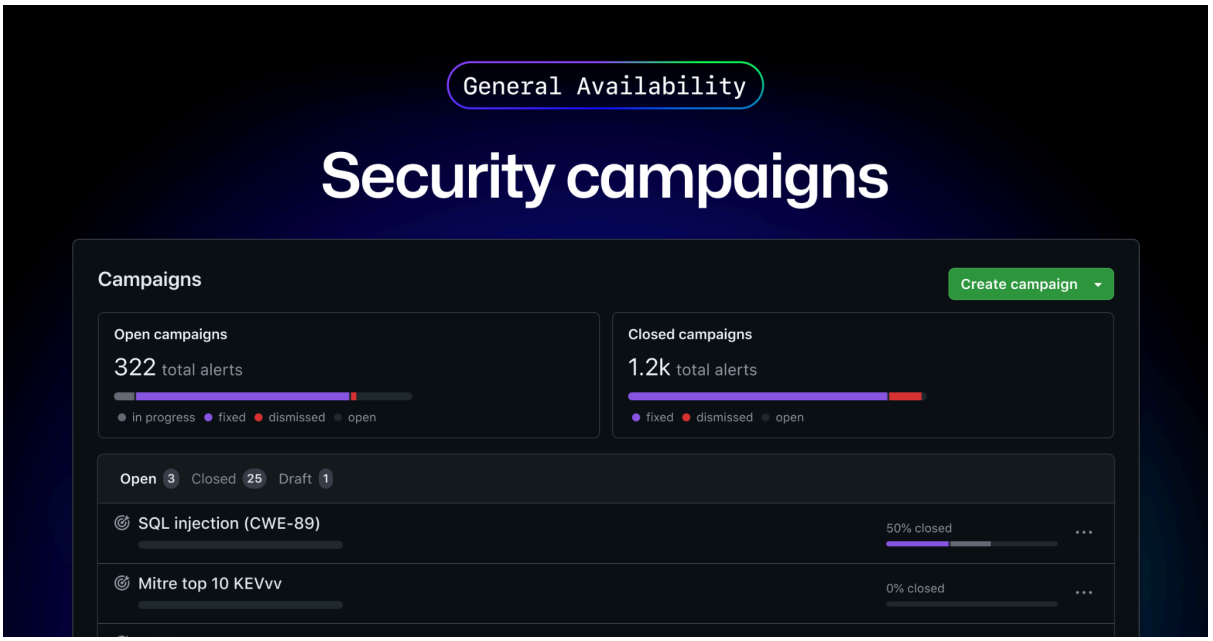
GitHub

PRESS RELEASE

2025年4月9日
GitHub Japan

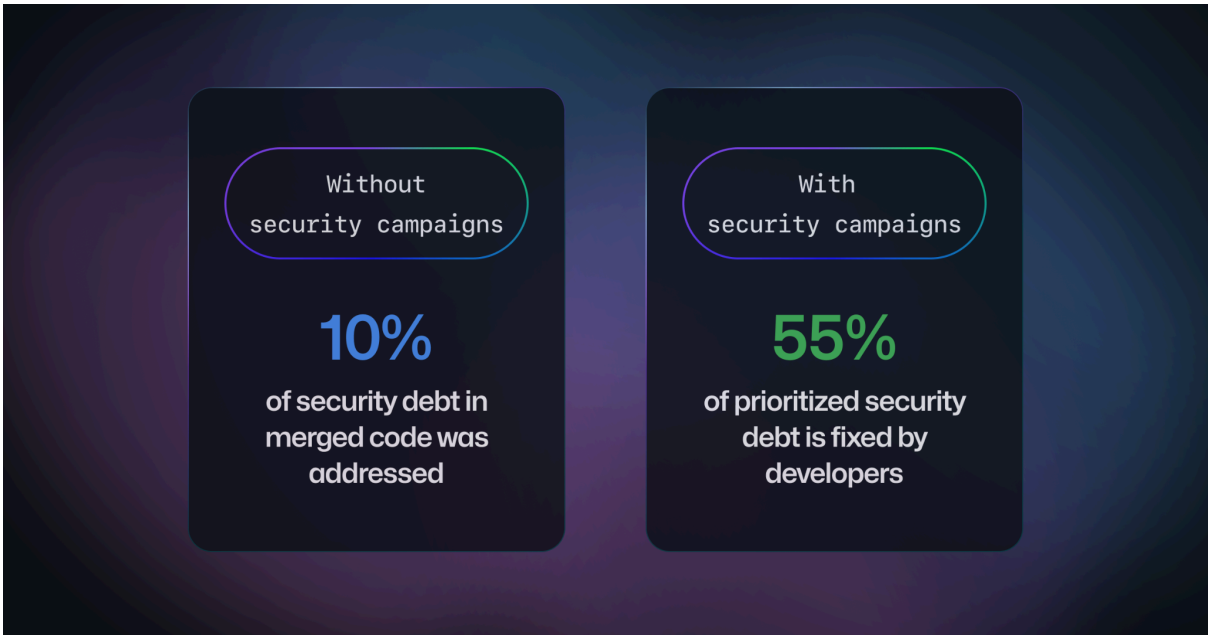
GitHub、開発者とセキュリティチームの協働でセキュリティ負債の大幅な削減を実現する「セキュリティキャンペーン」正式提供を開始

2025年4月8日（米国時間）- 米国カリフォルニア州サンフランシスコ - 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は、GitHub Advanced SecurityおよびGitHub Code Securityを利用中のすべてのユーザーに向けて、開発者とセキュリティチームの協働によってソフトウェアの脆弱性を体系的に解消する「セキュリティキャンペーン」の正式提供を開始したことを発表しました。従来の個別対応では困難だったセキュリティ負債の一元管理とリスクの優先順位付けを実現し、セキュリティ課題への解決スピードを飛躍的に向上させます。



セキュリティ負債の**90%**が未対応という現実

セキュリティアラートへの対応よりも、機能のリリースに時間を費やしたいと考える開発者が多いなか、Copilot Autofixのようなツールをプルリクエストに直接組み込むことで、セキュリティ問題の修正を最大60%高速化し、手動対応と比べて平均修復時間（MTTR）を大幅に短縮、本番環境に入る前の脆弱性検出を可能にします。結果として、バグ修正に費やす時間を抑え、コーディングに専念できる時間が増加します。



しかし、近年、ソフトウェア開発におけるセキュリティ対応の重要性は増す一方です。未対応の脆弱性は、「セキュリティ負債」として蓄積され、リスクの温床となります。GitHubのデータによれば、企業が抱えるセキュリティ負債のうち、実際に対処されているのはわずか10%であり、残る90%は優先順位が付けられず未対応のまま残されています。一方、セキュリティキャンペーンに含まれたセキュリティ負債のうち55%がすでに修正されています。

セキュリティキャンペーンは、セキュリティチームと開発者をつなぎ、脆弱性修正プロセスをワークフロー内で、かつ大規模に効率化することで、ギャップを解消します。Copilot Autofix を活用して一度に最大 1,000 件のコードスキャンアラートに対する修正案を生成し、セキュリティチームのトリアージや優先順位付けを支援します。開発者は Autofix を使用して開発のスピードを損なうことなく、迅速に問題を解決できます。

セキュリティキャンペーンの実践
昨年の「GitHub Universe」でパブリックプレビューが開始されたセキュリティキャンペーンは、セキュリティ対策のさまざまな段階にある組織で試験的に導入されました。組織全体のセキュリティ負債削減を目的とする場合や、重要なリポジトリのアラートを対象とした場合などにおいて、セキュリティキャンペーンは開発者とセキュリティチームの双方に有益性をもたらします。

Lumenの**DevSecOps**エンジニア、**Jose Antonio Moreno**氏は、次のように述べています。「セキュリティキャンペーンは、開発者の生活を簡素化してくれます。複数のリポジトリのアラートを簡単にグループ化できるため、トリアージと優先順位付けにかかる時間が短縮され、Copilot Autofixを使用して最も重要な問題を迅速に修正できます」

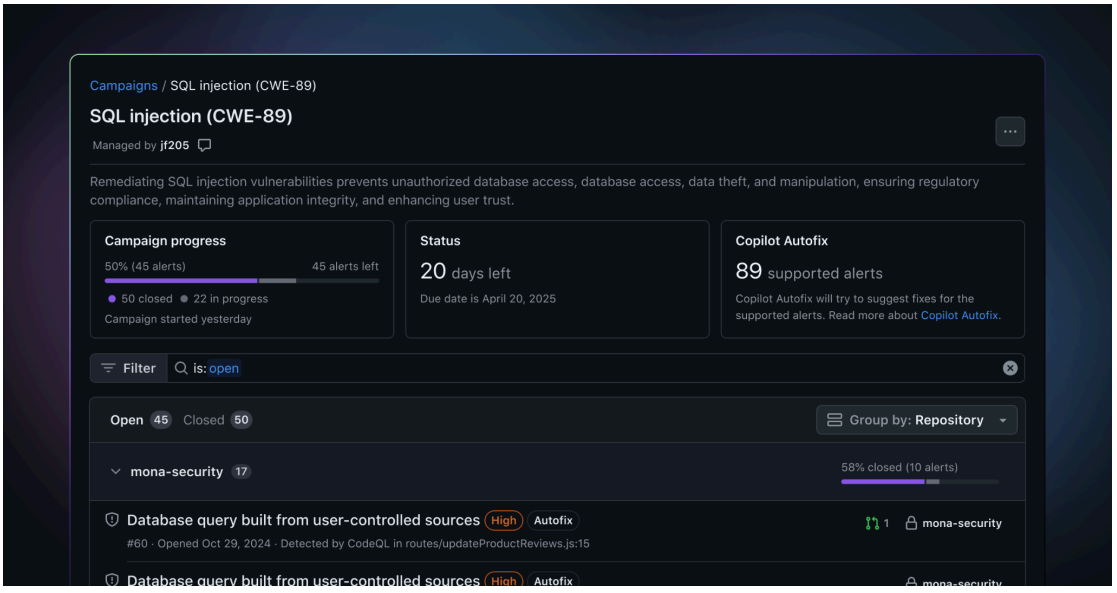
Alchemyのセキュリティエンジニア**GP**氏は、次のように述べています。「GitHubセキュリティキャンペーンは、私たちの開発チームにとって画期的なものです。既存の脆弱性について知ることができ、エンジニアが一丸となって修正に取り組めるようになり、修正にかかる時間も大幅に短縮されました」

初期の導入結果では、セキュリティキャンペーンに含まれるアラートのうち55%が修正されており、キャンペーンに含まれないアラートの10%と比較して、5.5倍の改善が確認されています。ア

ラートがキャンペーンに含まれる場合、セキュリティチームがどのアラートに取り組むべきかの優先順位をあらかじめ明示することで、開発者はセキュリティ負債の修正など対応すべき課題に、より多くの時間を費やすことができることを示しています。GitHubのデータによれば、実際、キャンペーンに含まれるアラートは、キャンペーンに含まれないアラートと比較して、開発者のエンゲージメントが約2倍に向上しています。

セキュリティキャンペーン：その仕組み
コードベースに既存するセキュリティ問題のトリアージや優先順位付けは、通常のソフトウェア開発ライフサイクルの一環として行われる必要があります。しかし、開発スピードが求められる製品チームは、セキュリティアラートの精査と対応に必要な時間を確保することが困難です。多くのソフトウェア組織には、こうしたリスクを理解し、対応できるセキュリティチームが存在します。セキュリティキャンペーンは、開発者とセキュリティチームが持つ異なる専門性を融合し、セキュリティ負債に対処するための新たな協働体制を実現します。

1. リスクの優先順位付け：セキュリティチームは、リポジトリ全体のリスクを評価し、対処すべきアラートを優先順位付けします。セキュリティキャンペーンには、キャンペーンの範囲設定を支援するために、よく使われるテーマ（MITRE Top 10 Known Exploited Vulnerabilitiesなど）をベースにしたテンプレートや、GitHub セキュリティ概要の全体的なリスク状況をまとめた統計やメトリクスが用意されています。
2. 通知と作業管理：選定されたアラートに対して、キャンペーンの影響を受ける開発者へ通知が送られます。キャンペーンで定義された作業はGitHub 上で他の機能作業と同様に計画・管理が可能です。



3. 自動修正提案：Copilot Autofixがキャンペーン内のすべてのアラートに対し、自動修正案とカスタムヘルプテキストをただちに作成開始します。アラートの修正は、差分確認後にプルリクエストを作成するだけで完了します。

セキュリティキャンペーンは単なるアラートのリストではありません。キャンペーンは、アラートを通知で補完し、開発者や開発チームが責任を持つアラートを確実に認識できるようにします。開発者とセキュリティチームとの協働を強化するために、キャンペーンには担当マネージャーが任命され、キャンペーンの進捗を監督し、開発者を支援します。セキュリティマネージャーは、GitHub 上

で組織レベルのビューを通じて、進捗の全体像を把握し、必要に応じて開発者と協力することが可能です。

セキュリティキャンペーンの正式提供に伴い、以下の新機能も利用可能となりました。

- ドラフトセキュリティキャンペーン：セキュリティマネジャーは、キャンペーンの範囲を繰り返し検討し、内容を公開前にドラフトとして保存が可能になりました。ドラフトキャンペーンを使用することで、セキュリティマネジャーは、作業が本稼働する前に、最も優先順位の高いアラートが含まれていることを事前に確認できます。
- **GitHub Issues**の自動作成：セキュリティマネジャーは、キャンペーンに含まれるアラートに対して、リポジトリごとに GitHub Issuesが自動的に作成・更新されます。チームでの進捗確認や管理、議論するために使用できます。
- 組織レベルのセキュリティキャンペーン統計：セキュリティマネジャーは、現在進行中および過去のキャンペーンに関する進捗状況を示す統計情報を集約して可視化できるようになりました。

関連資料

- セキュリティキャンペーンは、GitHub Advanced Security または GitHub Code Security を利用中のすべてのユーザーが利用可能です。導入方法や具体的な設定手順は、GitHub公式ドキュメントを参照ください。また、GitHub Code Security がどのように大規模なコードのセキュリティ確保に貢献するかについての詳細は、デモを参照ください。

GitHub Blog
英語：
https://github.blog/security/application-security/found-means-fixed-reduce-security-debt-at-scale-with-github-security-campaigns/
日本語：
https://github.blog/jp/2025-04-09-found-means-fixed-reduce-security-debt-at-scale-with-github-security-campaigns/

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、提供の実現に向けた世界有数の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1.5億人以上が、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

【本件に関するお問い合わせ先】
GitHub PR 事務局（PRAP Japan）
担当：板東、金
GitHub@prap.co.jp