Training

Apple導入と管理

試験対策ガイド

目次

試験について

「Apple導入と管理」試験では、大きな組織でAppleデバイスを大規模に導入、保護、管理するために必要な、ツール、サービス、ベストプラクティスに関する理解を確認します。試験に合格すると、Apple Certified IT Professionalデジタルバッジを取得できます。さらに詳しくは、Apple Training（英語）を参照してください。

この試験は、iOS 17、iPadOS 17、macOS Sonomaを基準に作成されています。

試験に備える

試験の範囲には、「Apple導入と管理」コースのトピックに加えて、このガイドに掲載されている学習目標が含まれます。試験に合格するには、Appleの複数のリソースで学習し、Appleデバイスの導入と管理に関わる直接的な経験を積む必要があります。この試験に備えるには、経歴、技術的な専門知識、Appleデバイスの導入と管理に関わる経験に応じて、30～60時間かかります。

試験に備えるには、次のアプローチが有効です。

- 組織でのiPhone、iPad、Macユーザのサポートに習熟する。
- 組織でAppleデバイスの導入と管理に関わる実践的な経験を積む。
- このガイドの学習目標を読み、学習する必要があるリソースを特定する。
- 「Apple導入と管理」（英語）コースを完了する。内容とリンクされたリソースを学習し、演習を行い、各記事やチュートリアルの理解度チェックの質問を使って知識を強化する。
- このガイドに掲載されている例題を使用して練習する。

学習目標

導入

デバイス所有モデルが組織の導入戦略に与える影響について説明する。

- ユーザ所有デバイスを登録する（英語）
- 組織のアプリとデータを管理する（英語）
- Appleがユーザデータを組織のデータから分離する方法
- ユーザが自分の個人用デバイスを登録する方法

シングルサインオン（SSO）やEntra ID（旧Azure AD）などのID管理と認証サービスを評価し、Appleデバイス上の組織のリソースに対する安全なアクセスを管理する。

- 認証とユーザサービスを評価する（英語）
- macOSのプラットフォームシングルサインオン

Appleデバイスのプロファイルとペイロードに関して、組織のネットワークインフラストラクチャを評価する。

- ネットワークトラフィックを管理する（英語）
- Appleデバイスのネットワーク使用ルールMDMペイロードの設定

アカウント駆動型デバイス登録の要件をプロファイルベースのデバイス登録と比較する。

- アカウント駆動型デバイス登録

組織所有のデバイスを導入するシナリオで、Appleデバイスを導入する際に考慮が必要な事柄を特定する。

- 登録と設定アシスタントを管理する（英語）
- デバイス登録について（英語）
- デバイス登録とMDM
- 自動デバイス登録とMDM

シナリオに沿って、所有モデルと購入先が異なるデバイスの導入戦略を作成する。

- デバイス割り当てを管理する（英語）
- Apple Business Managerでデバイスサプライヤを管理する
- Apple School Managerでデバイスサプライヤを管理する

Apple ConfiguratorとMDMの、管理対象デバイスに関連する様々な特長と機能を比較し、対比する。

- Apple Configuratorの機能の詳細（英語）
- 「サービスに戻す」ためのデバイスの準備（英語）
- Appleデバイスを復活させる／復元する
- iPhone、iPad、またはApple TVデバイスをアップデートする／復元する

モバイルデバイス管理が、Appleデバイスで設定を構成するユーザにどのように影響するかを説明する。

- 設定アシスタントパネルのオプション
- AppleデバイスのファイアウォールMDMペイロードの設定

宣言型デバイス管理について説明する。

- MDMの仕組みを理解する(英語)
- AppleのMDMフレームワークの詳細(英語)
- デバイスにクエリーを送る(英語)
- 宣言型デバイス管理とAppleデバイスの概要
- 宣言

Appleの管理フレームワークの主な目的と機能を把握する。

- AppleのMDMフレームワークの詳細(英語)
- セキュリティ戦略を策定する(英語)
- ソフトウェアアップデートを管理する(英語)
- モバイルデバイス管理プロファイルの概要
- Appleデバイスのソフトウェア・アップデートについて
- MDMを使ってソフトウェア・アップデートをAppleデバイスに導入する
- Appleデバイスを消去する

所有権と各登録タイプの登録オプションについて説明する。

- デバイスの所有権と登録のプランニング(英語)
- セキュリティ戦略を策定する(英語)
- Appleデバイスの登録タイプの概要
- デバイス登録とMDM
- 自動デバイス登録とMDM
- Appleデバイスの監視について

Apple Business ManagerとApple School Manager

Apple Business ManagerまたはApple School Managerを組織のサードパーティMDMソリューションにリンクする。

- MDMサーバを追加する(英語)
- Apple Business Managerでサードパーティの MDMサーバにリンクする
- Apple School Managerでサードパーティの MDMサーバにリンクする

Apple Business ManagerまたはApple School Managerのディレクトリ同期要件について説明する。

- 認証とユーザサービスを評価する(英語)
- Apple Business ManagerまたはApple School Managerを使用する(英語)
- Apple Business ManagerでGoogle WorkspaceとのFederated Authenticationを使用する

Apple Business ManagerまたはApple School Managerと統合するための、パブリックIDプロバイダまたは社内IDプロバイダの基準を特定する。

- Apple Business ManagerまたはApple School Managerを使用する（英語）
- Apple School Managerが対応しているStudent Information Systems（SIS）について

組織がApple Business ManagerまたはApple School Managerを使用する理由を説明する。

- デバイスの所有権と登録のプランニング（英語）
- Apple Business ManagerまたはApple School Managerを使用する（英語）
- 配布方法を選択する（英語）
- 組織のアプリとデータを管理する（英語）
- Apple School Managerでのユーザアカウントの調査
- Apple School ManagerとStudent Information System（SIS）を統合する
- 引き換えコードから管理配布への移行
- Apple School Managerにコンテンツトークンを移行する
- Apple Business Managerにコンテンツトークンを移行する
- Appleデバイスでのコンテンツの配付の概要
- Appleデバイスの登録タイプの概要
- 自動デバイス登録とMDM

Apple Business ManagerまたはApple School Managerで様々な役割と場所を使用する目的を特定する。

- Apple Business ManagerまたはApple School Managerを使用する（英語）
- Apple School Managerでの役割と権限について

配布後のアプリとブックの一括購入ライセンスの所有者について説明する。

- アプリとブックを通じてコンテンツを購入する（英語）
- 配布方法を選択する（英語）
- 組織のアプリとデータを管理する（英語）
- Appleデバイスでのコンテンツの配付の概要

Apple ConfiguratorからApple Business ManagerまたはApple School Managerにデバイスを追加する。

- 組織にデバイスを手動で追加する（英語）
- Apple Business ManagerにApple Configuratorからデバイスを追加する
- Apple School ManagerにApple Configuratorからデバイスを追加する

Apple Business ManagerまたはApple School Managerでコンテンツを一括購入する。

- アプリとブックを通じてコンテンツを購入する（英語）
- Apple Business Managerでコンテンツトークンを管理する
- Apple School Managerでコンテンツトークンを管理する

Apple Business ManagerまたはApple School Managerでコンテンツトークンを管理する。

- アプリとブックを通じてコンテンツを購入する（英語）
- Apple Business Managerでコンテンツトークンを管理する
- Apple School Managerでコンテンツトークンを管理する

Apple Business ManagerまたはApple School Managerで別の場所にライセンスを転送する。

- アプリとブックを通じてコンテンツを購入する（英語）
- Apple Business Managerでライセンスを別の場所に転送する
- Apple School Managerでライセンスを別の場所に転送する

ネットワーク

Appleデバイスによる使用に関して、組織のネットワークインフラストラクチャ（Wi-Fiの通信範囲と容量、プロキシ、ファイアウォール、VPN、Bonjourなど）を構成する。

- ネットワークを準備する（英語）
- 適切なWi-Fiの容量を取得する
- エンタープライズネットワークでApple製品を使う
- AppleソフトウェアTCPおよびUDPポート
- インフラストラクチャ要件

Appleデバイスを既存のネットワークに統合するための要件と技術的な検討事項をまとめる。

- ネットワークを準備する（英語）
- エンタープライズネットワークでApple製品を使う

macOSのコンテンツキャッシュによって、自身のネットワークでダウンロードされたAppleコンテンツがどのようにキャッシュされ、最適化されるかを説明する。

- コンテンツキャッシュについて理解する（英語）
- コンテンツキャッシュを計画する／設定する

サブネット全体でコンテンツキャッシュがどのように機能するかを理解する。

- コンテンツキャッシュについて理解する（英語）
- コンテンツキャッシュの仕組み

管理対象AppleデバイスをWi-Fiネットワークに加えることに関する主な検討事項を把握する。

- ネットワークを準備する（英語）
- Wi-Fiネットワークに参加する（英語）
- iOS、iPadOS、macOSが自動接続するワイヤレスネットワークの決定方法

組織がAppleデバイスをネットワークに接続するために使用するワイヤレス認証方法を構成する。

- Wi-Fiネットワークに参加する（英語）
- AppleデバイスのWEP、WPA、WPA2、WPA2／WPA3のMDM設定
- ワイヤレスネットワークへの安全なアクセス
- AppleデバイスをWi-Fiネットワークに接続する方法

802.1Xワイヤレスネットワークに接続するようAppleデバイスを構成する。

- ネットワークを準備する（英語）
- Wi-Fiネットワークに参加する（英語）
- Appleデバイスを802.1Xネットワークに接続する

MDMで使用される主なペイロードと設定を特定し、管理対象Appleデバイスを構成して、サポートされる認証プロトコルを使ってサポートされるWi-Fiネットワークに自動的に接続する。

- Wi-Fiネットワークに参加する（英語）
- AppleデバイスのEAP（Extensible Authentication Protocol）のMDM設定

MDMを使ってVPN常時接続を自動的に使用するようにデバイスを構成する。

- AppleデバイスでVPNを使用する（英語）
- Appleデバイス導入でのVPNの概要

MDMソリューションの管理対象のアプリ、ドメイン、またはデバイス全体のリレーネットワーク拡張機能を構成する。

- 組織のアプリとデータを管理する（英語）
- AppleデバイスのリレーMDMペイロードの設定

AppleデバイスのWi-Fiおよびモバイルネットワークのネットワークの優先順位を構成する。

- Wi-Fiネットワークに参加する（英語）
- ネットワークトラフィックを管理する（英語）
- アプリの優先順位を設定する（英語）
- AppleデバイスのCisco FastlaneのMDM設定

AppleデバイスのグローバルHTTPプロキシペイロード設定を構成する。

- ネットワークトラフィックを管理する（英語）
- AppleデバイスのグローバルHTTPプロキシMDMペイロードの設定
- AppleデバイスのDNSプロキシMDMペイロードの設定

APNと通信するためにMDMで使用される主なポートとプロトコルを特定する。

- ネットワークを準備する（英語）
- APNを利用できるようにデバイスを構成する

リレーが管理対象のアプリ、ドメイン、またはデバイス全体に適用できることを理解する。

- AppleデバイスのリレーMDMペイロードの設定
- Appleデバイスでネットワークリレーを使用する
- ネットワークリレー
- iOS、iPadOS、macOS、およびtvOSのネットワークリレー

組織の戦略を評価・推奨し、Appleの固有サービスにデバイスがスムーズにアクセスできるようネットワーク構成を最適化する。

- macOSのワイヤレスローミング（法人のお客様向け）
- iOS、iPadOS、macOSが自動接続するワイヤレスネットワークの決定方法
- AppleデバイスでのWi-Fiローミングのサポート

クラスルームとApple Remote Desktopの画面監視をサポートするようネットワークを構成する。

- Appleソフトウェア製品で使われているTCPおよびUDPポート
- インフラストラクチャ要件

セキュリティ

Appleデバイスのパスコード構成オプションを特定する。

- パスコードペイロードを使用する(英語)
- AppleデバイスのパスコードMDMペイロードの設定

監視対象のAppleデバイスに適用される主な制限を把握する。

- 制限ペイロードを使用する(英語)
- Appleデバイスの監視について
- MDMでの監視対象Appleデバイスの制限

非監視対象のAppleデバイスに適用される主な制限を把握する。

- 制限ペイロードを使用する(英語)
- MDMでのAppleデバイスの制限を確認する

FileVault用にキーを保存できる場所など、macOS、iOS、iPadOSで暗号化される項目について説明する。

- FileVaultでデータを保護する(英語)
- 所属団体の復旧キーとパーソナル復旧キー

管理対象Appleデバイスに関連する、紛失モードの主な目的と機能を把握する。

- MDMを使って紛失モードを管理する(英語)
- 紛失したデバイスを管理する(英語)
- 紛失または盗難にあった監視対象デバイスの位置情報を検索する
- Appleデバイスをロックする／検索する

管理対象Appleデバイスに関連する、アクティベーションロックの主な目的と機能を把握する。

- アクティベーションロックを管理する(英語)
- recoveryOSパスワード
- Appleデバイスでのアクティベーションロック
- iPhoneおよびiPadでの組織に紐付いたアクティベーションロック

Appleデバイスの様々な種類の生体認証機能について説明する。

- Touch IDのセキュリティ
- Touch IDの先進のセキュリティテクノロジーについて
- Face IDとTouch IDの用途
- MacでTouch IDを使用する
- iPhoneでFace IDを設定する

Appleのセキュリティモデルの主な構成要素について説明する。

- デバイス登録について(英語)
- Secure Enclave
- Face IDとTouch IDのセキュリティ
- ハードウェアセキュリティの概要
- Appleプラットフォームのセキュリティ

組織がプラットフォームの整合性を損なうことなく安全に実行されるアプリを管理対象Appleデバイスにインストール・管理できるようにする組織のセキュリティポリシーをMDM設定に適用する。

- 組織のアプリとデータを管理する(英語)
- アプリをデバイスに配付する
- Appleデバイスに管理対象アプリを配付する

サポート

キーチェーンとは何かを把握し、ユーザがmacOSのキーチェーンアクセスで何ができるかを説明する。

- キーチェーンのデータ保護
- Macで「パスワード」設定を変更する

macOS復旧と、それを使用してユーザに何ができるかについて説明する。

- Macの起動時のキーコンビネーション
- Appleシリコンを搭載したMacのmacOS復旧で利用できるアプリ
- macOS復旧から起動する

「コンソール」とは何か、またユーザの問題に関する切り分けやトラブルシューティングにどのように「コンソール」を使うことができるかについて説明する。

- コンソールユーザガイド(Mac向け)
- Macの「コンソール」でログメッセージ、アクティビティ、またはレポートを共有する

デジタル証明書の主な構成要素を識別し、特定する。

- 証明書を管理する(英語)
- Appleデバイスの証明書管理の概要

テザリングキャッシュをセットアップする。

- コンテンツキャッシュの概要
- Macでコンテンツキャッシュを設定する
- AppleデバイスのデバイスネットワークMDMクエリー
- MDMを使用した「コンテンツキャッシュ」>「インターネット接続を共有」の仕組み

「ターミナル」とは何か、またユーザの問題に関する切り分けやトラブルシューティングにどのように「ターミナル」を使うことができるかについて説明する。

- コンソールユーザガイド(Mac向け)
- ターミナルユーザガイド(Mac向け)
- AppleネットワークアクセステストでWi-Fiをテストする

キャッシュサービスでサポートされているコンテンツの種類を特定する。

- コンテンツキャッシュについて理解する(英語)
- macOSのコンテンツキャッシュが対応しているコンテンツタイプ

FileVaultがmacOSの起動プロセスに加える変更について説明する。

- FileVaultでデータを保護する(英語)
- macOS復旧の概要
- Appleシリコンを搭載したMacでmacOS復旧を使用する
- Intelプロセッサを搭載したMacでmacOS復旧を使用する
- MacでのFileVaultの仕組み
- FileVaultを使用してMacのデータを保護する
- macOSでのFileVaultによるボリュームの暗号化
- 導入時にセキュアトークン、ブートストラップトークン、およびボリューム所有権を使用する
- モバイルデバイス管理でFileVaultを管理する

復旧キー、個人の復旧キー、MDMエスクローの重要性について説明する。

- FileVaultでデータを保護する(英語)
- MacでのFileVaultの仕組み
- FileVaultを使用してMacのデータを保護する
- Macの起動時のキーコンビネーション
- Appleシリコンを搭載したMacのmacOS復旧で利用できるアプリ
- macOS復旧から起動する
- 所属団体の復旧キーとパーソナル復旧キー
- AppleデバイスのFileVault MDMペイロードの設定

Macでコンテンツキャッシュを構成する。

- コンテンツキャッシュについて理解する(英語)
- コンテンツキャッシュを有効にする(英語)
- コンテンツキャッシュの詳細設定を構成する(英語)
- コンテンツキャッシュを最適化する(英語)
- Macでコンテンツキャッシュを設定する
- Macの「コンテンツキャッシュ」設定を変更する
- Macのコンテンツキャッシュの「クライアント」オプションを変更する
- Macのコンテンツキャッシュの「ペアレント」オプションを変更する
- Macのコンテンツキャッシュの「ピア」オプションを変更する
- Macのコンテンツキャッシュのストレージオプションを変更する
- コンテンツキャッシュの概要
- Macでコンテンツキャッシュを設定する
- Appleデバイスのデバイスネットワーク情報MDMクエリー
- MDMを使用した「コンテンツキャッシュ」>「インターネット接続を共有」の仕組み
- macOSのコンテンツキャッシュが対応しているコンテンツタイプ

モバイルデバイス管理（MDM）

MDMとは何か、またその仕組みについて説明する。

- デバイス登録について（英語）
- 登録プロファイル

MDMへの移行を計画する。

- MDMへの移行計画の概要
- 新しいMDMソリューションを構成する
- MDMにデバイスを再登録する

ユーザ所有のデバイスをMDMソリューションに手動で登録する。

- デバイス登録について（英語）
- ユーザ所有デバイスを登録する（英語）
- ユーザ登録とMDM
- ユーザ登録と管理対象Apple ID
- ロックダウンモードについて

ユーザ所有と組織所有の管理対象Appleデバイスで、MDMの管理者が行うことができる事柄を比較し、対比する。

- MDMの仕組みを理解する（英語）
- セキュリティ戦略を策定する（英語）
- 登録と設定アシスタントを管理する（英語）
- ユーザ所有デバイスを登録する（英語）
- AppleデバイスでVPNを使用する（英語）
- MDMを使って紛失モードを管理する（英語）
- 自動進行と自動デバイス登録（macOS）
- AppleデバイスのMDMコマンド
- Appleデバイスをロックする／検索する
- デバイスと企業データを管理する
- AppleデバイスのMDMコマンド
- Per App VPN
- AppleデバイスのVPN設定の概要
- ユーザ登録とアプリ別ネットワーク
- ユーザ登録用のMDMコマンド

MDMソリューションで登録プロファイルを作成し、割り当てる。

- 自動デバイス登録MDMペイロードリスト
- Appleデバイスのホーム画面レイアウトMDMペイロードの設定

Apple Configuratorを使ってMDMソリューションにiPhone、iPad、Apple TVデバイスを登録する。

- Apple Configuratorの機能の詳細(英語)

Appleデバイスで構成できる設定アシスタントのオプションを特定する。

- Appleデバイスの設定アシスタントMDMペイロードの設定
- Appleデバイスの設定アシスタントを管理する

iPhone、iPad、Macでアカウント駆動型デバイス登録を使ってMDMソリューションに登録する。

- 組織のアプリとデータを管理する(英語)
- アカウント駆動型デバイス登録
- Appleがユーザデータを組織のデータから分離する方法
- デバイス登録とMDM

監視対象のAppleデバイスのみに適用される制限を特定する。

- セキュリティ戦略を策定する(英語)
- 制限ペイロードを使用する(英語)
- MDMでの監視対象Appleデバイスの制限
- Appleデバイスの監視について
- MDMでのiPhoneおよびiPadデバイスの制限
- MDMでのAppleデバイスの制限を確認する

ユーザがアプリをインストールまたは削除できないようにする。

- セキュリティ戦略を策定する(英語)
- 組織のアプリとデータを管理する(英語)
- アプリを削除またはインストールできないようにする(英語)
- MDMでのAppleデバイスの制限を確認する
- MDMでのiPhoneおよびiPadデバイスの制限
- Appleデバイスの通知MDMペイロードの設定
- Appleデバイスに管理対象アプリを配付する

Appleデバイスで緊急セキュリティ対応を管理する。

- ソフトウェアアップデートを管理する(英語)
- 制限ペイロードを使用する(英語)
- 緊急セキュリティ対応とMDM

管理対象のiPhoneまたはiPadでManaged Open In制限を構成する。

- 組織のアプリとデータを管理する(英語)
- 管理対象アプリの制限と機能

登録時にパスコードの使用を強制する。

- セキュリティ戦略を策定する(英語)
- 登録と設定アシスタントを管理する(英語)
- パスコードペイロードを使用する(英語)
- AppleデバイスのパスコードMDMペイロードの設定
- 設定アシスタントパネルのオプション
- 自動進行と自動デバイス登録(macOS)
- 自動デバイス登録MDMペイロードリスト

MDMソリューションを使用して、Appleデバイスのパスコード要件を構成する。

- パスコードペイロードを使用する(英語)
- AppleデバイスのパスコードMDMペイロードの設定

MDMソリューションを使って管理対象MacコンピュータでFileVaultを強制する。

- FileVaultでデータを保護する(英語)
- ブートストラップトークン

紛失モードとアクティベーションロックを管理対象デバイスに適用する。

- セキュリティ戦略を策定する(英語)
- MDMを使って紛失モードを管理する(英語)
- アクティベーションロックを管理する(英語)
- 紛失したデバイスを管理する(英語)
- iPhoneおよびiPadでの組織に紐付いたアクティベーションロック
- 紛失または盗難にあった監視対象デバイスの位置情報を検索する

MDMソリューションを使ってデバイスを安全にワイプする方法を実際に示す。

- 紛失したデバイスを管理する(英語)
- Appleデバイスを消去する

管理対象Appleデバイスでサポートされている、MDMからのクエリーの種類を特定する。

- デバイスにクエリーを送る(英語)
- AppleデバイスのセキュリティMDMクエリー

管理対象のiPhone、iPad、MacおよびApple TVデバイスのソフトウェアアップデートを保留する。

- ソフトウェアアップデートを管理する(英語)
- ソフトウェアアップデートおよびアップグレードを延期する

MDMを使用して、デバイスで何を管理し、実施することができるかを列挙する。

- セキュリティ戦略を策定する(英語)
- 制限ペイロードを使用する(英語)
- MDMでの監視対象Appleデバイスの制限
- Appleデバイスの監視について
- MDMでのiPhoneおよびiPadデバイスの制限
- MDMでのAppleデバイスの制限を確認する
- AppleデバイスのMDMコマンド

`cfgutil`スクリプトを使用してApple Configuratorに含まれない繰り返しタスクを自動化する。

- Apple Configuratorの機能の詳細(英語)
- Apple Configurator 2のコマンドラインツールを使用する

iPhoneおよびiPadのEraseDeviceコマンドを使って、MDMソリューションで「サービスに戻す」ためにデバイスをすぐにリセットする。

- 「サービスに戻す」ためのデバイスの準備(英語)
- iPhoneおよびiPadの「サービスに戻す」
- Appleデバイスを消去する
- デバイス消去コマンドの詳細(英語)

MDMソリューションで組織所有のAppleデバイスの設定アシスタントを構成する。

- 登録と設定アシスタントを管理する(英語)
- 設定アシスタントパネルのオプション

MDMを使用して管理対象Appleデバイスに関する詳細情報を表示する。

- デバイスにクエリーを送る(英語)
- ユーザ登録のMDMクエリー
- Appleデバイスのデバイス情報MDMクエリー
- Appleデバイスのデバイスネットワーク情報MDMクエリー
- Appleデバイスのオペレーティングシステム MDMクエリー
- Appleデバイスのインストール済みApp MDMクエリー
- Appleデバイスのセキュリティ MDMクエリー

管理対象Appleデバイスで制限を使用する目的または機能を特定する。

- セキュリティ戦略を策定する(英語)
- コンテンツキャッシュについて理解する(英語)
- 制限ペイロードを使用する(英語)
- コンテンツキャッシュを設定する
- MDMでの監視対象Appleデバイスの制限
- MDMでのiPhoneおよびiPadデバイスの制限
- MDMでのAppleデバイスの制限を確認する

iPhone、iPad、Macのアクセサリ制限を管理する。

- ThunderboltとUSBを用いたペアリングを管理する(英語)
- ホストとのペアリングのMDM管理

モバイルデータ通信を備えたデバイスを導入する。

- MDMを使ってモバイルデータ通信を備えたデバイスを導入する
- eSIMの変更制限について

例題

試験対策として、以下の例題に挑戦してみましょう。回答後に、解答集で正解を確認してください。これらの例題は実際に出題される問題とは異なりますが、問題の形式は同様です。

問題1

管理対象アプリが取り消された際、Apple Business ManagerまたはApple School Managerで誰がそのライセンスを保持しますか？

A. デバイスのユーザ

B. 所属組織

C. 管理対象Apple IDを持つユーザ

D. 個人のApple IDの所有者

問題2

Macで起動ボリュームが保護されているかどうかを確認するために使用できるセキュリティMDMクエリーは次のうちどれですか？

A. 「探す」が有効

B. パスコードの有無

C. 安全な起動状態

D. ハードウェア暗号化タイプ

問題3

共有iPadのユーザをサポートするため、管理対象のMac miniでコンテンツキャッシュを300 GBのキャッシュサイズで構成したところ、ユーザから、iClouDに保存されている大きなファイルのダウンロードに以前よりも時間がかかるようになったと伝えられました。

iCloudユーザデータのダウンロードの速度を上げるにはどうすればよいですか？

A. キャッシュサイズを増やす。

B. MDMコマンド「`PurgeCache`」を使ってキャッシュを消去する。

C. 何もしない。iCloudユーザデータはコンテンツキャッシュには保存されない。

D. 「`/Library/Application Support/Apple/AssetCache`」フォルダを削除する。

問題4

ユーザのファイルに対する不正アクセスを防ぎつつMacコンピュータがWebサイトにアクセスできるかどうかを確認するためには、次のどのセキュリティMDMクエリーを使用しますか？

A. ファイアウォール設定

B. 「探す」が有効

C. パスコードの有無

D. ハードウェア暗号化タイプ

問題5

BetterBagの情報セキュリティチームは、デバイス登録済みのMacコンピュータの「システム設定」で、ユーザが構成プロファイルを手動でインストールできないようにしたいと考えています。

これを実装するため、管理対象Macコンピュータに必要なものは次のうちどれですか？

A. 監視モードであること。

B. macOS 13以降を搭載していること。

C. Apple Business Managerで割り当てられていること。

D. 自動デバイス登録で登録されていること。

問題6

BetterBagのITチームは、Macのユーザが、指定された起動ボリューム以外のボリュームから起動できないようになっていることを確認したいと考えています。

そのためには次のどのセキュリティMDMクエリーを使用しますか？

A. 「探す」が有効

B. パスコードの有無

C. ファームウェアパスワードのステータス

D. ハードウェア暗号化タイプ

問題7

BetterBagのカスタムアプリが予期せず終了します。アプリのデベロッパはログレポートを要求しています。

適切なログを見つけて送るにはどうすればよいですか？

A. 「アクティビティモニタ」を開き、「表示」をクリックして「システム診断を実行」を選択する。

B. ターミナルで「`tail -f /Applications/BetterBag.app/Contents/MacOS/BetterBag`」と入力する。

C. 「コンソール」を開き、サイドバーから「ログレポート」をクリックし、BetterBagを検索してログを選択して「共有」ボタンをクリックする。

D. 「コンソール」を開き、サイドバーから「診断レポート」をクリックし、BetterBagを検索してログを選択して「共有」ボタンをクリックする。

問題8

クライアントまたはサーバを安全に識別し、それらの間の通信を暗号化するために使用できる2つの証明書のコンポーネントは次のうちどれですか？

A. 公開鍵と秘密鍵

B. 信頼キーと信頼証明書

C. 中間証明書と信頼キー

D. 信頼証明書と中間証明書

問題9

Leticiaは、新入社員のグループが自身の管理対象iPadデバイスで、権限のないユーザがオリエンテーションファイルにアクセスできないように設定していることを確認する必要があります。

そのために使用できるセキュリティMDMクエリーは次のうちどれですか？

A. パスコードの有無

B. 安全な起動状態

C. ファームウェアパスワードのステータス

D. アクティベーションロックが管理可能

問題10

BetterBagでは、FileVault暗号化を通じて、管理対象Macコンピュータのすべてを保護する必要があります。

BetterBagのMDMソリューションで、モバイルアカウントに安全なトークンを付与するためにエスクローする必要があるものは次のうちどれですか？

A. コンテンツトークン

B. ブートストラップトークン

C. パーソナル復旧キー

D. 所属団体の復旧キー

問題11

BetterBagのセキュリティチームは、盗難された管理対象iPhoneデバイスを回収したいと考えています。

盗難されたiPhoneを見つけるために有効にするMDM設定は次のうちどれですか？

A. Appleのマップ

B. 探す

C. 位置情報サービス

D. 管理対象紛失モード

問題12

BetterBagではすべての管理対象Appleデバイスに対して自動デバイス登録を使っており、次のユーザにデプロイする前に、前のユーザのMacからすべてのデータを削除する必要があります。

デバイスの再プロビジョニングに使用できるMDMコマンドは次のうちどれですか？

A. 管理対象アプリを削除

B. プロビジョニングプロファイルを削除

C. プロビジョニングプロファイルをインストール

D. すべてのコンテンツと設定を消去

問題13

BetterBagの経理チームはiPadデバイスに含まれる財務データの安全性を確保したいと考えています。

機密データが安全であることを確認するために使用できるセキュリティMDMクエリーは次のうちどれですか？

A. 安全な起動状態

B. ハードウェア暗号化タイプ

C. ファームウェアパスワードのステータス

D. アクティベーションロックが管理可能

問題14

BetterBagでは、小売店のキオスクiPadデバイスに顧客がログインできないことを確認したいと考えています。

そのためには次のどのセキュリティMDMクエリーを使用しますか？

A. 安全な起動状態

B. ファームウェアパスワードのステータス

C. アクティベーションロックが管理可能

D. プロファイルでのパスコード準拠

問題15

紛失または盗難されたiPhoneまたはiPad上のデータへの不正アクセスを防ぐために役立つMDMコマンドは次のうちどれですか？

A. `ActivationLockRequest`

B. `DeviceLock`

C. `EraseDevice`

D. `SetAutoAdminPassword`

問題16

BetterBagのセキュリティチームは、従業員がiPadデバイスを紛失や盗難から守るための要件を満たしていることを確認したいと考えています。

そのために使用すべきセキュリティMDMクエリーは次のうちどれですか？

A. 「探す」が有効

B. 安全な起動状態

C. ファームウェアパスワードのステータス

D. アクティベーションロックが管理可能

問題17

元従業員の管理対象iPhoneをサービスに戻す必要がありますが、組織のMDMソリューションではアクティベーションロックを削除できません。

組織に紐付くアクティベーションロックを無効にするにはどうすればよいですか？

A. アクティベーションロック画面で、iCloud設定に個人のApple ID資格情報を入力する。

B. アクティベーションロック画面で、デバイス登録トークンを作成した管理対象Apple ID資格情報を入力する。

C. Apple Business ManagerまたはApple School Managerでデバイスを特定し、「アクティベーションロックをクリア」コマンドを送信する。

D. MDMソリューションを使用して、デバイスに「パスコードをクリア」コマンドを送信する。デバイスベースのアクティベーションロックは自動的に無効になる。

問題18

BetterBagのITチームは、経営幹部のiPadデバイスを、利用可能な最も安全な暗号化技術を用いて組織のWi-Fiネットワークにアクセスするよう構成したいと考えています。また、BetterBagのWi-Fiネットワークで、最新規格をサポートしていない可能性のあるその他のデバイスとの互換性が保たれるようにする必要もあります。

これらの要件を満たす可能性が最も高い認証方法は次のうちどれですか？

A. WPA2パーソナル

B. WPA3エンタープライズ

C. Wi-Fi Protected Access

D. Wired Equivalent Privacy

問題19

あなたは寄付されたMacコンピュータを手動でApple School Managerに追加し、MDMソリューションに登録しました。

Macコンピュータを手動でMDMソリューションに追加して登録した後の管理ステータスはどうなりますか？

A. 監視対象になり、ユーザはいつでも登録を解除できる。

B. 監視対象にはならず、ユーザはいつでも登録を解除できる。

C. ユーザは、最大30日間デバイス管理からデバイスを解放できる。

D. ユーザは、最大60日間デバイス管理からデバイスを解放できる。

問題20

Macコンピュータの重要なファイルの場所が保護されていることを確認するには、次のどのセキュリティMDMクエリーを使用しますか？

A. 「探す」が有効

B. パスコードの有無

C. ハードウェア暗号化タイプ

D. システム整合性保護が有効

問題21

シェルスクリプトを作成し、Mac用のApple Configuratorで特定のプロセスを自動化したい場合、次のどのターミナルコマンドを使用しますか？

A. `automator`

B. `cfgenrollment`

C. `cfgutil`

D. `startosinstall`

問題22

Apple Business Managerに登録されている監視対象iPhoneでスキップするよう設定できない設定アシスタントの画面は次のうちどれですか？

A. Apple ID

B. 言語

C. 位置情報サービス

D. 利用規約

問題23

BetterBagのユーザの管理対象iPhoneの「設定」で、「モバイル通信プランのインストールの準備ができました」という通知が表示されました。そのユーザが通話することができたとしても、管理対象iPhoneでモバイル通信プランをインストールすることはできません。

モバイル通信プランをインストールできない理由として最も可能性が高いものは次のうちどれですか？

A. eSIMがすでに使用されている。

B. そのiPhoneではApple Lookup Serviceにアクセスできない。

C. `AllowESIMModification`制限が有効になっている。

D. `AllowESIMModification`制限が無効になっている。

問題24

iPhoneで通信事業者の（SM-DP+）サーバからeSIMプロファイルをダウンロードするMDMコマンドは次のうちどれですか？

A. InstallESIM

B. CarrierActivation

C. Provision Cellular Plan

D. Refresh Cellular Plans

問題25

グローバルHTTPプロキシMDMペイロードで自動プロキシ設定を構成する設定は次のうちどれですか？

A. 認証タイプ

B. パスワード

C. プロキシPAC URL

D. セキュリティタイプ

問題26

Apple Business ManagerまたはApple School Managerで、デバイスの追加、割り当て、割り当て解除、解放を行うデフォルトの権限を持つロールは次のうちどれですか？

A. 管理者

B. コンテンツマネージャ

C. マネージャ

D. スタッフ

問題27

BetterBagでは、すべてのiPhoneおよびiPadデバイスでパスコードの最長有効期間を必須としています。

MDMソリューションで設定できるパスコードの最長有効期間は次のうちどれですか？

A. 90日間

B. 180日間

C. 365日間

D. 730日間

問題28

MDMソリューションで、新しい監視対象iPadデバイスからアクティベーションロックバイパスコードを取得できる最大日数は次のうちどれですか？

A. 7日間

B. 15日間

C. 21日間

D. 90日間

問題29

全体的な管理状態をデバイスに伝え、MDMソリューションの組織と機能の詳細を説明するために使われる宣言タイプは次のうちどれですか？

A. デバイス

B. 登録

C. 管理

D. セキュリティ

問題30

Nishaは、多数のMacコンピュータを導入する準備を進めており、承認されたMacコンピュータのみがコンテンツキャッシュの登録をできるようにしたいと考えています。

この設定を構成する必要があるペイロードは次のうちどれですか？

A. コンテンツキャッシュ

B. プライバシーとセキュリティ

C. 制限

D. システム設定

解答集

問題1 : B

問題2 : C

問題3 : A

問題4 : A

問題5 : B

問題6 : C

問題7 : C

問題8 : A

問題9 : A

問題10 : B

問題11 : D

問題12 : D

問題13 : B

問題14 : D

問題15 : C

問題16 : A

問題17 : B

問題18 : A

問題19 : C

問題20 : D

問題21 : C

問題22 : B

問題23 : D

問題24 : D

問題25 : C

問題26 : A

問題27 : D

問題28 : B

問題29 : C

問題30 : C

試験の詳細

- この試験の名称は「『Apple導入と管理』試験」(DEP-2024-ENU)です。
- 試験は採点対象となる90問ほどの技術的な質問で構成され、120分以内に完了する必要があります。
- 合格に必要な最低スコアは75%です。スコアは四捨五入されません。
- この試験では、多肢選択式の単一または複数回答方式が使用されています。
- 試験中にリソースや参照資料を確認することはできません。

試験を受ける

「Appleの導入と管理」試験は、Pearson OnVUEシステムを通じてオンラインで受けられます。試験の時間を確保して、一度で最後まで終了するようにしてください。試験を受けるには、プライベートなスペースと、政府発行の最新の身分証明書が必要です。

Pearson OnVUEを使ったオンライン試験について詳しくは、こちらのショートビデオを参照してください。

スケジュールを設定して試験を受けるには、次の手順に従います。

1. 自身のApple IDとパスワードを使用してACRS(Apple認定記録システム)にサインインします。
2. 「受験可能な試験」をクリックします。「『Apple導入と管理』試験」をクリックして試験の登録プロセスを開始します。
3. 「試験と認定資格の連絡先情報」セクションを更新します。追加情報に関する質問に答えます。試験を受けるために特別な配慮を求める場合は、関連するフィールドに入力してください。「送信」ボタンをクリックします。
4. 通知ページで、「手続きを続行する試験:『Apple導入と管理』試験」という文を見つけます。「Pearson VUEで続行」をクリックします。
5. 手順に従って試験のスケジュールを設定し、支払いを行います。

試験当日は、次の手順に従います。

1. 試験の開始予定時刻の30分前に、自身のApple IDとパスワードを使ってACRSにサインインします。
2. ホームページで「『Appleの導入と管理』試験」をクリックします。
3. 「試験を開始する」(Begin Exam)をクリックし、表示される手順に従います。

試験の終了後、スコアがPearsonからメールで届きます。1回で合格できなかった場合、試験を再度購入して7日後に再試験を受けることができます。合格するまで最大4回試験を受けられます。

認定資格について

Apple認定ITプロフェッショナルデジタルバッジを取得することで、自身を差別化し、進化する求人市場で競争力を持ち、Appleブランドの力を活用することができます。

試験に合格すると、デジタルバッジの取得手順に関するメールがCredlyから送信されます。

デジタルバッジは、取得日から2年間有効です。有効期限は取得日によって異なります。再認定試験が公開されたらバッジの有効期限が切れる前に受験して、バッジを最新の状態に保ちましょう。また、再認定試験が公開されたらすぐに確認できるように、定期的にApple Training（英語）のWebサイトにアクセスし、ACRSにサインインすることをお勧めします。