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

1. 研究背景

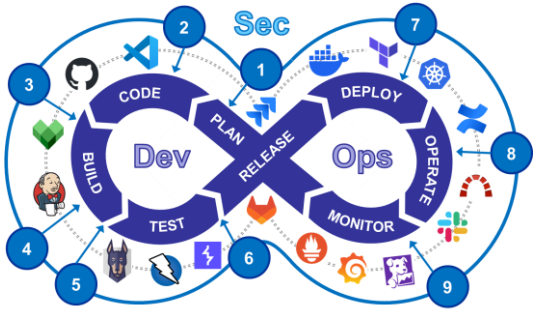
システム開発・運用業務の自動化／効率化を目的に，多くのDevSecOpsツールが導入され，ツールチェーンによりパイプラインが構築される．複雑化するDevSecOpsパイプライン自体も，ソフトウェアサプライチェーン（SSC）攻撃の標的となっており，開発成果物（アーティファクト）と同様に対策が必要であるが，ツールが管理されず，DevSecOpsパイプラインのSSCを保護するためのフレームワークも確立されていない．

2. 研究目的

■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. DevSecOpsパイプラインへの適用手順（提案手法）



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する
②：DevSecOpsパイプラインをコード化し（Pipeline as a Code），リポジトリで管理する
③：SLSA(Supply-chain Levels for Software Artifacts)を基に，CI/CDパイプラインを構築する
④：ビルドプロセスにおいてSBOMおよびPBOMを自動生成する
⑤：SBOMを拡張し，DevSecOpsパイプラインをPBOMとして管理する
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可能とする
⑦：整合性が保証された環境でデプロイを実行する（ブルーグリーンデプロイの活用）
⑧：開発成果物（アーティファクト）と共に，DevSecOpsパイプラインも脆弱性管理対象とする
⑨：開発成果物（アーティファクト）と共に，DevSecOpsパイプラインもモニタリング対象とする

4. 今後の予定

■DevSecOpsに取り組む企業へ実態調査を実施．
- ・RQ1：DevSecOpsパイプライン（ツールチェーン）のSSCが管理されていないのではないか．
- ・RQ2：ツールチェーンのSSCが管理されていない状況で，多くのツールが導入されてないか．
- ・RQ3：ツール導入時のリスク管理が十分に実施されていないのではないか．
- ・RQ4：ツール運用規定は適切に設計されているか．（特権ID管理や認証方式など）
- ・RQ5：日本の業界構造特有の課題があるのではないか．

■提案手法の実装と評価
- ・検証環境を用意し，実際にDevSecOpsパイプラインを構築することで提案手法の実装を目指す．
- ・提案手法によって，ソフトウェアサプライチェーンに関するリスクをどの程度低減可能か評価する．
- ・システム開発の現場において，導入することが可能であるか評価する．