# Vexトレーニングテキスト

# DAST スキャニング 基礎編



目次



**Version 1.1**

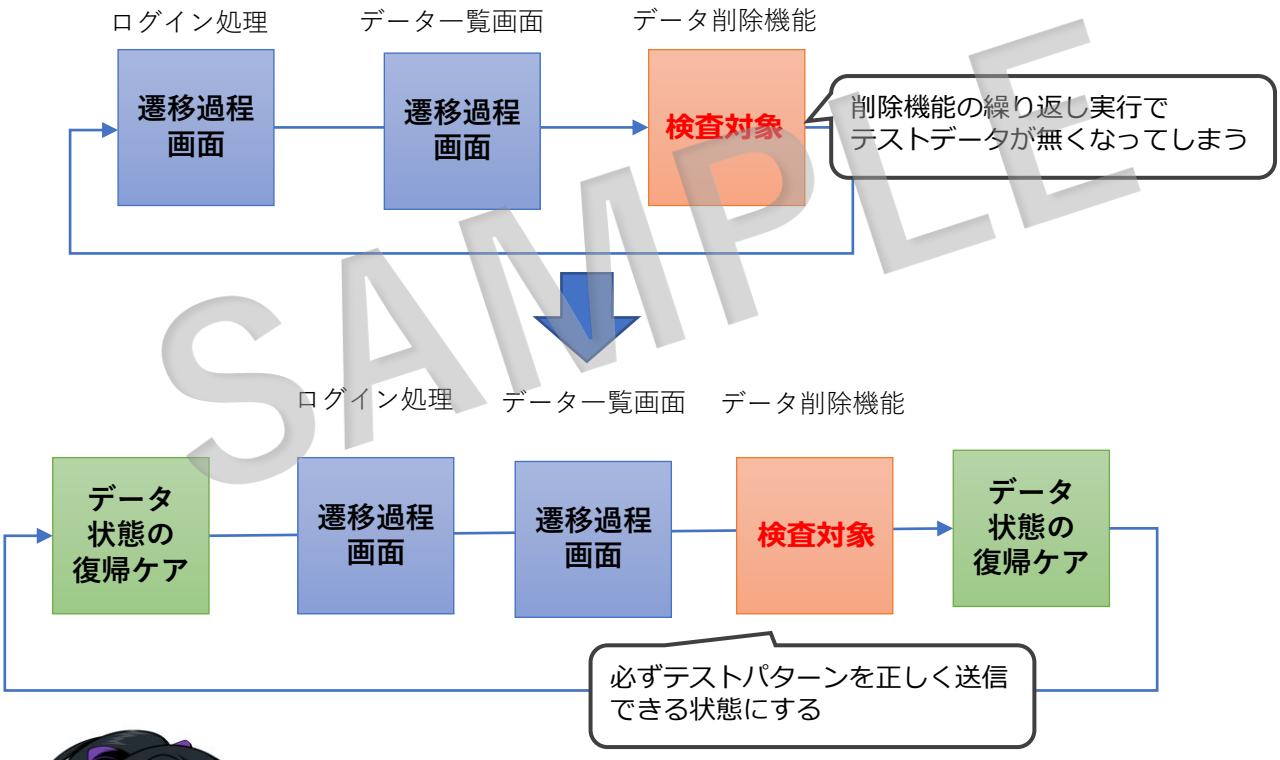
# 1. DASTツール使用時のアプローチ

VexはDAST(***D***ynamic ***A***pplication ***S***ecurity ***T***esting)に分類されるセキュリティテストを実施します。DASTとは実際に動作しているアプリケーションにテストパターンを送信し、アプリケーションの動作状態を観測するセキュリティテストの手法です。Vexに限らずDASTツール使用時はツール設定の考え方にいくつかのポイントがあります。

## 1-1. DASTツール使用時の原則

DASTツールは、検査対象画面に大量の検査パターンを送信します。
検査パターンを送信するごとに、検査対象画面のデータステータスを同一の状態(テストパターンを送信できる状態)となるよう、テストシナリオ設定をする必要があります。

### 例：削除機能をテストする場合




繰り返しテストパターンを送信できるように、テストシナリオ（画面の遷移順）を構成しましょう。

# 2.画面遷移の分析

DASTのテストシナリオはいくつかのパターンに分類されます。本章では代表的なテストシナリオパターンを解説します。

| | 機能分類 | 基本パターン |
|---|---|---|
| 1 | 認証機能<br>（ログイン、ログアウト） | ・アカウントロック<br>・重複ログインチェック |
| 2 | データ登録系機能 | ・登録数制限-アカウント単位の制限がある場合<br>・登録数制限-対象サイト全体で制限がある場合 |
| 3 | データ削除系の機能 | |
| 4 | データ編集系の機能 | ・繰り返し編集処理が可能な場合<br>・繰り返し編集処理が不可能な場合 |
| 5 | キャプチャ認証系機能 | ・原則不可<br>・特例で検証用環境や実装不備がある場合 |

基本パターンに沿って、どのような画面遷移を構成すればよいか検討してみましょう。

# 3.データフローの分析

データフローの分析は以下の観点があります。

| | 分析観点 | 基本パターン |
|---|---|---|
| 1 | 各画面に対して引き継ぐデータはどれか | ・セキュリティトークン<br>・データ識別のID<br>・日付・時刻情報 |
| 2 | データの発行箇所はどこか | ・データが必要となる画面の直前に発行される場合<br>・必要なデータが複数画面で発行される場合<br>・画面からの引継ぎでなく新たにデータを発行する場合 |

引き継ぐデータはアプリケーションにより異なり、様々なデータがあります。
アプリケーションを分析して、各データがどのように使われるかを理解しましょう。

# Vexトレーニングテキスト

## VCA
## 模擬試験
## シナリオ解説編



Version 1.2

# 目次

# 2. 模擬試験サイトについて

模擬試験の検査対象Webアプリケーションは、UBsecurePict社の商品販売管理サイトです。管理サイトには、ログイン機能、ユーザ管理、商品管理など一般的な機能が実装されています。

模擬試験で出題されている検査対象機能は以下の機能となります。出題対象の機能は模擬試験環境上のヒアリングシートより確認可能です。

| 機能カテゴリ | 出題対象となる検査対象機能 |
|---|---|
| 1　認証機能 | ・　ログイン |
| 2　データ閲覧系機能 | ・　カタログ一覧 |
| 3　データ登録系機能 | ・　管理者アカウント登録<br>・　カテゴリ登録 |
| 4　データ削除系の機能 | ・　管理者アカウント削除 |
| 5　データ編集系の機能 | ・　管理者アカウント変更<br>・　管理者パスワード変更<br>・　ユーザ情報変更 |
| 6　CAPTCHA認証系機能 | ・　ユーザパスワードリセット<br>・　ユーザ情報変更 |



セキュリティ検査を始める前に、検査対象サイトの機能概要を把握しましょう

# 3. セキュリティテスト対象の概要把握

セキュリティテストを円滑にすすめるためには、セキュリティテスト対象となるWebアプリケーションの機能概要を把握し、Webアプリケーションの仕様に沿ったテストシナリオを作成する必要があります。

本章では、 Webアプリケーションの仕様に沿ったテストシナリオを作成するための、Webアプリケーションの分析方法を解説します。

## ■ 解説概要

効果的・効率的なテストシナリオを作成するためには、Webアプリケーションの利用用途や全体像の把握と、テスト対象機能の動作確認が重要となります。これには、 2つの目的があります。

### 目的1. Webアプリケーションのビジネスリスクを把握する

セキュリティテストの目的は、Webアプリケーションに存在するリスク（脆弱性）を洗い出すことにあります。Webアプリケーションの利用目的や想定利用シーン、取扱情報を含めたアプリケーション全体像を把握することで、Webアプリケーションにおけるビジネスリスクを明確にすることができます。

また、ビジネスリスクが明確になれば、リスクに応じたテストスコープ（テスト対象範囲）の判断が可能となり、効率的にセキュリティテストを実施できるようになります。

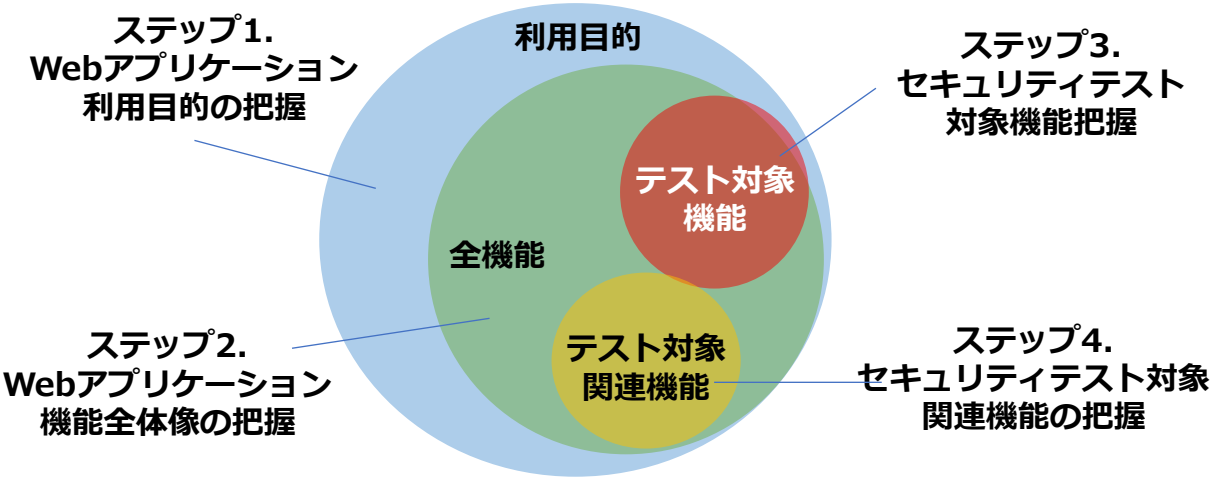
### 目的2. テスト対象機能の仕様とテストシナリオに利用可能な関連機能を把握する

セキュリティテストでは、連続で安定的にアクセス可能なテストシナリオを作成する必要があります。テストシナリオは、テスト対象機能の仕様に合わせて画面遷移順とデータフロー(データの受け渡し)を設定する必要があるため、以下のような内容を確認する必要があります。

- 対象機能のアクセスに必要なアクセス権限/アクセス時のデータ要否など
- データ量や実行回数の制限、データ作成方法など

なお、テスト対象機能の仕様によっては、テスト対象以外の機能へのアクセスを必要とするケースもあるため、利用可能な関連機能(パーツ)についても把握しておく必要があります。

Webアプリケーションの分析ステップは以下のイメージとなります。



# 4. 認証機能のテストシナリオ

本章では認証機能のテストシナリオ構築について解説します。模擬試験の出題範囲において認証機能に属する画面は以下の通りです。

| Function ID | 機能名 |
|---|---|
| MNGAUT0001 | ログイン入力 |
| MNGAUT0002 | ログイン処理(リダイレクト) |

## ログイン入力～ログイン処理(リダイレクト)

### ■ 解説対象機能

| Function ID | 機能名 |
|---|---|
| MNGAUT0001 | ログイン入力 |
| MNGAUT0002 | ログイン処理(リダイレクト) |



## ■ 解説概要

ログイン処理に対するテストシナリオを検討します。一般的にログイン処理のテストシナリオにおいて、最も注意すべき点は、認証機能に対するセキュリティ対策機構の実装有無です。セキュリティ対策機構を考慮せずにテストシナリオを構築すると、認証機能がロックされます。（一定時間ログイン試行ができないなどの状態となります。）

認証機能に対する一般的なセキュリティ対策機構の例を以下に示します。

| 認証機能に対するセキュリティ対策機構 | 概要 |
|---|---|
| 1　アカウントロック（連続認証失敗時） | 連続してログインを失敗すると、<br>・一定時間ログインができなくなる<br>・ロックの解除操作が必要となる　など |
| 2　アカウントロック（単位時間辺りのログイン試行） | 単位時間あたり（例：1分間、10分間など)に大量のログイン試行を検知すると、<br>・一定時間ログインができなくなる<br>・ロックの解除操作が必要となる　など |
| 3　重複ログイン検知 | 同一アカウントで、既存のログイン中セッションがあると、ログインができない。<br>実装方法はさまざまあるが、重複ログインを検知した場合は、関連セッションを強制的にログアウトさせる画面が表示されるケースなどがある |



模擬試験サイトではアカウントロック（連続認証失敗時）が実装されています。そのため、本章ではアカウントロックを回避するためのテストシナリオの作成方法を解説します。

本章で学ぶ内容

✓ アカウントロックを確認する方法
✓ アカウントロックを回避するためのテストシナリオ
✓ CSRFトークンの設定
✓ ログアウト処理の設定

# Vexトレーニングテキスト

## VCA
## 模擬試験
## トリアージ解説編



Version 1.0

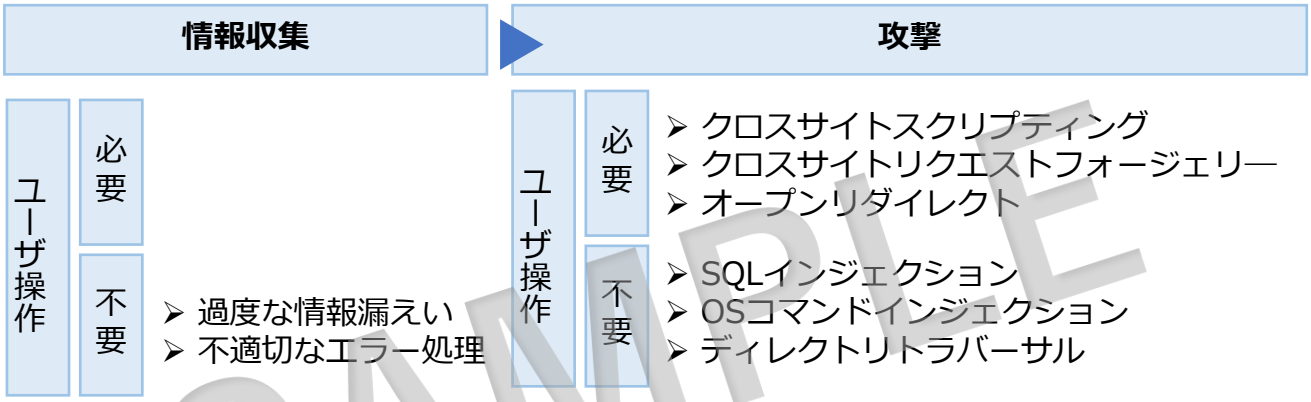
# 目次

# 2. 模擬試験で出題される脆弱性

VCAで出題対象となる脆弱性一覧は以下の通りです。

1. **過度な情報漏えい**
2. **不適切なエラー処理**
3. **クロスサイトスクリプティング**
4. **クロスサイトリクエストフォージェリー**
5. **オープンリダイレクト**
6. **SQLインジェクション**
7. **OSコマンドインジェクション**
8. **ディレクトリトラバーサル**

サイバーセキュリティの攻撃工程は様々な工程に分解することが可能です。Webアプリケーションに関する脆弱性を「情報収集」、「攻撃」の工程に分類すると以下のようになります。






情報収集に関する脆弱性は、システム内部の情報収集が可能です。利用プロダクトのバージョンやサーバ内部のパス情報などを取得することが可能です。これらの情報は、別の攻撃を実行する際に活用される可能性があります。

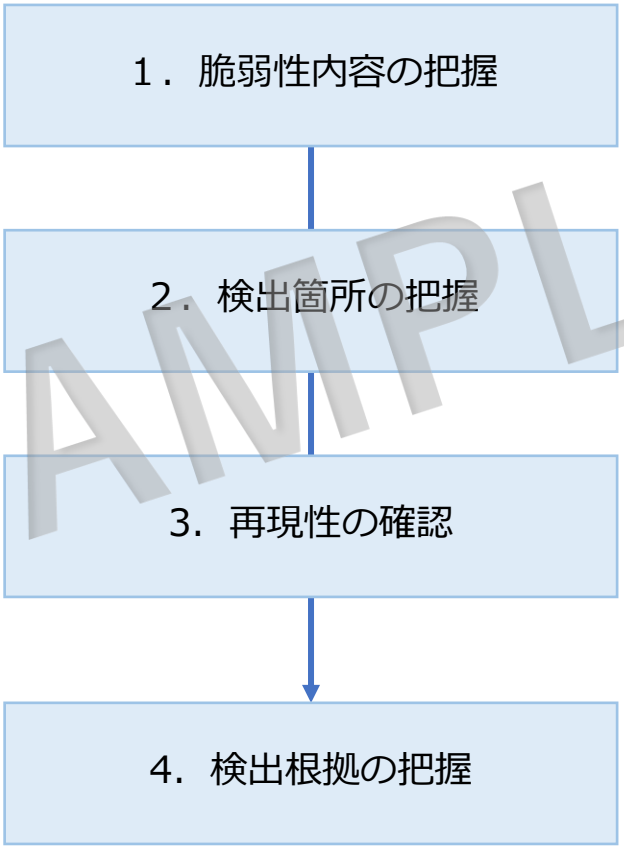
また、攻撃手法の分類としては、「ユーザ操作を必要する攻撃」と「ユーザ操作を必要としない攻撃」に分類されます。「ユーザ操作を必要する攻撃」は、「受動的攻撃」とも呼ばれます。受動的攻撃とは、攻撃者は脆弱性が発動するような罠を作成し、利用者を罠に誘導する攻撃です。受動的攻撃に属する攻撃としては、クロスサイトスクリプティング、クロスサイトリクエストフォージェリーなどがあります。

「ユーザ操作を必要としない攻撃」は、「能動的攻撃」とも呼ばれます。攻撃者はWebアプリケーションに直接攻撃を実行します。SQLインジェクションやOSコマンドインジェクションなど、○○インジェクションと呼ばれる脆弱性は大半が能動的脆弱性に分類されます。

# 3. 脆弱性判定の基本アプローチ

DASTツールで検出された脆弱性の精査（検知 or 過剰検知)をするため基本的なステップを解説します。ここで解説する内容は、Vexに限らず多くのツールに活用できる内容となっています。

ツールで検出された脆弱性の精査フローは以下のようになります。1～2の工程で、どのような脆弱性が、どこの画面で検出しているかを把握します。次に、再現性があることを確認します。最後に、ツールが脆弱性を検出した根拠を確認します。






次ページから各ステップについて詳細に解説していきます。

## 3-1. 脆弱性内容の把握

まずは、検出した脆弱性の内容（概要）について理解することが大切です。Vexでは検査結果の詳細画面から、脆弱性の概要解説を確認することが可能です。