トップエスイー修了制作

モデル検査技法を用いた マリシャスコードパターンの分析

JPCERT コーディネーションセンター　椎木 孝斉　takayoshi.shiigi@jpcert.or.jp

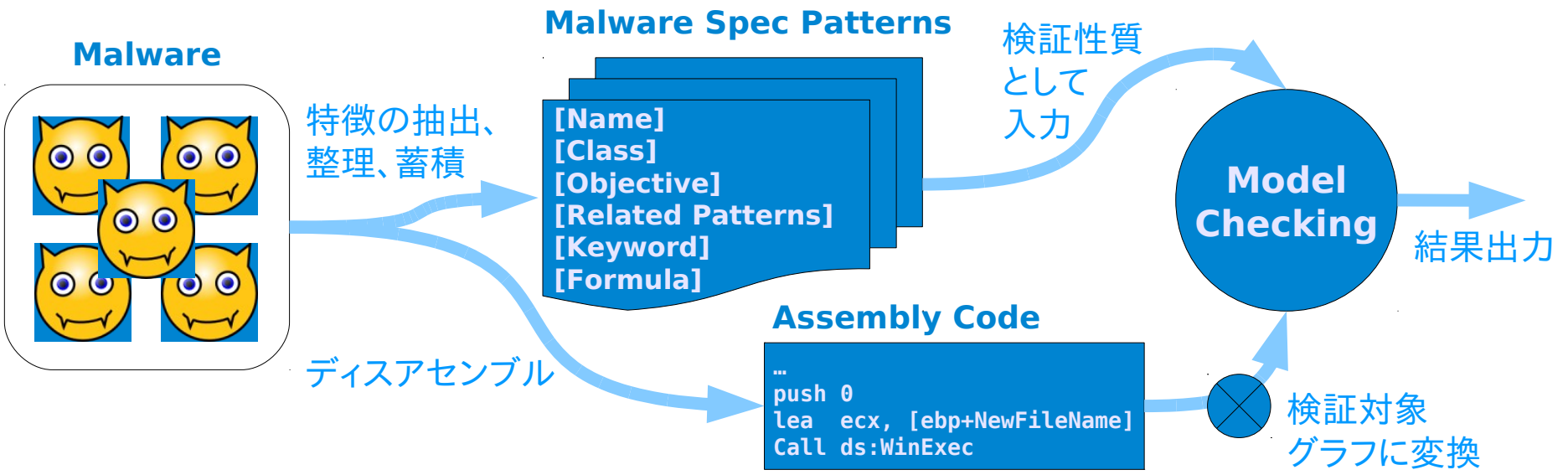
セキュリティ上の問題点

・近年、インターネットセキュリティインシデントの多くがマルウエアに関連するものとなっており、その対応が大きな課題となっている。
・マルウエア対策を行うためには、その脅威を明らかにするために分析を行う必要があるが、マルウエアの分析（特にコード分析）は難しく、必要な知識の蓄積、共有も十分ではない。

手法・ツールの適用による解決

・マルウエアのコード分析（静的分析）に必要な情報（マルウエアの挙動の特徴、分析ノウハウ等）をパターン（Malware spec pattern）として整理された形式で、作成、蓄積する。
・作成されたMalware spec patternについて、分析対象のマルウエアがその性質を満たすかどうかをモデル検査技法を用いて検証する。

提案手法の概要



Malware Spec Patternの例

[Name]
Downloader
[Class]
Common malware behavior
[Description]
Malware download program from remote site and execute it. .....
[Objective]
- To achieve initial attack smart....
[Related patterns]
Write exec
[Keyword]
URLDownloadFileA
WinExec | CreateProcess | ShellExecute
[Formula]
and @apicall(URLDownloadFileA(0, [_], [x]))
(EX EU @noassign(x) @@Exec(x))

期待される効果

・マルウエアの挙動の特徴や、分析ノウハウ等を様々なパターンとして、再利用可能な形で作成しておくことで、マルウエア分析に関する知識の蓄積、共有が可能となる。

・マルウエアのコード分析（静的分析）とモデル検査技法を組み合わせた検査を行うことで、より効率的、効果的なマルウエア分析を実施することが期待でき、対策に役立てることができる。

・今回提案する手法を分析者や技術者が使い易いツールとして実装することで、形式手法やモデル検査技法といった手法の当該分野への適用を進めることができる。