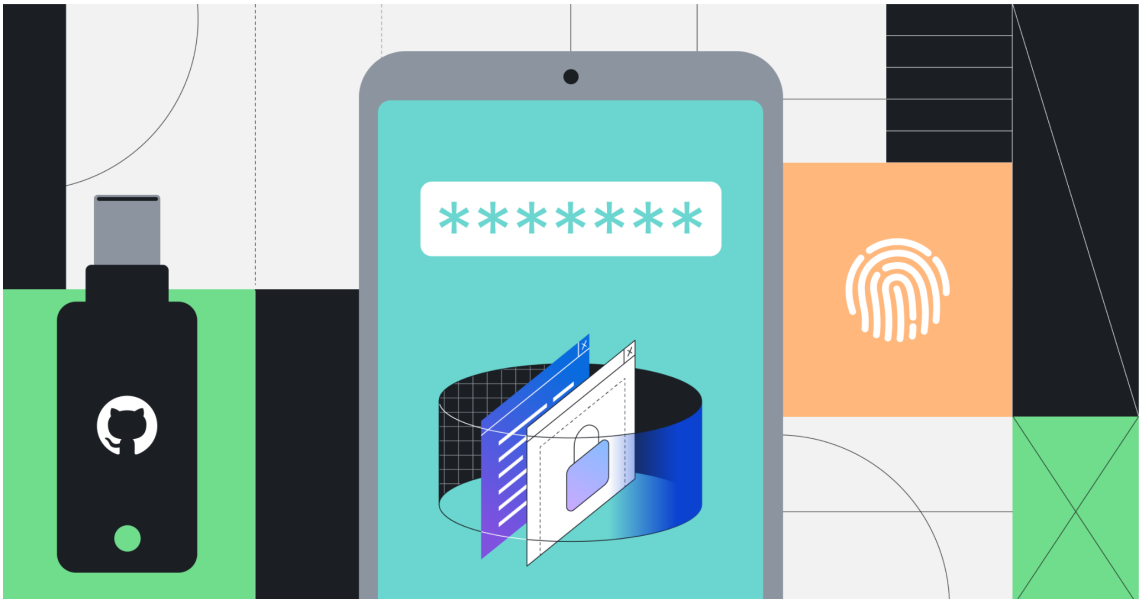
GitHub

NEWS RELEASE

2023年3月17日
ギットハブ・ジャパン合同会社

GitHub、ソフトウェアのセキュリティ水準向上のため 3月13日より 2要素認証（2FA)を開始

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3月9日(米国時間)に3月13日から、2023年末までにGitHub.comでコードを投稿するすべての開発者に2要素認証（2FA）の有効化を義務付ける取り組みを正式に展開すると発表しました。



2022年、GitHubではGitHub.com上のコードに貢献するすべての開発者に対し、2023年末までに2要素認証(2FA)を有効化するよう求める取り組みを発表しました。

GitHubはソフトウェアサプライチェーンの中核を担っており、ソフトウェアサプライチェーンの安全性を確保する上で起点となるのは開発者だと考えています。この2FAに関する取り組みは、プラットフォーム全体を横断する取り組みの一環として、アカウントのセキュリティ向上によりソフトウェア開発の安全性を確保することを目的としています。開発者のアカウントはソーシャルエンジニアリングやアカウントの乗っ取り(ATO)の標的になることが多く、このような攻撃からオープンソースエコシステムの開発者と消費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上で第一歩であり、最も重要なステップです。

3月13日から2FA要件の展開を開始

3月13日より1年かけて、開発者と管理者のグループを対象に、2FA登録要件の通知を予定しています。小規模のグループから通知を開始し、段階的に展開していくことで、開発者

の登録を滞りなく進めるとともに、年内に大規模なグループへと移行する前に必要に応じて調整を行うことができます。

ご利用のアカウントが登録の対象として選ばれると、通知メールが届き、GitHub.com上では登録を促すバナーが表示されます。2FAの設定は45日以内に実施してください。この期間中はリマインダーが表示されますが、それ以外は通常どおりにGitHubを使用できます。期限が過ぎるとGitHub.comへの初回アクセス時に2FAの有効化を求められるようになります。期限後も、登録の催促通知を最長で1週間、スヌーズ機能で繰り返し再表示させることができますが、それ以降はアカウントへのアクセスが制限されます。このスヌーズ期間は、設定期限を過ぎてサインインした時点から始まるため、休暇中または不在で対応できない場合でも業務に戻ってから1週間の猶予があります。

早期登録の対象グループに入っていない場合でもこちらから簡易なステップで、2FAを設定できます。

2FAでGitHubアカウントの安全性確保がより簡単に

GitHubは、アカウントの所有者のみがいつでもアカウントにアクセスできるよう、信頼性と安全性に優れた手法を採用して、2FA登録をできる限り簡単に行えるようにしました。このプログラムの準備にあたり、GitHubは2FAエクスペリエンスの強化に取り組んできました。

下記にて、主なポイントをご紹介します。

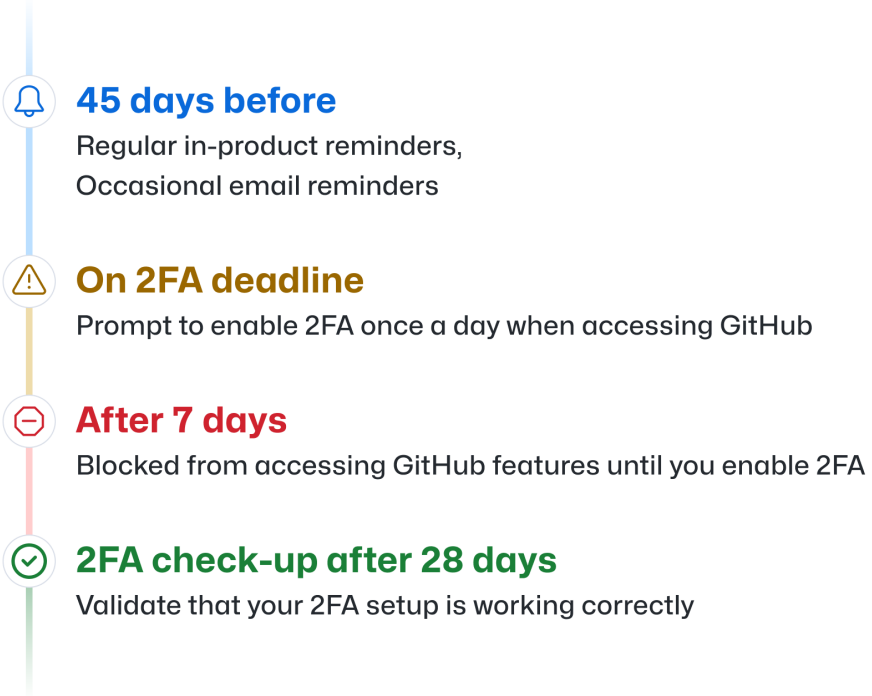
- **2FA**設定後に**2**番目の要素を検証：GitHub.comユーザーが2FAを設定すると、28日後にプロンプトが表示され、2FAを実行して2番目の要素の設定を確認するよう求められます。このプロンプトにより、認証アプリケーション(TOTPアプリ)の設定ミスによるアカウントのロックアウトを回避できます。2FAを実行できない場合は、アカウントからロックアウトされることなく、2FA設定をリセットできるショートカットが表示されます。
- **2**番目の要素を複数登録：ユーザーがいつでもアカウントにアクセスできるようにするには、使いやすい2FA方式を採用することが重要であるため、認証アプリケーション(TOTP)とSMS番号の両方を同時に登録できるようにしました。GitHubが推奨するのは、SMSよりもセキュリティキーやTOTPアプリケーションの利用ですが、両方を同時に設定できるようにすることで、開発者が有効化でき、アクセスしやすく、わかりやすい別の2FAオプションを提供することにより、ロックアウトを減らすことができます。
- 優先する**2FA**方式を選択：新しい優先オプションによって、アカウントへのログイン時やsudoプロンプトの使用時に優先的に使用する2FA方式を設定することができ、サインイン時に常にお気に入りの方式が最初に表示されます。優先する2FA方式としてTOTP、SMS、セキュリティキー、GitHub Mobileを選択できます。GitHubでは、可能な限りセキュリティキーとTOTPを使用することを強く推奨します。SMSによる2FAは、同レベルの保護を提供できないため、NIST 800-63Bでは現在推奨されていません。特に強力な方式として広く活用されているのは、WebAuthnのセキュアな認証標準に対応する方式であり、物理的なセキュリティキー、およびWindows HelloやFace ID/Touch IDといったテクノロジーをサポートするパーソナルデバイスが含まれます。

- **2FA**によるロックアウトに備えてメールのリンクを解除：GitHubのアカウントでは固有のメールアドレスが必要です。そのため、ロックアウトされたユーザーがアカウントを新たに作ろうとしても、いつも優先的に使い、あらゆる大事な場面で指定しているメールアドレスを使うことができません。今回、この機能を利用することで、2FAを有効化したGitHubアカウントへのサインインや復旧ができなくなった場合も、メールアドレスのリンクを解除できるようになりました。SSHキーやPAT、過去にGitHubにサインインしたデバイスがなくてアカウントを復旧できなくても、新しいGitHub.comアカウントを簡単に作り直して、コントリビューショングラフを本来あるべきとおり緑色に保てます。

使いやすさとフィッシングに対抗できる強力な認証機能を兼ね備えているパスキーについては、既にGitHub社内でテストを実施しており、パスキーの提供時期については、後日アップデートいたします。

≪リマインダー≫2FAの有効化が必要になった場合の流れ

GitHubは、ユーザー側の予期しない作業の中断や生産性の損失を最小限におさえ、アカウントのロックアウトを防ぐために、2FAの取り組みを展開していくプロセスを設計しました。これから段階的に、複数のユーザーグループに2FA有効化の依頼をお送りします。対象のグループは、過去に実行したアクションや貢献したコードに基づき選出されます。



1. 所属グループが2FA有効化の対象として選ばれたものの、まだ有効化が行われていない場合は、2FA有効化の期限を知らせる通知メールが届きます。また、2FAの設定方法に関する情報や推奨されるベストプラクティスが送られます。通知メールは期限の約45日前に送信されます。
<詳細>

    - 2FA有効化のスケジュールが決まると、GitHub.comで毎週リマインダーのバナーが表示されるようになり、そのバナーから2FA登録を進めることができます。
    - 加えて、2FA有効化の期限を知らせるメールも不定期で届きます。
2. 有効化の期限が過ぎると、毎日GitHub.comへの初回アクセス時に2FAの有効化を求められます。このプロンプトは、ユーザーが都合のよい時に対応できるよう、1日1回、最長で1週間スヌーズ機能で繰り返し再表示させることができますが、1週間が経過した後は、2FAを有効化するまでGitHub.comにアクセスできなくなります。
   <詳細>
    - この1週間のスヌーズ期間は、有効化の期限が過ぎた後、初めてGitHubにアクセスした時に始まります。休暇中にGitHub.comからロックアウトされることはありません。
3. 2FA有効化の28日後、GitHub.comを使用中に、2FA設定が正常に機能しているかを検証する2FAチェックアップを実行するよう求められます。過去にサインインしたユーザーは、登録中に2番目の要素を誤って設定したり紛失したりした場合、2FAを再設定できます。

ユーザーのプロジェクトが軌道に乗る、あるいはユーザーが重要なリポジトリのメンテナーになった場合、前触れなく、既に2FA有効化スケジュールが始まっているグループの対象者になることがあります。その場合、45日の2FA設定期間が翌日から開始され、上記と同じスケジュールで進行します。

ソフトウェアサプライチェーンのセキュリティ確保はチーム作業

オープンソースのソフトウェアは普及率が高く、90%の企業が自社開発のソフトウェアにオープンソースを使用していると報告しています。GitHubはオープンソースのエコシステムで重要な位置を占めているからこそ、アカウントのセキュリティ確保を重視しています。強力な認証機能と2FAの採用は、ベストプラクティスして長年にわたり認められているため、GitHubでは、ソフトウェアサプライチェーン保護の一環として、このベストプラクティスを広く展開する義務があると考えています。

GitHub Blog
英語:
https://github.blog/2023-03-09-raising-the-bar-for-software-security-github-2fa-begins-march-13/

日本語:
https://github.blog/jp/2023-03-17-raising-the-bar-for-software-security-github-2fa-begins-march-13/

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

GitHub NEWS RELEASE

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