松浦研究室

[コンパイラ推定によるマルウェア対策技術の高精度化]

生産技術研究所　情報・エレクトロニクス系部門
Department of Informatics and Electronics, IIS
http://kmlab.iis.u-tokyo.ac.jp
情報セキュリティ
情報理工学系研究科　電子情報学専攻

機械語命令列に基づくマルウェア対策技術

Anti-malware Technologies Based on Machine Instruction Sequence

マルウェア（悪意のあるソフトウェア）への対策において、機械語命令列は生成に用いられたコンパイラの種類や最適化オプションなどの影響を受けやすく、それに起因して検知や分類の精度が低下する特性があります。

本研究室では、コンパイラの種類や最適化オプションを推定することでこの影響を削減し、精度を向上させる研究をしています。

確率モデルによるコンパイラ推定手法

Compiler Estimation Method by Stochastic Model

機械語命令の並びを遷移として捉え、コンパイラごとに隠れマルコフモデルでモデル化しています。このモデルをもとに尤度を算出することで、最も尤もらしいと考えられるコンパイラを推定します。これにより、現在マルウェアの生成に用いられたコンパイラを70%ほどの精度で推定可能です。

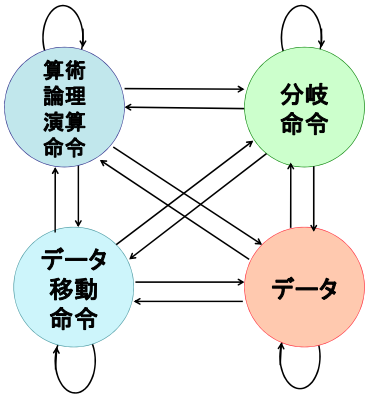

図1. 機械語命令列の状態遷移モデル

マルウェア対策技術の精度向上への応用

Application to Precision Improvement of Anti-Malware Technologies

コンパイラ推定の結果を、マルウェア対策技術の精度向上に応用しています。例えば、図2のように事前にコンパイラ別に分類しておくことで、コンパイラの種類による影響を回避でき、精度の向上が期待されます。

この研究成果は、単一の手法だけでなく、機械語命令列に基づいた様々なマルウェア対策技術に広く適用することが可能です。

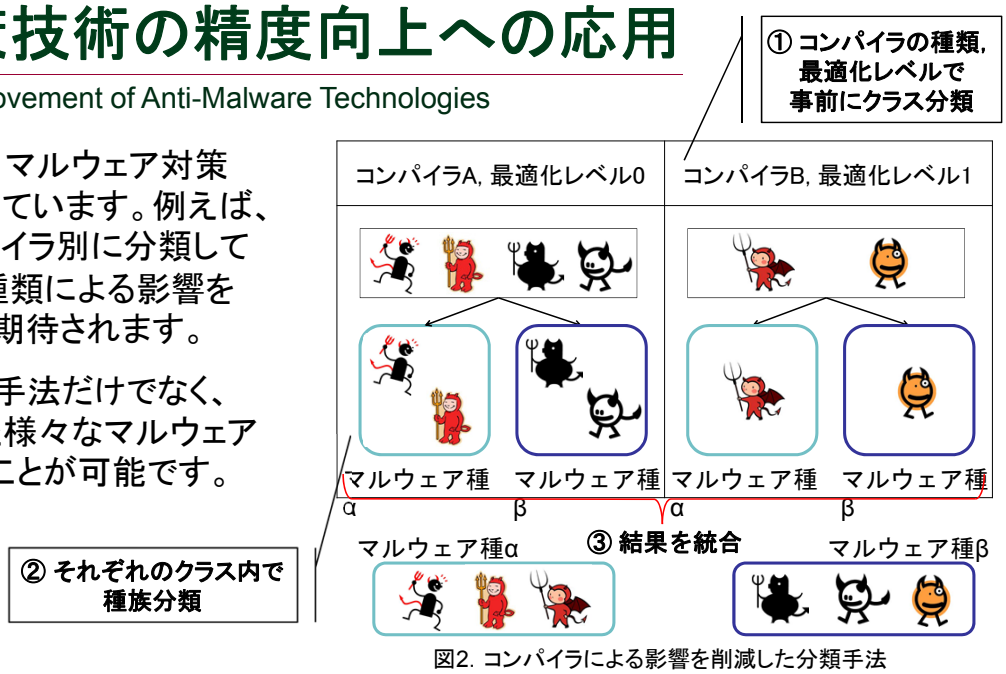

図2. コンパイラによる影響を削減した分類手法