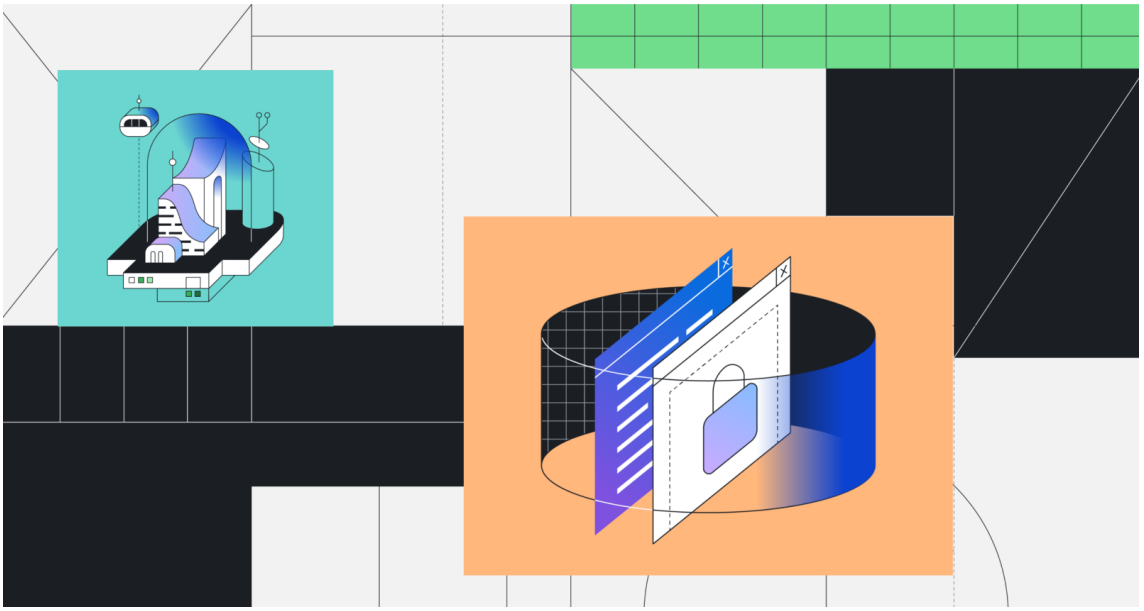
GitHub

NEWS RELEASE

2022年12月23日
ギットハブ・ジャパン合同会社

GitHub、secret Scanningの機能をアップデート

- GitHub Advanced Securityでカスタムパターンのプッシュ保護が可能に
- GitHub上のパブリックリポジトリで漏洩したシークレットを無料で追跡可能に



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、12月15日（米国時間）にsecret Scanningの機能のアップデートを発表しました。

GitHub Advanced Securityを利用する組織の管理者は、ワンクリックでプッシュ時にカスタムパターンを保護することが可能に

アプリケーションセキュリティに関する特に有効なイニシアチブは、開発者の作業効率の向上に役立ちます。GitHub Advanced Securityを利用することで、企業はプッシュ保護を用いてシークレットの漏洩を阻止し、下流工程での修正時間を数百時間も節約できます。プッシュ保護を4月にリリースして以来、既に100種類、8,000件以上のシークレット漏洩を阻止してきました。

カスタムパターンを定義している企業は、定義済みのカスタムパターンに対してプッシュ保護を有効化をすることが可能となりました。カスタムパターンのプッシュ保護はパターンごとに設定でき、どのパターンを公開するか（もしくはどのパターンを最初にドラフトモードとして、徐々に改良していくか）を選べるのと同様に、プッシュ保護を行うパターンを誤検知に基づいて決定することができます。

「シークレットをプッシュしようする場合、即座に気付くことができます。GitHubのsecret scanningのプッシュ保護のおかげで、シークレットがコードベースにプッシュさ

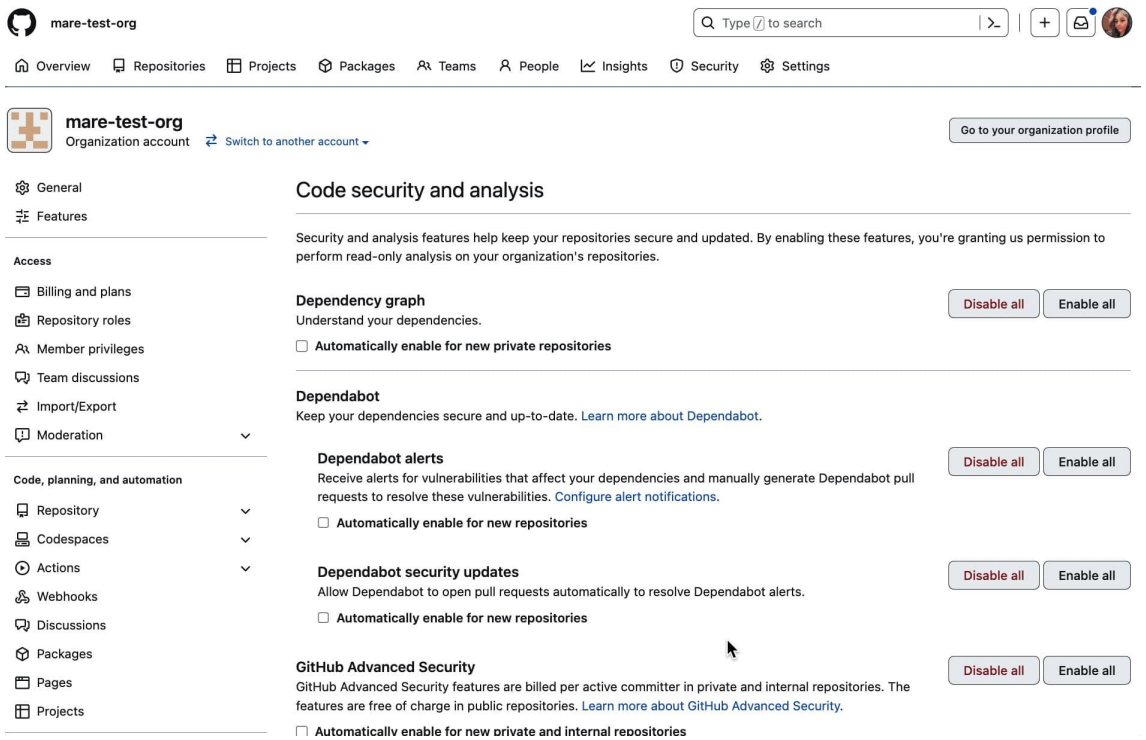
れることを防止できるため、膨大な時間を節約することが可能です。仮に外部のスキャンツールだけを利用して、シークレットが既に公開された後にリポジトリをスキャンする場合、シークレットを迅速に取り消したうえで、コードをリファクタリングする必要があります。GitHubのsecret　scanningとプッシュ保護を開発者のフローに直接統合することで、時間を節約できることに加え、ベストプラクティスについて開発者に情報を提供することが可能となります」

- Intel、ソフトウェアエンジニアリングディレクター、David Florey氏

プッシュ保護の有効化
カスタムパターンの定義は、リポジトリ、Organization、およびEnterpriseのレベルで行えます。また、カスタムパターンのプッシュ保護をOrganizationまたはリポジトリのレベルで有効化することも可能となりました。プッシュ保護を有効にすると、コントリビュータがプッシュしようとするコードに定義済みパターンと一致するパターンが含まれている場合に、ブロックが適用されます。

カスタムパターンを定義するためには、Organizationのコードセキュリティ設定ページに移動し、GitHub Advanced Securityとsecret scanningを有効にすることで、UIから新しいカスタムパターンを作成できます。また、公開前にカスタムパターンをドライランすることが可能です。

パターンを公開し、そのパターンによって生成されるアラートに誤検知が少ないことを確認した後、カスタムパターンのページで[Push　protection]の横にある[Enable]をクリックしてください。GitHubでは、カスタムパターンのアラートを定期的にチェックし、開発者のために誤検知のノイズを可能な限り少なく抑えられているかを確認することを推奨しています。プッシュ保護を戦略的に活用することで、コントリビュータがセキュリティアラートを信頼し、必要に応じて適切に処理できるようになります。



Secret scanningの詳細

Secret scanningアラートは、すべてのパブリックリポジトリで無料で利用できます。また、GitHub Advanced Securityの一部として、プッシュ保護とプライベートリポジトリのカバレッジも提供します。これには、code scanningやサプライチェーンセキュリティのインサイトが含まれます。GitHub Advanced Securityの導入やデモについては、こちらから。

Secret scanningアラートにより、**GitHub**上のパブリックリポジトリで流出したシークレットを追跡し、対処可能に

データ漏洩の原因として特に多いのがシークレットや認証情報を公開してしまうことですが、追跡が十分に行われることはあまり多くありません[1]。このようなデータ漏洩は特定までに平均327日を要し、認証情報の漏洩が深刻な結果につながる可能性があることが明らかとなっています。しかしながら、依然として、企業は大規模な漏洩の検出や迅速な対応、公開されてしまったシークレットの修正に多くの労力を割かれています。

GitHubでは、Secret scanningパートナープログラムを通じて多くのサービスプロバイダーと提携し、すべてのパブリックリポジトリを対象に、漏洩した認証情報にフラグ付けを行っています。200個を超えるトークンフォーマットに基づいてリポジトリをスキャンし、関連のあるパートナーと協力して、共通のお客様を保護しています。2022年には、パブリックリポジトリで公開されている170万個以上の潜在的なシークレットをパートナーに通知し、トークンの悪用を阻止しました。

GitHubコミュニティのすべての無料パブリックリポジトリに対して、無料で利用できる**secret scanning**の提供を開始

Secret scanningアラートは、コードにシークレットの漏洩がある場合にユーザーに直接通知します。きわめて迅速な保護を実現するためにパートナーにも通知しますが、リポジトリに関する包括的な保護手段をユーザー自身が所有できるようになりました。また、セルフホスト型のHashiCorp Vaultのキーが公開されている場合など、パートナーには通知できないシークレットについてのアラートも通知します。すべてのアラートをいつでも簡単に追跡して、漏洩元を詳しく調査したり、アラートに対して実行されるアクションを監査できます。

パブリックリポジトリで***Secret scanning***アラートを活用することで、シークレットの公開を阻止し、安心してオープンソースを利用することが可能

「*Secret scanning*のおかげで、対処すべき重要な事象を多く見つけることができました。*AppSec*側としては、コードに含まれる問題を可視化するための最良の方法であることが多いです」

- Postmates、スタッフセキュリティエンジニア、*David Ross*氏

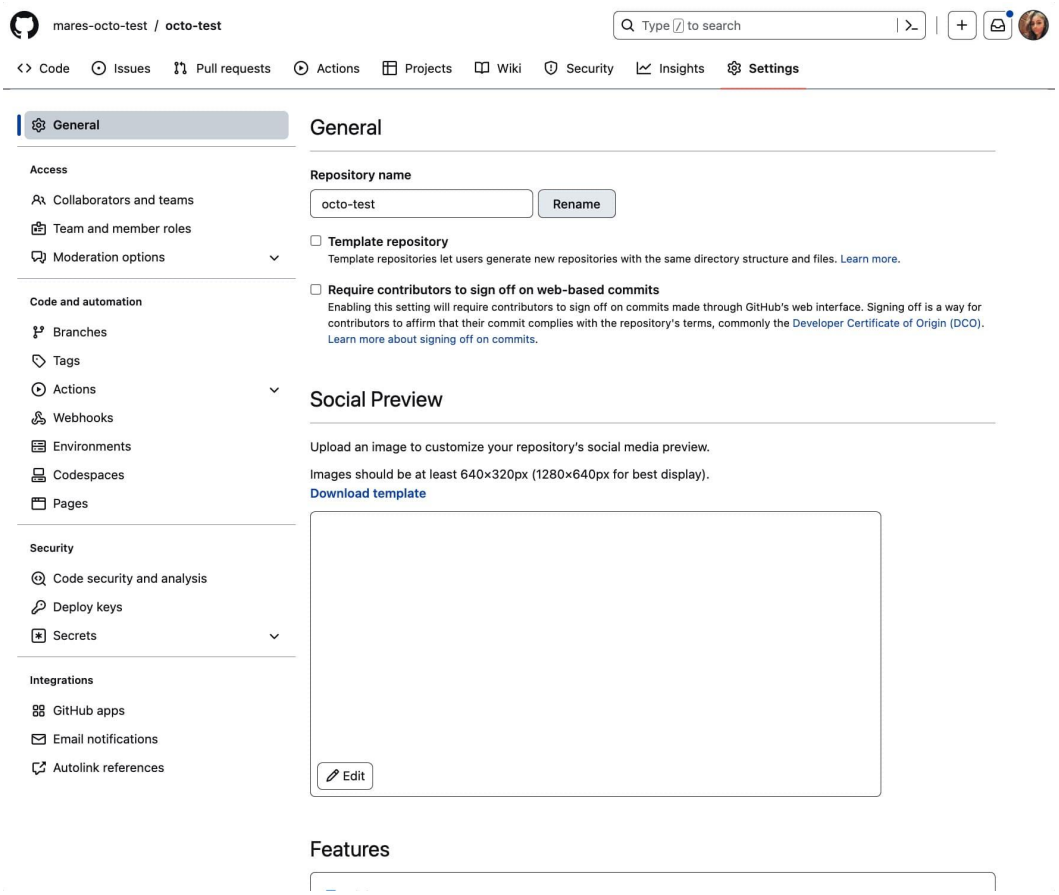
---

[1]IBM「Cost of a Data Breach 2022」https://www.ibm.com/reports/data-breach

利用を開始するには

パブリックリポジトリを対象に、パブリックベータ版secret scanningの段階的な展開を開始しており、2023年1月末までに、すべてのユーザーがこの機能を利用できるようになる予定です。早期の利用を開始したい場合や、ご質問またはフィードバックがある場合は、コードセキュリティディスカッションでリクエストを送信してください。

リポジトリでsecret scanningアラートを利用できるようになった後、[Code security and analysis]設定の下にあるリポジトリの設定でアラートを有効化することが可能です。検出されたシークレットを確認するには、リポジトリの[Security]タブに移動し、サイドパネルの[Vulnerability alerts]の下にある[Secret scanning]を選択します。ここでは、検出されたシークレットが一覧で表示されており、いずれかのアラートをクリックすると、漏洩シークレット、その場所、修正のための推奨アクションが示されます。



リポジトリのsecret scanningアラートを有効にする方法について、詳しくは、GitHubのドキュメントをご確認ください。

GitHub Blog
英語:
https://github.blog/2022-12-15-leaked-a-secret-check-your-github-alerts-for-free/

https://github.blog/2022-12-15-github-advanced-security-customers-can-now-push-protect-their-custom-patterns/

GitHub NEWS RELEASE

日本語:
https://github.blog/jp/2022-12-22-leaked-a-secret-check-your-github-alerts-for-free/

https://github.blog/jp/2022-12-22-github-advanced-security-customers-can-now-push-protect-their-custom-patterns/

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「開発者ファースト」の思想のもと、開発者のコラボレーションおよび困難な問題解決、世界にとって重要なテクノロジーの創出を促進させるための開発環境を提供しています。また、ソフトウェアを起点とする新たな未来を創造し、世界に変化をもたらすため、個人または企業規模に関わらず、ベストなコラボレーションができるコミュニティの拡大を支援しています。
安全なソフトウェア開発には、日常のワークフローの中でできる限り早いタイミングで脆弱性を発見し、対処できる仕組みづくりが重要です。GitHubは、企業とオープンソースのメンテナーが、ソフトウェア開発のライフサイクル全体を通じて、安全にコーディングできるようにするツールとプロセスを構築しています。
GitHubは、開発者がコードを開発、共有、そしてリリースする場です。学生や趣味で開発を行う人、コンサルタント、エンタープライズの開発者、経営者など、初心者から高い専門性をもつ世界8,300万人以上の方々および400万以上のOrganizationに利用されています。GitHubは単なるソースコードを共有する場ではありません。GitHubはオープンソースコラボレーションの源としてさまざまなソリューションを提供します。

【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