

システム面でも「安心・安全」を後押し

セブン&アイ・ネットメディア OSSを含む網羅的な脆弱性チェックを導入

「omni7」などのシステム開発に携わるセブン&アイ・ネットメディアは、脆弱性チェックツールを採用し、オープンソースも含む網羅的なセキュリティ対策に取り組んでいる。



Web サービスやスマートフォン向けアプリの開発をする際にも高品質、短納期の開発が求められており、顧客が望む機能をスピーディーに実現するには、オープンソースソフトウェア（OSS）の利用が不可欠だ。

日本シノプシスの調査「2018 Open Source Security and Risk Analysis レポート」によると、何らかの形でオープンソースのコンポーネントを利用している商用ソフトウェアの割合は96%に上る。ソースコードベースでみると、オープンソースが含まれる割合は実に57%に達し、自社開発コードよりも多い結果だ。

一方で問題となるのが、OSSに存在する脆弱（ぜいじゃく）性への対応だ。過去に発生した幾つかのセキュリティインシデントからも、OSSがはらむリスクは明らかだ。

開発工数の削減や高機能の実現を考えるとOSSを利用しない手はないが、脆弱性によって被害を受ける恐れも少なくない。セブン・イレブンやイトーヨーカドーなど多様な業態にまたがり、世界18カ国に約6万7000店舗、日本国内だけでも約2万2000店舗を展開している流通大手のセブン&アイグループは、この問題にどう取り組んだのだろうか。同グループのITシステムを担うセブン&アイ・ネットメディアに聞いた。

多様化するニーズに応えるサービスをOSS活用で迅速に開発

セブン&アイ・ネットメディアはセブン&アイグループのIT子会社として、さまざまなシステムのデザインや開発・運用に携わっている。一口に流通と言っても、セブン&アイグループの場合はコンビニエンスストアや総合スーパー、百貨店、専門店と異なる業態で構成される。グループ全体としてITへの取り組みを強化しており、セブン&アイ・ネットメディアが果たす役割は広がっている。

セブン&アイ・ネットメディアの取締役で常務執行役員の飯田克也氏は、「複数の業態を連携させ、ネットとリアルを融合させることで、お客さま一人一人のニーズにいつでもどこでもお応えすることを目指している」と説明する。

統合に当たっては、事業会社ごとに異なる環境、異なるツールで開発されてきたシステムとの連携を図りつつ、顧客の環境やニーズに合わせ新規サービスやアプリ開発を進めてきた。その中で、OSSの活用は不可欠だという。「お客さまから求められるサービスは非常に多様化している。そうしたニーズに柔軟かつスピーディーに応えるために、さまざまな部分でOSSを導入して開発をしている」（飯田氏）

PoCで脆弱性を網羅的に洗い出す効果を確認し、「Black Duck Hub」を採用

一方で、セブン&アイ・ネットメディアが懸念していたのが、OSSに含まれる脆弱性への対応だ。同社は、システム開発に当たって、単体テストや結合テストの時点で商用のスキャンツールを用いて脆弱性の有無をチェックしてきた。

だが、こうしたテストには網羅性がないことが課題だった。「これまで用いたツールは、シナリオを組み立ててセキュリティをチェックするもので、ソースコードのホワイトボックステストのような網羅的な仕組みではない」と、同社デジタルソリューション本部クラウド推進部システム管理チーム、主任の廣瀬康幸氏は振り返る。

そこでセブン&アイ・ネットメディアが目を向けたのが、日本シノプシスが提供する「Black Duck Hub」だった。OSSを含めて脆弱性をチェックし管理できるツールを探す中で見つけた製品だ。サーバとスキャナー、クラウドに構築されたナレッジベースの3つで構成され、スキャナーでソースコードをスキャンし、その結果をナレッジベースでチェックし、脆弱性の有無を判断する非常にシンプルな構成である。「脆弱性情報が格納されているナレッジベースには、日本シノプシス独自の脆弱性情報も含めて約14万件もの情報が片々〜駈籠こ景柶者 ざれていり

自社開発システムで、気付かなかった脆弱性を発見

同社は Proof of Concept (PoC) を実施し、社内セキュリティ基準をクリアした Web システムとスマホアプリをスキャンしてみることにした。この結果、「高」に分類される脆弱性が Web システムとスマホアプリのそれぞれで見つかった。

セブン&アイ・ネットメディアはこの結果を目の当たりにし、従来利用してきたツールでは発見できなかった脆弱性を洗い出すことができ、脆弱性対応の強化につながると判断した。検出した脆弱性をグラフで可視化できること、コンポーネントごとに脆弱性の個数や脆弱性がないバージョンを明示できて対応に重宝することもポイントとなり、導入を決定。2017 年 11 月に運用を開始した。

「開発者に負荷をかけない」運用ルールを模索し、改善

セブン&アイ・ネットメディアでは見つかった脆弱性を修正するための手戻りや差し替え、コンポーネントのバージョンアップになるべく早く対処できるよう、開発プロセスの V 字モデルでいう一番下の、開発・プログラミングの段階でスキャンをかけることにした。

同社デジタルソリューション本部クラウド推進部システム管理チーム、マネージャーの出田ユカリ氏は、「スキャンをして改修し、チェックする……という PDCA サイクルに載せて運用する

必要が 0 タル 8 頁番・プログラミ i 忒肅 鰭 9 莞 多館 9 嚙理チーム、プリーユ 遵ウ 嶸 チェッォ / 游鯡澆尺ト 罍 涌