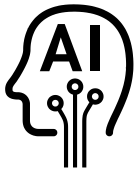


# OpenText Application Security Aviator

HITACHI

— 脆弱性への対策を生成AIによって効率化！ —



OpenText Application Security Aviatorは、静的解析ツールであるOpenText Application Security Testingから利用可能な生成AIによる支援機能です。

静的解析に関するお悩みを、生成AIを利用した OpenText Application Security Aviator を活用することで解決しましょう！ 次のようなお悩みがあれば、是非ご相談ください。



## お悩みの例

OpenText Application Security Aviatorを使えば…



静的解析では誤検知が多く発生し、問題のないコードまで脆弱性に繋がる可能性ありと判断される場合がある。

解析結果すべてに対し、誤検知かどうかを選別する作業は最終的に人手によって実施しており、非常に手間が掛かる。



生成AIによって、脆弱性に繋がる可能性がある項目の内容を理解し、誤検知かどうかを自動的に判断します。また、その判断理由についても丁寧に説明されるため、開発者がその正確性を的確に判断することができます。



静的解析を実施した結果、検知された脆弱性を修正しなければならないが、どのように修正すれば良いのかがわからない。

推奨される修正方法だけでなく、そのまま使えるサンプルコードまで提案してほしい。



脆弱性の説明に加えて、生成AIによって提案された修正コードの例が表示されます。これまでは開発者自身が深く検討する必要があった作業を技術的に支援し、効率化することが可能です。

～ 上記以外のさまざまなお悩みに関しても、お気軽にご相談ください！ ～

# OpenText Application Security Aviator 利用イメージ

**Aviatorによるフィードバック**

☆ Fortify Aviator 2024/07/05 02:35:57 PM  
Changed Auditor Status from 'Pending Review' to 'Remediation Required'

☆ Fortify Aviator 2024/07/05 02:35:57 PM  
The code is vulnerable to SQL injection because concatenating user input (username and password) allows an attacker to inject malicious SQL code or execute arbitrary SQL commands.

To fix this vulnerability, the following code should be used for string binding instead of string concatenation:

In file src/main/java/com/fortify/aviator/demo/HomeController.java, replace lines 44-47 by the following lines:

```
String query = "SELECT 1 FROM users WHERE username = ? AND password = ?";  
try (PreparedStatement stmt = connection.prepareStatement(query)) {  
    stmt.setString(1, username);
```

OpenText Static Application Security Testingの検出結果（この例ではSQLインジェクション）に対し、OpenText Application Security Aviatorが右記のような結果を表示します

Aviatorが「対策要」のステータスを自動でセット

修正方法と、修正コード案をAviatorが提示

## OpenText Application Security Aviator はどこから利用する？

### ■ OpenText Static Application Security Testing (オンプレ) の場合

Fortify CLI を利用し、OpenText Application Security 経由で利用します。

(詳細な手順はマニュアルに記載されています)

SAST Aviatorを始めるには以下の手順を実行してください:

1. FCLIをダウンロード
2. カスタマー管理者を登録してください
3. 個別ユーザー向けのトークン生成
4. アプリケーションを作成
5. SASTアビエータータグを適用してください
6. トリガー監査/一括監査実施
7. 自動修復を行う

### ■ OpenText Core Application Security (SaaS) の場合

opentext | Core Application Security CE 25.2 アプリケーション ダッシュボード

JP JavaWebApp > zip

静的スキャンの設定

静的スキャンの詳細

評価タイプ: Static Asses

この評価のステータス: 使用権

13738 - 評価 (26/01/07 に終了)

Fortify Aviator

Fortify Aviator はすべてのテクノロジー スタックで利用できます。  
<https://aws.amazon.com/marketplace/pp/prodview-3b3i27cz6kzw2>

スキャンの設定時にチェックを入れるだけ!

## ご参考価格

### ■ OpenText Static Application Security Testing (オンプレ) の場合

【年間サブスクリプション】57.6万円～

### ■ OpenText Core Application Security (SaaS) の場合

【静的、静的+に対して1評価ユニット追加】18万円～

※各種条件有り。

詳しくはお問い合わせください。

※本リーフレット中の会社名、商品名は各社の商標、または登録商標です。 ※本文中および図中では、TMマーク、®マークは表記しておりません。 ※製品の仕様は、改良のため、予告なく変更する場合があります。 ※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認のうえ、必要な手続きをお取ください。なお、ご不明な場合は、当社担当営業にお問い合わせください。 ※本リーフレット中の情報は、作成時点のものです。

株式会社日立ソリューションズ

[www.hitachi-solutions.co.jp](http://www.hitachi-solutions.co.jp)

本リーフレット掲載商品・サービスの詳細情報

[www.hitachi-solutions.co.jp/microfocus-enterprise/#a\\_fortify](http://www.hitachi-solutions.co.jp/microfocus-enterprise/#a_fortify)