論 文 内 容 の 要 旨

博士論文題目 Reversing Malicious Intents in Web Scripts: from Automating Deobfuscation to Assigning Concepts
「ウェブスクリプトの悪意を暴く：難読化の自動解読からコンセプトの割り当てまで」

氏　　名 Gregory BLANC

This thesis addresses the problem of how to infer the intentions purported by malicious client-side scripts when they are concealed to evade detection.
A central contribution of the thesis is the proposal of a client-side analysis system able to thwart advanced techniques of evasion such as obfuscation, while trying to minimize time performance overheads to preserve usability.

A first stage allows the detection of hierarchical patterns characteristic of obfuscation, in order to extract suspicious script code. A subtree matching pushdown automaton identifies such patterns in the abstract syntax tree representation of script programs.

In a second stage, the programming concepts are revealed by deobfuscating obfuscated strings using rewriting logic. Obfuscated strings can be reduced to a normal form by considering deobfuscation as a set of terminating and confluent rewrite rules.

Finally, the deobfuscated script is decomposed in object units, each implementing a distinct concept. These concepts are then assigned a higher-level concept by using prior knowledge of the script programming language, in order to reverse the initial intention of the developer.

氏　名	Gregory BLANC

（論文審査結果の要旨）

本論文では、最近広く活用されているWeb2.0型サービスにおいて広く使われている Java Script 言語で構築されたアプリケーションの内、クライアント側で実行されるスクリプトによるアプリケーション対象として、そこに悪意有るコードが内包されているかどうか、別の言い方をすればマルウェアかどうかの判定を行う手法についての研究をまとめたものである。現在 CGM と総称されるようなウェブサービスでは、ユーザ側からのデータの入力等、双方向型の情報交換が発生する。より高度なユーザインタフェースを提供するために、Java Scriptを使ったクライアント側で実行されるアプリーションとして実装されることも広く行われている。しかしクライアント側での実行を伴うために、近年 Java Script によるマルウェアも増加している。本研究では、クライアント側に実装されるマルウェア解析機構を実装したことが主な貢献である。特に、従来手法と事なり、難読化解読プロセスを経た後で、ソースコード解析（静的解析）を行い、マルウェアが実行しようとしたことを判明しようとした挑戦が評価出来る。従来手法では、安全な環境で実際にアプリケーションを実行して評価する動的解析が一般的であったが、事象の完全な解明は難しく、静的解析の必要が専門家らによって指摘されていた。本研究は、まさにこの挑戦を行ったものであり、高く評価することができる。また、単純なソースコード解析ではなく、実行時の意図を判明させるために、より論理的な解析を行っているところも新規性が高い。本研究では、単に本方式を提案するだけでなく、プロトタイプ実装を行い、既存の悪意を持った Java Script（難読化有り）アプリケーションに適用し、その実効性の確認も併せて行っている。当然ながら、マルウェア開発側の実装技術の向上に対応していくためには継続的な開発と解析環境整備が必要であるが、本手法により多くのマルウェア解析が可能になり、同時にユーザ保護にも大きく貢献することが期待できる。

以上により、本博士論文は研究内容について新規性並びに有効性があることが認められ、博士（工学）の学位を授与するにあたって十分な内容であると認められる。