製品のセキュリティ

富士通の製品開発部門でのセキュリティ向上への取り組みの中から、オープンソースソフトウェアの脆弱性対応と人材育成に関する活動をご紹介します。

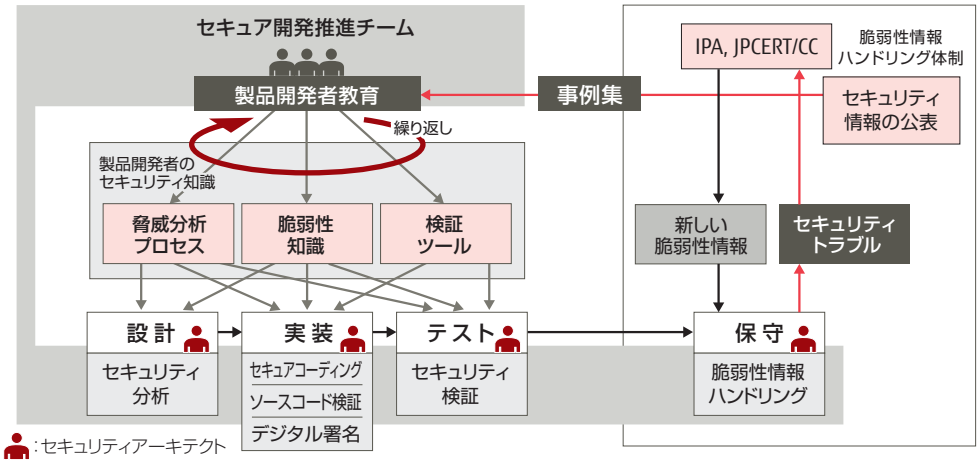
≫ ソフトウェア製品のセキュリティ品質向上への取り組み

富士通では、ファームウェアを含めたソフトウェア製品のセキュリティ品質を向上させるため、セキュア開発推進チームを中心に、下図に示す取り組みを行っています。具体的には、開発プロセスに次の1.から4.に示すセキュリティ品質を確保する活動を組み込んでいます。

1. 設計工程では、セキュリティ分析（脅威分析）と設計への反映を行います。
2. 実装工程では、脆弱性を作り込まないコーディング（セキュアコーディング）、ツールによるソースコード検証、必要に応じてプログラムへのデジタル署名を行います。
3. テスト工程では、ツールによるセキュリティ検証と、セキュリティ観点でのテストを行います。
4. 保守工程では、IPAやJPCERT/CCと連携して、セキュリティ脆弱性監視、迅速なセキュリティ修正パッチの提供、およびセキュリティ情報の公表を行います。

各工程においては、セキュリティ対応の専門知識を有したセキュリティアーキテクトを各部門に配置し、開発活動における適切なセキュリティ対応の浸透を図っています。開発者全体の1割の人材を確保しています。

ソフトウェア製品のセキュリティ対応プロセス



≫ オープンソースソフトウェアを利用した出荷済製品のセキュリティ確保の活動

「4.保守工程」の一環として行っているオープンソースソフトウェア（Open Source Software：OSS）を利用した製品のセキュリティ確保の活動をご紹介します。昨今のソフトウェア製品のニーズの多様化に伴い、当社製品で利用するOSSの種類も増えています。このため、それぞれのOSSの脆弱性に迅速に対応することが重要になってきています。そこで、OSSの脆弱性への対処を網羅的、効率化するための「OSS脆弱性対応システム」を社内のSE部門と共同で構築し、対応漏れの防止と迅速な対応に努めています。

OSS脆弱性対応システムの概要

1. OSS脆弱性情報の情報源にJVN iPedia脆弱性対策情報データベース※1を採用しています。これにより、NVD（National Vulnerability Database）※2番号が割り当てられた脆弱性を網羅しています。
2. 製品リポジトリに格納されている情報を基に、脆弱性情報の収集対象OSSを設定しています。これにより、製品で利用している全てのOSSを、脆弱性調査の対象とすることができます。
3. OSS脆弱性対応システムに収集された脆弱性情報は、製品リポジトリに格納されている製品別OSS情報と照合の上、即座に製品開発者に通知されて、脆弱性対応が始まります。

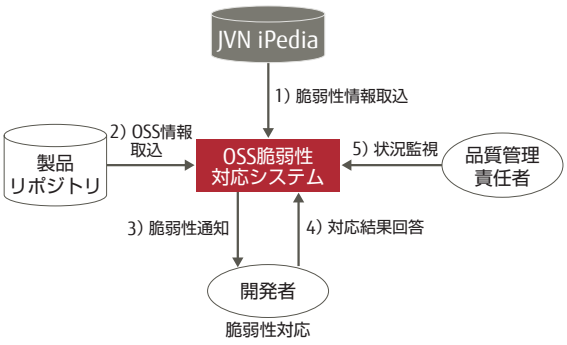
4. セキュリティは優先度の高い問題と位置付けられており、OSS脆弱性も優先度を上げて調査を実施します。対応状況は製品開発部門の品質管理責任者がチェックしており、対応が停滞していた場合は指導が行われます。

なお、情報源として、各種のインターネット公開情報も利用します。

〔※1〕JVN iPedia脆弱性対策情報データベース：JPCERT/CCと情報処理推進機構（IPA）が共同で管理している脆弱性情報データベース。2007年以降にNVDに登録された脆弱性情報を網羅している。

〔※2〕NVD（National Vulnerability Database）：米国NIST（National Institute of Standard and Technology）が管理している脆弱性データベース。

OSS脆弱性対応システムの概要



製品開発者教育

ソフトウェア製品開発部門のセキュリティ教育には、プロフェッショナル人材に向けた「セキュリティアーキテクト教育」と、一般の製品開発者・製品検査担当者に向けた「一般教育」の2系統があります。

セキュリティアーキテクト認定制度

セキュリティアーキテクトとは、ソフトウェア製品のセキュリティ品質を向上させるための、セキュリティ対応活動の推進役となる社内プロフェッショナル資格であり、ソフトウェア製品開発部門では育成プログラムを含むセキュリティアーキテクト認定制度を運用しています。

セキュリティアーキテクトの育成プログラムは、各開発担当部署から推進された候補者に対して数ヶ月かけて4つのフェーズにより実施されるカリキュラムであり、①事前学習と課題作成、②集合教育（演習形式）、③脅威分析レポートの作成、④認定ヒアリングで構成されます。

セキュリティアーキテクトとして認定された後は、スキルアッププログラムとして、下図に示す以下の内容の研修会を年1～2回の頻度で、定期的に開催しています。

- 他部署のセキュリティ活動紹介
- 社内障害事例紹介
- 専門組織の研究報告
- セキュアなソフトウェアの開発プロセス（最新情報）

研修会を通して、個々のスキルアップや知識の更新を図ると共に、意見交換や情報交換が行われることにより、セキュリティアーキテクト同士の意識啓発を図っています。

一般教育

一般教育は、新人教育をはじめとするe-Learningや集合教育のほかに各部門内での教育、社外講師を招いてのセミナーなど、様々なメニューを用意して、セキュリティ対応能力の向上を図っています。

脆弱性やセキュア開発プロセスなど重要な事項は、開発者にも必要な知識となることから、セキュリティアーキテクト教育と共通で一般教育でも提供しています。

製品開発者教育マップ