CompTIA A+ 認定資格試験 Core 2 出題範囲

試験番号：**CORE 2 (220-1102)**

CompTIA

試験について

CompTIA A+ 認定資格を取得するには、Core1 (220-1101) とCore2 (220-1102) の2つの試験に合格する必要があります。CompTIA A+ Core 1 (220-1101) および Core 2 (220-1102) 認定試験は、以下のような業務において必要とされる知識と技能を評価します。

- エンドユーザー向けのコンピューター機器、モバイルデバイス、およびソフトウェアのインストール、構成、保守を行う
- 顧客の要件を基にコンポーネントを提供する
- ネットワークの基礎を理解し、基本的なサイバーセキュリティ手法を適用して脅威を軽減する
- 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を、適切かつ安全に診断、解決、ドキュメント化する
- トラブルシューティングの技能を適用し、適切なコミュニケーション技能を用いて顧客サービスを提供する
- スクリプト、クラウド技術、仮想化、および企業環境における複数 OS のデプロイの基礎を理解する

これらのスキルは、ヘルプデスクサポート担当者、デスクトップサポート技術者、または現場サービス技術者などの職務における、12 ヵ月間の実務経験に相当します。出題範囲に掲載された項目は、認定資格試験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ものではありません。

認定資格試験の認証

CompTIA A+ Core 2 (220-1102) 試験は、国際標準化機構 (ISO) 17024 標準への準拠を、国家規格協会 (ANSI) によって認定されており、出題範囲の定期的な見直しとアップデートを行っています。

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や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」）とは提携関係になく、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。個々の教材が無許可扱いになるかどうかを確認するには、CompTIA (examsecurity@comptia.org) までメールにてご確認ください。

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。この出題範囲に掲載されてない場合でも、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	A+ Core 2 (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	ヘルプデスクのサポート技術者、デスクトップサポート技術者、または現場サービス技術者などの職務における 12 ヵ月間の実務経験
合格スコア	700（100-900 のスコア形式）

試験の出題範囲（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	31%
2.0	セキュリティ	25%
3.0	ソフトウェアのトラブルシューティング	22%
4.0	運用手順	22%
計		**100%**

Windows 11 に関する注意事項

本認定の範囲には、Microsoft が定めるメインストリームサポートが終了していない Microsoft® Windows® の各バージョン（Windows11 までのバージョンで、Windows11 を含む）が含まれます。したがって、出題範囲のメインタイトルに Microsoft Windows の特定のバージョンが示されていない場合、Windows10 および Windows11 に関連する内容がその出題範囲に含まれる場合もあります（職務に関係しているため）。

1.0 オペレーティングシステム

1.1 Microsoft Windows の各エディションの基本的な機能を識別できる。

- **Windows 10** の各エディション
  - Home
  - Pro
  - Pro for Workstations
  - Enterprise
- 機能の違い
  - ドメインアクセスとワークグループ
  - デスクトップスタイル / ユーザーインターフェース
  - Remote Desktop Protocol (RDP) が使用可能かどうか
  - ランダムアクセスメモリ (RAM) サポートの制限
  - BitLocker
  - gpedit.msc
- アップグレードパス
  - インプレースアップグレード

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

- ナビゲーション
  - cd
  - dir
  - md
  - rmdir
  - ドライブナビゲーションの入力：M C：または D：または x：
- コマンドラインツール
  - ipconfig
  - ping
  - hostname
  - netstat
  - nslookup
  - chkdsk
  - net user
  - net use
  - tracert
  - format
  - xcopy
  - copy
  - robocopy
  - gpupdate
  - gpresult
  - shutdown
  - sfc
  - [command name] /?
  - diskpart
  - pathping
  - winver

1.3 与えられたシナリオに基づいて、Microsoft Windows 10 オペレーティングシステム (OS) の機能とツールを使用できる。

- タスクマネージャー
  - サービス
  - スタートアップ
  - パフォーマンス
  - プロセス
  - ユーザー
- **Microsoft Management Console (MMC)** スナップイン
  - イベントビューアー (eventvwr.msc)
  - ディスクの管理 (diskmgmt.msc)
  - タスクスケジューラー (taskschd.msc)
  - デバイスマネージャー (devmgmt.msc)
  - 証明書マネージャー (certmgr.msc)
  - ローカルユーザーとグループ (lusrmgr.msc)
  - パフォーマンスモニター (perfmon.msc)
  - グループポリシーエディター (gpedit.msc)
- 追加ツール
  - システム情報 (msinfo32.exe)
  - リソースモニター (resmon.exe)
  - システム構成 (msconfig.exe)
  - ディスククリーンアップ (cleanmgr.exe)
  - ディスクデフラグ (dfrgui.exe)
  - レジストリエディター (regedit.exe)

1.4 与えられたシナリオに基づいて、Microsoft Windows 10 の適切な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
- デバイスとプリンター
- プログラムと機能
- ネットワークと共有センター
- システム
- **Windows Defender** ファイアウォール
- メール
- サウンド
- ユーザーアカウント
- デバイスマネージャー
- インデックスオプション
- 管理ツール
- ファイルエクスプローラーのオプション
  - 隠しファイルを表示する
  - 拡張子を表示しない
  - 全般オプション
  - オプションの表示
- 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
  - ノート PC を閉じた際の動作を選択する
  - 高速スタートアップで起動する
  - Universal Serial Bus (USB) を選択した一時停止
- **Ease of Access**

1.5 与えられたシナリオに基づいて、Windows の適切な設定を使用できる。

- 時刻と言語
- アップデートとセキュリティ
- パーソナライズ
- アプリ
- プライバシー
- システム
- デバイス
- ネットワークとインターネット
- ゲーム
- アカウント

1.6 与えられたシナリオに基づいて、クライアント / デスクトップ上で Microsoft Windows のネットワーキング機能を構成できる。

- ワークグループとドメインのセットアップ
  - 共有リソース
  - プリンター
  - ファイルサーバー
  - ドライブの割り当て
- ローカル **OS** のファイアウォール設定
  - アプリケーションの制限と例外
  - 構成
- クライアントネットワークの構成
  - インターネットプロトコル (IP) アドレススキーム
  - ドメインネームシステム (DNS) の設定
  - サブネットマスク
  - ゲートウェイ
  - 静的と動的
- ネットワーク接続の確立
  - 仮想プライベートネットワーク (VPN)
  - ワイヤレス
  - 有線
  - Wireless Wide Area Network (WWAN)
- プロキシの設定
- パブリックネットワークとプライベートネットワーク
- ファイルエクスプローラーのナビゲーション - ネットワークパス
- 従量制接続と制限

1.7 与えられたシナリオに基づいて、アプリケーションのインストールと構成に関する概念を適用できる。

- アプリケーションのシステム要件
  - 32 ビットと 64 ビットで異なるアプリケーションの要件
  - 外付けグラフィックカードと内蔵グラフィックカード
  - Video Random-Access Memory (VRAM) の要件
  - RAM の要件
  - 中央処理装置 (CPU) の要件
  - 外部ハードウェアトークン
  - ストレージの要件
- アプリケーションの **OS** 要件
  - アプリケーションの OS 互換性
  - 32 ビット OS と 64 ビット OS
- 配信方法
  - 物理メディアとダウンロード
  - ISO 搭載可能
- 新規アプリケーションに関するその他の検討事項
  - デバイスへの影響
  - ネットワークへの影響
  - オペレーションへの影響
  - ビジネスへの影響

1.8 一般的なタイプの OS とその目的を説明できる。

- ワークステーション **OS**
  - Windows
  - Linux
  - macOS
  - Chrome OS
- 携帯電話 / タブレットの **OS**
  - iPadOS
  - iOS
  - Android
- 様々なファイルシステムの種類
  - New Technology File System (NTFS)
  - File Allocation Table 32 (FAT32)
  - Third extended filesystem (ext3)
  - Fourth extended filesystem (ext4)
  - Apple File System (APFS)
  - extensible File Allocation Table (exFAT)
- ベンダーのライフサイクルによる制限
  - エンドオブライフ (EOL)
  - アップデートの制限
- **OS** 間の互換性に関する懸念

1.9 与えられたシナリオに基づいて、OS のインストールを実施し、様々な OS 環境においてアップグレードを実施することができる。

- ブート方法
  - USB
  - 光学式メディア
  - ネットワーク
  - ソリッドステート / フラッシュドライブ
  - インターネットベース
  - 外部 / ホットスワップドライブ
  - 内蔵ハードドライブ（パーティション）
- インストールの種類
  - アップグレード
  - リカバリーパーティション
  - クリーンインストール
  - イメージのデプロイ
  - 修復インストール
  - リモートネットワークインストール
  - その他の検討事項
    M サードパーティーのドライバー
- パーティショニング
  - GUID [Globally Unique IDentifier] Partition Table (GPT)
  - Master Boot Record (MBR)
- ドライブフォーマット
- アップグレードに関する検討事項
  - バックアップファイルとユーザーの選択
  - アプリケーションとドライバーのサポート / 後方互換性
  - ハードウェアの互換性
- 機能のアップデート
  - 製品ライフサイクル

1.10 macOS/ デスクトップ OS の一般的な機能とツールを識別できる。

- アプリケーションのインストールとアンインストール
  - ファイルの種類
    - .dmg
    - .pkg
    - .app
  - App Store
  - アンインストールプロセス
- **Apple ID** と企業の制限
- ベストプラクティス
  - バックアップ
  - アンチウィルス
  - アップデート / パッチ
- システムの選択
  - ディスプレイ
  - ネットワーク
  - プリンター
  - スキャナー
  - プライバシー
  - アクセシビリティ
  - Time Machine
- 機能
  - マルチデスクトップ
  - Mission Control
  - Keychain
  - Spotlight
  - iCloud
  - ジェスチャー
  - Finder
  - リモートディスク
  - ドック
- ディスクユーティリティ
- **FileVault**
- **Terminal**
- 強制終了

1.11 Linux クライアント / デスクトップ OS の一般的な機能とツールを識別できる。

- 一般的なコマンド
  - ls
  - pwd
  - mv
  - cp
  - rm
  - chmod
  - chown
  - su/sudo
  - apt-get
  - yum
  - ip
  - df
  - grep
  - ps
  - MAN
  - top
  - find
  - dig
  - cat
  - nano
- ベストプラクティス
  - バックアップ
  - アンチウイルス
  - アップデート / パッチ
- ツール
  - シェル / ターミナル
  - Samba

2.0 セキュリティ

2.1 様々なセキュリティ対策とその目的を要約できる。

- 物理的セキュリティ
  - アクセスコントロールが実施される玄関
  - バッジリーダー
  - ビデオによる監視
  - 警報システム
  - モーションセンサー
  - ドアロック
  - 機器のロック
  - 警備員
  - 侵入防止ゲート
  - 柵
- スタッフ向けの物理的セキュリティ
  - キーフォブ
  - スマートカード
  - 鍵
  - 生体認証
  - M 網膜スキャナー
  - M 指紋スキャナー
  - M 掌紋スキャナー
  - 照明
  - 磁気センサー
- 論理的セキュリティ
  - 最小権限の原則
  - アクセス制御リスト (ACL)
  - 多要素認証 (MFA)
  - E メール
  - ハードトークン
  - ソフトトークン
  - ショートメッセージサービス (SMS)
  - 音声通話
  - 認証アプリケーション
- モバイルデバイス管理 **(MDM)**
- **Active Directory**
  - ログインスクリプト
  - ドメイン
  - グループポリシー / アップデート
  - 組織単位 (OU)
  - ホームフォルダー
  - フォルダーのリダイレクト
  - セキュリティグループ

2.2 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
  - Wi-Fi Protected Access 2 (WPA2)
  - WPA3
  - Temporal Key Integrity Protocol (TKIP)
  - Advanced Encryption Standard (AES)
- 認証
  - Remote Authentication Dial-in User Service (RADIUS)
  - Terminal Access Controller Access-Control System (TACACS+)
  - Kerberos
  - 多要素

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

- マルウェア
  - トロイの木馬
  - ルートキット
  - ウイルス
  - スパイウェア
  - ランサムウェア
  - キーロガー
  - ブートセクターウイルス
  - クリプトマイナー
- ツールと方法
  - 復旧モード
  - アンチウィルス
  - アンチマルウェア
  - ソフトウェアファイアウォール
  - フィッシング対策トレーニング
  - 一般的な脅威に関するユーザー教育
  - OS の再インストール

2.4 一般的なソーシャルエンジニアリング攻撃、脅威、および脆弱性を説明できる。

- ソーシャルエンジニアリング
  - フィッシング
  - ビッシング
  - ショルダーサーフィン
  - ホエーリング
  - テールゲート（共連れ）
  - なりすまし
  - ゴミ箱あさり
  - エビルツイン
- 脅威
  - 分散型サービス拒否攻撃 (DDoS)
  - サービス拒否攻撃 (DoS)
  - ゼロデイ攻撃
  - スプーフィング攻撃
  - オンパス攻撃
  - ブルートフォース攻撃
  - 辞書攻撃
  - インサイダーの脅威
  - SQL (Structured Query Language) インジェクション
  - クロスサイトスクリプティング (XSS)
- 脆弱性
  - システムのコンプライアンス違反
  - パッチが適用されていないシステム
  - 保護されていないシステム（アンチウイルスが適用されていない / ファイアウォールが適用されていない）
  - 保守が終了した OS
  - 機器持ち込み (BYOD)

2.5 与えられたシナリオに基づいて、Microsoft Windows OS の基本的なセキュリティ設定を管理および構成できる。

- **Defender** ウイルス対策
  - アクティベート / ディアクティベート
  - 更新済みの定義
- ファイアウォール
  - アクティベート / ディアクティベート
  - ポートセキュリティ
  - アプリケーションセキュリティ
- ユーザーとグループ
  - ローカルアカウントと Microsoft アカウント
  - 一般アカウント
  - 管理者
  - ゲストユーザー
  - パワーユーザー
- **OS** のログインオプション
  - ユーザー名とパスワード
  - Personal Identification Number (PIN)
  - 指紋認証
  - 顔認識
  - シングルサインオン (SSO)
- **NTFS** パーミッションと共有パーミッション
  - ファイルとフォルダーの属性
  - 継承
- 管理者として実行、一般ユーザーとして実行
  - User Account Control (UAC)
- **BitLocker**
- **BitLocker To Go**
- **Encrypting File System (EFS)**

2.6 与えられたシナリオに基づいて、ワークステーションを構成し、セキュリティのベストプラクティスを満たすことができる。

- 保存データの暗号化
- パスワードのベストプラクティス
  - 複雑さの要件
    - M 長さ
    - M 文字の種類
  - 有効期限の要件
  - Basic Input/Output System (BIOS) /Unified Extensible Firmware Interface (UEFI) パスワード
- エンドユーザーのベストプラクティス
  - スクリーンセーバーロックを使用する
  - 使用していない場合はログオフする
  - 重要なハードウェアのセキュリティ強化 / 保護（ラップトップ PC など）
  - 個人を特定可能な情報 (PII) とパスワードのセキュリティ強化
- アカウント管理
  - ユーザー権限の制限
  - ログイン時間の制限
  - ゲストアカウントの無効化
  - 試行失敗時にロックアウトを使用
  - タイムアウト / スクリーンロックを使用
- 管理者のデフォルトユーザー名 / パスワードの変更
- 自動実行の無効化
- オートプレイの無効化

2.7 モバイルデバイスと組み込みデバイスをセキュアにする一般的な方法を説明できる。

- 画面ロック
  - 顔認識
  - PIN コード
  - 指紋認証
  - パターン
  - スワイプ
- リモートワイプ
- 現在位置アプリ
- **OS** アップデート
- デバイスの暗号化
- リモートバックアップアプリ
- ログイン失敗時の制限
- ウイルス対策 / マルウェア対策
- ファイアウォール
- ポリシーと手順
  - 機器持ち込みと会社所有
  - プロファイルのセキュリティ要件
- モノのインターネット **(IoT)**

2.8 与えられたシナリオに基づいて、データ破壊と廃棄の一般的な方法を使用できる。

- 物理的な破壊
  - ドリル
  - シュレッディング
  - 消磁
  - 焼却
- 再利用または転用のベストプラクティス
  - 消去 / ワイピング
  - ローレベルフォーマット
  - 標準フォーマット
- アウトソーシングの概念
  - サードパーティーベンター
  - 破壊 / リサイクル証明書

2.9 与えられたシナリオに基づいて、SOHO 無線 / 有線ネットワーク上で適切なセキュリティ設定を構成できる。

- ホームルーターの設定
  - デフォルトのパスワードを変更する
  - IP フィルタリング
  - ファームウェアの更新
  - コンテンツのフィルタリング
  - 物理的配置 / セキュアな場所
  - Dynamic Host Configuration Protocol (DHCP) 予約
  - 静的 WAN IP
  - Universal Plug and Play (UPnP)
  - スクリーニングされたサブネット
- ワイヤレス固有の方法
  - Service Set Identifier (SSID) の変更
  - SSID ブロードキャストの無効化
  - 暗号化の設定
  - ゲストアクセスの無効化
  - チャネルの変更
- ファイアウォールの設定
  - 未使用ポートの無効化
  - ポート転送 / ポートマッピング

2.10 与えられたシナリオに基づいて、ブラウザとそれに関連するセキュリティ設定をインストールおよび構成できる。

- ブラウザのダウンロードとインストール
  - 信頼できるソース
    M ハッシュ化
  - 信頼できないソース
- 拡張機能とプラグイン
  - 信頼できるソース
  - 信頼できないソース
- パスワードマネージャー
- セキュアな接続 / サイト – 有効な証明書
- 設定
  - ポップアップブロッカー
  - ブラウズデータの消去
  - キャッシュの消去
  - プライベートブラウジングモード
  - サインイン / ブラウザデータの同期
  - 広告ブロッカー

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、Windows OS の一般的な問題をトラブルシューティングできる。

- 一般的な症状
  - ブルースクリーン (BSOD)
  - 動作が遅い
  - ブートの問題
  - 頻繁にシャットダウンする
  - サービスが起動しない
  - アプリケーションのクラッシュ
  - メモリ不足の警告
  - USB コントローラーリソースの警告
  - システムが不安定
  - OS が見つからない
  - プロファイルの読み込みが遅い
  - 時刻のずれ
- 一般的なトラブルシューティング手順
  - 再起動
  - サービスの再起動
  - アプリケーションのアンインストール / 再インストール / アップデート
  - リソースを追加する
  - 要件を確認する
  - システムファイルのチェック
  - Windows の修復
  - 復元
  - 再イメージ
  - アップデートのロールバック
  - 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、パーソナルコンピューター (PC) の一般的なセキュリティ問題をトラブルシューティングできる。

- 一般的な症状
  - ネットワークにアクセスできない
  - デスクトップのアラート
  - アンチウイルス保護に関する偽のアラート
  - システムまたは個人ファイルの改変 M ファイルの喪失 / 名前変更
  - OS 内の望ましくない通知
  - OS のアップデート失敗
- ブラウザ関連の症状
  - ランダム / 頻繁に生じるポップアップ
  - 証明書に関する警告
  - リダイレクト

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. マルウェアの症状を調査および検証する
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化する（**Windows** の場合）
4. 感染したシステムを修復する
   a. アンチマルウェアソフトをアップデートする
   b. スキャンおよび除去のテクニック（セーフモード、プレインストール環境など）
5. スキャンをスケジュールしてアップデートを実行する
6. システムの復元を有効化し、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一般的な問題をトラブルシューティングできる。

- 一般的な症状
  - アプリケーションが起動しない
  - アプリケーションが閉じない / クラッシュする
  - アプリケーションがアップデートできない
  - 反応が遅い
  - OS がアップデートできない
  - バッテリーの寿命の問題
  - ランダムに再起動する
  - 接続の問題
    M Bluetooth
    M Wi-Fi
    M 近距離無線通信 (NFC)
    M AirDrop
  - 画面が自動回転しない

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一般的なセキュリティ問題をトラブルシューティングできる。

- セキュリティの懸念事項
  - Android パッケージ (APK) のソース
  - 開発者モード
  - ルートアクセス / 脱獄
  - ブートレグ / 悪意のあるアプリケーション
    M アプリケーションスプーフィング
- 一般的な症状
  - ネットワークトラフィックが多い
  - 応答時間が遅い
  - データ使用制限の通知
  - インターネット接続の制限
  - インターネット接続できない
  - 広告の数が多い
  - 偽のセキュリティ警告
  - アプリケーションの予期しない挙動
  - 個人ファイル / データの漏洩

4.0 運用手順

4.1 与えられたシナリオに基づいて、ドキュメント化に関するベストプラクティスを実施し、システム情報管理をサポートできる。

- チケットシステム
  - ユーザー情報
  - デバイス情報
  - 問題の説明
  - カテゴリ
  - 重大度
  - エスカレーションレベル
  - 書面での明快かつ簡潔なコミュニケーション
    - M 問題の説明
    - M 進捗ノート
    - M 問題の解決
- 資産管理
  - 在庫リスト
  - データベースシステム
  - アセットタグと ID
  - 調達ライフサイクル
  - 保証とライセンス
  - 割り当てユーザー
- ドキュメントの種類
  - 利用規約 (AUP)
  - ネットワークトポロジー図
  - 規制のコンプライアンス要件
    - M スプラッシュスクリーン
  - インシデント報告
  - 標準作業書
    - M ソフトウェアパッケージのカスタムインストール手順
  - 新規ユーザーのセットアップのチェックリスト
  - エンドユーザーの使用停止のチェックリスト
- ナレッジベース / 記事

4.2 変更管理の基本的なベストプラクティスを説明できる。

- ドキュメント化されたビジネスプロセス
  - ロールバック計画
  - サンドボックステスト
  - 責任を負うべきスタッフメンバー
- 変更管理
  - リクエストフォーム
  - 変更の目的
  - 変更範囲
  - 変更の日付と時刻
  - 影響を受けるシステム / インパクト
  - リスク分析
    - M リスクレベル
  - 変更委員会の承認
  - エンドユーザーの承認

4.3 与えられたシナリオに基づいて、ワークステーションのバックアップと復旧の手法を実施できる。

- バックアップと復旧
  - フル
  - 増分
  - 差分
  - 合成
- バックアップのテスト
  - 頻度
- バックアップのローテーションスキーム
  - オンサイトとオフサイト
  - Grandfather-Father-Son (GFS)
  - 3-2-1 バックアップルール

4.4 与えられたシナリオに基づいて、一般的な安全手順を使用できる。

- 静電気防止 **(ESD)** ストラップ
- **ESD** マット
- 機器の接地
- 適切な電源処理
- 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
- 政府の規制の遵守
- 人員の安全
  - PC の修理前に電源を切る
  - 持ち上げ方法
  - 電気火災への安全対策
  - 安全ゴーグル
  - エアフィルターマスク

4.5 環境的な影響とローカル環境のコントロールを要約できる。

- 取り扱いと廃棄に関する **MSDS**（化学物質等安全データシート）文書
  - バッテリーの正しい廃棄
  - トナーの正しい廃棄
  - その他のデバイスや資産の正しい廃棄
- 温度と湿度の認識、および適切な換気
  - ロケーション / 機器の配置
  - 清掃
  - エアーダスター / 掃除機
- 電力サージ / 電圧低下 / 電源故障
  - バッテリーバックアップ
  - サージサプレッサー

4.6 禁止されているコンテンツ / アクティビティ、およびプライバシー、ライセンス、ポリシーの各概念の重要性を説明できる。

- インシデント対応
  - 証拠の連鎖
  - 必要に応じて経営陣および法執行機関に連絡する
  - ドライブのコピー（データの完全性と保全）
  - インシデント文書
- ライセンス / デジタル著作権管理 **(DRM)** / エンドユーザー向け使用許諾契約 **(EULA)**
  - 有効なライセンス
  - 有効期限内のライセンス
  - 個人使用ライセンスと企業使用ライセンス
  - オープンソースライセンス
- 規制されるデータ
  - クレジットカードトランザクション
  - 政府発行の個人情報
  - PII
  - 健康情報
  - データ保持要件

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用し、プロフェッショナルとして対応できる。

- プロフェッショナルとしての外見と服装
  - 環境に合った服装を選ぶ
    - M フォーマル
    - M ビジネスカジュアル
- 適切な言葉を使用し、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
- 顧客の言葉に耳を傾け、メモを取り、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
  - 個人的な中断
- 難しい顧客や状況への対処
  - 顧客との言い争いや自己弁護を避ける
  - 顧客の問題を過小評価しない
  - 簡単に決めつけない
  - 顧客の話を明確にする（詳細を質問しながら問題点を絞り込む、問題点を再度述べる、質問をして理解していることを確認する）
  - 自分が経験したことを SNS で公表しない
- すべきこと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
  - 必要に応じて修理または交換の選択肢を示す
  - 提供するサービスを適切にドキュメント化して提示する
  - 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
  - コンピューター、机の上、プリンターなどに置かれている資料

4.8 スクリプトの基本を識別できる。

- スクリプトファイルの種類
  - .bat
  - .ps1
  - .vbs
  - .sh
  - .js
  - .py
- スクリプトの用途
  - 基本的な自動化
  - マシンの再起動
  - ネットワークドライブの再マッピング
  - アプリケーションのインストール
  - バックアップの自動化
  - 情報 / データ収集
  - アップデートの実行
- スクリプトを使用する際のその他の検討事項
  - 意図せずマルウェアを混入させる
  - 気づかないままシステム設定を変更する
  - リソースの取り扱いミスによるブラウザまたはシステムのクラッシュ

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。

- 手法 / ツール
  - RDP
  - VPN
  - 仮想ネットワークコンピューター (VNC)
  - Secure Shell (SSH)
  - Remote Monitoring and Management (RMM)
  - Microsoft Remote Assistance (MSRA)
  - サードパーティーのツール
    - M 画面共有ソフトウェア
    - M ビデオ会議ソフトウェア
    - M ファイル転送ソフトウェア
    - M デスクトップ管理ソフトウェア
- 各アクセス方法のセキュリティに関する検討事項

CompTIA A+ Core 2 (220-1102) 略語リスト

下記は CompTIA A+ Core 2 (220-1102) 試験で使用される略語の一覧です。包括的な試験準備プログラムの一環として、リストを復習し、知識の習得に努めてください。

略語	定義
AAA	Authentication, Authorization, and Accounting
AC	Alternating Current
ACL	Access Control List
ADF	Automatic Document Feeder
AES	Advanced Encryption Standard
AP	Access Point
APFS	Apple File System
APIPA	Automatic Private Internet Protocol Addressing
APK	Android Package
ARM	Advanced RISC [Reduced Instruction Set Computer] Machine
ARP	Address Resolution Protocol
ATA	Advanced Technology Attachment
ATM	Asynchronous Transfer Mode
ATX	Advanced Technology Extended
AUP	Acceptable Use Policy
BIOS	Basic Input/Output System
BSOD	Blue Screen of Death
BYOD	Bring Your Own Device
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CD	Compact Disc
CDFS	Compact Disc File System
CDMA	Code-Division Multiple Access
CERT	Computer Emergency Response Team
CIFS	Common Internet File System
CMD	Command Prompt
CMOS	Complementary Metal-Oxide Semiconductor
CPU	Central Processing Unit
CRL	Certificate Revocation List
DC	Direct Current
DDoS	Distributed Denial of Service
DDR	Double Data Rate

略語	定義
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual Inline Memory Module
DKIM	DomainKeys Identified Mail
DMA	Direct Memory Access
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DoS	Denial of Service
DRAM	Dynamic Random-Access Memory
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DVI	Digital Visual Interface
DVI-D	Digital Visual Interface-Digital
ECC	Error Correcting Code
EFS	Encrypting File System
EMI	Electromagnetic Interference
EOL	End-of-Life
eSATA	External Serial Advanced Technology Attachment
ESD	Electrostatic Discharge
EULA	End-User License Agreement
exFAT	Extensible File Allocation Table
ext	Extended File System
FAT	File Allocation Table
FAT12	12-bit File Allocation Table
FAT16	16-bit File Allocation Table
FAT32	32-bit File Allocation Table
FSB	Front-Side Bus
FTP	File Transfer Protocol
GFS	Grandfather-Father-Son
GPS	Global Positioning System
GPT	GUID [Globally Unique Identifier] Partition Table
GPU	Graphics Processing Unit
GSM	Global System for Mobile Communications
GUI	Graphical User Interface

略語	定義
GUID	Globally Unique Identifier
HAL	Hardware Abstraction Layer
HAV	Hardware-Assisted Virtualization
HCL	Hardware Compatibility List
HDCP	High-bandwidth Digital Content Protection
HDD	Hard Disk Drive
HDMI	High-Definition Multimedia Interface
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IaaS	Infrastructure as a Service
ICR	Intelligent Character Recognition
IDE	Integrated Drive Electronics
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Mail Access Protocol
IOPS	Input/Output Operations Per Second
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPS	In-Plane Switching
IPSec	Internet Protocol Security
IR	Infrared
IrDA	Infrared Data Association
IRP	Incident Response Plan
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITX	Information Technology eXtended
KB	Knowledge Base
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LC	Lucent Connector
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light-emitting Diode
MAC	Media Access Control/Mandatory Access Control
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MBR	Master Boot Record
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Multifunction Device
MFP	Multifunction Printer
MMC	Microsoft Management Console

略語	定義
MOU	Memorandum of Understanding
MSDS	Material Safety Data Sheet
MSRA	Microsoft Remote Assistance
MX	Mail Exchange
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NetBIOS	Networked Basic Input/Output System
NetBT	NetBIOS over TCP/IP [Transmission Control Protocol/Internet Protocol]
NFC	Near-field Communication
NFS	Network File System
NIC	Network Interface Card
NTFS	New Technology File System
NVMe	Non-volatile Memory Express
OCR	Optical Character Recognition
OLED	Organic Light-emitting Diode
ONT	Optical Network Terminal
OS	Operating System
PaaS	Platform as a Service
PAN	Personal Area Network
PC	Personal Computer
PCIe	Peripheral Component Interconnect Express
PCL	Printer Command Language
PE	Preinstallation Environment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PoE	Power over Ethernet
POP3	Post Office Protocol 3
POST	Power-On Self-Test
PPP	Point-to-Point Protocol
PRL	Preferred Roaming List
PSU	Power Supply Unit
PXE	Preboot Execution Environment
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Independent (or Inexpensive) Disks
RAM	Random-Access Memory
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFI	Radio Frequency Interference
RFID	Radio Frequency Identification
RJ11	Registered Jack Function 11
RJ45	Registered Jack Function 45
RMM	Remote Monitoring and Management
RTO	Recovery Time Objective
SaaS	Software as a Service
SAN	Storage Area Network

略語	定義
SAS	Serial Attached SCSI [Small Computer System Interface]
SATA	Serial Advanced Technology Attachment
SC	Subscriber Connector
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy Protection
SCSI	Small Computer System Interface
SDN	Software-defined Networking
SFTP	Secure File Transfer Protocol
SIM	Subscriber Identity Module
SIMM	Single Inline Memory Module
S.M.A.R.T.	Self-monitoring Analysis and Reporting Technology
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SODIMM	Small Outline Dual Inline Memory Module
SOHO	Small Office/Home Office
SPF	Sender Policy Framework
SQL	Structured Query Language
SRAM	Static Random-Access Memory
SSD	Solid-State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
ST	Straight Tip
STP	Shielded Twisted Pair
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TN	Twisted Nematic
TPM	Trusted Platform Module
UAC	User Account Control
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UNC	Universal Naming Convention
UPnP	Universal Plug and Play
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VA	Vertical Alignment
VDI	Virtual Desktop Infrastructure
VGA	Video Graphics Array
VLAN	Virtual LAN [Local Area Network]
VM	Virtual Machine
VNC	Virtual Network Computer
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRAM	Video Random-Access Memory
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN [Local Area Network]
WMN	Wireless Mesh Network
WPA	WiFi Protected Access
WWAN	Wireless Wide Area Network
XSS	Cross-site Scripting

CompTIA A+ Core 2 (220-1102) ハードウェアとソフトウェアのリスト

**CompTIA では、A+ Core 2 (220-1102) 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でも、トレーニングの提供に必要なラボ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

- 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
- 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 と印刷管理機能を搭載した Windows サーバー
- モニター
- プロジェクター
- SOHO 用ルーター / スイッチ
- アクセスポイント
- Voice over Internet Protocol (VoIP) 電話
- プリンター
  - レーザー / インクジェット
  - ワイヤレス
  - 3D プリンター
  - 感熱式
- サージサプレッサー
- 無停電電源 (UPS)
- スマートデバイス (モノのインターネット [IoT] デバイス)
- ハイパーバイザーを搭載したサーバー
- パンチダウンブロック
- パッチパネル
- ウェブカメラ
- スピーカー
- マイク

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
- ワイヤレスネットワークインタフェースカード (NIC)
- ファン / 冷却装置 / ヒートシンク
- CPU
- 各種のコネクター / ケーブル
  - USB
  - High-Definition Multimedia Interface (HDMI)
  - DisplayPort
  - Digital Visual Interface (DVI)
  - Video Graphics Array (VGA)
- アダプター
  - Bluetooth 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 / コネクター
- AC（交流）アダプター
- 光学式ドライブ
- ねじ / スタンドオフ
- 筐体
- 保守キット
- マウス / キーボード
- キーボード・ビデオ・マウス (KVM)
- コンソールケーブル
- ソリッドステートドライブ (SSD)

ツール

- ドライバー
- マルチメーター
- ワイヤーカッター
- 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
- 静電気防止 (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
- Wi-Fi アナライザー
- SATA-USB コネクター

ソフトウェア

- OS
  - Linux
  - Chrome OS
  - Microsoft Windows
  - macOS
  - Android
  - iOS
- プレインストール環境 (PE) ディスク / ライブコンパクトディスク (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

CompTIA