがメモリ基板の両面に 16 個実装されている物や、256M ビットのメモリチップがメモリ基板の片面に 8 個実装

されている物があります。

メモリにはチップ規格とモジュール規格があり、チップ規格はメモリの動作周波数、モジュール規格はメモリの転送速度などを定めています。

1.2.2.3. ECC メモリとの non-ECC メモリの違い

ECC(誤り訂正符号/Error-Correcting Code)は、メモリーエラーの存在を検出し、エラーが発生したビットを特定して、正しい値に修正する機能です。

種類	特徴	
ECC メモリ	<p>64 ビットデータに対し 8 ビットの冗長ビットを付加し、1 ビットエラーの訂正と 2 ビットエラーの検出が可能。</p> <p>メモリーエラーの発生時は、4bit あるいは 8bit (DRAM の 1word) 単位でデータが失われる可能性が高くなる。この場合は ECC でエラー訂正や検出が不可能となり、DRAM チップが 1 個故障するとシステムダウンする。</p> <p>エラー検出とエラー訂正の仕組みが複雑でコストが高くなる。</p>	
non-ECC メモリ (非 ECC メモリ)	<p>エラー訂正機能がない分、高速なアクセスが可能</p>	
	パリティ付 メモリ	メモリ内の一定単位(通常 8 ビット)ごとに、それらのビットの値を加算した結果の最下位の 1 ビットの値を、パリティビット(冗長ビット)として保存するメモリを付加したメモリ。 奇数個のエラー検出は可能だが、偶数個のビットにエラーがあると検出できない。 ECC よりも構造が簡単で低コストで実装可能。

表 1.14. ECC メモリと non-ECC メモリの相違

□ レジスターード(バッファード)メモリ

レジスターード(Registered)メモリは、レジスタバッファチップを搭載し、レジスタバッファで電気信号の整流や增幅機能を持たせたメモリモジュールで、タイミングのずれを補正し動作を安定化させます。

一般的に ECC 機能と共に提供されるため、ECC メモリには ECC レジスターード(バッファード)メモリと ECC アンバッファードメモリが存在します。ECC レジスターード(バッファード)メモリの使用が可能かは、マザーボードの仕様に依存します。

ECC レジスターードメモリと ECC アンバッファードメモリの混在はできません。

1.2.2.4. ピンの数

メモリモジュールには、SIMM(シム/Single Inline Memory Module)、DIMM(ディム/Dual Inline Memory Module)、RIMM(リム/Rambus Inline Memory Module)などの種類があります。各モジュールのピン数を次の表の通りです。

種類	特徴
SIMM	DRAM を使うメモリモジュール

	30 ピンもしくは 72 ピン。 増設時には同じ SIMM を 2 枚 1 組で使用。
DIMM	現在一般的に使用されている DRAM を使うメモリモジュール
	SDRAM 144 ピン
	DDR SDRAM 168 ピン
	DDR2 SDRAM、DDR3 SDRAM 240 ピン DDR2 と DDR3 は、同ピン数だが互換性はなく、混在できない(モジュールの切れ込み位置が異りソケットに装着できない)
	DDR4 SDRAM 284 ピン
	RDRAM や Direct RDRAM を使うメモリモジュール。 184 ピン DIMM をベースとするが DIMM との互換性はなく、現在はほとんど使用されていない。RDRAM は Rambus Dynamic Random Access Memory の略

表 1.15. SIMM,DIMM,RIMM

1.2.2.5. DDR2、DDR3

DIMM には、SDRAM、DDR、DDR2、DDR3、DDR4 の種類があります。DIMM の DRAM は、すべてシステムバスのクロック信号に同期して動作する SDRAM で、DDR(ディディアル/ Double Data Rate)は各 SDRAM のスピードを表し、SDRAM の前に付けて種類を表していましたが、今では SDRAM を省略し単に DDR と呼びます。特徴は次の表の通りです。

種類	特徴
SDRAM	Synchronous DRAM メインメモリに使われるメモリ規格。 システムバスのクロック信号に同期して動作する DRAM
DDR SDRAM	Double Data Rate SDRAM 理論上データ転送速度 : SDRAM の 2 倍 クロック信号の立ち上がり時と立ち下がり時の両方でデータの読み書きが行えるダブルデータレート (DDR) モード(高速データ転送)機能を持つ 動作電源電圧 : DDR SDRAM (2.5V/2.6V)
DDR2 SDRAM	Double Data Rate 2 SDRAM 理論上データ転送速度 : DDR SDRAM の 2 倍、SDRAM の 4 倍 内部クロックの 2 倍の外部クロックを用いる 動作電源電圧 : DDR2 SDRAM (1.8V)
DDR3 SDRAM	Double Data Rate 3 SDRAM 理論上データ転送速度 : DDR2 SDRAM の 2 倍、DDR SDRAM の 4 倍、SDRAM の 8 倍 動作電源電圧 : DDR3 SDRAM (1.5V)、DDR3L SDRAM (1.35V)、DDR3U SDRAM (1.25V) で、消費電力低減、低発熱を実現
DDR4 SDRAM	Double Data Rate 4 SDRAM 理論上データ転送速度 : DDR3 SDRAM の 2 倍 メモリ容量 : DDR3 SDRAM の 2 倍 消費電力 : DDR3 の 60% (40%削減)

表 1.16. SDRAM の種類

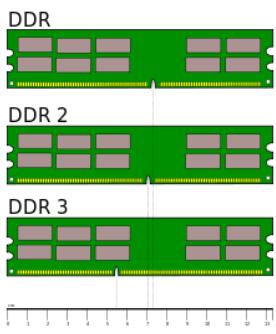


図 1.10. DDR,DDR2,DDR3

□ メモリバンク

メモリバンクは、コンピューターがメモリを一定サイズで管理する区分です。メモリコントローラのアクセス要求はメモリバンクごとに行われます。メモリモジュールは1枚～3枚で構成されます。

メモリバンク A に A1、A2 スロット、メモリバンク B に B1、B2 スロットがある場合、A1 と B1 を 1 セット、A2 と B2 を 1 セットとして同色のスロットとなっています。



図 1.11. メモリバンク

マザーボードにより異なりますが、同一色のスロットが 1 セットとなっていることが多い、メモリ増設やメモリ交換時に、同一色のメモリスロットメモリを装着しますが、メモリモジュールを装着するスロットの順番が決まっている場合もあるので装着前に確認します。

1.2.2.6. メモリタイミング

メモリタイミング(メモリアクセスタイミング)とは、メモリアクセスの手順に必要な時間(クロック数)を表す表記で、「8-8-8-24」といった 4 つの数値で表されます。

4 つの数字は一般的に、先頭から順に次の内容を表しています。数字の並びはタイミングの発生順とは一致していません。(また、表記順は異なる場合があります)

メモリタイミングの要素	説明
①CAS Latency	CAS(Column address strobe)遅延(Latency) 記憶素子の列指定後から記憶素子への読み書きを開始するまでの遅延時間
②RAS to CAS Delay	RAS(Row address strobe)から CAS 間の遅延(Latency) 記憶素子の行指定後から記憶素子の列指定を開始するまでの遅延時間
③RAS Precharge	記憶素子へのアクセス終了後から別の記憶素子の行(Raw)指定を開始するまでの遅延時間
④RAS Activate to Precharge	記憶素子の行(Row)指定後から記憶素子へのアクセス終了までの最小時間

表 1.17. メモリタイミング

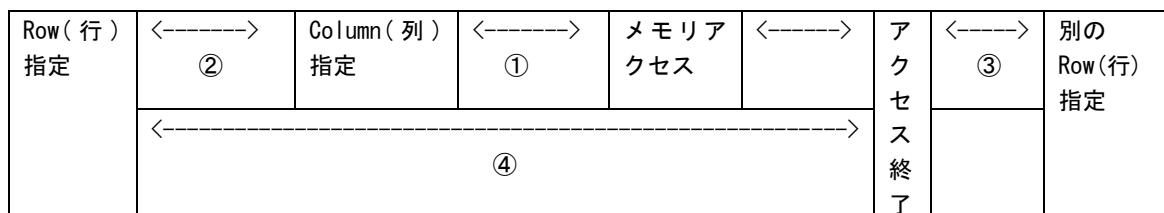


図 1.12. メモリタイミング

□ CAS レイテンシー

CAS(キャス/ Column address strobe latency)レイテンシーは、SDRAM の性能を表す指標です。メモリタイミングの中で発生する遅延の 1 つで、メモリタイミングの最初の値です。

半導体記憶素子を格子状に並べたメモリは、データの読み書きに、素子の行(row)と列(column)を指定します。レイテンシーは列指定の CAS 信号の発行後データの読み書きが行われるまでにかかる遅延時間(単位はクロック数)で CL=9 などと表します。実際の遅延時間はクロック数との関係で決まります。

計算例 : クロックが 16000Hz、CL=9 の場合の遅延時間

$$(1/16000) \times 9 = 0.0005625\text{sec}$$

CAS レイテンシーの異なるメモリを混在させて装着すると、動作は遅い方(遅延の大きい方)に合わされます。

1.2.2.7. メモリペアリング

メモリのペアリングは、チップスペアリング(またはチップスキル)と呼ばれ、ECC ではダウンが避けられない DRAM チップの故障に対し、データを 1 ビットずつ異なる DRAM に分散保存し、1 つの DRAM チップが故障した場合に大量の 1 ビットエラー発生として扱い ECC を使ったエラー訂正を可能にする技術です。

ただし、2 つの DRAM が同時に故障するとチップスペアリングでもシステムダウンします。ダブルチップスペアリングは、2 つの DRAM の同時故障でもシステムダウンしないように

改良を加えた技術で、メモリ障害によるサーバー停止の発生を低減します。

1.2.3. 拡張スロット

機能拡張カードを接続するための拡張バスと拡張カードスロットには様々な規格がありますが、代表的な規格として PCI 、 PCI-X 、 PCI-E(PCI Express) が挙げられます。ビットレート(最大転送速度/帯域幅)などの特徴は次の表のようになります。

拡張バス	特徴	
PCI	Peripheral Components Interconnect Intel 社の提唱したパラレル入出力バス規格。 Windows のプラグアンドプレイ機能に対応。 3.3V または 5V で動作する。(スロットの切れ込み位置が異なる) ユニバーサル(ユニバーサリー)カードは 3.3V/5V の両方で動作する。(両方の切れ込みがある) チップセットに接続される。	
	PCI 33 動作クロック 33MHz 規格 (初期)	PCI 33, 32 bit データバス幅 : 32 ビット、最大データ転送速度 : 133 MB/s PCI 33, 64 bit データバス幅 : 64 ビット、最大データ転送速度 : 266 MB/s
	PCI 66 動作クロック 66MHz 規格 (後期)	PCI 66, 32 bit データバス幅 : 32 ビット、最大データ転送速度 : 266 MB/s PCI 66, 64 bit データバス幅 : 64 ビット、最大データ転送速度 : 533 MB/s
PCI-X	Peripheral Component Interconnect-X。Intel を除いた PC メーカーが主導で立ち上げ、後に Intel も参加し策定された規格。PCI を継承し高速化したパラレル入出力バス規格。 3.3V の PCI との互換性を維持している。(ユニバーサルカードを含む) 最大転送速度(帯域幅)は 4.26GB/s PCI-X バスに PCI カードを装着可能。 PCI バスに PCI-X カードを装着した場合、動作モードは PCI に限定される。 チップセットに接続される。	
PCIe	PCI-Express シリアル入出力バス規格 PCI/PCI-X との互換性はない レーンを複数たばねて使用し、低レイテンシ(遅延)と高帯域幅を可能とする x1、x2、x4、x8、x16、x32 などの仕様がある 8b/10b エンコーディングするため理論値と実効値がある PCI Express スロット CPU に直接接続される。	
	世代	帯域幅
	Gen1 (Ver1.0/.1)	理論値 x1: 2.5Gb/s x8: 20Gbps, 2.5GB/s x16: 40Gbps, 5GB/s x32: 80Gb/s, 10GB/s 実効値 x1: 2.0Gb/s x8: 16Gbps, 2.0GB/s x16: 32Gbps, 4GB/s x32: 64Gb/s, 8GB/s
	Gen2 (Ver2.0)	理論値 x1: 5Gb/s x8: 40Gbps, 5GB/s x16: 80Gbps, 10GB/s x32: 160Gb/s, 20GB/s 実効値 x1: 4Gb/s x8: 32Gbps, 4GB/s x16: 64Gbps, 8GB/s x32: 128Gb/s, 16GB/s
	Gen3 (Ver3.0)	理論値 x1: 10Gb/s x8: 80Gbps, 10GB/s x16: 160Gbps, 20GB/s x32: 320Gb/s, 40GB/s 実効値 x1: 8Gb/s x8: 64Gbps, 8GB/s x16: 128Gbps, 16GB/s x32: 256Gb/s, 32GB/s

表 1.18.拡張カードの種類

PCI 、 PCI-X 、 PCI-E(PCI Express) の拡張スロットの形状の相違を次の図に示します。

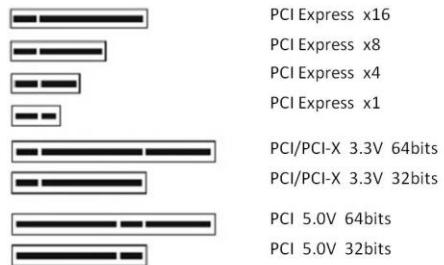


図 1.13. 拡張スロットの形状の違い

1.2.4. NIC

NIC(ネットワークインターフェースカード/Network Interface Card)は、ネットワークとの接続機能を提供します。

LANが普及した当初は、マザーボード上に搭載されておらず機能拡張カードとして提供されたため「NIC」と呼ばれますが現在は、オンボードで提供されることが一般的です。

サーバー専用機では、ネットワークとの接続を冗長構成にするために2つ以上のNICインターフェースを持つ場合があります。

1.2.5. ハードディスク

ハードディスクドライブ(HDD/Hard Disk Drive)は、補助記憶装置の一種で、磁性体を塗布した円盤を高速に回転させ、磁気ヘッドを移動させることで、情報の読み出し/書き込みを行います。

ディスクを回転させる、ヘッドを移動させるなどの機械的な可動部分を持つため、コンピューターの他の部品に比べ情報の読み書きには時間がかかります。コンピューター本体内のベイに装着する内蔵型と外部に置く外付け型がありますが、一般的なサーバーでは少なくとも内蔵型を1台装着し、ブートローダー、OSが記録されています。



図 1.14. ハードディスク

ホットスワップ対応のディスクは電源を入れたまま安全に脱着することができます。

1.2.6. ライザーカード

ライザーカードは、拡張スロットを搭載した機能拡張カードです。1U のラックマウントサーバーのマザーボードに機能拡張カードを装着した場合、PC の厚さよりもカードが高くなり蓋が閉まらなくなるため、背の低いライザーカードを垂直に差し、そこに機能拡張カードをマザーボードと平行に装着することで装着を可能にします。



図 1.15. ライザーカード(1U のラックマウント型サーバー用)

複数の機能拡張カードが同時に機能しない状態になった場合は、ライザーカードが故障している可能性があります。

1.2.7. RAID コントローラー

RAID コントローラーは、複数のディスク装置をあたかも一台の装置であるかのように扱う回路で、機能拡張カードやオンボードの形で提供されます。RAID コントローラーを使用する RAID システムは、ハードウェア RAID と呼ばれます。

RAID コントローラーは、専用のユーティリティソフトウェアを使用して、様々な RAID 構成を管理者が設定します。RAID コントローラーは、接続されている全てのディスク装置を直接制御しており、OS に代わってディスクの詳細を掌握しています。

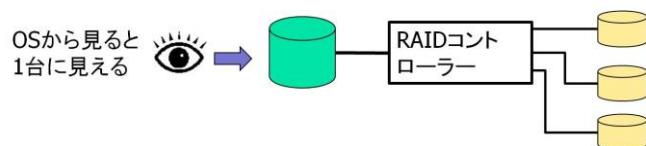


図 1.16. ハードウェア RAID コントローラーの役割

OS は RAID コントローラーにより管理されている論理ドライブを、あたかも物理ディスクであるかのように扱います。RAID コントローラーは RAID レベル 5 と 6 では CPU に代わりデータ復元のための情報となるパリティを計算し、CPU のパリティ計算の負荷を下げるすることができます。

1.2.8. ファームウェア

ファームウェアは、コンピューターなどの機器内部に固定的に組み込まれるソフトウェアで、基本的な入出力を行う BIOS や、アレイコントローラー、SAS ハードディスクドライブ、NIC の制御、高機能な設定プログラム(ユーティリティプログラム)機能などを提供します。ハードウェアに格納されているためファーム(硬い/firm)ウェアと呼ばれます。

一般的に機器本体や機能拡張カードに内蔵、搭載される ROM(書き換え可能なフラッシュリードオンリーメモリ)など、電源を切っても内容の消えないメモリ(不揮発メモリ)に記録されます。

フラッシュ ROM に記録されるファームウェアは、新しいファームウェアが配布された場合に内容を更新/修正することができます。

1.2.9. BIOS/UEFI

BIOS(バイオス ; Basic Input/Output System)は、機器の基本的な入出力処理を行うためのプログラムで、ROM に搭載されているファームウェアの一種です。

UEFI(ユーティリティ/Unified Extensible Firmware Interface)または EFI は、従来の BIOS インターフェースに代わる OS とファームウェアとの間のソフトウェアインターフェースを定義する仕様で、業界団体 Unified EFI Forum の下で開発が進められています。(UEFI の基となった EFI は、インテルと HP の共同開発です。)

1.2.9.1. CMOS バッテリー

BIOS の設定内容は CMOS に保存され、電源を切ってしても内容はリチウムイオン電池でバックアップされ維持されます。CMOS に保存された BIOS の設定内容を CMOS セットアップと呼びます。



図 1.17. CMOS バッテリー

1.2.10. USB インターフェース/ポート

USB 接続用のコンポーネント。ディスク、NIC、HID デバイスなどを接続するために使用されます。

バージョン	最大データ転送速度	インターフェースの色
USB2.0	480Mbps	黒
USB3.0	5Gbps (5120Mbps)	青

表 1.19. USB2.0 と 3.0

1.2.11. ホットスワップ対応コンポーネントとホットスワップ非対応コンポーネントの違い

ホットスワップ(hotswap)は、電源を入れたままでコンポーネントを脱着できる機能で、活線挿抜とも呼ばれます。ハードディスクやメモリなどホットスワップ対応の機器は、無停止性が要求されるサーバーで、コンピューターを停止せずに故障したコンポーネントの取り外しや交換が可能です。

ホットスワップ未対応の機器は、一旦 OS をシャットダウンし機器の電源をオフにした後でないと、故障したコンポーネントの取り外しや交換ができません。

ホットプラグ(hotplug)は、電源を入れたままの機器に新しいコンポーネントを装着した時に、OS に自動認識され、必要なドライバーが組込まれて使用可能になる機能ですが、ホットスワップの別称としても使用されます。