CyberRes

ブローシャ

# Fortify on Demand 動的アプリケーション セキュリティテスト

# 動的アプリケーション セキュリティテスト

Fortify on Demand は、アプリケーションセキュリティをサービスとして提供するプラットフォームです。ソフトウェアセキュリティ保証プログラムを簡単に作成、改良、拡張するために必要なセキュリティテスト、脆弱性管理、専門知識、サポートを提供します。Fortify on Demand は DevOps のスピードに合わせて、開発者への継続的なフィードバックを行い、開発ツールチェーンに組み込まれた拡張性の高い**セキュリティテスト**により、**安全な開発**を支援します。

## ソフトウェア開発ライフサイクル全体にわたってアプリケーションを保護

企業のアプリケーションポートフォリオは、規模においても、複雑性においても、急速に拡大しています。お客様がビジネスを継続する上で、リスクや脆弱性からアプリケーションを保護することは、必要不可欠になっています。ソフトウェア開発ライフサイクル (SDLC) のすべてのフェーズでアプリケーションを保護する必要があります。アプリケーションのセキュリティは、コードの開発段階から始まります。テストを通じてコードを検証し、アプリケーションの本番稼働後も継続して監視を行います。アプリケーションセキュリティプログラムをソフトウェア開発ライフサイクル (SDLC) 全体に組み込むことが、ポリシーの遂行、コンプライアンス、継続的なセキュリティの実施を確実に行う最もコスト効率に優れた方法であると実証されています。品質保証 (QA) フェーズでソフトウェアの脆弱性を特定するには、動的アプリケーションセキュリティテスト (DAST) が欠かせません。

## ソフトウェアセキュリティに不可欠な Fortify on Demand の動的評価

Fortify on Demand の動的評価は、ソースコードの静的アプリケーションセキュリティテストを補完するもので、稼働中や疑似的な本番環境でしか検出されない脆弱性を特定できます。動的テストでしか検出できない脆弱性の例としては、設定関連の脆弱性や、高度なハッキング手法、アプリケーションのビジネスロジックを対象とした特殊な攻撃経路などがあります。

Fortify on Demand 動的アプリケーションセキュリティテスト (DAST) の評価は、次のような機能を備えています。

- 標的となるアプリケーションに対する実際のハッキング手法や攻撃を再現
- 複雑な Web アプリケーションや Web サービスを対象にした包括的なセキュリティ分析
- 攻撃対象領域をくまなくクローリングして悪用される可能性のある脆弱性を検出
- サイト間 VPN や Fortify on Demand の公式データセンター IP アドレスのホワイトリスト化を通じて社内アプリケーションをテスト可能

当社の DAST テクノロジーは、Web アプリケーション、Web サービス、モバイルブラウザー用に最適化されたアプリケーションをサポートしています。Fortify on Demand の DAST 評価が他と異なるのは、必須要素である WebInspect **自動テスト、手動分析、オプションのアクティブ IAST** の 3 つが統合されている点です。

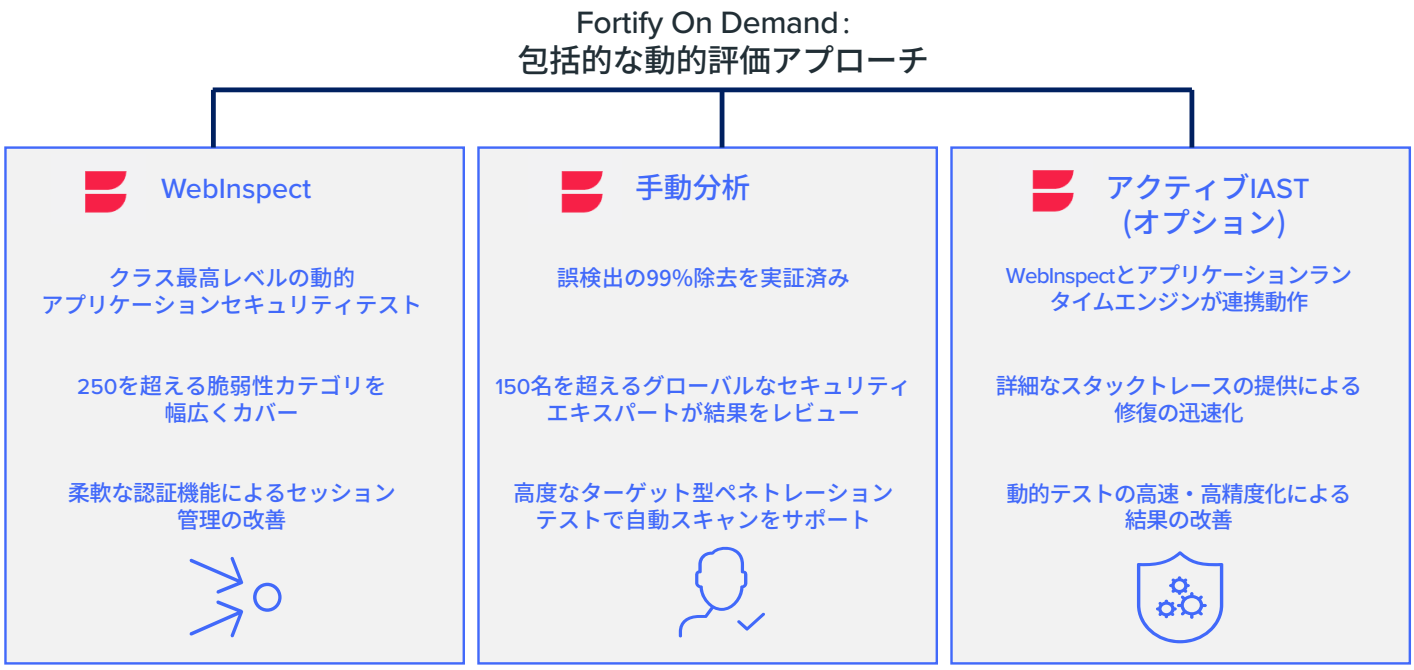


**図 1.** Fortify on Demand：包括的な動的評価アプローチ

## WebInspect の最先端 DAST 機能を活用

WebInspect は、Fortify on Demand DAST の基盤であり、業界をリードする動的 Web アプリケーションセキュリティ評価ソリューションです。今日の複雑な Web アプリケーションや Web サービスのセキュリティの脆弱性を細部まで分析するように設計されています。Fortify on Demand は、QA や、ステージング、本番環境にあるすべての Web アプリケーションや Web サービスから潜在的な脅威を検出します。

WebInspect の機能は次のとおりです。

- 250 を超える独自の脆弱性カテゴリをカバー
- スキャンの自動スケジュール設定と、スキャンブラックアウト期間中のスキャンの一時停止 / 再開のビルトインサポートにより時間とリソースを削減
- 柔軟な認証処理により、特に複雑なアプリケーションにおいてセッション管理が改善
- HTML5、Flash、JavaScript など、クライアント側言語を幅広くサポート
- 言語に依存しないスキャンテクノロジーによりほぼすべてのサーバー側言語に対応
- シングルページアプリケーション (SPA) や Web サービスを評価可能

## 当社の専任アプリケーションセキュリティエキスパートがスキャン結果を手動で分析

Fortify on Demand は、お客様の社内アプリケーションセキュリティチームの右腕になります。当社は、企業が新アプリケーションの開

発に多大な時間とコストを費やしていることを理解しています。広範にわたるレポートをレビューし、スキャンカバレッジを検証して誤検出を除外する時間や専門知識がない場合もあります。Fortify on Demand は、実用的な結果を確実に提供することを目的としています。そのため、さらに一歩踏み込んだサポートとして、150 人を超えるグローバルなセキュリティエキスパートから成る専任チームが、初期の動的スキャンの結果をすべて手動でレビューします。これには誤検出の切り分けと除外も含まれます。Fortify On Demand テストチームが実行するタスクには、次のようなものがあります。

- 必要に応じて認証用マクロを開発
- スキャンカバレッジの検証
- 手動監査と自動監査の両方を集約した結果から誤検出の 99% 以上を除去――修復にかかる時間とリソースを削減

また、当社のチームは、Fortify on Demand のテスト手法を使用して対象の Web アプリケーションや Web サービスを最大 8 時間にわたり手動で分析して、高度な標的型ペネトレーションテストで WebInspect のスキャン結果を補強することもできます。当社のエキスパートは、アプリケーションの認証スキーマ、セッション管理、アクセス制御を細かく調査し、ロジックの欠陥や開発者の誤った想定の有無を調査します。このような分析や調査により、人間が介入しなければ検出できない次のような脆弱性を特定できます。

- ユーザーアカウントを収集する機能
- 多段階認証のバイパス
- パスワードリセットの欠陥
- 他のユーザーのデータまたは機密性の高いコンテンツへのアクセス
- 水平方向や垂直方向の特権昇格
- ショッピングカートの支払いなどの重要なトランザクションステップのスキップ
- 割引やビジネス上の制限規定の悪用
- 開発者の誤った想定によるビジネスロジックの欠陥

## Fortify on Demand に含まれる動的評価を強化するためのアクティブ IAST オプション

アプリケーションセキュリティソリューションに Fortify が採用される理由として、イノベーションとリーダーシップがあります。当社が Fortifyon Demand のお客様に対して、動的評価時にアクティブ **IAST ( 対話型アプリケーションセキュリティテスト ) エージェント**を統合できるオプションを提供しているのもその一例です。IAST エージェントはアプリケーションランタイムサーバーにインストールされ、Fortify on Demand の動的評価の実行中に WebInspect と自動的に同期されます。IAST エージェントのメリットは次のとおりです。

- カバレッジの改善 ( 攻撃対象領域となるすべての主要コンポーネントをすべてテスト )
- 精度の向上 ( 誤検出の減少 )
- 迅速な修復 ( 詳細なスタックトレースの提供により個々の問題を識別 )

## 柔軟な動的評価サービスオプション

Fortify on Demand の動的評価は、明確なアプリケーションセキュリティ目標に対応できるように 2 つのサービスレベルで提供されます。どちらのサービスレベルもサブスクリプションまたはシングルスキャンとして購入できます。サブスクリプションパッケージでは、12 か月間、回数制限なくアプリケーションをスキャンできます。また、利用中の動的アプリケーションセキュリティテストプログラムが継続的にサポートされます。

どちらのサービスオプションが適しているかは、アプリケーションのリスクレベルによって異なります。

1. **Fortify on Demand の動的評価のサブスクリプション**は、すでにデプロイされている比較的リスクの低いアプリケーションや、ビジネスクリティカルとまでは言えないアプリケーションに最適です。動的評価は、より自動化された形で管理でき、サブスクリプション期間の間、繰り返し行われるリリースや新しい機能強化の際にセキュリティテストを行うことができます。
2. **Fortify on Demand の動的 + 評価サブスクリプション**は、ビジネスクリティカルでリスクの高いアプリケーションに最適です。潜在的な脆弱性をすべて特定するには、Fortify on Demand チームによる追加の手動分析が必要です。特に、個人情報の収集や金融取引の処理を行うアプリケーションには不可欠です。アプリケーションがセキュリティ被害を受けた場合の潜在的なリスクが高いほど、手動のテストや分析の必要性も高くなります。

ライフサイクルやコンプライアンス要件が限定的なアプリケーションには、シングルスキャンのほうが適している場合があります。シングルスキャンには、フルスキャンの結果として早期に報告された脆弱性の修復を検証するための修復スキャンも 1 回含まれます。修復スキャンは、最初の評価から 30 日以内に行う必要があります。大規模な手動テストを伴う Web サービスアプリケーションテストは、シングルスキャンとしてのみ利用できます ( サブスクリプションでは利用できません )。

**比較：Fortify on Demandの「動的」と「動的+」評価サービスのサブスクリプション**

| | Fortify on Demand の動的評価 | Fortify on Demand の動的 + 評価 |
|---|---|---|
| アプリケーションタイプ | Web サイトまたは Web サービス | Web サイトまたは Web サービス |
| WebInspect DAST | ○ | ○ |
| 認証 | ○ | ○ |
| セキュリティエキスパートによるレビュー (誤検出の除外を含む) | ○ | ○ |
| アクティブIAST | オプション | オプション |
| 手動脆弱性テスト | × | ○ |

## Fortify on Demand が提供する完全な動的スキャンソリューション

Fortify on Demand は、完全なソフトウェアセキュリティ保証を提供する、お客様のサービスパートナーとしてのアプリケーションセキュリティです。当社の動的評価は従来の DAST を超えるものです。今日の脅威の状況では、ビジネスを確実に保護する多角的なアプローチが必要なのは確かです。以下のすべてに対応しているのは、Fortify on Demand だけです。

- WebInspect を活用した包括的な動的アプリケーションセキュリティテスト
- 150 人以上のアプリケーションセキュリティエキスパートから成るグローバルチームによる広範なスキャン結果の手動レビュー
- アクティブ IAST などの最先端テクノロジー

## さあ始めましょう

Fortify は、業界をリードするセキュリティ調査に基づいた非常に包括的な静的および動的アプリケーションセキュリティテストテクノロジーを提供します。

詳細情報はこちら：
**www.microfocus.com/ja-jp/cyberres/application-security/fortify-on-demand**

お問い合わせ先：CyberRes.com
この記事はいかがでしたか？シェアはこちら

**マイクロフォーカスエンタープライズ株式会社**
jp-info-enterprise@microfocus.com
**www.microfocus-enterprise.co.jp**



CyberRes
A Micro Focus Line of Business