プレスリリース　奈良先端大　大阪大学 THE UNIVERSITY OF OSAKA　九州大学 KYUSHU UNIVERSITY

2026 年 7 月 28 日

報道関係者各位

国立大学法人　奈良先端科学技術大学院大学
国立大学法人　大阪大学
国立大学法人　九州大学

100 万件超のファジング実行ログを分析し ソフトウェアのバグ検出実態を解明 ～継続的ファジングの効果を実証、より安全な オープンソースソフトウェア開発へ指針を提示～

【概要】

奈良先端科学技術大学院大学（学長：塩﨑　一裕）の白井 達也さん（博士後期課程）、柏 祐太郎准教授、飯田 元教授と、大阪大学（総長：熊ノ郷　淳）大学院情報科学研究科の Olivier Nourry 助教（コンピュータサイエンス専攻）、奈良女子大学（学長：高田　将志）の藤原 賢二講師、九州大学（総長：石橋　達朗）の亀井 靖高教授らの研究グループは、Google が運用するオープンソースソフトウェア（以下、OSS）向け継続的ファジング（注 1）サービス「OSS-Fuzz」（注 2）から収集した約 112 万件のファジングセッションを分析し、継続的ファジングがソフトウェアのバグ発見にどのように寄与するかを定量的に明らかにしました。

研究グループは、OSS-Fuzz に参加する 878 の OSS プロジェクトを対象に、ファジングの実行履歴、検出されたバグ、コードカバレッジ（コード網羅率）（注 3）の変化を解析しました。その結果、(1) 約 36%のプロジェクトが導入直後の初回セッションでバグを検出していること、(2) コードカバレッジが継続的ファジングの実施とともに増加し続けること、(3) コードカバレッジの変動がバグ検出と強く関連していること、(4) 開発者が提供するシードコーパス（初期入力データ）（注 4）が長期的なバグ検出に寄与すること、を見出しました。

本成果は、現代社会の基盤となっている OSS の開発者がいつ、どのようにファジングを導入・運用すべきかについて、データに基づく具体的な指針を提供するものであり、より安全な OSS 開発・サイバーセキュリティ強化への貢献が期待されます。

本研究成果は、ソフトウェア工学分野で国際的影響力の高い学術誌 IEEE Transactions on Software Engineering に 2026 年 4 月 13 日(月)に公開されました(DOI:10.1109/TSE.2026.3683879)。

【背景と目的】

ソフトウェアの脆弱性を悪用したサイバー攻撃は社会に深刻な影響を与えており、安全なソフトウェア開発の重要性が高まっています。特に、商用ソフトウェアの 97%以上が何らかの形で OSS を利用していると報告されており、OSS のセキュリティ確保は社会全体の安全性に直結する課題となっています。

ファジングは、プログラムに想定外の入力を大量に与えて異常動作を誘発することで、バグや脆弱性を発見する代表的な手法です。近年では、ファジングを継続的インテグレーション（CI）の枠組みに組み込み、短いサイクルで繰り返し実行する「継続的ファジング」が広く普及しつつあります。Google が運営する OSS-Fuzz は世界中の主要な OSS プロジェクトに対してこのサービスを提供しており、これまでに 1 万 3 千件以上の脆弱性、5 万件以上のバグの修正に貢献してきました。

しかしながら、継続的ファジングがいつ、どのような頻度でバグを発見するのか、長期間運用した場合にどの程度の効果が得られるのかといった点については、定量的な知見がほとんど得られていませんでした。本研究は、OSS-Fuzz の大規模な実行ログを活用して、継続的ファジングの実態を実証的に明らかにすることを目的としました。

【研究の内容】

研究グループは、OSS-Fuzz に参加する 878 の OSS プロジェクトを対象に、約 112 万件のファジングセッションのログ、不具合報告（イシューレポート）、コードカバレッジレポートを収集し、以下の 4 つの観点から分析を行いました。

(1) ファジングバグが検出されるタイミング

分析の結果、約 36%のプロジェクトでは継続的ファジングを導入した初回のセッションでバグが検出され、2 回目のセッションでも約 20%のプロジェクトで新たなバグが検出されました。これは、多くのバグが OSS-Fuzz 導入以前から既にコード中に潜んでいたことを示しています。バグの検出率は最初の 25 セッションまでは 5%以上を維持しましたが、26 回目以降は中央値で約 2.19%程度に落ち着きました（図 1）。

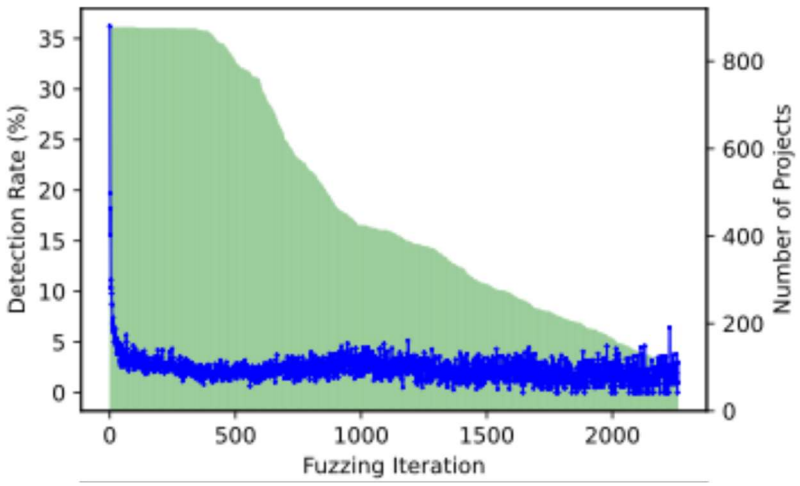

図 1：ファジングセッション中にバグを検出したプロジェクトの割合

(2) コードカバレッジの推移
　継続的ファジングの実行回数とコードカバレッジとの間には強い正の相関（スピアマンの順位相関係数 $\rho \fallingdotseq 0.96$）が確認され、ファジングを継続することでテストの到達範囲が継続的に拡大していくことが定量的に示されました。

(3) カバレッジ変動とバグ検出の関係
　コードカバレッジに変動（増加または減少）が生じた直後にバグが多く検出される傾向が確認されました。これは、コード変更によって新たに到達可能となった処理経路や、テスト対象の変化に伴って顕在化するバグが存在することを示しています。

(4) 開発者が提供するシードコーパスの長期的効果
　開発者がシードコーパスを指定したプロジェクトでは、指定していないプロジェクトに比べてバグ検出率の中央値が約 2.4 倍（約 3.15% 対 約 1.29%）に達し、シードコーパスの整備が継続的ファジングの性能向上に有効であることが示されました。

　これらの結果は、継続的ファジングが導入直後から長期運用にいたるまで、一貫して脆弱性検出に寄与していることを大規模データで初めて実証したものです。

【今後の展開】
　本研究で得られた知見は、OSS 開発者および CI/CD インフラ提供者がファジング戦略を設計するうえで重要な指針となります。具体的には、(1) ファジングは開発の早い段階で導入するほど効果が高い、(2) 導入直後の 25 セッション程度までは特に多くの計算資源を割り当てる価値がある、(3) 大きなコード変更が発生したタイミングでは、カバレッジが一時的に低下する場合でもファジングを実行する意義がある、(4) 開発者は早期からシードコーパスを整備することで、長期的にバグ検出効率を高められる、といった実践的な提言につながります。

　研究グループは今後、コード変更の内容に応じた動的なファジング戦略の設計や、機械学習を活用したバグ予測技術の開発に取り組む予定です。また、OSS-Fuzz で検出されたバグの修正履歴を解析することで、開発者の脆弱性対応プロセスの改善にも貢献していきます。これらの研究を通じて、OSS エコシステム全体のセキュリティ向上と、安全な情報社会の実現に貢献することを目指します。

【謝辞】
　本研究は、JSPS 科研費（JP24K02921、JP24K02923、JP25K21359）、JST 戦略的創造研究推進事業 さきがけ（JPMJPR22P3）、JST ASPIRE 事業（JPMJAP2415）、JST AIP 加速研究（JPMJCR25U7）の支援を受けて実施されました。

【用語解説】
注 1 ファジング（fuzzing）：プログラムに対してランダムまたは半ランダムに生成した入力を大量に与え、異常動作（クラッシュ、メモリエラーなど）を引き起こすことでバグや脆弱性を発見するソフ

トウェアテスト手法。「継続的ファジング」とは、このファジングを継続的インテグレーション（CI）の枠組みに組み込み、コード変更のたびに短いサイクルで繰り返し実行する運用形態を指す。

注 2 OSS-Fuzz：Google が提供するオープンソースソフトウェア向けの継続的ファジングサービス。1,000 以上のプロジェクトが利用しており、これまでに 1 万 3 千件以上の脆弱性および 5 万件以上のバグの発見・修正に貢献している。

注 3 コードカバレッジ（コード網羅率）：テストによって実行されたソースコードの割合。一般的に、カバレッジが高いほどテストの網羅性が高いとされ、ファジングの効果を測定する指標として広く用いられる。

注 4 シードコーパス（初期入力データ）：ファジングを開始する際に、開発者が事前に用意するテスト入力値の集合。プログラムが期待する形式の入力例を含むことで、ランダム生成だけでは到達しにくいコード領域へファジングを誘導する役割を果たす。

【掲載論文】
タイトル：Large-Scale Empirical Analysis of Continuous Fuzzing: Insights from 1 Million Fuzzing Sessions
著者：Tatsuya Shirai, Olivier Nourry, Yutaro Kashiwa, Kenji Fujiwara, Yasutaka Kamei, Hajimu Iida
掲載誌：IEEE Transactions on Software Engineering
DOI：10.1109/TSE.2026.3683879

【お問い合わせ先】
<研究に関すること>
奈良先端科学技術大学院大学 先端科学技術研究科 情報科学領域 ソフトウェア設計学研究室
准教授 柏 祐太郎
TEL：0743-72-5972
E-mail：yutaro.kashiwa@is.naist.jp
研究室紹介ホームページ：https://sdlab.naist.jp/

大阪大学 大学院情報科学研究科 コンピュータサイエンス専攻 ソフトウェア工学講座
助教 OLIVIER NOURRY
E-mail：nourry@ist.osaka-u.ac.jp
研究室紹介ホームページ：https://sel.ist.osaka-u.ac.jp/index.html.ja

九州大学 大学院システム情報科学研究院
教授 亀井 靖高
TEL：092-802-3728
E-mail：kamei@ait.kyushu-u.ac.jp

＜報道に関すること＞
奈良先端科学技術大学院大学 企画総務課 渉外企画係
TEL：0743-72-5112　FAX：0743-72-5011
E-mail：s-kikaku@ad.naist.jp

大阪大学 大学院情報科学研究科 研究戦略企画室
TEL：06-6105-5907
E-mail：ura-press@ist.osaka-u.ac.jp

九州大学 広報課
TEL：092-802-2130 FAX：092-802-2139
E-mail：koho@jimu.kyushu-u.ac.jp