研究開発構想（個別研究型）
サプライチェーンセキュリティに関する不正機能検証技術の確立
（ファームウェア・ソフトウェア）

「バイナリー静的解析による不正機能および脆弱性の検証技術の研究」

研究開発実施報告書（年次）

令和6（2024）年度

研究代表者
森　彰
産業技術総合研究所　サイバーフィジカルセキュリティ研究センター　研究チーム長

１．当該年度における研究開発の実施概要

（１）研究開発概要

ファームウェア等に不正機能や脆弱性が存在するかを、プログラム実行やソースコード参照を行うことなく検証する自動化技術を開発します。プログラム解析技術に加えて生成系 AI 技術を活用することで、人手による作業なしに自動検証が行えるようにします。検証結果に加えて、機能を単位としたソフトウェアの構成情報やリスクを明確に説明するリスク評価ケースを提供することで、利用者による不正機能や脆弱性への対応を支援します。

（２）実施内容と成果の概要（研究開発開始から当該年度末まで）

令和 6(2024)年度

これまでに開発を進めてきた静的バイナリー解析ツールを改良し、Wi-Fi ルーターのような実機器のファームウェアに潜む脆弱性を検査することが可能であることを示しました。コマンドインジェクションのようにデータの流れを追跡するだけで同定できる脆弱性に加えて、スタックオーバーフローのようにデータ書き込みが行われるメモリ領域の配置を計算しなければならない脆弱性(の一部)も同定できるようになりました。プログラムを実行しなくてもソースコードがなくても解析を行えることが大きな特徴です。

脆弱性を発見するだけではなく、その危険性をわかりやすく説明したリスク評価ケースと呼ぶ定型ドキュメントを、アシュアランスケースの手法を応用して作成する研究を行いました。アシュアランスケースは、エビデンスをもとにシステムの安全性、信頼性を議論し説得するための文書化技術ですが、これを脆弱性等のリスクを説明するために利用することで、ソフトウェアのサプライチェーンを通じた対策の迅速化につながると考えています。こうしたリスク評価ケースを記述するためのガイドラインのドラフトを作成しました。

脆弱性の対応については SBOM(Software Bill of Materials)の利用が推進されていますが、SBOM では手が届かないような細かな機能単位でのソフトウェア依存関係が重要になると考えられます。ビルドオプションや実行オプションによって生じる細粒度のソフトウェア構成情報を活用するための研究開発を行なっています。どのような依存関係があるか調査して分類し、必要な対策について検討を行いました。

生成 AI 技術の高度化とセキュリティへの応用スピードには目覚ましいものがあります。本課題においても、コード理解能力を有した大規模言語モデルを活用して、バイナリーコード解析を支援する手法について研究開発を行なっています。公開されている言語モデルを利用して、実用レベルの脆弱性分析が可能であることを、実験を通して確認しました。

２．主たる研究分担者一覧

横山 浩之(国際電気通信基礎技術研究所 適応コミュニケーション研究所 所長)

白石 善明(神戸大学 大学院工学研究科 教授)

橋本 政朋(千葉工業大学 人工知能・ソフトウェア技術研究センター 主席研究員)