# GitHub Advanced Security の活用法

”開発組織のセキュリティ課題を解決するための　Tipsコードの安全性を高めるための
最新ツールとベストプラクティス ”

2024年10月15日


Yuichi Tanaka
Principal Solution Engineer

Shota Sando
Enterprise Sales, Director

イントロダクション

開発組織が直面する課題

GitHub Advanced Securityが目指すあり方

導入方法・ケーススタディ

質疑応答

# イントロダクション

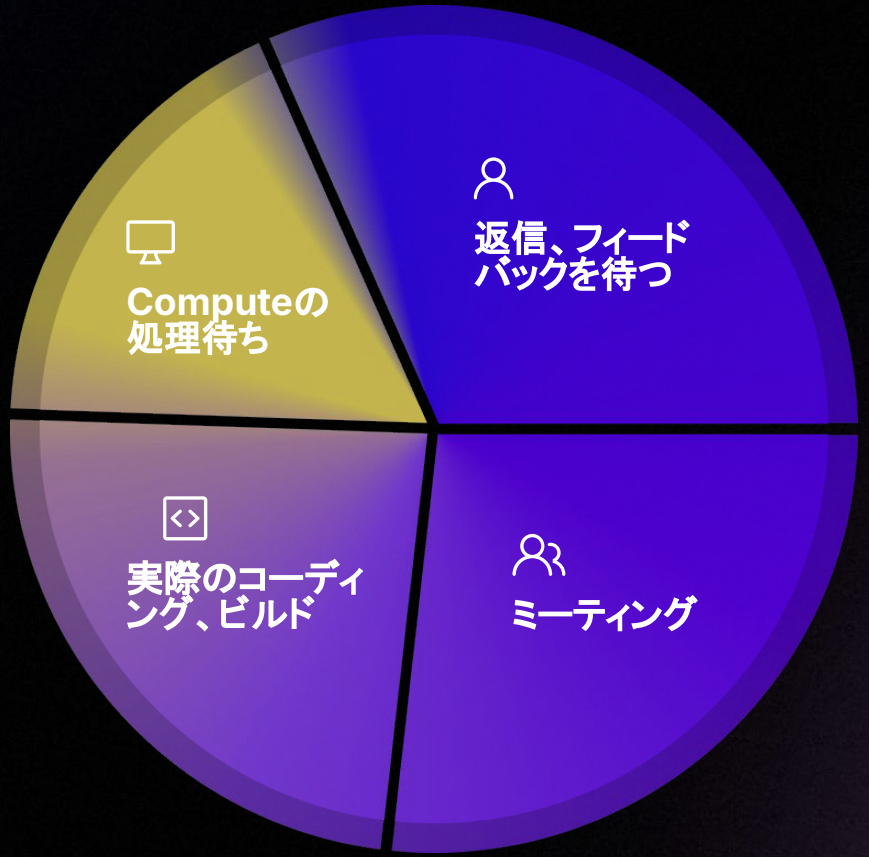
# What is GitHub
# "It is all about empowering developers"

1. **コラボレーションの促進** : GitHubは、チームやコミュニティが共同でプロジェクトを進めるためのプラットフォームです。これにより、開発者同士が意見を交換し、共同作業を行いやすくなります。

2. **学びの機会** : GitHubにはオープンソースプロジェクトが数多く存在し、開発者はこれらのプロジェクトを通じて新しい技術やベストプラクティスを学ぶことができます。

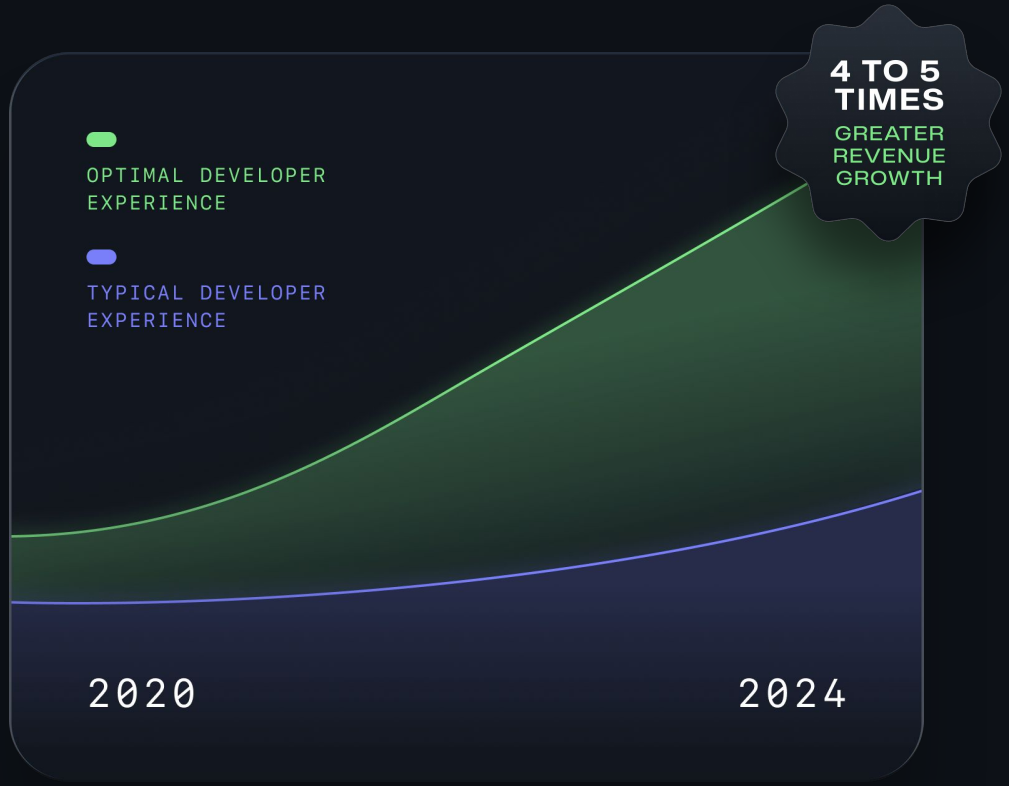
3. **成長の支援** : GitHubは、開発者が自分のスキルを向上させるためのリソースやコミュニティを提供し、キャリアの成長を支援します。

# A day in the life of a developer



# 開発者体験
# が違いを生む

マッキンゼーの調査によると、開発者の労働環境が改善された企業は、競合他社に比べて4〜5倍の収益成長を達成している。



# 開発組織、開発者の生産性をコンポーネント

Team ← Productivity → Individual

GitHub Enterprise

- セキュアに保管
- コラボレーション向上
- ワークフロー自動化
- スケーラビリティ
- パフォーマンス可視化
- 開発エコシステムの効率化
- 教育と知識の共有

GitHub Advanced Security

- セキュリティーの自動化
- 迅速な修正
- 継続的なセキュリティー評価
- 規制遵守の支援
- 教育と意識の向上
- シフトレフトの開発文化

GitHub Copilot

- コーディング効率化
- 学習のサポート
- エラーの削減
- コードの再利用
- レビューの簡素化
- プロジェクトスピード
- 新しい技術の吸収によるコードの柔軟性

# アプリケーション セキュリティーの今

セキュリティリスク

**アプリケーション** が攻撃ベクターの第1位。

侵害の80%はWebアプリケーションの悪用によって発生している。

Verizon Data Breach Investigations Reports 2023

停滞するプロセス

**発見された脆弱性の87% は、9ヶ月後も存在している。**

最初の271日間に発見され、修復された脆弱性はわずか13%。

メンド・オープンソース・リスク・レポート 2022

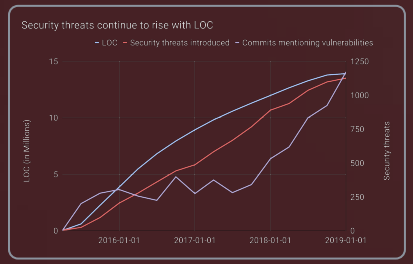
より高い効果を求めて

**AI-powered security** はより大きなROIを提供すると組織は考えている。

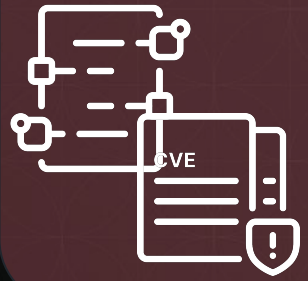
84%の経営幹部が、従来のサイバーセキュリティ・ソリューションよりも生成AIサイバーセキュリティ・ソリューションを優先する予定。

IBM CEO's Guide to Generative AI、2023年

# 増加するセキュリティー侵害リスク




**コードの量**：開発者が作成するコードの量が膨大で、手動での脆弱性検出が困難。特に、アジャイル開発やデブオプス（DevOps）環境では、コードが頻繁に更新されるため、スキャンやレビューが追いつかないことが多いです。




**優先順位付けの難しさ**：脆弱性が発見されても、その深刻度や影響度に基づいて優先順位を付けるのは難しく、リソースをどこに集中させるべきか判断が求められます。

**人員不足**：AppSec専門家は需要が高く、優秀な人材を確保するのが難しいため、チームが人手不足になることが多い。このため、既存のメンバーが多くのタスクを抱えることになります。

**ツールの活用**：自動化ツールや静的解析ツールを導入している企業もありますが、それでも誤検知や偽陽性の問題があり、全ての脆弱性を適切に評価・修正するのが難しいです。

# 6億3000万円

**日本での平均データ侵害により発生するコスト**

---

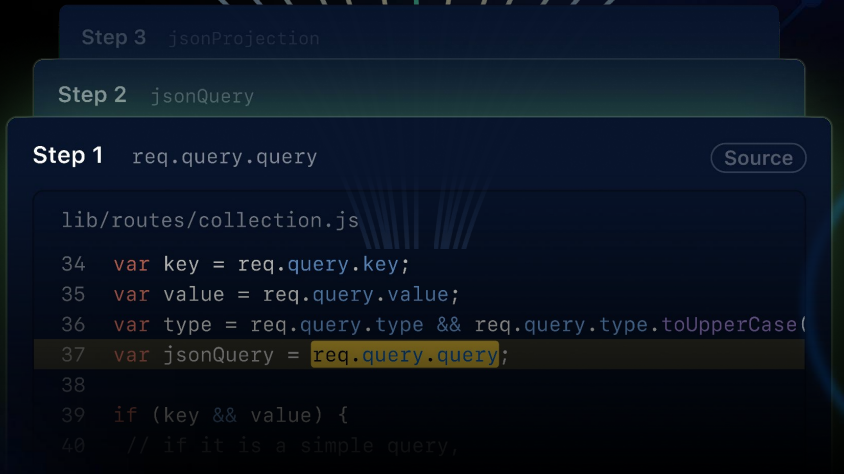
# 1/3

3分の1以上がシャドー・データ
（管理されていないデータソースに保存されたデータ）に関与

出典 - IBM: 2024年データ侵害のコストに関する調査

# 検出するだけでは十分ではない

組織には、検出したもののまだ修復できていない**脆弱性**がバックログに何千もある。



# 開発組織が直面する課題

# 現代のソフトウェアに求められる品質特性

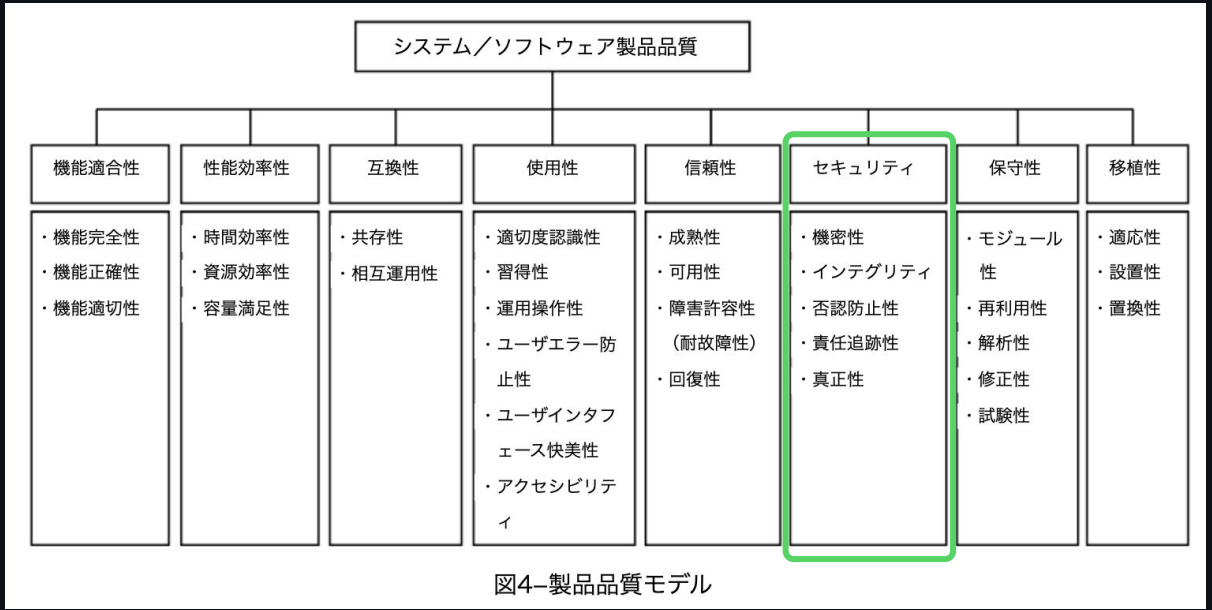


図4–製品品質モデル

JIS X 25010より引用

https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS+X+25010%3A2013

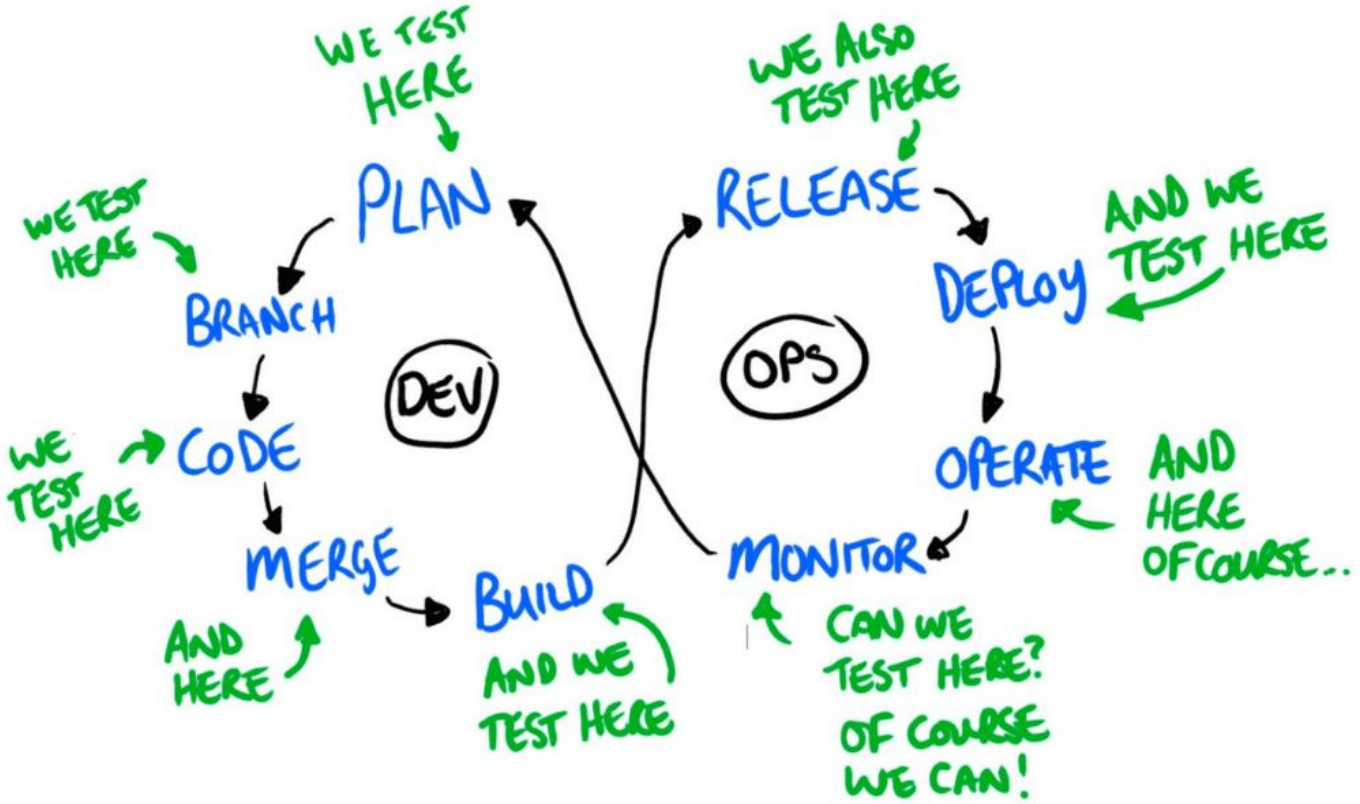
コード解析やテスト自体が
ソフトウェアの品質を
向上させるわけではない

“

**「テストフェーズ、テストプロセスによって質を上げる、
あるいは保つのではなくて、開発プロセス全体の中で
取り組んでいくことが重要です。
そもそも後からテストをする時代ではなく、
全体から質を作り込んでいくことが今の主流です（後略）」**

「品質とスピードに関する16の質問に答えてみた」

https://pr.forkwell.com/tech_event_reports/test-study-01/#toc-23




https://pr.forkwell.com/tech_event_reports/test-study-01/#toc-23

# 開発組織の責務

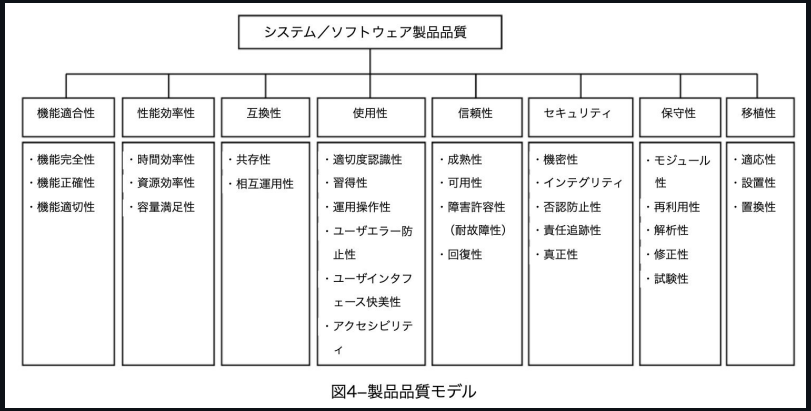
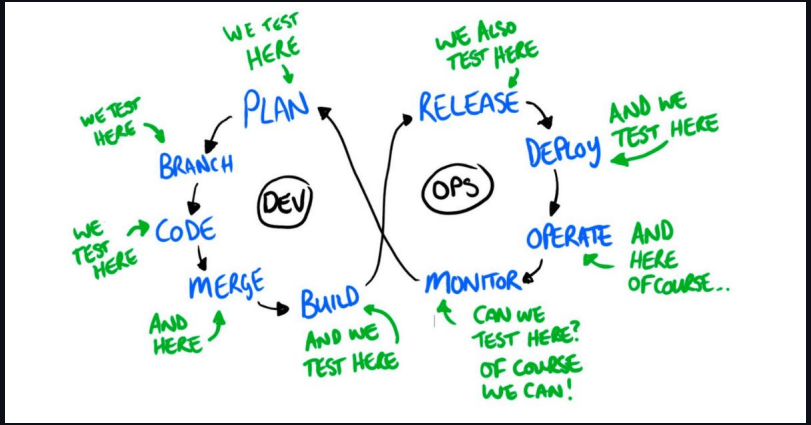
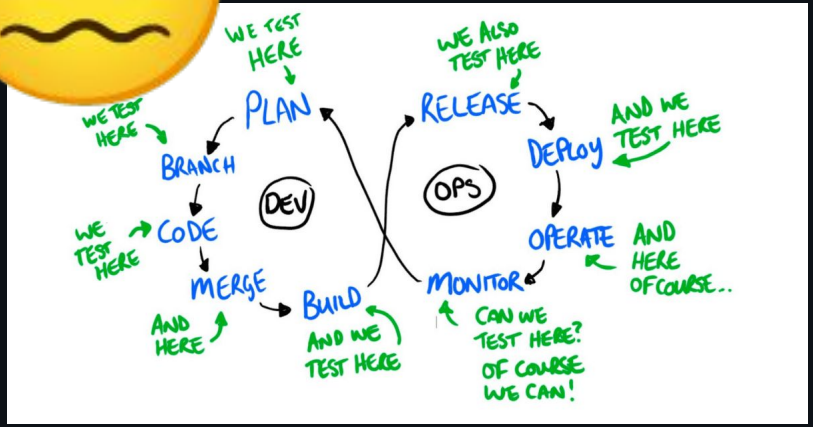


図4–製品品質モデル



# 開発組織の責務

図4–製品品質モデル



# GitHub Advanced Security が目指すあり方

# Found means fixed

GitHub Advanced SecurityはCopilotの技術を活用して、コード解析によって検出された脆弱性に対して、修正の提案を作成し、脆弱性の解消を促進します。

### リスクの低減

- これまでに見つかった脆弱性に対してキャンペーンを設定することで、優先して取り組むものを明確にする
- セキュリティ負債を減らし脆弱性が悪用される可能性を低減

### 開発者の生産性の向上

- GitHubでの開発フローに自然に統合された形で脆弱性の説明と修正提案が提示されるため、開発者のスキル向上にも有効
- 開発スピードを犠牲にすることなくリスクを減らす

### セキュリティと開発の調和

- セキュリティチームの要件を満たすと同時に、開発者の革新とスピードをサポートする
- セキュリティ負債の増加を抑制し、新たなリスクを削減する

# Dependabot

脆弱な依存関係を検知し修正提案を作成

### 自動的に脆弱性を検知し、修正提案となるプルリクエストを作成

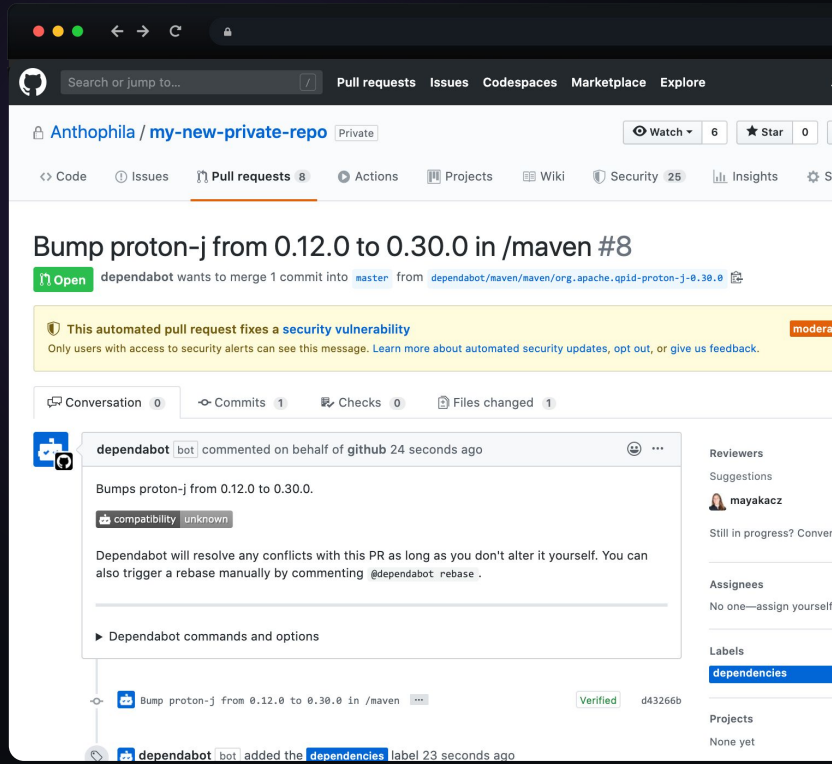
みなさんのリポジトリを常時監視し、脆弱な依存関係が見つかり次第、アラートするだけでなく、その脆弱性が修正されているバージョンにアップデートするためのプルリクエストを自動で作成。

### 開発ワークフローに統合

プルリクエストという、開発者が通常の変更で使うワークフローがそのまま依存関係の脆弱性の修正にも使われます。

### 豊富な脆弱性データ

GitHub自身でGitHub Advisory Databaseという脆弱性データベースを管理・公開しています。このデータベースに新しい脆弱性情報が追加・レビューされるたびにその依存関係を使っているリポジトリに通知




GitHub Advanced Security

# Code scanning

みなさんのコードの中の脆弱性を検知して修正を提案

### 脆弱性を即座に検知・修正

メインのコードベースにマージする前にソースコード内の脆弱性を検知することで、製品に脆弱性が入り込むのを抑止

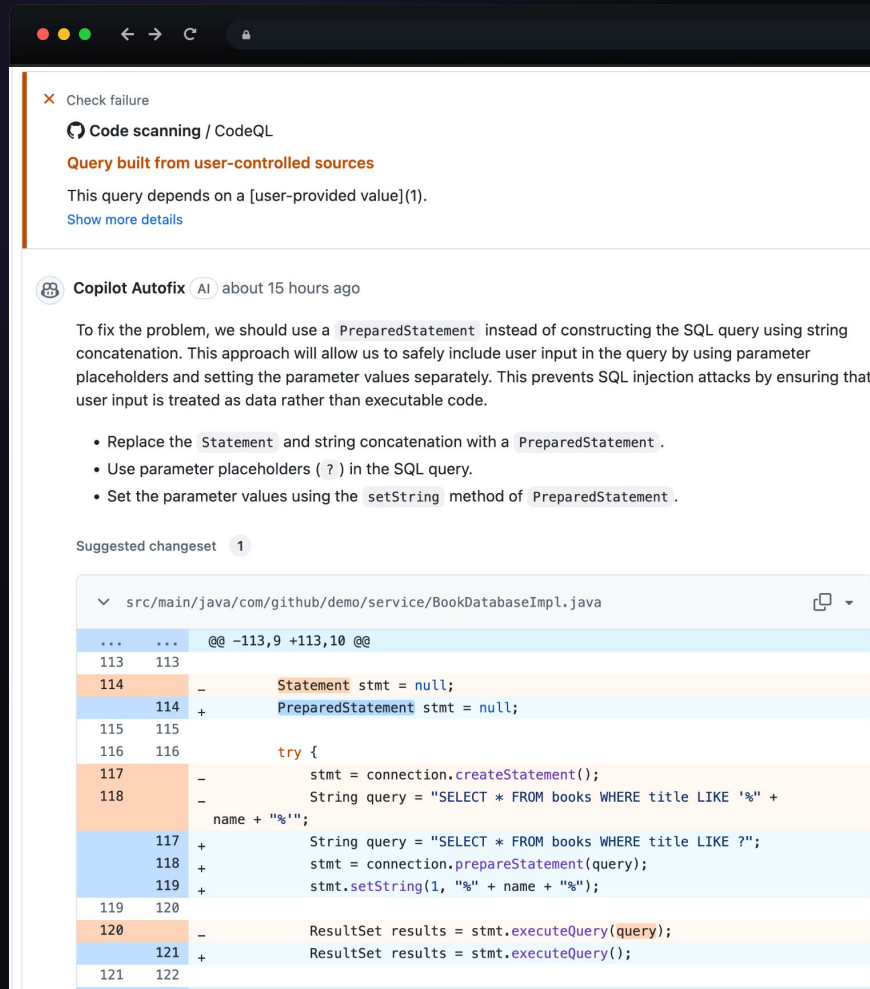
### 修正提案も合わせて作成

生成AIの力を活用し、脆弱性の指摘に加え、それを修正するための変更提案も同時に作成

### 開発ワークフローに統合

プルリクエストの中で解析結果の指摘や修正提案が提示されるため、開発者は普段通りの開発ワークフローでより安全なソフトウェアを構築が可能に

GitHub Advanced Security



# Secret scanning

ハードコードされたシークレットを検知

### 可能な限り早い段階でシークレットを検知

GitHubにコードをpushするたびに、ハードコードされたシークレットが含まれていないかどうかを解析し、見つかった場合には即座に管理者とpushした開発者に通知

### さまざまなパターンに対応

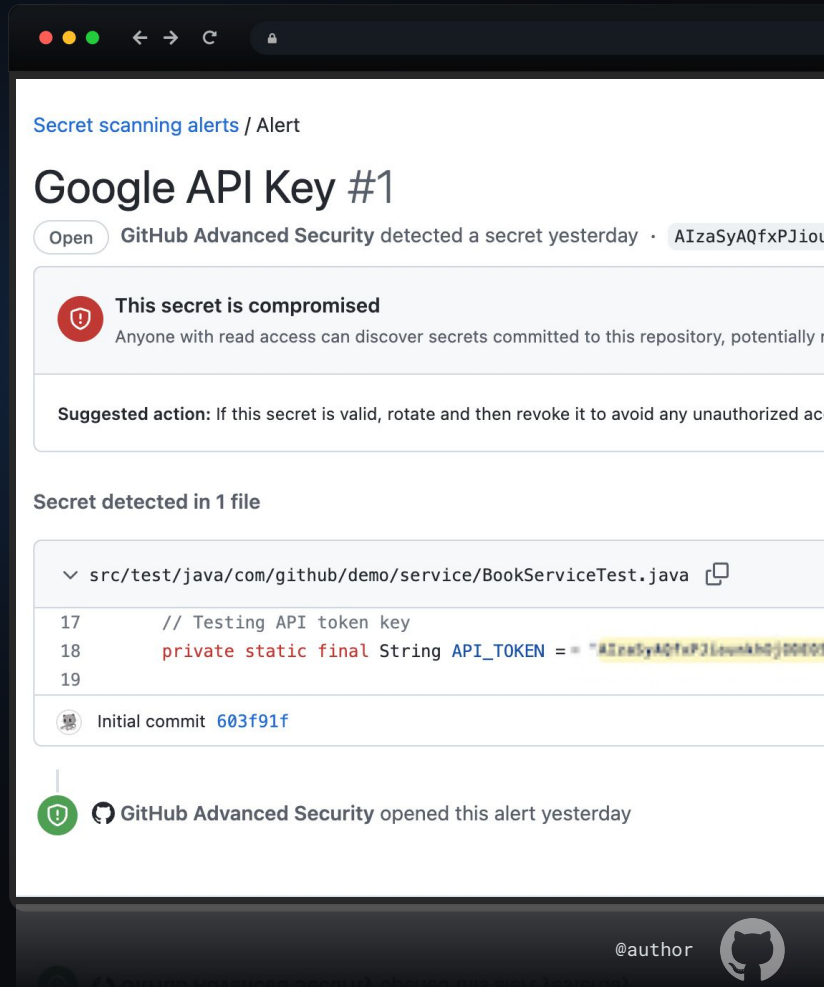
SaaSやIaaSサービスのトークンだけでなく、AIによるシークレット文字列の検知や、みなさまご自身でカスタムのパターンを追加することが可能

### Push protection

GitHubにコードをpushするタイミングで、シークレットを検知し、そのpushを拒否する設定も可能

### 一部のシークレットに関しては漏洩した事実をGitHub内で報告し、無効化することも可能

ハードコードされたシークレットは漏洩したものとして別のシークレットに置き換える作業を省力化





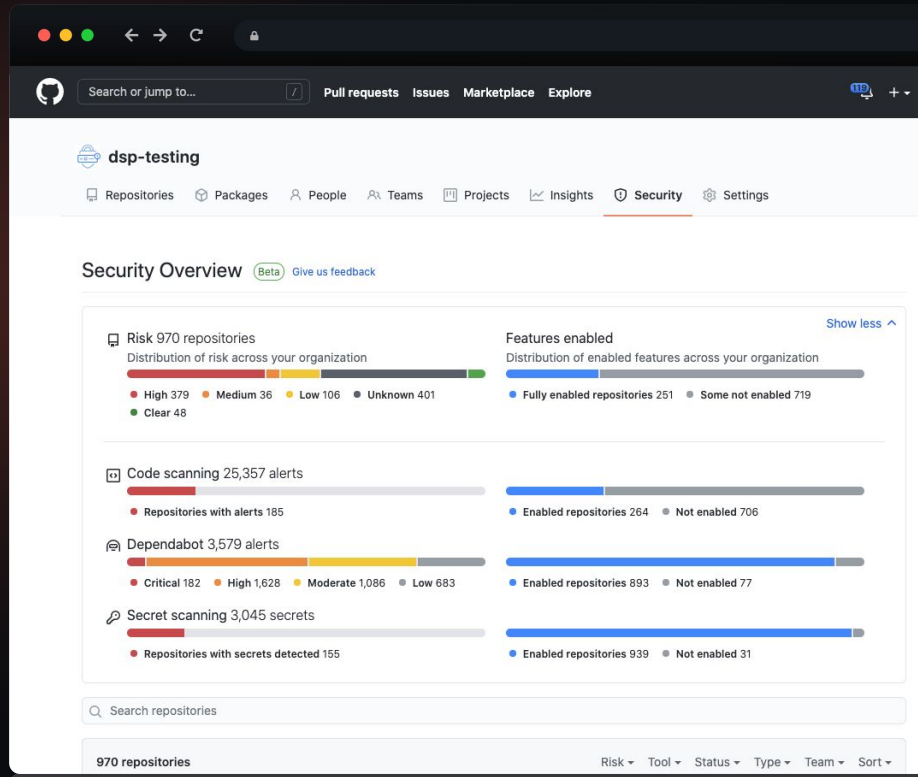

@author

# Security Overview

GitHub上のあらゆるセキュリティ機能の結果を集約するダッシュボード。アラート数の時系列の推移など、さまざまな観点を提供

リスクの高いリポジトリを特定することが可能

あるオープンソースライブラリに深刻な脆弱性が見つかった時に、自社内のどのリポジトリにその影響があるのかを調べることも可能






@author

# 導入方法・ケーススタディ

# 価格

Pay-as-you-go

**GitHub Enterprise**

**$21 USD**
per user/ per month

***GitHub Advanced Security**

**$49 USD**
per active committer
/ per month

GitHubは、ユニークユーザーライセンスモデルを使用し、GitHub Enterpriseの総ライセンスシート数を毎月課金。複数のデプロイメントオプション（クラウドとサーバーなど）をご利用の場合、GitHub はクラウドとサーバーのデプロイメントにまたがるユニークユーザー数に基づいてライセンスシート数を決定します。

*GitHub Advanced Security が有効になっているプライベートリポジトリで作業する一意のコミッター(共同作成者) に対して料金が課金。過去90 日間にこれらの有効化されたリポジトリに貢献したコミッター（コミットをプッシュした人）は、コミッター数にカウントされます

GitHub Professional/Expert Services

# Focus Areas

## Enterprise Foundation

Enterprise Foundation では、インストールとアップグレード、ユーザーとリポジトリのマイグレーション、GitHub と組織間のアクセスコントロールの実装をサポートします。

## Security & Compliance

GitHub のサービスは、特定のリポジトリに対する脆弱性検出の誤検出や偽陰性を減らすのに役立ちます。このサービスには、信頼性の高い結果を開発者コミュニティに確実に提供するための脅威モデリング演習やクエリのカスタマイズ・コンサルティングが含まれる場合があります。

GitHub Professional Services はお客様のVisionを実現するための支援サービスです

お客様の状況や目標に応じたソリューションを提供します

## CI/CD

CI/CDツールと統合するか、GitHub Actionsを使用してプラットフォームベースのCI/CDプロセスを確立します。組織のリスク許容度に基づいてビルドを成功させるためのベストプラクティスを組み込んでいます。

## Collaboration & Community

コラボレーションとコミュニティは、インナーソースとオープンソースの両方のコンポーネントを活用する開発に関するプラクティスを組み込んでいます。ベストプラクティスのコンサルテーション、コラボレーションのセットアップ、GitHubのイベントベースのリポジトリトリガーの使用に関する推奨事項が含まれます。

## Security & Compliance

GitHub のサービスは、特定のリポジトリに対する脆弱性検出の誤検出や偽陰性を減らすのに役立ちます。このサービスには、信頼性の高い結果を開発者コミュニティに確実に提供するための脅威モデリング演習やクエリのカスタマイズ・コンサルティングが含まれる場合があります。

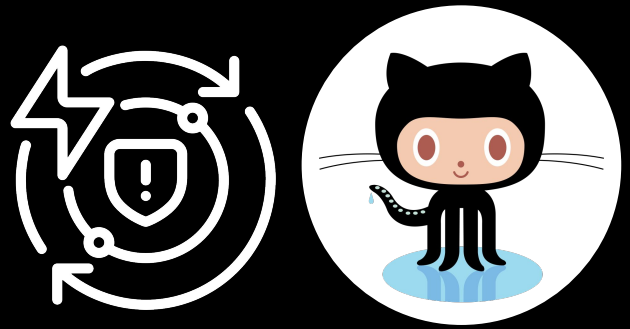
- 大手金融機関と提携し、**堅牢なシークレット管理プロセスを設計** し、包括的かつ実行可能な改善戦略を提供。これにより、オンプレミスからクラウドホストサービスへの移行に関する規制当局の承認を得ることができ、業務の効率化と市場投入までの時間の大幅な短縮を実現した。

- 大手製造業向けにカスタムCodeQLクエリをカスタマイズし、コードのセキュリティと品質基準を最適化。これにより、**コードレビューの迅速化** と**ISO標準**への準拠が実現し、開発サイクルの効率化が促進されました。

- 的を絞った技術的ガイダンスを提供することで、保険会社の**シフトレフト**を加速させた。セキュリティに早期にフォーカスすることで、脆弱性を大幅に削減し、開発者の生産性を向上させ、全体的な修復負担を軽減しました。

- 顧客に合わせたアドバイザリーサービスを提供し、**GHAS 導入計画の作成と実行** を指導した。定期的なレビューにより継続的な改善を保証し、セキュリティ態勢の測定可能な向上を促進し、手作業による介入に費やす時間を削減した。

# どのような企業が GHASにマッチしているのか？



**開発環境の統合**
GitHubを中心に開発フローを構築している企業は、 Advanced Securityの機能を直接統合することで、開発とセキュリティのワークフローを一元化 できます。

**DevOps文化の推進**
DevSecOpsを実現したい企業にとって、セキュリティを開発プロセスの 初期段階 から組み込むことができるため、効率的です。

**規模の大きなリポジトリ管理**
多数のリポジトリやコンポーネントを管理している企業は、 SASTやSCAの自動化機能により、脆弱性の早期発見 が可能です。

**コンプライアンス要件の遵守**
セキュリティ基準や規制に対応する必要がある企業は、 Advanced Securityの機能を利用してリスクを管理 できます。

**開発チームのセキュリティ意識の向上**
開発者がセキュリティを意識する 文化を育成 したい企業には、GitHub上でのリアルタイムなフィードバックが役立ちます。

# 質疑応答