動的解析ログを活用した静的解析補助手法

中島 将太[1,†1]　大月 勇人[1]　明田 修平[1]　瀧本 栄二[1]　齋藤 彰一[2]　毛利 公一[1]

概要：マルウェア対策では，マルウェア解析が重要である．一般的にマルウェア解析は，動的解析，静的解析の手順で行う．しかし，静的解析は動的解析で得られた情報を活かせていない．特に，動的解析時に記録した API 呼び出し情報と逆アセンブルコードを対応付けていないため，静的解析時に API 呼び出し情報を活用できていない．また，静的解析を行うためにはマルウェアの実行に関するすべてのコードを取得する必要がある．以上の背景から，本論文では動的解析時の API 呼び出し情報とマルウェアの実行に関するすべてのコードを取得し，静的解析を補助する手法を提案する．さらに提案手法をシステムコールトレーサ Alkanet と逆アセンブラ IDA へ適用し，マルウェア 25 検体を解析することで提案手法の有効性を示す．

本招待論文は，情報処理学会論文誌に掲載されました「動的解析ログを活用した静的解析補助手法」[1] についてご紹介いただくものです．

参考文献

[1] 中島将太，大月勇人，明田修平，瀧本栄二，齋藤彰一，毛利公一：動的解析ログを活用した静的解析補助手法，情報処理学会論文誌，Vol. 59, No. 2, pp. 800–811 (2018).

[1] 立命館大学
[2] 名古屋工業大学
[†1] 現在，サイバーディフェンス研究所