SANS サイバーセキュリティのトレーニング、認定、学位、および研究のための最も信頼できる情報源

GIAC CERTIFICATIONS

# SEC401: Security Essentials: Network, Endpoint, and Cloud

GSEC Security Essentials giac.org/gsec

6日間 プログラム | 46 CPEs | ラップトップが必要になります

## SEC401で習得する事項

- サイバーセキュリティの中核となる分野と、検知、応答、防止の基礎に基づいたセキュリティプログラムの構築方法
- 組織内で優先度の高いセキュリティ問題に対処し、効果的なセキュリティソリューションにつながる正しい行動をとることに焦点を当てた、実践的なヒントとコツ
- 敵対者がどのように戦術や技術を変えていくのか、それに合わせてどのように防御を変えていくのか
- ランサムウェアとは何か、そしてランサムウェアからどのように防御するか
- 持続的脅威の指標に基づいた、防御可能なネットワークアーキテクチャ（VLAN、NAC、802.1x）を活用する方法
- 強固な認証（Multi-Factor Authentication）の側面を含むアイデンティティおよびアクセス管理（IAM）の方法論
- マルチクラウドの概念を含む、トップ3のクラウドプロバイダー（Amazon、Microsoft、Google）の強みと違いを活用する方法
- 様々なツールを使用してシステムの目に見える弱点を特定し、弱点が発見されたら、システムをより安全にするために設定する方法（有能な脆弱性管理プログラムの現実的かつ実用的な適用）。
- tcpdumpやWiresharkなどのツールを使用して、ネットワーク通信プロトコルをスニッフィングし、ネットワーク通信の内容（アクセス認証情報を含む）を特定する方法
- Windows、Linux、macOSのコマンドラインツールを使用してシステムを分析し、危険性の高い指標を探し出す方法、および継続的な監視を自動化するための基本的なスクリプトの概念。
- 攻撃対象領域の検証に使用するネットワーク可視化マップの構築方法、およびハードニングと構成管理による攻撃対象領域の削減のための最良の方法の決定方法
- セキュリティに関して、勝つ組織と負ける組織がある理由、そして最も重要なのは、勝つ側に回る方法です。

このコースでは、攻撃を未然に防ぎ、攻撃者を検知するための最も効果的な手法について学びます。仕事に戻ってすぐに使える実践的なテクニックです。ネットワーク・システム環境に危害を加えようとする様々なサイバー攻撃者との戦いに勝利するためのヒントやテクニックが満載です。

組織は常に狙われているため、最終的な侵害に備えなければなりません。今日では、かつてないほど迅速な検知と対応が重要になっています。攻撃者が自組織の環境に存在する期間が長ければ長いほど、その影響は甚大なものとなり、ダメージも大きくなります。情報セキュリティにおける最も重要な問題は、「いかに早く敵を検知し、対応し、修復するか」ということかもしれません。

情報セキュリティとは、適切な防御領域に焦点を当てることであり、特に組織の独自性に適用することが重要です。SEC401では、コンピュータや情報セキュリティの用語や基本的な仕組みを学び、それを自組織のニーズに合わせて適用する方法を学びます。また、システムや組織のセキュリティを担当する際に必要となる、本質的かつ効果的なセキュリティの知識を得ることができます。

SEC401は、情報セキュリティの初心者の方から、専門的な知識を持つベテランの方まで、オンプレミスやクラウドを問わず、重要な情報や技術資産を保護・保全するために必要な情報セキュリティのスキルとテクニックを提供します。また、学んだ概念を、現代の敵対者の立場に立って、勝利のための防御戦略に直接適用する方法も紹介します。これが私たちの戦い方であり、これが私たちの勝ち方です。

## 「SEC401: Security Essentials: Network, Endpoint, and Cloud」はあなたにとって正しいコースですか？

次のことを自問して見てください。

- 一部の組織は侵入され危険に晒されているものの、他の組織はそうではない理由を十分に理解していますか？
- ネットワーク上のシステムが侵害された場合、そのシステムを見つけることができると確信していますか？
- 各セキュリティデバイスの有効性を知り、それらが全て正しく構成されていることを確認していますか？
- 適切なセキュリティ基準が設定され、セキュリティ上の意思決定を行うために経営陣と意思疎通していますか？

SEC401は、ブートキャンプスタイルのハンズオンラボを通じて、これらの質問に答えるために必要な情報セキュリティに関する知識を提供します。

**「SEC401は、素晴らしいナレッジベースを提供します。サイバーセキュリティに携わるすべての人にとって、SEC401は不可欠であると言えます」**

—Thomas Wilson, Agile Systems

**sans.org/sec401**

- このコースのプレビューを見る
- このコースが開催されるイベントを探す

詳細については、Japan@sans.org またはお電話（+81 3 3242 6276）にてお問い合わせください。

# コース詳細

### SECTION 1: ネットワークセキュリティとクラウドの基礎

攻撃者が企業のリソースにアクセスする主な侵入経路は、インターネットに接続されたネットワークを経由することです。組織はできるだけ多くの攻撃を阻止しようとしますが、最終的にすべての攻撃を防げるわけではないため、少なくともタイムリーに検知することが必須になります。したがって、このようなディフェンシブルなネットワークアーキテクチャをどのように構築するかを理解することが重要です。ディフェンシブルなネットワークについての議論は、クラウドに関する理解と、考慮しなければならない重要なセキュリティ上の注意事項を抜きにしては成り立ちません。システムアーキテクチャや設計の種類、通信フロー、さらにはルーターやファイアウォールなどのデバイスを使用した攻撃防御方法を知り、理解することも同様に重要です。この最初のセクションでは、トレーニング全体に共通する知識基盤を確立するための必須事項などについて説明します。

**主なトピック:** ディフェンシブルネットワークアーキテクチャ、プロトコルとパケット分析、仮想化

### SECTION 2: Defense-in-Depth（多層防御）

このセクションでは、システムに対する大規模な脅威と、それに対する防御方法を見ていきます。多層防御と呼ばれる原則を利用して、防御を重ねる必要があることを学びます。まずは情報保証の基礎から始まり、IAM (Identify and Access Management)、そして、現代の敵の存在下で機能し得る最新のセキュリティ対策（CIS Critical Controls、MITRE ATT&CKなどの活用）に焦点を移し、最後にBYOD（Bring Your Own Device）からMDM（Mobile Device Management）まで、モバイルデバイスの利点とセキュリティリスクについて徹底的に議論します。

**主なトピック:** 多層防御、IAM、Critical Controls、認証とパスワードセキュリティ、セキュリティフレームワーク、DLP、モバイルデバイスセキュリティ

### SECTION 3: 脆弱性管理とインシデントレスポンス

脆弱性は、攻撃者が悪用する弱点のことです。このセクションでは、脆弱性が発生するさまざまな領域を発見する手法を学ぶため、脆弱性アセスメントとペネトレーションテストから始まり、攻撃の方法論、適切な対応計画を作成する方法までをカバーします。

**主なトピック:** 脆弱性アセスメント、ペネトレーションテスト、攻撃とマリシャスソフトウェア、Webアプリケーションセキュリティ、セキュリティオペレーションとログ管理、デジタルフォレンジックとインシデントレスポンス

### SECTION 4: データセキュリティテクノロジー

セキュリティ対策に特効薬はありません。しかし、多くのセキュリティ問題の解決に役立つと思われながらほとんどの組織で実装されていない技術があります。その技術とは暗号化です。暗号化はメッセージの意味を隠してしまうことで、権限のない者による機密情報の読み取りを阻止できます。このセクションでは、暗号化のさまざまな側面と企業の資産を保護するための暗号の使用法について見ていきます。関連分野として、ステガノグラフィや情報の隠ぺいについてもカバーします。

**主なトピック:** 暗号化、暗号化アルゴリズムとその実装、暗号の利用、ネットワークセキュリティデバイス、エンドポイントセキュリティ

### SECTION 5: WindowsとAzureのセキュリティ

Windowsがシンプルだった頃を覚えているでしょうか。Windows XPが小さなワークグループを占めていた以前のことはどうでしょうか。あれから、多くの技術的革新があり、今日ではWindowsTabletやAzure、Active Directory、PowerShell、Office365、Hyper-V、仮想デスクトップインフラ（VDI）などが私たちの周りに普及していますが、マイクロソフトはGoogleやApple、アマゾンをはじめとしたクラウドサービスの巨人たちを相手に覇権争いを繰り広げています。言うまでもなく、セキュアにできることが全てです。Windowsは、世界中で最も広く使われ、かつターゲットにされているOSです。同時に、Active Directory、PKI、BitLocker、AppLocker、およびユーザーアカウント制御の複雑さは、課題でもあり有益にも成り得ます。このセクションでは、Windowsセキュリティの世界をいち早くマスターするとともに、作業を簡素化・自動化するためのツールについて学習します。自動化と監査、フォレンジックを通して、Windowsセキュリティの堅固な基礎を築くことができます。

**主なトピック:** Windowsセキュリティインフラストラクチャ、Windows as a Service、Windowsアクセスコントロール、セキュリティポリシーの適用、Microsoftクラウドコンピューティング、自動化・ロギング・監査

### SECTION 6: Linux、Mac、スマートフォンのセキュリティ

多くの組織では、それほど多くのUnix/Linuxシステムは所有していませんが、最も保護すべき重要なシステムの一部です。このセクションでは、Linuxシステムのセキュリティを向上させるために必要な実践的なガイダンスを提供します。Linux初心者のための背景情報を含む実践的な手引きから、あらゆるレベルの専門家向けのセキュリティアドバイスや「ベストプラクティス」までを包含する内容になっています。例えば、コンテナとは何か、コンテナは何をするのか、コンテナ管理のベストプラクティスについて学びます。また、LinuxとUNIXの概念を理解するため、Microsoft AzureとAWSを比較検証し、AppleのMacOS を確認してコースを終了します。

**主なトピック:** Linux の基礎:、Linuxセキュリティの強化とインフラストラクチャ、コンテナ化されたセキュリティ、AWSの基礎、AWSセキュリティコントロール、AWSの堅牢化、macOSのセキュリティ

## 受講対象者

- 情報セキュリティに関する知識を整理したいと考えているセキュリティ担当者
- 情報セキュリティに関する専門用語や概念について、さらに理解を深めたいと考えているマネージャクラスの方
- セキュリティが主業務ではないが、効果的なセキュリティについて理解する必要のある運用担当者
- 防御的なネットワーク構築に関連する知識が必要なITエンジニア・管理者
- 攻撃者にさらされやすいシステムの構築や保守を担う管理者
- セキュリティスキルの基盤を固めておきたいフォレンジックアナリスト、ペネトレーションテスター、監査者
- 情報システムやネットワークにある程度の経験を持ち、情報セキュリティ業務に初めて携わる方

**GSEC**
Security Essentials
giac.org/gsec

### GIAC Security Essentials

GIACセキュリティエッセンシャル(GSEC)認定は、単純な用語や概念を超えて、情報セキュリティに関する実務家の知識を検証します。GSEC認定資格者は、セキュリティ・タスクに関して、ITシステムの実務を担当する資格があることを証明します。

- アクティブディフェンス、ディフェンスインデプス、アクセスコントロールとパスワード管理
- 暗号：基本概念、アルゴリズムと展開、応用
- 防御可能なネットワークアーキテクチャ、ネットワークとプロトコル、ネットワークセキュリティ
- インシデント処理と対応、脆弱性スキャンと侵入テスト
- Linux セキュリティ：構造、パーミッション、アクセス、ハードニングとセキュリティ、監視と攻撃検知、セキュリティユーティリティ
- セキュリティポリシー、コンティンジェンシープラン、クリティカルコントロール、ITリスクマネジメント
- Web通信セキュリティ、仮想化・クラウドセキュリティ、エンドポイントセキュリティ
- Windows：アクセスコントロール、自動化、監査、フォレンジック、セキュリティインフラ、ネットワークサービスの保護