認定ガイド

Intel Security 認定製品スペシャリスト

McAfee Network Security Platform (NSP)

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 Network Security Platform (NSP)** 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 NSP 試験（MA0-101）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 — Network Security Platform (NSP)

この試験の合格者は、McAfee Network Security Platform 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できます。この試験は、McAfee NSP 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: MA0-101
- 関連トレーニング: McAfee Network Security Platform Administration (4 日間)
- 問題数: 100
- 試験時間: 120 分
- 合格スコア: 70%
- 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 Network Security Platform Administration トレーニング (**https://mcafee.netexam.com/catalog.html**)
- McAfee NSP の 1 年以上の使用経験
- McAfee Service Portal (**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 Network Security Platform 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 Network Security Platform Administration**（4 日間）の受講をお勧めします。

このコースは、McAfee Network Security Platform（NSP）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、NSP の導入計画、Manager のインストールと構成、ユーザーとリソースの管理、ポリシーの構成と管理、脅威の分析と脅威への対応、効率性向上のためのセキュリティポリシーの調整を行えるようになります。

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 NSP 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

セットアップ

- NSP のインストール
  （サーバーの要件、計画など）
- NSP の構成
  （ドメイン、ユーザーアカウント、認証、対応管理、通知など）
- NSP のナビゲーション
- センサーのインストール
  （センサーのサイジング、計画、配置、ポート、運用モードなど）
- センサーの構成（CLI コマンドなど）
- 保守とトラブルシューティング
  （バックアップ、データベースの調整、ファイルの削除など）
- 統合（EPO、NTBA、GTI など）

ポリシー管理

- Policy Manager（作成、割り当てなど）
- IPS ポリシー
  （カスタム攻撃エディタ、攻撃の定義、インポート/エクスポート、システム調整など）
- 高度なマルウェアポリシー
- 検査オプションポリシー
- 接続制限ポリシー
- ファイアウォールポリシー
- サービス品質（QoS）ポリシー
- 例外
  （ルールの無視、ファイルハッシュ例外、ドメイン名例外など）
- オブジェクト
  （ポリシーグループ、ルールオブジェクト、攻撃セットプロファイルなど）

イベント管理

- ダッシュボード監視
- 脅威分析
  （脅威エクスプローラ、マルウェア検出、攻撃ログ、pcap 分析、パターンの認識など）
- 対応アクション
  （ホワイトリスト、ブラックリスト、アップデートポリシー、無視ルールの作成など）
- レポート

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 NSP 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. **初期構成の際に、センサーへの管理接続に使用できるのは次のうちどれですか？**
   - **A** RJ45
   - **B** RJ11
   - **C** 監視ポート
   - **D** コンソールポート
2. **アラートとパケットログをアーカイブするには、次のどのパスを選択する必要がありますか？**
   - **A** [Manage] | [Maintenance] | [Archiving]
   - **B** [Manage] | [Alerts] | [Archiving]
   - **C** [Maintenance] | [Alerts] | [Archiving}
   - **D** [Manage] | [Maintenance] | [Alerts] | [Archiving]
3. **なぜ DBAdmin ツールは、NSM 内で実行可能なシステム保守タスクの実行方法として望ましいのですか？**
   - **A** Manager 上の追加のワークロードを削減する
   - **B** 信頼性
   - **C** スピード
   - **D** 使いやすさ
4. **センサーを構成する前に、次のどの手順を完了しておく必要がありますか？**
   - **A** センサー IP アドレスの設定
   - **B** Manager へのセンサーの追加
   - **C** センサーのユーザー名とパスワードの設定
   - **D** センサーゲートウェイアドレスの設定
5. **センサーのヘルスチェックのためにセンサー上で発行できるのは、次のどのコマンドですか？**
   - **A** show sensor health
   - **B** show health status
   - **C** show config
   - **D** check health
6. **Policy Manager で、インターフェイスレベルで修正できないポリシーは、次のどの場所で初期作成されたものですか？**
   - **A** 親ドメイン
   - **B** 子ドメイン
   - **C** トップドメイン
   - **D** 隣接しないドメイン
7. **ルールセットを適用できないのは、次のどのポリシーですか？**
   - **A** 同一のルールセットが両方のトラフィックフローに適用されているポリシー
   - **B** 1 つのルールセットがすべてのトラフィックに適用されているポリシー
   - **C** 各トラフィックフローに異なるルールセットが適用されているポリシー
   - **D** 各トラフィックフローに 2 つのルールセットが適用されているポリシー
8. **デバイスレベルで、IPS ポリシーを変更して追加/除外できないのは次のうちどれですか？**
   - **A** Default McAfee Attacks（デフォルトのマカフィー攻撃）
   - **B** Modified McAfee Attacks（修正されたマカフィー攻撃）
   - **C** Custom McAfee Format Attacks（カスタムマカフィーフォーマット攻撃）
   - **D** Custom Snort Attacks（カスタム Snort 攻撃）

9. NSP CLI で、L2 モード機能を有効にするのは次のどのコマンドですか?

A layer2 mode off

B layer2 mode on

C layer2 mode assert

D layer2 mode deassert

10. ドメインレベルの例外オブジェクトがセンサーレベルで割り当てられている場合、次のどの項目が該当しますか?

A そのセンサー上でそのオブジェクトを使用する他のリソースに影響はない。

B そのセンサー上でそのオブジェクトを使用する他のリソースにも影響がある。

C 管理者に警告するために、Fault レベルの警告が NSM に送信される。

D センサーレベルの設定が無視される。ドメインレベルの設定が常に優先される。

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

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