セキュリティテスト実施報告書

[1. 概要 2](#_Toc5052688)

[ テスト実施日時 3](#_Toc1005055806)

[ テスト方法 3](#_Toc1107254609)

[ テスト対象 3](#_Toc520799175)

[ 備考 3](#_Toc2079935773)

[2. リスクと信頼度の評価 3](#_Toc2030007083)

[ Risk（リスク） 4](#_Toc63541671)

[ Confidence（信頼度） 4](#_Toc547082819)

[3. セキュリティテスト結果詳細 4](#_Toc1488406155)

[ Content Security Policy (CSP) Header Not Set 5](#_Toc225921059)

[ Missing Anti-clickjacking Header 6](#_Toc1643872906)

[ Strict-Transport-Security Header Not Set 7](#_Toc952681916)

[ Cross-Domain JavaScript Source File Inclusion 8](#_Toc1847674930)

[ X-Content-Type-Options Header Missing 9](#_Toc238084691)

[ Modern Web Application 10](#_Toc1177984055)

[ Information Disclosure - Suspicious Comments 11](#_Toc220898894)

[ Re-examine Cache-control Directives 12](#_Toc1094128071)

## 概要

品質保証として、ドローン生産在庫管理システムのセキュリティテストを実施しました。

セキュリティ診断ツール「OWASP ZAP（オワスプ・ザップ）」を用いて、Webアプリケーションの脆弱性をチェックし、実施結果を報告します。

### テスト実施日時

2024/12/30 18時00分 - 21時00分

### テスト方法

OSASP ZAPによる脆弱性診断

### テスト対象

ドローン生産在庫管理システム

<https://jmrzqmv6aa.ap-northeast-1.awsapprunner.com>

### 備考

なし

## リスクと信頼度の評価

### Risk（リスク）

この項目がどれだけ重大なセキュリティリスクを引き起こす可能性があるかを示します。

* + 高: 高いリスク、重大なセキュリティ問題。
  + 中: 中程度のリスク、注意すべきだが致命的ではない。
  + 低: 低いリスク、重大な問題ではない。
  + 情報: 情報提供のみで、特に脅威ではない。

### Confidence（信頼度）

この脆弱性が実際に存在するかどうかの確信度です。

* + 高: 高い確信度で、その問題が実際に存在すると判断された。
  + 中: 中程度の確信度、問題がある可能性があるが、確実ではない。
  + 低: 低い確信度、誤検知の可能性がある。

## セキュリティテスト結果詳細

総警告数： 8件

リスクレベル別の内訳

* + 中リスク： 2件
  + 低リスク： 3件
  + 情報レベル： 3件

信頼度別の内訳

* + 高信頼度： 2件
  + 中信頼度： 4件
  + 低信頼度： 2件

下記の通り記載します。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| * 診断結果項目   診断結果項目の説明   |  |  | | --- | --- | | Risk | Confidence | | リスクレベル | 信頼度レベル |   診断結果：  診断結果の詳細を記載します。  対応案：  対応案を記載します。 |

### Content Security Policy (CSP) Header Not Set

Content Security Policy (CSP) ヘッダーが設定されていない

|  |  |
| --- | --- |
| Risk | Confidence |
| 中 | 高 |

診断結果：

CSP（コンテンツセキュリティポリシー）ヘッダーが設定されていないため、スクリプトの実行やクロスサイトスクリプティング攻撃（XSS）のリスクがあります。

対応案：

1. サーバーで以下のようなCSPヘッダーを設定します：

|  |
| --- |
| css  Content-Security-Policy: default-src 'self'; script-src 'self'; object-src 'none'; |

1. 必要に応じて、script-srcやimg-srcで許可するドメインを指定します。
2. テスト環境でCSPポリシーを適用して、誤動作がないか確認します。

### Missing Anti-clickjacking Header

クリックジャッキング防止ヘッダーが不足している

|  |  |
| --- | --- |
| Risk | Confidence |
| 中 | 中 |

診断結果：

X-Frame-Optionsヘッダーが設定されておらず、クリックジャッキング攻撃に対して脆弱です。

対応案：

1. サーバーで以下のヘッダーを追加します：

|  |
| --- |
| mathematica  X-Frame-Options: SAMEORIGIN |

または

|  |
| --- |
| css  Content-Security-Policy: frame-ancestors 'self'; |

1. 必要に応じて外部サイトでの埋め込みを許可する場合は、そのドメインを明示的に指定します。

### Strict-Transport-Security Header Not Set

HSTS ヘッダーが設定されていない

|  |  |
| --- | --- |
| Risk | Confidence |
| 低 | 高 |

診断結果：

HTTP Strict Transport Security（HSTS） ヘッダーがないため、プロトコルダウングレード攻撃のリスクが高まります。

対応案：

1. サーバーに以下のヘッダーを設定します：

|  |
| --- |
| lua  Strict-Transport-Security: max-age=31536000; includeSubDomains; preload |

1. 必要に応じてpreloadオプションを使用してHSTSプリロードリストに登録します。

### Cross-Domain JavaScript Source File Inclusion

クロスドメインJavaScriptのソースファイルが含まれている

|  |  |
| --- | --- |
| Risk | Confidence |
| 低 | 中 |

診断結果：

サードパーティのJavaScriptソースが使用されており、不正なコードの実行リスクがあります。

対応案：

1. 信頼できるドメインのJavaScriptのみを使用します。
2. 可能な限りサードパーティのスクリプトを自サーバーでホスティングします。
3. 外部スクリプトを使用する場合、CSPポリシーで許可するソースを明確に指定します。

### X-Content-Type-Options Header Missing

X-Content-Type-Optionsヘッダーが欠落している

|  |  |
| --- | --- |
| Risk | Confidence |
| 低 | 高 |

診断結果：

MIMEタイプスニッフィング攻撃を防ぐためにX-Content-Type-Optionsヘッダーが必要です。

対応案：

1. サーバーに以下のヘッダーを設定します：

|  |
| --- |
| css  X-Content-Type-Options: nosniff |

1. これにより、ブラウザが指定されたMIMEタイプを強制的に使用します。

### Modern Web Application

モダンウェブアプリケーションの識別

|  |  |
| --- | --- |
| Risk | Confidence |
| 情報 | 中 |

診断結果：

アプリケーションが最新技術を使用していることを示す情報で、攻撃者がシステム特有の攻撃方法を検討する可能性があります。

対応案：

1. 使用しているフレームワークやライブラリのバージョン情報を隠す設定を検討します。
2. サーバーのレスポンスヘッダー（例: X-Powered-By）を削除します。

### Information Disclosure - Suspicious Comments

疑わしいコメントによる情報漏洩

|  |  |
| --- | --- |
| Risk | Confidence |
| 情報 | 低 |

診断結果：

開発中の情報やデバッグコメントが含まれており、攻撃者に悪用される可能性があります。

対応案：

1. ソースコードをレビューして、不必要なコメントを削除します。
2. 特にパスワード、APIキー、開発中の情報などが含まれていないことを確認します。

### Re-examine Cache-control Directives

Cache-Controlヘッダーの見直しが必要

|  |  |
| --- | --- |
| Risk | Confidence |
| 情報 | 低 |

診断結果：

適切なキャッシュ制御がされていないため、セッション管理やプライバシーリスクがあります。

対応案：

1. セッションや機密情報を含む応答に以下のヘッダーを設定します：

|  |
| --- |
| yaml  Cache-Control: no-store, no-cache, must-revalidate  Pragma: no-cache |

1. 静的リソースには適切なキャッシュポリシーを設定します。