審 査 の 結 果 の 要 旨

氏　　名　　碓井 利宣

本論文は、「Automation of Building Malicious Script Analysis Systems for Diverse Execution Environments （悪性スクリプト解析における多環境対応のためのシステム自動構築に関する研究）」と題し、実行可能バイナリ以外の形式を持つマルウェアである悪性ファイル、とくに悪性スクリプトを解析するシステムに関して、多様な実行環境に汎用的に適用するためにシステムを自動的に構築する新たな枠組みを開拓するとともに、多角的な解析機能を実現するための方式を体系的に示している。論文の構成は「Introduction」を含め７章からなる。

第１章は「Introduction（序論）」で、本研究の背景として、サイバーセキュリティにおける喫緊の課題である悪性ファイルの解析および検出について述べ、研究の位置付けを明らかにしている。とくに、脆弱性を悪用するエクスプロイトファイルとスクリプト実行環境を悪用する悪性スクリプトへの対策が重要であること、および、そうした対策の多様な環境への適用に課題があり汎用的に適用可能な技術の確立に大きな意義があることが、明らかにされている。

第２章は「Static Return-Oriented Programming Chain Detection（Return-Oriented Programmingチェーンの静的検出）」と題し、エクスプロイトファイルが用いるReturn-Oriented Programming (ROP) チェーンと呼ばれる攻撃コードを、そのバイト列を学習することで、人手で定義されたルールを要さずに精度よく検出する方式を提案している。この方式は実際の実行を伴わない静的検出のため多様な環境に適用可能であり、既存の動的検出技術や脆弱性緩和機構を補完した多層防御によりエクスプロイトファイルの根絶に向けて大きく貢献することを示している。

第３章は「Automatically Building Script API Tracers（スクリプトAPIトレーサの自動構築）」と題し、スクリプトエンジンのバイナリ解析により、悪性スクリプトの解析ツールの一つであるスクリプトAPIトレーサを自動的に構築する方式を提案している。とくに、バイナリ解析時に入力するスクリプトに工夫を施すことで解析システムの構築に必要な情報を引き出すという、第３章から第５章にかけて共通する新たな解析の枠組みを、提案している。この方式の実装を通して、解析システムの自動構築により多様なスクリプト言語やスクリプトエンジンに対して汎用的な解析を実現できることを明らかにしている。

第４章は「Automatically Building Script Multi-Path Explorers（スクリプトマルチパスエクスプローラの自動構築）」と題し、スクリプトエンジンのバイナリ解析により、悪性スクリプトの解析ツールの一つであるスクリプトマルチパスエクスプローラを自

動的に構築する方式を提案している。この方式を通して、スクリプトを解釈実行する仮想機械の解析によって実行経路の制御に要するアーキテクチャ情報を取得できることを明らかにするとともに、その情報に基づいて構築されたマルチパスエクスプローラが解析妨害機能を具備した悪性スクリプトの挙動の解析に貢献することを実験的に示している。

第５章は「Automatically Building Script Taint Analysis Frameworks（スクリプトテイント解析フレームワークの自動構築）」と題し、スクリプトエンジンのバイナリ解析により、スクリプトに対するテイント解析フレームワークを自動的に構築する方式を提案している。この方式では、型変換がスクリプトのテイント解析に固有の問題を引き起こすことを明らかにするとともに、型変換を司る関数を特定することでその問題の解消を実現している。これにより、多様なスクリプトに対するテイント解析を可能にすることで、悪性スクリプトの具備する解析妨害機能の仕組みの解明をはじめとした様々な解析の実現に貢献することを示している。

第６章は「Overall Discussion（全体の議論）」と題し、本研究の全体に関する横断的な議論を展開している。とくに、第３章から第５章にかけて提案している方式の統合で構築される解析システムがいかなる多角的な解析能力を持つか明らかにするとともに、その応用によって既存のマルウェア検出および分類をいかに高度化できるかを論じている。また、研究で得られた洞察に基づき、今後のスクリプトエンジン開発のあるべき姿についてサイバーセキュリティの観点から提言している。

最後に第７章は「Conclusion（結論）」で、本研究の総括を行い、併せて将来展望について高い見識で述べている。

以上これを要するに、本論文は、悪性ファイル、とくに悪性スクリプトに対する解析システムを多様な環境に適用可能とするために自動構築する方式を、種々の解析機能を実現する観点から体系的に論じたものであり、多角的な解析を通した悪性ファイル対策の高度化により、また、解析システムの自動構築による多様な環境への適用という新たな取り組みの開拓により、そして両者合わせてマルウェア対策研究に有益な将来展望を与えることにより、電子情報学、特に情報セキュリティ工学上貢献するところが少なくない。

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。