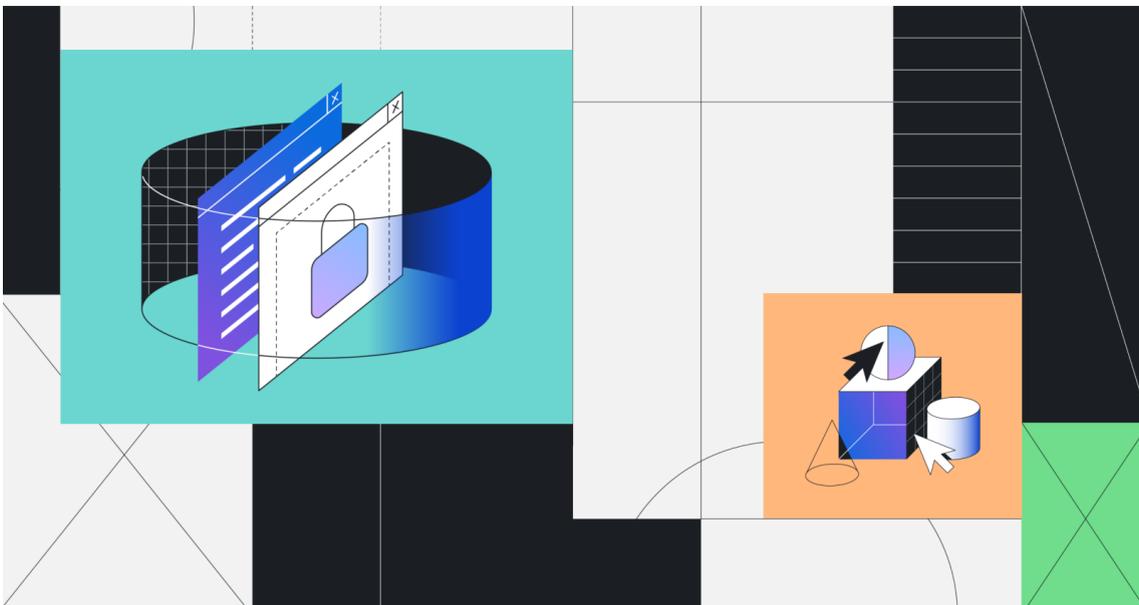


2022年5月16日
ギットハブ・ジャパン合同会社

GitHub、すべてのユーザーのアカウントを 2023年末までに2要素認証(2FA)で保護

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、5月4日(米国時間)にGitHub.com上でソースコードの開発に貢献するすべてのユーザーに対して、2023年の終わりまでに、1つ以上の2要素認証(2FA)形式を有効化することを発表しました。



ソフトウェアサプライチェーンのスタート地点は開発者であり、その開発者のアカウントは頻繁にソーシャルエンジニアリングの攻撃対象になる、あるいはアカウント乗っ取りのターゲットにされます。こうしたタイプの攻撃から開発者を保護することは、[サプライチェーンの安全性を確保するための防御](#)として最初の一手であると同時に、最重要事項でもあります。GitHubにはソフトウェア開発者を保護してきた長い歴史において、[不正アクセスを受けた既知のユーザーパスワードを見つけて無効化する](#)、[堅牢なWebAuthnセキュリティキーのサポートを提供する](#)、[すべてのnpmパブリッシャーを強化されたログイン検証に登録する](#)などの取り組みを実施してきました。

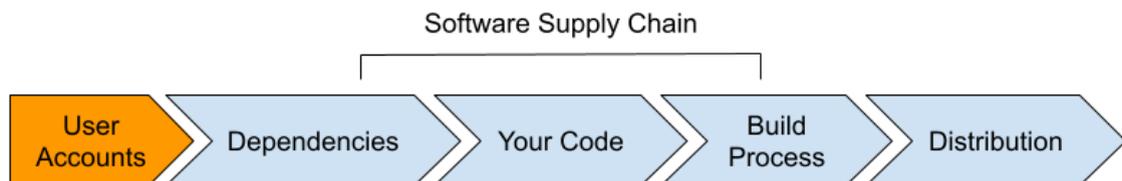
今回の2FAへの対応は、GitHubアカウントのセキュリティを強化することでソフトウェア開発のエコシステムをより安全に保護することを目的とした、プラットフォーム全体の取り組みの一環です。GitHubは、ソフトウェア開発に貢献するすべてのユーザーに対し、2023年の終わりまでに1つ以上の2要素認証(2FA)形式を有効化することを決定しました。

GitHubでは、強力なアカウントセキュリティによって開発者のエクスペリエンスが犠牲になることのないよう尽力しています。今後も、セキュリティ基準の進化に合わせて、ユーザーを安全に認証する新しい方法(パスワードレス認証など)を積極的に模索していきます。開発者はどこにいても、認証やアカウントリカバリに関する[さらに多くのオプション](#)や、アカウント侵害の防止とリカバリーに役立つ機能改善を利用できるようになります。

アカウントのセキュリティと2FAが重要である理由

2021年11月、2FAを有効にしていなかった開発者アカウントへのセキュリティ侵害が原因で発生したnpmパッケージの乗っ取りをきっかけに、GitHubはnpmアカウントのセキュリティに対して新たな投資を行いました。現在はnpmアカウントのセキュリティ[向上](#)への取り組みを継続しながら、GitHubを使用している開発者アカウントの保護にも同様に尽力しています。

大半のセキュリティ侵害は、未知のゼロデイ攻撃によるものではなく、ソーシャルエンジニアリング攻撃、認証情報の盗用または漏えい、被害アカウントやその先のリソースへの広範なアクセス権を攻撃者に提供する手段など、低コストの攻撃が関係しています。侵害されたアカウントは、プライベートコードを盗んだり、そのコードに悪意のある変更をPushするために使用されてしまいます。これにより、侵害されたアカウントに関連付けられている個人や企業だけでなく、攻撃を受けたコードを利用するすべてのユーザーも危険に晒されることとなります。結果的に、広範なソフトウェアエコシステムやサプライチェーンの下流に影響を与える可能性は多大になります。



これに対する最善の防御は、パスワードによる基本的な認証を越えた手段を講じることです。GitHubでは既にこの方針を採用し、[Git操作とAPIに対するBasic認証を非推奨](#)とし、ユーザー名とパスワードに加えて[メールベースのデバイス確認を要求する](#)ようにしています。2FAは強力な第二の防衛線であり、[実証済みの成功例](#)にもかかわらず、ソフトウェア開発エコシステム全体での2FAの採用率は、まだ低い状態です。現在、1つ以上の2FA形式を使用しているのは、GitHubのアクティブユーザーの約16.5%、npmユーザーの約6.44%に過ぎません。

npmの2FAアップデート

GitHubでは今年2月に、[上位100パッケージのすべてのメンテナ](#)を、2FAを必須とするnpmレジストリに登録しました。3月には、すべてのnpmアカウントを強化済みの

ログイン検証に登録しました。5月31日には、上位500パッケージのすべてのメンテナーに対して2FAを必須にする予定です。最終的には、[今年の第3四半期](#)までに、利用するユーザー数が500人を超えていたり、毎週のダウンロード数が100万回に上るメンテナーも対象にする予定です。今後さらに、npmに対して2FAを要求することから得た知識を活用し、その教訓をGitHub.comでの取り組みに応用していきます。

世界最大の開発者プラットフォームであり、すべての開発者にとってのホームであるGitHub.comには、ソフトウェア開発エコシステム全体のセキュリティ水準を引き上げるチャンスと責任の両方を持っていると信じています。ソフトウェアサプライチェーンの全体的なセキュリティを向上させるために、GitHubではプラットフォームならびに幅広い業界に深く投資していますが、アカウント侵害のリスクへの対処を怠ると、投資価値が根本的に制限されてしまいます。GitHubは、引き続きこの課題解決に向けて取り組みを進め、一人ひとりの開発者のための安全なプラクティスを通じて、サプライチェーンのセキュリティ向上を促進するよう尽力していきます。

個人ユーザー

最近リリースしたiOSおよびAndroidアプリGitHub Mobile上で2FAが利用可能になっています。GitHub Mobile での2FAの設定方法は、[こちら](#)からご確認ください。GitHub Mobile 2FAを設定するには、その他の形式の2FAを1つ以上有効にする必要があります。詳細については、以下のとおりです。

フィッシングに対抗するWebAuthnセキュリティキーのエクスペリエンスまたはその他のオプションは[こちら](#)をご確認ください。

セキュリティキーの採用を促進するために、GitHubではYubiKeyなどのセキュリティキーを重要な[オープンソースプロジェクト](#)のメンテナーに配布し、セキュリティキーを[GitHubショップ](#)で販売しています。[SoloKeys](#)や[Titan Security Keys](#)もご利用いただけます。

GitHub.comの2FAに関するその他のドキュメントは、[こちら](#)からご確認ください。npmアカウントに2FAを設定するには、[こちら](#)をご確認ください。

リカバリーコードの保存と、1つ以上の[アカウントリカバリ方法](#)の設定も必要になります。

OrganizationとEnterprise

GitHub.comのOrganizationおよびEnterpriseのオーナーは、自分の[Organization](#)および[Enterprise](#)のメンバーに対して2FAを要求することも可能となっています。これらの設定を有効にすると、2FAを使用しないOrganizationおよびEnterpriseのメンバーとオーナーは、そのOrganizationまたはEnterpriseから排除されます。

今後について

今後数か月の間に、GitHub.comユーザーに対する将来的な2FA要件について、詳細情報とタイムラインをお伝えする予定です。GitHubは、コードをコミットする、Pull RequestやMergeする、GitHub Actionsを使用する、パッケージの公開などを行う人々に対して、2FAを求めることは適切であると考えていますが、スムーズで利用しやすい操作性も確保したいとも思っています。アカウントの保護とリカバリーに役立つように設計していく今後の機能改善と新機能にご注目ください。

GitHub Blog

英語:

<https://github.blog/2022-05-04-software-security-starts-with-the-developer-securing-developer-accounts-with-2fa/>

日本語:

<https://github.blog/jp/2022-05-13-software-security-starts-with-the-developer-securing-developer-accounts-with-2fa/>

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7,300万人にのぼる開発者および400万以上の組織に利用されるソフトウェア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、オープンソースプロ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