



CompTIA A+認定資格試験： Core 2出題範囲

試験番号：CORE 2 (220-1002)



試験について

受験者は、CompTIA A+ Core2受験に際し、本出題範囲をご確認ください。CompTIA A+認定資格を取得するためには、Core1 (220-1001) とCore2 (220-1002) の2つの試験に合格する必要があります。CompTIA A+ Core 2では、エントリーレベルのITプロフェッショナルに相当する必要なスキルを評価します。CompTIA A+ 220-1002試験は、少なくとも12ヶ月の実務経験で得られる知識やスキルを目安に設計されています。

- ・顧客の要求に基づいたコンポーネントの組み立て
- ・エンドユーザー向けPC、モバイル機器、ソフトウェアのインストール、構成、保守
- ・ネットワークングおよびセキュリティ/フォレンジックについての基本的理解
- ・ハードウェアおよびソフトウェアに起こる一般的な問題の適切で安全な診断・解決・記録
- ・トラブルシューティングスキルの実践
- ・適切なカスタマーサポートの提供
- ・スクリプティング、仮想化、デスクトップイメージング、運用環境の展開についての基本的理解

ここに掲載された例は出題の目的を明確にするためのものであり、試験の出題内容を完全に網羅した一覧ではありませんので、ご注意ください。

認定資格試験の認証

CompTIA A+は、ISO 17024標準への準拠を米国国家規格協会 (ANSI) より認定されており、定期的な出題範囲の見直しおよびアップデートを行っています。

試験開発

CompTIA試験は、エントリーレベルの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一読ください。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) までお問い合わせください。

注意事項

箇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。本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。必要に応じて、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けます。

試験情報

試験番号	CompTIA A+ Core2 (220-1102)
問題数	最大90問
出題形式	単一/複数選択、パフォーマンスベーステスト
試験時間	90分
推奨経験	ITサポートスペシャリストとしての12カ月の経験
合格ライン	700 (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 オペレーティングシステム	27%
2.0 セキュリティ	24%
3.0 ソフトウェアのトラブルシューティング	26%
4.0 運用手順	23%
計	100%



1.0 オペレーティングシステム

1.1 一般的なオペレーティングシステムの種類とその目的を比較対照できる。

- | | | |
|---|--|--|
| <ul style="list-style-type: none"> • 32ビットと64ビット <ul style="list-style-type: none"> - RAMの制限 - ソフトウェアの互換性 • ワークステーションのオペレーティングシステム <ul style="list-style-type: none"> - Microsoft Windows - Apple Macintosh OS - Linux | <ul style="list-style-type: none"> • 携帯電話/タブレットのオペレーティングシステム <ul style="list-style-type: none"> - Microsoft Windows - Android - iOS - Chrome OS • ベンダー固有の制限 <ul style="list-style-type: none"> - End-of-life - 更新の制限 | <ul style="list-style-type: none"> • オペレーティングシステム間の互換性の問題 |
|---|--|--|

1.2 Microsoft Windowsバージョンの機能を比較対照できる。

- | | | |
|---|--|---|
| <ul style="list-style-type: none"> • Windows 7 • Windows 8 • Windows 8.1 • Windows 10 | <ul style="list-style-type: none"> • 法人と個人のニーズ <ul style="list-style-type: none"> - ドメインアクセス - BitLocker - メディアセンター | <ul style="list-style-type: none"> - BranchCache - EFS • デスクトップスタイル/ユーザーインターフェース |
|---|--|---|

1.3 一般的なOSインストール時の考慮事項とアップグレード方法を要約できる。

- | | | |
|--|--|---|
| <ul style="list-style-type: none"> • ブート方法 <ul style="list-style-type: none"> - 光ディスク (CD-ROM、DVD、Blu-ray) - 外付けドライブ/フラッシュドライブ (USB/eSATA) - ネットワークブート (PXE) - 内蔵固定ディスク (HDD/SSD) - 内蔵ハードドライブ (パーティション) • インストールのタイプ <ul style="list-style-type: none"> - 無人インストール - インプレースアップグレード - クリーンインストール - リペアインストール - マルチブート - リモートネットワークインストール - イメージの展開 - リカバリーパーティション - リフレッシュ/復元 | <ul style="list-style-type: none"> • パーティショニング <ul style="list-style-type: none"> - ダイナミック - ベーシック - プライマリ - 拡張 - 論理 - GPT • ファイルシステムのタイプ/フォーマット <ul style="list-style-type: none"> - ExFAT - FAT32 - NTFS - CDFS - NFS - ext3、ext4 - HFS - スワップパーティション - クイックフォーマットとフルフォーマット | <ul style="list-style-type: none"> • 必要に応じて、代替のサードパーティ製ドライバーをロードする • ワークグループとドメインのセットアップ • 時刻/日付/地域/言語の設定 • ドライバのインストール、ソフトウェアおよびWindowsのアップデート • 工場出荷時リカバリーパーティション • 正しいパーティション/フォーマットに設定されたブートドライブ • 必要条件/ハードウェアの互換性 • アプリケーションの互換性 • OSの互換性/アップグレードパス |
|--|--|---|



1.4 与えられたシナリオに基づいて、適切なMicrosoftのコマンドラインツールを使用できる。

- ナビゲーション
 - dir
 - cd
 - ..
- ipconfig
- ping
- tracert
- netstat
- nslookup
- shutdown
- dism
- sfc
- chkdsk
- diskpart
- taskkill
- gpupdate
- gpresult
- format
- copy
- xcopy
- robocopy
- net use
- net user
- [command name]/?
- 一般権限と管理者権限のそれぞれで利用可能なコマンドの違い

1.5 与えられたシナリオに基づいて、Microsoftオペレーティングシステムの機能とツールを使用できる。

- 運用管理
 - コンピューターの管理
 - デバイスマネージャー
 - ローカルユーザーとグループ
 - ローカルセキュリティポリシー
 - パフォーマンスモニター
 - サービス
 - システム構成
 - タスクスケジューラー
 - コンポーネントサービス
 - データソース
 - 印刷管理
 - Windowsメモリ診断
 - Windowsファイアウォール
 - セキュリティの詳細
 - イベントビューアー
 - ユーザーアカウント管理
- MSConfig
 - 全般
 - ブート
 - サービス
 - スタートアップ
 - ツール
- タスクマネージャー
 - アプリケーション
 - プロセス
 - パフォーマンス
 - ネットワーク
 - ユーザー
- ディスクの管理
 - ドライブのステータス
 - マウント
 - 初期化
 - パーティションの拡張
 - パーティションの分割
- パーティションの縮小
- ドライブ文字の割り当て/変更
- ドライブの追加
- アレイの追加
- ストレージスペース
- システムユーティリティ
 - Regedit
 - Command
 - Services.msc
 - MMC
 - MSTSC
 - Notepad
 - Explorer
 - Msinfo32
 - DxDiag
 - ディスクのデフラグ
 - システムの復元
 - Windowsアップデート

1.6 与えられたシナリオに基づいて、Microsoft Windowsのコントロールパネルユーティリティを使用できる。

- インターネットオプション
 - 接続
 - セキュリティ
 - 全般
 - プライバシー
 - プログラム
 - 詳細設定
- ディスプレイ/ディスプレイ設定
 - 解像度
 - 色の解像度
 - リフレッシュレート
- ユーザーアカウント
- フォルダーオプション
 - 隠しファイルを表示
 - 拡張子を非表示
 - 全般オプション
 - オプションの表示
- システム
 - パフォーマンス（仮想メモリ）
 - リモート設定
 - システム保護
- Windowsファイアウォール
- 電源オプション
 - 休止状態
 - 電源プラン
- スリープ/一時停止
- スタンバイ
- 資格情報マネージャー
- プログラムと機能
- ホームグループ
- デバイスとプリンター
- サウンド
- トラブルシューティング
- ネットワークと共有センター
- デバイスマネージャー
- BitLocker
- 同期センター



1.7 アプリケーションのインストールと構成のコンセプトを要約できる。

- システム要件
 - ドライブスペース
 - RAM
- OS要件
 - 互換性
- インストールと展開の方法
 - ローカル (CD/USB)
 - ネットワークベース
- ローカルユーザー権限
 - インストール用のフォルダー/ファイルアクセス
- セキュリティの考察
 - デバイスへの影響
 - ネットワークへの影響

1.8 与えられたシナリオに基づいて、クライアント/デスクトップに Microsoft Windows ネットワーキングを設定できる。

- ホームグループとワークグループ
- ドメインのセットアップ
- ネットワーク共有/管理者共有/ドライブのマッピング
- プリンター共有とネットワークプリンターマッピング
- ネットワーク接続の確立
 - VPN
 - ダイアルアップ
 - 無線
 - 有線
 - WWAN (携帯電話)
- プロキシの設定
- リモートデスクトップ接続
- リモートアシスタンス
- ホーム、社内、パブリックネットワークの設定
- ファイアウォールの設定
 - 例外
 - 構成
 - Windowsファイアウォールの有効化/無効化
- Windowsでの代替IPアドレスの設定
 - IPアドレス指定
 - サブネットマスク
 - DNS
 - ゲートウェイ
- ネットワークカードのプロパティ
 - 半二重/全二重/自動
 - 速度
 - Wake-on-LAN
 - QoS
 - BIOS (オンボードNIC)

1.9 与えられたシナリオに基づいて、Mac OSとLinuxクライアント/デスクトップオペレーティングシステムの機能とツールを使用できる。

- ベストプラクティス
 - 定期的なバックアップ
 - 定期的なディスクメンテナンス
 - システムアップデート/App Store
 - パッチ管理
 - ドライバー/ファームウェアの更新
 - アンチウイルス/マルウェア対策の更新
- ツール
 - バックアップ/Time Machine
 - 復元/スナップショット
 - イメージリカバリ
 - ディスクメンテナンスユーティリティ
 - シェル/ターミナル
 - 画面共有
 - 強制終了
- 機能
 - 複数デスクトップ/Mission Control
 - キーチェーン
 - Spotlight
 - iCloud
 - ジェスチャー
 - Finder
 - リモートディスク
 - ドック
 - Boot Camp
- Linuxの基本コマンド
 - ls
 - grep
 - cd
 - shutdown
 - pwdとpasswd
 - mv
 - cp
 - rm
 - chmod
 - chown
 - iwconfig/ifconfig
 - ps
 - su/sudo
 - apt-get
 - vi
 - dd
 - kill



2.0 セキュリティ

2.1 物理的なセキュリティ対策の重要性を要約できる。

- ・マントラップ
- ・バッジリーダー
- ・スマートカード
- ・保安要員
- ・ドアのロック
- ・生体認証ロック
- ・ハードウェアトークン
- ・ワイヤロック
- ・サーバーロック
- ・USBロック
- ・プライバシー画面
- ・キーフォブ
- ・名簿による入館規制

2.2 論理的なセキュリティのコンセプトを説明できる。

- ・Active Directory
 - ログインスクリプト
 - ドメイン
 - グループポリシー/更新
 - 組織単位
 - ホームフォルダー
 - フォルダーのリダイレクト
- ・ソフトウェアトークン
- ・MDMポリシー
- ・ポートセキュリティ
- ・MACアドレスのフィルタリング
- ・証明書
- ・アンチウイルス/マルウェア対策
- ・ファイアウォール
- ・ユーザー認証/強力なパスワード
- ・多要素認証
- ・ディレクトリへのアクセス権
- ・VPN
- ・DLP
- ・アクセスコントロールリスト
- ・スマートカード
- ・メールフィルター
- ・信頼できる/信頼できないソフトウェアソース
- ・最小権限の原則

2.3 無線セキュリティプロトコルと認証方法を比較対照できる。

- ・プロトコルと暗号化
 - WEP
 - WPA
 - WPA2
 - TKIP
 - AES
- ・認証
 - 単要素
 - 多要素
 - RADIUS
 - TACACS

2.4 与えられたシナリオに基づいて、適切なツールと方法を使用してマルウェアを検出、削除、防止できる。

- ・マルウェア
 - ランサムウェア
 - トロイの木馬
 - キーロガー
 - ルートキット
 - ウイルス
- ・ツールと方法
 - ボットネット
 - ワーム
 - スパイウェア
 - アンチウイルス
 - アンチマルウェア
- ・リカバリコンソール
- ・バックアップ/復元
- ・エンドユーザーの教育
- ・ソフトウェアファイアウォール
- ・DNS構成

**2.5** ソーシャルエンジニアリング、脅威、脆弱性を比較対照できる。

- | | | |
|---|--|--|
| <ul style="list-style-type: none"> • ソーシャルエンジニアリング <ul style="list-style-type: none"> - フィッシング - スピアフィッシング - なりすまし - ショルダーサーフィン - テールゲート（共連れ） - ダンプスターダイビング（ゴミ箱あさり） | <ul style="list-style-type: none"> • DDoS • DoS • ゼロデイ攻撃 • 中間者攻撃 • ブルートフォース攻撃 • 辞書攻撃 • レインボーテーブル • スプーフィング | <ul style="list-style-type: none"> • システムのコンプライアンス違反 • ゾンビ |
|---|--|--|

2.6 Microsoft Windows OSの基本的なセキュリティ設定別の違いを比較対照できる。

- | | | |
|--|---|--|
| <ul style="list-style-type: none"> • ユーザーとグループ <ul style="list-style-type: none"> - 管理者 - パワーユーザー - ゲスト - 一般ユーザー • NTFSアクセス許可と共有アクセス許可 <ul style="list-style-type: none"> - 許可と拒否 | <ul style="list-style-type: none"> - フォルダーおよびファイルの移動とコピーの違い - ファイル属性 • 共有ファイルとフォルダー <ul style="list-style-type: none"> - 管理者共有とローカル共有 - 許可の伝達 - 継承 • システムファイルとフォルダー | <ul style="list-style-type: none"> • ユーザー認証 <ul style="list-style-type: none"> - シングルサインオン • 管理者として実行、一般ユーザーとして実行 • BitLocker • BitLocker To Go • EFS |
|--|---|--|

2.7 与えられたシナリオに基づいて、ワークステーションを保護するセキュリティのベストプラクティスを実装できる。

- | | | |
|--|---|---|
| <ul style="list-style-type: none"> • パスワードのベストプラクティス <ul style="list-style-type: none"> - 強力なパスワードの設定 - パスワードの失効 - スクリーンセーバーでパスワードを要求する - BIOS/UEFIのパスワード - パスワードの要求 • アカウント管理 <ul style="list-style-type: none"> - ユーザー権限の制限 - ログオン時間の制限 | <ul style="list-style-type: none"> - ゲストアカウントの無効化 - ログイン失敗時のロックアウト - タイムアウト/画面ロック - デフォルトの管理者ユーザーアカウント/パスワードの変更 - Active Directoryの基本機能 <ul style="list-style-type: none"> - アカウントの作成 - アカウントの削除 - パスワードのリセット/アカウントのロック解除 - アカウントの無効化 | <ul style="list-style-type: none"> • 自動実行の無効化 • データの暗号化 • パッチ/更新管理 |
|--|---|---|



2.8 与えられたシナリオに基づいて、モバイル機器の安全対策を実装できる。

- 画面ロック
 - 指紋認証
 - 顔認証
 - スワイプロック
 - パスコードロック
- リモートワイプ
- 現在位置アプリ
- リモートバックアップアプリ
- ログイン失敗時の制限
- アンチウイルス/マルウェア対策
- パッチ/OSアップデート
- バイオメトリック認証
- フルデバイス暗号化
- 多要素認証
- 認証アプリ
- 信頼できるソース、信頼できないソース
- ファイアウォール
- ポリシーと手順
 - BYODと会社所有デバイスの違い
 - プロファイルのセキュリティ要件

2.9 与えられたシナリオに基づいて、適切なデータ破壊と廃棄の方法を実装できる。

- 物理的な破壊
 - シュレッダー
 - 穴あけ/ハンマー
 - 電磁的破壊（消磁）
 - 焼却
 - 破棄証明書
- 再利用または転用のベストプラクティス
 - ローレベルフォーマット（物理フォーマット）と通常のフォーマット（論理フォーマット）
 - 上書き
 - 完全消去

2.10 与えられたシナリオに基づいて、SOHOワイヤレス/有線ネットワークの保護手段を構成できる。

- ワイヤレス固有の方法
 - デフォルトのSSIDの変更
 - 暗号化の設定
 - SSIDブロードキャストの無効化
 - アンテナとアクセスポイントの配置
 - 無線出力レベル
 - WPS
- デフォルトのユーザー名/パスワードの変更
- MACフィルタリングの有効化
- スタティックIPアドレスの割り当て
- ファイアウォールの設定
- ポート転送/ポートマッピング
- ポートの無効化
- コンテンツのフィルタリング/ベアレンタルコントロール
- ファームウェアの更新
- 物理的セキュリティ



3.0 ソフトウェアのトラブルシューティング

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

- ・一般的な症状
 - パフォーマンスの低下
 - 制限つき接続
 - ブートできない
 - OSが見つからない
 - アプリケーションのクラッシュ
 - ブルースクリーン
 - ブラックスクリーン
 - 印刷の問題
 - サービスが開始しない
- ・一般的な解決策
 - 起動が遅い
 - プロファイルの読み込みが遅い
 - ハードドライブのデフラグ
 - 再起動
 - タスクの中止
 - サービスの再起動
 - ネットワーク設定の更新
 - OSの再イメージ/リロード
 - 更新のロールバック
- デバイスドライバーのロールバック
- 更新の適用
- アプリケーションの修理
- ブート順の更新
- Windowsサービス/アプリケーションの無効化
- アプリケーション起動の無効化
- セーフブート
- Windowsプロファイルの再構築

3.2 与えられたシナリオに基づいて、PCのセキュリティの問題をトラブルシューティングし、解決できる。

- ・一般的な症状
 - ポップアップ
 - ブラウザーによるリダイレクト
 - セキュリティの警告
 - パフォーマンスの低下
 - インターネット接続の問題
 - PC/OSのフリーズ
 - アプリケーションのクラッシュ
- OSの更新失敗
- 偽装セキュリティツール（ローグウェア）
- スパム
- システムファイル名の変更
- ファイルの消失
- ファイルのアクセス権の変更
- メールの乗っ取り
- メールに関するユーザーからの反応
- 不明な送信済みメールへの自動返信
- アクセス拒否
- 無効な証明書（信頼されたルートCA）
- システム/アプリケーションのログエラー

3.3 与えられたシナリオに基づいて、マルウェア除去手順のベストプラクティスを使用できる。

1. マルウェア症状を特定し、調査する。
2. 感染したシステムを隔離する。
3. システムの復元を無効にする（Windowsの場合）。
4. 感染したシステムを修復する。
 - a. マルウェア対策ソフトウェアを更新する。
 - b. スキャンおよび除去テクニック（セーフモード、プリインストール環境）。
5. スキャンをスケジュールして更新を実行する。
6. システムの復元を有効にし、復元ポイントを作成する（Windowsの場合）。
7. エンドユーザーを教育する。



3.4 与えられたシナリオに基づいて、モバイルOSとアプリケ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。

• 一般的な症状

- 表示がぼやける
- 無線が途切れる
- ワイヤレス接続できない
- Bluetooth接続できない
- 外部モニターに表示できない
- タッチスクリーンが反応しない
- アプリがダウンロードできない
- パフォーマンスの低下
- 暗号化されたメールが読めない
- バッテリー寿命が極端に短い
- オーバーヒート
- システムのフリーズ
- スピーカーから音が出ない
- タッチスクリーンの反応が不正確
- システムのロックアウト
- アプリのログエラー

3.5 与えられたシナリオに基づいて、モバイルOSとアプリケーションのセキュリティ問題をトラブルシューティングすることができる。

• 一般的な症状

- 信号が途切れる/信号が弱い
- バッテリーが充電できない
- データ速度の低下
- 意図しないWiFi接続
- 意図しないBluetoothペアリング
- 個人ファイル/データの漏洩
- 制限を超えたデータ転送
- 無許可のアカウントアクセス
- 無許可の位置情報追跡
- 無許可のカメラ/マイク起動
- リソース利用率が高い



4.0 運用手順

4.1 文書の種類に関連するベストプラクティスを比較対照できる。

- ・ネットワーク構成図
- ・ナレッジベース/記事
- ・インシデントのドキュメント
- ・規則およびコンプライアンスのポリシー
- ・利用規約
- ・パスワードポリシー
- ・インベントリ管理
 - アセットタグ
 - バーコード

4.2 与えられたシナリオに基づいて、基本的な変更管理のベストプラクティスを実装できる。

- ・文書化されたビジネスプロセス
- ・変更の目的
- ・変更範囲
- ・リスク分析
- ・変更プラン
- ・エンドユーザーの承認
- ・委員会の変更
 - 承認
- ・バックアウト計画
- ・ドキュメントの変更

4.3 与えられたシナリオに基づいて、基本的な災害防止と復旧防止方法を実装できる。

- ・バックアップと復旧
 - イメージレベル
 - ファイルレベル
 - 重要なアプリケーション
- ・バックアップのテスト
- ・UPS
- ・サージ保護
- ・クラウドストレージとローカルストレージのバックアップ
- ・アカウント復旧オプション

4.4 一般的な安全手順を説明できる。

- ・機器接地
- ・コンポーネントの適切な取り扱いと保管
 - 静電気防止バッグ
 - ESDストラップ
 - ESDマット
 - 自己接地
- ・有害廃棄物の取り扱い
 - バッテリー
 - トナー
 - CRT
 - 携帯電話
 - タブレット
- ・対人安全
 - PCの修理前に電源を切る
 - 貴金属の取り外し
 - 持ち上げ技法
- 重量制限
- 電気火災への安全対策
- ケーブル管理
- 安全ゴーグル
- エアフィルターマスク
- ・政府の規制に従う



4.5 環境への影響と適切な管理措置について説明できる。

- ・取り扱いおよび廃棄に関わるMSDS文書
- ・温度、湿度レベルの認識および適切な換気
- ・電力サージ、電圧低下、停電
 - バッテリーバックアップ
 - サージサプレッサー
- ・浮遊微粒子への対策
 - 格納装置
 - エアフィルター/マスク
- ・粉塵およびゴミ
 - エアーダスター
 - 吸引クリーナー
- ・政府の規制に従う

4.6 禁止されているコンテンツ/行動への対応プロセス、プライバシー、ライセンス、ポリシーの概念を説明できる。

- ・インシデント対応
 - 初期対応
 - 身元確認
 - 正規なルートからの報告
 - データ/デバイスの保存
 - 文書の使用/文書変更
 - 証拠の連鎖
 - 証拠/文書化プロセスの追跡
- ・ライセンス/DRM/EULA
 - オープンソースライセンスと商用ライセンス
- 個人向けライセンスと企業向けライセンス
- ・規制されるデータ
 - 個人情報 (PII)
 - PCI
 - GDPR
 - 医療情報 (PHI)
- ・すべてのポリシーとセキュリティのベストプラクティスに従う

4.7 与えられたシナリオに基づいて、適切なコミュニケーション技術を使い、プロフェッショナルとして対応できる。

- ・適切な言葉を使用する・業界用語、略語、隠語はできるだけ避ける
- ・前向きな姿勢を保つ/自信を示す
- ・顧客の言葉を傾聴し (メモを取る)、途中で口を挟まない
- ・文化に配慮する
 - 適切な役職名を使用する
- ・時間を守る (遅れる場合は顧客に連絡する)
- ・注意の妨げとなる要素を取り除く
 - 私用電話
 - メッセージング/SNSサイト
 - 顧客対応中の同僚との話
 - 個人的な中断
- ・難しい顧客や状況への対処
 - 顧客との言い争い/言い訳口調を避ける
 - 顧客の問題を過小評価しない
 - 簡単に決めつけない
 - 顧客の話を確認する (詳細を質問しながら問題点を絞り込む、確認のため問題点や質問を繰り返す)
 - 自分の経験したことをSNSで公表しない
- ・すべきこと/スケジュールを明文化してこれを守り、顧客に進捗を伝える
 - 別な修理/交換オプションがある場合は顧客に伝える
 - 提供するサービスについて適切に文書化して提示する
 - 顧客/ユーザーに対して事後調査を実施し、満足度を確認する
- ・顧客の機密資料を適切に扱う
 - コンピュータ、デスクトップ、プリンターなどに置かれている資料



4.8 基本のスクリプトを特定できる。

- スクリプトファイルの種類

- .bat
- .ps1
- .vbs
- .sh
- .py
- .js

- 環境変数

- コメントシンタックス
- 基本のスクリプト構成
 - 基本ループ
 - 変数

- 基本データの種類

- 整数
- スtring

4.9 与えられたシナリオに基づいて、リモートアクセス技術を使用できる。

- RDP
- Telnet
- SSH
- サードパーティーのツール
 - 画面共有機能
 - ファイル共有
- 各アクセス方法のセキュリティについての考慮

CompTIA A+ 略語一覧

下記はCompTIA A+認定資格試験で使用される略語の一覧です。受験の際には、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	詳細説明	略語	詳細説明
AC	Alternating Current	CGA	Computer Graphics and Applications
ACL	Access Control List	CIDR	Classless Inter-Domain Routing
ACPI	Advanced Configuration Power Interface	CIFS	Common Internet File System
ADF	Automatic Document Feeder	CMOS	Complementary Metal-Oxide Semiconductor
ADSL	Asymmetrical Digital Subscriber Line	CNR	Communications and Networking Riser
AES	Advanced Encryption Standard	COMx	Communication port (x=port number)
AHCI	Advanced Host Controller Interface	CPU	Central Processing Unit
AP	Access Point	CRT	Cathode-Ray Tube
APIPA	Automatic Private Internet Protocol Addressing	DaaS	Data as a Service
APM	Advanced Power Management	DAC	Discretionary Access Control
ARP	Address Resolution Protocol	DB-25	Serial Communications D-Shell Connector, 25 pins
ASR	Automated System Recovery	DB-9	Serial Communications D-Shell Connector, 9 pins
ATA	Advanced Technology Attachment	DBaaS	Database as a Service
ATAPI	Advanced Technology Attachment Packet Interface	DC	Direct Current
ATM	Asynchronous Transfer Mode	DDoS	Distributed Denial of Service
ATX	Advanced Technology Extended	DDR	Double Data Rate
AUP	Acceptable Use Policy	DDR RAM	Double Data Rate Random Access Memory
A/V	Audio Video	DFS	Distributed File System
BD-R	Blu-ray Disc Recordable	DHCP	Dynamic Host Configuration Protocol
BIOS	Basic Input/Output System	DIMM	Dual Inline Memory Module
BD-RE	Blu-ray Disc Rewritable	DIN	Deutsche Industrie Norm
BNC	Bayonet-Neill-Concelman	DLT	Digital Linear Tape
BSOD	Blue Screen of Death	DLP	Digital Light Processing or Data Loss Prevention
BYOD	Bring Your Own Device	DMA	Direct Memory Access
CAD	Computer-Aided Design	DMZ	Demilitarized Zone
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart	DNS	Domain Name Service or Domain Name Server
CD	Compact Disc	DoS	Denial of Service
CD-ROM	Compact Disc-Read-Only Memory	DRAM	Dynamic Random Access Memory
CD-RW	Compact Disc-Rewritable	DRM	Digital Rights Management
CDFS	Compact Disc File System	DSL	Digital Subscriber Line
CERT	Computer Emergency Response Team	DVD	Digital Versatile Disc
CFS	Central File System, Common File System, or Command File System	DVD-RAM	Digital Versatile Disc-Random Access Memory
		DVD-ROM	Digital Versatile Disc-Read Only Memory
		DVD-R	Digital Versatile Disc-Recordable
		DVD-RW	Digital Versatile Disc-Rewritable

略語	詳細説明	略語	詳細説明
DVI	Digital Visual Interface	HTTP	Hypertext Transfer Protocol
DVI-D	Digital Visual Interface-Digital	HTTPS	Hypertext Transfer Protocol Secure
ECC	Error Correcting Code	I/O	Input/Output
ECP	Extended Capabilities Port	IaaS	Infrastructure as a Service
EEPROM	Electrically Erasable Programmable Read-Only Memory	ICMP	Internet Control Message Protocol
EFS	Encrypting File System	ICR	Intelligent Character Recognition
EIDE	Enhanced Integrated Drive Electronics	IDE	Integrated Drive Electronics
EMI	Electromagnetic Interference	IDS	Intrusion Detection System
EMP	Electromagnetic Pulse	IEEE	Institute of Electrical and Electronics Engineers
EPROM	Erasable Programmable Read-Only Memory	IIS	Internet Information Services
EPP	Enhanced Parallel Port	IMAP	Internet Mail Access Protocol
ERD	Emergency Repair Disk	IMEI	International Mobile Equipment Identity
eSATA	External Serial Advanced Technology Attachment	IMSI	International Mobile Subscriber Identity
ESD	Electrostatic Discharge	IP	Internet Protocol
EULA	End User License Agreement	IPConfig	Internet Protocol Configuration
EVGA	Extended Video Graphics Adapter/Array	IPP	Internet Printing Protocol
Ext2	Second Extended File System	IPS	Intrusion Prevention System
exFAT	Extended File Allocation Table	IPSec	Internet Protocol Security
FAT	File Allocation Table	IR	Infrared
FAT12	12-bit File Allocation Table	IrDA	Infrared Data Association
FAT16	16-bit File Allocation Table	IRP	Incident Response Plan
FAT32	32-bit File Allocation Table	IRQ	Interrupt Request
FDD	Floppy Disk Drive	ISA	Industry Standard Architecture
FPM	Fast Page Mode	ISDN	Integrated Services Digital Network
FSB	Front-Side Bus	ISO	International Organization for Standardization
FTP	File Transfer Protocol	ISP	Internet Service Provider
FQDN	Fully Qualified Domain Name	JBOD	Just a Bunch of Disks
GDDR	Graphics Double Data Rate	KB	Knowledge Base
GDI	Graphics Device Interface	KVM	Kernel-based Virtual Machine
GUI	Graphical User Interface	KVM	Keyboard-Video-Mouse
GUID	Globally Unique Identifier	LAN	Local Area Network
GPS	Global Positioning System	LBA	Logical Block Addressing
GPT	GUID Partition Table	LC	Lucent Connector
GPU	Graphics Processing Unit	LCD	Liquid Crystal Display
GSM	Global System for Mobile Communications	LDAP	Lightweight Directory Access Protocol
HAL	Hardware Abstraction Layer	LED	Light Emitting Diode
HAV	Hardware Assisted Virtualization	LPD/LPR	Line Printer Daemon/Line Printer Remote
HCL	Hardware Compatibility List	LPT	Line Printer Terminal
HDCP	High-Bandwidth Digital Content Protection	LVD	Low Voltage Differential
HDD	Hard Disk Drive	MAC	Media Access Control/Mandatory Access Control
HDMI	High Definition Media Interface	MAN	Metropolitan Area Network
HIPS	Host Intrusion Prevention System	MAPI	Messaging Application Programming Interface
HPFS	High Performance File System	mATX	Micro Advanced Technology Extended
HTML	Hypertext Markup Language	MAU	Media Access Unit/Media Attachment Unit
HTPC	Home Theater PC	MBR	Master Boot Record
		MBSA	Microsoft Baseline Security Analyzer

略語	詳細説明	略語	詳細説明
MDM	Mobile Device Management	PCIe	Peripheral Component Interconnect Express
MFA	Multifactor Authentication	PCIX	Peripheral Component Interconnect Extended
MFD	Multifunction Device	PCL	Printer Control Language
MFP	Multifunction Product	PCMCIA	Personal Computer Memory Card International Association
MicroDIMM	Micro Dual Inline Memory Module	PE	Preinstallation Environment
MIDI	Musical Instrument Digital Interface	PGA	Pin Grid Array
MIME	Multipurpose Internet Mail Extension	PGA2	Pin Grid Array 2
MIMO	Multiple Input Multiple Output	PGP	Pretty Good Protection
MMC	Microsoft Management Console	PII	Personally Identifiable Information
MP3	Moving Picture Experts Group Layer 3 Audio	PIN	Personal Identification Number
MP4	Moving Picture Experts Group Layer 4	PHI	Personal Health Information
MPEG	Moving Picture Experts Group	PKI	Public Key Infrastructure
MSConfig	Microsoft Configuration	PnP	Plug and Play
MSDS	Material Safety Data Sheet	PoE	Power over Ethernet
MT-RJ	Mechanical Transfer Registered Jack	POP3	Post Office Protocol 3
MUI	Multilingual User Interface	PoS	Point of Sale
NaaS	Network as a Service	POST	Power-On sSelf-tTest
NAC	Network Access Control	POTS	Plain Old Telephone Service
NAS	Network-Attached Storage	PPM	Pages Per Minute
NAT	Network Address Translation	PPP	Point-to-Point Protocol
NetBIOS	Networked Basic Input/Output System	PPTP	Point-to-Point Tunneling Protocol
NetBEUI	Networked Basic Input/Output System Extended User Interface	PRI	Primary Rate Interface
NFC	Near Field Communication	PROM	Programmable Read-Only Memory
NFS	Network File System	PS/2	Personal System/2 connector
NIC	Network Interface Card	PSTN	Public Switched Telephone Network
NiCd	Nickel Cadmium	PSU	Power Supply Unit
NiMH	Nickel Metal Hydride	PVA	Patterned Vertical Alignment
NLX	New Low-profile Extended	PVC	Permanent Virtual Circuit
NNTP	Network News Transfer Protocol	PXE	Preboot Execution Environment
NTFS	New Technology File System	QoS	Quality of Service
NTLDR	New Technology Loader	RADIUS	Remote Authentication Dial-In User Server
NTP	Network Time Protocol	RAID	Redundant Array of Independent (or inexpensive) Discs
NTSC	National Transmission Standards Committee	RAM	Random Access Memory
NVMe	Non-volatile Memory Express	RAS	Remote Access Service
OCR	Optical Character Recognition	RDP	Remote Desktop Protocol
OEM	Original Equipment Manufacturer	RF	Radio Frequency
OLED	Organic Light Emitting Diode	RFI	Radio Frequency Interference
OS	Operating System	RFID	Radio Frequency Identification
PaaS	Platform as a Service	RGB	Red Green Blue
PAL	Phase Alternating Line	RIP	Routing Information Protocol
PAN	Personal Area Network	RIS	Remote Installation Service
PAT	Port Address Translation	RISC	Reduced Instruction Set Computer
PC	Personal Computer	RJ-11	Registered Jack Function 11
PCI	Peripheral Component Interconnect	RJ-45	Registered Jack Function 45
PCI	Payment Card Industry		

略語	詳細説明	略語	詳細説明
RMA	Returned Materials Authorization	TKIP	Temporal Key Integrity Protocol
ROM	Read-Only Memory	TLS	Transport Layer Security
RPO	Recovery Point Objective	TN	Twisted Nematic
RTC	Real-Time Clock	TPM	Trusted Platform Module
RTO	Recovery Time Objective	UAC	User Account Control
SaaS	Software as a Service	UDF	User Defined Functions or Universal Disk Format or Universal Data Format
SAN	Storage Area Network	UDP	User Datagram Protocol
SAS	Serial Attached SCSI	UEFI	Unified Extensible Firmware Interface
SATA	Serial Advanced Technology Attachment	UNC	Universal Naming Convention
SC	Subscription Channel	UPnP	Universal Plug and Play
SCP	Secure Copy Protection	UPS	Uninterruptible Power Supply
SCSI	Small Computer System Interface	URL	Uniform Resource Locator
SCSI ID	Small Computer System Interface Identifier	USB	Universal Serial Bus
SD card	Secure Digital Card	USMT	User State Migration Tool
SEC	Single Edge Connector	UTM	Unified Threat Management
SFC	System File Checker	UTP	Unshielded Twisted Pair
SFF	Small Form Factor	UXGA	Ultra Extended Graphics Array
SFTP	Secure File Transfer Protocol	VA	Vertical Alignment
SIM	Subscriber Identity Module	VDC	Volts DC
SIMM	Single In-Line Memory Module	VDI	Virtual Desktop Infrastructure
SLI	Scalable Link Interface or System Level Integration or Scanline Interleave Mode	VESA	Video Electronics Standards Association
S.M.A.R.T.	Self-Monitoring, Analysis, and Reporting Technology	VFAT	Virtual File Allocation Table
SMB	Server Message Block	VGA	Video Graphics Array
SMTP	Simple Mail Transfer Protocol	VLAN	Virtual LAN
SNMP	Simple Network Management Protocol	VM	Virtual Machine
SoDIMM	Small Outline Dual Inline Memory Module	VNC	Virtual Network Computer
SOHO	Small Office/Home Office	VoIP	Voice over Internet Protocol
SP	Service Pack	VPN	Virtual Private Network
SPDIF	Sony-Philips Digital Interface Format	VRAM	Video Random Access Memory
SPGA	Staggered Pin Grid Array	WAN	Wide Area Network
SRAM	Static Random Access Memory	WAP	Wireless Access Protocol/Wireless Access Point
SSD	Solid State Drive	WEP	Wired Equivalent Privacy
SSH	Secure Shell	WIFI	Wireless Fidelity
SSID	Service Set Identifier	WINS	Windows Internet Name Service
SSL	Secure Sockets Layer	WLAN	Wireless Local Area Network
SSO	Single Sign-on	WMN	Wireless Mesh Network
ST	Straight Tip	WPA	Wireless Protected Access
STP	Shielded Twisted Pair	WPA2	WiFi Protected Access 2
SXGA	Super Extended Graphics Array	WPS	WiFi Protected Setup
TACACS	Terminal Access Controller Access-Control System	WUXGA	Wide Ultra Extended Graphics Array
TCP	Transmission Control Protocol	WWAN	Wireless Wide Area Network
TCP/IP	Transmission Control Protocol/Internet Protocol	XGA	Extended Graphics Array
TDR	Time Domain Reflectometer	ZIF	Zero-Insertion-Force
TFTP	Trivial File Transfer Protocol	ZIP	Zigzag Inline Package

CompTIA A+ ハードウェアとソフトウェアの一覧

CompTIAでは、A+認定資格試験の受験準備をされる方への参考用に、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デモ、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も役立ちます。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

- Appleタブレット/スマートフォン
- Androidタブレット/スマートフォン
- Windowsタブレット/スマートフォン
- Chromebook
- ノートパソコン (Windows/Mac/Linux)
- デスクトップパソコン (Windows/Mac/Linux)
- Active Directoryと印刷管理機能搭載Windowsサーバー
- モニター
- プロジェクター
- SOHO用小規模ルーター/スイッチ
- アクセスポイント
- VoIP電話
- プリンター
 - レーザー/インクジェット
 - 無線
 - 3Dプリンター
- サージサプレッサー
- UPS
- VRヘッドセット
- スマートデバイス (IoTデバイス)

予備のパーツ/ハードウェア

- マザーボード
- RAM
- ハードドライブ
- 電源
- ビデオカード
- サウンドカード
- ネットワークカード
- ワイヤレスNIC
- ファン/冷却装置/ヒートシンク

- CPU
- コネクタ/ケーブル
 - USB
 - HDMI
 - Etc.
- アダプター
- ネットワークケーブル
- 未終端ネットワークケーブル/コネクタ
- ACアダプター
- 光学式ドライブ
- ネジ/スタンドオフ
- 筐体
- 保守キット
- マウス/キーボード
- KVM
- コンソールケーブル

ツール

- スクリュードライバー
- マルチメーター
- ワイヤカッター
- パンチダウンツール
- クリンパー
- 電源テスター
- ケーブルストリッパー
- 標準的なテクニカルツールキット
- ESDストラップ
- サーマルペースト
- ケーブルテスター
- ケーブルトナー
- WiFiアナライザー
- SATA-USBコネクタ

ソフトウェア

- オペレーティングシステム
 - Linux
 - Chrome OS
 - Microsoft Windows
 - Mac OS
 - Android
 - iOS
- PEディスク/ライブCD
- アンチウイルスソフトウェア
- 仮想化ソフトウェア
- アンチマルウェア
- ドライバーソフトウェア