GitHub

NEWS RELEASE

2024年4月25日
ギットハブ・ジャパン合同会社

GitHub、2FAで数百万人の開発者の安全を担保

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, Inc.（本社：米国サンフランシスコ）は、2024年4月24日(米国時間)、2022年に発表し、2023年から開始したGitHub.com上にソースコードを投稿するすべての開発者に2FA（2要素認証）を義務付けるというイニシアチブの初期結果を発表しました。

GitHub は、ソフトウェア・エコシステムをより安全にするという責任の一環として、2FA の適用を大幅に増加させました。テクノロジーはセキュリティ上の脅威の拡散に対抗するために大きく進歩しましたが、次のサイバー攻撃を防ぐには、セキュリティの基本を正しく理解することが重要です。その上でソフトウェア・エコシステムを保護する取り組みは、ソフトウェアを設計、開発、メンテナンスする開発者を保護するものでなければなりません。

世界最大の開発者コミュニティのホームであるGitHubは、ソフトウェアサプライチェーンのセキュリティ向上を支援できる稀な存在です。2022年5月、サプライチェーンセキュリティの水準を高めるため、開発者のセキュリティに取り組むイニシアティブを発表しました。強固な多要素認証は、アカウントの乗っ取りやそれに続くサプライチェーンの侵害に対する最善の防御策の一つであり、GitHubは2023年末までに、GitHub.comでコードを利用するユーザーに対し、1つ以上の2要素認証（2FA）の有効化を必須要件とするという野心的な目標を設定しました。

その後、開発者にとってシームレスなエクスペリエンスに最適化するため、この必須要件の展開に関するリサーチとデザインに1年分の投資を行い、その後、要件の規模を拡大し続けながら、ユーザーのオンボーディングを成功させるために段階的なロールアウトを行いました。開発者がGitHub.comで可能な限り安全に利用できるようにするためのGitHubの取り組みはこれに留まりません。今回、GitHubの2FA登録の第１段階の結果を共有します。

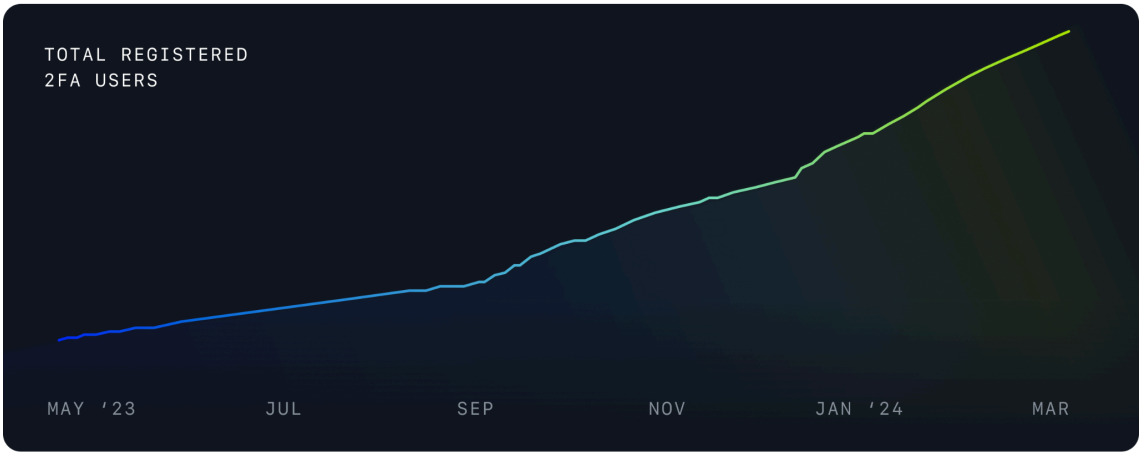
今回の主な結果は以下の通りです。

- GitHub.comでの2FAの導入が大幅に増加。ソフトウェアサプライチェーンに最も重要な影響を与えるユーザーに焦点を当てました。

- ユーザーは、パスキーを含む、より安全な 2FA の手段を採用しました。
- 2FAに関連するサポートチケットの件数が減少しました。これは、サポートプロセスの改善だけでなく、ユーザー調査や設計を前もって行った結果です。
- RubyGems、PyPI、AWSのような他の組織も、ソフトウェアサプライチェーン全体のハードルを上げることに参加しており、2FA採用の大幅な増加が、この課題は克服可能であることを証明しています。

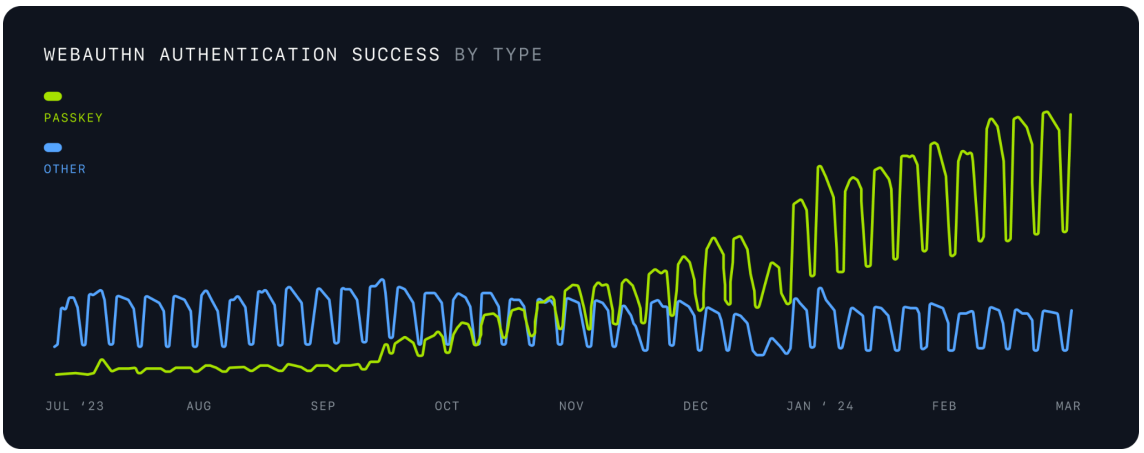
2FAの採用

2023年3月に2FA必須要件の展開を開始して以来、GitHub.comの全アクティブ・コントリビュータにおける**2FA**の採用率が**54%**増加しました。2023年に2FAの必須要件を受け取ったコード・コントリビュータのうち、**95%**近くがオプトインしており、登録者は増え続けています。



より強力で信頼性の高い認証

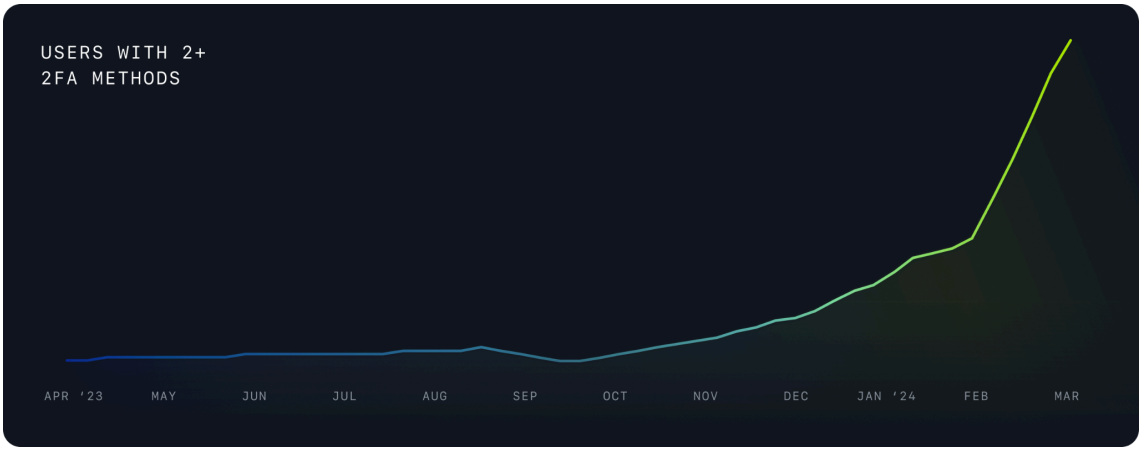
このイニシアチブの主な焦点は、ユーザーにより安全な2FA手段、特に現在セキュリティとユーザビリティの最強の組み合わせを提供するパスキーの採用を促すことでした。2023年7月にパスキーをパブリックベータとしてリリースして以来、**140**万近くのパスキーが**GitHub.com**に登録されました。さらにパスキーは日々の使用において、WebAuthnに裏打ちされた他の形式の2FAを急速に追い越しました。



GitHubはパスキーを強く推進していますが、GitHubが世界中の開発者に柔軟性、信頼性、セキュアな認証方法を提供し続けることも重要です。GitHubでは、SMSを2FAのオプションとして引き続きサポートし、他の方法を採用できないユーザーにも、可能な限りよりセキュア

な方法を採用してもらえるよう、2FAオンボーディングのワークフローを意図的に設計しています。この作業により、2023年初頭から2024年初頭の間に、第二要因としての**SMS**のシェアは全体で**23%**近くまで減少しました。GitHubは、パスキーの採用促進を続ける一方で、よりセキュアでないファクタータイプの利用を減少させる余地が大いにあると見ており、GitHub プラットフォームの開発者の大多数にとってパスキーがファーストチョイスとなる未来を予見しています。

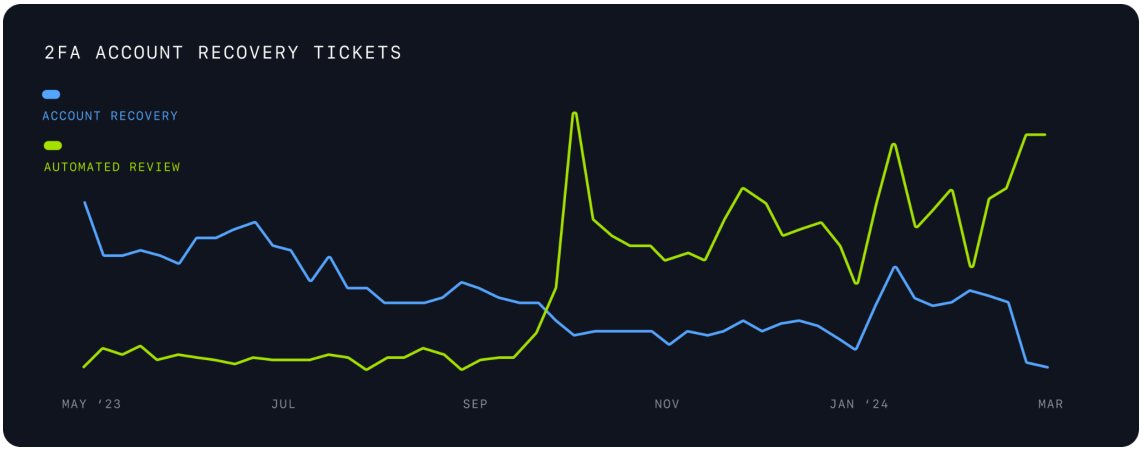
最後に、登録体験の改善とパスキーの展開の結果、ユーザーが**2**つ以上の形式の**2FA**を設定する可能性が**47%**高まったというデータがあります。各要素を追加することで、ユーザーがすべての要素を失い、ロックアウトされる可能性がはるかに低くなり、よりスムーズで信頼性の高いユーザー体験が得られます。



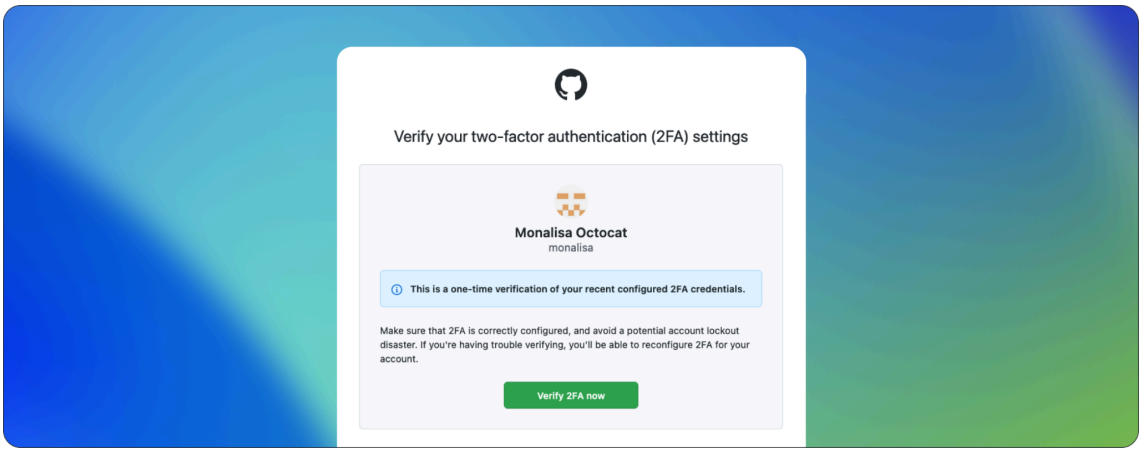
ユーザー体験とサポート

シームレスなユーザーエクスペリエンスという約束を守りつつ、開発者が強固なアカウントセキュリティを採用できるようにために、GitHubは 2FA オンボーディングフローの刷新、GitHub モバイルアプリの 2FA の追加、プライマリ 2FA 要素のユーザーオプションの増加など、多くの改善に投資してきました。プラットフォームでの相対的な利用が増えるにつれて、2FA 関連のサポートチケットが増えると考えるのが妥当でしょうが、結果は想像とは反し、展開に先立ち、ユーザーエクスペリエンスとデザインに多大な投資を行ったため、**2FA**関連のサポートチケットは**3**分の**1**に減少しました。

さらに、社内のワークフローを最適化し、サポート・チームの自動化を進めた結果、人的介入を必要とする**2FA**アカウント回復のサポート・チケットが**54%**減少しました。現在、アカウント復旧リクエストチケットの75%以上は、プロダクト内のワークフローから生じています。このワークフローでは、ユーザーからリカバリーの詳細を収集し、リスク要因や、安全だとわかっているシナリオ（サインインしたままアカウント・リカバリーを行うなど）を自動的にチェックします。このデータ収集と審査により、サポートチームがこれらの復旧の試みをレビューする時間が劇的に短縮され、ロックアウトされたユーザーが安全にアカウントに戻ることができるようになり、GitHubは2FAの登録を数百万人のユーザーに拡大することができるようになりました。



また、ユーザーが自分の設定を確認できるように、2FAの設定から28日後に行われる2FA確認のチェックアップも導入しました。このチェックアップはフェイルセーフであり、**25%**のユーザーが設定ミスやファクター紛失の際にアカウントの再設定を成功させ、ユーザーのアカウントロックアウトを回避し、GitHub のアカウント復旧サポート量を大幅に削減しました。



エコシステムへの影響

GitHubは、GitHub.com上の開発者の安全を守ることを第一に考えていましたが、GitHubとnpmが独自の2FA必須要件を設定した後、より多くの組織がこの呼びかけに応じることを目標に、展開のアプローチを意図的に透明化しました。2FAが正常に有効化されたユーザーアカウントはすべて、攻撃者が組織や重要なオープンソースソフトウェアを侵害するベクトルを1つ減らすことになります。この2年間で、**RubyGems**、**PyPI**、**AWS**が、**GitHub**の共有エコシステムとソフトウェアサプライチェーンをセキュアにするために、**2FA**の利用拡大を推進する取り組みに参加しました。

今後の展望

ソフトウェアサプライチェーンとそれを担当する開発者の安全を守ることに終わりはありません。初期作業では、ユーザー権限や具体的な行動の影響に基づいて、個別のユーザー・グループに優先順位をつけました。

また、2FAを採用するために、携帯電話にアクセスできなかったり、使用するコンピュータの

ソフトウェアを制御できなかったりするユーザーをサポートするための、業界全体の重要な作業もまだ残っています。グローバル・プラットフォームであるGitHubは、誰もがソフトウェアを開発でき、より簡単でセキュアなものにするためのツールにアクセスできるべきだと考えており、開発者に強力な認証を導入するための取り組みも継続中です。GitHubは、開発者自身、開発者が取り組んでいるプロジェクト、開発者が参加しているコミュニティを保護するためのソリューションを見つけ出すことを続け、世界中の異なるセットアップや環境を持つ人々を制限することなく、ソフトウェアサプライチェーン全体のセキュリティを大幅に向上させるバランスの取れたアプローチを取るよう努力していきます。

今後については、ユーザーエクスペリエンスの継続的な監視と改善を行いながら、2024年中にさらに多くのGitHub.comユーザーに2FAへの登録を必須要件とする方法を評価中です。GitHubは、セッションやトークンのバインディングなど、2FAの有無にかかわらず、開発者とその組織がアカウント漏洩のリスクをより適切に管理できるような、追加のアカウントセキュリティ機能を調査しています。また、パスキーやセキュリティキーのような、プラットフォーム上で開発者が利用できる最もセキュアな要素の採用を引き続き推進し、開発者がよりセキュアな認証タイプに「ステップアップ」するのを支援したいと考えています。これらの取り組みの最優先事項は、セキュリティを簡単で効果的にすることです。

GitHubは、ソフトウェアのエコシステムを安全にする役割を担っており、プラットフォームは責任あるソフトウェアの消費者であると同時に、ソフトウェアに貢献するコントリビュータであることを使命とするべきです。**GitHub**は、エコシステム全体を守るために正しいことだと信じているからこそ、大規模な**2FA**に取り組むことを選びました。また、他の組織も一緒に参加することが不可欠であると考えています。このようなGitHubの取り組みが、ユーザーエクスペリエンスに悪影響を与えることなく、セキュリティの水準を大幅に引き上げることが可能であることを示しており、他の組織にも、可能であれば自分たちのプラットフォームで2FAを必須要件とすることを強く検討するよう促しています。

この取り組みに参加したい場合は、自身のアカウントで2FAを有効にするか、パスキーを採用するか、組織で2FAを必須要件にしてください。

GitHub Blog
英語：https://github.blog/2024-04-24-securing-millions-of-developers-through-2fa/

日本語：https://github.blog/jp/2024-04-25-securing-millions-of-developers-through-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
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、提供を実現に向け世界有数のAI搭載開発者プラットフォームです。『Fortune 100』(グローバル企業の総収入ランキングトップ100)に名を連ねる90社の開発者を含む1億人以上の人々がGitHubを利用し、4億2,000万以上のリポジトリで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。
GitHub.com　(日本語サイト https://github.co.jp)

【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