

実務に役立つ サーバー運用管理の基礎

CompTIA

Server+

テキスト

SK0-004対応



TAC

目次

序章 本書の前提条件

本書の前提知識	2
---------------	---

第1章 サーバースystem基礎

1-1 サーバーとは何か	7
1-1-1 コンピュータシステム	8
1-1-2 サーバーの役割	11
1-1-3 サーバーの形状 (筐体)	17
1-2 サーバアーキテクチャー	21
1-2-1 CPU	22
1-2-2 メモリ	32
1-2-3 マザーボード	43
1-2-4 拡張バス・拡張カード	48
1-2-5 BIOS/UEFI	56
1-2-6 電源ユニット	61
1-2-7 サーバラック	66

第2章 サーバースystemを支える技術

2-1 ネットワーク技術	77
2-1-1 通信プロトコル	78
2-1-2 ネットワークインターフェース層	84
2-1-3 インターネット層 (ネットワーク層)	94
2-1-4 トランスポート層	103
2-1-5 アプリケーション層 (上位層)	106
2-2 ストレージ技術	117
2-2-1 ストレージの種類と特徴	118
2-2-2 ストレージの実装とインターフェース	123
2-2-3 ストレージの選定基準	130
2-2-4 サーバからのストレージ利用	133

2-2-5	RAID	139
2-2-6	サーバーとストレージの接続形態	148
2-2-7	NAS	152
2-2-8	SAN	155
2-3	仮想化技術	165
2-3-1	仮想化技術	166
2-3-2	サーバー仮想化とハイパーバイザー	168
2-3-3	仮想マシンとネットワーク	172
2-3-4	サーバー仮想化における留意点	180
第3章	サーバーシステムの導入	
3-1	導入計画	189
3-1-1	サーバーシステムの導入とライフサイクル	190
3-1-2	サーバーシステムの基本計画(要件定義)	194
3-1-3	サーバー設計時の留意点	200
3-1-4	ストレージ設計時の留意点	205
3-1-5	ネットワーク設計時の留意点	209
3-2	事業継続計画	215
3-2-1	事業継続計画	216
3-2-2	予備サイト	219
3-2-3	バックアップとレプリケーション	221
3-3	サーバー利用環境	225
3-3-1	サーバーラックの導入	226
3-3-2	UPS	232
3-3-3	サーバーシステムの冷却	239
3-3-4	環境管理	242
3-3-5	物理的セキュリティ	250
3-4	サーバーOSのセットアップ	255
3-4-1	サーバーのセットアップ	256
3-4-2	手動インストールと自動インストール	262
3-4-3	サーバーのセキュリティ対策	265
3-4-4	ネットワークのセキュリティ対策	270
3-4-5	ストレージのセキュリティ対策	277

3-4-6	サーバーの高可用性対策	283
-------	-------------	-----

第4章 サーバースステムの運用管理

4-1	サーバースステムの運用管理	295
4-1-1	サーバーの運用管理	296
4-1-2	構成管理・資産管理	298
4-2	モニタリング	301
4-2-1	モニタリング	302
4-2-2	サーバーモニタリング項目	304
4-2-3	代表的なシステム監視技術	306
4-2-4	モニタリングソフトウェアの活用	308
4-2-5	OSによるリモート管理	311
4-3	ソフトウェアメンテナンス	315
4-3-1	ソフトウェアメンテナンス	316
4-3-2	バックアップ	318
4-4	ハードウェアメンテナンス	325
4-4-1	ハードウェアメンテナンス	326
4-4-2	ハードウェア監視技術	328
4-4-3	データの破棄	330

第5章 トラブルシューティング

5-1	トラブルシューティングの考え方	337
5-1-1	トラブルシューティングの必要性	338
	トラブルシューティングの手順	339
5-2	ハードウェアトラブルの例	345
5-2-1	ハードウェア障害の例	346
5-2-2	環境	349
5-3	ソフトウェアトラブルの例	355
5-3-1	ソフトウェアトラブルの例	356
5-4	ネットワークトラブルの例	363

5-4-1	ネットワークトラブルの例	364
5-5	ストレージトラブルの例	369
5-5-1	一般的なストレージ障害例	370
5-5-2	ストレージアレイ側での障害例	373
5-6	セキュリティトラブルの例	377
5-6-1	セキュリティトラブルの例	378
5-7	トラブルシューティングのためのツール	383
5-7-1	ハードウェア診断ツール	384
5-7-2	コマンドの活用	386
5-7-3	システムツールの活用	392
5-7-4	セキュリティツール	395

学習にあたり

本書の使い方

これから Server+ (SK0-004) 試験を受験する方は、本書を最初から順番に読み進めていくことをおすすめします。興味のある章から読むこともできますが、知識を体系的に学習しやすいように本書は構成されています。

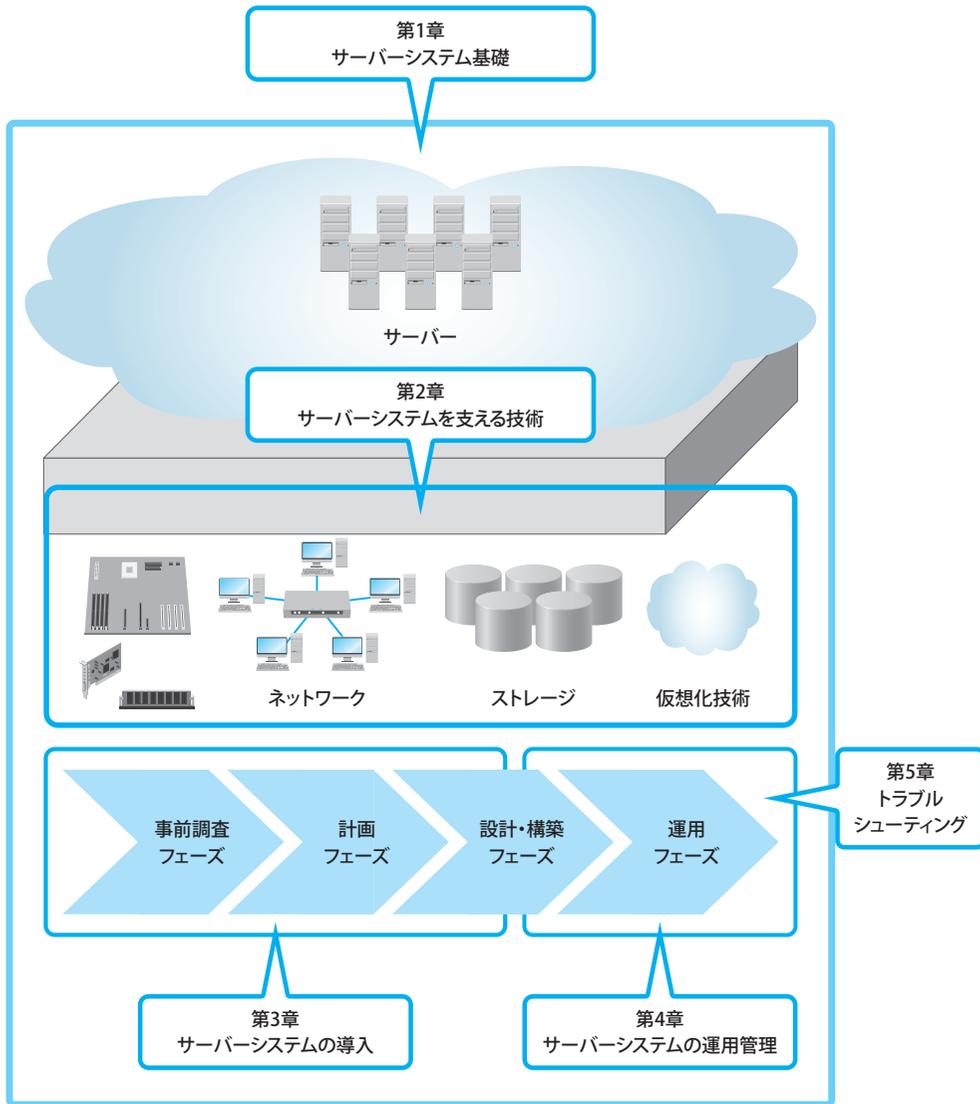
本書では学習した内容の理解度を確認するため、セクションごとにポイントをまとめた確認問題を、章末には章末問題を用意しました。

本書の構成

- ・ 本書は章・節・項目に分けて構成されています。
- ・ 各章の初めには、「この章で学ぶこと」と、その章で学習する節のタイトルが表記されています。「この章で学ぶこと」には章全体で学習する内容がまとめられているので、最初にその章で学習する内容の全体像を把握しましょう。
- ・ 各節の初めには、その節内で学ぶ項目のタイトルが表記されています。
- ・ 節の初めには、「学習ポイント」があげられています。ポイントを掴み、効率よく学習を進めてください。
- ・ 重要な部分は、**太字**で表記されています。
- ・ 欄外には、本文中の※印の付いた語句についての補足説明が記載されています。より深い理解に役立ちます。
- ・ 節ごとに穴埋め式の確認問題があります。学習した内容の習得度を確認できます。
- ・ 章末には選択式の章末問題があります。

※ 難しい英語名称は名称の後のカッコ()内に、読み方とフルスペルを表示しています。
複数の読み方がある場合については、一般的なものを表示しました。

Server+ テキストの全体像



序章

本書の前提条件

この章で学ぶこと

本書の前提条件である知識を確認しましょう。

序-1 本書の前提知識

序-1 本書の前提知識

本書では、CompTIA A+とCompTIA Network+の資格をお持ちの方、またはそれらと同等の知識をお持ちの方を前提に、サーバー業務を行うITエンジニアが必要とする知識を体系的に説明しています。

また、本書はPCやネットワークに関する解説を副次的に行うことはあっても、それを主体とはしていません。そのため、次の関連用語について事前にご確認いただき、不明なものがあれば、本書での学習の前に内容を確認しておくことをお勧めします。

用語	CompTIAテキスト対応
・MBR (Master Boot Record)	A+ 電源ユニット/BIOS
・LDAP	A+ プロトコル
・イントラネットとエクストラネット	Network+ ネットワークの基礎知識
・VLAN	Network+ ネットワークデバイス
・SSL/TLS	Network+ 上位層のプロトコル
・ファイアウォール ・ネットワークベース ・ホストベース ・ポートセキュリティ ・ルーターアクセスリスト (ACL) ・DMZ (DeMilitarized Zone)	Network+ セキュリティ対策
・秘密鍵 ・公開鍵 ・PKI (Public Key Infrastructure) ・認証局 (Certificate Authority) ・IEEE802.1x ・RADIUS ・TACACS ・TACACS+	Network+ 暗号化と認証
・VPN ・IPsec	Network+ リモートアクセスとVPN
・NAC (Network Access Control) ・パブリックとプライベート	Network+ ネットワーク設計に必要な知識

※表中の用語とテキスト対応は、本書のシリーズ刊とのものです。また、対応に変更がある場合には、次のWebページにてご案内します。

http://www.tac-school.co.jp/it/comptia/comptia_seigo.html

次の に当てはまる言葉を答えてください。

- 1. コンピューター起動時には起動ドライブの ① にアクセスし、ブートストラップコードが実行されます。
- 2. ② は、通信プロトコルTCP/IPなどのインターネットの標準技術を利用し、社内や組織内に構築したネットワークです。
- 3. ファイアウォールには、コンピューター上で動作する ③ とネットワーク上で動作する ④ があります。
- 4. ⑤ はCisco Systems社が独自に拡張した認証プロトコルです。
- 5. 公開鍵暗号方式は ⑥ と ⑦ のペアを作成し、 ⑥ だけを公表します。

答え

①MBR②イントラネット③ホストベース④ネットワークベース⑤TACACS+⑥公開鍵⑦秘密鍵

章末問題

Q₁

ブラウザを利用して安全な買い物をする場合に利用されるプロトコルは、次のうちどれですか。

- a. IPSec
- b. SSL
- c. NetBEUI
- d. DMZ

A

b

ブラウザで安全な通信を行う際に利用されるのがSSL (Secure Socket Layer) です。IPSec (Security Architecture for Internet Protocol) もセキュアプロトコルですが、VPNで使用されます。

NetBEUI (NetBIOS Extended User Interface) は、Windowsで使われていたプロトコルです。

DMZ (DeMilitarized Zone) は、ファイアウォールによって外部ネットワークからも内部ネットワークからも隔離されたセグメントのことです。

Q₂

あらかじめ設定しておいたルールに基づいて、フィルタリングを行うセキュリティ装置は、次のうちどれですか。

- a. ファイアウォール
- b. MBR
- c. ハブ
- d. PKI

A

a

ファイアウォールの基本的な機能の1つがフィルタリングです。フィルタリングは、IPアドレスやプロトコル、ポート番号、接続時間など、あらかじめ設定しておいたルールに基づいて、そのパケットを通過させてよいかどうかを判断する機能です。

MBR (Master Boot Record) は、ハードディスクにある起動に関する情報のことです。

ハブは、複数のコンピューターからのケーブルをまとめて接続する集線装置です。

PKI (Public Key Infrastructure) は、公開鍵基盤とも呼ばれる公開鍵暗号を安全に利用できるようにする仕組みのことです。

第1章

サーバーシステム基礎

この章で学ぶこと

本章では、サーバーを理解する上でベースとなるサーバーシステム基礎について学習します。

サーバーとは何か、サーバーの役割やサーバーハードウェア、そして、サーバーを格納するラックなどについて学習していきましょう。

1-1 サーバーとは何か

1-2 サーバーアーキテクチャー

1-1

サーバーとは何か

1-1-1 コンピューターシステム

1-1-2 サーバーの役割

1-1-3 サーバーの形状 (筐体)

学習ポイント

ここでは、コンピューターシステムの定義と、その代表的な処理形態であるホスト集中型システム、クライアントサーバー型システムの概要を解説します。

1 コンピューターシステム

私たちが普段から何気なく使っている「システム」という語句は、本来「個々の要素が有機的に組み合わされた体系」、「まとまりをもつ全体像」、「組織」、「体制」といった意味を持ちます。そして、近年の社会、企業活動では、コンピューターやネットワークは必要不可欠な存在であり、それらによって形成したシステムは、**コンピューターシステム**または**情報システム**と呼ばれています。すなわち、コンピューターシステムは、基本的に単体で存在するものではなく「各コンピューターを構成するハードウェアやソフトウェア、そしてネットワーク（ネットワーク機器、回線、プロトコル）などの構成要素が、情報を適切に処理するために有機的に結びつき、目的を達成するために構成されたシステム、または、その運用管理体制までを含んだ全体像」と定義することができます。

2 コンピューターシステムの処理形態

コンピューターシステムを構成するコンピューター群が、データを処理する形態は、大きく**ホスト集中型**と**クライアントサーバー型**に分類されます。

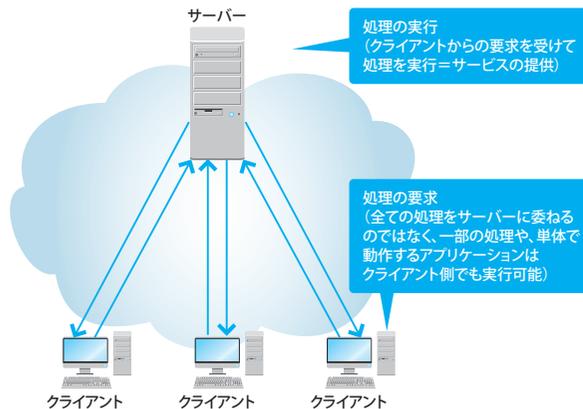
● ホスト集中型システム

ホスト集中型のシステムでは、処理すべきデータやアプリケーション（プログラム）のほぼすべてがホストコンピューターに格納されます。これにより、端末側は、ホスト側から送信された情報（文字コード）を表示したり、データを入力したりする入出力の機能しか持たなくてもよくなります。ホスト集中型システムは、すべてのデータやプログラムがホストによって一元管理でき、運用保守などが行いやすい利点があります。しかし、例えばデータベースを用いるシステムを稼働させた場合、データベースそのものも、データベースに対して検索、更新などを行う基本的なアプリケーション機能もホスト側に実装することになります。いうまでもなく、これはホストに相当な負荷を強いることになります。

● クライアントサーバー型システム

コンピューターシステムが企業などで利用され始めた当初は、メインフレームや汎用機と呼ばれるホストコンピューターを中心として、ホスト集中型が広く普及しました。当時はPCを含め端末の性能が低く、また高速なネットワーク回線などのインフラ環境も整っていなかったためです。しかし、1990年以降は、PCの性能が飛躍的に向上し、LANやインターネットの普及も進みました。これにより、すべての処理をホストに任せるのではなく、ネットワークと各PCの性能を活用することで、効率的な分散処理を実現する、クライアントサーバー型システムが徐々に浸透していきました。

クライアントサーバー型システムでは、システム処理を、要求を実行する側と、要求を出す側とで機能分担し、効率的に処理していきます。このとき、要求を実行する側が、特定のサービスを提供する**サーバー** (Server)、そして要求を出す側が、そのサービスを利用する**クライアント** (Client) です。そしてクライアントは、かつてホスト集中型が普及していた時代の「単なる表示端末」とは異なり、それ自身に基本的な処理性能を持ちます。そのため、データベースを用いるシステムを稼働させる場合も、それを実現するためのアプリケーション機能の一部を実装した上で、サーバーと連携しながら、効率的な情報処理を可能にしています。



クライアントサーバー型システム

また、サーバーも、1台だけでその処理や機能を実現する必要はなく、処理に応じて複数のサーバーを用意し、適宜連携させることで、大規模な演算や複雑な業務処理に対応できるようにしています。なお、クライアントサーバー型のシステムは、記述上C/S型などと省略表記されることがありますが、本書では、これ以降、サーバーシステムと表記していきます。

3 サーバーシステムの発展

近年では、モバイル環境などのネットワークを含めたインフラ環境が一層整備され、サーバーシステムは、PCだけでなく、スマートフォンやタブレットからの利用（マルチデバイス対応）が一般的になりつつあります。

また、サーバーシステム自体も、Webシステム（「1-1-2」で説明）は当たり前ものとなり、その構築方法も、オンプレミス（on-premise）^{*}だけでなく、クラウドを活用する動きが進んでいます。加えて、オンプレミス、クラウドに関わらず、サーバー構築には、仮想化技術の導入が浸透し、システムの再利用性や可用性を高める動きが進んでいます。仮想化技術の詳細は、「2-3」で解説します。

オンプレミス

コンピューターシステムを保有し、自社組織内の設備で運用する形態。オンプレミスは、サーバー構築の自由度に大きなメリットがあるものの、原則自社内で調達、構築、運用する必要があり、サーバー構築の迅速性や再利用性という点からはクラウド利用に劣るとされることが多い。