つなごう。驚きを。幸せを。

2026 年 2 月 24 日

NTT 株式会社
NTT ドコモビジネス株式会社

ソフトウェア開発プロセスのセキュリティ実践を妨げる要因を大規模コード分析と開発者調査により解明

～開発者の「認知不足・負担・誤解」を特定し、AI／自動化時代のセキュアな開発プロセスを加速～

発表のポイント：

- ◆ 大規模なソフトウェアリポジトリ分析※1 により、ソフトウェア開発における開発・公開・更新を自動化する仕組み（CI/CD、継続的インテグレーション／継続的デリバリー）におけるセキュリティ対策が、実運用でどの程度実践されているかを明らかにしました。
- ◆ 開発者へのアンケート調査によって、上記のセキュリティ対策が実践されない背景にある認知不足、運用上の負担、および誤解といった人的要因を明らかにしました。
- ◆ これらの知見を活用することで、CI/CD におけるセキュリティ対策の実効性を高め、開発現場への定着を促進するとともに、より安全なソフトウェア開発の推進が期待できます。

NTT 株式会社(以下 NTT)と NTT ドコモビジネス株式会社(旧 NTT コミュニケーションズ株式会社、以下 NTT ドコモビジネス)は、早稲田大学と、CI/CD 基盤として広く利用されている「GitHub Actions※2」を対象に、公式に推奨されているセキュリティ対策の実施状況と、その実践を妨げる要因について調査を実施しました(以下 本研究)。約 34 万件の公開リポジトリに対する大規模分析と 100 名以上の開発者へのアンケート調査を組み合わせることで、「GitHub Actions」の 5 種類の主要なセキュリティ対策の実施率が平均 17.5%（最小 0.6%～最大 52.9%）と低水準にとどまっている実態を定量的に明らかにするとともに、その背景として、対策に対する認知不足や適用対象に関する誤解、運用負担への懸念といった人的要因が実践を妨げていることを示しました(以下 本成果)。本成果を踏まえ、CI/CD を活用して開発・提供するサービス全体のセキュリティ強化を推進し、お客さまが安心して利用できるサービス提供につなげていきます。

なお、本成果は、2026 年 2 月に米国サンディエゴで開催されるサイバーセキュリティ分野のトップ国際会議の一つである「Network and Distributed System Security Symposium※3 2026（NDSS 2026）」に採択されました。

1. 背景

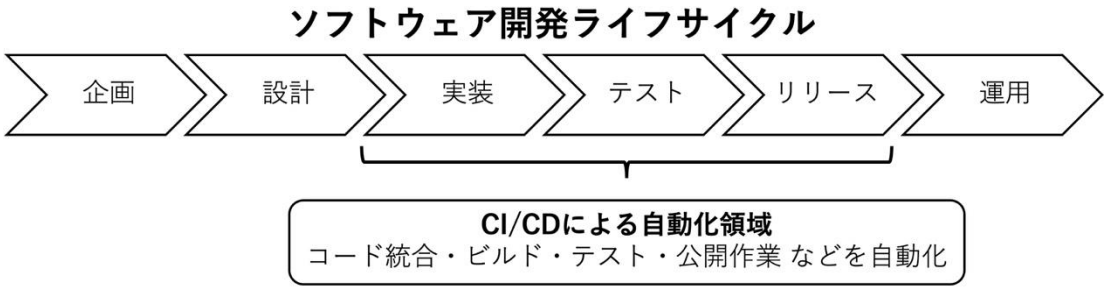
近年、ソフトウェア開発の効率化を目的として、CI/CD が広く普及しています。CI/CD は、ソフトウェア開発ライフサイクルにおけるプログラムのテストや公開作業などの各種プロセスを自動化する仕組みであり、開発の迅速化や人的ミスの削減、品質の安定化などに貢献しています。現在では多くの企業の開発者が、ソフトウェア開発の基盤技術として日常的に利用しています※4。

なかでも「GitHub Actions」は、世界最大級のソフトウェア開発プラットフォームである「GitHub※5」上で利用できる CI/CD サービスであり、個人開発者から企業の大規模開発まで、幅広い開発現場で利用されています。

一方で、CI/CD 環境はソフトウェアの配布や更新を自動で行う仕組みであるため、認証情報の管理不備や、設定変更時のレビュー不足などの運用上の問題があると、不正なプログラムの混入など、ソフトウェアサプライチェーン全体に影響をおよぼす重大なセキュリティインシデントにつながるリスクがあります。実際に、2020 年にはソフトウェアの更新プロセスが悪用され、最大約 18,000 の組織が影響を受ける可能性のある大規模なサプライチェーン攻撃が発生し、政府機関や民間企業で実際の侵害が確認されました。

また、2025 年には、「GitHub Actions」上で多くの開発者が利用していた開発作業を自動化する共通プログラムが不正に書き換えられ、開発時に利用される認証情報が外部に漏えいする事案も報告されています。

「GitHub Actions」では、こうしたリスクを低減するためのセキュリティ対策や推奨設定が示されていますが、実際の開発現場でそれらがどの程度実践されているのか、また実践を妨げている要因については、これまで十分に明らかにされていませんでした。



<図１：ソフトウェア開発サイクルにおける CI/CD による自動化領域>

2. 本研究の概要

本研究では、「GitHub Actions」を利用する公開ソフトウェアリポジトリおよび開発者を対象とした調査を実施しました。

本研究のポイントは 2 点あります。

① 実際の CI/CD 設定を対象とした大規模データ分析

「GitHub Actions」を利用するリポジトリのうち、一定程度正常に「GitHub Action」を利用していると判断できる※6すべてのリポジトリ(約 34 万件)を対象に、CI/CD の設定ファイルを自動的に

分析しました。実際の開発現場で、セキュリティ対策がどの程度適切に設定されているかを、幅広く数値で明らかにしています。

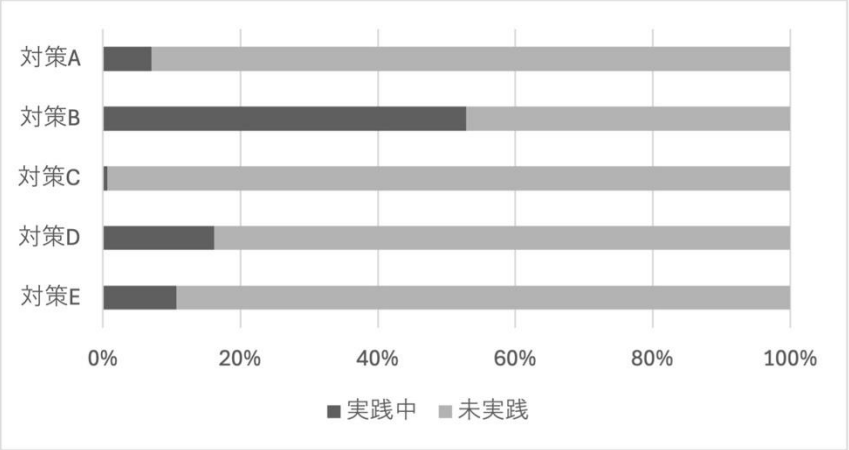
② 過去最大規模の開発者アンケートで実態と要因を解明

「GitHub Actions」を利用する開発者 102 名に対してアンケート調査を実施し、セキュリティ対策を実践していない理由や、その判断に至る背景を分析しました。従来の開発者など実務者に対する研究（回答者数 80～90 人規模）を上回る過去最大規模であり、人とシステムの関係性を研究するヒューマンコンピュータインタラクション分野で、学術的に確立された調査手法に基づいて設計されています。

3．本研究の成果

本調査から、「GitHub Actions」の 5 種類の主要なセキュリティ対策は、実施率が平均 17.5%（最小 0.6%～最大 52.9%）と全体的に低い水準にとどまっていることが分かりました。特に、専用のツールや機能を活用する対策については、十分に活用されていない実態が確認されました。また、開発者調査の結果、セキュリティ対策が実践されない主な要因として、対策の存在が十分に認知されていないことおよび運用の手間が増えるという負担感が挙げられました。加えて、「自身の開発には関係ない」といった誤解も一部で確認されました。

これらの知見は、CI/CD セキュリティの向上にはガイドラインの提示だけでは不十分であり、開発者の理解や負担感を考慮した技術的な支援や開発の仕組みが不可欠であることを示しています。本研究で得られた結果は、開発者への適切な通知設計、プラットフォームや IDE※7 による支援強化など、セキュリティ対策の実効性を高めるための具体的な施策検討に活用可能です。



<図 2 ：GitHub Actions におけるセキュリティ対策※8の実践状況>

さらに本研究では、得られた分析結果と改善に向けた示唆を、GitHub 社に共有しました。CI/CD エコシステム全体の安全性向上に資する知見としてこのようなフィードバックを行うことで、プラットフォームレベルでのセキュリティ改善にも貢献しました。

4．各社の役割

・NTT：開発者アンケート調査における分析手法の設計、および大規模分析・開発者調査の結果にもとづく改善方策・提言の検討。

・NTT ドコモビジネス：「GitHub」上の大規模リポジトリ分析における分析手法の設計および調査、ならびに開発者アンケート調査の実施。
・早稲田大学：開発者アンケート調査、および大規模リポジトリ分析に関するアドバイス。

5．今後の展開

NTT は、NTT ドコモビジネスと連携し、これらの取り組みを NTT グループ全体に展開することで、グループ横断のセキュリティ基盤の高度化を推進します。

NTT ドコモビジネスは、本研究で得られた知見をもとに、CI/CD 環境を活用して開発・提供するサービス全体のセキュリティ強化を推進します。開発プロセスへのセキュリティ対策の組み込みを通じて、セキュリティ・バイ・デザイン※9 に基づくサービス開発を強化します。加えて、自社が提供する CI/CD プラットフォーム「Qmonus Value Stream※10」においても、本研究成果を今後の改善に活用することを検討します。これにより、お客さまが安心・安全に利用できる信頼性の高いサービス提供につなげていきます。

【論文情報】

・Yusuke Kubo, Fumihiro Kanei, Mitsuaki Akiyama, Takuro Wakai, Tatsuya Mori, "Action Required: A Mixed-Methods Study of Security Practices in GitHub Actions," NDSS 2026.

【用語解説】

※1：「ソフトウェアリポジトリ分析」とは、インターネット上で公開されているソフトウェアの保管場所(リポジトリ)に含まれる開発データや設定ファイルを収集・解析し、開発の実態やセキュリティ対策の実施状況などを明らかにする分析をさします。

※2：「GitHub Actions」とは、GitHub が提供する CI/CD（継続的インテグレーション／継続的デリバリー）サービスです。ソフトウェアのテスト、ビルド、公開、更新といった作業をあらかじめ定義した手順に基づいて自動実行することができ、ソフトウェア開発の効率化や人的ミスの削減に広く利用されています。

※3：Network and Distributed System Security Symposium(NDSS)とは、USENIX Security、IEEE Security and Privacy（S&P）、ACM CCS と並び、同分野で特に評価の高い主要な国際会議の一つとして位置づけられています。投稿論文のうち厳格な専門家による査読を通過したもののみが採択されます。

※4：Continuous Delivery Foundation（CD Foundation）および SlashData™が公開した「State of CI/CD Report 2024：The Evolution of Software Delivery Performance」によると、2024 年第 1 四半期時点で、開発者の 83%が DevOps 関連の活動に携わっており、CI/CD を含む開発自動化の取り組みが広く普及していることが示されています。
出典：Continuous Delivery Foundation / SlashData™, “State of CI/CD Report 2024: The Evolution of Software Delivery Performance”, https://cd.foundation/state-of-cicd-2024/

※5：GitHub とは、世界最大級のソフトウェア開発プラットフォームであり、プログラムのソースコードをインターネット上で管理・共有・共同開発するためのサービスです。世界中の多くの開発者や企業に利用されており、ソフトウェア開発において広く普及しているプラットフォームの一つです。

※6: GitHub では、ブラウザのブックマークのように、ユーザがお気に入りのリポジトリにスターをつけることで、後にリポジトリを参照しやすくする仕組みがあります。今回はスターが 10 以上ついている、つまりブックマークしているユーザが 10 人以上いるリポジトリを調査対象としました。あまりにもスターが少ないリポジトリは、作った後そのまま放置されていたり、個人の習作のためだけに利用されたりなど、調査に適しないリポジトリを多く含むと考えられるため、対象リポジトリの選定にスター数を利用しました。

※7：IDE（Integrated Development Environment：統合開発環境）とは、プログラムの作成、編集、動作確認など、ソフトウェア開発に必要な機能を一つにまとめた開発者向けのソフトウェアです。近年では、コードの誤り検出やセキュリティ上の問題を開発段階で支援する機能も備えられています。

※8: GitHub Actions におけるセキュリティ対策とは、ソフトウェアの開発・更新を自動化する過程において、不正な変更や情報漏えいなどのリスクを低減するために GitHub が公式に推奨している代表的な対策を指します。本研究では、以下の 5 つの対策を調査対象としました。

- 対策 A. CODEOWNERS の利用 ：重要な設定ファイルや自動化処理に関するファイルの変更に対して、あらかじめ指定された担当者による確認（レビュー）を必須とする仕組み。不正または意図しない変更の混入を防ぐことを目的としています。
- 対策 B. スクリプトインジェクション対策（Mitigating Script Injection）：外部から渡される情報を安全な方法で扱うことで、自動処理の中で意図しない命令や不正な処理が実行されることを防ぐ対策。
- 対策 C. OpenSSF Scorecard の利用 ：ソフトウェア開発における設定について、セキュリティ上の観点から問題がないかを定期的に点検・評価する仕組み。
- 対策 D. 第三者製アクションのバージョン固定（Pinning Third-party Actions）：自動処理で利用する外部プログラムについて、実行される内容が意図せず変更されないよう、利用するバージョンや識別子を明確に固定する対策。
- 対策 E. Dependabot の利用：自動処理で利用している外部プログラムに更新があった場合に、安全な最新版への更新を支援する仕組み。脆弱性を含む古いバージョンの利用を防ぐことを目的としています。

※9：セキュリティ・バイ・デザイン（Security by Design）とは、システムやソフトウェアを設計・開発する初期段階から、セキュリティ対策を前提として組み込む考え方です。後から対策を追加するのではなく、設計段階で脆弱性が生じにくい構造とすることで、継続的かつ効率的に安全性を確保することを目的としています。

※10：「Qmonus Value Stream(クモナス バリュー ストリーム)」とは、NTT ドコモビジネスが提供する、アプリケーションを商用環境にリリースするまでの一連の作業(構築、試験など)をまとめて管理し、自動化する CI/CD プラットフォームです。アプリケーション開発者がビジネスロジックの開発に集中できるよう、検証済みのクラウドアーキテクチャや CI/CD パイプラインの自動化を支援し、継続的な価値提供を可能にします。