

**オープンソース・ソフトウェアの
セキュリティ確保に関する調査報告書**

2003年3月



情報処理振興事業協会

セキュリティセンター

総論

情報インフラの構成要素として、オープンソース・ソフトウェア（Open Source Software）が利用されるケースが増えている。その一方で、オープンソース・ソフトウェアのセキュリティが重要な問題となってきている。オープンソース・ソフトウェアでは基本的にセキュリティは保証されておらず、自己責任において利用されるべきものとされている。しかしオープンソース・ソフトウェアのセキュリティについて深く検討もせず導入を行ったために、その脆弱性をつかれて、不正にアクセスされる例は年々増大しており、利用者側でのオープンソース・ソフトウェアのセキュリティ確保が急務とされてきている。

オープンソース・ソフトウェアのセキュリティに関しては、オープンソース・ソフトウェアを利用する側と、開発する側の両面から考える必要がある。オープンソース・ソフトウェアを開発する側からは、ISO/IEC 15408 などの評価制度がセキュリティ確保の手段として挙げられる。しかし、オープンソース・ソフトウェアは開発そのものがオープンであり、商用のソフトウェアの開発とは違った開発モデルが採用されており、必ずしも ISO/IEC 15408 には適していない。ISO/IEC 15408 では保証要件として技術的要素だけでなく、開発体制などの保証要件も満たされなければならない。オープンソース・ソフトウェアの開発には適用しにくい。一方、オープンソース・ソフトウェアを利用する側からすればこうした側面が、セキュリティの問題となる。コストが低いから仕方ないという考え方もあるが、利用する以上、オープンソース・ソフトウェアのセキュリティを自己責任において評価するための仕組みやガイドが示されていることが重要である。

オープンソース・ソフトウェアの利用は、今日ビジネスにおいても急激に増大しており、オープンソース・ソフトウェアのセキュリティ確保のための技術的、方策的な対策に対する重要性は増している。本調査では、オープンソース・ソフトウェアの特徴を考慮し、オープンソース・ソフトウェアの利用者（SI ベンダー等を含む）の立場から、有益な情報を取りまとめ、利用に際してセキュリティを確保するためのフレームワークを作成することを目的とし、オープンソース・ソフトウェアの安全な利用のための技術的、方策的な項目について調査を実施したものである、

本調査報告書は、以下の 6 部から構成される。

第 部 オープンソース・ソフトウェアのセキュリティ確保

オープンソース・ソフトウェアのセキュリティに関する議論をまとめ、いかにしてオープンソース・ソフトウェアのセキュリティを確保していくかについてみていく。ここではオープンソース・ソフトウェアのセキュリティ確保のフレームワークを提案する。本フレームワークは、オープンソース・ソフトウェアのセキュリティを確保するために、(1)ソースコード検査、(2)脆弱性対応、(3)運用管理の3項目を継続的に実施するための枠組みである。それぞれの詳細については第 部、第 部、第 部に示す。

第 部 効率的なソースコード検査技術の調査

ソースコードの検査を自動的に行うためのツールに関しての調査である。各ツールがどのような脆弱性コードの検出に効果があり、どういった技術が利用されているのかについて機能的な説明を行う。また実際の脆弱性を持つソフトウェアを用いて、どの程度の検査の精度があるのかについて検証する。

第 部 セキュアな実行コード・実行環境技術の調査

セキュアな実行コードを作成するツールや、ソフトウェアをセキュアに実行するための実行環境に関しての調査である。各ツールがどのような脆弱性に効果があり、どのような技術が利用されているのか機能的な説明を行う。また実際の脆弱性をもつソフトウェアを用いて、どの程度脆弱性への対応が行われるのかについて検証する。

第 部 オープンソース・ソフトウェアをセキュアに保つための運用ガイド

オープンソース・ソフトウェアを運用管理していくためのガイドを示す。ここでは、オープンソース・ソフトウェアの運用モデルを提案し、そのモデルに基づき、利用者が運用管理としてどのようなことをしなければならないのかについて整理する。

第 部 効率的なソースコード検査技術利用ガイド

ソースコード検査ツールの一つである RATS を取り上げ、インストールや利用方法について説明する。

第 部 セキュアな実行コード・実行環境技術利用ガイド

実行コード生成技術の一つである Stack Smashing Protector と、実行環境の一つである Libsafe を取り上げ、インストール方法や利用方法について説明する。