



## CompTIA Cloud+ 試験出題範囲

試験番号: CV0-001

CompTIA Cloud+認定資格は、クラウドコンピューティングの環境において、設計・構築、保守・運用を実施される IT エンジニアの方に必要なスキルと知識を証明するワールドワイドの認定資格です。

CompTIA Cloud+認定資格の取得者は、一般的なクラウドの用語と方法論を理解し、クラウド環境の実装、保守・運用、およびクラウド技術とインフラ(サーバーやネットワーク、ストレージ、仮想化技術など)を提供するために必要とされるスキルと知識を習得していることが証明されます。また、セキュリティを考慮し、クラウド環境や仮想化アプリケーションを IT 業界のベストプラクティスとされている方法を用いて実装できるスキルが証明されます。

CompTIA Cloud+認定資格試験の受験者の方は、下記のような方が取得されることをお勧めしています。

- CompTIA Network+/CompTIA Storage+ Powered by SNIA を取得されている方。(CompTIA 認定資格の取得は、受験の際の必須条件ではありません。)
- IT ネットワーク、ネットワークストレージ、データセンター管理者などのネットワークに関連した職務での業務経験を少なくとも 24~36 か月経験されている方。
- ハイパーバイザーなどの仮想サーバー技術に精通をされている方。(各ベンダーから提供されている認定資格の取得は、受験の際の必須条件ではありません。)

以下は試験分野および各分野の出題比率表です。

試験分野	出題比率
第1章 クラウドのコンポーネントとモデル	12%
第2章 仮想化	19%
第3章 インフラストラクチャ	21%
第4章 リソースマネジメント	13%
第5章 セキュリティ	16%
第6章 システムマネジメント	11%
第7章 クラウドを活用した事業継続	8%
合計	100%

分野別に取扱例があげられていますが、これらがすべての出題傾向を網羅しているわけではありません。また、この出題範囲に掲載がない場合でも各分野に関連する技術、プロセス、あるいはタスクについて、試験に含まれる可能性があります。本出題範囲は、予告なく変更される場合がございます。あらかじめご了承ください。

CompTIA では、提供している認定資格試験の内容にて現在必要されているスキルを反映するため、また試験問題の信頼性維持のため、定期的な改訂を行っています。必要な場合、現在の出題を基に試験を改訂する場合があります。この場合、現在の試験に関連する資料・教材等は、継続的にご利用いただくことが可能です。

## 第 1 章 クラウドのコンポーネントとモデル(12%)

### 1.1 それぞれのクラウドサービスを比較対照できる。

- SaaS (NIST 定義による)
- IaaS (NIST 定義による)
- CaaS
- PaaS
- XaaS
- DaaS
- BPaaS
- サービスモデルの違いによるアカウントビリティ(Accountability)と責任(Responsibility)

### 1.2 それぞれのクラウド運用モデルとサービスを比較対照できる。

- プライベート(Public)
- パブリック(Public)
- ハイブリッド(Hybrid)
- コミュニティ(Community)
- オンプレミスとオフプレミスのホスティングの違い
- 運用モデルの違いによるアカウントビリティ(Accountability)と責任(Responsibility)
- モデルの違いによるセキュリティ
  - ・ マルチテナント方式
  - ・ データ分散
  - ・ ネットワーク分離
  - ・ 法律や法令の確認
- 選択した運用モデルから機能とパフォーマンスを検証する
- オーケストレーションプラットフォーム

### 1.3 クラウドの特徴や用語を要約することができる。

- 伸縮性(Elasticity: エラスティシティ)
- オンデマンド・セルフ・サービス/ジャスト・イン・タイム
- Pay-as-you-grow
- チャージバック
- ユビキタス
- リソースプールの測定
- マルチテナント
- クラウドバースティング
- Rapid deployment (ラピッドディプロイメント)
- オートメーション

### 1.4 ストレージコンポーネントの目的を説明することができる。

- Object ID
- メタデータ
- Blob データ
- 拡張メタデータ
- ポリシー
- レプリカ
- アクセスコントロール

## 第 2 章 仮想化 (19%)

### 2.1 それぞれのハイパーバイザー、およびクラウドのタイプを説明することができる。

- Type1 と Type2
  - ・ ベアメタル型とホスト OS 型の違い
  - ・ パフォーマンスとオーバーヘッドの検討
  - ・ ハイパーバイザー型での特別なシステム要件
- プロプライエタリとオープンソースの違い
- 一般ユーザーと法人ユーザーの違い
  - ・ ワークステーションとインフラストラクチャの利用

### 2.2 仮想化マシンやデバイスのインストール、設定、管理を行うことができる。

- テンプレートの作成、インポート、エクスポートと仮想マシン
- ゲストツールのインストール
  - ・ ドライブ
  - ・ 管理ツール
- スナップショットとクローニング
- イメージバックアップとファイルバックアップ
- 仮想 NIC
  - ・ 仮想化ネットワーク
  - ・ IP アドレス
  - ・ デフォルトゲートウェイ
  - ・ ネットマスク
  - ・ ブリッジング
- 仮想ディスク
  - ・ Limits
  - ・ SCSI/ATA ID
- 仮想スイッチ. Virtual switches
  - ・ VLAN
  - ・ インターフェース設定
- VLAN
  - ・ ID の割り当て
  - ・ インターフェースの結合
- VSAN
  - ・ ID の割り当て

### 2.3 特定のシナリオを想定し、仮想リソースの移行を実行することができる。

- 各種要件の定義
- メンテナンススケジュール
- 移行動機
  - ・ パフォーマンスの問題
  - ・ テスト
  - ・ アップグレード
  - ・ 利用 (Utilization)
- ストレージの移行
  - ・ 仮想的と物理的の違い
- オンラインとオフライン間の移行
- Physical to Virtual (P2V)

- Virtual to Virtual (V2V)
- Virtual to Physical (V2P)

#### 2.4 クラウド環境の仮想化によるメリットを説明することができる。

- リソースのシェア/シェアードリソース
- エラスティシティ (Elasticity)
  - ・ 時間ごとのサービス/実施までの平均期間
  - ・ リソースのプール
  - ・ 拡張性
  - ・ 可用性
  - ・ 移行性
- ネットワークとアプリケーションの分離
- インフラ・コンソリデーション
- 仮想データセンターの作成

#### 2.5 クラウド環境を構築するために必要な仮想化コンポーネントを比較対照することができる。

- 仮想ネットワークコンポーネント
  - ・ 仮想 NIC
  - ・ 仮想 HBA
  - ・ 仮想ルーター
- 共有メモリー
- 仮想 CPU
- ストレージの仮想化
  - ・ 共有ストレージ
  - ・ クラスタ化されたストレージ
  - ・ NPIV

## 第3章 インフラ(21%)

### 3.1 それぞれのストレージテクノロジーを比較対照することができる。

- NAS(Network Attached Storage)
  - ・ ファイルレベルのアクセス
  - ・ 共有ストレージ
- DAS(Direct Attached Storage)
  - ・ ブロックレベルのアクセス
  - ・ 専用ストレージ
- SAN(Storage Area Network)
  - ・ ブロックレベルのアクセス
  - ・ 共有ストレージ
  - ・ HBA
  - ・ LUN マスキング
  - ・ ゾーンニング
  - ・ WWN
  - ・ ファイバーチャネルプロトコル
- さまざまなアクセスプロトコル
  - ・ FCoE
  - ・ FC
  - ・ イーサネット
  - ・ iSCSI
- プロトコルとアプリケーション
  - ・ IP
  - ・ FCP
  - ・ iSCSI
- 管理方法の違い

### 3.2 ストレージ設定の概念を説明することができる。

- ディスクタイプ
  - ・ SSD とスピニングを比較する
  - ・ インターフェースのタイプ
  - ・ アクセススピード
- 階層化
  - ・ 各階層のパフォーマンスレベル
  - ・ ポリシー
- RAID レベル
  - ・ RAID 1
  - ・ RAID 0
  - ・ RAID 1+0
  - ・ RAID 0+1
  - ・ RAID 5
  - ・ RAID 6
- ファイルシステムの種類
  - ・ UFS
  - ・ EXT
  - ・ NTFS
  - ・ FAT

- ・ VMFS
- ・ ZFS

**3.3 ストレージのプロビジョニングを実行することができる。**

- LUN の作成
- 共有ネットワークの作成
- ゾーンニングと LUN マスキングの設定
- マルチパスの設定
- NAS と SAN の容量を追加する
  - ・ オペレーションへのインパクト
  - ・ ダウンタイム
  - ・ ベストプラクティス

**3.4 あるシナリオを想定した上で、適切なネットワークの設定を実行することができる。**

- NAT
- PAT
- サブネッティング/スーパーネッティング
- VLAN と VLAN タギング
- ネットワークポートの設定
- 物理的、または仮想環境でのスイッチとルーターの設定
  - ・ ルーティングテーブル

**3.5 ネットワークの最適化の重要性を説明することができる。**

- WAN
- LAN
- MAN
- 帯域幅
- レイテンシー(遅延)
- 圧縮
- キャッシング
- ロードバランシング
- 同じサブネット上のデバイス

**3.6 特定のシナリオを想定し、基本的なネットワークの接続に関するトラブルシューティングを実行することができる。**

- ツール
  - ・ ping
  - ・ tracert/traceroute
  - ・ telnet
  - ・ netstat
  - ・ nslookup/dig
  - ・ ipconfig/ifconfig
  - ・ route
  - ・ arp
- ドキュメントとデバイスの設定の確認
- システムログの確認

### 3.7 一般的なネットワークプロトコル、ポート、トポロジーを説明することができる。

- トランクポート
- ポートバインディング/アグリゲーション
- Well-known ポート
  - ・ 80
  - ・ 21
  - ・ 22
  - ・ 25
  - ・ 53
  - ・ 443
  - ・ 68
- Well-known プロトコル
  - ・ HTTP
  - ・ FTP
  - ・ HTTPS
  - ・ FTPS
  - ・ SFTP
  - ・ SSH
  - ・ DNS
  - ・ DHCP
  - ・ SMTP
- ネットワークのタイプ
  - ・ イン트라ネット
  - ・ エクストラネット
  - ・ インターネット

### 3.8 仮想環境を有効にするために使用される一般的なハードウェアと機能を説明することができる。

- BIOS/ファームウェアの設定
- 最小メモリー容量と構成
- CPU の数
- コアの数
- NIC の数、速度、および設定
- 内部ハードウェアの互換性
- HBA
- ストレージメディア
  - ・ テープ
  - ・ SSD
  - ・ USB
  - ・ ディスク

## 第 4 章 リソースマネジメント(13%)

4.1 あるシナリオを想定した上で、適切なリソースモニタリング技術を選択し、実行することができる。

- プロトコル
  - ・ SNMP
  - ・ WMI
  - ・ IPMI
  - ・ Syslog サービス
- アラート方式
  - ・ SMTP
  - ・ SMS
  - ・ SNMP
  - ・ Web サービス
  - ・ Syslog
- ベースラインとしきい値の確定
- 特定のイベントに対して自動応答を設定
- プロセス使用率/リソース使用率の確認

4.2 あるシナリオを想定した上で、適切な方法論(ベストプラクティス)を使用し、物理的な(host)リソースの割り当てを実行することができる。

- メモリー
- CPU
- ストレージとネットワークの割り当て
- エンタイトルメント/クォーター(共有)
  - ・ ハードリミット
  - ・ ソフトリミット
- 予約
- ライセンス
- リソースプール

4.3 あるシナリオを想定した上で、適切な方法論(ベストプラクティス)を使用し、仮想の(guest)リソースの割り当てを実行することができる。

- 仮想 CPU
- メモリー
- ストレージとネットワークの割り当て
- エンタイトルメント/クォーター(共有)
- ハードリミット、ソフトリミット
- 予約、ライセンス
- 動的リソース割り当て
- リソースプール
- 物理リソースの仮想リソースへのリダイレクトとマッピング
  - ・ シリアル
  - ・ USB
  - ・ パラレルポートマッピング

4.4 あるシナリオを想定した上で、リモートアクセスのための適切なツールを使用することができる。

- リモートハイパーバイザーアクセス
- RDP

- SSH
- コンソールポート
- HTTP

## 第5章 セキュリティ(16%)

5.1 それぞれのネットワークセキュリティコンポーネント、ツール、ベストプラクティスを説明することができる。

- ACL
- VPN
- IDS/IPS ハードウェア/ソフトウェアベースのファイアーウォール
- DMZ
- レビューと監査ログ
- 攻撃の種類
  - ・ DDoS 攻撃
  - ・ Ping of death 攻撃
  - ・ Ping flood 攻撃

5.2 それぞれのストレージセキュリティコンポーネント、ツール、ベストプラクティスを説明することができる。

- 難読化(オブファスケーション)
- アクセスコントロールリスト
- ゾーンニング
- LUN マスク
- ユーザーとホストの認証
- レビューと監査ログ

5.3 さまざまな暗号化技術と方法論の違い比較対照することができる。

- PKI
- IPsec
- SSL/TLS
- Cipher
  - ・ AES
  - ・ 3DES
  - ・ RSA
  - ・ DSA
  - ・ RC4
  - ・ RC5
- 送信中のデータの暗号化と保存されたデータの暗号化

5.4 アクセスコントロールの方法を識別することができる。

- ロールベースアクセス制御(RBAC: Role-based administration)
- 強制アクセス制御(MAC: Mandatory access controls)
- 任意アクセス制御(DAC: Discretionary access controls)
- マルチファクタ認証
- シングルサインオン
- フェデレーション認証

5.5 ゲストとホストを強化する技術を実装することができる。

- 不要なポートやサービスを無効にする
- ユーザーのクレデンシャル(管理認証資格情報)
  - ・ デフォルトパスワードの変更
- ホストベース/ソフトウェアファイアーウォール
- アンチウイルスソフトウェア

- パッチの適用
- デフォルトアカウントの無効化

## 第 6 章 システムマネジメント(11%)

### 6.1 クラウド環境におけるポリシーと手順を説明することができる。

- ネットワークと IP の計画/文書化
- 標準化と文書化の構成
- 変更管理のベストプラクティス
  - ・ 文書化
  - ・ 構成管理
  - ・ 資産管理
  - ・ 承認プロセス
  - ・ バックアウトプラン(切り戻し計画)
- 構成管理
  - ・ CMDB(構成管理データベース)
  - ・ 承認プロセス
  - ・ 構成コントロール
- キャパシティ管理
  - ・ 変更のモニタリング
  - ・ トレンド
- システムライフサイクル管理
- メンテナンスウィンドウ
  - ・ サーバーのアップグレードとパッチの適用

### 6.2 あるシナリオを想定した上で、物理ホストのパフォーマンスを診断、修復、最適化することができる。

- ディスクパフォーマンス
- ディスクチューニング
- ディスクレイテンシー
- ディスクのスワップ領域
- I/O チューニング
- パフォーマンス管理とモニタリングツール
- ベースラインの確立と適切なツールによる文書の作成
- ハイパーバイザー設定のベストプラクティス
  - ・ メモリーバルーニング
  - ・ I/O スロットリング
  - ・ CPU 待ち時間
- 仮想環境における設定変更の影響
- 一般的な障害
  - ・ ディスク障害
  - ・ HBA 障害
  - ・ メモリー障害
  - ・ NIC 障害
  - ・ CPU 障害

### 6.3 ホストとゲストに関連した一般的なパフォーマンスの概念を説明することができる。

- IOPS
- リードファイルとライトファイル
- ファイルシステムのパフォーマンス
- メタデータのパフォーマンス
- キャッシング

- 帯域幅
- スループット(ボンディング/チーミング)
- ジャンボフレーム
- ネットワークレイテンシー
- ホップカウント
- QoS
- マルチパス
- ロードバランシング
- スケーラビリティ
  - ・ 対角スケーリング、垂直スケーリング(スケールアップ)、水平スケーリング(スケールアウト)の違い

#### 6.4 クラウドサービスを展開する際の適切なテスト手法を実行することができる。

- レプリケーションテスト
- レイテンシーテスト
- 帯域幅テスト
- ロードバランシングテスト
- アプリケーションサーバーテスト
- ストレージテスト
- アプリケーション配信テスト
- サービスのパフォーマンステストとアプリケーションのパフォーマンステスト
- ペネトレーションテスト
- 脆弱性評価
- テスト時の職務の分離

## 第7章 クラウドを活用した事業継続(8%)

### 7.1 災害復旧(ディザスタリカバリー)の方式と概念を比較対照できる。

- 冗長化
- フェールオーバー
- 地理的多様性
- フェイルバック
- レプリケーション
- サイトのミラーリング
- ホットサイト
- コールドサイト
- ウォームサイト
- バックアップとリカバリー
- アーカイブとオフサイトストレージ
- レプリケーションの種類
  - ・ 同期
  - ・ 非同期
- RTO
- RPO
- MTBF(平均故障間隔)
- MTTR(平均修復時間)
- ミッションクリティカルな要件

### 7.1 可用性の要件を満たすためのソリューションを展開することができる。

- フォールトトレランス
  - ・ 高可用性
  - ・ ローカルクラスタリング/ジオクラスタリング
  - ・ 非高可用性リソース
- マルチパス
- ロードバランシング

## CompTIA Cloud+ 略語一覧

下記はCompTIA Cloud+認定資格試験で使用される略語の一覧です。受験者は、試験準備の一環として、これら用語を復習し、理解することをお勧めします。

ACL	—	Access Control List
API	—	Application Programming Interface
APM	—	Application Performance Monitor
ATA	—	Advanced Technology Attachment
BCP	—	Bridge Control Protocol
BIA	—	Business Impact Analysis
BIOS	—	Basic Input/Output System
BMR	—	Bare Metal Restore
BPaaS	—	Business Process as a Service
BUN	—	Backup Network
C2C	—	Cloud to Cloud
C2D	—	Cloud to Database
CAB	—	Change Advisory Board
CAN	—	Campus Area Network
CaaS	—	Communication as a Service / Computing as a Service
CAS	—	Content Addressed Storage
CIIS	—	Client Integration Implementation Service
CMDB	—	Configuration Management Database
CNA	—	Converged Network Adapter
COLO	—	Co-Location
COOP	—	Continuity of Operations Plan
CRL	—	Certificate Revocation List
CRM	—	Customer Relationship Management
CSP	—	Content Service Provider
D2C	—	Datacenter to Cloud
DaaS	—	Data as a Service
DAC	—	Discretionary Access Control
DAS	—	Direct Attached Storage
DBaaS	—	Database as a Service
DBMS	—	Database Management Server
DCB	—	Datacenter Bridging
DHCP	—	Dynamic Host Control Protocol
DMZ	—	Demilitarized Zone
DNS	—	Domain Name Service
DRP	—	Disaster Recovery Plan
FC	—	Fibre Channel
FCoE	—	Fibre Channel over Ethernet
FTP	—	File Transfer Protocol
ftps	—	FTP over SSL
GPT	—	GUID Partition Table
GUI	—	Graphical User Interface
HA	—	High Availability
HAV	—	Hardware Assisted Virtualization

HBA	—	Host Bus Adapter
HTTPS	—	Hypertext Transfer Protocol Secure
IaaS	—	Infrastructure as a Service
ICMP	—	Internet Control Management Protocol
IDS	—	Intrusion Detection System
IFCP	—	Internet Fibre Channel Protocol
IPMI	—	Intelligent Platform Management Interface
IPS	—	Intrusion Protection system
IQN	—	Initiator Qualified Name
ISP	—	Internet Service Provider
iSCSI	—	Internet SCSI
ISNS	—	Internet Storage Name Service
JBOD	—	Just of bunch of Disks
L2TP	—	Layer 2 Tunneling Protocol
LAN	—	Local Area Network
LUN	—	Logical Unit Number
MAC	—	Mandatory Access Control
MAN	—	Metropolitan Area Network
MBR	—	Master Boot Record
MDF	—	Main Distribution Facility
MSP	—	Managed Service Provider
MTBF	—	Mean Time Between Failure
MTTF	—	Mean Time To Failure
MTTR	—	Mean Time To Recovery
MTU	—	Maximum Transmission Unit
NAS	—	Network Attached Storage
NFS	—	Network File System
NIS	—	Network Information Service
NNTP	—	Network News Transport Protocol
NOC	—	Network Operations Center
NPIV	—	N_Port ID Virtualization
OLA	—	Operational Level Agreement
OSD	—	Object Storage Device
P2P	—	Physical to Physical
P2V	—	Physical to Virtual
PaaS	—	Platform as a Service
PAT	—	Port Address Translation
PIT	—	Point-in-Time backup or snapshot
QA	—	Quality Assurance
RAID	—	Redundant Array of Inexpensive Disks
RBAC	—	Role-based Access Control
PBX	—	Public Branch Exchange
RDP	—	Remote Desktop Protocol
RIP	—	Routing Information Protocol
RPO	—	Recovery Point Objective
RTO	—	Recovery Time Objectives
SaaS	—	Software as a Service
SAN	—	Storage Area Network
SAS	—	Serial Attached SCSI

SATA	—	Serial ATA
SCSI	—	Small Computer System Interface
SDLC	—	Software Development Life Cycle
SFTP	—	Secure FTP
SLA	—	Service Level Agreement
SNMP	—	Simple Network Management Protocol
SSD	—	Solid State Disk
SSH	—	Secure Shell
SSO	—	Single Sign-On
TCO	—	Total Cost of Operations
TTD	—	Technical Training Device
UAT	—	Universal Access Transceiver
UDP	—	Universal Datagram Protocol
UPS	—	Universal Power Supply
UTA	—	Universal Target Adapter
V2P	—	Virtual to Physical
V2V	—	Virtual to Virtual
VAT	—	Virtual Allocation Table
VCPU	—	Virtual CPU
VLAN	—	Virtual LAN
VM	—	Virtual Machine
VNIC	—	Virtual NIC
VPN	—	Virtual Private Network
VRAM	—	Virtual RAM
VSAN	—	Virtual SAN
Vswitch	—	Virtual Switch
VTL	—	Virtual Tape Library
WAN	—	Wide Area Network
WWNN	—	WorldWide Node Name
WWPN	—	WorldWide Port Name
XaaS	—	anything as a Service

## CompTIA Cloud+学習の際の設備/装置の一覧

\*\* CompTIA Cloud+試験準備のため、CompTIAでは下記のハードウェアとソフトウェアのサンプル一覧を提示しています。トレーニングを実施している企業でも、トレーニングの提供に必要な実機等をご検討いただく際に、ご確認ください。各トピックスの一覧はサンプルのリストであり、すべてを網羅しているわけではありません。

### 機器

- ルーター
- ファイアーウォール
- SAN/NSA/DAS/HBA
- 少なくとも2台のサーバー
- 複数台のPCスイッチ
- タブレットPC/PDA/スマートフォン等

### 予備のパーツ/ハードウェア

- キーボード、マウス、モニター
- CAT6ケーブル
- 予備のドライブ
- 予備のベアメタルサーバー
- 光ファイバーケーブル
- 予備のHBA
- 予備のCD/DVD

### ツール

- ドライバー
- クリンピングツール
- Server administrative software tools

### ソフトウェア

- ネットワークスニッファー
- ポートスキャナー
- ハイパーバイザー (Type1、Type2)
- クライアントとサーバーのOS
- 複数種のインターネットブラウザ
- ハイパーバイザー管理ソフトウェア
- データベースソフトウェア
- ネットワーク管理ソフトウェア

### その他

- インターネットアクセス
- クラウドサービスプロバイダーへの外部からのアクセス (無料サービス)
- 管理ツール (Adminパック)
- セルフサービスポータル