GitHub

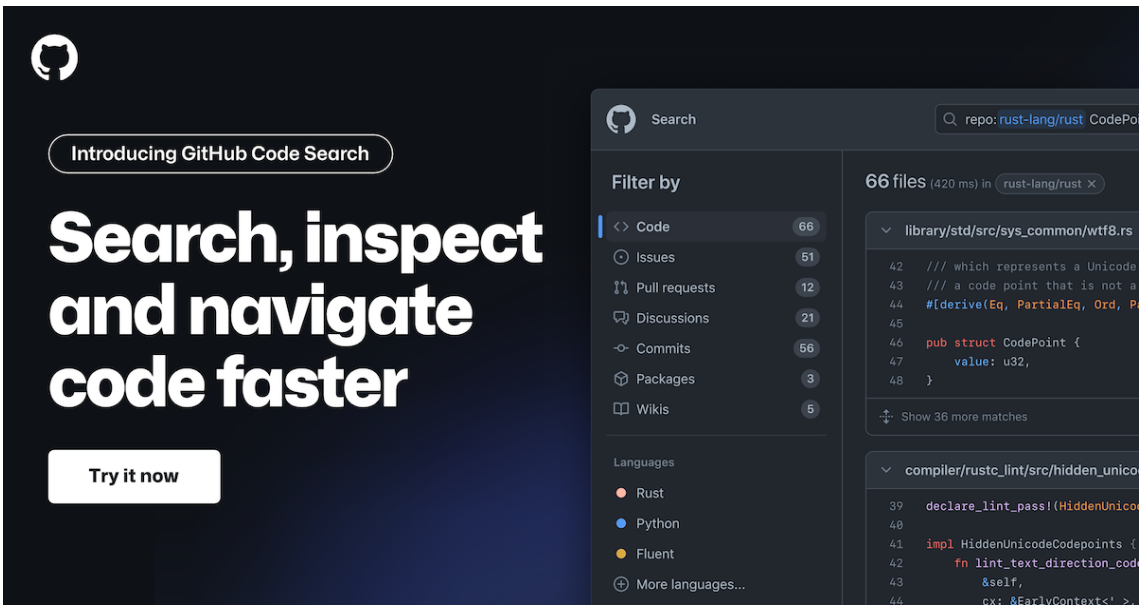
NEWS RELEASE

2023年5月17日
ギットハブ・ジャパン合同会社

GitHub、コードビューとコード検索および secret scanningプッシュ保護の一般提供(GA)を発表

オープンソースプロジェクトおよびビジネスユースを含む、ソフトウェアの開発プラットフォームを提供するGitHub, Inc.（本社：米国サンフランシスコ）は、2023年5月8日(米国時間)にコード検索とコードビューの一般提供(GA)、及び2023年5月9日(米国時間)にプッシュ保護の一般提供(GA)を開始をそれぞれ発表しました。

コード検索とコードビューの一般提供(GA)を開始



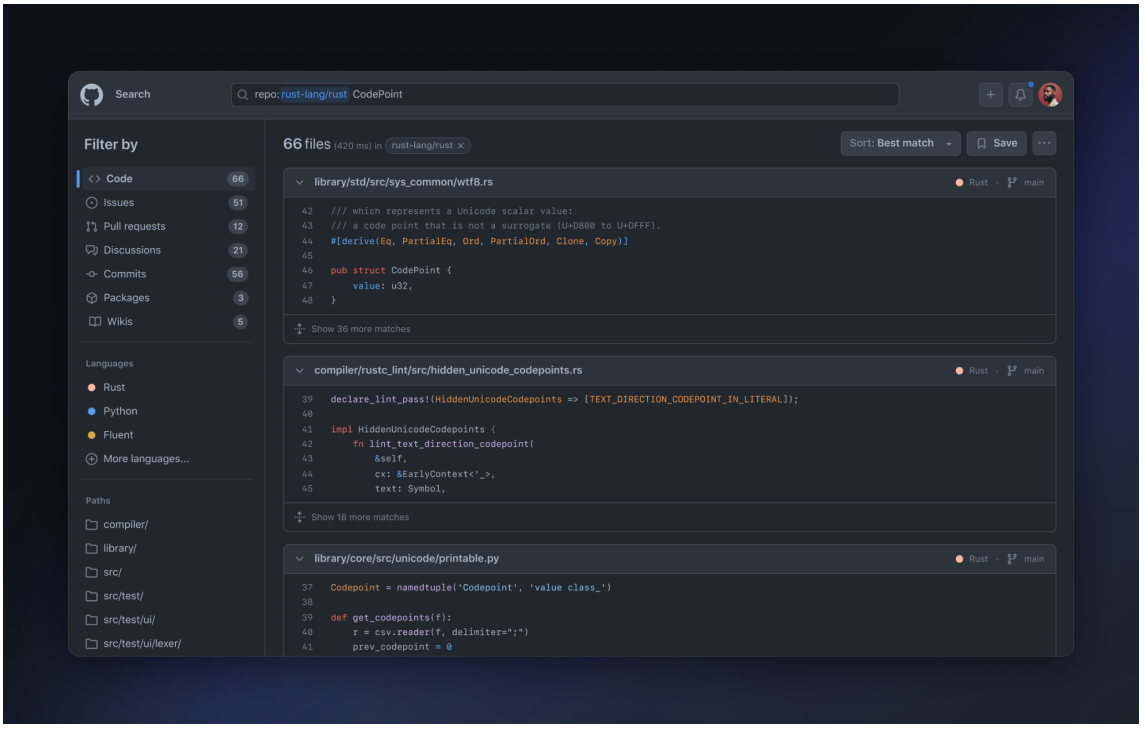
新機能の計画や実装、バグの調査、プルリクエストのレビューなど、開発者は通常、コードを書くことよりも、コードを読んで理解することに多くの時間を費やしています。

GitHubではこの2年間、コード検索の改善計画を立て、それを実現するテクノロジーを提案してきました。そして5月8日(米国時間)、GitHub.comの全ユーザを対象に、新しいコード検索とコードビューの一般提供(GA)を開始しました。

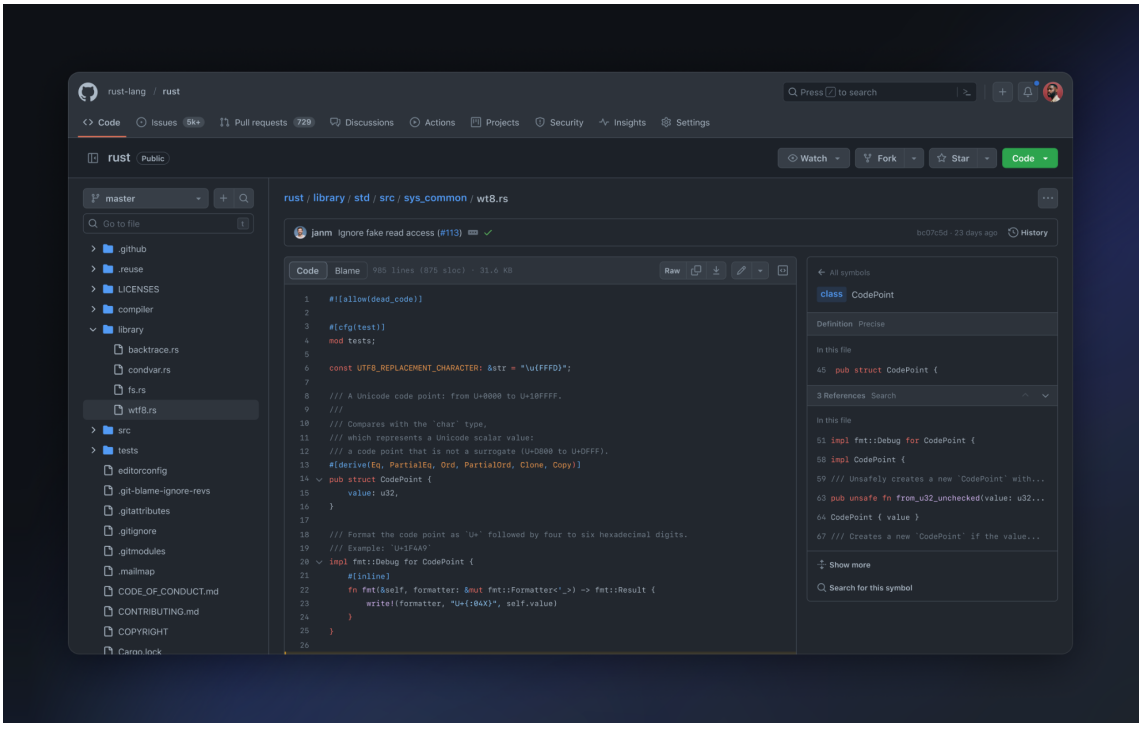
これにより、開発者がコードを迅速に検索、閲覧、理解できるようにすること、重要な情報の前後関係がわかるようにすること、そして最終的には開発者の生産性を高めることが可能となりました。実現に向けては、GitHub.comに3つの強力な新機能を導入しました。

最初に、検索インターフェイスを一新し、コードの提案や補完、結果の切り分けができるようにしました。

2つ目として、新しいコード検索エンジンを完全にゼロから構築しました。このエンジンは驚くほど高速(従来のコード検索の約2倍の速度)かつ高機能(部分文字列クエリ、正規表現、シンボル検索をサポート)で、コードを理解し、最も関連性の高い結果を優先的に提示します。



そして3つ目として、GitHubのコードビューを完全に再設計し、検索、閲覧、コードナビゲーションを緊密に統合しました。



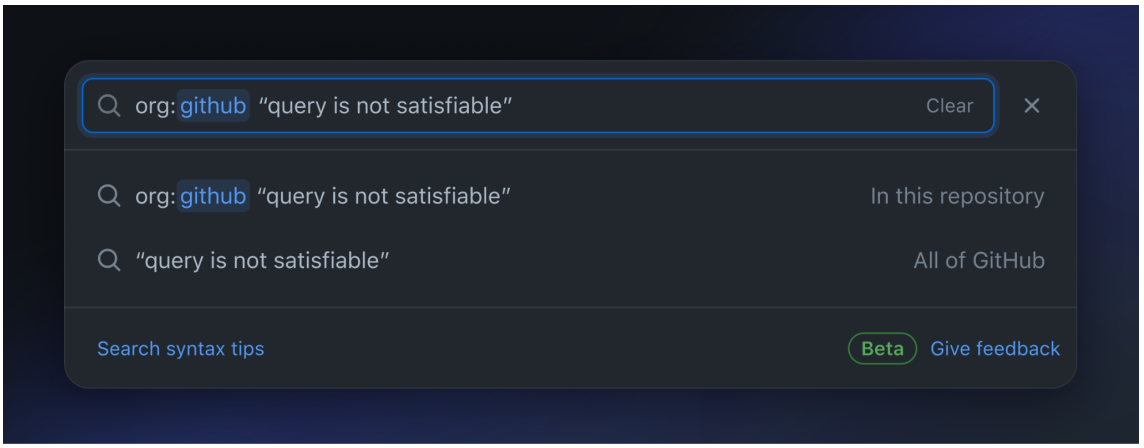
GitHub NEWS RELEASE

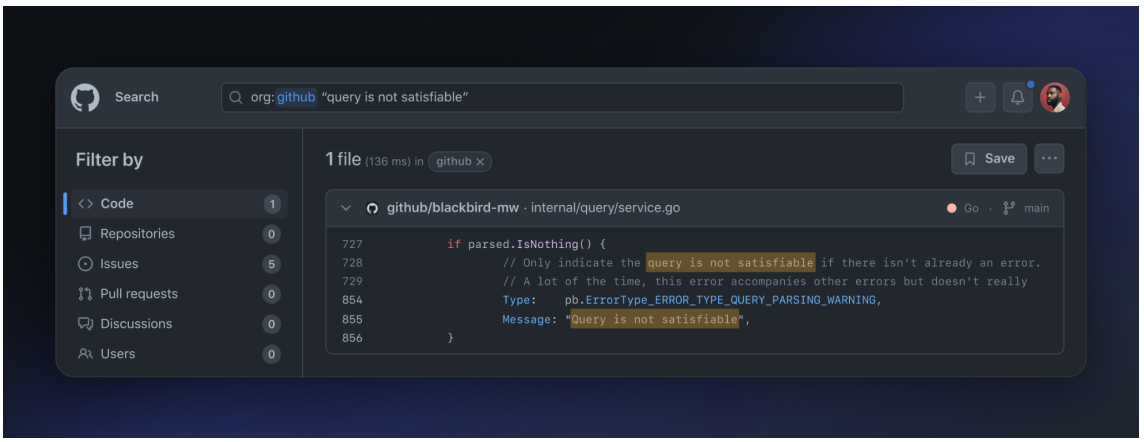
GitHubのコード検索では、世界中のコードをすぐに利用できます。実際の機能について、下記にまとめます。

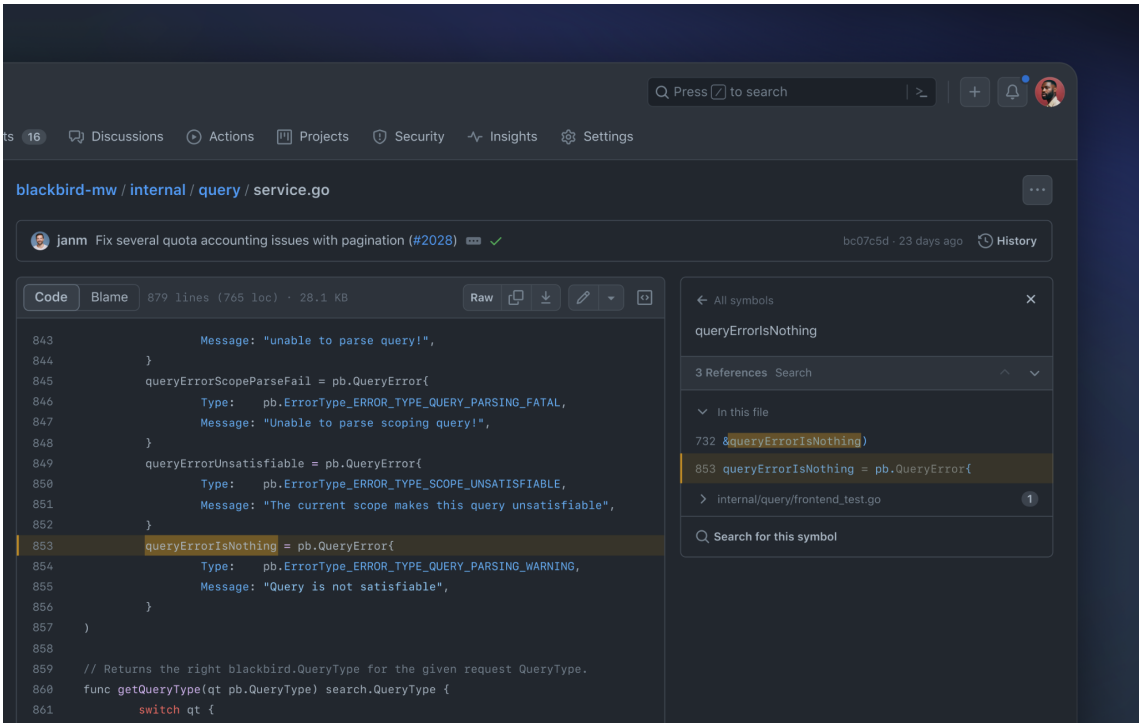
バグの修正

あるユーザーが、利用するサービスから「query is not satisfiable」というエラーメッセージが届くと訴えていると仮定します。このエラーメッセージがどのシステムで生成されたのか、どのリポジトリに存在するコードなのか不明です。

コード検索がない場合、多数のリポジトリのクローンを作成してgrepで調べたり、知識の豊富な同僚に尋ねたりする必要があるでしょう。しかし、コード検索を利用することで、組織の全コードをまとめて瞬時に検索することが可能です。







ここでは1件の結果が返されています。その結果の中に`queryErrorIsNothing`という定数があり、該当するエラー文字列が含まれています。

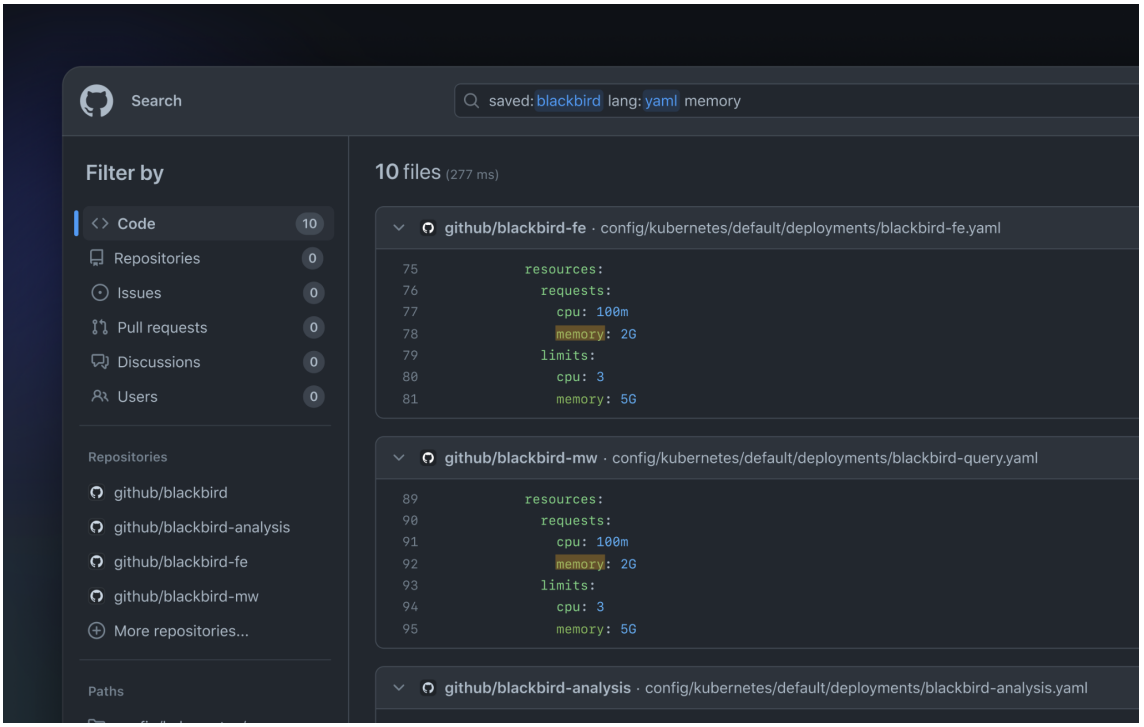
シンボルペインでは、この定数の定義と定数が使われている2つの場所を確認できます。1か所はこのファイル内、もう1か所はテスト内で使用されています。この定数が使われている場所を確認すれば、今回のエラーが生じる理由が判明します。また、テストに移動すると、この問題を引き起こすクエリの例を確認することが可能です。

これで、今回のエラーの原因を判別できただけでなく、このエラーの起動方法を示すサンプルテストも入手することができました。ここから、codespaceを起動してさらに深く掘り下げたり、Copilotを使用して別のテストを作成することも可能です。

設定の検索

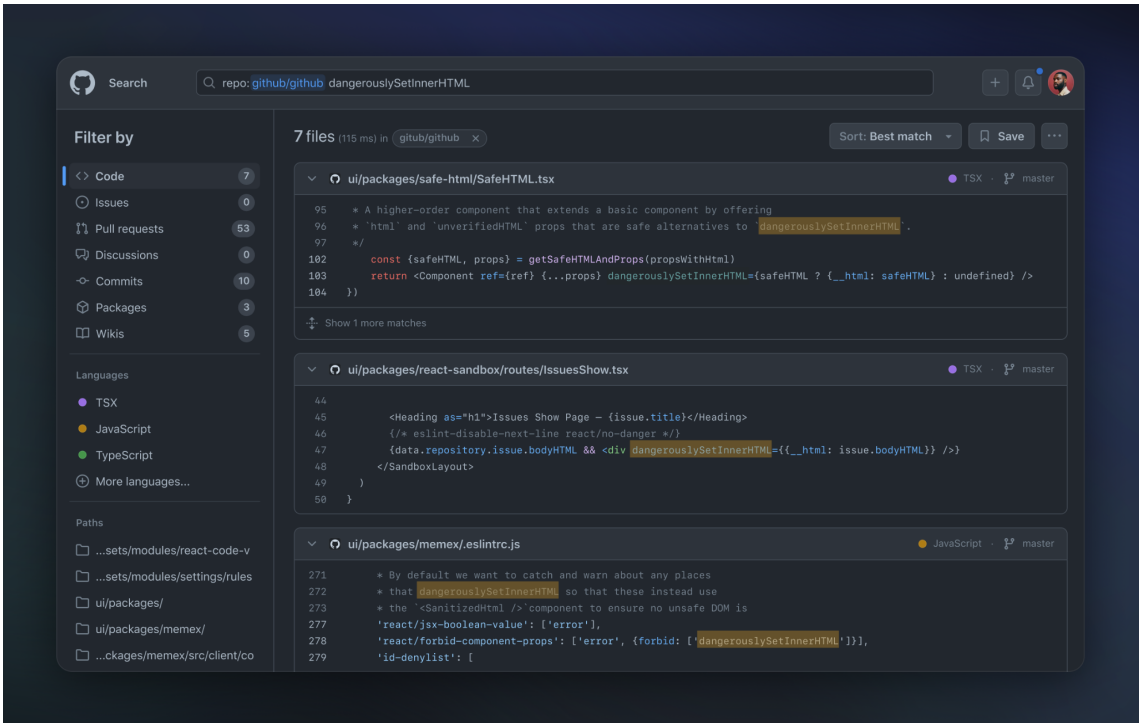
利用者の会社ではKubernetesを利用しており、インフラストラクチャチームが「クラスターのメモリーが不足している」と訴えていると仮定します。サービスがリクエストするメモリー量はどれくらいでしょうか。また、その量を減らすことは可能でしょうか。

チームのコード全体から「memory」という単語を含むYAML設定ファイルを検索すると、すぐにチームのサービスのKubernetes設定ファイルと使われているメモリー量を確認できます。この検索へのリンクをインフラストラクチャチームに直接送信し、それらのサービスに割り当てられているメモリー量について話し合いを始めることができます。



脆弱性の発見
チームでReactを利用している場合、`dangerouslySetInnerHTML`というプロパティに馴染みがあるかもしれません。このプロパティでは、文字列を使用して要素にHTMLを直接挿入可能です。しかし、その名前(dangerously)が示すとおり、システムにとって危険となる場合もあります。DOMに挿入される文字列が信頼できないものである場合、セキュリティの脆弱性が生じる可能性があります。

GitHub.com内のコードであるgithub/github全体を検索し、使用状況を確認しましょう。

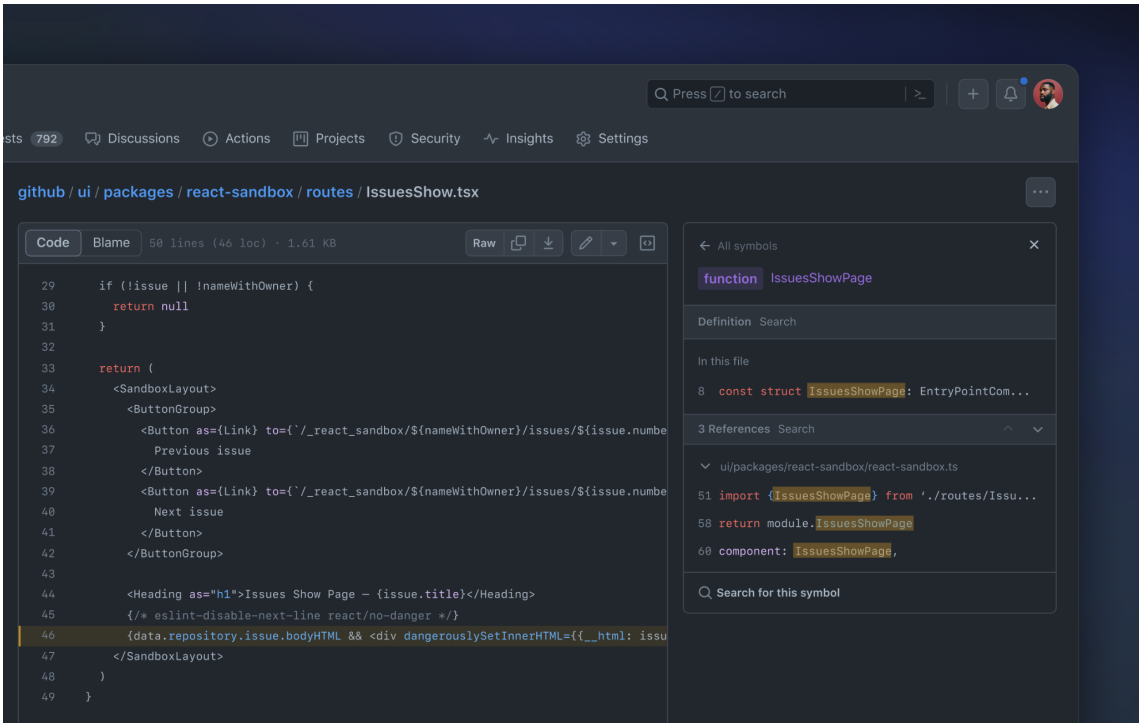


すぐにいくつかの結果を確認できます。その中には、dangerouslySetInnerHTMLの使用を禁止する文法チェッカールールも含まれています。一方、IssuesShowという脆弱性があるかもしれないコンポーネントも存在します。

コードビューでこうしたコンポーネントを表示し、シンボル名をクリックすると、その使用状況を確認することが可能です。今回の検索結果では、他の1つのファイルで使われているようです。

ここでは、このコンポーネントのレンダリングに使われる正確なルートを確認できます。このルートはサンドボックステスト環境の一部であるため、安全であると判明しました。

GitHub NEWS RELEASE



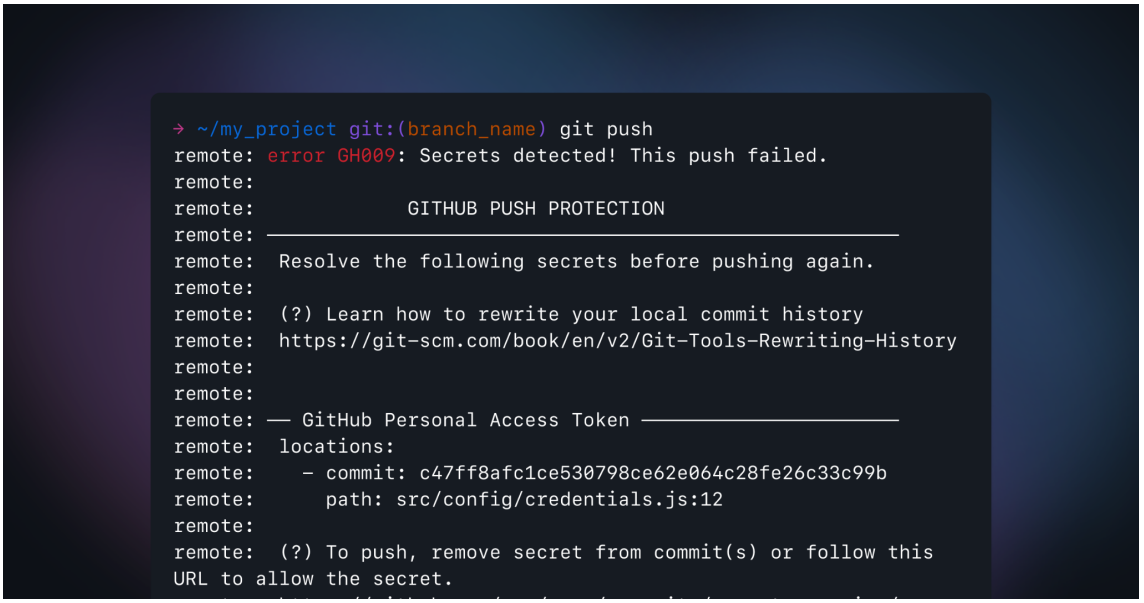
コードインテリジェンスの新時代

GitHubが新しいコード検索とコードビューを開発した目的は、開発者がコードベースに散在する重要な情報をすばやく検索できるようにすること、その情報の前後関係がわかるようにすること、そして最終的には開発者の生産性を高めることです。今後、GitHubでは、ソフトウェア開発のあらゆる側面にAIを活用したインテリジェンスを浸透させていきます。

プッシュ保護の一般提供(GA)を開始、すべてのパブリックリポジトリで無料利用が可能に

GitHubは、GitHub Advanced Security (GHAS)ライセンスを購入しているユーザーのプライベートリポジトリを対象に、プッシュ保護の一般提供(GA)を開始しました。さらに、オープンソースに携わる開発者やメンテナーが事前にコードを保護できるよう、すべてのパブリックリポジトリに対してプッシュ保護を無料で提供します。

GitHub NEWS RELEASE



GitHubは、ワークフローに直感的なセキュリティ機能を組み込み、開発者が利用できるようにすることで、共に協力して、セキュリティ対応をリアクティブなものからプロアクティブなものへと変えることができると考えています。2022年4月にGitHub Advanced Security（GHAS）のユーザ向けにシークレットスキャンのプッシュ保護機能のベータ版をリリースして以降、プッシュ保護を利用している開発者は、17,000件に及ぶ潜在的なシークレット漏えいを防止し、公開されたシークレットの無効化、入れ替え、修正にかかる時間として95,000時間以上を削減しています。

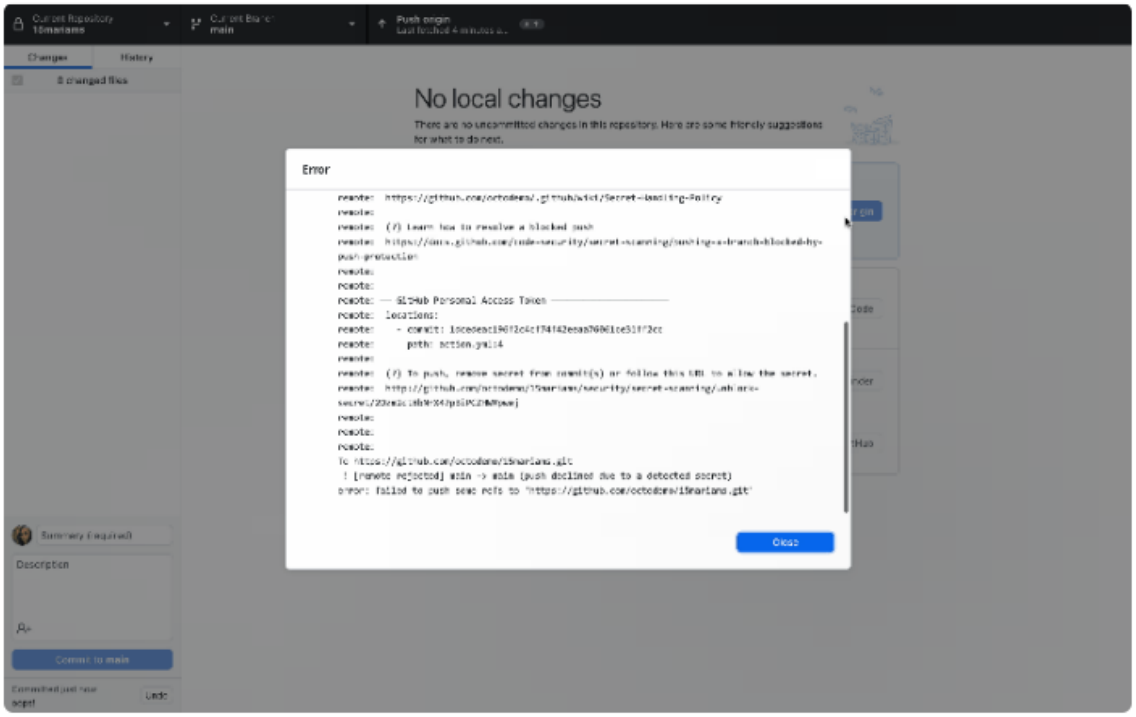
プッシュ保護は、高度に識別可能なシークレットをコミット前にスキャンすることで、開発者の利便性を損なうことなくシークレットの漏えいを防止します。GitHubでは、サービスプロバイダーと緊密に連携し、トークンの誤検出率を低く抑えることで、アラートに対する開発者の信頼を確保しています。コード内でシークレットが検出されると、開発者のIDEまたはコマンドラインインターフェイスに直接、シークレットが公開されないようにするための修正ガイダンスが表示されます。

Fidelity InvestmentsのALMツールおよびプラットフォーム担当プロダクトエリアリーダーであるGer McMahon氏は、次のように説明しています。「プッシュ保護付きのSecret Scanningを開発ワークフローに直接組み込むことで摩擦が減少し、開発者は安全かつ質の高いコードを作成できるようになりました」

プッシュ保護はどのように不協和のない開発を実現するのか

開発者が必要としているのは、信頼できるツールであり、GitHubではこのことを念頭に置いてプッシュ保護を設計しました。シークレットを含んだコミットをプッシュした場合、プッシュ保護のメッセージと合わせて、シークレットの種類、場所、公開時の修正方法に関する情報が表示されます。コミット履歴からシークレットを削除すると、コミットを再プッシュすることが可能です。プッシュ保護は誤検出率の低いシークレットのみをブロックするため、コミットがブロックされた時点で調査する必要があるとわかります。

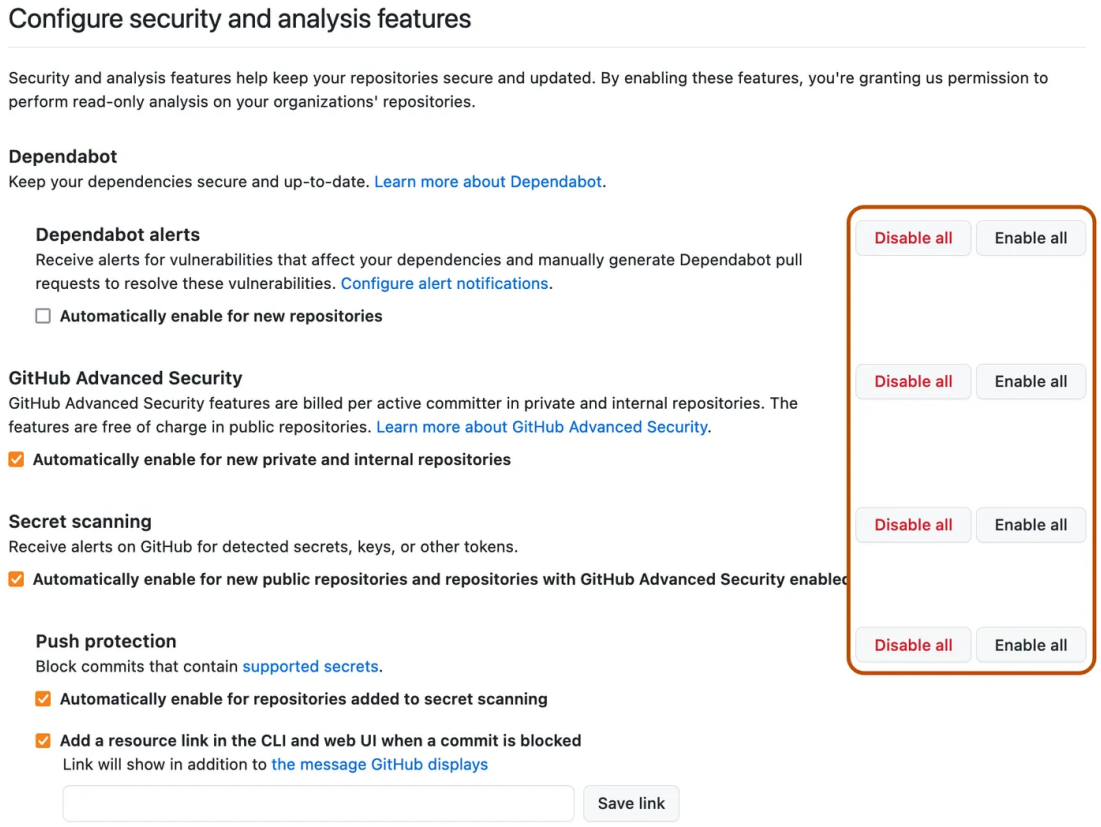
場合によっては、機能停止を迅速に解決してからシークレットに対処するなど、シークレットを含むコードをプッシュしなければならない緊急事態が生じることがあります。このような場合、「テストに使用した」「誤検出である」「後で修正する許容可能なリスクである」といった理由を提示することで、プッシュ保護をバイパスできます。リポジトリ管理者、組織の管理者、およびセキュリティ管理者はすべてのバイパスについてメールでアラートを受け取り、企業や組織の監査ログ、アラート表示画面、REST API、webhookイベントなどを通じて、任意のバイパスを監査することができます。



KPMGのディレクター兼クラウドプラクティスリードであるLeo　Stolyarov氏によると、このアプローチにより、スピードを犠牲にすることなく、セキュリティ態勢を向上させることができると言います。「シークレットスキャンのプッシュ保護は開発フローにおける不協和を生じさせない機能です。開発者体験を損なうことなく、より高いセキュリティ意識とシークレット漏えいからの保護を実現しています」

プッシュ保護の詳細と使用を開始する方法

リポジトリ、組織、企業でプッシュ保護を有効にするには、[Code　security　and　analysis(コードのセキュリティと分析)]設定に移動し、[Secret　scanning]のセクションまでスクロールします。[Enable　all(すべて有効にする)]ボタンを選択すると、[Secret　scanning]とそのサブセットのプッシュ保護を有効にすることが可能です。



プッシュ保護を自動的に有効にする、もしくは、[プッシュ保護]セクションにあるチェックボックスにチェックを付けることで、プッシュ保護メッセージに表示するカスタムリソースリンクを指定することも可能です。これにより、企業や組織で新規作成されたリポジトリにプッシュ保護が適用されるようになります。

また、GitHub Advanced Securityを利用している場合は、カスタムシークレットパターンのプッシュ保護を有効にすることで、デプロイメントをさらにカスタマイズすることもできます。

プッシュ保護、GitHub Advanced Security、secret scanningパートナープログラムの詳細については、GitHubのドキュメントをご確認ください。

GitHub Blog
英語：https://github.blog/2023-05-08-github-code-search-is-generally-available/
https://github.blog/2023-05-09-push-protection-is-generally-available-and-free-for-all-public-repositories/

日本語：
https://github.blog/jp/2023-05-16-github-code-search-is-generally-available/
https://github.blog/jp/2023-05-16-push-protection-is-generally-available-and-free-for-all-public-repositories/

GitHub NEWS RELEASE

GitHubに関する情報は、こちらからもご覧いただけます。
Blog: (英語) https://github.blog (日本語) https://github.blog/jp
Twitter: (英語) @github(https://twitter.com/github)
(日本語) @GitHubJapan(https://twitter.com/githubjapan)

【GitHub について**】https://github.co.jp**
GitHubは、すべての開発者のためのグローバルホームとして、安全なソフトウェアを構築、拡張、提供するための統合された開発者プラットフォームです。フォーチュン100社に採択された企業のうち90社に所属する開発者を含む1億人以上がGitHubを利用し、3億3千万以上のリポジトリで素晴らしいものを共に創造しています。GitHubのすべてのコラボレーション機能によって、個人やチームがより迅速に、より高品質なコードを書くことがかつてないほど容易になっています。

【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