



# CompTIA Cloud+

## 認定資格試験出題範囲

試験番号 : **CV0-002**



# About the Exam

CompTIA Cloud+認定資格は、クラウドコンピューティング環境で働くITエンジニアに必要な知識を評価する国際的に認知された認定資格です。CompTIA Cloud+試験は、以下の必要な知識とスキルを証明します。

- ・ 標準的なクラウド手法を理解する
- ・ クラウドテクノロジー（ネットワーク、ストレージ、仮想化テクノロジーなど）を実装、保守、提供する
- ・ ITセキュリティについて理解し、クラウドの実装に関連する業界のベストプラクティスを使用する

CompTIA Cloud+認定資格試験は、以下を目安に設計されています。

- ・ CompTIA Network+認定資格および/またはCompTIA Server+認定資格相当の知識とスキル（CompTIA Cloud+を受験の際の必須要件ではありません）
- ・ ITネットワーク、ネットワークストレージ、またはデータセンター管理における24～36ヶ月以上の業務経験
- ・ サーバー仮想化のための主要なハイパーバイザー技術に精通している（仮想化に関するベンダー認定資格を取得している必要はありません）
- ・ クラウドサービスモデル（IaaS、PaaS、SaaS）の定義の理解
- ・ 一般的なクラウド展開モデル（プライベート、パブリック、ハイブリッド）の定義の理解
- ・ パブリックIaaSクラウド環境での業務経験

## 試験開発

CompTIA認定資格試験は、ITプロフェッショナルに必要とされるスキルと知識に関して検討する、専門分野のエキスパートによるワークショップ、および業界全体へのアンケート調査結果に基づいて策定されています。

## CompTIA認定教材の使用に関するポリシー

CompTIA Certifications, LLCは、無許可の第三者トレーニングサイト（通称「ブレインダンプ」）とは提携関係がなく、これらが提供するいかなるコンテンツも公認・推薦・容認しません。CompTIAの認定資格試験の受験準備にこのような教材を使用した個人は、CompTIA受験者同意書の規定に基づいて資格認定を取り消され、その後の受験資格を停止されます。CompTIAでは、無許可教材の使用に関する試験実施ポリシーをよりよく理解していただくための取り組みを進めています。認定資格試験を受験される方は、[CompTIA 認定資格試験実施ポリシー](#)をご確認ください。CompTIAの認定資格試験を受験するための学習を始める前には、必ずCompTIAが定めるすべてのポリシーをご確認ください。受験者には、**CompTIA受験者同意書**の規定を遵守することが求められています。個々の教材が不正教材（通称「ブレインダンプ」）扱いになるかどうかを確認するには、CompTIAの担当窓口（[examsecurity@comptia.org](mailto:examsecurity@comptia.org)）までお問い合わせください。

## 注意

簡条書きで挙げられた項目は、すべての試験内容を網羅するものではありません。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、あるいはタスクを含む問題が出題される可能性があります。CompTIAでは、提供している認定資格試験の内容に現在必要と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、継続的な試験内容の検討と問題の改訂を行っています。必要な場合、現在の出題範囲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。

## 試験情報

試験番号	CV0-002
問題数	最大で90問
出題形式	単一/複数選択、シミュレーション
試験時間	90分
推奨経験	<ul style="list-style-type: none"><li>• ITネットワーク、ネットワークストレージ、またはデータセンター管理における24~36ヶ月以上の業務経験</li><li>• サーバー仮想化のための主要なハイパーバイザー技術に精通している（仮想化に関連するベンダー資格を取得している必要はありません）</li><li>• CompTIA Network+認定資格または/およびCompTIA Server+認定資格相当の知識とスキル（を受験の際の必須要件ではありません）</li><li>• クラウドサービスモデル（IaaS、PaaS、SaaS）の定義の理解</li><li>• 一般的なクラウド展開モデル（プライベート、パブリック、ハイブリッド）の定義の理解</li><li>• パブリックIaaSクラウド環境での業務経験</li></ul>
合格ライン	750（100~900のスコア形式）

## 出題範囲（試験分野）

下表は、この試験における試験分野（ドメイン）と出題比率の一覧です：

試験分野	出題比率
1.0 コンフィグレーションとデプロイメント	24%
2.0 セキュリティ	16%
3.0 メンテナンス	18%
4.0 マネジメント	20%
5.0 トラブルシューティング	22%
合計	100%



# 1.0 コンフィグレーションとデプロイメント

1.1 与えられたシナリオに基づいて、システム要件を分析し、システム展開を成功に導くことができる。

- ・場面に応じた適切なコマンド、構造、ツール、オートメーション/オーケストレーション
- ・プラットフォームおよびアプリケーション
- ・クラウドコンポーネントおよびサービスのインタラクション
  - ネットワークコンポーネント
  - アプリケーションコンポーネント
  - ストレージコンポーネント
  - コンピュートコンポーネント
  - セキュリティコンポーネント
- ・非クラウドコンポーネントおよびサービスのインタラクション
- ・ベースライン
- ・ターゲットホスト
- ・既存のシステム
- ・クラウドアーキテクチャ
- ・クラウドエレメント/ターゲットオブジェクト

1.2 与えられたシナリオに基づいて、展開計画を実行することができる。

- ・変更管理プロセスを適用する
  - 承認
  - スケジューリング
- ・関連文書を参照し、標準的な操作手順に従う
- ・ワークフローを実行する
- ・展開されるシステムのオートメーションやオーケストレーション（該当するもの）を設定する
- ・必要に応じてコマンドとツールを使用する
- ・結果を記録する

1.3 与えられたシナリオに基づいて、システム要件を分析して、特定のテスト計画が適切かどうかを判断することができる。

- ・テスト計画に含まれている基本環境についての考慮事項
  - 共有コンポーネント
    - ストレージ
    - コンピュート
    - ネットワーク
  - 本番環境/開発環境/QA環境
  - サイジング
  - パフォーマンス
- ・高可用性
- ・接続性
- ・データの整合性
- ・適切な機能
- ・レプリケーション
- ・ロードバランシング
- ・オートメーション/オーケストレーション
- ・テスト技術
  - 脆弱性テスト
  - ペネトレーションテスト
  - 負荷テスト



1.4 与えられたシナリオに基づいて、テスト結果を分析して、システム要件に対してテストが成功したかどうかを判断することができる。

- テスト環境の成功要因指標を検討する
  - サイジング
  - パフォーマンス
  - 可用性
  - 接続性
  - データの整合性
  - 適切な機能性
- 結果を記録する
- ベースライン比較
- SLAの比較
- クラウドパフォーマンスに影響を与える数値

1.5 与えられたシナリオに基づいて、仮想ネットワーク展開の際のサイジング、サブネット化、および基本ルーティングを分析することができる。

- クラウド展開モデル
  - パブリック
  - プライベート
  - ハイブリッド
  - コミュニティ
- ネットワークコンポーネント
- クラウドに拡張する場合の適用可能なポートおよびプロトコルについての考慮事項
- 最適なプラットフォームに応じたネットワークのコンフィグレーションを定義する
  - VPN
  - IDS/IPS
  - DMZ
  - VXLAN
  - 必要なアドレススペース
- ネットワークセグメンテーションおよびマイクロセグメンテーション
- クラウドリソースがSLAおよび/または変更管理要件と一貫性があるかどうかを判断する

1.6 与えられたシナリオに基づいて、展開のために必要なCPUとメモリサイジングを分析することができる。

- 使用可能なリソースと提案されたリソース
  - CPU
  - RAM
- メモリ技術
  - バースティングおよびバルーニング
  - オーバーコミットメント比率
- CPUテクノロジー
  - ハイパースレッディング
  - VT-x
  - オーバーコミットメント比率
- HA/DRへの影響
- パフォーマンスについての考慮事項
- コストについての考慮事項
- 省エネルギー
- 専用コンピューティング環境と共有コンピューティング環境



1.7 与えられたシナリオに基づいて、展開のために適切なストレージタイプと保護機能を分析することができる。

- リクエストされたIOPSと読み取り/書き込みスループット
- 保護機能
  - 高可用性
    - フェイルオーバーゾーン
  - ストレージレプリケーション
    - リージョナル
    - マルチリージョナル
    - 同期と非同期
  - ストレージミラーリング
  - クローニング
  - 冗長レベル/要素
- ストレージタイプ
  - NAS
  - DAS
  - SAN
  - オブジェクトストレージ
- アクセスプロトコル
- 管理上の違い
- プロビジョニングモデル
  - シック・プロビジョニング
  - シン・プロビジョニング
  - 暗号化要件
  - トークン化
- ストレージ技術
  - 重複排除技術
  - 圧縮技術
- ストレージ層
- ストレージのオーバーコミット
- 適応可能なプラットフォームのセキュリティ設定
  - ACLs
  - 難読化
  - ゾーニング
  - ユーザー/ホストの認証および承認

1.8 与えられたシナリオに基づいて、移行の成功のために、ワークロード（ストレージ、ネットワーク、コンピュータ）の特性を分析することができる。

- 移行タイプ
  - P2V
  - V2V
  - V2P
  - P2P
  - ストレージ移行
  - オンライン移行とオフライン移行
- ワークロードの送信元および宛先のフォーマット
  - 仮想化フォーマット
  - アプリケーションおよびデータのポータビリティ
- ネットワーク接続とデータ転送の方法
- ワークロード移行の標準的な操作手順
- 環境の制約
  - 帯域幅
  - 労働時間の制限
  - ダウンタイムの影響
  - ピーク時間枠
  - 法的規制
  - フォロー・ザ・サン制約/タイムゾーン

1.9 与えられたシナリオに基づいて、特定のクラウドソリューションを適用するためのインフラストラクチャ拡張に必要な要素を特定することができる。

- 認証管理要素
  - 識別
  - 認証
  - 承認
    - 承認
    - アクセスポリシー
  - フェデレーション
    - シングルサインオン
- 要件を満たす適切なプロトコル
- インフラストラクチャサービスを展開するための要素についての考慮事項：
  - DNS
  - DHCP
  - 証明書サービス
  - ローカルエージェント
  - アンチウイルス
  - ロードバランサー
  - 多要素認証
  - ファイアウォール
  - IPS/IDS



## 2.0 セキュリティ

2.1 与えられたシナリオに基づいて、特定のクラウドインフラストラクチャ要件を満たすセキュリティ設定とコンプライアンスコントロールを適用することができる。

- 企業のセキュリティポリシー
- 選択されたプラットフォームにセキュリティ基準を適用する
- 環境を管理するコンプライアンスおよび監査の要件
  - データに適用される法令
- 暗号化技術
  - IPSec
  - SSL/TLS
  - 他の暗号化技術

- キーおよび証明書の管理
  - PKI
- トンネリングプロトコル
  - L2TP
  - PPTP
  - GRE
- 適切なオートメーションおよびオーケストレーションプロセスを実装する
- 適用可能なプラットフォームをコンピュータに適用する

- ための適切な構成
- 不要なポートとサービスを無効にする
  - アカウント管理ポリシー
  - ホストベース/ソフトウェアファイアウォール
  - アンチウイルス/マルウェア対策ソフトウェア
  - バッチング
  - 初期設定されているアカウントの無効化

2.2 与えられたシナリオに基づいて、セキュリティテンプレートに従ってアクセス要件を満たすように、ターゲットオブジェクトに適切なACLを適用することができる。

- クラウド上のオブジェクトの承認
  - プロセス
  - リソース
    - ユーザー
    - グループ
    - システム
      - コンピュート
      - ネットワーク

- ストレージ
- サービス
- クラウドサービスモデルがセキュリティ実装に及ぼす影響
- クラウド展開モデルがセキュリティ実装に及ぼす影響

- アクセスコントロール方法
  - ロールベース管理
  - 強制アクセス制御
  - 任意アクセス制御
  - 非任意アクセス制御
  - 多要素認証
  - シングルサインオン

2.3 与えられたクラウドサービスモデルに基づいて、特定のセキュリティ要件を満たすように、定義されたセキュリティテクノロジーを実装することができる。

- データ分類
- ネットワークセグメンテーションおよびマイクロセグメンテーションの概念
  - ネットワーク
  - ストレージ
  - コンピュート
- 定義されたとおりに暗号化を使用する

- 定義された多要素認証を使用する
- 定義された監査/コンプライアンス要件を適用する



2.4

与えられたクラウドサービスモデルに基づいて、適切なセキュリティ自動化手法をターゲットシステムに適用することができる。

- ツール
  - APIs
  - ベンダーアプリケーション
  - CLI
  - ウェブGUI
  - クラウドポータル
- 手法
  - オーケストレーション
  - スクリプティング
  - カスタムプログラミング
- セキュリティサービス
  - ファイアウォール
  - アンチウイルス/マルウェア対策
  - IDS/IPS
  - HIPS
- システムおよびサービスに対するセキュリティツールの影響
  - 影響範囲
- システムのクリティカルリティに関連するセキュリティ自動化手法の影響
  - 影響範囲





## 3.0 メンテナンス

3.1 与えられたクラウドサービスモデルにおいて、特定のパッチを適用するための適切な方法を決定することができる。

### •パッチが適用されるべきクラウド要素の範囲

- ハイパーバイザー
- 仮想マシン
- 仮想アプライアンス
- ネットワーキングコンポーネント
- アプリケーション
- ストレージコンポーネント
- クラスタ

### •パッチ適用方法および標準的な操作手順

- 本番環境/開発環境/QA環境
- ローリングアップデート
- ブルー・グリーンデプロイメント
- フェイルオーバークラスタ

### •パッチ適用される要素に関連する演算順序を使用する

- 依存性の考慮

3.2 与えられたシナリオに基づいて、クラウド要素を更新するための適切な自動化ツールを適用することができる。

### •更新のタイプ

- ホットフィックス
- パッチ
- バージョン更新
- ロールバック

### •自動化のワークフロー

- Runbook 管理
- 単一ノード

- オークストレーション
- 複数ノード
- 複数ランブック

### •自動化ツールによって実行されるアクティビティ

- スナップショット
- クローニング
- パッチング

- リスタート
- シャットダウン
- 保守モード
- アラートの有効化/無効化

3.3 与えられたシナリオに基づいて、適切なバックアップまたは修復方法を適用することができる。

### •バックアップタイプ

- スナップショット/redirect-on-write
- クローン
- フル
- 差分
- 増分
- チェンジブロックトラッキング/  
デルタトラッキング

### •バックアップターゲット

- レプリカ
- ローカル
- リモート

### •その他の考慮事項

- SLAs
- バックアップスケジュール
- 構成
- オブジェクト
- 依存関係
- オンライン/オフライン



3.4 与えられたクラウドベースのシナリオに基づいて、適切な災害復旧方法(DR)を適用することができる。

- クラウドサービスプロバイダのDR能力
- その他の考慮事項
  - DRのためのSLA
  - RPO
  - RTO
  - 企業ガイドライン
- クラウドサービスプロバイダガイドライン
- 帯域幅またはISPの制限
- 技術
- サイトミラーリング
- レプレーション
- ファイル転送
- アーカイブ
- サードパーティのサイト

3.5 与えられたクラウドベースのシナリオに基づいて、事業継続を確実にする適切な手法を適用することができる。

- 事業継続計画
  - 代替サイト
  - オペレーションの継続性
  - 接続性
  - エッジサイト
  - 機材
  - 可用性
  - パートナー/サードパーティ
- BCPおよびHAのためのSLA

3.6 与えられたシナリオに基づいて、適切なメンテナンス自動化手法をターゲットオブジェクトに適用することができる。

- メンテナンススケジュール
- メンテナンスタスクの影響と範囲
- メンテナンス自動化手法の影響と範囲
- 適切なオーケストレーションを含める
- メンテナンス自動化タスク
  - ログの消去
  - ログのアーカイブ
  - ドライブの圧縮
  - 無効アカウントの削除
  - 失効したDNSエントリの削除
  - 放棄されたりソースの削除
  - ファイアウォールから古くなったルールを削除する
  - セキュリティから古くなったルールを削除する
  - リソースの再利用
  - 対象オブジェクトのためにACLを維持する



## 4.0 マネジメント

4.1 与えられたシナリオに基づいて、異常の有無を判断したり、将来必要とされるクラウドリソースを予測したりするために定義された指標を分析することができる。

### ・モニタリング

- ターゲットオブジェクトのベースライン
- ターゲットオブジェクトの異常
- 一般的なアラート方法/メッセージ
- ベースラインからの偏差に基づくアラート
- イベント収集

### ・イベント相関

- ・リソース容量の予測
  - アップサイズ/増加
  - ダウンサイズ/減少
- ・イベント収集をサポートするポリシー
- ・適切なアラート通知に関するポリシー

4.2 与えられたシナリオに基づいて、クラウドリソースの適切な配分を決定することができる。

### ・クラウド展開モデルに基づいて必要とされるリソース

- ハイブリッド
- コミュニティ
- パブリック
- プライベート

### ・クラウド環境のキャパシティ/拡張性

### ・サポート契約

- クラウドサービスモデルのメンテナンスに関する責任

### ・構成管理ツール

### ・リソースパランシング手法

### ・変更管理

- 諮問機関

### - 承認プロセス

- 実行した措置の文書化

### - CMDB

- スプレッドシート

4.3 与えられたシナリオに基づいて、クラウドリソースのプロビジョン/デプロビジョンのタイミングを決定することができる。

### ・使用パターン

### ・クラウドバースティング

- 自動スケーリング手法

### ・クラウドプロバイダの移行

### ・クラウド範囲の拡張

### ・アプリケーションライフサイクル

- アプリケーションの展開

### - アプリケーションのアップグレード

- アプリケーションの配信終了

### - アプリケーションの交換

### - アプリケーションの移行

### - アプリケーション機能用途

- 増加/減少

### ・ビジネスニーズの変更

- 合併/買収/売却

### - クラウドサービス要件の変更

- 規制や法律の変更の影響



4.4 与えられたシナリオに基づいて、セキュリティとポリシー要件を満たすように、クラウド環境におけるアカウントのプロビジョニング技術を実装することができる。

- 識別
- 認証方法
  - フェデレーション
  - シングルサインオン
- 承認方法
  - ACL
  - 許可
- アカウントのライフサイクル
- アカウント管理ポリシー
  - ロックアウト
  - パスワード複雑性ルール
- 自動化やオーケストレーションのアクティビティ
  - ユーザーアカウント作成
  - 許可設定
- リソースアクセス
- ユーザーアカウント消去
- ユーザーアカウント無効化

4.5 与えられたシナリオに基づいて、ベースラインを満たしていることを確認するために展開結果を分析することができる。

- 結果を確認する手順
  - CPU使用率
  - RAM使用量
  - ストレージ利用率
  - パッチのバージョン
- ネットワーク利用状況
- アプリケーションバージョン
- 監査の有効化
- 管理ツールのコンプライアンス

4.6 特定の環境および関連するデータ（例えば、パフォーマンス、キャパシティ、トレンド）が与えられた場合、クライテリアを満たすように適切な変更を適用することができる。

- パフォーマンスの傾向を分析する
- ベースラインを参照する
- SLAを参照する
- クラウドターゲットオブジェクトのチューニング
  - コンピュート
  - ネットワーク
  - ストレージ
  - サービス/アプリケーションリソース
- 期待パフォーマンス/キャパシティを満たすための推奨変更
  - スケールアップ/ダウン（垂直）
  - スケールイン/アウト（水平）

4.7 SLA 要件に基づいて、報告する適切な指標を決定することができる。

- チャージバック/ショーバックモデル
  - 企業ポリシーに基づいたレポート
  - SLAに基づいたレポート
- ダッシュボードとレポート
  - 使用量
  - 接続性
- レイテンシー
- キャパシティ
- 全体の使用状況
- コスト
- インシデント
- 健全性
- システム可用性
  - アップタイム
  - ダウンタイム



## 5.0 トラブルシューティング

5.1 与えられたシナリオに基づいて、展開の際の問題を  
トラブルシューティングすることができる。

- ・展開における一般的な問題
  - ワークフローの内訳
  - 異なるクラウドプラットフォームに関連する統合の問題
  - リソースの競合
- 接続の問題
  - クラウドサービスプロバイダの停止
  - ライセンスの問題
  - テンプレートの設定ミス
- 時刻同期の問題
  - 言語サポート
  - 自動化の問題

5.2 与えられたシナリオに基づいて、一般的なキャパシティに関する問題を  
トラブルシューティングすることができる。

- ・クラウドキャパシティの限界の超過
  - コンピュート
  - ストレージ
  - ネットワーク
    - IPアドレスの限界
    - 帯域幅の限界
  - ライセンス
- ユーザー数の分散
  - APIリクエストのリミット
  - バッチジョブのスケジューリングに関する問題
- ・元のベースラインからの偏差
  - ・計画されていない拡張

5.3 与えられたシナリオに基づいて、自動化・オーケストレーションの問題を  
トラブルシューティングすることができる。

- ・ワークフローの内訳
  - アカウントのミスマッチの問題
  - 管理計画の不履行
  - サーバー名の変更
  - IPアドレスの変更
- ロケーションの変更
  - バージョン・機能のミスマッチ
  - 自動化ツールの非互換性
  - ジョブ検証の問題

5.4 与えられたシナリオに基づいて、接続性の問題を  
トラブルシューティングすることができる。

- ・一般的なネットワーキング問題
  - 不正確なサブネット
  - 不正確なIPアドレス
  - ゲートウェイの誤り
  - 不正確なルーティング
  - DNSエラー
  - QoS問題
  - 正しく設定されていないVLANまたはVXLAN
  - 正しく設定されていないファイアーウォールルール
- 不十分な帯域幅
  - レイテンシー
  - 正しく設定されていないMTU/MSS
  - 正しく設定されていないプロキシ
- ・ネットワークツールのアウトプット
  - ・ネットワーク接続ツール
    - ping
    - tracert/traceroute
    - telnet
    - netstat
    - nslookup/dig
- ipconfig/ifconfig
  - route
  - arp
  - ssh
  - tcpdump
- ・トラブルシューティングのためのリモートアクセスツール



### 5.5 与えられたシナリオに基づいて、セキュリティの問題をトラブルシューティングすることができる。

- ・認証の問題
  - アカウントのロックアウト/失効
- ・承認の問題
- ・フェデレーションおよびシングルサインオンの問題
- ・証明書の失効
- ・証明書の設定ミス
- ・外部からの攻撃
- ・内部からの攻撃
- ・特権エスカレーション
- ・内部の役割変更
- ・外部の役割変更
- ・セキュリティデバイス障害
- ・ハードニングが正しく設定されていない
- ・暗号化されていないコミュニケーション
- ・許可なしの物理的アクセス
- ・暗号化されていないデータ
- ・弱いまたは旧式のセキュリティ技術
- ・不十分なセキュリティ制御およびプロセス
- ・トンネリングまたは暗号化問題

### 5.6 与えられたシナリオに基づいて、トラブルシューティング手法を説明することができる。

- ・変更を実施する際は、必ず前もって会社のポリシーや手順、および影響について考慮する。
1. 問題を特定する
    - ユーザーに質問し、コンピューターに対するユーザー変更を明確にして、バックアップを実施してから変更を行う
  2. 推定原因の仮説を立てる（明白と思われる点も確認する）
    - 必要なら症状に応じた外部・内部調査を実施する
  3. 仮説を検証して原因を特定する
    - 仮説が証明された場合、問題解決に向けた今後の対応を決定する
    - 仮説が証明されなかった場合、仮説を立て直すか、エスカレーションする
  4. 問題解決のための対応計画を策定し、実行に移す
  5. システム全体の機能を検証し、該当する場合は予防対策を実施する
  6. 原因、対策、結果を文書化する

# 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。受験者には、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。

略語	用語	略語	用語
AAA	Authentication, Authorization, and Accounting	DAS	Direct Attached Storage
ACL	Access Control List	DBA	Database Administrator
AES	Advanced Encryption Standard	DBaaS	Database as a Service
API	Application Programming Interface	DBMS	Database Management Server
APM	Application Performance Monitor	DES	Data Encryption Standard
ARP	Address Resolution Protocol	DFS	Distributed File System
BCP	Business Continuity Plan	DHCP	Dynamic Host Configuration Protocol
BGP	Border Gateway Protocol	DIMM	Dual In-line Memory Module
BIA	Business Impact Analysis	DLP	Data Loss Prevention
BLOB	Binary Large Object	DMZ	Demilitarized Zone
BMR	Bare Metal Restore	DNS	Domain Name Service
BPaaS	Business Process as a Service	DR	Disaster Recovery
CAB	Change Advisory Board	DRaaS	Disaster Recovery as a Service
CaaS	Communication as a Service/ Computing as a Service	DRP	Disaster Recovery Plan
CapEx	Capital Expenditures	DSA	Distributed Services Architecture
CAS	Content Addressed Storage	ECAB	Emergency Change Advisory Board
CASB	Cloud Access Security Broker	ECC	Elliptic Curve Cryptography
CI/CD	Continuous Integration/Continuous Deployment	FAT	File Allocation Table
CIFS	Common Internet File System	FC	Fibre Channel
CIIS	Client Integration Implementation Service	FCIP	Fibre Channel over IP
CLI	Command Line Interface	FCoE	Fibre Channel over Ethernet
CMDB	Configuration Management Database	FIM	File Integrity Monitoring
CM	Configuration Management	FTP	File Transfer Protocol
CMP	Cloud Management Platform	FTPS	FTP over SSL
CMS	Content Management System	GPT	GUID Partition Table
CNA-	Converged Network Adapter	GPU	Graphics Processing Unit
CNAME	Canonical Name	GRE	Generic Routing Encapsulation
COLO	Co-location	GUI	Graphical User Interface
COOP	Continuity of Operations Plan	HA	High Availability
CPU	Central Processing Unit	HBA	Host Bus Adapter
CRL	Certificate Revocation List	HDFS	Hadoop Distributed File System
CRM	Customer Relationship Management	HIPS	Host Intrusion Prevention System
CSA	Cloud Systems Administrator	HTTPS	Hypertext Transfer Protocol Secure
CSP	Cloud Service Provider	IaaS	Infrastructure as a Service
DaaS	Desktop as a Service	IAM	Identity and Access Management
DAC	Discretionary Access Control	ICMP	Internet Control Management Protocol
		IDP	Intrusion Detection and Prevention

略語	用語	略語	用語
IDS	Intrusion Detection System	OpEx	Operating Expenditure
IFCP	Internet Fibre Channel Protocol	OS	Operating System
IGRP	Interior Gateway Routing Protocol	OSPF	Open Shortest Path First
IOPS	Input/output Operations Per Second	OVA	Open Virtual Appliance
IPC	Instructions Per Cycle	OVF	Open Virtualization Format
IPMI	Intelligent Platform Management Interface	P2P	Physical to Physical
IPS	Intrusion Protection System	P2V	Physical to Virtual
IPSec	Internet Protocol Security	PaaS	Platform as a Service
IQN	Initiator Qualified Name	PAC	Proxy Automatic Configuration
IRM	Information Rights Management	PAM	Pluggable Authentication Modules
ISP	Internet Service Provider	PAT	Port Address Translation
iSCSI	Internet Small Computer Systems Interface	PBX	Private (or Public) Branch Exchange
ISNS	Internet Storage Name Service	PCI	Payment Card Industry
ITIL	Information Technology Infrastructure Library	PCS	Private Cloud Space
JBOD	Just a Bunch of Disks	PII	Personally Identifiable Information
JSON	JavaScript Object Notation	PIT	Point-in-Time
KMS	Key Management System	PKI	Public Key Infrastructure
KVM	Keyboard Video Mouse	PSK	Pre-Shared Key
L2TP	Layer 2 Tunneling Protocol	QA	Quality Assurance
LAN	Local Area Network	QoS	Quality of Service
LDAP	Lightweight Directory Access Protocol	RAID	Redundant Array of Inexpensive Disks
LUN	Logical Unit Number	RBAC	Role-Based Access Control
MAC	Mandatory Access Control	RC5	Rivest Cipher 5
MBR	Master Boot Record	RDP	Remote Desktop Protocol
MDF	Main Distribution Facility	ReFS	Resilient File System
MFA	Multifactor Authentication	RIP	Routing Information Protocol
MPIO	Multipath Input/Output	RPO	Recovery Point Objective
MPLS	Multiprotocol Label Switching	RTO	Recovery Time Objective
MSP	Managed Service Provider	SaaS	Software as a Service
MTBF	Mean Time Between Failure	SAML	Security Assertions Markup Language
MTTF	Mean Time To Failure	SAN	Storage Area Network
MTTR	Mean Time To Recovery	SAS	Serial Attached SCSI
MTU	Maximum Transmission Unit	SATA	Serial Advanced Technology Attachment
NAC	Network Access Control	SCP	Session Control Protocol
NAS	Network Attached Storage	SCSI	Small Computer System Interface
NAT	Network Address Translation	SDLC	Software Development Life Cycle
NFS	Network File System	SDN	Software Defined Network
NFV	Network Function Virtualization	SED	Self-Encrypting Drive
NIC	Network Interface Controller	SFTP	Secure FTP
NIS	Network Information Service	SHA	Secure Hash Algorithm
NOC	Network Operations Center	SIEM	Security Incident Event Manager
NPIV	N_Port ID Virtualization	SIP	Session Initiation Protocol
NTFS	New Technology File System	SLA	Service Level Agreement
NTLM	NT LAN Manager	SMB	Server Message Block
NTP	Network Time Protocol	SNMP	Simple Network Management Protocol
NVMe	Non-Volatile Memory Express	SOP	Standard Operating Procedure
ODBC	Open Database Connectivity	SSD	Solid State Disk
OLA	Operational Level Agreement	SSH	Secure Shell



略語	用語
SSL	Secure Sockets Layer
SSO	Single Sign-On
TCO	Total Cost of Operations
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTD	Technical Training Device
TTL	Time To Live
UAT	User Acceptance Testing
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
VDI	Virtual Desktop Infrastructure
VHD	Virtual Hard Disk
VLAN	Virtual LAN
VM	Virtual Machine
VMDK	Virtual Machine Disk
VMFS	Virtual Machine File System
VNC	Virtual Network Computing
VNIC	Virtual NIC
VoIP	Voice over IP
VPC	Virtual Private Cloud
VPN	Virtual Private Network
VRAM	Virtual RAM
VRF	Virtual Routing and Forwarding
VRR	Vulnerability Remediation Request
VSAN	Virtual SAN
vSwitch	Virtual Switch
VTL	Virtual Tape Library
VXLAN	Virtual Extensible Local Area Network
WAF	Web Application Firewall
WAN	Wide Area Network
WMI	Windows Management Implementation
WWNN	World Wide Node Name
WWPN	World Wide Port Name
WWUI	World Wide Unique Identifier
XaaS	Anything as a Service
ZFS	Z File System

# CompTIA Cloud+ハードウェアとソフトウェア一覧

本リストは、CompTIA Cloud+の受験準備として役立てていただくためのハードウェアとソフトウェアのリストです。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習室コンポーネントを作成したい場合に役立ちます。各トピックに箇条書きで挙げられた項目は例であり、すべてを網羅するものではありません。

## 機材

- ・ハイパー・コンバージド・インフラストラクチャ/システム
  - 共有ストレージ/ハードドライブ
  - SANスイッチ
  - バックアップサービス
  - クラウドサービスへのレプリケーション
  - 仮想ファイアウォール
  - コンピュート (CPU、RAMなど)
- ・クライアントPCのためのスイッチ
- ・ルーター
- ・SaaS、PaaS、IaaS環境へのアクセス
- ・クライアントPC (ラップトップ/デスクトップ)

## 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

## ソフトウェア

- ・自動化ツール
- ・ハイパーバイザ (Type1、Type2)
- ・クライアントおよびサーバーOS
- ・各種インターネットブラウザ
- ・ハイパーバイザ管理ソフトウェア
- ・クラウド管理ソフトウェア
- ・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へのリモートアクセス (無料サービス)
- ・管理ツール (管理パック)
- ・セルフサービスプロビジョニングポータル