コースコード：F5-BIG-ASM-ESS
税込価格：481,800円 (税抜価格：438,000円)
日数：4日間

---

## トレーニング内容

この4日間のコースは、ウェブアプリケーションへのHTTPベースアタックの検知、軽減、防御に必要な専門知識を理解頂くためのコースです。本コースでは、アプリケーション･セキュリティ･ポリシーを実装するための最も簡単なレベルから始まり、より複雑な構成の設定までを学習します。本コースには、ブルートフォースやウェブスクレイピング、レイヤ7 DDoS、その他現在の攻撃ベクトルに対してのウェブアプリケーションの防御についての解析やハンズオンが含まれます。

## ここに注目!!

## 受講対象者

このコースの受講対象者は次の通りです。

本コースは、BIG-IP ASMシステムのインストレーション、セットアップ、構成、運営の責任を負うシステム管理者およびネットワーク管理者の方を対象としています。

## 前提条件

このコースを受講する前に受講者が習得しておく必要がある知識およびスキルは次のとおりです。

Administering BIG-IP
を受講された方、またはF5-CA認定資格を取得済みの方、もしくは同等の知識をお持ちの方

## 目的

このコースを修了すると次のことができるようになります。

BIG-IP ASMシステムの機能と設定を理解し、基本的な管理からアドバンスオブジェクトの設定構築までの実施

## アウトライン

Chapter 1: BIG-IP システムのセッティング
- BIG-IP システム紹介
- BIG-IP システムの初期設定
- BIG-IP システムのアーカイブ作成
- F5 サポートリソースとツールの利用

Chapter 2: BIG-IPトラフィックプロセス

- LTMでのトラフィックプロセッシングの理解
- ローカルトラフィックポリシーとASM概観

Chapter 3: ウェブアプリケーションコンセプト
- ウェブアプリケーションの構造解
- 一般的なセキュリティメソッド概観
- HTTPの検査 & ウェブアプリケーションコンセプト
- HTTP ヘッダーの検査
- HTTP レスポンスの検査
- HTML コンポーネントの検査
- ASM での ファイルタイプ 、URLs、パラメータの解析方法
- Fiddler HTTP プロキシツールの使用方法

Chapter 4: ウェブアプリケーションの脆弱性
- OWASP トップ 10の 脆弱性の検査
- ASMでのリスク軽減の概要

Chapter 5: セキュリティポリシー
- ポジティブとネガティブセキュリティモデルについて
- デプロイメントウィザード: ローカルトラフィックデプロイメント
- デプロイメントウィザード: コンフィグレーションセッティング
- バイオレーションとセキュリティポリシービルディング
- バイオレーションの確認

Chapter 6: アタックシグネチャ
- アタックシグネチャの定義
- アタックシグネチャの機能
- アタックシグネチャセットの定義
- ユーザ定義アタックシグネチャについて
- アタックシグネチャのアップデート
- アタックシグネチャとステージングの理解

Chapter 7: ポジティブセキュリティビルディング
- セキュリティポリシーコンポーネントの定義
- エンティティラーニングを通してのセキュリティ
- ステージングとエンフォースメントの復習
- セレクティブモードの理解
- 識別の学習: 本当の脅威 vs. 誤検出

Chapter 8: クッキーとその他のヘッダー
- ASM クッキーの目的
- 許可されたクッキーと強制されたクッキーの理解
- HTTP ヘッダーのセキュリティプロセッシングの設定

Chapter 9: リポーティングとロギング
- ASMのリポーティング性能
- PCI コンプライアンスリポートの生成
- セキュリティイベントリポートの生成

Chapter 10: ユーザ権限、ポリシー変更と管理
- ユーザ権限とパーティションの理解
- セキュリティポリシーの編集とエキスポート

Chapter 11: 実習プロジェクト1

Chapter 12: アドバンスパラメータハンドリング
- パラメータの定義
- スタティックパラメータの定義

- ダイナミックパラメータと抽出の設定

Chapter 13: アプリケーションテンプレート
- アプリケーションテンプレートの概観

Chapter 14: ポリシービルダー
- ポリシービルダー概観
- ポリシータイプの定義
- ポリシービルダールール

Chapter 15: ウェブ アプリケーション ボーナビリティ スキャナー
- ASMとアプリケーションボーナビリティースキャナーの統合
- 脆弱性の解決
- XMLスキャナーアウトプットの使用

Chapter 16: ログインエンフォースメント、セッショントラッキングとフロー
- ログインページの定義
- ログインエンフォースメントの設定
- セッションとユーザアタッキングの設定
- フローの設定
- フローコントロールの設定

Chapter 17: 異常検知
- 異常検知の定義
- ブルートフォースアタックの防止
- ウェブスクラッピングの防止
- ジオロケーション エンフォースメント
- IP アドレス例外設定

Chapter 18: ASM and iRules
- iRules と iRuleイベントの定義
- ASM iRule イベントモードの使用
- iRule 構文
- ASM iRule コマンド

Chapter 19: Web 2.0 サポート: AJAX と JSON
- Asynchronous JavaScript と XMLの定義
- JavaScript Object Notation (JSON)の定義
- JSON プロファイルの設定

Chapter 20: XML と ウェブサービス
- XMLの定義
- XML プロファイルの設定
- XML アタックシグネチャ

Chapter 21: 復習と最終実習プロジェクト