

2023年7月18日
ギットハブ・ジャパン合同会社

GitHub、パスワードレス認証をGitHub.comに導入

～ パブリックベータ版でパスキーの利用が可能に ～

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、2023年7月12日 (米国時間)に、GitHub.comにパスワードレス認証を導入したことを発表しました。

GitHubは、ユーザーエクスペリエンスを損なうことなく、すべての開発者が強固なアカウントセキュリティを担保できるよう支援しています。[GitHub全体の取り組みは2FA\(2要素認証\)から始まり](#)、本日、パスキー認証をパブリックベータ版として公開するに至りました。

パスキーの利用を開始するには、オプトインを許可し、セキュリティキーをパスキーにアップグレードすることで、パスワードと2FA方式から、パスキーへ変更されます。

多くのセキュリティ侵害は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、認証情報の盗用もしくは漏洩、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、低コストな攻撃によるものです。実際、我々が頼りにしているパスワードは、[データ漏洩の80%以上](#)の根本原因となっています。

パスキーは、従来のセキュリティキーの機能をベースに、より簡単な設定と強化された復元性を加えたものです。安全性と利便性に優れた方法で、アカウントがロックアウトされるリスクを最小限に抑えながら、アカウントを保護することができます。パスキーによって、パスワードに基づく侵害の根絶という、パスワードレス認証の実現に近づくことができます。

GitHubアカウントでのパスキー利用方法

GitHubアカウントでパスキーを有効にするには、右上のプロフィール写真をクリックして「Feature Preview」メニューを開きます。次に、「Passkeys」を選び、「Enable」をクリックします。パスキーを有効化できた後、有効なセキュリティキーをパスキーにアップグレード、あるいは新しいパスキーの登録が可能になります。

https://github.blog/wp-content/uploads/2023/07/register_key.mp4?_=1

最新のデバイスは、最初からパスキーをサポートしているため、パスキーを設定するのみで利用が可能になります。パスキーが有効化されている場合、サインイン時にブラウザでパスキーの設定が可能かどうかを確認されます。設定済みのデバイスに、まだパスキーが設定されていない場合は、設定を依頼するメッセージが表示され

ます。堅牢で安全な認証情報をすべてのデバイスに登録することで、デバイスの紛失によるアカウントのロックアウト防止につながります。

パスキーがパスワードの代わりになる仕組み

GitHub.comのパスキーにはユーザー認証が必要です。つまり、2つの要素を1つの要素としてカウントします。2つの要素とは、ユーザー自身またはユーザーが知っているもの(指紋、顔、PINなど)、もしくはユーザーが持っているもの(物理的なセキュリティキーやデバイスなど)です。この強力な認証により、GitHubはパスワードが無くても、ユーザー本人がサインインしていることを確認できます。また、ブラウザーサポートが拡張されたことにより、ブラウザーの自動入力システムで、ログインページから直接パスキーを使ってサインインするよう自動的に提案できるようになりました。

https://github.blog/wp-content/uploads/2023/07/use_key.mp4?_=2

さらに、2FAを有効にしているユーザーだけでなく、すべてのユーザーがパスキーのみを使用してサインインすることができます。

複数のデバイス間でパスキーを使用する方法

パスキーは、設定したデバイスだけではなく、複数のデバイス間で使用することもできます。「デバイス間認証」という新たな認証方式では、スマートフォンの存在を確認することにより、スマートフォンやタブレットでパスキーを使ってデスクトップにサインインすることができます。過去にリンクしたデバイスを選択するか、スマートフォンでQRコードをスキャンしてサインインを実行すれば、デスクトップ上ですべてのサインインが行われます。スマートフォンやタブレットは物理的にノートPCやデスクトップの近くにある必要があるため、デバイス間認証ではFIDO(ファイド:Fast Identity Online)のフィッシング耐性が保持されます。

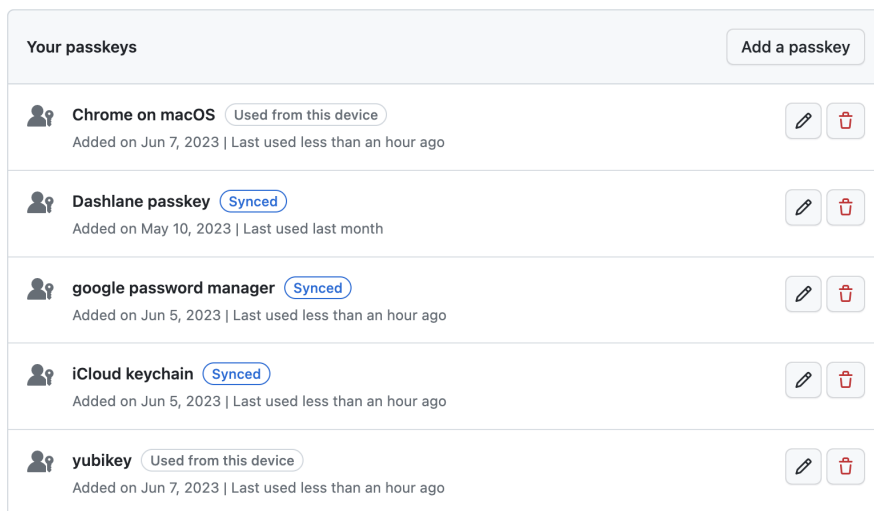
下記にて、実際の動作をご覧ください。

<https://prap.gigapod.jp/fa708760fdcd99beefe4992f08add58021b386316>

複数のデバイス間での使用に加えて、多くのパスキーはデバイス間での同期が可能であるため、キーを失くしたことによってアカウントからロックアウトされることがなくなります。パスキープロバイダーによっては、パスキーがデバイス間で自動的に同期されます。 iCloudアカウントではiOSからmacOSにパスキーが同期され、GoogleパスワードマネージャーではAndroidデバイス間で同期し、1PasswordやDashlaneのようなパスワードマネージャーは、インストールしたデバイス間でパスキーを同期させることができます。OSやブラウザーベンダー間の拡張同期サポートは現在対応を進めているところですが、核となる同期エンジンは既に存在しています。

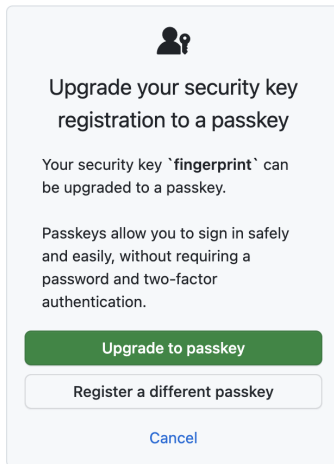
しかし、すべてのパスキーがデバイス間で同期されるわけではありません。ユーザー設定では、同期していると報告された認証情報に [Synced] というラベルが表示さ

れ、同期済みであることが確認できます。リスクモデルによっては、非同期のキーが望ましい場合もあるため、パスキーの設定の希望は、ユーザーが選択できます。



セキュリティキーをパスキーにアップグレードする方法

ご使用のGitHubアカウントのセキュリティキーをアップグレードすることで、その力をフルに発揮できる状態かもしれません。セキュリティキーが、ユーザー本人であることを確認できるもの(Touch ID、Windows Hello、Androidの指紋認証、PINロックされたキー、生体認証ハードウェアキー)である場合、アップグレードの対象となります。次に、そのセキュリティキーでサインインした時に、パスキーにアップグレードするかどうかを尋ねられ、パスキープロバイダーに再登録されます。この再登録により、認証時にパスキーが確実に検出され、サポートされている場合は同期されます。パスキーはプライバシーを保護するものであるため、正しい認証情報をアップグレードしていることを確認できるよう、アップグレード処理の中で何度かパスキーを入力しなければならない場合があります。処理が終わったら、パスワードのない環境の完成です。



詳細情報

GitHub.comの認証方法として、より高い柔軟性、信頼性、安全性を担保できるものを提供し続けたいと思っています。詳しくは、下記よりドキュメントをご確認ください。

<https://docs.github.com/ja/authentication/authenticating-with-a-passkey/about-passkeys>

GitHub Blog

英語:

<https://github.blog/2023-07-12-introducing-passwordless-authentication-on-github-com/>

日本語:

<https://github.blog/jp/2023-07-13-introducing-passwordless-authentication-on-github-com/>

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、すべての開発者のためのグローバルホームとして、安全なソフトウェアを構築、拡張、提供するための統合された開発者プラットフォームです。フォーチュン100社に採択された企業のうち90社に所属する開発者を含む1億人以上がGitHubを利用し、3億3千万以上のリポジトリで素晴らしいものを共に創造しています。GitHubのすべてのコラボレーション機能によって、個人やチームがより迅速に、より高品質なコードを書くことがかつてないほど容易になっています。

【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