損保ジャパン

Contrast Securityの製品を活用して DXプロジェクトを推進するSOMPOグループ

200万件もの脆弱性チケットに悩まされていた巨大プロジェクトの工数削減を実現

SOMPO 損保ジャパン

事業内容

各種損害保険商品、サービスを主軸に、デジタル技術を活用した事故対応サービス、ドライブレコーダーを活用した安全運転支援サービスなどを提供。近年では変化する時代を見据え、自動運転やシェアリング事業など新たな分野にも事業領域も拡大。

デジタルトランスフォーメーション（DX）無しでは生き残れないというほどの危機感を持ち、「未来革新プロジェクト」を推進しているSOMPOホールディングスでは、脆弱性対応の工数削減に向けContrast Securityの製品群を採用している。

会社概要

会社名
損害保険ジャパン株式会社

正味収入保険料
2兆1,847億円（2019年度）

資本金
700億円

創業
1888年（明治21年）10月

従業員
24,689名

住所
東京都新宿区西新宿1-26-1

URL
www.sompo-japan.co.jp

今や様々な業界がデジタル化の波に直面し、変革を迫られている。国内保険大手の損害保険ジャパンを中核とするSOMPOホールディングスも例外ではない。同社は、デジタルトランスフォーメーション（DX）を抜きにして生き残りはあり得ないというほどの危機感を持って、「未来革新プロジェクト」を推進している。

このプロジェクトでは、COBOLで開発され長年にわたって同社の事業を支えてきた基幹アプリケーションを、Javaをはじめとするオープン系技術に置き換え、より付加価値の高いサービスをより迅速に提供することを目指した基盤作りを進めている。金融・保険系システムというと、あらかじめ決まった仕様に沿ってフルスクラッチで開発するイメージが根強いが、未来革新プロジェクトでは、開発効率を向上させるため適材適所でオープンソースソフトウェア（OSS）も活用しながら開発を進めている。

申請と実態の齟齬やトリアージに苦戦してきた脆弱性対応

数万もの代理店、その先にいる十万を超える顧客に付加価値の高いサービスを提供するという要件ももちろん重要だが、そのためにセキュリティをおろそかにし、顧客の個人情報が危機にさらされるようなことがあってはならない。それでなくとも保険・金融業界には、金融庁やFISCが示す、一般企業以上に高い水準のセキュリティ基準を満たすことが求められている。

そこでSOMPOホールディングスおよび未来革新プロジェクトの推進に当たるSOMPOシステムイノベーションズでは、開発者からの申請に基づいてアプリケーションで利用されているOSSコンポーネントの情報を集約し、「ソフトウェア部品表」として管理。日々公開される脆弱性情報を突き合わせ、社内ガイドラインで定められている一定の深刻度以上の脆弱性については対応することで、セキュアなソフトウェア開発ライフサイクルの実現に取り組んできた。

だが、このプロセスにはあまりに工数がかかりすぎ、脆弱性を指摘するセキュリティチーム、それを受けて修正作業に当たる開発チーム、共に負担が大きかったという。

そもそも未来革新プロジェクトは、「大規模な」と一言で片付けるにはあまりに大きな開発プロジェクトだ。約1億ステップにものぼるCOBOLプログラムを置き換えるために約2,000人の開発者が関わり、巨大なアプリケーションが約50種類も開発されている。一部のコンポーネントは海外でオフショア開発されており、人間の頭で全体を見通すのは困難な規模だ。

このため申請ベースのプロセスで検出される脆弱性の量も膨大で、チケット数は約200万件に上るほどだった。しかも、その中には多数の誤った情報が含まれていた。

損害保険ジャパン株式会社
IT企画部 セキュリティエバンジェリスト
一般社団法人 金融ISAC 脆弱性管理WG 副座長
小中俊典氏

金融ISACにて脆弱性WGの副座長として活動し、日々他の金融機関も脆弱性管理に苦しんでいること認識し、その課題に積極的に取り組むべきと考え、最適解を見つけ、会員企業と有益な情報共有をしたいと考えている。

Contrast SECURITY

損害保険ジャパン株式会社 IT企画部 セキュリティエバンジェリストの小中俊典氏は、「開発者に申請を委ねると、メジャーなOSS製品の情報しか上がってこなかったり、個人の解釈によって粒度もバラバラだったりして、大量の誤検知が生じていました」と振り返った。

その上、単純に文字列を付き合わせるだけで機械的に判断していたため、本当に修正対応が必要かどうかの判断を下すのはさらに一苦労だったという。「社内のガイドラインと照らし合わせ、脆弱性のトリアージを自動化させる仕組みが必要だと考えていました」(SOMPOシステムイノベーションズ株式会社 未来革新開発本部 基盤推進グループ ユニットリーダ、西山龍弥氏)

巨大なアプリケーションで、多数の開発者が関わるがゆえの難しさもあった。「これだけの規模になると、自分が開発している領域は把握できていても、細かなライブラリも含めて全体を見通せる人はほぼいません。セキュリティチームから脆弱性の指摘を受けても、『（実際は使っているかどうかも分からず）いや、自分の範囲ではそのOSSは使っていないので大丈夫』と返ってくることもありました」（小中氏）。脆弱性の深刻度に基づく対応の優先順位を決める以前に、使っているか使っていないかのやり取りで時間を消費してしまうこともあったという。

SOMPOシステムイノベーションズ株式会社
未来革新開発本部
基盤推進グループ ユニットリーダ
西山龍弥氏

「Contrast OSS」の結果を基に、ファクトベースでの建設的な開発を実現

脆弱性対応に要する時間を短縮し、負荷を軽減して開発作業のスピードを高めるには、自己申告に基づく管理の代わりに、何らかの自動化された仕組みが必要だ――SOMPOシステムイノベーションズではそう考え、2020年初めから脆弱性スキャナの導入に向け、検討を開始した。

そしていくつかの製品を比較検討した結果採用を決定したのが、Contrast Securityが提供する「Contrast OSS」だった。

Contrast OSSは、アプリケーションに含まれるOSSを依存関係も含めて検出し、CVSS(Common Vulnerability Scoring System：共通脆弱性評価システム）に基づいて深刻度を分類してコンソール上に表示する。もれなく検出するだけならば他のツールでも可能だったが、「この脆弱性に対応すべきか否か」の判断を下しやすくなる情報を合わせて得られることが、Contrast OSS採用の決め手になったという。

「Contrast OSSで脆弱性が検出されると、例えば脆弱なライブラリが何回呼び出されたかといったことまで通知してくれます。開発現場が『そのライブラリは使ってないよ』と言ってきても明確なエビデンスがあるため、そこで押し問答することなく、対処に向けた次の議論に進むことができます。

Contrast SECURITY

単にCVSSの数値を表示するだけでなく、利用されているライブラリやコンポーネントのバージョンをContrast OSSが抽出し、本当に対処が必要な問題を優先的に示してくれる点も助かりました。

従来は関係者が集まって、この脆弱性に対処するべきか否かといったことを侃々諤々（かんかんがくがく）話し合い、ときには社内の力関係も加わって議論が紛糾したりして、どんどん工数が消費されていました。Contrast OSSによってファクトベースで判断を下せるようになり、そうした工数はほぼゼロになりました」（西山氏）

Contrast Security日本法人による手厚いサポートが得られたことも、スムーズな導入に繋がった。セキュリティチームも開発チームも共に議論に費やす時間を減らすことができ、検出した脆弱性ごとに1人月程度の工数が削減できたという。

結果として「対処すべき脆弱性の件数が圧倒的に減りました。また、セキュリティチームとしては、Contrast OSSの画面を見るだけで済むようになりました。」と西山氏は評価する。時々、どうしても修正が難しい脆弱性の対応について相談に乗るくらいで、建設的な議論ができるようになっています」と述べた。

Contrast OSSが備えるモニタリング機能の活用も進めている。機能要件に比べ、セキュリティという非機能要件はなかなか対応のモチベーションが上がりにくい。そこで、各開発チームが指摘された脆弱性にどのように対応し、いつ対応が完了するかといった事をスコアリングにより評価し、ゲーム理論を生かすことで、各開発チームが競争し脆弱性の対応促進ができないかと考えているという。

未来革新プロジェクトでは、各アプリケーションのテストフェーズでContrast OSSを活用しているが、4月に予定しているライブラリの本番リリース以降も活用を継続する。「脆弱性は次々に出てくるため、継続的に回して対応していきます」（西山氏）

アジャイルで開発が進む新規アプリにもContrast Security製品を活用し、DevSecOps実現へ

SOMPOホールディングスでは未来革新プロジェクト以外にも、DXに向けた様々な取り組みを進めている。その1つが、損害保険ジャパンが開発を進めている、傷害保険見積もりのための新規アプリケーションだ。

ケーススタディ：損保ジャパン

このアプリケーション開発プロジェクトでは、長らく企業システム開発の主流だったウォーターフォール方式に代わりアジャイル開発を採用。基盤にコンテナ技術を活用し、こまめにリリースしていく方針だが、そこで課題となるのがセキュリティの担保だ。開発プロセスの中にセキュリティを組み入れ、アジャイルならではの開発スピードを生かしつつセキュリティ品質を保つため、Contrast Securityの製品群でProof of Concept（PoC）を実施し、その有効性を確認済みだ。

「これまでのウォーターフォール方式の開発では、テストの段階になってはじめて脆弱性診断を実施するという具合に、後のフェーズでセキュリティを検査していました。しかしセキュリティ対応というものは、後のフェーズになればなるほど対応工数もコストもかさみます。開発プロセスのもっと前の段階で脆弱性を検知できないかと問題意識を抱えていたところにContrast Securityの話を聞き、プロジェクトに取り入れてみました」（SOMPOホールディングス株式会社 IT企画部 プロジェクトマネージャ、土屋敏行氏）

具体的には、Vue.jsとJavaを組み合わせて開発しているアプリケーションの脆弱性をContrast AssessとContrast OSSでチェックし、開発者とセキュリティ担当者が一体となって対応を進めるDevSecOpsの実現に取り組んでいる。特に、アジャイルで継続的に開発を進めていく中での役割に期待しているという。

「リリース時点できちんと脆弱性対応を終えていたとしても、リリース後も様々な機能追加や保守を行っていくことになります。また、リリース時点には発覚していなかった脆弱性も発見されていくため、継続的な監視が必要です。しかし外部の業者にずっと診断してもらうのは予算の面からも、開発スピードの面からも非現実的です」（土屋氏）。そこにContrast Assessを活用することで、リリースサイクルを維持しながらセキュリティを担保していきたいという。

試験導入の段階ではあるが「これまでは見つけられていなかった脆弱性を早期に見つけ、すぐに対処することで、非機能面の品質が上がったことがメリットです」と土屋氏。今後、それでも修正しきれない脆弱性に対する攻撃をリアルタイムに保護するContrast Protect（RASP）についても検証済みで、今後はグループ内に横展開していきたいという。

SOMPOホールディングス株式会社
IT企画部 プロジェクトマネージャ
土屋敏行氏

Contrast SECURITY

先進的なアプリケーション・セキュリティを活用することがDX推進のポイントの1つに

DXという言葉はキラキラ輝いて見えるが、実際のシステム開発がいかに一筋縄ではいかないか、システムの話だけではなく時に調整も含めた泥臭い話が必要、ということは、多くの人が実感していることだろう。

スケジュール管理も含めたマネジメント、ハンドリングに心を配りながら、ここまでDXを推進してきた経験を踏まえ、小中氏は「DXは、ただリソースを確保し、どんどん人を投入すればできるものではないという教訓を得ました。セキュリティも同様です。ただ作ればいいというのではなく、新しい仕組みを入れていくことが必要だと思います」と述べ、それによって建設的に、小中氏の表現を借りれば「さわやかに」開発ができる環境が整っていくとした。

今後DevSecOpsを推進して、開発の生産性とセキュアコーディングの品質、その両方を高めながら、脆弱性に関する情報を的確に示してエンジニアの判断に要する時間を減らし、本来の仕事に専念できる環境を整える上でも、Contrast Securityの継続的なイノベーションに期待しているという。

Contrast SECURITY

Contrast Securityはアプリケーションセキュリティにおけるリーディングカンパニーです。Webアプリケーションの開発段階でアプリケーションに潜む脆弱性を高精度で解析し、本番環境では外部からの攻撃を迅速に検知しブロックすることが出来ます。特許取得済み技術「ディープセキュリティ・インスツルメンテーション」により、企業はソフトウェア開発ライフサイクル(SDLC) への展開を簡単且つ迅速に実現します。従来の非効率的なアプリケーションセキュリティ(SAST、DASTおよびWAF)から完全に置き換えることにより、時間やコストを消費する脆弱性スキャンの排除やインフラ業務、セキュリティエンジニアのリソースを軽減します。Contrastのアプリケーションセキュリティは、SDLCを加速し、未知の脅威からアプリケーションを保護しながらビジネスの成長を促進します。

100-0005
千代田区丸の内2-2-1
岸本ビルヂング6階
TEL:050-3733-8284

製品に関するお問い合わせ：JPNSales@contrastsecurity.com