CompTIA Mobility+ 試験出題範囲

試験番号: MB0-001

CompTIA Mobility+認定資格は、モバイルコンピューティング環境において構築、運用、管理を実施する IT エンジニアに求められるスキルと知識を証明するワールドワイドの認定資格です。

CompTIA Mobility+認定資格の取得者は、モバイルデバイスの機能や無線通信の環境を実装、運用、管理を実施する際に必要とされるスキルと知識を習得していることが証明されます。また、適切なセキュリティやユーザビリティを考慮しながら、モバイル環境を設計、実装、サポート、管理を実施できるスキルを所有していることが証明されます。

CompTIA Mobility+認定資格試験の受験者の方は、下記のような方が取得されることをお勧めしています。

- CompTIA Network+、またはこれに相当する実務能力を有している方
- 企業のモバイルデバイス環境の管理者としての業務経験を少なくとも 18 ヶ月経験されている方。

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　無線通信（OTA：Over-The-Air Technology）	13%
第2章　ネットワークインフラストラクチャー	15%
第3章　モバイルデバイスマネジメント	28%
第4章　セキュリティ	20%
第5章　トラブルシューティング	24%
合計	100%

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。本出題範囲は、予告なく変更される場合がございます。あらかじめご了承ください。

CompTIA では、提供している認定資格試験の内容にて現在必要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、定期的な改訂を行っています。必要な場合、現在の出題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。

第 1 章　無線通信（OTA:Over-The-Air Technology）（13%）

1.1 それぞれの携帯電話で用いられるテクノロジーを比較対照できる。

- CDMA
- TDMA
- GSM
  - Edge
  - GPRS
- WiMAX
- UMTS
- CSD
- EVDO
- HSPA
- HSPA+
- LTE
- 異なるネットワーク間でのローミングやスイッチング

1.2 想定されたシナリオにおいて、適切なオプションを用いて WiFi クライアントを設定、実装することができる。

- Bluetooth
- PAN
- 802.11a/b/g/n/ac
  - 関連する周波数帯とチャネル
- SSID
  - ブロードキャスト/クローズドシステム
- 認証方法
- ポータブルホットスポット

1.3 高周波（RF）の原理とその機能を比較対照できる。

- 高周波（RF）の特性
  - 周波数
  - 変調
  - 帯域幅
  - 波長
  - 振幅
  - 位相
- 伝播理論
  - 吸収
  - 屈折
  - 反射
  - 減衰
  - 干渉
- アンテナ
  - 無指向性
  - 準指向性
  - 双方向性
  - 八木
  - パラボラ
- ファラデーケージ

1.4 無線通信環境を確実にするための実地調査を正確に解釈することができる。

- 容量
- 通信可能範囲
- 信号の強度
- 受信信号強度
- スペクトラム分析
- 周波数分析
- 実地調査資料/サイトマップ
  - ワイヤレスと携帯電話の実地調査
- 事後実地調査

第 2 章　ネットワークインフラストラクチャー（15%）

2.1　物理的、または論理的インフラテクノロジーとプロトコルを比較対照できる。

- トポロジ
  - メッシュ
  - ポイントツーポイント
  - ポイントツーマルチポイント
  - アドホック
- ファイアウォールの設定
  - ポート設定
  - プロトコル
  - フィルタリング
  - DMZ
- デバイス
  - ゲートウェイ
  - プロキシ
  - VPN コンセントレータ
  - 自立型アクセスポイント
  - 無線 LAN
  - コントローラー
  - Lightweight アクセスポイント（LAP）
- サービスと設定
  - ActiveSync
  - Dynamic VLAN
  - サブネッティング

2.2　有線ネットワークと無線ネットワークが通信する際に使用されるテクノロジーについて説明することができる。

- 帯域幅とユーザーの制限
  - バックホーリングトラフィック
  - QoS
  - トラフィックシェーピング
- ハードウェアの違い
- トラフィックのルーティング
- IP アドレッシング
  - TCP
  - UDP
  - NAT
  - DNS
  - DHCP
- MAC アドレス
- SNMP
- ICMP
- AP のための PoE

2.3　OSI 参照モデルのレイヤーを説明することができる。

- レイヤー1 – 物理層
- レイヤー2 – データリンク層
- レイヤー3 – ネットワーク層

- レイヤー4 – トランスポート層
- レイヤー5 – セッション層
- レイヤー6 – プレゼンテーション層
- レイヤー7 – アプリケーション層

2.4 災害復旧の原則とモバイル機器に与える影響について説明することができる。

- サーバーのバックアップ
- デバイスのバックアップ
- ディレクトリサービスサーバー
- バックアップの頻度
- 高可用性
- DR のロケーション

2.5 モバイルデバイス用の一般的なネットワークポートとプロトコルを比較対照できる。

- 20/21 – FTP
- 22 – SSH、SFTP、SCP
- 25 – SMTP
- 53 – DNS
- 80 – HTTP
- 110 – POP3
- 135 – MAPI
- 143 – IMAP
- 443 – HTTP over TLS/SSL（HTTPS）
- 465 – SMTP over SSL
- 587 – Alternate SMTP
- 989/990 – FTPS
- 2175 – Airsync
- 2195 - 2196 – APNS & Feedback
- 3389 – RDP
- 4101 – SRP
- 4200 – UDP
- 5223 – Jabber
- 5228-5230 – GCM

第 3 章　モバイルデバイスマネジメント（28%）

3.1　デバイスの性能を証明するために必要なポリシーを説明することができる。

- IT ポリシーとセキュリティポリシーの遵守
  - セキュリティとユーザビリティのバランス
- ベンダーデフォルトのアプリケーション間の相違
- OS の変更とカスタマイズ
  - OS ベンダー
  - OEM
  - 電話通信キャリア
- バックアップ、リストアおよびリカバリーポリシー

3.2　企業の要件に合わせてモビリティソリューションを比較対照できる。

- モバイルデバイスマネジメント
  - パスワードの強度
  - リモートワイプ
  - リモートロック/アンロック
  - アプリケーションストア
- モバイルアプリケーション管理
  - アプリケーションストア
- コンテンツのプッシュ
- デバイスプラットフォームのサポート
- インフラストラクチャーのサポート
- オンプレミスと SaaS の比較
- 管理者権限
- マルチインスタンス
- 高可用性
- デバイスグループ
- ロケーションベースのサービス
  - ジオロケーション
  - ジオフェンシング
- 性能と機能に関する監視とレポート
- 他の製品/デバイスとの相互運用性
- Telecommunication expense management (TEM：通信費管理)
- セルフサービスポータル
- キャプティブポータル（Web 認証）

3.3　指定された要件にもとづいて、モバイルソリューションを実装、設定することができる。

- ソリューションのインフラストラクチャーを確保するため担当者と連携する
- プロファイルの作成
- ディレクトリサービスのセットアップ
- 初期証明書の発行
- EULA
- 指定された要件にもとづいたグループプロファイル
  - 法人所有
  - BYOD
  - エグゼクティブ
  - 管理

- コンサルタント
- B2B

- パイロット、テスト、評価
- ドキュメントの作成と更新
- 次のパイロットへフィードバックを報告
- SDLC
- 承認、トレーニング、公開

3.4 モバイルデバイスのオンボーディングとオフボーディングを設定することができる。

- 携帯電話通信回線上でのデバイスのアクティベーション
- OTA アクセス対応のモバイルデバイス
  - ワイヤレスカード、携帯電話カード、SD カード
- オンボーディングと提供プロセス
  - マニュアル
  - セルフサービス
  - バッチ
  - リモート
  - IMEI や ICCID
  - デバイスの登録（SCEP）
  - プロファイルの設定
- オフボーディングとデプロビジョニング
  - 従業員の退職時
  - マイグレーション
  - アプリケーション
  - コンテンツ
  - リサイクル
  - 適切な資産の処分
  - ディアクティベーション（無効化）

3.5 モバイルデバイスの操作と管理手順を実装することができる。

- コンテンツとアプリケーションの配布、およびコンテンツ管理システムの集中管理
  - 配布方法
    - ーサーバーベース
    - ーコンテンツの更新/変更
    - ーアプリケーションの変更
    - ーパーミッション
- 効率的な展開方法
  - デバイスの数
  - ユーザー数
- リモート機能
  - ロック/アンロック
  - リモートワイプ
  - リモートコントロール
  - 位置サービス
  - レポーティング
- ライフサイクル管理
  - 証明書有効期限/リニューアル
  - アップデート
  - アップグレード

- パッチ
- 変更管理
- 製造/販売/サポートの終了
  - OS
  - デバイス
  - アプリケーション

3.6 モバイルデバイスのバックアップ、データ復旧とデータ分離のための最適な方法を実行することができる。

- 企業サーバーへの企業データのデバイスバックアップ
- ベンダー/サードパーティのサーバーへの個人データのデバイスバックアップ
- ローカルデバイスへのバックアップ：内蔵ストレージ、SD カード、SIM
- データ復旧
  - バックアップのテスト
  - 企業データの復元
  - 個人データの復元

3.7 モバイル機器に影響を与える変更を含む新しいテクノロジーへの意識を高く維持するための最適な方法を実行することができる。

- OS ベンダー
- OEM（ハードウェア）
- 通信キャリア
- サードパーティのアプリケーションベンダー
- 新しいリスクと脅威

3.8 モバイルアプリケーションと関連するテクノロジーを構成して、展開することができる。

- メッセージング規格
  - MAPI
  - IMAP
  - POP
  - SMTP
- ベンダーのプロキシとゲートウェイサーバの設定
- 情報トラフィックトポロジー
  - サードパーティの NOC とオンプレミス、ホストの比較
- プッシュ通知テクノロジー
  - APNS
  - GCM
  - ActiveSync
- 社内アプリケーションの要件
  - アプリケーションパブリッシング
  - プラットフォーム
  - ベンダーの要件
  - 証明書
  - データ通信
- モバイルアプリケーションの種類
  - ネイティブアプリケーション
  - Web アプリケーション
  - ハイブリッドアプリケーション

第 4 章　セキュリティ（20%）

4.1　モバイル環境においてセキュリティを確保するための様々な暗号方式を識別することができる。

- データ通信中
  - IPSEC
  - VPN
  - SSL
  - HTTPS
  - WPA/TKIP
  - WPA2
  - TLS
  - SRTP
  - RSA
  - WEP
  - SSH
  - RC4
  - CCMP
  - EAP 方式
- 保存データ
  - AES
  - DES
  - 3DES
  - Two-Fish
  - ECC
- フルディスク暗号化（記憶領域の暗号化）
- ブロックレベルの暗号化
- ファイルレベルの暗号化
- フォルダレベルの暗号化
- リムーバブルメディアの暗号化

4.2　モバイルデバイスでのアクセス制御を最適な方法で設定することができる。

- 認証の概念
  - マルチファクタ
    - ーバイオメトリクス
    - ークレデンシャル
    - ートークン
    - ーピン
  - デバイスのアクセス
  - ワイヤレスネットワーク
    - ー企業と個人の比較
  - アプリケーションのアクセス
- PKI の概念
- 証明書の管理
- ソフトウェアのコンテナベースのアクセスとデータの分離

4.3　セキュリティ要件に対応した監視とレポートテクノロジーを説明することができる。

- デバイスのコンプライアンスとレポート監査情報
- サードパーティのデバイス監視アプリケーション（SIEM）
- モバイルデバイスのアクティビティとトラフィックに関連する適切なログの監視

4.4 リスク、脅威と、モバイルエコシステムへの影響の軽減策を説明することができる。

- ワイヤレスのリスク
  - 不正なアクセスポイント
  - DoS 攻撃
  - タワースプーフィング
  - ジャミング
  - Warpathing
  - man-in-the-middle 攻撃
  - 脆弱なキー
- ソフトウェアのリスク
  - App Store の使用
  - ウイルス
  - トロイの木馬
  - ワーム
  - マルウェア
  - スパイウェア
  - ジェイルブレイク（Jailbreak）
  - ルーティング
  - キーロガー
  - サポートされていない OS
- 組織的なリスク
  - BYOD の影響
  - セキュアな個人的デバイス
  - リムーバブルメディア
  - 個人データを抹消
  - ネットワーク/サーバー上の不明なデバイス
- ハードウェアのリスク
  - デバイスクローニング
  - デバイスの盗難
  - デバイスの損失
- 軽減策の実行
  - アンチウイルス
  - ソフトウェアファイアウォール
  - アクセスレベル
  - パーミッション
  - ホストベースおよびネットワークベースの IDS/IPS
  - アンチマルウェア
  - アプリケーションのサンドボックス
  - TPM（Trusted platform modules：信頼できるプラットフォームモジュール）
  - データコンテナ
  - コンテンツフィルタリング
  - DLP
  - デバイスのセキュリティ強化
  - 物理ポートの無効化

4.5 指定されたシナリオにもとづいて、適切なインシデントの対応と復旧手順を実行することができる。

- インシデントの識別
- ポリシーにもとづいた対応の決定と実行

- インシデントのレポート
  - エスカレーション
  - 文書化
  - キャプチャログ

第 5 章 トラブルシューティング（24%）

5.1 指定されたシナリオにもとづいて、それぞれのトラブルシューティングの方法を実行することができる。

- 問題を特定
  - 情報を収集する
  - 状況を確認する
  - ユーザーへ質問をする
  - 変更された事柄があるかを確認する
- 想定される原因の仮説を立てる
  - 明確な質問をする
- 原因を特定するために仮設をテストする
  - 仮説が確定した場合には、問題を解決するために次の工程を決定する
  - 仮説が確定しない場合には、新しい仮説を立てなおすか、エスカレーションする
- 問題を解決するためのアクションプランを立て、潜在的な影響を特定する。
- ソリューションを実行し、必要に応じてエスカレーションする
- 全てのシステムが完全に機能していることを確認し、必要に応じて適切は予防措置を講じる
- 原因、対策、結果を文書化する

5.2 指定されたシナリオにもとづいて、一般的にデバイスに起こる障害のトラブルシューティングを実施することができる。

- バッテリーの寿命
- 同期の問題
- 電源装置の障害
- パスワードのリセット
- デバイスの故障/破損
- 停電

5.3 指定されたシナリオにもとづいて、一般的にアプリケーションに起こる障害のトラブルシューティングを実施することができる。

- アプリケーションが見つからない
- 構成の変更
- App Store の問題
- メールの障害
- ロケーションサービスの障害
- OS やアプリケーションのアップグレードに関連する障害
- プロファイルの認証と承認の問題

5.4 指定されたシナリオにもとづいて、一般的に無線通信（Over-The-Air）に起こる障害のトラブルシューティングを実施することができる。

- 遅延（レイテンシー）
- モバイルデバイスの電波障害
- ネットワークに接続できない
- ローミング障害

- モバイルのアクティベーション
- メールの障害
- VPN の障害
- 証明書の問題
- APN の障害
- ポート構成の障害
- ネットワークの飽和状態

5.5 指定されたシナリオにもとづいて、一般的にセキュリティに起こる障害のトラブルシューティングを実施することができる。

- 期限の切れた証明書
- 認証の失敗
- ファイアウォールの設定ミス
- フォルスポジティブ（False positives：検出すべきでないイベントの検出）
- フォルスネガティブ（False negatives：検出すべきイベントが検出できていない）
- 無期限のパスワード
- 期限の切れたパスワード
- コンテンツフィルタリングの設定ミス

CompTIA Mobility+ 略語一覧

下記はCompTIA Mobility+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。

AD	—	Active Directory
AP	—	Access Point
APN	—	Access Point Name
APNS	—	Apple Push Notification Service
AUP	—	Acceptable Use Policy
B2B	—	Business to business
BYOD	—	Bring your own Device
CDMA	—	Code Division Multiple Access
CME	—	Coronal Mass Ejection
CSD	—	circuit Switch Data
DHCP	—	Dynamic Host Configuration Protocol
DMZ	—	Demilitarized Zone
DNS	—	Domain Name Service
DR	—	Disaster Recovery
EULA	—	End User License Agreement
EVDO	—	Evolution Data Optimized
FTP	—	File Transfer Protocol
FTPS	—	FTP over SSL
GCM	—	Google Cloud Messaging for Android
GPRS	—	General Packet Radio Service
GSM	—	Global Standard for Mobility
HA	—	High Availability
HSPA	—	High Speed Packet Access
HTTP	—	Hyper Text Transfer Protocol
IMAP	—	Internet Message Address Protocol
IMAPS	—	Secure IMAP
IP	—	Internet Protocol
LAN	—	Local Area Network
LDAP	—	Lightweight Directory Access Protocol
LTE	—	Long Term Evolution
MAM	—	Mobile Application Management
MAPI	—	Messaging Application Programming Interface
MD5	—	Message Digest 5
MDM	—	Mobile Device Management
NAC	—	Network Access Control
NAT	—	Network Address Translation
OEM	—	Original Equipment Manufacturer
OS	—	Operating System
OSI	—	Open Systems Interconnect
PAN	—	Personal Area Network
PAT	—	Port Address Translation
PoE		Power over Ethernet
POP		Post Office Protocol

QoS	Quality of Service
RDP	Remote Desktop Protocol
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
SaaS	Software as a Service
SDLC	System Life Cycle Development
SFTP	Secure FTP
SIM	Subscriber Identity Module
SHA	Secure Hashing Algorithm
SMTP	Simple Mail Transport Protocol
SRP	Server Router Protocol
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSMTP	Secure SMTP
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications Standards
VLAN	Virtual LAN
VPN	Virtual Private Network
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access

CompTIA Mobility+学習の際の設備/装置の一覧

** CompTIA Mobility+試験準備のため、CompTIAでは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実機等をご検討いただく際に、ご確認ください。各トピックスの一覧はサンプルのリストであり、すべてを網羅しているわけではありません。

機器

- メッセージングサーバー
- MDMサーバー
- 高スペックのノートPC
- タブレット
- スマートフォン
- アクセスポイント
- ルーター
- スイッチ
- エアーカード
- ホットスポット
- プロジェクター/大画面のスクリーン
- ワイヤレスLANコントローラー
- PoEインジェクター
- ピコセル
- CPNコンセントレーター
- ファイアウォール
- ハードウェアトークン（セキュアID）

予備のパーツ/ハードウェア

- ケーブル（CAT5）
- 取り外し可能なメディア
- 様々なタイプのアンテナ
- 電源装置
- Syncケーブル
- SDカード

ツール

- スペクトラムアナライザ
- クリンパー

ソフトウェア

- Android
- iOS
- 様々なオペレーティングシステム：OS X、Windows、Linux、Unix
- メッセージングクライアントソフトウェア
- 証明書管理ソフトウェア
- MDM、MAM、MCMソフトウェア

その他

- インターネットアクセス