Secure Coding Checker

導入事例

▶KDDI株式会社 様

開発環境の異なるアプリのセキュリティ対策を一元管理する

スマートフォン、携帯電話の国内大手通信事業者である KDDI では、多数のアプリによるサービスを提供している。

一般的にスマートフォンは、夏／秋冬／春の各時期に発売されるため、提供するアプリについても新機種毎の対応が必要であり、且つ、既存機種への OS のバージョンアップ対応も必要となり、短い周期で品質管理を行わなければならない。特に KDDI として利用推奨しているアプリは多くのユーザーが使用するもので、脆弱性対策についても細心の注意を払う必要がある。しかし、アプリは多数あり、さらに開発するアプリごとに開発環境や進捗が異なっているため、複数のアプリを同じ基準にて検査し、かつ結果を一元管理できる環境が求められる。

検査と一元管理の方法として、KDDI では 2014 年 1 月から、ラックの Secure Coding Checker を採用し、アプリ担当者に対しガイドラインを提示して検査を行うよう促している。当初はテスト運用を行い、その後、試用期間を経て 2014 年夏より正式に導入にいたった。導入のきっかけは、「JSSEC（一般社団法人日本スマートフォンセキュリティ協会）のセキュアコーディングガイドに即した検査を行える機能性を備えていることと、瞬時に検査結果を確認できるスピード性だった」と、KDDI サービス統括本部サービス開発 1 部の溝口健次郎氏は語る。比較検討していた他社ツールと比べ、「ガイドに沿った検査が網羅されており、コストパフォーマンスに優れていた」点は大きな利点だったという。

目視での脆弱性チェックから飛躍的に工程がスピーディになった

KDDI では、2014 年の Secure Coding Checker 導入以前は、専任の担当者がソースコードをすべて机上確認で検査する方法を採っていた。しかし、この机上確認はいくつかの大きな問題があった。ひとつは作業工数とスピードの問題で、1 カ月に約 1 ～ 2 本というペースでしかチェックができなかったこと。もうひとつの問題は、ソースコード開示に対してアプリ担当者から難色を示されるケースが少なくなかったこと。その場合は、検査運用チーム側で脆弱性有無の確認がとれず、アプリ開発元のセキュリティ対策に頼るしかなかった。

溝口氏によると、「当時はアプリの数も少なく対応ができたが、数が増えるにつれ、処理が追いつかなくなってしまった。また、端末搭載アプリとして網羅性が無いこと、コストがかかることも問題となってきていた」という。そこでいくつかの Android アプリ向け脆弱性検査ツールを検討した結果、Secure Coding Checker をテストするに至った。

「導入のメリットとしてはいくつかあるが、スマー

トフォンに搭載するアプリがすべてカバーできるようになったことと、作業効率が格段に上がったことがもっとも大きかった」と、溝口氏は語る。目視の検査では最速でも３カ月で数個までしか対応できなかったが、１日で複数のアプリの検査を行え、さらに複数アプリの一元管理が可能になった。また、Secure Coding Checker は apk ファイルのみで即座にチェックできることも大きい。apk ファイルを登録するだけでその場ですぐ結果が出てくるので、何度もテストをして結果を収集できることはアプリ担当者にとってもメリットになっている。

さらに、「アプリの検査結果を個々にチェックする内製工数は必要であるが、外部のセキュリティ専門家に委託していた時代よりも、結果として全体の工数を減らせた」と、工数とコスト削減もメリットとして挙げている。

KDDI では、2019 年からは KDDI が提供するアプリすべてに脆弱性検査の実施をルール化し、その検査ツールとして Secure Coding Checker を採用している。KDDI サービス統括本部サービス開発１部の上松晴信氏は、「当初は検査結果で違反・注意が出るアプリが多く修正対応をお願いしていた。現在では、アプリ担当者のセキュリティ意識が高まり安全なコーディングをしていくようになった」と、その効果の大きさを語っている。

新任のアプリ担当者の危機管理意識もアップ

多数のアプリを開発している KDDI だが、Secure Coding Checker の導入は比較的容易だったという。まず、導入時にすべてのアプリ担当者に向けて、Secure Coding Checker を使う目的と内容についての説明会を行った。以降は、新任のアプリ担当者に対して説明を行っているが、簡単な説明内容でアプリ担当者に受け入れられているという。

上松氏によると、「Secure Coding Checker で初めてアプリを検査すると、違反・注意のアラートが多く出る。アプリのセキュリティ品質を高めるために、具体的にどのように対応すべきか相談されることが多い」という。それにより、アプリの脆弱性について危機感を持つようになるアプリ担当者も多く、脆弱性リスクに関しての危機管理への向上にもつながっていく。「検査結果に出た脆弱性がどのレベルのリスクなのか理解したうえでアプリ担当者に判断をしてもらう」と同時に、「過去の事例から蓄積した多数のノウハウを元に、検査運用チームからも対策についてアドバイスを行う」など、個々の事例に対応した対策をとっている。各アプリ担当者に対しては、検査結果での“違反・注意”と“不明”もゼロにするという基準を設け、各担当者が自分のアプリのリスクを完全に理解している状態であるように努めている。

上松氏によると、「アプリ仕様として“リスク受容”と仕分けする判断余地が設けられており融通が利く点も、Secure Coding Checker のメリット」だという。

迅速な対応で社内管理への移行もスムーズ

KDDI では、Secure Coding Checker 導入にともない、これまで一部を外部に任せていたアプリの検査管理を、社内ですべて行うようになった。「検査ツールを使ったことで利便性も上がり、内部で行うことによりコスト削減を図ることができた」と、上松氏はその理由について語る。「複数のアプリを管理する弊社の場合、アカウント発行管理が簡単に行え、複数の検査結果を同時に見られる機能が使いやすかった。検査運用を行っている現在、もしこの検査ツールがなかったら、アプリ開発に多大な影響が出てしまう」という。

また、KDDI では Secure Coding Checker についての意見や希望をアプリ担当者にアンケート調査を行い、開発元へ機能アップデートをリクエストして、さらなる使い勝手の向上をめざしている。

溝口氏は、「セキュアコーディングを行う重要性をもっとアプリの開発者に知ってほしい。どうやって意識づけしていくかが課題。答えがデジタルで出てくることで説得力が出る。まずは弊社でのセキュリティ対策を Secure Coding Checker でしっかり行い、できるところから啓蒙できればと思う」と語り、通信事業者としても、セキュリティ意識や脆弱性対策への啓蒙活動を行っていきたいとしている。

［お問い合わせ］
株式会社ラック
Secure Coding Checker 担当　E-mail sales@lac.co.jp
サービス紹介ページ https://www.lac.co.jp/service/consulting/scc.html