Windows API の監視による不正インストール検出手法の検討

040427180　三根健司
渡邊研究室

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，未知ウイルスの増加が問題となっており，様々な未知ウイルス検出システムが研究されている[1].

本稿では，ウイルスが多くの場合不正なプログラムをインストールすることに着目し，Windows API を監視することにより不正なインストールを検出する手法の検討を行った．

2. ウイルス検出技術とその問題点

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．

パターンマッチングは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．

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．

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．

3. Windows API の監視による不正インストール検出

ウイルスはコンピュータ起動時に実行されるように自分自身をインストールする． 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．

そこで，このレジストリ関連の Windows API の呼び出しをフックすることにより，レジストリの不正な書き換えを防止できないか検討した．

この Windows API 監視プログラム（以下監視プログラム）は現在のレジストリの状態を保存しておき，不正なインストールが生じた場合にレジストリを復元する．また，レジストリの変更を行ったプログラムをポップアップでユーザに対して表示することにより，インストールがユーザの意図に反していないかどうか判断を促す．また，正常なプログラムと不正なプログラムのリストをデータベースとして蓄積しておくことにより，不正なインストールの再発を防止する（図 1）．

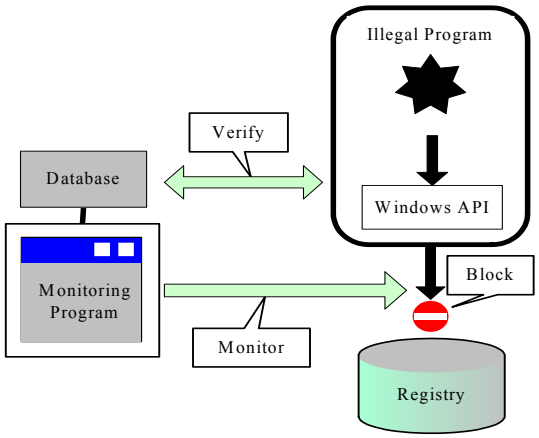


図 1 監視プログラムの動作

監視プログラムを利用することによりレジストリの変更を検出し，不正なインストールを防止することができる．監視プログラムは Windows アプリケーションであり，全プロセスのレジストリ関連の API をフックする DLL とフックを制御する実行ファイルを作成することにより実装を実現する．

4. まとめ

Windows API の監視による不正インストール検出手法の検討を行った．今後は，プログラムの実装と動作検証を行う．

参考文献

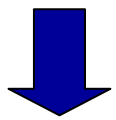
[1] 市川, 神園, 白石, 森井：”ウイルス解析を目的としたメモリ上の不正コード検出システムの構築”電子情報通信学会技術研究報告, Vol.104, No.422, pp.57-62, 2004.

Windows APIの監視による不正インストール検出手法の検討

040427180　**三根 健司**

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
- ウイルス対策ソフトでの利用が一般的



- ウイルス自体も難読化，複雑化
- 未知ウイルスの検出が課題

コンピュータウイルス

- 経済産業省の定義
- 第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり，自己伝染機能，潜伏機能，発病機能のうち一つ以上有するもの

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

ウイルスの動作

- ウイルスは多くの場合不正なプログラムをインストール
- Windows APIを用いてレジストリを変更し，コンピュータ起動時に自動実行するように設定
- 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
- 多くのウイルスはレジストリに直接登録

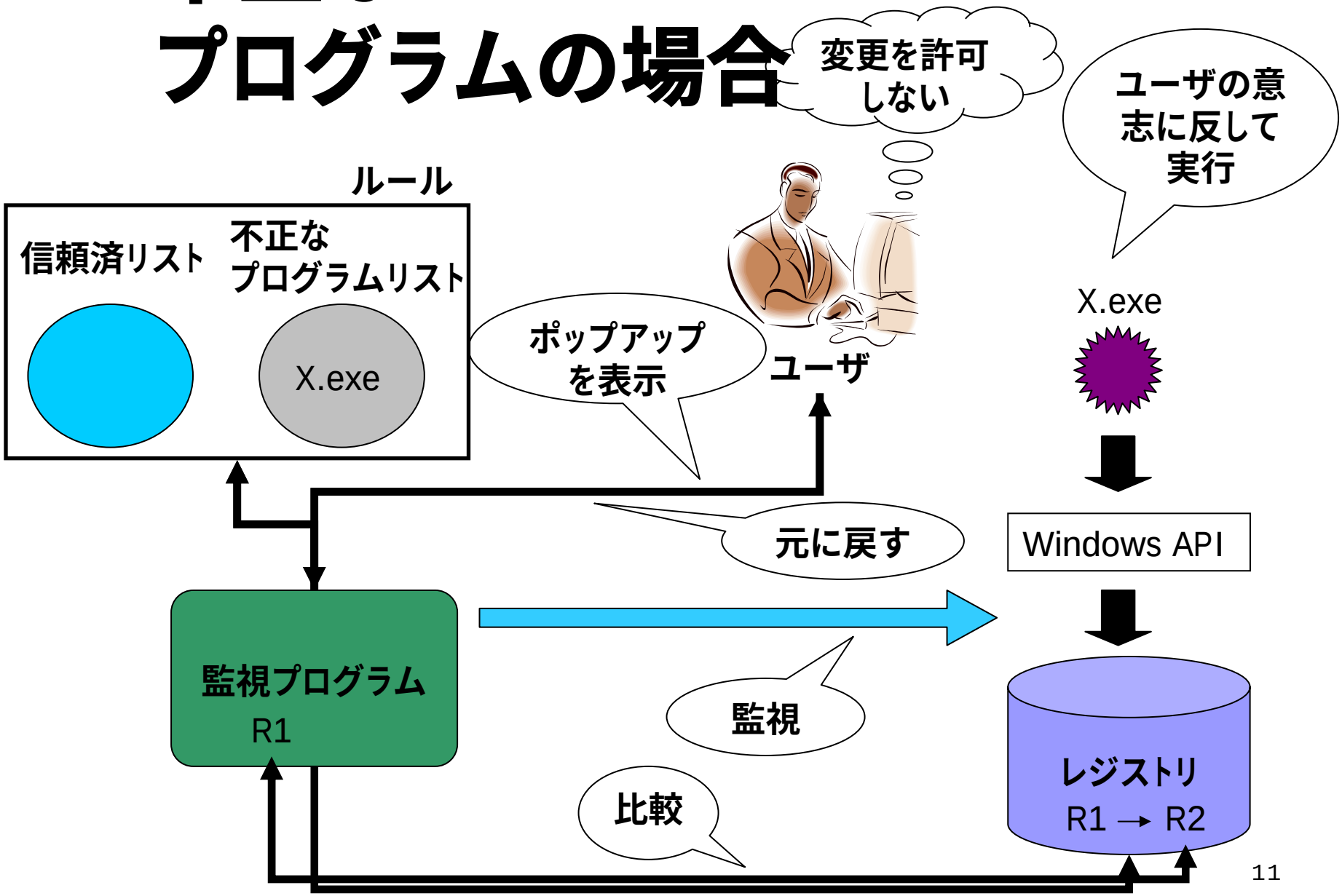
Windows APIの監視による不正インストール検出

- ウイルスが不正なプログラムをインストールすることに着目
- Windows APIを監視することによりレジストリが変更されたことを通知
- 変更されたレジストリを復元

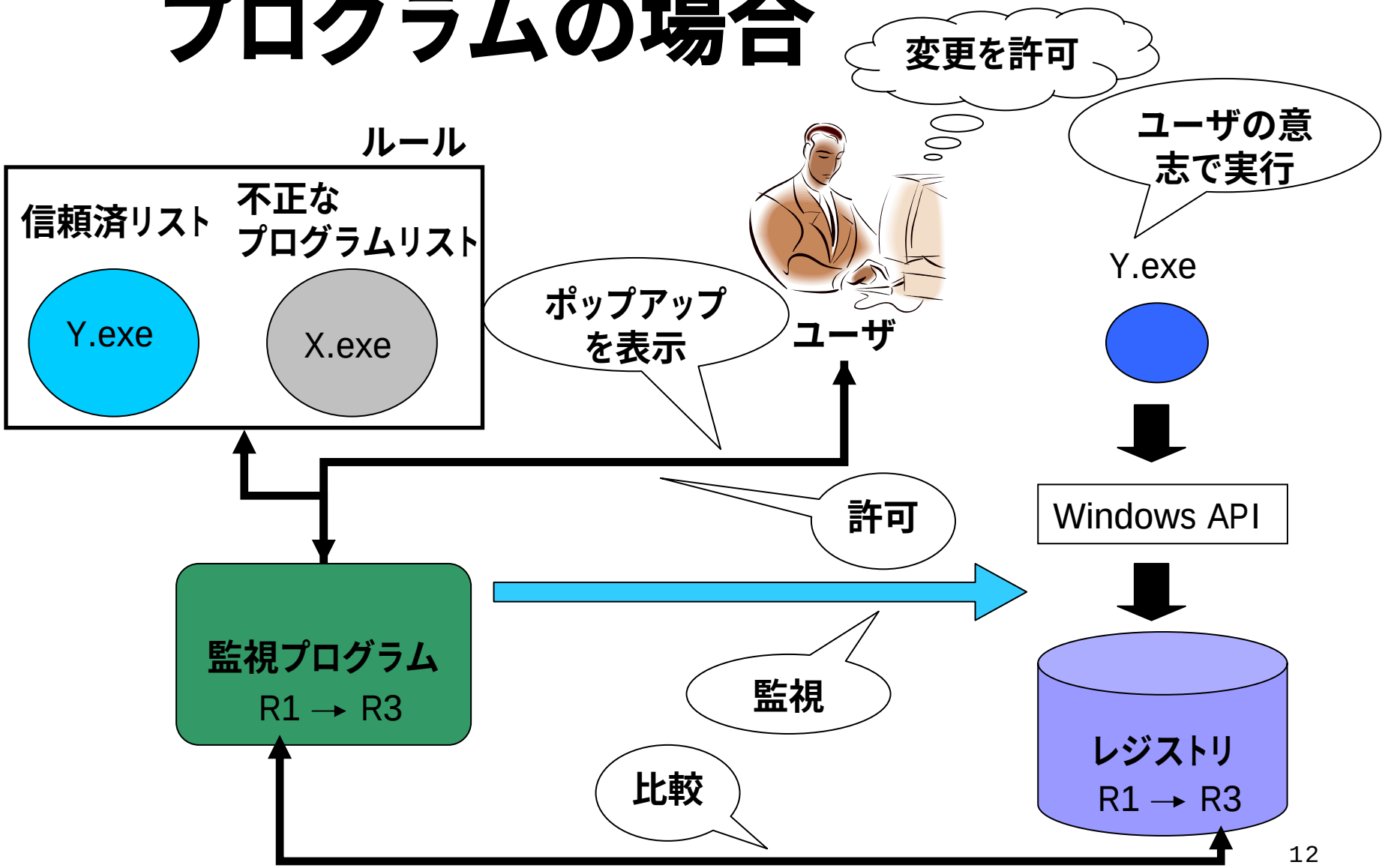
システムの構成

- 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、データベースとの比較、ユーザに対してポップアップを表示
- データベース
  - ウイルスのプログラム名、信頼済リストと不正なプログラム名のリスト

不正なプログラムの場合



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
  - プログラムの実装と動作検証