認定ガイド

Intel Security 認定製品スペシャリスト

Data Loss Prevention Endpoint (DLPe)

TM

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 Data Loss Prevention Endpoint (DLPe)** 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 DLPe 試験（MA0-103）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 — Data Loss Prevention Endpoint (DLPe)

この試験の合格者は、McAfee Data Loss Prevention Endpoint 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 DLPe 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: MA0-103
- 関連トレーニング: McAfee Data Loss Prevention Endpoint Administration (4 日間)
- 問題数: 60
- 試験時間: 165 分
- 合格スコア: 78%
- 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 Data Loss Prevention Endpoint Administration トレーニング (**https://mcafee.netexam.com/catalog.html**)
- McAfee DLPe 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 Data Loss Prevention Endpoint 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 Data Loss Prevention Endpoint Administratioin** (4 日間) の受講をお勧めします。

このコースは、McAfee Data Loss Prevention Endpoint (DLPe) 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 DLPe 導入計画の立案、既存の McAfee ePolicy Orchstrator 環境内への DLPe の導入、DLPe 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、DLPe 分類の使用方法と、重要な情報の追跡、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 DLPe 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

ネットワーキング

- ネットワーキングテクノロジの理論、原則、実務
- データネットワーキングの標準とプロトコル
- LAN および WAN テクノロジ
- ネットワーク管理
- ネットワークおよびルーティングプロトコル
- ベースライン条件
- 境界セキュリティ
- 内部ネットワークセキュリティ
- 基本インフラストラクチャ
- スニッフィング/ネットワーク監視
- TCP/IP と NAT/PAT

システム

- クライアント/サーバーテクノロジ
- グループポリシーの概要とセキュリティテンプレート
- Web 権限と許可
- 冗長化/フォールトトレランス/高可用性
- ドライブ暗号化
- システム管理
- 仮想環境
- プロセッサ（CPU）
- ベースライン条件
- システムのアクセスとナビゲーション
- マルチサーバー環境
- オペレーティングシステム

アプリケーション:

- データベース
- 冗長性
- Web プロトコル
- ベースライン条件

ポリシーと手順

- 権限、移譲、監査
- ユーザーアクセスを管理するポリシー
- ロール権限
- システムテスト手順
- プロアクティブな保護スキャンポリシー
- ネットワークパスワード手順
- 企業セキュリティポリシー
- デバイス利用ポリシー
- 変更管理手順
- 製品固有の保守手順
- インシデント対応手順
- ロール固有のエスカレーション手順
- 企業セキュリティ制御
- 企業セキュリティ戦略
- デバイスアクセス制御

アーキテクチャと統合のベストプラクティス

- 必要なセキュリティのレベル
- 問題隔離ツール/プラクティス
- 業界セキュリティ基準
- セキュリティ監視

セキュリティ基盤

- ファイアウォール
- コンピュータウイルス、スパイウェア、マルウェア、スパム
- ネットワーク脅威防止テクノロジ
- スパイウェア防止テクノロジ
- ファイアウォールテクノロジと侵入防止
- ヒューリスティックベースの保護
- 認証
- 脆弱性と修復技法
- マルウェアインシデント
- 内部の脅威と攻撃
- 外部の脅威と攻撃
- セキュリティプロトコル
- 暗号化
- ネットワークセキュリティポリシー
- ネットワークアクセス制御
- 一般的な脅威と脆弱性

運用と管理

- パスワード管理
- ネットワークおよびサポート管理ツールと手順
- パッチ管理
- セキュリティアラート、フロントライン分析、エスカレーション
- 侵入検知システム
- 監視ツール
- 問題特定
- インシデントと問題の分類
- 基本製品機能
- 製品ポリシー設定
- 製品レポート作成
- バージョン管理
- 詳細な製品機能
- 保護マテリアル

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 DLPe 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. **タグ付けされたデータの不正な配布を防止する必要がある場合、次のどの DLPe ルールを使用するのが最も適していますか?**
   - **A** 分類ルール
   - **B** データルール
   - **C** 保護ルール
   - **D** タグ付けルール
2. **重要でなくなったコンテンツの管理方法として、次のどのアクションが最も適切ですか?**
   - **A** evidence フォルダにコンテンツを追加する
   - **B** data-at-rest フォルダにコンテンツを追加する
   - **C** data-at-motion フォルダにコンテンツを追加する
   - **D** whitelist フォルダにコンテンツを追加する
3. **リムーバブルメディアとストレージデバイスを保護するのは、次のどの DLP コンポーネントですか?**
   - **A** DLP Endpoint Agent
   - **B** DLP Device Control
   - **C** DLP Incident Manager
   - **D** DLP Service WatchDog
4. **このクライアントソフトウェアがセーフモードで完全に機能するように構成するには、[Agent Configuration] のどのタブ上でこの機能を設定しますか?**
   - **A** [Miscellaneous] タブ
   - **B** [Security] タブ
   - **C** [Advanced Configuration] タブ
   - **D** [File Tracking] タブ
5. **DLP クライアントソフトウェアが完全に機能するように構成するには、次のどの手順を実行する必要がありますか?**
   - **A** On-the-Go 保護を有効にする
   - **B** Safe Mode オプションを有効にする
   - **C** Universal 保護を有効にする
   - **D** WatchDog サービスを有効にする
6. **Microsoft Outlook に [McAfee DLP] アイコンを表示するには、[Show Release from Quarantine Controls in Outlook] オプションを、[Agent Configuration] のどのタブ上で有効にする必要がありますか?**
   - **A** [Miscellaneous] タブ
   - **B** [Security] タブ
   - **C** [Advanced Configuration] タブ
   - **D** [File Tracking] タブ
7. **次のどの機能を使用すると、ブロッキングルールを一時中断できますか?**
   - **A** エージェントバイパス
   - **B** Master release (マスターリリース)
   - **C** Override key (オーバーライドキー)
   - **D** 隔離のリリース
8. **McAfee DLP Device Control ソフトウェアでは、次のどの定義をオフ (利用不可能) にできますか? (2 つ選択してください)**
   - **A** すべてのリムーバブルストレージデバイス
   - **B** McAfee Endpoint Encryption で暗号化されたコンテンツ
   - **C** McAfee Encrypted USB
   - **D** 権限管理
   - **E** Web 宛先

9. リポジトリフォルダとして最初に使用することが推奨されるのは、次のどのフォルダパス/名前ですか？該当するものをすべて選択してください。

A c:\dlp_resources\

B c:\dlp_resources\evidence

C c:\dlp_resources\blacklist

D c:\dlp_resources\whitelist

10. ディクショナリの検索一致の特徴は次のうちどれですか？該当するものをすべて選択してください。

A 大文字と小文字を区別する

B フレーズの検索一致を行える

C 部分文字列を検索できる

D UTF-8 をサポートする

解答キー

1. C
2. D
3. B
4. C
5. B
6. A
7. A
8. D、E
9. A、B、D
10. B、C、D

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