認定ガイド

Intel Security 認定製品スペシャリスト

Security Information Event Management (SIEM)

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 Security Information Event Management (SIEM)** 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 McAfee 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 SIEM 試験（MA0-104）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。

- McAfee 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 — Security Information Event Management (SIEM)

この試験の合格者は、McAfee SIEM 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 SIEM 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: MA0-104
- 関連トレーニング: McAfee SIEM Administration 101 (4 日間)、McAfee SIEM Advanced Administration 201 (4 日間)
- 問題数: 70
- 試験時間: 65 分
- 合格スコア: 63%
- 言語: 英語
- 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 SIEM Administration 101 トレーニング (**https://mcafee.netexam.com/catalog.html**)
- 4 日間の McAfee SIEM Administration 201 コース (**http://www.mcafee.com/us/services/product-training/index.aspx**)
- McAfee SIEM 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、McAfee 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 Securiy 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 SIEM 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 SIEM Administration 101**（4 日間）および/または **McAfee SIEM Administration 201** コースの受講をお勧めします。

McAfee SIEM Administration 101 コースは、McAfee Security Information and Event Management（SIEM）ソリューションのセットアップおよび管理に関する詳細なトレーニングを提供します。講義と実践的なラボでの演習を通じて、複雑な企業環境に効果的に SIEM ソリューションを導入する方法を習得できます。

McAfee SIEM Administration 201 コースでは、ガイド付きのデモと独立したラボ環境を活用して、McAfee SIEM アプライアンスを設定して操作し、企業環境で発生しやすいセキュリティの問題を解決します。

各コースに登録するには、**http://www.mcafee.com/us/services/product-training/index.aspx** にアクセスしてください。

実務（実地）経験

McAfee SIEM 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。

- ソリューションの計画
- 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

McAfee ServicePortal

McAfee 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。

Intel Security Expert Center コミュニティ

Intel Security 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/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

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
- セキュリティ監視
- 問題隔離ツール/プラクティス

セキュリティ基盤

- 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
- 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
- 内外の脅威と攻撃
- 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とアクセス制御
- 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。MCPS — SIEM 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. **レシーバーのプロパティを介してアクセスできるのは、次のどの機能ですか？**
   - **A** アラーム
   - **B** データソースプロファイル
   - **C** ウォッチリスト
   - **D** 資産の管理
2. **デフォルトのイベント集計は、次のどのフィールドで実行しますか？**
   - **A** シグネチャ ID
   - **B** ユーザー名
   - **C** 宛先ポート
   - **D** ソースポート
3. **機能的な SIEM スタックを構成するのは、次のどのコンポーネントですか？**
   - **A** Data Processing（データ処理）
   - **B** Correlation（相関）
   - **C** Mitigation（回避策）
   - **D** Policy Updating（ポリシーアップデート）
4. **Global Threat Intelligence（GTI）ウォッチリストに関する記述で、次のうち正しくないのものはどれですか？**
   - **A** サードパーティの脅威アドバイザリで構成される
   - **B** 不審/悪質な IP アドレスを含むウォッチリストで構成される
   - **C** スコアソースとして使用される
   - **D** McAfee からライセンス提供される
5. **ELM ストレージプールは、ミラーリングのオーバーヘッドのために何パーセントの割り当てスペースを必要としますか？**
   - **A** 1%
   - **B** 5%
   - **C** 10%
   - **D** 20%
6. **ネットワークから 12 時間にわたって、イベントおよびネットワークフローの統計値が収集されました。ファイアウォールは合計 450,000 イベント、UNIX サーバーは合計 62,000 イベント、Web アプリケーションは合計 1,200,500 イベント、ルーターは合計 150,000,000 フローを生成しました。この統計に基づくと、このネットワークの合計 EPS の値はどうなりますか？**
   - **A** 3,511
   - **B** 3,472
   - **C** 3,500
   - **D** 3,510
7. **McAfee Enterprise Security Manager（ESM）システムクロックのデフォルト設定は、次のどのタイムゾーンですか？**
   - **A** 国際日付け変更線西側
   - **B** 東部標準時
   - **C** グリニッジ標準時
   - **D** 地理的な場所

8. マルウェアの調査時に、アナリストは McAfee SIEM のどのウォッチリストを使用すると検索をすばやく絞り込めますか?

A Botnet - Control Channel（ボットネット - コントロールチャネル）

B Malware Detections（マルウェア検出）

C GTI Suspicious and Malicious（GTI 不審/悪質）

D Passive DNS - Malware Domain（パッシブ DNS - マルウェアドメイン）

9. 子データソースに関する記述で、次のうち正しくないものはどれですか?

A VIPS、Policy、および Agent の権限が付与される

B ［Receiver Properties］>［Data Sources］テーブルに表示される

C System Navigation ツリーに表示される

D データソースの合計数にはカウントしない

10. イベントデータベースが格納されるのは、次のうちどのアプライアンスですか?

A ESM

B ADM

C ELM

D DEM

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

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