

FPT Software

シノプシスのアプリケーション・セキュリティ・テストで
コード品質とセキュリティを強化



企業概要

FPT Software は、テクノロジー /IT サービス・プロバイダーである FPT Corporation (本社ベトナム、収益約 20 億米ドル) の子会社です。デジタル・トランスフォーメーション (DX) のパイオニアとして、FPT はスマート・ファクトリー・テクノロジー、デジタル・プラットフォーム、ロボティック・プロセス・オートメーション (RPA)、人工知能 (AI)、Internet of Things (IoT)、モビリティ、クラウド、マネージド・サービス、テストなど幅広い分野において世界最高クラスのソリューション・サービスを提供しています。

「開発ライフサイクルの
なるべく早期にコード品質と
セキュリティを改善してくれる
ツールを評価検討することに
しました。」

課題：ソフトウェア・プロジェクトの品質と セキュリティを改善する

FPT Software はソフトウェアの設計から開発、マイグレーション、モダナイゼーションまで、ライフサイクル全体にわたるサービスを顧客に提供しています。しかし顧客のシステムにソフトウェア・コンポーネントを納入しようとする、現在の相互接続環境を想定せず設計されたレガシー・コードやアーキテクチャに直面することもしばしばです。これらを現在最先端のアプリケーションで求められる品質とセキュリティ基準に適合させるには、徹底的なテストを実施する必要があります。

FPT Software の Do Van Khac 氏 (最高デリバリ責任者兼エグゼクティブ VP) は次のように述べています。「顧客の信用を獲得することが弊社にとって最重要事項であり、コード・セキュリティの強化には常に注意を払っています。特に、レガシー・コードおよびアーキテクチャの互換性の問題から生じるリスクには頻繁に直面しており、これらの修復には大きなコストがかかっていました。そこで、[開発ライフサイクル](#)のなるべく早期にコード品質とセキュリティを改善してくれるツールを評価検討することにしました。」

FPT のデリバリ・コマンド・センター (DCC) は、いくつかの[静的解析](#)ソリューションを詳細に評価した結果、同社には Coverity が最適であるとの結論に達しました。Coverity なら開発プロセスの早期にソフトウェアの問題を特定して修正できるため、コード・レビューを迅速化してコード品質とセキュリティを高められるだけでなく、開発プロセスの終盤になってこれら問題の対処に追われることもなくなり、修正にかかるコストも抑えることができます。

オープンソース・コンポーネントおよびライブラリを使用したソフトウェア開発が主流になる中で、顧客からは FPT が実施するソフトウェア・テストに[ソフトウェア・コンポジション解析](#) (SCA) も含めてほしいという要望が寄せられていました。そこで同社は 2019 年にシノプシスの Black Duck を導入し、現在はほぼすべてのソフトウェア・プロジェクトのテストに Coverity と Black Duck を併用しています。

「すべてのエンタープライズ、とりわけコード品質が何より重視される組込みシステムを専門にしている企業には、シノプシスの AST ツールを強く推奨します。」

ソリューション：Coverity と Black Duck

Coverity は重大なソフトウェア品質の不具合とセキュリティ脆弱性を特定してくれるため、[ISO-9001](#) や SEI CMMI レベル 5 などのスタンダードに準拠してセキュアで高品質なコードを開発できます。また、Black Duck の導入により、FPT はアプリケーションやコンテナに含まれるオープンソースおよびサードパーティ・コードに起因するセキュリティ、品質、ライセンス・コンプライアンスのリスクを管理するための包括的なソリューションを手にするようになりました。

「コード・スキャンおよびセキュリティ・チェックの強化に関して、シノプシスのソリューションは弊社の期待を上回りました。Coverity と Black Duck の導入により、弊社のソフトウェア品質と顧客満足度はいずれも大きく向上しています。Coverity のおかげで [OWASP Top 10](#) に挙げられたセキュリティ問題への対策も万全となり、Web アプリケーションに対する最も重大なセキュリティ・リスクへの対処能力をアピールできました。」(Do Van Khac 氏)

成果：開発者の生産性が向上

現在、FPT はシノプシスの Coverity と Black Duck を使用して年間で平均 200 件のプロジェクトを管理しており、これらの AST ツールはいずれも Jenkins ビルドに統合されています。

Do Van Khac 氏は次のように述べています。「シノプシスは多くの問題を解決してくれました。弊社は 2015 年に Coverity、2019 年に Black Duck を導入しましたが、シノプシスのアプリケーション・セキュリティ・テストには非常に満足しています。弊社の評価では、シノプシスのテストは誤検知と検知漏れがいずれも 10% 未満と低く、問題を正しく特定できるため、開発者の生産性向上につながる事が判明しています。これらツールには充実したレポート機能があり、顕在化したトレンドをリアルタイムで可視化できるため、問題にいち早く対処してリスクを最小化できます。」

「すべてのエンタープライズ、とりわけコード品質が何より重視される組込みシステムを専門にしている企業には、シノプシスのアプリケーション・セキュリティ・テスト・ソリューションを強く推奨します。」

シノプシスの特色

シノプシスのソフトウェア インテグリティ グループは、企業が安全で高品質なソフトウェアを構築し、リスクを最小限に抑えながらスピードと生産性の最大化に貢献します。シノプシスは、アプリケーション・セキュリティのリーダーであり、静的解析、ソフトウェア・コンポジション解析、動的解析ソリューションを提供しており、独自のコード、オープンソース・コンポーネント、およびアプリケーションの動作における脆弱性や不具合を迅速に見つけて修正します。

詳しくは、www.synopsys.com/jp/software をご覧ください。

日本シノプシス合同会社 ソフトウェア インテグリティ グループ
〒158-0094 東京都世田谷区玉川
2-21-1 二子玉川ライズオフィス

TEL: 03-6746-3600
Email: sig-japan@synopsys.com
www.synopsys.com/jp/software

©2020 Synopsys, Inc. All rights reserved. Synopsys は Synopsys, Inc. の米国およびその他の国における登録商標です。Synopsys の商標に関しては、こちらをご覧ください。
<http://www.synopsys.com/copyright.html> その他の会社名および商品名は各社の商標または登録商標です。2020 年 10 月