BLACKDUCK®

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。

セブン&アイ Net Media

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。

ブラック・ダックの調査「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」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、ブラック・ダックが提供する「Black Duck」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、ブラック・ダック独自の脆弱性情報も含めて約 14 万件もの情報が保存されている上、専任の担当者が数時間おきにアップデートしており、非常によくできた製品だと感じた」（廣瀬氏）

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ある。社内と調整し、時間をかけて運用ルールを作成した」と振り返る。

最も留意したのは「開発者に負荷をかけ過ぎないこと」（出田氏）だ。負荷をゼロにはできないが、セキュリティは顧客に安心・安全を届ける上で必須の事項。そのバランスを取ることに腐心したという。

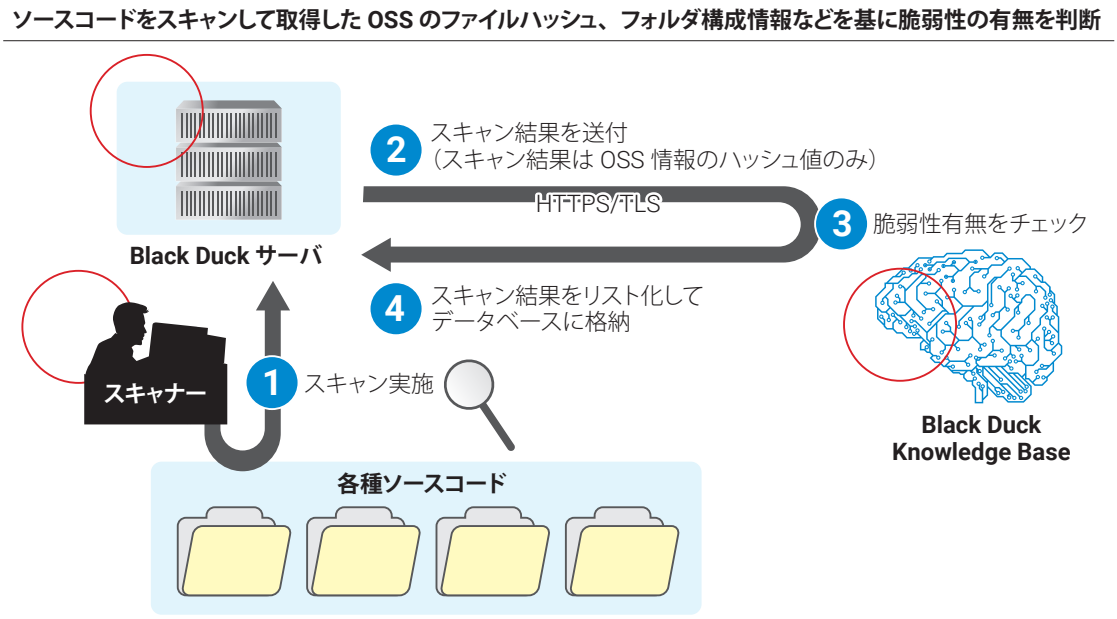
自身のコードを自身でチェックし、セキュリティ意識のさらなる向上を

Black Duckの導入によってセブン＆アイ・ネットメディアでは、これまで把握できなかったOSSを網羅的に管理する体制を整えた。

検査によって、非常に古いオープンソースのコンポーネントが発見されることもあるという。「オープンソースのライブラリを使うと、必要なものと一緒に余計なライブラリがくっついてくることもある。その余分なライブラリに古いモジュールが含まれることも往々にしてある。これまでなかなか見つけられなかったライブラリをBlack Duckで把握できるようになった」と飯田氏はいう。

セブン＆アイ・ネットメディアでは、廣瀬氏らセキュリティ担当にソースコードを渡してチェックをするのではなく、開発者自身がGUIでスキャンをして運用している。「自分たちが作ったもの、自分たちで管理しているものをスキャンした結果が目の前にぱっと出てくるので、開発者側のセキュリティに対する意識が高まっている」（廣瀬氏）ことも実感しているそうだ。

「開発者自身がBlack Duckの情報を基に、脆弱性のあるOSSと少ないOSSを見分け、より信頼性の高いOSSを用いて開発が進められるようになった」と出田氏。ひいては「システムを通してお客さまに安心・安全をお届けするというわれわれのミッションが、より現実になった」と廣瀬氏はいう。



Black Duckの概要

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

©2024 Black Duck Software, Inc. All rights reserved. Black Duck® は Black Duck Software, Inc. の米国およびその他の国における登録商標です。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。2024年9月