BLACK DUCK®

社会インフラを守るために

# 開発現場の人材不足対策と高速開発に寄与 日立製作所の DevSecOps を支える仕組みは

HITACHI

日立製作所の荒木保雄氏

日立製作所の三島典子氏

日立製作所の鈴木一平氏

ソフトウェア開発の現場は開発の高速化と効率化、品質向上、人材確保など、さまざまな課題に直面している。日立製作所はこれらを包括的に解決するために開発プロセスを抜本的に見直し、生成 AI や自動化などの最新技術を組み込むことを前提とした DevSecOps の体制を整備した。

DevSecOps の仕組みを組織に浸透させるために、同社はどのような活動をしているのか。静的解析や動的監視ツールの選定時に重視したポイントは。

## 開発における「人手不足」「品質のばらつき」を解決する鍵は

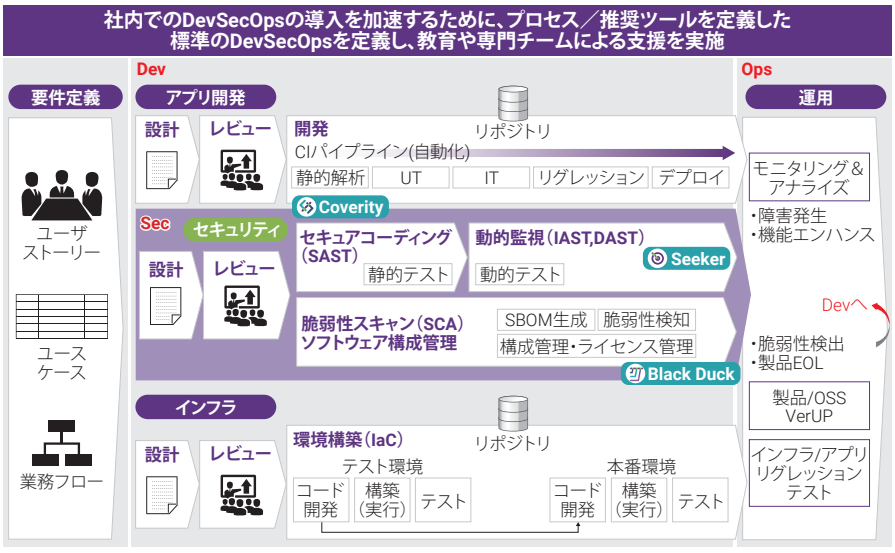
日立製作所は独自のシステム開発方法論「HIPACE」を基に、社会インフラを支えるミッションクリティカルなシステムを多数手掛け、開発効率を高めつつ高品質な IT サービス提供に努めてきた。同社が近年重視している課題が、人材不足と開発品質のばらつきだ。「だからこそ、いかに開発作業を自動化するかが鍵と考えています」。同社金融ビジネスユニット シニアテクノロジーエキスパートの荒木保雄氏は、こう説明する。

社会インフラを守る立場としてセキュリティ強化も無視できない要素だ。これらの要求を満たしつつ高速開発を実現する手法を突き詰めた結果、DevSecOps の導入は必須という結論に至った。サイバー脅威の高まりを背景に、政府機関はユーザー企業向けにセキュリティガイドラインを整備している。中でも金融業界は社会インフラとして重要度が高いことから金融庁は厳格なガイドラインを定めており、システム開発に関わる IT ベンダーに対しても脆弱（ぜいじゃく）性の少ない高品質なシステム開発体制を確保することを要求している。

金融デジタルイノベーション本部で主任技師を務める三島典子氏と鈴木一平氏のチームは、DevSecOps の実現に必要なプロセスとツールを選び、標準化した手法を「型」としてマニュアルを整え、金融ビジネスユニットに普及させる役割を担っている。「日立製作所では今までのプロセスを単に自動化するのではなく、自動化や生成 AI、クラウド活用を前提としたプロセスを整備して開発の考え方そのものを大きく変革させています」と三島氏は話す。

## 修正ガイダンス機能が開発者のスキルアップの助けに

荒木氏、三島氏、鈴木氏らのチームは、こうして型を作成した上で「なぜこの手法が必要か」を現場に繰り返し伝え、アプリケーション開発の自動化と DevSecOps の導入を推進してきた。静的解析にはブラック・ダック・ソフトウェアの「Coverity」を、動的監視には




金融ビジネスユニットにおける標準 DevSecOps

インタラクティブ・アプリケーション・セキュリティ・テスト（IAST）ツール「Seeker」を標準ツールとして採用。CI/CD ツールによって開発からテスト、リリース、フィードバックの反映まで連携させ、自動化している。現場の反響をヒアリングしながら一連のプロセスを改善し、推奨するツールと手法が現場に定着するまで継続的に支援している。

先行して普及し始めているのは Coverity だ。プロシージャ間解析やフルパス解析など静的解析ツールとしての機能が充実し、誤検知が少ないといった機能面のメリットもさることながら、採用の決め手になったのは「修正ガイダンスの分かりやすさ」だったという。

「開発者のスキルアップとコードの品質向上という目標に向けて、手を付けやすく成果の出やすい領域が静的解析ツールの活用でした。当社は以前からさまざまなコードチェッカーを利用していましたが、Coverity は解析結果が特に見やすく、気に入りました。検出された不具合ごとに表示される修正ガイダンスは、何をどのように修正すべきか一目で理解しやすいので開発者のスキルアップにつながります。人材不足の中でも効率的な育成につながる点は、大きなメリットに感じました」（三島氏）

ソースコードをチェックしてバグや脆弱性を洗い出すだけならば、オープンソースソフトウェアを含めてさまざまなツールで実現できる。荒木氏、三島氏、鈴木氏が取り組む標準化の基本方針としても、「効率良く目的を達成できるならば、どんなツールを使っても構わない。組織として推奨する手法は用意しておくが、強制はしない」というスタンスだ。金融デジタルイノベーション本部が Coverity による静的解析を推奨しているのは、コーディングしながら自力で間違いに気付ける学習効果を期待している点が大きい。

改善すべき要素を第三者も客観的に把握できるから、チームとしてのサポートがしやすくなる。プロジェクトの規模や内容によって具体的なタイミングは異なるものの、日立製作所は開発者の作業プロセスの中に Coverity を用いたコードのチェックを組み込み、品質確保に努めている。「Coverity は、人の手によるコードレビューでは見落としがちなエラーや不具合、実際に動かしてテストしなければ出てこないような問題まで検出できます。現場からは非常に便利だという声が上がっています」と鈴木氏は説明する。

その他、Java や TypeScript など幅広いプログラミング言語に対応していることやユーザーインタフェースが日本語化されていること、トライアルの段階から手厚いサポートを得られたこと、クラウドだけでなくオンプレミスでも動作することなどが評価のポイントとなった。検出された問題が適切に修正できたかどうかをトラッキングできる管理機能も便利だと鈴木氏は感じている。

## 開発プロセスの早期に問題を見つける手段として Seeker が活躍

テスト自動化ツールと組み合わせた Seeker の活用も進みつつある。日立製作所の標準開発プロセスでは、開発の最終段階で DAST（動的アプリケーション・セキュリティ・テスト）ツールを用いて深刻な脆弱性をチェックするルールを定めている。問題の検出が後工程になるほど手戻りの作業工数は大きくなる。こうした手戻りの工数削減と、なるべく初期段階で問題を見つけて対策するシフトレフト戦略において、Seeker が重要な役割を担っている。

開発段階で Coverity によって検出される指摘事項は多岐にわたるため、全てに対処するのは難しく、優先順位を付けざるを得ない。「そのため、現場の独自判断で優先度を下げてしまうリスクがありました」と三島氏は説明し、「Seeker を併用することで、アクティブ検証によって危険度の高い問題を指摘して判断をサポートしてくれるのではないかと考えています」と期待を寄せる。

アプリケーションサーバに IAST エージェントを入れ、バックグラウンドでトラフィックと実行フローを分析する形になるため、現場に負担がかかることもない。「自動テストの裏で Seeker が動作し、問題点があれば自動的にチケットを起票し、フィードバックサイクルが素早く回るように取り組んでいるプロジェクトもあります」と鈴木氏は話す。

## 現場の意見を聞きながらベストプラクティスを洗練させる

どんな組織でも、いったん確立した開発プロセスに手を加えるのは嫌がられがちだ。そのため荒木氏、三島氏、鈴木氏らは、「なぜ必要なのか」を現場に丁寧に説明することを心掛けている。「ツールだけを現場に持っていってもなかなか定着しません。現場の開発者に話を聞き、『ここが難しい』という意見があれば標準設定や手順書を作成する、といったサイクルを回し、段階的な普及を進めています」（鈴木氏）

成果を実感した後の浸透は速いようだ。Coverity を繰り返し活用することで、指摘されるエラー件数が逓減しているプロジェクトもある。「品質の数値化は難しいものですが、現場にヒアリングしてみると『あれだけテストをしたのに、こんなところにも脆弱性が残っていたのかと気付きが得られた』といった声を随所で聞きます。開発者のスキル向上につながっているという手応えを感じます」（三島氏）

「今はわれわれ専門のサポート部隊が推奨手法の定着に向けたサポートを提供していますが、ゆくゆくは現場で DevSecOps を推進できる人をもっと育てて、現場の誰もが DevSecOps の手法を習得した状態を目指したいと思っています」（鈴木氏）

## 「品質は上流工程で作るもの」という思想に立ち戻る

シフトレフトという概念が登場する前から、日立製作所はシステム開発において「品質は上流工程で作るもの」という思想を持っていた。しかし「最近は、最後にチェックして修正すればいい、という発想も見られがちです。Coverity や Seeker も活用しながら、本来の望ましい姿に戻していければと考えています」と荒木氏は言う。

同社における DevSecOps の取り組みは、トップダウンとボトムアップを組み合わせて進んできた。経営層が旗振り役として主導しながら、人材不足や品質向上の課題を解決するためにこれまでのやり方を変える必要があることを説き、それを実現させ、加速させるための支援組織を設立した。このサポート部隊が伴走しながら、プロセスの標準化と開発者の育成を後押ししている。「望ましい手法とツールをしっかり現場に定着させ、改善の成果を示し、売り上げや顧客満足に還元していかなければなりません」と荒木氏は意気込みを見せる。

## ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。詳しくは www.blackduck.com/jp をご覧ください。

**ブラック・ダック・ソフトウェア合同会社**

www.blackduck.com/jp