# DevSecOps環境における ソフトウェアサプライチェーン管理手法の提案

## Proposal of software supply chain management method in DevSecOps environment

吉村 隼哉・システム分科会・情報セキュリティ大学院大学

In DevSecOps, many tools are introduced to streamline and automate development and operations, and the DevSecOps pipeline is built using toolchains. However, a security framework to manage and verify these tools has not been established. In this study, we propose a new framework for software supply chain management for toolchains in the DevSecOps pipeline.

## 1. 研究背景

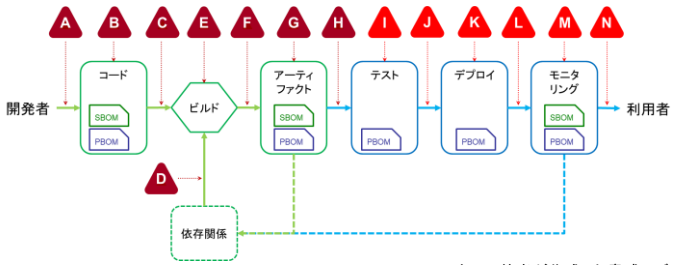
システム開発・運用業務の自動化／効率化を目的に，多くのDevSecOpsツールが導入され，ツールチェーンによりパイプラインが構築される．複雑化するDevSecOpsパイプライン自体も，ソフトウェアサプライチェーン（SSC）攻撃の標的となっており，開発成果物（アーティファクト）と同様に対策が必要であるが，ツールが管理されず，DevSecOpsパイプラインのSSCを保護するためのフレームワークも確立されていない．

## 2. 研究目的と提案手法

■DevSecOpsパイプライン全体でSSCを保護するフレームワークとして，以下の要件を満たす新たなフレームワークを提案する．

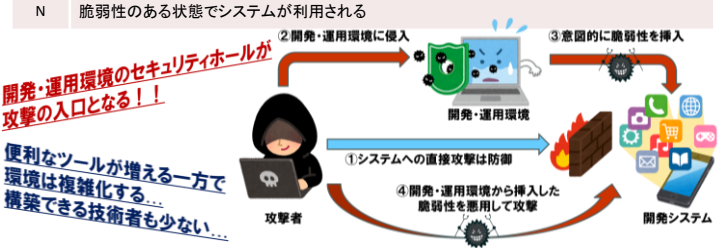
- ✓ **アーティファクトのSSC管理で使用されるSBOMを拡張し，PBOM（Pipeline Bill of Materials）としてパイプラインを管理可能**
- ✓ **PBOMを活用することで，DevSecOpsパイプライン全体で使用されるツールの整合性を機械的に検証可能**

## 3. 提案手法によりパイプライン全体を保護

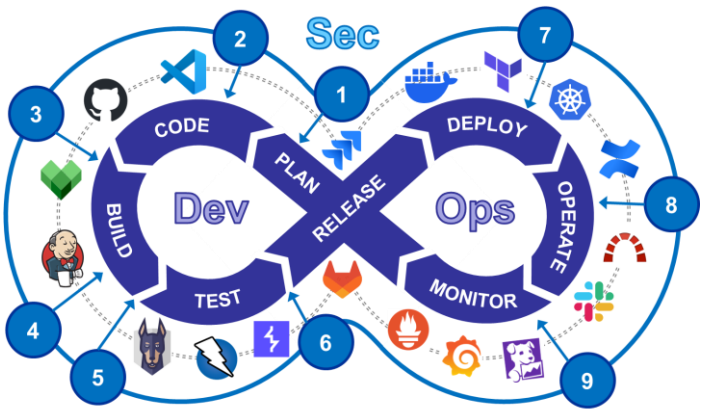



[1] SLSA(Supply-chain Levels for Software Artifacts) を元に筆者が作成した脅威モデル

| 脅威 | 既存フレームワーク（SLSA）で対応可能な脅威 [1] |
|---|---|
| A | 未承認のコードが送信（コミット）される |
| B | コードリポジトリが侵害される |
| C | 管理外（未承認）のソースがビルドに使用される |
| D | 悪意ある依存関係が追加される（改ざんされる） |
| E | ビルドプラットフォームが侵害され，攻撃コードがビルドされる |
| F | アーティファクトが改ざんされて保存される |
| G | 攻撃コードが含まれるミラーパッケージが作成され使用される |
| H | 攻撃コードが含まれるミラーパッケージがアップロードされる |
| **脅威** | **提案手法によって対応可能となる脅威** |
| I | テストツールの不備によって脆弱性が検知されない |
| J | テスト未実施のアプリケーションがデプロイに使用される |
| K | デプロイプラットフォームが侵害され攻撃コードがデプロイされる |
| L | デプロイされたソフトウェアが侵害される |
| M | モニタリングの不備によって異常が検知されない |
| N | 脆弱性のある状態でシステムが利用される |




## 4. DevSecOpsパイプラインへの適用手順




1. ：ツール導入時の規定を策定し，リスク評価した上でツールを導入
2. ：DevSecOpsパイプラインのコード化と管理（Pipeline as a Code）
3. ：SLSAモデルに基づいてセキュアなCI/CDパイプラインを構築
4. ：ビルドプロセスにおいてSBOMおよびPBOMを自動生成
5. ：SBOMを拡張し，DevSecOpsパイプラインをPBOMとして管理
6. ：使用されたツールとPBOMを比較することでツールの整合性を検証
7. ：整合性が保証された環境でデプロイ（ブルーグリーンデプロイの活用）
8. ：開発成果物と共に，DevSecOpsパイプラインも脆弱性管理
9. ：開発成果物と共に，DevSecOpsパイプラインもモニタリング

## 5. 導入効果

**Before：ツールが管理されず，セキュリティリスクのある環境**

**After：ツールを自動管理・検証し安全な開発・運用環境を実現**

## 6. 今後の予定

【外部発表】
・2025年3月：情報処理学会 第87回全国大会
【研究方針】
・提案手法の実装と評価
・DevSecOpsに取り組む企業へのヒアリング