認定ガイド

Intel Security 認定製品スペシャリスト

McAfee ePolicy Orchestrator (ePO)

Intel Security 認定を取得する理由

テクノロジとセキュリティの脅威が進化を続ける中、企業は最新の技法と技術に対応する最新の認定を取得している社員を必要としています。IDC のホワイトペーパーによると、ある調査では IT 管理者の 70% 以上が認定の取得は IT チームにとって有益であり、時間と費用をかけて維持する価値があると回答しています。

Intel Security 認定を取得すると、他のセキュリティプロフェッショナルとの違いを明確に示すとともに、認定試験で網羅されている重要なスキルを習得していることを実証できます。また、継続的な学習とプロとしての成長に対する真剣な姿勢が周囲から認識されるようになります。

Intel Security 認定プログラムについて

現在 Intel では、Intel Security 認定プログラムの一環として、業界で高いレベルの評価を得ている Intel Security 認定製品スペシャリストと Intel Security 認定セキュリティプロフェッショナルの 2 つの認定を提供しています。

Intel Security 認定製品スペシャリストは、特定のマカフィー製品または製品スイートの管理者（その製品または製品スイートの使用経験 1〜3 年）を対象としています。この認定レベルの取得者は、該当製品の次のような重要な知識を習得していることを実証できます。

- インストール
- 構成
- 管理
- 基本的なアーキテクチャとトラブルシューティング

Intel Security 認定セキュリティスペシャリストは、1〜3 年の経験を有するセキュリティ実務者（侵入テスター、監査人、コンサルタント、管理者）を対象としています。この認定レベルの取得者は、次のような高度な評価領域の知識を習得していることを実証できます。

- プロファイリングとインベントリ
- 脆弱性の識別
- 脆弱性の悪用
- 拡大する影響

このガイドについて

このガイドは、**Intel Security 認定セキュリティプロフェッショナル — ePolicy Orchestrator (ePO)** 試験の準備を支援するために作成されています。その他の認定試験や Intel Security 認定プログラムに関する詳細については、**www.mcafee.com** で [大企業のお客様]、[サービス]、[研修サービス] の順に選択して内容を確認してください。

ハイライト

このガイドは、Intel Security 認定製品スペシャリスト ePO 試験（MA0-100）の準備に役立つリソースとして作成されており、次の内容で構成されています。

- Intel Security 認定プログラムについて
- 試験の詳細
- 試験の準備に推奨するリソース
- ナレッジドメインのトピック
- サンプルの試験問題

intel Security

Intel Security 認定製品スペシャリスト — ePolicy Orchestrator (ePO)

この試験の合格者は、McAfee ePolicy Orchestrato ソリューションのインストール、構成、管理を正常に実行するために必要な知識とスキルを有していることが実証されます。この試験は、McAfee ePO 製品と関連テクノロジの 1〜3 年の使用経験を有するセキュリティプロフェッショナルを対象としています。

試験の詳細

- 関連試験: MA0-100
- 関連トレーニング: McAfee ePolicy Orchestrator Administration (4 日間)
- 問題数: 115
- 試験時間: 165 分
- 合格スコア: 72%
- 試験料: 150 米ドル (試験料は変更されることがあります。
  正確な料金については、**www.prometric.com/mcafee** で確認してください)。

試験の準備

この試験に推奨される準備:

- 4 日間の McAfee ePolicy Orchestrator Admininstration トレーニング (**https://mcafee.netexam.com/catalog.html**)
- McAfee ePO の 1 年以上の使用経験
- McAfee ServicePortal (**https://support.mcafee.com**)
- ナレッジドメイン (このガイドの後半を参照)
- サンプルの問題 (このガイドの後半を参照)

認定の登録

Intel Security では、包括的なテスト/評価サービスの主要グローバルプロバイダである Prometric と提携して認定プログラムの管理を行っています。Prometric によって、認定の開始から終了までのプロセスが簡易化されています。世界の 5,000 以上の拠点を利用して、都合に合わせて試験を受験し、Intel Security の認定を取得できます。

試験に登録するには、**www.prometric.com/mcafee** にアクセスしてください。

試験時間

Intel Security 認定プログラムの試験時間には、各試験施設で試験中に行われる次の活動の所要時間が含まれます。

- 試験問題の解答時間
- 指示を確認する時間と、試験終了後にコメントを提供する時間

Intel Security は、試験の内容および所要時間をいつでも変更できる権利を有します。試験内容と時間の最も正確な情報は、試験当日に試験プロバイダに確認してください。試験の開始前には、試験問題の解答時間を示す通知が画面に表示されます。

認定証明書

Intel Security 認定試験の合格者には、Intel Security Certification Program Candidate サイトへのアクセス権が付与されます。このサイトでは以下を入手できます。

- Intel Security 認定プログラム証明書、証明書共有ツールへのアクセス
- カスタム認定ロゴのダウンロード方法
- Intel 認定合格者向けの補足情報とオファー
- 合格者の連絡先情報の設定およびプロファイル
- ニュースとプロモーション

McAfee ePolicy Orchestrator Administration（4 日間）

試験前の正式なトレーニングの受講は義務ではありませんが、**McAfee ePolicy Orchestrator Administration**（4 日間）の受講をお勧めします。

このコースは、McAfee ePolicy Orchestrator（ePO）の使用方法に関する詳しいトレーニングを提供します。このコースを修了すると、McAfee ePO の導入計画、既存の McAfee ePolicy Orchstrator 環境内への ePO の導入、ePO システムコンポーネントの構成を行えるようになります。また、ePO 分類の使用方法と、重要な環境の追跡、保護、監視方法を習得できます。

このコースに登録するには、**https://mcafee.netexam.com/catalog.html** にアクセスしてください。

実務（実地）経験

McAfee ePO と関連テクノロジの 1 年以上の使用経験が必要です。以下に、推奨される実務的な活動の一部を示します。

- アーキテクチャ設計
- インストール/アップグレード
- 構成
- 管理
- トラブルシューティング

Technical ServicePortal

Technical ServicePortal は、次のような重要なツールとリソースへの単一アクセスポイントとして機能します。

- ドキュメンテーション
- セキュリティ掲示板
- 技術的な記事
- 製品のダウンロード
- ツール

ServicePortal には、**https://support.mcafee.com** からアクセスしてください。

Expert Center コミュニティ

Expert Center はマカフィー製品ユーザー向けのコミュニティです。Expert Center では、マカフィー製品に関する次のような重要情報を入手できます。

- 教育ビデオとホワイトペーパー
- エクスパートとその他のユーザー向けのディスカッションフィード
- ベースライン確立、および IT 環境強化のためのガイドライン
- 監視、対応、修復プロセスの効率化方法

Expert Center には、**https://community.mcafee.com/community/business/expertcenter** からアクセスしてください。

試験ナレッジドメイン

サーバーのインストールと設定

- インストール
  （デフォルトポート、コンポーネント、プロトコル、暗号化、ウィザードインストールの除外など）
- Web コンソール（ブラウザバージョン、UI のナビゲーション、切り取り/貼り付け機能、ブラウザの整理など）
- ユーザーアカウント
- 権限セット
- 自動対応
- ePO リポジトリ
  （ソース、フォールバック、SuperAgent、分散、マスターなど）
- エージェントハンドラ
  （インストールとルールなど）
- メニュー/設定/サーバー設定
- メニュー/設定/登録サーバー

サーバーの保守とトラブルシューティング

- サーバーの保守、ユーティリティ、サーバータスク
- SQL 保守
- ログファイル
- リカバリ
- パフォーマンス監視
- 状況チェック

製品とポリシーの管理

- ポリシーの管理
  （複製、割り当て、作成、削除、エクスポート、ポリシーカタログなど）
- スパー/エージェントポリシー
- 製品ポリシーの設定
- 拡張機能のインストール
- 製品の保守
- ポリシー割り当てルール
- 比較（ポリシーとタスクなど）
- クライアントタスク
  （作成、スケジューリング、適用、継承など）
- 製品の導入

McAfee エージェント

- インストール
  （イメージ、サードパーティ導入など）
- エージェント通信
- その他の機能
  （サーバーの中継、ピアツーピア、エージェントツーエージェント、階層など）
- ロギング
- 分散リポジトリ
- トラブルシューティング
  （sitelist. xml、重複する GUID など）

システムツリー

- システムツリーの作成
- システムツリーの配置とソート
- タグ
  （クライアントタスク/プロパティ/システム事前ソート/レポートのタグ付け、タグのグループ化など）
- システム情報
- 不正システム検出

クエリとレポート

- クエリの作成
- レポートの生成
- ダッシュボード/モニター
- 監査ログ
- イベント分析
  （脅威イベント、消去、脅威分析）

サンプルの試験問題

参考のために、以下に試験問題のサンプルを示します。Intel Security 認定製品スペシャリスト ePO 試験の問題は、形式も内容も以下に示す問題に類似しています。解答は問題の後に掲載されています。

1. **エージェントの通信を管理するのは次のどの ePO サービスですか?**
   - **A** イベントパーサー
   - **B** フレームワークサービス
   - **C** Tomcat
   - **D** Apache
2. **登録 LDAP サーバーは、次のどの認証タイプとともに使用されますか?**
   - **A** SQL 認証
   - **B** Windows 認証
   - **C** 証明書ベースの認証
   - **D** ePO 認証
3. **障害復旧に関する記述で正しいのは次のうちどれですか?**
   - **A** Keystore 暗号化パスフレーズの変更にはデータベース管理者権限が必要である。
   - **B** Keystore 暗号化パスフレーズは、サーバースナップショットに保管されている機密情報の暗号化と復号化に使用される。
   - **C** 障害復旧は、すべてのデータベースタイプに対してデフォルトで有効化されている。
   - **D** Keystore 暗号化パスフレーズを変更するには、以前のパスフレーズが必要である。
4. **割り当てをロックすることによって防止できるのは次のうちどれですか?**
   - **A** 親でのポリシーの変更
   - **B** クライアントタスクの変更
   - **C** 継承の変更
   - **D** ユーザーによる変更
5. **分散リポジトリ間でコンテンツをコピーするには、次のどのタスクを構成しますか?**
   - **A** アップデートタスク
   - **B** ミラータスク
   - **C** オンデマンドスキャンタスク
   - **D** オートアップデートタスク
6. **ポリシーは、次のどのファイルタイプを使用すると ePO にインポートできますか?**
   - **A** CSV
   - **B** PDF
   - **C** HTML
   - **D** XML
7. **「My Organization」グループに割り当てられているポリシーが削除された場合、代わりに次のどのポリシーが割り当てられますか?**
   - **A** McAfee Default
   - **B** Parent Group
   - **C** My Default
   - **D** Global Root
6. **ePolicy Orchestrator 管理者は、次のどの方法を使用すると ePolicy Orchestrator サーバーと直接通信できないネットワークブロードキャストセグメント内の資産を管理できますか?**
   - **A** ピアツーピア通信を有効にする
   - **B** エージェントを SuperAgent に変換する
   - **C** Agent Deployment URL を活用する
   - **D** エージェント中継サーバーを構成する

9. McAfee Agent を VDI モードでインストールする目的は何ですか?

A VDI モードを使用して、仮想環境内の非永続的仮想マシンの GUID の複製を防止する

B VDI モードによって、仮想クライアントと互換性のないポイント製品が誤ってインストールされないようにする

C 仮想マシンが再プロビジョニングされたときにエージェントを再インストールできるように、VDI モードを使用して管理資格証明を保管する

D 帯域幅を節約するために、VDI モードを使用して、同一クラスタ内の仮想マシンにアップデートプル用のソースを提供する

10. ポリシーとタスク管理を簡易化するのは、次のどの重要システムツリープロパティですか?

A Hierarchy (階層)

B Lock Policy (ポリシーのロック)

C Inheritance (継承)

D Enforcement (施行)

11. Active Directory の同期を構成する際、次のどの要素のために例外を作成できますか?

A 組織単位 (OU)

B セキュリティグループ

C ドメイングループ

D ユーザー

12. グループに 4 つのソート条件が割り当てられている場合、システムがこのグループに配置されるのは次のいくつの条件と一致したときですか?

A 1 つ

B 2 つ

C 3 つ

D 4 つ

解答キー
1. D
2. B
3. B
4. C
5. B
6. D
7. A
8. D
9. A
10. C
11. A
12. A

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com