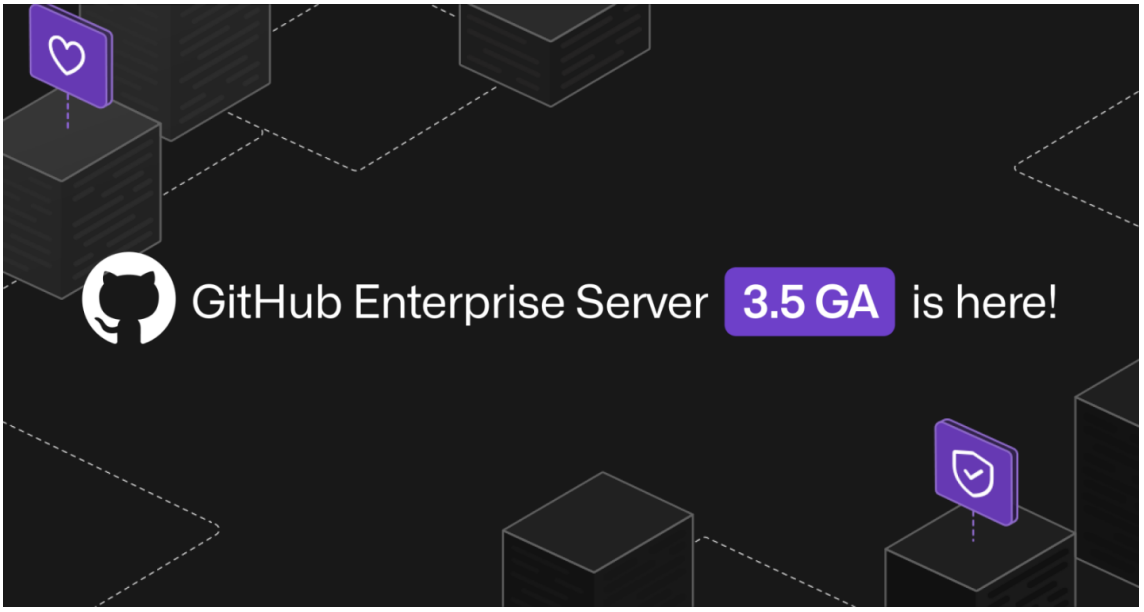
GitHub

NEWS RELEASE

2022年6月8日
ギットハブ・ジャパン合同会社

GitHub Enterprise Server 3.5をリリース

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31日（米国時間）に、GitHub Enterprise Server 3.5をリリースしたことを発表しました。今回のリリースでは、GitHub Container Registryへのアクセスの提供、Dependabotの追加、管理者機能の強化、さらにGitHub Advanced Securityの機能が追加されました。



GitHub Enterprise Server 3.5では、ソースコードを安全に維持するためのセキュリティ機能の追加、開発者エクスペリエンスのアップデート、自動化機能の追加に注力すると共に、GitHub Advanced Securityのアップデートも加え、60を超える新機能が追加されました。

最新バージョンはこちらからダウンロードいただけます。

GitHub Enterprise Server 3.5の機能紹介

GitHub Container Registryをパブリックベータ版で提供開始

昨年GitHub Container RegistryをGitHub Packagesでリリース以降、数千個のコンテナの公開や管理にレジストリが使用されています。また、このようなコンテナの利用回数は毎日数百万回にも上ります。

GitHub NEWS RELEASE

GitHub Enterprise Server 3.5以降で、GitHub Container Registryにアクセスできるようになりました。この機能は、管理者がManagement Consoleで有効化できます。今回のリリースにより、次のことが可能になりました。

- Organization内のコンテナに対してきめ細かい権限制御を設定する。
- Organization内のコンテナに対して、"プライベート"と"パブリック"の他に"インターナル"表示を設定する。
- データをOrganizationレベルで共有する。これにより、帯域幅とストレージの要件が削減されます。
- より緊密なGitHub Actionsワークフローとのインテグレーションを実現し、GITHUB_TOKENを介してワークフローからコンテナに安全にアクセスする。
- パブリックコンテナに匿名でアクセスする。これにより、認証情報を提供することなくパブリックコンテナにアクセスできます。
- Open Container Initiative (OCI)イメージを格納して管理する。

Dependabotの提供を開始

GitHub Enterprise Serverインスタンスをホストしているすべてのユーザーが、Dependabotを利用できるようになりました。Dependabotは次の3つのサービスで構成されています。

- **Dependabot**アラート：依存関係の脆弱性が検出されると、瞬時にアラートを送ります。
- **Dependabot**セキュリティアップデート：リポジトリに対するPull Requestを開くことで、脆弱性の検出時に依存関係がパッチ適用済みバージョンにアップグレードされます。
- **Dependabot**バージョンアップデート：Pull Requestを使ってすべての"依存関係を最新の状態で維持できます。これにより、脆弱性に対応できるだけでなく、旧バージョンから抜け出せなくなる可能性を軽減します。

Dependabotに関する詳細情報と、GitHub Enterprise Serverインスタンスでのセットアップ方法については、「Enabling Dependabot for your enterprise (Enterpriseの Dependabotの有効化)」と「Enabling the dependency graph for your enterprise (Enterpriseの依存グラフの有効化)」をご覧ください。

GitHub Actions

再利用可能なワークフローの提供を開始

再利用可能なワークフロー(正式には"テンプレート")は、一元管理されるワークフローの重要なコンポーネントです。この機能により、ワークフロー全体をまるでGitHub Actionsのように再利用できます。リポジトリ全体でワークフロー定義をコピーして貼り付ける代わりに、一行設定するだけで既存のワークフローを参照できます。

GitHub NEWS RELEASE

キャッシュサポートの提供を開始

GitHub Actionsを使用すると、ワークフローの中間出力と依存関係をキャッシュできます。これは、ジョブを高速化する効果的な方法です。

セルフホストランナーグループを特定のワークフローに制限

特定のEnterpriseおよびOrganizationのランナーグループにアクセスできるリポジトリを制限するだけでなく、管理者は特定のワークフローファイルとバージョンを選択して、アクセスをさらに詳細に制御できます。この機能を再利用可能なワークフローと組み合わせることで、Organization内でより安全な標準ワークフローを作成できます。

セルフホストランナーで自動アップデートを無効化

セルフホストランナーがソフトウェアアップデートを実行するタイミングをより細かく制御できるようになりました。ランナーに--disableupdateフラグを指定すると、新しいバージョンのランナーを利用できる場合でも、自動ソフトウェアアップデートの実行を試みることはありません。これにより、ユーザーの予定に合わせてセルフホストランナーをアップデートできます。特に、セルフホストランナーがコンテナ内にある場合に便利です。

Enterpriseの管理者向け

メンテナンスのための**IP**許可リスト

GitHubは、メンテナンス設定に新しいオプションを導入しました。これは、GitHub Enterprise Serverを健全な状態で維持し、メンテナンスモード中に何らかの運用変更が発生した後も本番環境のトラフィックを処理するためのオプションです。この変更により、管理者は、特定のIPアドレス セットに対してのみアプライアンスへのアクセスを許可できます。

GitHub Enterprise Serverの統計

プラットフォームの利用状況を把握するために、GitHub Enterprise Serverの指標を41個収集できるようになりました。こうした指標によって、ユーザーによる製品の利用状況についての洞察を得ることができ、チームによる運用状況もわかります。さらに、GitHub Enterprise Serverのあらゆる側面から最大限の価値を得られます。

セキュリティ

Audit logの対象に加わった**git**イベント

3つの新しいイベント(git.clone、git.fetch、git.push)が既存のAudit logイベントと共に組み込まれ、UIを介した検索、JSON/CSVを介したエクスポート、APIとストリーミングを介した検索に利用できます。Audit logを通じて、自分のアカウントでのUIおよびCLIアクティビティを、より詳細に監視できるようになります。これにより、管理、コンプライアンス、セキュリティ対応に関するニーズをより適切に満たすことができます。

GitHub NEWS RELEASE

GitHub Advanced Securityに含まれる機能

現在パブリックベータ版で提供されているSecret ScanniongのPush保護機能によってシークレットの漏洩を阻止

GitHub Advanced Securityを利用しているユーザーは、シークレットが含まれるPushをブロックできるようになりました。Push保護機能は、高度に識別可能なシークレットをスキャンし、その偽陽性率は1%未満です。開発者は識別されたシークレットを確認して削除するか、必要に応じてブロックを回避できます。詳細については、「Protecting pushes with secret scanning (シークレットスキャンでプッシュを保護する)」をご覧ください。

セキュリティ概要のOrganizationレベルビューの提供を開始。Enterpriseレベルビューのパブリックベータ版では、セキュリティリスクを数値化

GitHub Advanced Securityを利用しているユーザーは、OrganizationとEnterpriseの両レベルでセキュリティ概要にアクセスできます。セキュリティ概要はセキュリティ結果を集約し、リポジトリ中心のビューとアラート中心のビューでのSecret Scanning、Dependabot、Code Scanningの結果を表示します。

Secret ScanningがOrganizationレベルおよびリポジトリレベルのドライランに対応(パブリックベータ版)

品質に問題のあるカスタムパターンでは、Organizationまたはリポジトリ全体で数千件もの結果が生成される場合があります。この問題を解決するために、GitHub Advanced Securityをご利用のお客様は、公開前にスキャン機能をドライランできるようになりました。ドライランはOrganizationレベルおよびリポジトリレベルで使用でき、パブリックベータ版で提供されています。

CodeQLがさらに多くのセキュリティ問題を検出し、新しい言語バージョンに対応

GitHub Advanced Securityを利用しているユーザーは、新言語のサポート、多数のCWEに対応する検出機能の強化、パフォーマンスの向上など、CodeQLに対する幅広い機能改善のメリットを享受できるようになりました。詳細はこちらをご覧ください。

GitHub Enterprise Server 3.5のすべての新機能に関する詳細については、リリースノートをご確認いただくか、ダウンロードしてください。ご使用のGitHub Enterprise Serverが最新バージョンでない場合は、アップグレードアシスタントを使用して、現在のバージョンのGitHub Enterprise Serverから目的のバージョンへのアップグレードパスをご確認ください。

GitHub Blog
英語:
https://github.blog/2022-05-31-github-enterprise-server-3-5-is-now-generally-available/

日本語:
https://github.blog/jp/2022-06-07-github-enterprise-server-3-5-is-now-generally-available/

GitHub NEWS RELEASE

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