SECURITY FOR APP BUILDERS @ LOFT #1

セキュリティのシフトレフト

吉田 裕貴 (Yuki Yoshida)

Solutions Architect
Amazon Web Services Japan G.K.

自己紹介

名前: 吉田 裕貴 (よしだ ゆうき)
所属: アマゾンウェブサービスジャパン合同会社
ISV/SaaS Solutions Architect

好きな技術領域: セキュリティ、運用の効率化

趣味: 筋トレ、バイク、旅、狩猟

本日お話すること

日々の開発の中でよく「セキュリティは重要です」と言われていて、理解もしています。けれど「セキュリティ対策は後回し」になりがちです。

しかし今、生成AIの登場によって状況は一変しています。

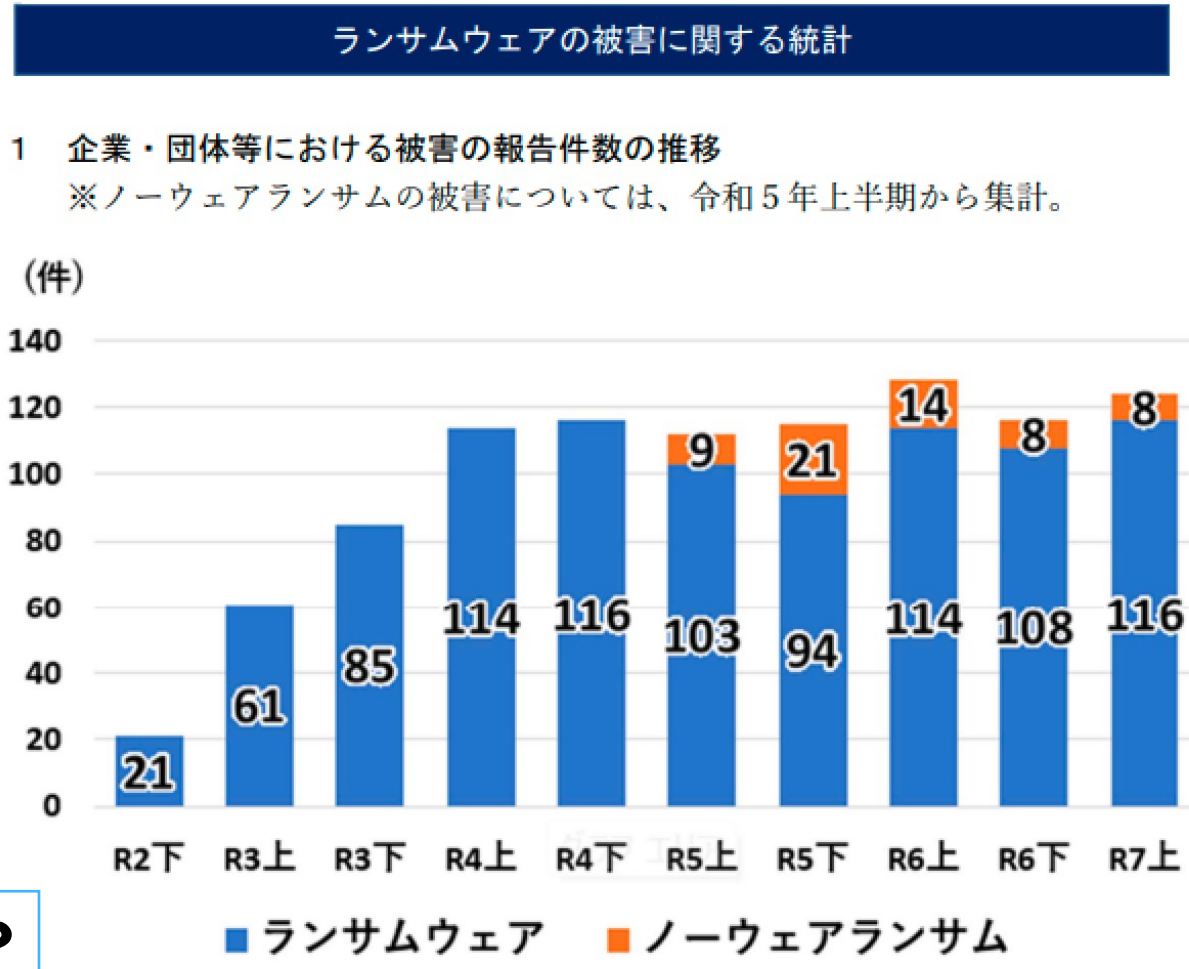
本日は、Amazon Q Developer や AWS の AI サービスを活用することで、**セキュリティの専門知識が少ない開発者でも、開発のライフサイクルにセキュリティを効果的に組み込む方法**をご紹介します。

令和7年上半期 サイバーセキュリティ動向

令和7年上半期のランサムウェア報告件数は 124 件となっています。

この数値の推移からもセキュリティ対策の継続的な強化が求められる状況が見えてきます。

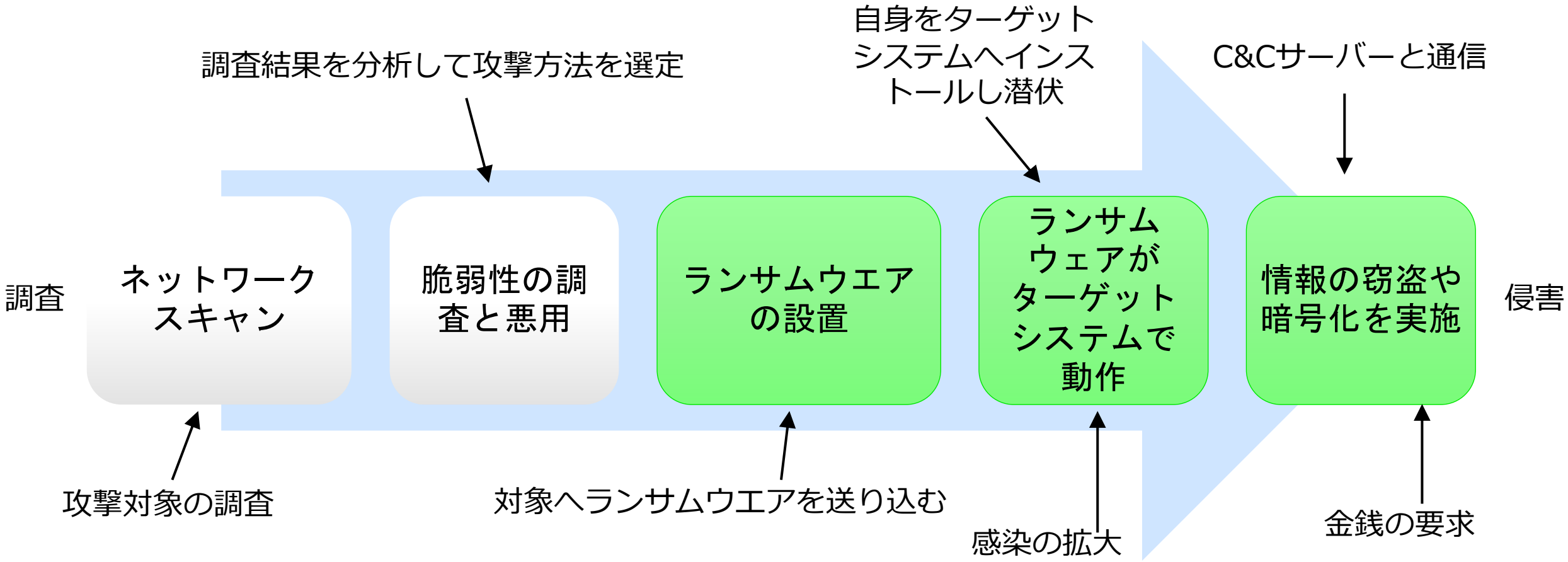
具体的に「何」を「どうやって」？



警視庁 令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について より抜粋

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

例) ランサムウエア（マルウエア）の感染経路



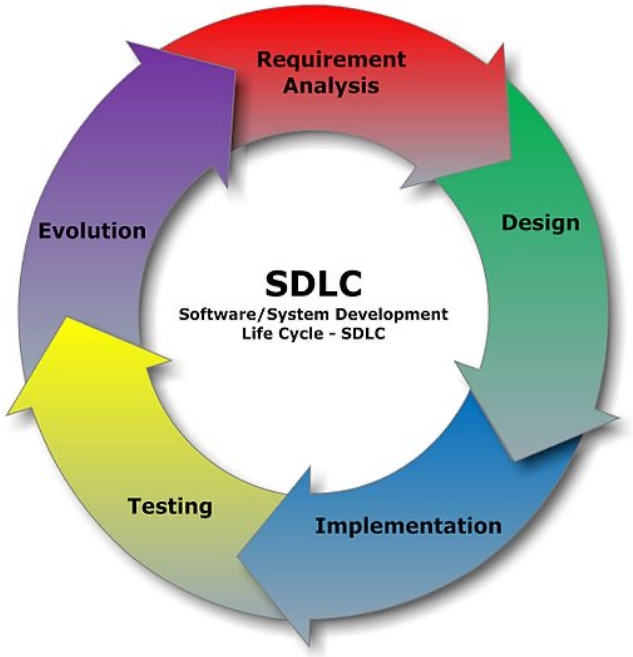
対象を調査し、脆弱な部分を利用して攻撃を仕掛けます。
つまり、これは**標準的なサイバー攻撃と同様の感染経路**

SHIFT LEFT - DevSecOps

シフトレフトとは、ソフトウェア開発ライフサイクル（SDLC）の早期段階でセキュリティ上の懸念に対処することを意味します

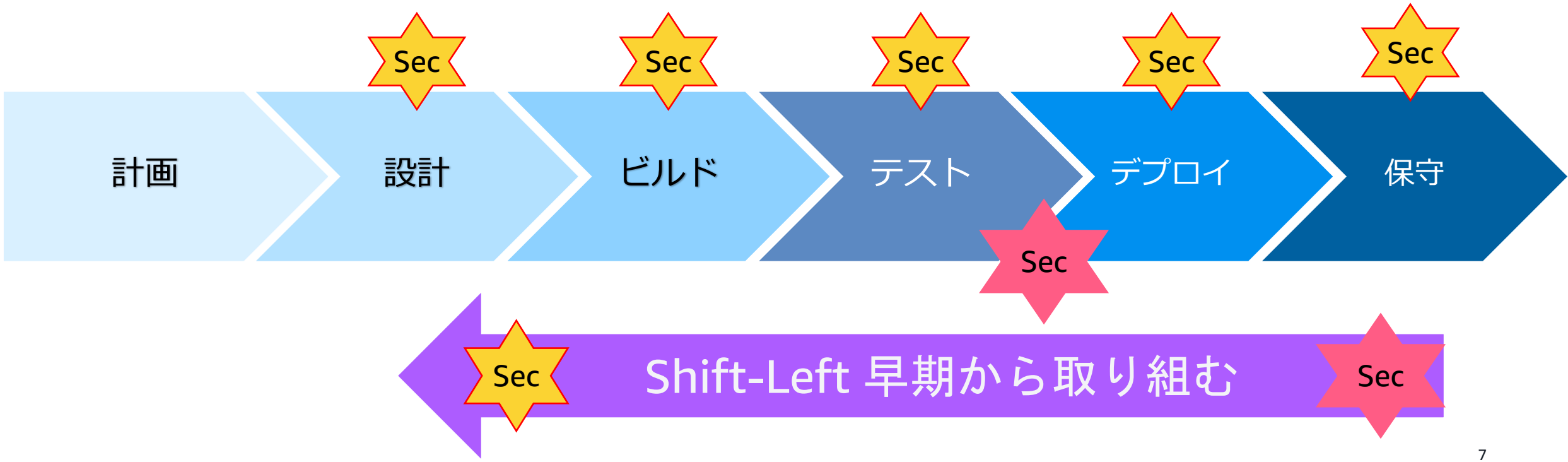
SDLC の各フェーズ

- Requirement analysis
- Planning
- Software design
- Software development
- Testing
- Deployment



SHIFT LEFT の価値

開発の早い段階でセキュリティを組み込むことで手戻りにかかる工数を削減する効果やセキュリティホールが見逃されて製品がリリースされるリスクを低減させる効果が期待できます。



DevSecOps を取り巻く状況の変化

DevSecOps 登場当時

開発者にセキュリティの専門知識を求める

ツールが出力する大量のアラートを手動で選別

セキュアコーディングの学習コストが必要

対応難易度が高い

2025年現在

AIと対話しながらリスクの本質を理解

Coding Agentが脆弱性を検出・修正案を提示

AI Agent が膨大なログから重要な情報を自動抽出

専門知識がなくても高品質なセキュリティ対応が可能に

Amazon Q Developer

開発者と IT 専門家がソフトウェア開発ライフサイクル（SDLC）全体を通してより迅速に構築できるよう支援

最も精度の高いコーディング推奨事項を提供

エージェントが自律的に機能実装、コードリファクタリング、ソフトウェアアップグレードなどを支援

Amazon Q は AWS の専門家であり、AWS 環境の最適化に精通

最高水準のセキュリティ脆弱性スキャンと修復機能を提供

Amazon Q はセキュリティとプライバシーを最初から考慮して構築されており、組織が生成 AI を安全に利用できるようにします

SDLC 全体を通した Amazon Q Developer の活用

調査

- 新規プロジェクトへより迅速に参加
- 新機能の計画立案
- AWS API の使用方法の理解
- 社内コードベースに関する質問

ビルド

- 対話型コーディングアシスタント
- ソフトウェア開発
- 対話型コーディング

テスト

- ユニットテスト生成によるテストカバレッジの向上
- セキュリティ脆弱性のスキャンと修復

デプロイ

- コードレビューの自動化
- デプロイリスクの評価
- ドキュメントの生成

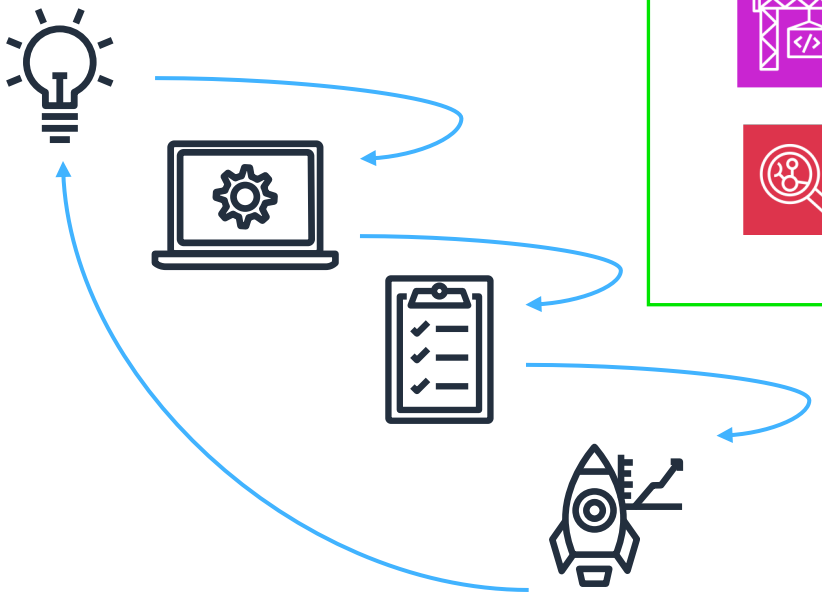
SDLC 全体を通した ツールの活用

設計 → ビルド → テスト → デプロイ& 保守

- SAST
- Secrets Detection
- Code Quality

- Test Code
- Document Maintenance

Amazon Q Developers



- SCA

AWS CodeBuild + 3rd party

Amazon Inspector

- Container scans

Elastic Container Service (ECR)

- Monitoring & logging
- Synthetic tests

Amazon CloudWatch

AWS CodeBuild + 3rd party

- DAST

AWS CodeBuild + 3rd party

- Monitoring & logging
- Synthetic tests

Amazon CloudWatch

AWS CodeBuild + 3rd party

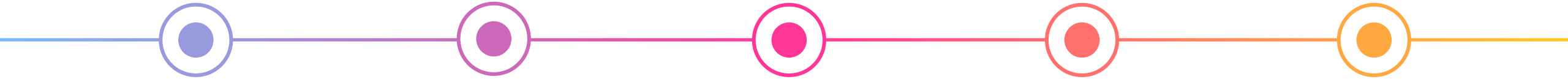
Amazon Inspector

参考: セキュリティ用語説明

SAST	Static Application Security Testing	ソースコードを静的に解析してセキュリティ脆弱性を検出する手法
DAST	Dynamic Application Security Testing	実行中のアプリケーションに対して外部からテストを行い、セキュリティ脆弱性を検出する手法
SCA	Software Composition Analysis	アプリケーションで使用されているオープンソースコンポーネントやサードパーティライブラリを分析し、セキュリティ脆弱性やライセンス問題を検出する手法

セキュリティトレーニング

AIを利用することで開発者にセキュリティを取り込んだ開発体験を



ガバナンスと
コンプライアンス

セキュアコーディング

リスク
マネジメント

コントロール

レジリエンス

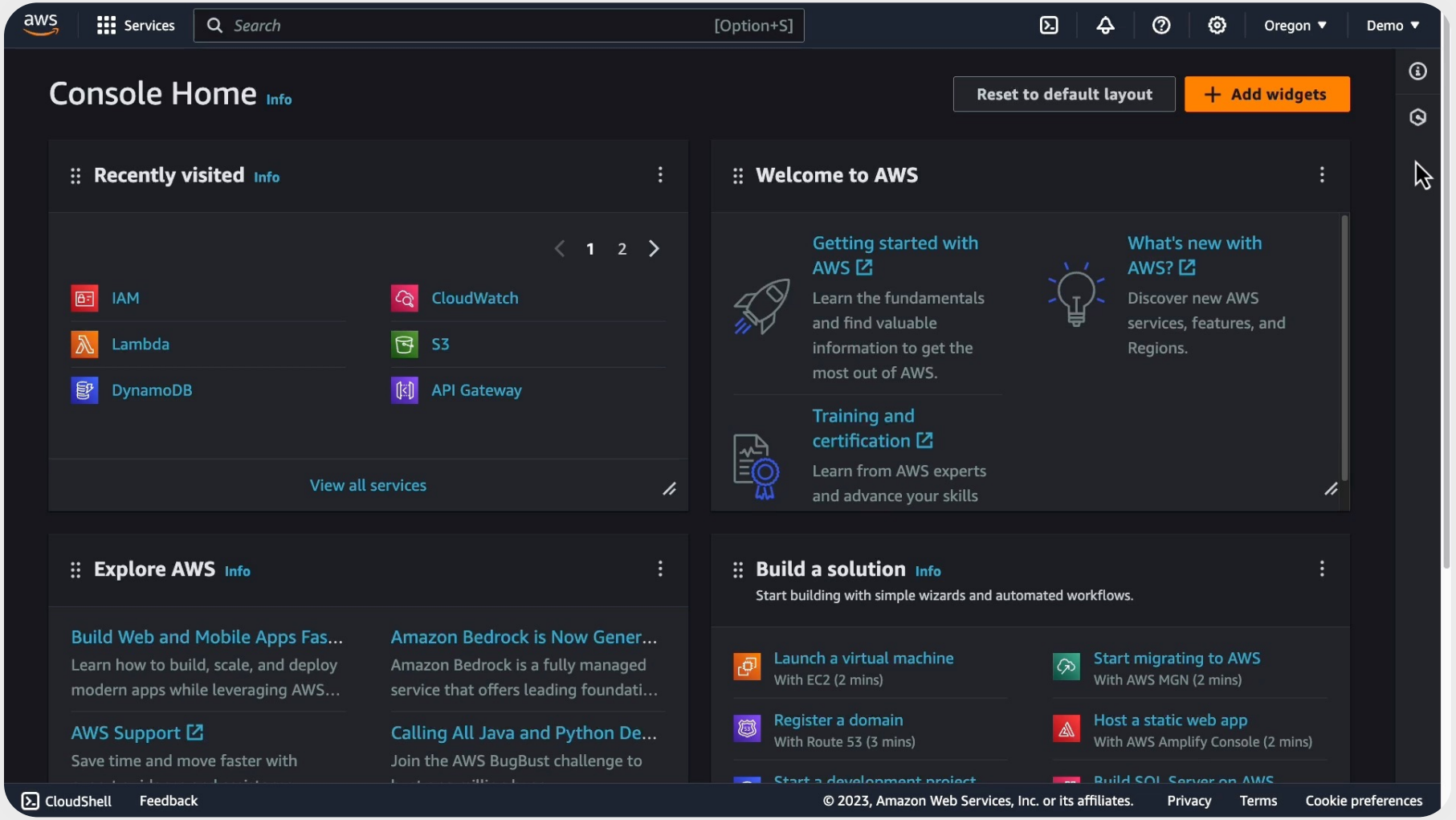
調査・設計を手助けする

Amazon Q Developers

- 利用するOSSのモジュールはセキュリティ的に安全か
  - すべてのモジュールのコード調査は人力で可能か
  - 生成AIによる静的なコード解析
  - 脅威モデリングの実施

「ビルダーのための脅威モデリング」でご紹介した内容になります

設計

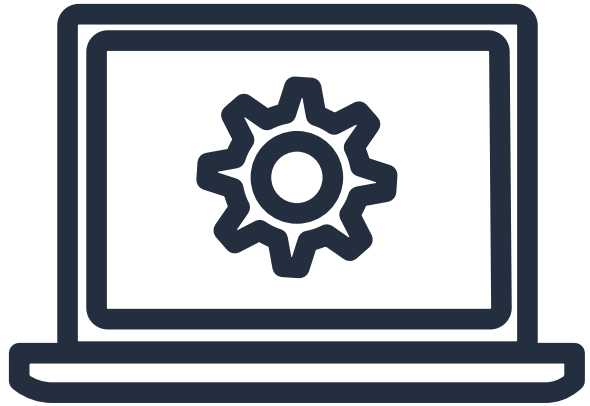


AWS の 17 年分の知識、ベストプラクティス、および Well-Architected のアドバイスに基づいて質問とガイダンスを取得

お客様のデータやシステムなどを活用して、ビジネスに特化したアプリケーションを作成

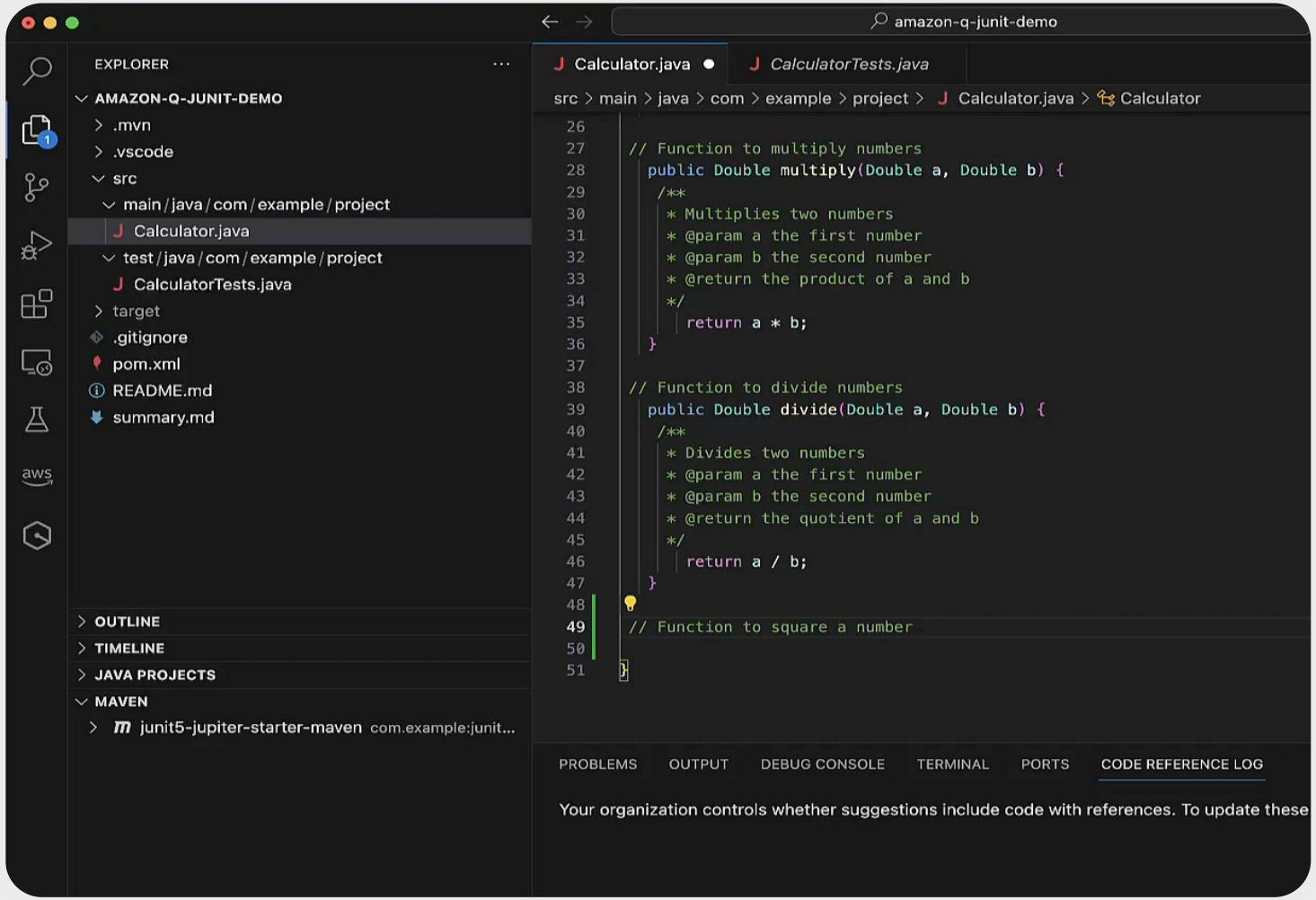
ビルドを手助けする

Amazon Q Developers



- セキュアコーディングの手助け
  - Ex.ハードコードされたパスワードの検出
  - プロジェクト及びコード記述時のスキャンと修正の提案

ビルド



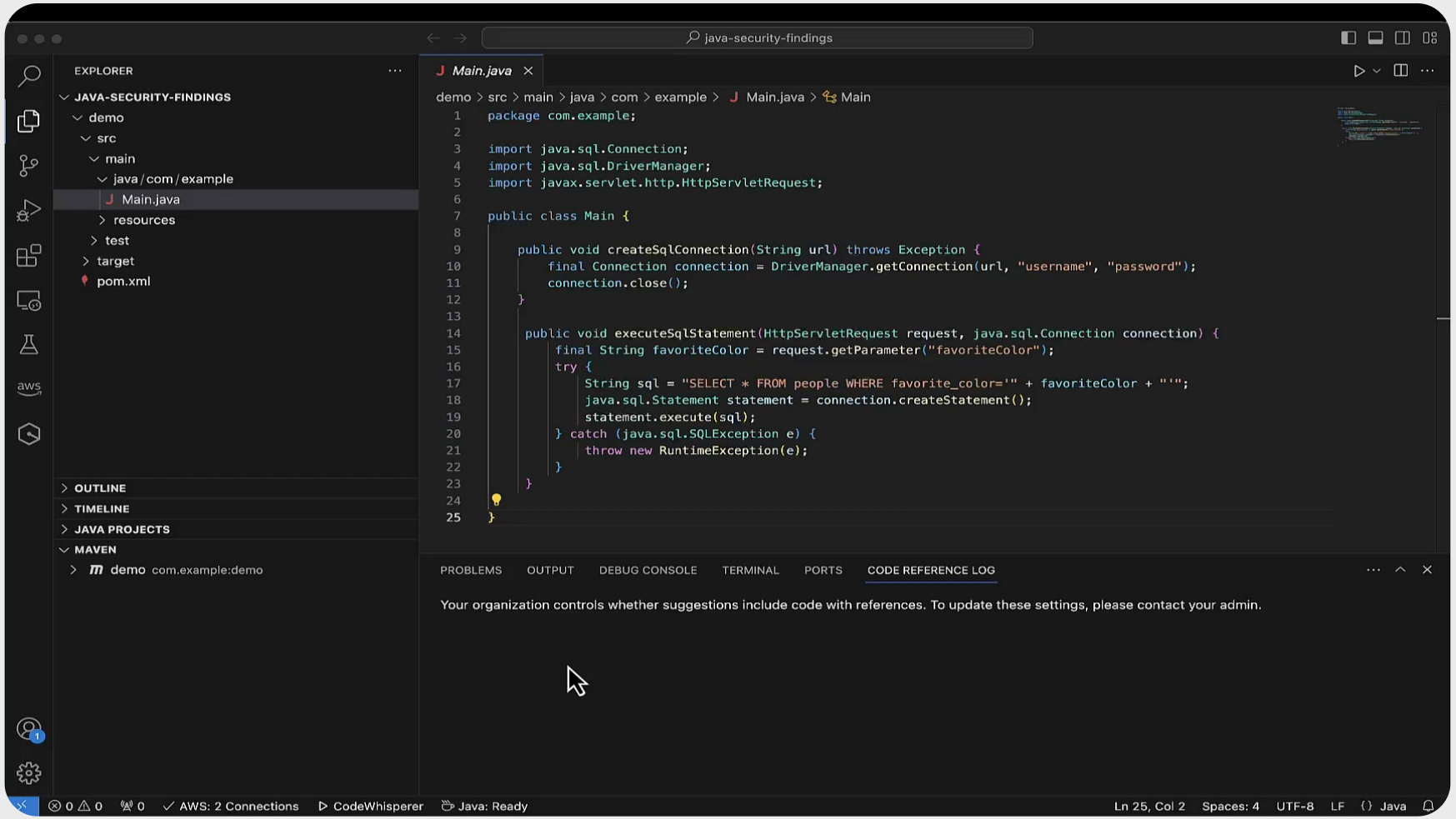
- コードの生成
- コードの説明
- インラインチャットでの対話
- コードベースの理解支援
- コードに合わせたカスタマイズ

テストを手助けする

Amazon Q Developers

- 生成 AI によるユニットテスト作成
- 生成AIによるテスト用モックデータの準備
- テスト結果のサマリやセキュリティとコード品質を向上させる修復策の生成

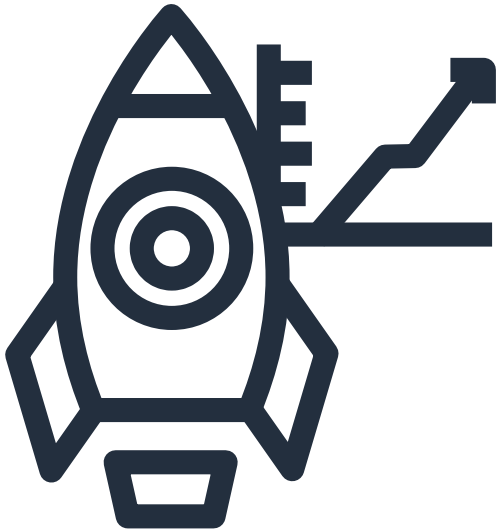
テスト



- 生成 AI によるユニットテスト作成
- セキュリティ脆弱性のプロジェクト全体スキャン
- セキュリティとコード品質を向上させる修復策の生成

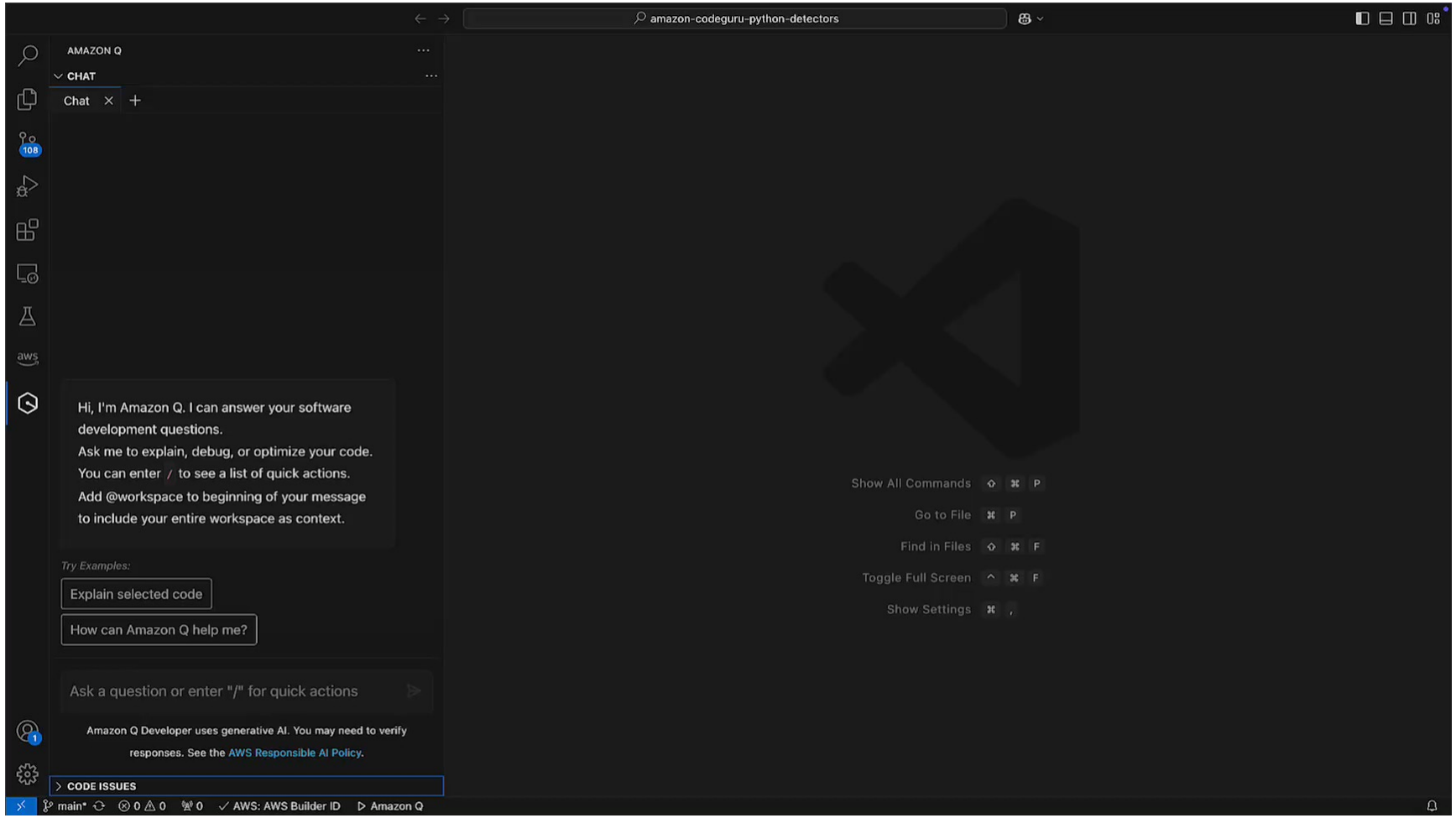
デプロイを手助けする

Amazon Q Developers



- デプロイ時にAIによるコードレビュー実施
- 属人化しない一貫したコードレビュー品質の担保

デプロイ

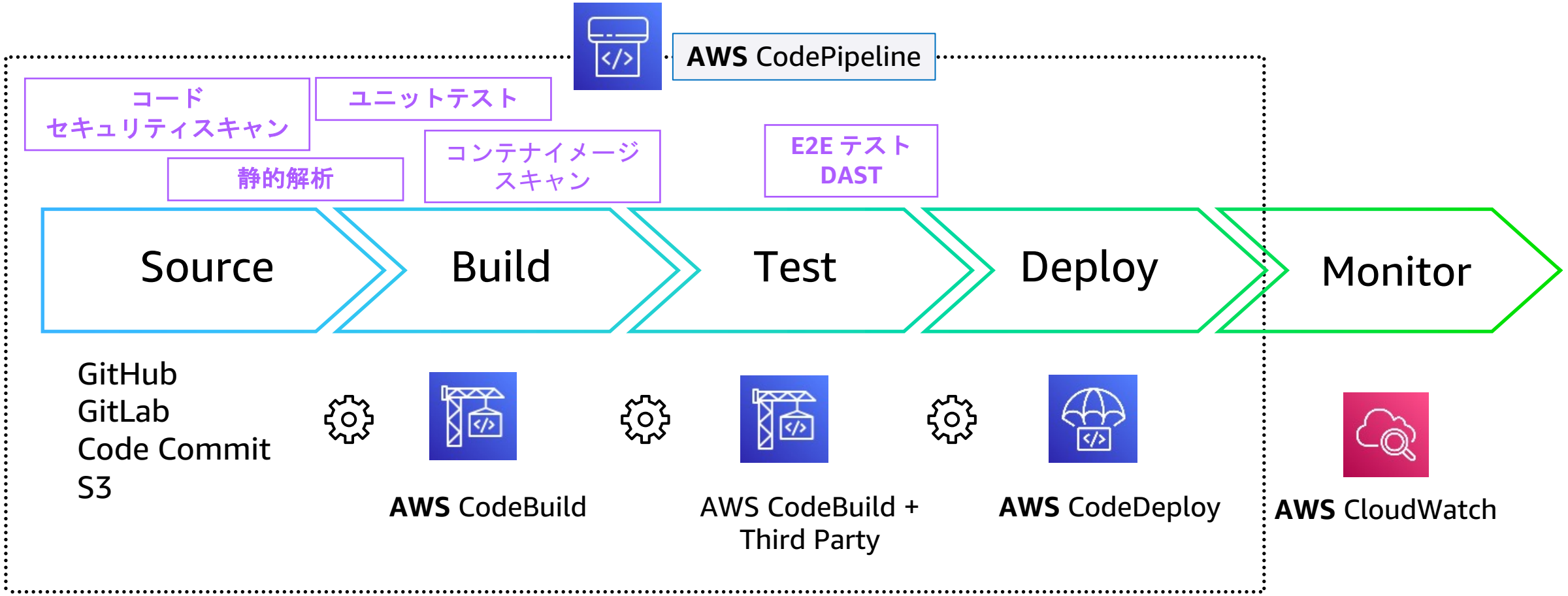


るコードレビューの自動化

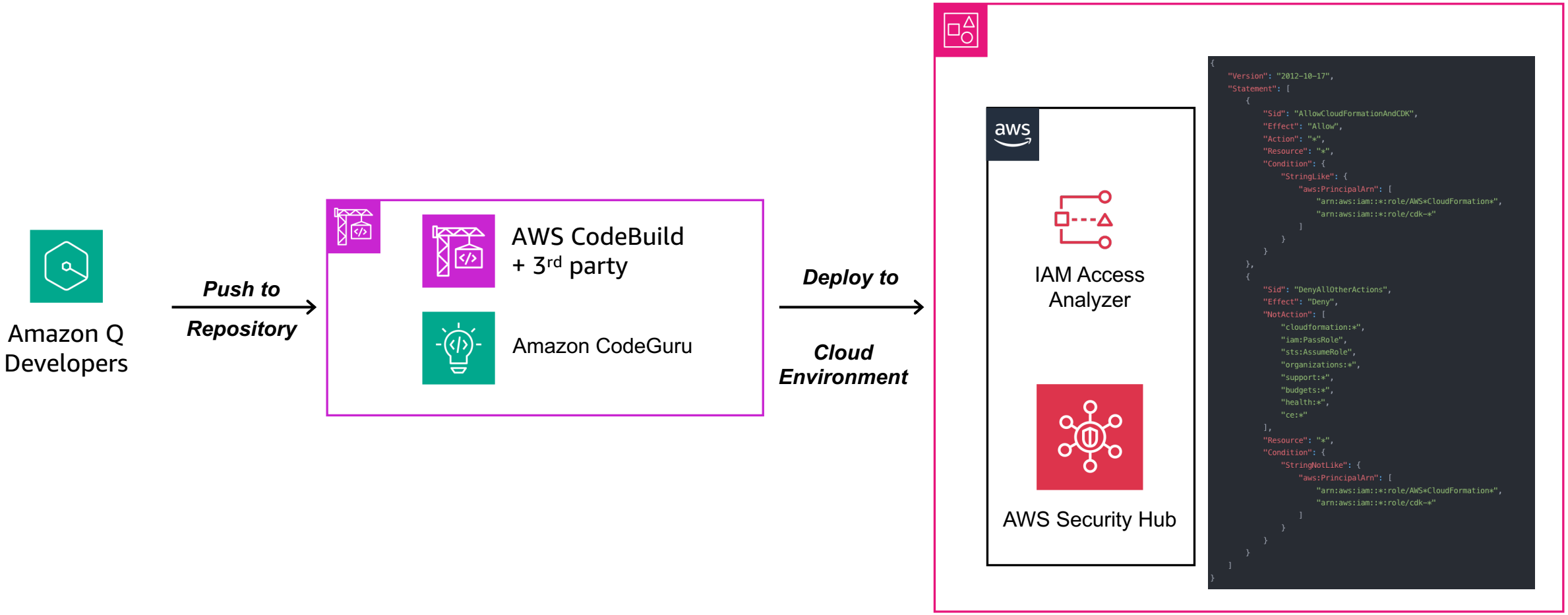
一般的なコード品質の問題を数時間ではなく数分で自動的に検出し解決

一貫したコードレビューの確保

デプロイパイプラインとの統合



デプロイパイプラインを通して IAM の権限を統制する



Thank you!