

DevSecOps – SDV、機能安全 アプリケーション開発のベストプラクティス

DevSecOpsの方法論をSDV開発に適用する取り組みが進んでいる。富士設備工業 電子機器事業部長 浅野義雄氏は「オートモーティブ・ソフトウェア・フロンティア 2025 ～SDV時代のソフトウェア開発とモビリティ社会のこれからを探る～」(主催：インプレス、共催：名古屋大学 未来社会創造機構 モビリティ社会研究所、2025年2月18日～20日)に登壇し、SDVアプリケーション開発や機能安全開発においてDevSecOpsを推進する重要性和ポイント解説した。

ソフトウェア開発における「DevSecOps」とは何か

「SDVでは、ソフトウェア開発工数が爆発的に増加する。開発後はソフトウェアの機能追加に対して安全に更新していく必要がある。開発スピードの向上も求められる。そうした課題に対応するのがDevSecOpsだ。すでにDevSecOpsは航空宇宙業界の大規模開発などに採用されはじめている」

日本国内の組込みシステム市場向けに、LDRA社などの優れた海外ベンダーの開発支援ツールを提供している富士設備工業 電子機器事業部。この講演は、LDRA社のJay Thomas (ジェイ・トーマス) 氏の講演を基に、最新情報を加えたものだ。Thomas氏は、SpaceX社の初期の従業員であり、Falconロケットのフライトソフトウェアを開発した人物。現在はLDRA社でフィールドエンジニアリング担当シニアディレクターを務めている。

浅野氏はまず、SDVを取り巻く現状や課題についてこう説明した。

「SDV開発は、従来の『終わりのある開発』から複数車種のバージョンアップや機能追加が続く『終わりのない開発』への変化だ。例えば、開発後も、ECUのバージョン整合性を維持したまま、OTA (Over the Air) で安全にソフトウェアを更新する必要がある。さらに開発スピードの向上も求められる。新興EVメーカーの開発スピードは従来の開発の2～3倍とも言われている。そうした課題に対応するためのベストプラクティスとなるのがDevSecOpsだ」

SDV開発も含めて従来のサイバーセキュリティ対策はリアクティブ(受け身)だったという。

「コードは比較的緩いガイドラインに従って開発され、その後、パフォーマンス、侵入、負荷、機能の各テストによってテストされ、ほぼ確実に見つかるような脆弱性に対処する。これは機能安全規格とは対照的に受け身だ。出荷直前に多くの脆弱性が露見して対応に追われることもあった。DevSecOpsはこうした課題にも対応できる」



浅野 義雄 氏
富士設備工業株式会社
電子機器事業部長



Jay Thomas 氏
Senior Director -
Field Engineering, LDRA

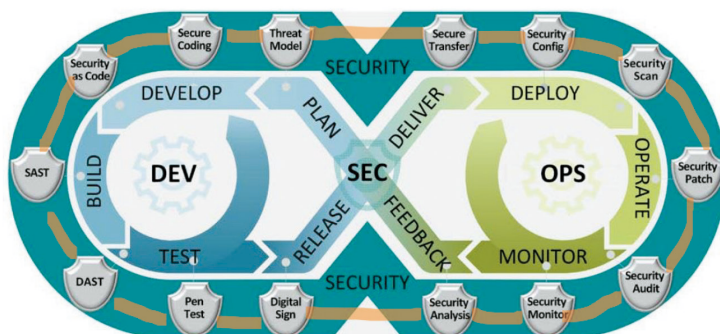
DevSecOpsは、ソフトウェア開発におけるサイバーセキュリティ対応のアプローチの1つだ。米国国防省では「ソフトウェア開発 (Dev)、セキュリティ (Sec)、運用 (Ops) を組み合わせて成果を最大にし、開発ライフサイクルを短縮するソフトウェア開発プラクティスの1つ」と説明している。

ポイントはシフトレフトとセキュリティバイデザインの推進

DevSecOpsの取り組みは、セキュアコーディング規約などに基づきながら、開発者、セキュリティ担当者、運用者が一体となり、継続的な開発プロセスの改善を行っていくものとなる。

米国国防省の「DevSecOpsイニシアティブ」による概略図

- ソフトウェア開発 (Dev)、セキュリティ (Sec)、情報技術運用 (Ops) を組み合わせて成果を安全にし、開発ライフサイクルを短縮する一連のソフトウェア開発プラクティス 出典: 米国国防総省のDevSecOpsイニシアティブ



出典: 米国国防総省のDevSecOpsイニシアティブ

「開発者は、コードが設計上安全であることをプロアクティブに（先手を打って）保証することで、開発の前倒しを行う『シフトレフト』を行う役割を担う。具体的には、要件に対して開発やビルド、テストを紐付け、それらの作業を反復しながら、開発と運用のなかにセキュリティを組み込むことを目指す。また、設計の初期段階からセキュリティを組み込むことは『セキュリティバイデザイン』と呼ばれる。これらにより、脆弱性を設計上排除したり、脆弱性が検出された場合にタイムリーに対処したりできるようになる」

DevSecOpsにおけるシフトレフトとセキュリティバイデザインは、機能安全にも適用することができる。

「シフトレフトやセキュリティバイデザインを推進することは、安全性を設計段階から組み込むことを目指す『セーフティバイデザイン』でのベストプラクティと共通する。これは、機能安全での実証済みの検証方法やツールは、セキュアコーディングおよびセキュリティに対する一貫したアプローチの堅実な基盤でもあるということだ」

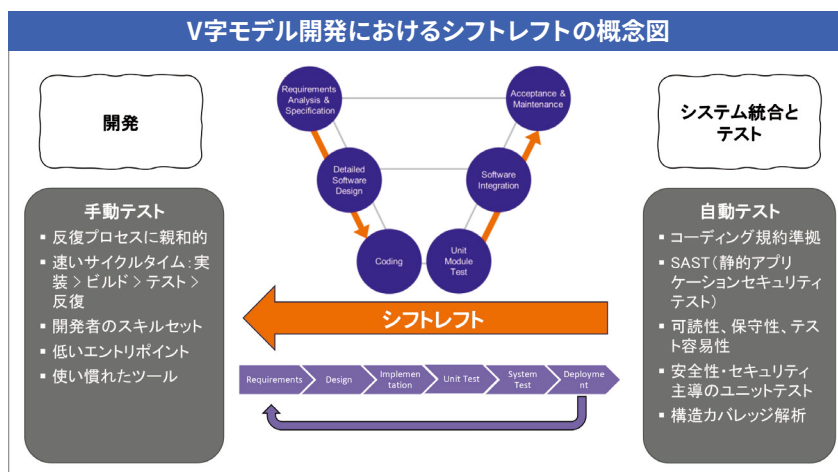
例えば、自動車に搭載する電気/電子システムの機能安全規格 ISO 26262 や自動車のサイバーセキュリティ対策規格 ISO/SAE 21434 に対応した開発で求められる、要件トレーサビリティやコーディング規約への準拠、ターゲットレベルでのテスト実行、規格準拠の管理などは、DevSecOpsにおけるセキュアコーディング規約への準拠や、早期かつ頻繁なテスト、双方向のトレーサビリティなどと基本的に同じ取り組みとなる。

「実際に、DevSecOps向けツールを使って、MISRAやCERT、CWEといったセキュアコーディング規約へのチェックを行い、それらをまとめてレポートにすることができる。また、DevSecOps向けツールにおけるテストケース自動生成機能を使って、機能安全規格の堅牢性試験、セキュアコーディングのファジングテストに利用できる」

基盤のコンテナ化やデジタルツインでの解析やテストを支援

では、DevSecOpsを推進するためにはどのような取り組みが必要になるのか。講演では、LDRAが提供するソリューションを活用して大きな成果を挙げた、航空宇宙業界の顧客事例がいくつか紹介された。

ある企業では、コードベースが大規模で、静的解析や動的解析に長い時間がかかっていた。解決策として取り組んだのは、テスト実行基盤のコンテナ化だ。機能要件などの変更によって回帰テストが発生するが、その効率化のために、基盤を



<https://ldra.com/capabilities/devsecops/>

コンテナ化し、並列実行できるようにした。

「DevSecOpsのプラットフォームにはGitLabを採用し、検証ツールのLDRAもコンテナ上で稼働させて、解析時間を最大6倍まで速めることができた。これにより、テスト頻度とソフトウェア品質が向上し、これまでより品質のよい新機能をよりスピーディーにリリースできるようになった。また、DevSecOpsを複数のプロジェクトに適用し、成果物を管理しながら、航空機向けガイドラインや規格への準拠状況をライフサイクル管理システムで管理できるようにした」

DevSecOpsの取り組みが進むと「デジタルスレッド」や「デジタルツイン」を構成していくことにつながる。デジタルスレッドは一貫性のあるデータを共有して有機的につなぐもので、デジタルツインは現実世界のモノを仮想空間上に再現するものだ。デジタルツインにより、仮想的なテストが迅速に実施できるようになると、新たなOTAアップデートの展開を安心して素早く行うことができるようになる。LDRAのツールは、デジタルツインでのデバッグやテストにも対応している。モデルが物理デバイスに対して忠実に機能することを確認するタイミング解析なども可能だ。

航空業界での知見やノウハウは、SDV開発にも適用できる。最後に浅野氏はこう訴えた。

「大手EVメーカーがDevSecOpsとコンテナの環境下でLDRAを数百ライセンス活用している。SDVでもDevSecOpsにより開発の柔軟性を高め、デプロイを高速化できる。デジタルツインで回帰テストすることでリリースサイクルを速められる。デジタルツインのシミュレーションで実世界でのパフォーマンスを評価できる」

お問合せ先



富士設備工業株式会社

電子機器事業部

<https://www.fuji-setsu.co.jp/>