



CompTIA Server+認定資格試験出題範囲

試験番号: SK0-004

はじめに

CompTIA Server+は、国際的に認知されているベンダーニュートラルの認定資格です。CompTIA Server+を取得することで、受験者の基本的なレベルのサーバーに関連するスキルと知識を証明することができ、また世界中で様々な企業に IT エンジニアの育成のため活用されています。

CompTIA Server+認定資格試験で評価されるスキルおよび知識は、IT 業界の識者により実施された職務能力分析 (JTA - Job Task Analysis)により策定され、2014 年第 3 四半期にワールドワイドで実施されたサーベイにより検証がされました。このサーベイの結果をもとに、試験分野の内容、およびそれぞれの分野の出題比率が、その分野の重要性に応じて決定されています。

CompTIA Server+は、18 ヶ月～24 ヶ月の実務経験で得られる知識とスキルを目安に設計されています。受験条件として問いませんが、CompTIA Server+認定資格試験を受験する際には、CompTIA A+を取得いただくか、またはこれに相当する実務経験を有することをお勧めします。

本試験では、サーバーの構築、保守、トラブルシューティング、セキュリティ、仮想化を含むサーバーのハードウェアとソフトウェアテクノロジーを保守/運用するためのスキルと知識を評価します。CompTIA Server+を取得することで、環境問題への配慮、災害復旧や一般的なセキュリティ手順と対応の重要性の理解、専門用語やコンセプトの理解、サーバーの役割や仕様、様々に変化する IT 環境での影響と対応についても理解していることを証明することができます。

この出題範囲には、試験分野、出題比率、出題例が含まれています。出題例は出題範囲を明確にするためであり、試験の出題内容そのものを反映している訳ではありませんので、ご注意ください。

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 サーバー設計	12%
第2章 サーバー管理	24%
第3章 ストレージ	12%
第4章 セキュリティ	13%
第5章 ネットワーク	10%
第6章 災害復旧	9%
第7章 トラブルシューティング	20%
合計	100%

CompTIA Authorized Materials Use Policy

CompTIA では、パートナー契約を締結していない、もしくは承認、推奨、許可されていないサードパーティーのトレーニングサイトで提供されるコンテンツは容認、許可をしていません。CompTIA 認定資格試験の受験のためこれらの教材を利用することは、CompTIA Candidate Agreement の取り決めにより、将来的に受験ができなくなる可能性があります。認定を受けていない教材を利用することに対する CompTIA 認定資格試験の方針をより明確にするため、CompTIA では全ての受験者に対して CompTIA Certification Exam policy を下記の Web サイトにて公開しています。

<https://certification.comptia.org/testing/test-policies/unauthorized-training-materials>

CompTIA 認定資格試験への学習を始める前に、CompTIA のポリシーをご確認ください。また、全ての受験者は、全ての試験に対して CompTIA Candidate Agreement を遵守する必要があります。

<http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx>

受験者の方が、教材を利用する前に、これらの教材が不正な教材かどうかを判断していただくために、Cert Guard を利用して検索をしていただくことができます。

<http://www.certguard.com/search.asp>

もしくは、下記のリストを参照していただくことも可能です。

<http://certification.comptia.org/Training/testingcenters/policies/unauthorized.aspx>

※ 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。

CompTIA は、配信されている試験内容を継続的にセキュリティ上問題がなく、最新の状態であることを監視しています。そのため、試験問題/本出題範囲は、必要に応じて、予告なく変更される場合がございます。予めご了承ください。また、変更がされた場合においても、全ての学習教材は、問題なくご活用いただけます。

第1章 サーバー設計(12%)

1.1 サーバーフォームファクターの機能と役割について説明することができる。

- ラックマウント
 - 寸法
 - 1U、2U、4U
 - ケーブルマネジメントアーム
 - レールキット
- タワー
- ブレードテクノロジー
 - ブレードエンクロージャー(ブロードシャーシ)
 - バックプレーン/ミッドプレーン
 - 電源ソケット
 - ネットワークモジュール/スイッチ
 - 管理モジュール
 - ブレードサーバー

1.2 与えられたシナリオに基づいて、サーバーコンポーネントの設置、設定、管理を実施することができる。

- CPU
 - マルチプロセッサとマルチコアの違い
 - ソケットの種類
 - キャッシュレベル:L1、L2、L3
 - スピード
 - コア
 - バス
 - クロック速度
 - CPU ステッピング
 - 設計
 - x86
 - x64
 - ARM
- RAM
 - ECC メモリとの non-ECC メモリの違い
 - DDR2、DDR3
 - ピンの数
 - SRAM と DRAM の違い
 - モジュールの設定
 - CAS レイテンシー
 - メモリタイミング
 - メモリベアリング
- バスの種類、バスチャネル、拡張スロット
 - 大きさの違いとビットレートの違い
 - PCI
 - PCIe
 - PCI-X
- NIC
- ハードディスク
- ライザーカード
- RAID コントローラー

- BIOS/UEFI
 - CMOS バッテリー
- ファームウェア
- USB インターフェース/ポート
- 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

1.3 電力と冷却のコンポーネントを比較対照することができる。

- 電源
 - 電圧
 - 110v、220v、-48v の違い
 - 208v と 440v/460v/480v の違い
 - ワット数
 - 消費電力
 - 冗長性
 - 単相電力 (1-phase power) と三相電力 (3-phase power) の違い
 - プラグの種類
 - NEMA
 - Edison
 - ツインロック
- 冷却
 - エアフロー
 - サーマルディスペンサー
 - バッフル/シュラウド
 - ファン
 - 液体冷却

第2章 サーバー管理(24%)

2.1 サーバー用 OS のインストールと設定をすることができる。

- サーバーの役割と目的の決定
- ファームウェアのアップデート
- BIOS/UEFI の設定
 - 起動順序
- ディスクの準備
 - RAID のセットアップ
 - パーティションの設定
 - フォーマット
 - ファイルシステムの種類
 - Ext 2、Ext3、Ext 4
 - NTFS
 - FAT32
 - ReiserFS
 - UFS
 - VMFS
 - ZFS
 - スワップ
- ホスト名の設定
- ローカルアカウントのセットアップ
- ネットワークへの接続
- ドメイン/ディレクトリの構成
- セキュリティ対策
 - パッチ
 - OS の要塞化
 - 企業における手順と標準のコンプライアンス
- サービスの有効化
- 機能/ロール/アプリケーションドライバのインストール
- パフォーマンスベースライン
 - サーバーの最適化
 - スワップ/ページファイルの最適化
- 無人/リモートからのインストール
 - イメージとクローニングの展開
 - インストール用スクリプト
 - PXE ブート
 - TFTP

2.2 サーバーの役割と必要条件を比較対照することができる。

- ウェブサーバー
- アプリケーションサーバー
- ディレクトリサーバー
- データベースサーバー
- ファイルサーバー
- プリンタサーバー
- メッセージングサーバー
- メールサーバー
- ルーティング/リモートアクセスサーバー

- ネットワークサービスサーバー
 - DHCP
 - DNS/WINS
 - NTP

2.3 与えられたシナリオに基づいて、サーバーを管理するためのアクセスとコントロールを使用することができる。

- ローカルハードウェア管理
 - KVM
 - シリアル
 - 仮想管理コンソール
- ネットワークベースのハードウェア管理
 - KVM over IP
 - ILO
 - iDRAC
- ネットワークベースのオペレーティングシステム管理
 - RDP
 - SSH
 - VNC
 - コマンドライン/シェル

2.4 与えられたシナリオに基づいて、適切なサーバー管理手法を実施することができる。

- 変更管理
- パッチ管理
 - OS のアップデート
 - アプリケーションのアップデート
 - セキュリティソフトウェアのアップデート
 - ファームウェアのアップデート
 - デバイスドライバのアップデート
 - 互換性リスト
 - OS
 - ハードウェア
 - アプリケーション
 - テストとバリデーション
- 停電と SLA (サービスレベルアグリーメント)
 - 計画ダウンタイム
 - 計画外ダウンタイム
 - インパクト分析
 - クライアントへの通知
 - MTTR
- パフォーマンスの監視
 - CPU 利用率
 - メモリ利用率
 - ネットワーク利用率
 - ディスク利用率
 - ディスク IOPS
 - ストレージ容量
 - パフォーマンスベースラインとの比較
 - プロセス監視とサービス監視
 - ログ監視

- ハードウェアメンテナンス
 - システムヘルスインジゲータの確認
 - LED
 - エラーコード
 - ビープコード
 - LCD メッセージ
 - 故障したコンポーネントの交換
 - ファン
 - ハードディスク
 - RAM
 - バックプレーン
 - 電源装置
 - 予防保守
 - 埃の掃除
 - 適切なエアフローの確認
 - 適切なシャットダウン手順
- フォールトトレランスと高可用性の手法
 - クラスタリング
 - アクティブ/アクティブ
 - アクティブ/パッシブ
 - ロードバランス
 - ラウンドロビン
 - ハートビート

2.5 資産管理と文書化の重要性を説明することができる。

- 資産管理
 - ライセンス
 - ラベリング
 - 保証書
 - ライフサイクルマネジメント
 - 調達
 - 利用
 - エンドオブライフ
 - 廃棄/リサイクル
 - インベントリ(棚卸)
 - 作成
 - 製品モデル
 - シリアルナンバー
 - 資産タグ
 - 文書化
 - サービスマニュアル
 - ネットワーク図
 - アーキテクチャ設計書
 - データフロー設計書
 - リカバリー文書
 - ベースライン文書
 - 変更管理ポリシー
 - SLA(サービスレベルアグリーメント)
 - サーバー設定
 - セキュアに保管されるべき機密文書

2.6 仮想化コンポーネントの目的と運用方法を説明することができる

- ホストとゲスト
- 仮想マシン用の管理インターフェース
- ハイパーバイザー
 - Type1
 - Type2
 - ハイブリッド
- ハードウェアの互換性リスト
 - BIOS/UEFI の互換性サポート
 - CPU 互換性サポート
 - AMD-V / Intel VT
- ホストとゲスト間のリソース配分
 - CPU
 - ストレージ
 - メモリー
 - ネットワーク接続
 - ダイレクトアクセス(ブリッジング)と NAT の違い
 - 仮想 NIC
 - 仮想スイッチ
 - ビデオカード

第3章 ストレージ(12%)

3.1 与えられたシナリオに基づいて、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、展開することができる。

- ディスクの仕様
 - RPM
 - 寸法/規格
 - 容量
 - バス幅
 - IOPS
 - シークタイムとレイテンシー(遅延)
 - 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
- インターフェース
 - SAS
 - SATA
 - SCSI
 - USB
 - ファイバーチャネル
- ハードディスクと SSD の違い

3.2 与えられたシナリオに基づいて、最適な方法(ベストプラクティス)を使用して RAID を設定することができる。

- RAID のレベルとパフォーマンスの考慮
 - 0
 - 1
 - 5
 - 6
 - 10
- ソフトウェア RAID とハードウェア RAID の違い
 - パフォーマンスの考慮
- 設定上の要件
 - 容量
 - バスの種類
 - ドライブ RPM
- ホットスワップのサポートと分岐
- ホットスペアとコールドスペアの違い
- アレイコントローラー
 - メモリー
 - バッテリーバックアップ式キャッシュ
 - 冗長コントローラー

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を要約することができる。

- DAS
- NAS
 - iSCSI
 - FCoE
- SAN
 - ファイバーチャネル
 - LUN と LUN マスキング

- HBA とファブリックスイッチ
- JBOD
- テープ
 - ドライブ
 - ライブラリー
- 光学ドライブ
- フラッシュ/コンパクトフラッシュ/USB ドライブ

3.4 与えられたシナリオに基づいて、将来的な成長を見越した適切なストレージ容量と計画を算出することができる。

- 10 進数と 2 進数のディスクサイズの計算(1000 と 1024 の違い)
- ディスククォータ
- 圧縮
- 容量計画の考慮
 - オペレーティングシステムの拡張
 - パッチ
 - サービスパック
 - ログファイル
 - テンポラリーディレクトリー
 - データベース
 - アプリケーションサーバー
 - ファイルサーバー
 - アーカイブ

第4章 セキュリティ(13%)

4.1 物理セキュリティの方法と概念を比較対照することができる。

- 多要素認証
 - 何を持っているか
 - 何を知っているか
 - 誰か
- セキュリティの概念
 - マントラップ
 - RFID チップ
 - ID カード
 - バイオメトリック
 - キーパッド
 - アクセスリスト
 - セキュリティガード
 - セキュリティカメラ
 - キーロック(Keys&Locks)
 - キャビネット
 - ラックマウント
 - サーバー
 - 安全(Safe)

4.2 与えられたシナリオに基づいて、サーバー要塞化の手法を適用することができる。

- OS の要塞化
 - 不必要なサービスの停止/不必要なポートを閉じる
 - 必要とされるソフトウェアのみをインストールする
 - 最新のシステムパッチをインストールする
- アプリケーションの要塞化
 - 最新のパッチをインストールする
 - 不必要なサービス/役割/機能を無効にする
- エンドポイントセキュリティ
 - HIDS
 - アンチマルウェア
- 脆弱性スキャンを基にセキュリティの問題を修正する
- ハードウェアの要塞化
 - 不必要なハードウェア、物理ポート、デバイスを無効にする
 - BIOS のパスワード
 - WOL(Wake on LAN)を無効にする
 - ブートの順序を設定する
 - シャーシロック/侵入検知

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を説明することができる。

- ファイアーウォール
 - ネットワークベース
 - ホストベース
- ポートセキュリティ/802.1x / NAC
- ルーターアクセスリスト
- NIDS

- 認証プロトコル
 - LDAP
 - RADIUS
 - TACACS
 - TACACS+
- PKI
 - 秘密鍵
 - 公開鍵
 - 認証局 (Certificate authority)
 - SSL/TLS
- VPN
- IPsec
- VLAN
- セキュリティゾーン
 - DMZ
 - パブリックとプライベート
 - イン트라ネットとエクストラネット

4.4 企業のポリシーに基づいて、論理的なアクセス制御の方法を実装することができる。

- アクセスコントロールリスト
 - ユーザー
 - グループ
 - 役割 (ロール)
 - リソース
 - ファイルシステム
 - ネットワーク ACL
 - 周辺機器
 - 管理者権限
 - 配布リスト
- パーミッション (権限)
 - Read (読み取り)
 - Write/Modify (書き込み/変更)
 - Execute (実行)
 - Delete (削除)
 - フルコントロール/スーパーユーザー
 - ファイルとシェアの違い

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テクニックを実行することができる。

- ストレージの暗号化
 - ファイルレベルの暗号化
 - ディスクの暗号化
 - テープの暗号化
- ストレージメディア
 - ソフトウェアレベルでの消去
 - ファイルの削除
 - ハードウェアレベルでの消去
 - 全てのセクターのゼロアウト
 - 物理的な破壊
 - リモートワイプ

4.6 与えられたシナリオに基づいて、適切な環境管理と手法を実施することができる。

- 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)
 - UPS
 - ランタイムとバッテリー容量の検討
 - 接続されたデバイスの自動正常のシャットダウン
 - 電源の定期的なテスト
 - 最大負荷
 - バイパス回路
 - リモート管理
 - PDU(電源タップ)
 - 別々の回路へと接続する冗長的なラック PDU
 - キャパシテ計画
 - PDU の評価
 - UPS の評価
 - 潜在的な消費電力
 - 複数回路
 - 電源を別にした PDU の冗長構成
- 安全性
 - ESD の手順
 - 消火設備
 - 適切な持ち上げ方法
 - ラックの安全性
 - 床荷重の制限
 - シャープエッジとピンチポイント
- HVAC
 - 部屋とラックの温度と湿度
 - 監視とアラート通知
 - 空気の流れ
 - フィラーパネル/バッフル/ブランクパネル
 - ホットアイルとコールドアイル

第5章 ネットワーク(10%)

5.1 与えられたシナリオに基づき、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ことができる。

- IPv4 と IPv6 の違い
- デフォルトゲートウェイ
- CIDR 表記とサブネットティング
- パブリック IP アドレスとプライベート IP アドレス
- 静的 IP 割り当てと DHCP の違い
- DNS
 - FQDN
 - プライマリ DNS サフィックス/ドメイン検索
- WINS
- NetBIOS
- NAT/PAT
- MAC アドレス
- ネットワークインターフェースカードの設定
 - NIC チューニング
 - 二重通信
 - 全二重
 - 半二重
 - オート
 - 速度
 - 10/100/1000 Mbps
 - 10 Gbps

5.2 様々なポートとプロトコルを比較対照することができる。

- TCP と UDP の違い
- SNMP 161
- SMTP 25
- FTP 20/21
- SFTP 22
- SSH 22
- SCP 22
- NTP 123
- HTTP 80
- HTTPS 443
- TELNET 23
- IMAP 143
- POP3 110
- RDP 3389
- FTPS 989/990
- LDAP 389/3268
- DNS 53
- DHCP 68

5.3 与えられたシナリオに基づき、ケーブルを敷設し、適切なケーブル管理手順を実施することができる。

- カッパー・ケーブル(銅線)

- パッチケーブル
 - クロスオーバー
 - ストレート
 - ロールオーバー
- CAT5
- CAT5e
- CAT6
- ファイバーケーブル
 - シングルモード
 - マルチモード
- コネクタ
 - ST
 - LC
 - SC
 - SFP
 - RJ-45
 - RJ-11
- ケーブルの設置とルーティング
 - ケーブルチャンネル
 - ケーブルマネジメントトレイ
 - 縦配線用
 - 横配線用
 - ラベリング
 - 曲げ半径
 - ケーブルバンド

第6章 災害復旧(9%)

6.1 災害復旧原則の重要性を説明することができる。

- サイトの種類
 - 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(複製)の方法
 - Disk to disk
 - Server to server
 - Site to site
- 運用の継続
 - 災害復旧計画
 - 事業継続計画
 - ビジネスインパクト分析
 - 誰が影響を受けるか
 - どんな影響を受けるか
 - 影響の重要度

6.2 与えられたシナリオに基づき、適切なバックアップの手法を実行することができる。

- バックアップ手法
 - フル/通常
 - コピー
 - 増分
 - 差分
 - スナップショット
 - 部分バックアップ
 - ベアメタル回復
 - オープンファイル
 - データ復元と OS 復元の違い
- バックアップメディア
 - リニアアクセス
 - テープ
 - ランダムアクセス
 - ディスク
 - リムーバルメディア
 - 光メディア
- メディアと復元の最適手法(ベストプラクティス)
 - ラベリング
 - 整合性の検証
 - 復元のテスト
 - テープのローテーションと保持
- メディアの保管場所
 - オフサイト
 - オンサイト
 - セキュリティの検討
 - 保管環境の検討

第7章 トラブルシューティング(20%)

7.1 トラブルシューティングの理論と方法を説明することができる。

- 問題を特定し、影響範囲を判断する
 - ユーザー/ステークホルダーに質問を行い、サーバー/環境に加えた変更について特定する
 - 必要となる文書/ログを収集する
 - 可能であれば、必要に応じて問題を再現する
 - 可能であれば、変更を行う前にバックアップを実行する
- 明確な質問により、可能性の高い原因の仮説を立てる
 - 複数の問題を引き起している障害に共通の要素があるかどうかを確認する
- 原因を判断する理論をテストする
 - 理論が裏付けられたら、問題解決のための次のステップを決定する
 - 理論が裏付けられない場合は、新しい理論を確立するか、エスカレーションを行う
- 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
- 解決策を実行し、必要に応じてエスカレーションする
 - 一度に一つの変更のみを行い、問題が解決するかをテスト/確認する
 - 問題が解決しない場合は、実施した変更を元に戻し、新しい変更を実施する
- システム全体の機能を確認し、該当する場合には、適切な予防策を講じる
- 根本的な原因分析を実施する
- 発見事項、対応、結果を文書化する

7.2 与えられたシナリオに基づき、適切なツールと方法を選択した上で、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ことができる。

- 一般的な障害
 - POST の失敗
 - 加熱
 - メモリーの障害
 - オンボードコンポーネントの障害
 - プロセッサの障害
 - 不正なブートシーケンス
 - 拡張カードの障害
 - Operating system not found エラー
 - ドライブの障害
 - 電源装置の障害
 - I/O の障害
- 障害に共通する原因
 - サードパーティにより提供されているコンポーネント、または互換性のないコンポーネント
 - 互換性のない、または不適切な BIOS
 - 冷却装置の障害
 - コンポーネントの不一致
 - バックプレーンの障害
- 環境の問題
 - 埃
 - 湿度
 - 温度
 - 電源サージ/故障
- ハードウェアツール
 - 電源テスター(マルチメーター)
 - ハードウェアの診断

- エアダスター (Compressed air)
- ESD (静電気放電) 設備

7.3 与えられたシナリオに基づいて、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ことができる。

- 一般的な障害
 - ユーザーがログインできない
 - ユーザーがリソースにアクセスできない
 - メモリーリーク
 - ブルースクリーン (BSOD) / STOP エラー
 - OS boot failure
 - ドライバーの問題
 - プロセスの暴走
 - ドライブをマウントできない
 - システムログの書き込みができない
 - OS のパフォーマンスが遅い
 - パッチアップデートの失敗
 - サービスの失敗
 - シャットダウンできない
 - ユーザーが印刷できない
- 一般的な障害の原因
 - ユーザーアクセスコントロール (UAC/SUDO)
 - 破損したファイル
 - ハードディスクの空き容量の不足
 - システムリソースの不足
 - 仮想メモリー (設定のミス、破損)
 - フラグメンテーション
 - プリンタサーバーのドライバー/サービス
 - プリントスプーラー
- ソフトウェアツール
 - システムログ
 - 監視ツール (リソースモニター、パフォーマンスモニター)
 - デフラグツール
 - ディスク管理ツール (使用領域、空き領域、ボリューム/ドライブマップ)

7.4 与えられたシナリオに基づき、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ことができる。

- 一般的な障害
 - インターネットに接続できない
 - メールの送受信ができない
 - リソースが使用できない
 - DHCP サーバーが正しく設定されていない
 - 機能しない、または到達しない
 - Destination host unreachable エラー
 - Unknown host エラー
 - デフォルトゲートウェイが正しく設定されていない
 - サービスプロバイダーでの障害
 - ホスト名/FQDN を検索できない

- 一般的な障害の原因
 - 不適切な IP アドレス
 - VLAN の設定
 - ポートセキュリティ
 - 不適切なサブネッティング
 - コンポーネントの障害
 - 誤った OS ルーティングテーブル
 - ケーブル不良
 - ファイアウォール(正しく設定されていない、ハードウェアの故障、ソフトウェアの不具合)
 - NIC が正しく設定されていない、ルーター/スイッチの障害
 - DNS と DHCP いずれか/両方の障害
 - hosts ファイルが正しく設定されていない
 - IPv4 と IPv6 の不適切な設定の違い
- ネットワークツール
 - ping
 - tracert / traceroute
 - ipconfig / ifconfig
 - nslookup
 - net use / mount
 - route
 - nbtstat
 - netstat

7.5 与えられたシナリオに基づき、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ことができる。

- 一般的な障害
 - ファイルへのアクセスが遅い
 - OS not found エラー
 - データが利用できない
 - バックアップが実行できない
 - エラーランプ
 - デバイスのマウントができない
 - ドライブが利用できない
 - 論理ドライブにアクセスできない
 - データの破損
 - I/O パフォーマンスが遅い
 - リストアの障害
 - キャッシュの失敗
 - 複数ドライブの障害
- 一般的な障害の原因
 - メディアの障害
 - ドライブの障害
 - コントローラーの障害
 - HBA の障害
 - 接続が緩んでいる
 - ケーブルの障害
 - 正しく設定されていない
 - 不適切なターミネーション
 - ブートセクターの破損
 - ファイルシステムテーブルの破損

- アレイの再構築
- 不適切なディスクパーテーション
- セクター不良
- キャッシュバッテリーの障害
- キャッシュの遮断
- 容量不足
- 不適切な RAID の設定
- 不適切なドライブ
- バックプレーンの障害
- ストレージツール
 - パーティショニングツール
 - ディスク管理
 - RAID アレイ管理
 - アレイ管理
 - システムログ
 - net use / mount コマンド
 - 監視ツール

7.6 与えられたシナリオに基づき、適切なツールと方法を選択し、セキュリティ関連する障害を効果的に診断することができる。

- 一般的な障害
 - ファイルの完全性の問題
 - 権限昇格
 - アプリケーションが読み込むことができない
 - ネットワークファイル/共有ファイルにアクセスできない
 - ファイルを開くことができない
 - 過度のアクセス
 - 過度のメモリー使用率
- 一般的な障害の原因
 - 開放されたポート
 - 有効なサービス
 - 無効なサービス
 - 侵入検知の設定
 - アンチマルウェアの設定
 - ローカルポリシー/グループポリシー
 - ファイアウォールルール
 - 不適切に設定された権限
 - ウイルス感染
 - 悪意のあるプロセス/悪意のあるサービス
- セキュリティツール
 - ポートスキャナー
 - スニファー
 - 暗号化
 - チェックサム
 - telnet クライアント
 - アンチマルウェア

CompTIA Server+ 略語一覧

下記はCompTIA Server+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。

*nix	Unix/Linux/Solaris/OS X/BSD
ACL	Access Control List
AD	Active Directory
AIT	Advanced Intelligent Tape
AMD-V	AMD Virtualization
ARM	Advanced RISC Machines
BBWC	Battery-Backed Write Cache
BIOS	Basic Input/Output System
BSOD	Blue Screen of Death
CAS	Column Address Strobe
CAT5	Category 5
CAT5e	Category 5 enhanced
CAT6	Category 6
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interpreter
CMOS	Complementary Metal Oxide Semiconductor
CPU	Central Processing Unit
CRU	Customer Replaceable Unit
CUPS	Common Unix Printing System
DAS	Direct Attached Storage
DC	Domain Controller
DDoS	Distributed Denial of Service
DDR	Double Data Rate
DDR2	Double Data Rate2
DDR3	Double Data Rate3
DHCP	Dynamic Host Configuration Protocol
DLT	Digital Linear Tape
DMA	Direct Memory Access
DMZ	Demilitarized Zone
DNS	Domain Name Service
DSRM	Directory Services Restore Mode
DTX	Discontinuous Transmission
ECC	Error Correcting Code
ESD	Electrostatic Discharge
FAT	File Allocation Table
FCoE	Fibre Channel over Ethernet
FQDN	Fully Qualified Domain Name
FRU	Field Replaceable Unit
FTP	File Transfer Protocol
FTPS	File Transfer Protocol over SSL
GFS	Grandfather Father Son
GPU	Graphics Processing Unit
GUI	Graphical User Interface
HBA	Host Bus Adapter
HCL	Hardware Compatibility List
HID	Human Interface Device

HIDS	Host Intrusion Detection System
HIPS	Host Intrusion Prevention System
HTTP	Hyper Text Transport Protocol
HTTPS	Secure Hyper Text Transport Protocol
HVAC	Heating Ventilation and Air Conditioning
iDRAC	Integrated Dell Remote Access Control
IIS	Internet Information Services
ILO	Integrated Lights Out
IMAP4	Internet Mail Access Protocol
Intel-VT	Intel Virtualization Technology
IOPS	Input Output Operations per Second
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPSEC	Internet Protocol Security
IPv6	Internet Protocol Version 6
iSCSI	Internetworking Small Computer System Interface
JBOD	Just a bunch of disks
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LC	Local Connector
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
LKGC	Last Known Good Configuration
LOM	Lights Out Management
LTO	Linear Tape-Open
LUN	Logical Unit Number
MIB	Management Information Base
MMC	Microsoft Management Console
MTTR	Mean Time To Recover
NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NEMA	National Electronic Manufacturers Association
NetBIOS	Network Basic Input Output System
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NLB	Network Load Balancing
NOS	Network Operating System
NTFS	New Technology File System
NTP	Network Time Protocol
NX	No Execute
OEM	Original Equipment Manufacturer
OS	Operating System
OSPF	Open Shortest Path First
OTDR	Optical Time Domain Reflectometer
PAT	Port Address Translation
PBX	Private Branch Exchange
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
PCI-X	Peripheral Component Interconnect Extended

PDU	Power Distribution Unit
PKI	Public Key Infrastructure
POP3	Post Office Protocol (version 3)
POST	Power on Self-Test
PXE	Preboot Execution Environment
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Inexpensive/Integrated Disks/Drives
RAM	Random Access Memory
RAS	Remote Access Server
RDP	Remote Desktop Protocol
RFID	Radio Frequency Indemnification
RIS	Remote Installation Service
RISC	Reduced Instruction Set Computer
RJ-45	Registered Jack 45
RPM	Rotations per Minute
SAN	Storage Area Network
SAS	Serial Attached SCSI
SATA	Serial ATA
SC	Standard Connector
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Small Form Factor Pluggable
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SMP	Symmetric Multiprocessing
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Straight Tip
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol / Internet Protocol
TDR	Time Domain Reflectometer
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UAC	User Account Control
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UFS	Unix File System
UID	Unit Identification
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMFS	VMWare File System
VNC	Virtual Network Computing
VoIP	Voice over IP
VPN	Virtual Private Network

VRM	Voltage Regulator Module
VSS	Volume Shadow Service
VT	Virtualization Technology
WBEM	Web-based Enterprise Management
WDS	Windows Deployment Services
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
WOL	Wake on LAN
WORM	Write Once Read Many
WSUS	Windows Software Update Services
XD	Execute Disable
ZFS	Zettabyte File System

CompTIA Server+ トレーニング用推奨機材一覧

機器

- サーバー
- 複数 NIC
- リモート管理インターフェース
- RAID コントローラー
- SAS ドライブ、または SATA ドライブ
- 一般的なラックエンクロージャー
- ラップトップ、またはデスクトップ
- スイッチ
- イーサネットケーブル
- 光ファイバーケーブル
- スマート UPS
- PDU
- LCD スクリーン
- KVM
- シリアルケーブル
- サーモスタット
- 冷却デバイス

予備のパーツ/ハードウェア

- ハードディスク
- RAM
- 電源装置
- ケーブル
- 電源ケーブル
- ケーブル/zip wrap

ツール

- 回路計 (デジタルマルチメータ)
- ドライバー
- レンチ
- ハンマー
- 懐中電灯
- 掃除機
- エアダスター
- ケーブルテスター

ソフトウェア

- 仮想化ソフトウェア
- 複数種のサーバー用オペレーティングシステム (Windows/Linux)
- ホストベースセキュリティスイツ
- 脆弱性評価のソフトウェア
- PuTTY
- パケットアナライザー
- NMAP