Windows API の監視による未知ウイルス検出手法の検討

三根　健司*，鈴木　秀和，渡邊　晃(名城大学)

Researches on Virus Detection Method based on Windows API Monitoring

Kenji Mine, Hidekazu Suzuki, Akira Watanabe (Meijo University)

１．はじめに

近年，急速にインターネットが普及したことによりコンピュータウイルス（以下ウイルス）による被害の増加が大きな社会問題となっている．特にウイルスが難読化，複雑化して検出が困難であることや，未知のウイルスを検出できないことが問題となっており，未知ウイルス検出システムが研究されている(1)(2)．本稿では，Windows API を監視することにより未知ウイルスを検出する手法の検討を行ったのでそれについて報告する．

２．ウイルス検出技術

ウイルス対策ソフトに用いられているウイルス検出技術にはパターンマッチング，ヒューリスティックスキャン，ビヘイビアブロッキングなどがある．

パターンマッチングはあらかじめウイルスの特徴（パターン）を記述したファイル（ウイルス定義ファイル）をウイルス対策ソフト内に持っておき，この情報と検査対象ファイルを比較する手法である．

ヒューリスティックスキャンは動作前のプログラムの内容をチェックし，システム領域や DLL の書き換えなど，通常のプログラムが実行しないようなウイルス特有の挙動をしていないか予測して検知する手法である．

ビヘイビアブロッキングは既に実行されているプログラムが発行するシステムコールなどの動作を監視して，レジストリの内容の変更やディスクへの書き込みなどの動作とあらかじめ定義された「ウイルスらしいふるまい」と比較して悪質なプログラムかどうかを判断する手法である．

３．ウイルス対策ソフトの問題点

パターンマッチングは誤検出の可能性が低い技術であるが，常にウイルス定義ファイルを最新の状態にしておかなければ新種のウイルスに対応できない．また，ウイルス定義ファイルを作成するために数時間を要するため，ウイルスの拡散が速い場合に更新が追いつかないという問題がある．

ヒューリスティックスキャン，ビヘイビアブロッキングは未知のウイルスを検出できるが，誤って正常なプログラムをウイルスと判断してしまう可能性がある．また，ウイルスによる不正な指令なのか正常なプログラムの指令なのかを判断するためのルールを定義することが難しいという問題点がある．

４．Windows API の監視による未知ウイルス検出

ウイルスはコンピュータ起動時に自分自身が実行されるように，レジストリの内容を変更する場合が多い．Windows でコンピュータ起動時にプログラムを実行する方法は，スタートアップのフォルダにプログラムのショートカットを作成する方法と，レジストリに直接登録する方法がある．多くのウイルスプログラムは Windows API を用いてレジストリを直接書き換える．この Windows API の呼び出しを予め定義された正常なプログラムの指令によるものか，またはウイルスの不正な指令によるものかを判断するルールに基づいて監視することにより，レジストリの不正な書き換えを防止し，未知ウイルスを検出することができる（Fig1）．

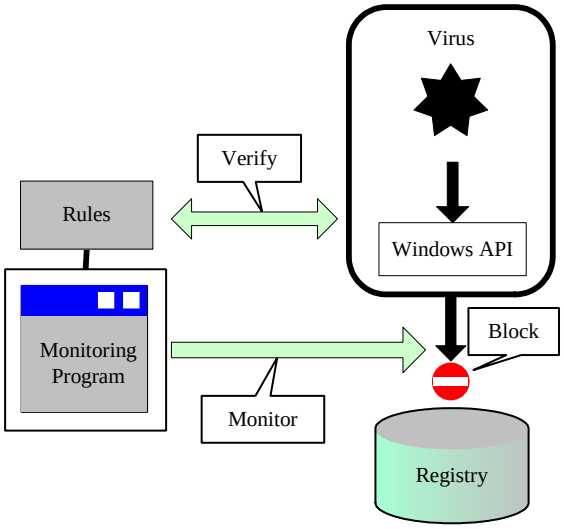


Fig.1. The method of Windows API Monitoring

５．むすび

Windows API の監視による未知ウイルス検出手法の検討を行った．今後は，さらに詳細にこの検出手法を検討し，プログラムの実装と動作検証を行う．

文　献

(1)市川，神園，白石，森井：”ウイルス解析を目的としたメモリ上の不正コード検出システムの構築”電子情報通信学会技術研究報告，Vol.104, No.422, pp.57-62, 2004

(2)松浦，加藤，小島：”未知のコンピュータ・ウイルス検出プログラムの開発”情報処理学会研究報告，Vol.2003，No.18，pp.89-94，2003

Windows APIの監視による未知ウイルス検出手法の検討

名城大学　理工学部
三根　健司　鈴木　秀和　渡邊　晃

研究背景

- インターネット普及によりコンピュータウイルスによる被害の増加
- 特にウイルスが難読化、複雑化
- 未知ウイルスの検出が課題

ウイルス検出技術

- パターンマッチング

  あらかじめウイルスの特徴を記述したファイル（ウイルス定義ファイル）をウイルス対策ソフト内に持っておき、この情報と検査対象ファイルを比較する手法
- 既存のウイルスを検出するのに有効

ウイルス検出技術

- ヒューリスティックスキャン

  動作前のプログラムの内容をチェックし、システム領域やDLLの書き換えなど、通常のプログラムが実行しないようなウイルス特有の挙動をしていないか予測して検知する手法
- 未知のウイルスに対応

ウイルス検出技術

- ビヘイビアブロッキング

  既に実行されているプログラムが発行するシステムコールなどの動作を監視して、レジストリの内容の変更やディスクへの書き込みなどの動作とあらかじめ定義された「ウイルスらしいふるまい」と比較して悪質なプログラムかどうかを判断する手法
- 未知のウイルスに対応

ウイルス対策ソフトの問題点

- パターンマッチングではウイルス定義ファイルを常に最新の状態にしておかなければ新種のウイルスに対応できない
  - ウイルス定義ファイルを作成するためには数時間が必要
- ヒューリスティックスキャン、ビヘイビアブロッキングでは誤って正常なプログラムをウイルスと判断してしまう問題

Windows APIの監視による未知ウイルス検出

- Windowsにおいてウイルスがコンピュータ起動時に自分自身が実行されるように設定する方法
  - スタートアップのフォルダにプログラムのショートカットを作成
  - レジストリに直接登録
- 多くのウイルスプログラムはWindows APIを用いてレジストリを直接書き換える

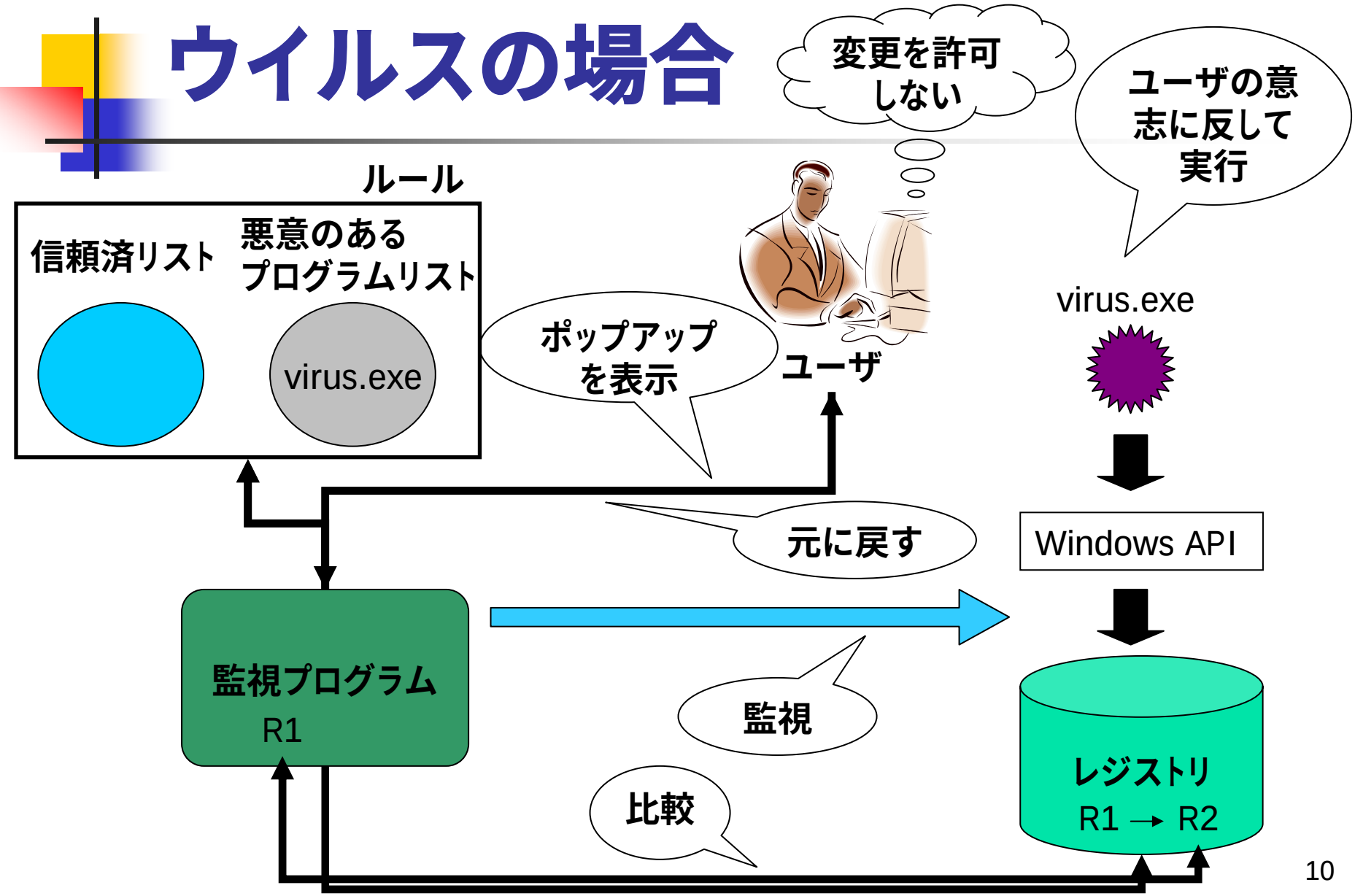
Windows APIの監視による未知ウイルス検出

- Windows APIの呼び出しを監視することでレジストリの不正な書き換えを防止
- 正常なプログラムの指令によるものかウイルスの不正な指令によるものかを判断するルールに基づいて監視
- 未知ウイルスを検出可能

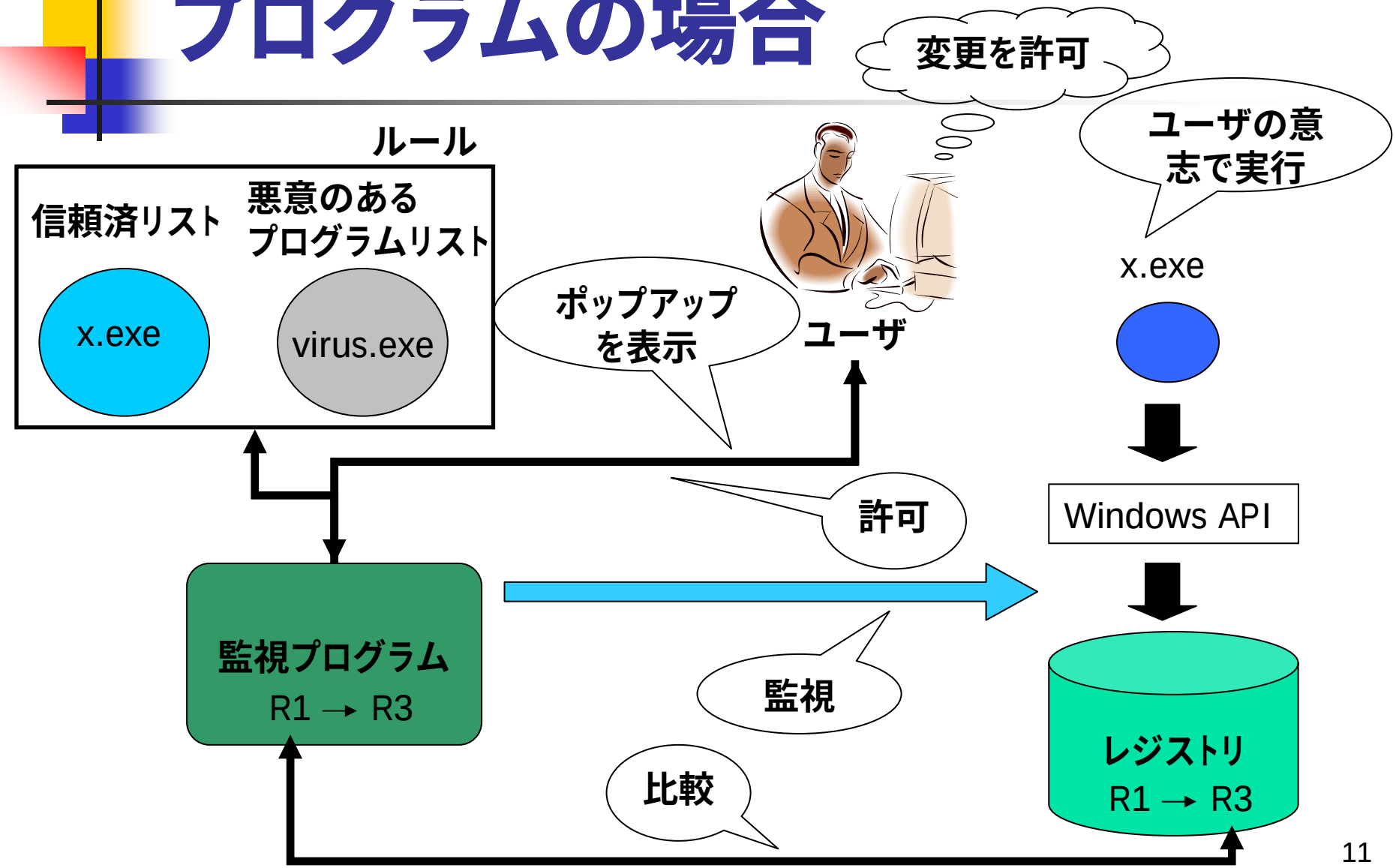
システムの構成

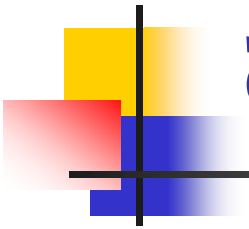
- 監視プログラム
  - Windows APIを監視し、レジストリの内容の比較と保存、ルール定義との比較、ユーザに対してポップアップを表示
- ルール定義
  - ウイルスのプログラム名とウイルスらしい振る舞いのデータベース、信頼済リストと悪意のあるプログラムリスト

ウイルスの場合


変更を許可しない
ユーザの意志に反して実行
ルール
信頼済リスト
悪意のあるプログラムリスト
virus.exe
ポップアップを表示
ユーザ
virus.exe
元に戻す
Windows API
監視プログラム
R1
監視
レジストリ
R1 → R2
比較

正常なプログラムの場合





むすび

- Windows APIの監視による未知ウイルス検出手法の検討
- 今後の課題
  - より詳細な検出手法の検討
  - システムの自動化
  - プログラムの実装と動作検証