理論とシステムソフトウェアの融合で安全・安心なIoTを実現する

研究ソフトウェア信頼性保証のためのソフトウェア認証機構

山下 直希[1] 合田 憲人[1,2] 丹生 智也[3] 坂根 栄作[1] 竹房 あつ子[1,2] 小野 泰司[4] 石川 裕[5] 青木 信雄[2]
1国立情報学研究所, 2総合研究大学院大学 3国立遺伝学研究所, 4情報セキュリティ大学院大学, 5大妻女子大学

どんな研究？

本研究では、IoT機器などに使われるソフトウェアに悪意のあるものが混ざるリスクに対応するため、**第三者による検査・証明**を通じて信頼性を確認できる仕組みを整備する
それにより誰でも安全に研究ソフトウェアを利用・共有できる環境の実現を目指している

何がわかる？

- ソフトウェアが安全な方法で作られたことを確認できる
- ソフトウェアに脆弱性がないか確認できる
- 新たに脆弱性が発見された場合にも利用者がすぐに対応できる

背景・目的・研究内容

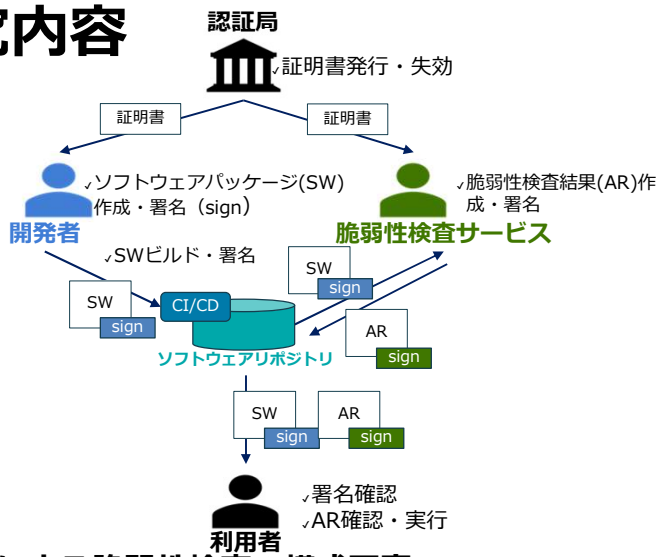
研究背景

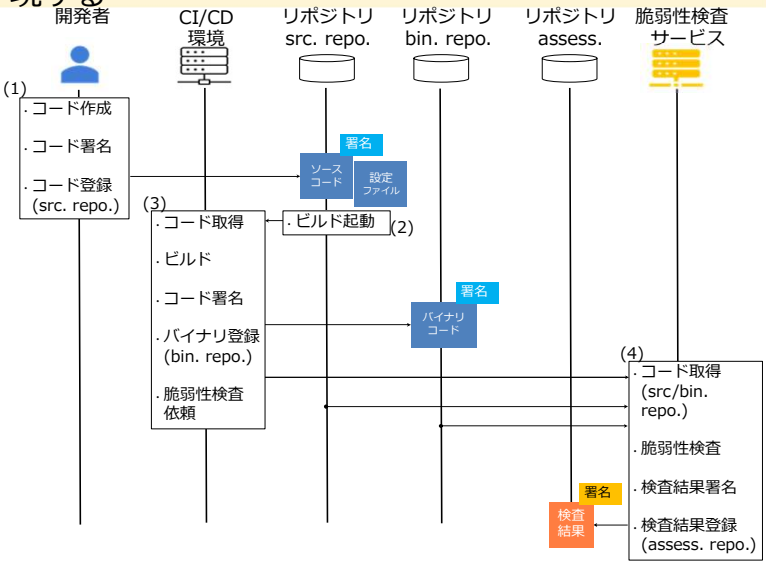
研究者は開発や実験でフリーソフトウェアを利用することが多いが、脆弱性や悪意のある処理が含まれている可能性があり、重大な被害を引き起こすリスクがある。こうしたソフトウェアを安心して利用するための方法が十分に整備されておらず、安全な活用を妨げる要因となっている。

研究目的

研究ソフトウェアの安全な利用を可能にするため、ソフトウェアの完全性と安全性を客観的に確認できる仕組みの構築を目的とする
開発者の電子署名・ソフトウェアの構築過程の監視・第三者機関による脆弱性検査を組み合わせて実現する

研究内容





第三者による脆弱性検査の構成要素：

脆弱性検査サービス：ソフトウェアの脆弱性を検査をする第三者機関
認証局：開発者・脆弱性検査サービスに電子署名用の証明書の発行する機関
ソフトウェアリポジトリ：ソフトウェア・脆弱性検査結果が登録されるリポジトリ

ソフトウェアの構築過程の監視・脆弱性検査：

(1)開発者がアプリケーションコードをリポジトリに登録
(2)CI/CD環境上で自動的にビルド処理を起動
(3)バイナリコードを生成し、電子署名の上でバイナリリポジトリに登録（ビルドログを生成）
脆弱性検査サービスへの検査依頼を送信
(4)検査対象のコードを取得、電子署名の検証後、CVE等に基づくコードスキャンや静的解析ツールによる検査を実施し、検査結果を署名付きでリポジトリに登録

今後の課題：

- ソフトウェア認証機構のスケーラビリティ検証
- システムの安全性検証など、実環境での運用を見据えた課題の解決

JST CREST 「形式検証とシステムソフトウェアの協働によるゼロトラストIoT」https://zt-iot.nii.ac.jp/
国立情報学研究所,京都大学,情報セキュリティ大学院大学,東京情報デザイン専門職大学