# OWASP Top 10 演習ワークシート（受講者用）

指示：各章の問いに対して、実際に環境で確認した結果や考察を記入してください。

## 1. アクセス制御の不備 (A01)

シナリオ：/admin に誰でもアクセスできる。実際に /admin にアクセスして結果を記載せよ。対策案（箇条書き）を3つ書け。

## 2. 暗号化の不備 (A02)

シナリオ：ユーザーパスワードが平文または可逆保存されている。なぜ問題かを簡潔に説明し、安全な保存方法を記せ。

## 3. インジェクション (A03)

シナリオ：検索フォームに任意の入力で挙動を変えられる。脆弱な入力と想定される攻撃例を1つ記載し、対策を1つ示せ。

## 4. 安全でない設計 (A04)

シナリオ：ログイン失敗時に詳細エラーが返る。設計上の問題点を2つ挙げ、改善案を示せ。

## 5. 設定ミス (A05)

シナリオ：デバッグモードや不要な公開ファイルがある。どのファイルや設定を点検すべきか、チェックリストを作れ。

## 6. 脆弱・古いコンポーネント (A06)

シナリオ：依存ライブラリに既知脆弱性の通知がある。優先順位付けの基準と初動対応を記せ。

## 7. 認証・識別の不備 (A07)

シナリオ：パスワードリセットトークンが推測可能。安全なトークン運用の要件を箇条書きで示せ。

## 8. ソフトウェア／データ整合性の失敗 (A08)

シナリオ：外部ライブラリを署名検証なしで使用。整合性確認の手順を簡潔に説明せよ。

## 9. ログ・監視の不備 (A09)

シナリオ：重要な失敗ログが未記録。どのイベントをログに残すべきか、優先度を3つ挙げよ。

## 10. SSRF (A10)

シナリオ：ユーザー指定URLをサーバが取得する。安全に実演するための運用ルールを3つ挙げよ。

# 模範解答（要点）

サーバ側の認可チェック不足が原因。対策：エンドポイント毎の権限チェック、RBAC/ABAC、最小権限

可逆保存は漏洩時に危険。対策：bcrypt/Argon2等のKDFとユニークソルト

入力をSQLとして組み込むと構造が変化する。対策：プリペアドステートメント、入力検証

詳細エラーは情報漏洩につながる。対策：内部ログにのみ詳細を残し、利用者には一般的なメッセージを返す。

チェック項目：デバッグ設定、不要ファイル、公開ディレクトリ、CSP等。自動化スキャン導入

優先度は利用頻度・CVSS・影響範囲で決定。初動はSBOM確認、テスト、段階的適用

トークンは推測困難・短命・一度限り、有効期限と関連通知を必須にする

手順：配布元確認、ハッシュ/署名検証、CIでの整合性チェック、SBOMの管理

優先ログ：認証失敗、権限変更、重要設定変更。ログの保全と監視を実装

運用ルール：実演はローカルで隔離、ホワイトリストのみ許可、不要な外部接続を遮断