GitHub

NEWS RELEASE

2021年4月13日
ギットハブ・ジャパン合同会社

GitHub Advanced Securityに新機能を追加

～セキュリティ概要のベータ版開始と
プライベートリポジトリ向けSecret Scanningを提供～

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、3月30日（米国時間）、セキュリティ機能群として提供するGitHub Advanced Securityに新機能が追加されたことを発表しました。

GitHub Advanced Securityは、OSSコミュニティが主導する開発者ファーストのアプローチのもと、安全なアプリケーション開発を可能にしています。今回、主に2つの機能がアップデートされました。

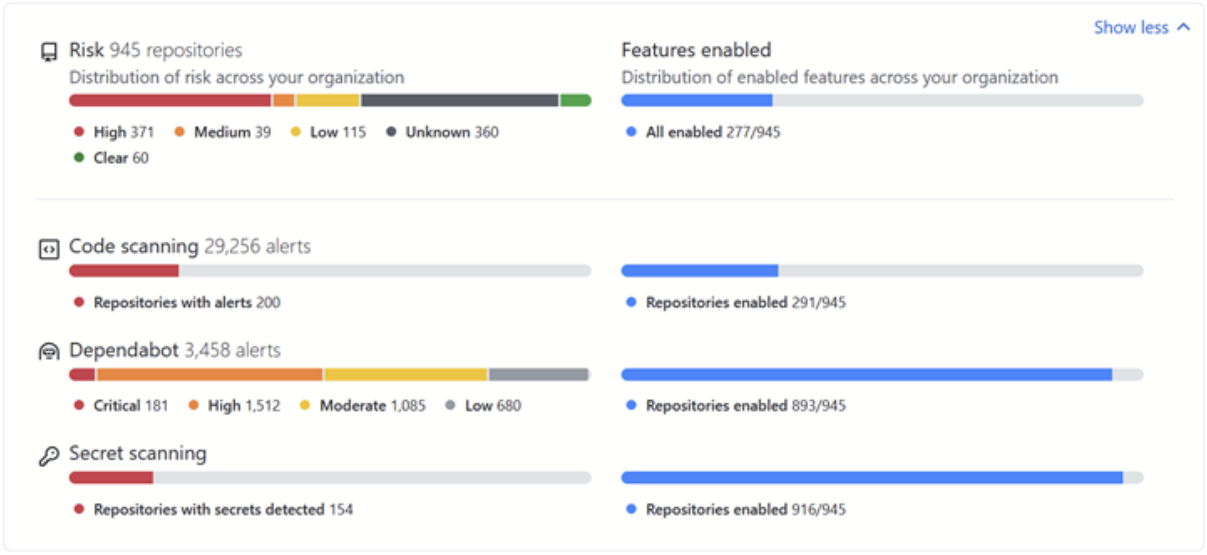
- セキュリティ概要のベータ版開始 - GitHubでホスティングしているアプリケーションがセキュリティリスクに晒されている場合、その概要を確認できるようになりました。
- プライベートリポジトリ向け**Secret Scanning**の提供を開始 - 範囲が拡大されたことでパートナーが35社以上になりました。

セキュリティ概要の導入

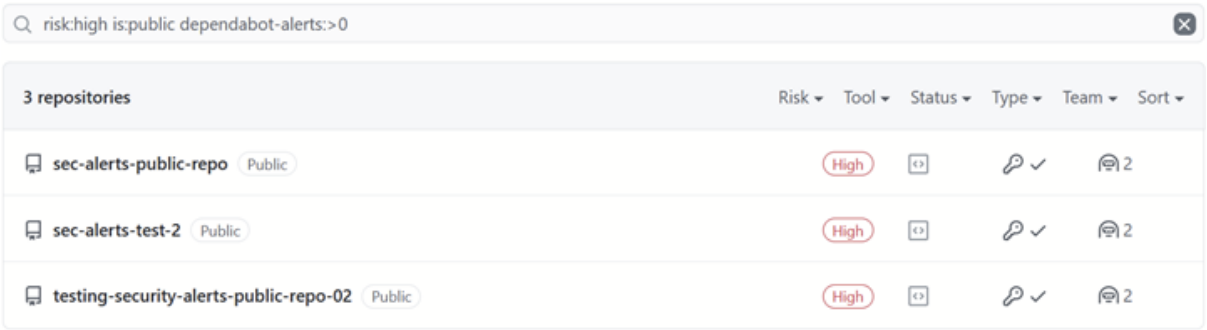
GitHubが提供するセキュリティ機能には、アプリケーションのセキュリティリスクを検出・修正するための強力なツールがあります。今回新たに導入されたセキュリティ概要は、ユーザーがアプリケーションセキュリティチームの一員あるいは開発リーダーとして、何百個または何千個というリポジトリを管理するにあたり、重要な機能となります。

GitHub Advanced Securityを使用するユーザーは、Code Scanning、Dependabot、Secret Scanningによって検出されたアプリケーションのセキュリティリスクを、セキュリティ概要の画面1か所で確認できるようになりました。セキュリティ概要には、こうした既知のセキュリティリスクに限らず、セキュリティ機能が設定されていないことが原因で、未知のリスクが発生している箇所についても情報が表示されます。

管理者は、有効化されているGitHubのセキュリティ機能と、検知した情報をOrganizationのSecurityタブで確認することが可能です、既知のセキュリティリスクに対して、どこから対処すべきかを分かりやすくするため、アクティブなアラートの数と重大さに基づいて、各リポジトリに対してリスクカテゴリーが割り当てられます。



包括的なフィルターセットを使用して、関心のあるリポジトリだけに焦点を合わせることも可能です。Dependabotアラートがあるハイリスクなパブリックリポジトリなど、特定のリポジトリにのみ関心がある場合は、類似したリポジトリだけを表示するよう、ビューを指定することも可能になっています。



さらに、個々のリポジトリ、割り当てられているリスクカテゴリー、リポジトリに対して有効化されているセキュリティ機能、アクティブなアラート数を確認することもできます。リポジトリの詳細を確認してから各機能の有効化に加え、アラートの詳細を確認してから実行することも可能です。

担当するリポジトリに関して、開発者とマネージャーの両方が同じ情報を把握していることは重要です。OrganizationがGitHub Teamを利用してリポジトリへのアクセスを管理している場合には、GitHub Teamの[Security(セキュリティ)]タブにもチームメンバーに関する情報が表示されます。

プライベートリポジトリ向けSecret Scanningの提供開始

2020年5月に発表したベータ版以降、GitHubではプライベートリポジトリ向けSecret Scanningを拡充してきました。ベータ版の発表以降、次の3点が改善されています。

- 35社を超えるパートナーからのトークンをカバーするように、Secret Scanningのパターン範囲を拡大。
- Secret Scanningアラート用のAPIとwebhookを追加。
- シークレットのコミット時にコミット作者(および管理者)への通知の送信を開始。

上記の内容はGitHub Enterprise Cloudで利用が可能ですが、今後、GitHub Enterprise Server 3.1にもすべて実装される予定です。GitHubでは、プライベートリポジトリ向けのSecret Scanningに対して、カスタムパターンのサポートなど、さらに多くの改善を計画しています。このSecret Scanningは、パブリックリポジトリにおいてこれまでに公開状態になってしまった5,000以上のシークレットを検出し、取り消した実績があります。プライベートリポジトリ向けにもSecret Scanningの提供を開始することは、GitHubにとって大きな一歩となります。

GitHub Advanced Securityの詳細について

- 新しいセキュリティ概要とSecret Scanningの詳細については、各GitHub Docsをご確認ください。
- 新しいセキュリティ概要およびプライベートリポジトリ向けSecret Scanningはどちらも、GitHub Advanced Securityの一部として提供されます。GitHubが安全なアプリケーションのリリースに役立つ仕組みから、より詳しく確認いただけます。また、お使いのアカウントでのGitHub Advanced Securityを有効にできるかについては、営業担当にお問い合わせください。

GitHub Blog
英語
https://github.blog/2021-03-30-github-advanced-security-security-overview-beta-secret-scanning-private-repos/
日本語
https://github.blog/jp/2021-04-13-github-advanced-security-security-overview-beta-secret-scanning-private-repos/

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（ギットハブ）は世界で5,600万人にのぼる開発者および300万の組織に利用される開発プラットフォームです。プログラミング環境にオープンな会話と協調を重んじるコミュニケーションによって、コラボレーションを促進する開発環境を提供しています。これらの開発を実現するワークフローで必要となるコードレビュー、プロジェクトおよびチームマネージメント、ソーシャルコーディング、ドキュメント管理などに、これまで以上の効率性と透明性をもたらし、より高速かつ品質の高いソフトウェア開発を支援しています。
GitHubは多様なユースケースに適した開発プラットフォームを用意しており、オープンソースジェクトから企業における機密性の高いソフトウェア開発までに対応できます。無料で利用できるパブリックリポジトリは、オープンソースプロジェクトにて多く利用されています。プライベートリポジトリが利用できる有償サービスとして GitHub Enterprise や GitHub One などのプランも提供しています。
2008年に米国サンフランシスコで創業したGitHub, Inc.は、初の海外支社として、2015年に日本支社を開設しました。

【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