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）

プログラム・オフィサー（PO）

松本　勉
産業技術総合研究所 フェロー

サプライチェーンの複雑化やグローバル化が進展する中、情報システムに対し悪意のある機能が組み込まれるおそれがあるなどの、いわゆるサプライチェーン・リスクへの対応・対処が日々重要な課題となってきています。この様な社会的背景のもと、本構想の目標達成に向けて、＜不正機能の意図性に関する評価手法＞、＜ソフトウェア構成の情報を活用した不正機能の検証手法＞および＜システム・サービスのレジリエンス性の確保に関する手法＞の三種類の手法の開発を目指します。

不正機能検証という重要な研究テーマに関して、実践的に活用可能な技術プロダクトを創出するために求められる、具体的なツール・システムへの要求や潜在的なニーズをヒアリングしつつ、POとしてKプログラムへのご期待に添えるよう、研究実施者の皆さまと共に研究を進めてまいります。

研究開発構想概要

❶ 意図性の評価

過去の事例の分析により、不正機能の体系化・類型化を行うとともに、不正機能が意図的に埋め込まれた可能性を評価する方法論を整理し、ツール化するための開発・実証を行う。

❷ 不正機能の検証

OSSのみではなくプロプライエタリソフトウェアも対象に、ソフトウェア構成情報を活用した不正機能検証の効率化・高度化の方法論を整理し、ツール化するための開発・実証を行う。

❸ レジリエンス性の確保

重要インフラ分野における制御システムについて、インシデント発生時のシステム・サービスへの影響を最小限に留めるために、残存リスクを最小化するための対策候補を自動的に生成・提案する方法論を整理し、ツール化するための開発・実証を行う。

支援対象となる技術　▶不正機能検証技術（ファームウェア・ソフトウェア）

予算額　最大25億円程度

研究開発構想の詳細はこちらから
https://www8.cao.go.jp/cstp/anzen_anshin/20230310_mext_2.pdf

■ 分科会委員（アドバイザー）

新井 悠　株式会社ＮＴＴデータグループ 技術革新統括本部 品質保証部 情報セキュリティ推進室 エグゼクティブ・セキュリティ・アナリスト
井上 克郎　立命館大学 情報理工学部 特別招聘教授
岩村 誠　ＮＴＴ株式会社 ＮＴＴ社会情報研究所 上席特別研究員
後藤 厚宏　情報セキュリティ大学院大学 情報セキュリティ研究科 教授

■ 研究開発課題

公募枠　ソフトウェア構成の情報を活用した不正機能の検証手法

グラント番号　JPMJKP24K1

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部門 総括研究主幹

課題概要

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。

グラント番号　JPMJKP24K2

脆弱性と不正機能検知によるサプライチェーンセキュリティのリスク評価手法の研究開発

研究代表者
山内　利宏
岡山大学 学術研究院環境生命自然科学学域 教授

課題概要

ファームウェアに含まれるバイナリコードやそのソースコードを対象として、攻撃に悪用される可能性のある脆弱性や不正機能を高い精度で検知する手法を研究開発します。また、サプライチェーン上で連携するシステム間の脆弱性や不正機能を考慮したリスク評価手法や、リスク評価に基づくリスクマネジメント手法を確立します。これらの研究成果の有効性を評価できるツールも開発します。

公募枠　システム・サービスのレジリエンス性の確保に関する手法

グラント番号　JPMJKP24K3

サイバー攻撃下の抗堪性を確保するインフラ運用支援システムの実現

研究代表者
高倉　弘喜
国立情報学研究所 アーキテクチャ科学研究系 教授

課題概要

サイバー攻撃の完全阻止が困難で、かつ、攻撃で発生する被害への対応中でもサービス継続に必須の機能の維持を求められる重要インフラにおいて、そのレジリエンス(抗堪（こうたん）性)確保に取り組みます。特に、物理現象や化学反応の制御など瞬時に停止できない重要インフラの題材として医療に焦点を当て、人の安全が確保できるまで被害拡大を抑えつつ、被害が発生した機器の隔離の可否判断、代替措置の確保までの必須機能の維持を自動で行う手法を開発します。

公募枠　不正機能の意図性に関する評価手法

グラント番号　JPMJKP24K4

不正機能の意図性評価に関する方法論整理及び評価ツールの開発

研究代表者
金居　良治
株式会社FFRIセキュリティ 専務取締役 最高技術責任者（兼）ナショナル・セキュリティ事業本部長

課題概要

本研究開発では、不正機能事例の調査および不正機能の類型化・体系化を行った上で、意図性評価の方法論整理および意図性評価ツールの開発を行います。意図性評価の方法論整理においては、不正機能の技術的な特徴や外部の周辺情報など、不正機能の意図性を示す観点を網羅的に整理し、複合的な視点で意図性を評価する方法を開発します。意図性評価ツールの開発においては、評価者の入力に従い意図性評価の結果を出力する機能および評価に必要な情報を収集・蓄積・参照可能な機能を開発します。