GitHub NEWS RELEASE

2024年11月20日
GitHub Japan

GitHub Secure Open Source Fundを発表
全ての人々のためにオープンソースエコシステムのセキュリティを支援

AIを活用したソフトウェア開発者プラットフォームとして世界をリードするGitHub（本社：米国サンフランシスコ）は11月19日（米国時間）、オープンソースプロジェクトのセキュリティと持続可能性を経済的にかつプログラムを通して支援するためのプログラム「GitHub Secure Open Source Fund」のパートナー募集を開始したことを発表しました。応募の受付は、2025年1月8日(水)午後4時59分（日本時間）まで随時実施します。なお、本プログラム及び資金提供は2025年初旬に開始予定です。

本プログラムでは、Alfred P. Sloan Foundation、American Express、Chainguard、HeroDevs、Kraken、Mayfield Fund、Microsoft、1Password、Shopify、Stripe、Superbloom、Vercel、Zerodhaなどの支援を受けて、GitHubが125のプロジェクトに125万ドル（約1億9千万円）を投資します。本発表を皮切りに、オープンソースセキュリティへの資金提供というGitHubのミッションに賛同するパートナーを引き続き募集します。また、純粋な経済的支援とは別に、3週間のプログラムを通じて、メンテナーにセキュリティ教育、メンターシップ、ツール導入、認定などのサポートを提供します。

本プログラムの背景
昨今、世界中で活用が進むオープンソースを管理している人々にとって、セキュリティは重要である一方、人気のあるオープンソースプロジェクトを運営する際に必要とされる作業において優先順位をつけることが難しい場合があります。さらに、最近の調査によると、組織がオープンソースに数十億ドル（数千億円規模）を投資しているものの、サイバーセキュリティ監査は重視されていません。オープンソースプロジェクトが、セキュリティ上の問題の原

因となることを懸念する一方、すべてを最新の状態に保ち、セキュリティレポートに対処し、対策を講じるには時間がかかります。業務の合間にプロジェクトを管理している場合、その時間を確保することは至難の業です。

GitHubは、メンテナー、財団、同業他社と話し合いをするなかで、支援の新しい方法を考えました。あるメンテナーにとっては、資金があればセキュリティ対策に集中する時間を確保できます。また、別のメンテナーにとっては、学ぶ機会や専門家からの支援、コミュニティのサポートが役立つこともあります。GitHub Secure Open Source Fundは、他のオープンソース資金提供者やコミュニティ主導のセキュリティ実践からの教訓を基に構築された、資金調達と連動した初のコーホートベースのプログラムです。目標は、共通の目的を持つメンテナーや資金提供者からなるセキュリティを重視するコミュニティを構築し、スケーラブルな方法でプロジェクトのセキュリティを改善することです。コミュニティは、セキュリティリスクの低減、プロジェクトのセキュリティステータスに関する可視性と洞察、一貫したレポートにより、恩恵を受けることができます。

エコシステム全体に目を向けた場合、依存関係グラフは、単にソフトウェアのつながりではなく、それ以上だと確信しています。オープンソースの成功と持続可能性を支えているのは、その基盤となる人々です。セキュリティに投資する理由は、セキュリティがグローバルなソフトウェア・エコシステムにとって極めて重要であり、多くの組織にとって、Secure by DesignやEU Cyber Resilience Actのような政策に対応し、長期的な持続可能性を確保するために不可欠であるからです。

American Expressの**Chief Technology Officer**であるヒラリー・パッカー（**Hilary Packer**）氏は、次のように述べています。「オープンソースは、私たちの開発者がイノベーションを推進し、協力し、共有することを可能にすることで、American Expressが世界最高の顧客体験を毎日提供することに役立っています。オープンソースソフトウェアのセキュリティは、当社にとって長年の優先事項です。この重要なプログラムを支援できることを誇りに思います。このプログラムは、スケーラブルな方法でセキュリティを向上させ、オープンソースのメンテナーが安全なソフトウェアを実装するためのサポートを提供します」

Zerodhaの**CTO**であるケイラシュ・ナード（**Dr. Kailash Nadh**）博士は、次のように述べています。「私たちは、非常に大きな恩恵を受けているFOSS（フリー＆オープンソースソフトウェア）エコシステムへの長年のコミットメントに基づき、GitHub Secure Open Source Fundへの支援を行っています。このプログラムは、FOSS開発者に直接資金を届けると同時に、すべての人に利益をもたらす重要なセキュリティ改善を可能にするという、非常に魅力的なWin-Winの取り組みであると考えています」

プログラムの参加資格と特典
GitHubは、セキュリティ教育、専門家との連携、コミュニティサポート、プロモーション、年2回のセキュリティ現状報告レポートを提供します。メンテナーは、セキュリティの原則、GitHub Copilot や Copilot Autofix のようなツールを実践的に学び、セキュリティの改善、セキュリティリスクの削減、ダウンストリームユーザーの信頼性向上に役立ちます。資金はすべて、**GitHub Sponsors**を通じてメンテナーに直接提供されます。現在、有効なオープンソースライセンスを持つオープンソースプロジェクトのメンテナーであり、GitHub Sponsorsがサポートするいずれかの地域在住であれば、どなたでも応募可能です。

参加者に提供される内容は、以下の通りです。

- 資金：プログラムのマイルストーンとチェックポイントに沿って、各プロジェクトにつき1万ドル（約150万円）の資金提供
- 教育：1対1の指導、ワークショップ、グループセッション、プロジェクト作業、メンターシップを組み合わせた、毎週5〜10時間参加を必要とする3週間のプログラム。プロジェクトは、プログラムマネージャー、GitHub Security Labの間で合意されたプロジェクト固有のセキュリティマイルストーンに向けた作業にも重点的に取り組む
- チェックイン：教育プログラム終了6ヶ月後と12ヶ月後のチェックポイント
- **GitHub Security**とのオフィスアワー：GitHub Security Labチームとの専用時間を設け、インシデント管理の計画とサポートのための効果的なセキュリティポリシーとベストプラクティスを確立
- 交流機会：GitHub Sponsors、資金提供者、コミュニティメンバー、GitHubリーダーとのQ&Aセッション
- 専門知識：GitHub Security Labのセキュリティ専門家への問合せ、GitHub Sponsors、資金提供者、コミュニティメンバー、GitHubリーダーとのQ&Aセッションでの知識の共有
- ツール：GitHub Copilot、Copilot Autofix、シークレットスキャンなどのツールを含む、GitHub関連製品の無償利用とトレーニング
- コミュニティ：新しいGitHub Secure Open Sourceコミュニティへのアクセス
- 終了後のサポート：GitHubから継続的なネットワーキングとサポートの機会を提供
- ポリシー教育：Secure by DesignやEU Cyber Resilience Actなどのポリシーに対応するためのプロジェクト準備
- 認定と状況報告レビュー：プログラム認証と年2回のセキュリティ状況報告レビュー

2024年のオープンソース資金調達状況について

GitHubは、開発者、パートナー、顧客のコミュニティなしには成り立ちません。GitHub Sponsorsを通じて、組織がオープンソースの依存関係に投資する際に与える影響を目の当たりにしてきました。一般的な依存関係のサポート、新しいアイディアの実現、さらにフルタイムのキャリア創出などオープンソースに投資する影響は多岐にわたります。GitHub Sponsorsによる組織向けのサポートを導入して以来、MicrosoftやStripeを含む5,800以上の組織が、GitHub上のメンテナーやプロジェクトに投資し、前年比で約40%増加しています。当プラットフォームはメンテナーがプロジェクトに費やす時間を増やすために、累計で6000万ドル（約90億円）以上の資金調達を可能にしました。

ただし、オープンソースに対する組織や企業の支援に関しては、まだ氷山の一角にすぎません。今夏、GitHubはLinux FoundationとハーバードのLaboratory for Innovation Science at Harvard (LISH)の研究者と提携し、現在のオープンソース資金調達状況についてさらに詳しく調査しました。

発表されたレポートにおいて、主な結果は、以下の通りです。

- 調査対象の組織は、オープンソースに年間17億ドル（約2,600億円）を投資していることから、オープンソースエコシステム全体で年間約77億ドル（約1兆1兆1,900億円）が投資されていると推定
- 投資の86%は、資金提供組織に勤務する従業員や契約社員による労働力のコントリビューションであり、残りの14%は直接的な経済的支援に該当
- 組織の65%は一般的に、どこにどのようにコントリビューションを行っているかを

知っているが、コントリビューションの具体的な内容については38%が明確でない
- セキュリティの取り組みはバグとメンテナンスに重点を置き、包括的なセキュリティ監査を優先事項としているのはわずか6%であった

オープンソースへのさらなる資金調達を拡大することで、全員が恩恵を受けることができます。そして、オープンソースセキュリティなどの課題にエコシステムとして取り組むことで、オープンソースの持続可能性に不可欠な資金やリソースをより多く確保できると考えています。すべてのオープンソースプロジェクトやメンテナーがセキュリティのための資金やトレーニングを利用できるわけではないからこそ、GitHubは申請可能な基金を創設しました。トレーニング、ツール導入、指導、経済的支援を受けることで、プロジェクトのセキュリティ改善に時間を費やすことができるようになり、飛躍的な進歩を遂げることが可能になります。GitHubは、エコシステムを形成する他の団体、プロジェクト、コミュニティの活動に勇気づけられています。CURIOUSS、Ecosyste.ms、ハーバード大学のLaboratory for Innovation Science at Harvard (LISH)、Mozilla Foundation、OpenJS、OpenSSF、Open Source Initiative、Open Technology Fund、Open Source Collective、Sovereign Tech Fund、Sustain OSSなどのエコシステムパートナーは、本アイデアを実現するにあたり、積極的に関与し、インプット、フィードバック、アイディアを提供しました。

Linux Foundationのリサーチ**SVP**であるヒラリー・カーター（**Hilary Carter**）氏、**Linux Foundation**の**OpenSSF**チーフアーキテクトであるクリストファー・ロビンソン（**Christopher Robinson**）氏は、次のように述べています。「GitHub Secure Open Source Fundが、重要なプロジェクトや開発者と直接関わり、彼らのソフトウェアやコミュニティのセキュリティ対策の改善を支援することで、私たちのOpenSSFコミュニティから学んだことを応用してくれることを期待しています。私たちは以前から、オープンソースを支える原動力は人々であることを理解しており、このモデルがGitHub、ハーバード大学、Linux Foundation、そしてOpenSSFコミュニティ間の研究協力を基盤としていることを嬉しく思うとともに、この取り組みがオープンソースの持続可能性とセキュリティに良い影響をもたらすことを楽しみにしています」

10億人の未来を支えるために
GitHub Secure Open Source Fundは、オープンソースを安全に確保するための取り組みの一歩です。GitHubは、GitHub Secure Open Source Fundが将来のために有益であると確信し、投資の影響をモニタリングしながら、学びを共有していきます。このような新しいプログラムが、積極的なセキュリティ文化を奨励し、また、組織がオープンソースセキュリティへの投資価値をステークホルダーへ提示することを支援し、より多様で安全なオープンソースエコシステムを構築することを願っています。そして、経済的支援、安全なオープンソースの実践の推進、専門知識の共有、安全な実践の提唱など、どのような形においても、より強固で回復力のあるオープンソースコミュニティの構築に貢献していきます。

GitHub Blog
英語:
https://github.blog/news-insights/company-news/announcing-github-secure-open-source-fund/
日本語: https://github.blog/jp/2024-11-20-announcing-github-secure-open-source-fund/

GitHubに関する情報は、こちらからもご覧いただけます。
Press Release：https://github.com/newsroom

Blog: (英語) https://github.blog (日本語) https://github.blog/jp
X: (英語) @github https://twitter.com/github
(日本語) @GitHubJapan https://twitter.com/githubjapan

【GitHub について】
GitHubは、すべての開発者のためのグローバルなホーム(家)として、安全なソフトウェアの開発、拡張、提供の実現に向け世界有数のAI搭載開発者プラットフォームです。グローバル企業の総収入ランキングトップ100の『Fortune 100』に名を連ねる90%以上の企業の開発者を含む1億人以上が、GitHubを利用し素晴らしい共同作業を行っています。GitHubが提供するあらゆるコラボレーション機能により、個人やチームはかつてないほど容易に、より速く、より良いコーディングを実現しています。また、77,000を超える組織がGitHub Copilotを導入しています。
https://github.com/about
https://github.co.jp (日本語)

【製品／サービスに関するお問い合わせ先】
ギットハブ・ジャパン営業およびサポート窓口
Email: jp-sales@github.com