インストール時の特性を利用したワーム検出の一手法

早川　顕太*，鈴木　秀和，渡邊　晃(名城大学)

A Worm Detection Method based on the Characteristics at the Time of Installation

Kenta Hayakawa, Hidekazu Suzuki, Akira Watanabe (Meijo University)

１．研究背景

インターネットの急速な普及に伴いマルウェアの被害が年々深刻になっている。トレンドマイクロの調査(1)によると、2012年に全世界で最も検出されたマルウェアはワームである。ワームは自ら他の PC へと感染を広めるため、被害が大きくなる。

また、近年ではボットと呼ばれる攻撃者の命令に応じて悪意活動を行うマルウェアが流行している。ボット感染 PC は一般にボットネットを形成し、攻撃者の指示により一斉に動作を開始する。ボットネットは大きいほど大規模な攻撃を行うことができる。それゆえ、ボットは感染 PC を増やすためにワームと同様の機能を備えるものが多い。

本稿では、ワーム・ボットに固有なインストールの特性を利用した検出手法を提案する。

２．ワームの振る舞い

ワームは独立した実行ファイルとして存在し、自身を複製して他の PC に拡散する性質をもったタイプのマルウェアである。ワームは PC の感染前後の各々で、次の活動を行うことにより、他の PC へと感染を広めていく。

PC 感染前、PC 内へ持ち込まれたワームは侵入活動を行う。侵入活動では拡散活動や目的の活動（キーロガーやバックドアなど）を最大限に行うために、システムフォルダなどの潜伏先フォルダ内に自身をコピーし、それを OS 起動時に自動実行するように登録する(Fig.1 左図の Infect 部分)。

PC 感染後、OS 起動時に自動実行されたワームは拡散活動を行う。拡散活動では他の PC への感染を行うため、リムーバルディスク、共有フォルダ、添付ファイル付きメールなどに自身のコピーを作成する(Fig.1 右図の Spread 部分)。これらを媒体として、他の PC に自身を持ち込ませ再び侵入活動を行う。

ワームは侵入活動に使用したコードが、侵入後も拡散活動において必要となるため、基本的に自身をコピーする必要がある。このとき、単純なコピーではなくプログラムの振る舞いを保ったままコードを変化させるポリモーフィック技術を用いるものもある。

３．提案方式

提案方式は、ワームの侵入活動(Fig.1 左図の Infect 部分)を検出する方法である。レジストリの自動実行に登録する API をリアルタイムで監視（フック）し、自動実行に登録される実行ファイルとそれを実行しているプロセスの実行ファイルを比較する。その結果、類似性が高ければそのプロセスをワームとして検出し、アラートを出す。

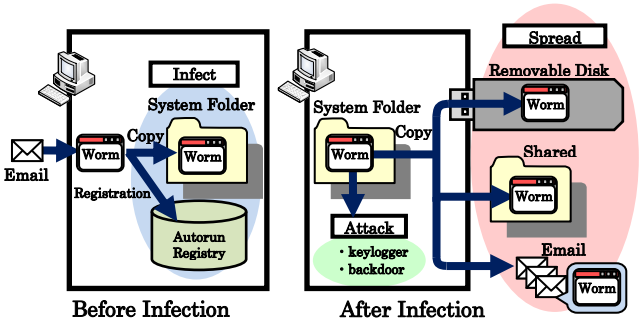


Fig.1. The behavior of the worm

ワームは侵入活動において、システムフォルダなどに実行ファイルを作成し、自動実行するように登録する。この挙動は一部の正規インストーラにおいても見られる。しかしながら、ワームは自身のコピー、インストーラは別のプログラムを作成し自動実行へ登録することから、「自動実行へ登録する側とされる側の類似性」という概念を用いることにより、ワームとインストーラを区別する。

ワームは自身のコピーを自動実行するように登録するため、類似性が高い。ポリモーフィック技術を用いてコードを変化させても、その全てを変化させることはできないため類似性が検出できる。

実行によりインターネット上からアプリをダウンロードするタイプのインストーラについては、インストーラとアプリはまったく別のプログラムであるため類似性が低い。インストーラ自身に内包されたアプリケーションをインストールするタイプのインストーラについても、一般にアプリは圧縮して格納されているため類似性が低い。

類似性には、ヘッダ部分の一致率やインストールする側のコードがインストールされる側に含まれているかどうかなどを尺度とすることが可能である。

4. むすび

本稿では、ワームの振る舞いを考察し、自身のコピーを自動実行に登録するような振る舞いをワーム固有な振る舞いとして検出する方法を検討した。今後はこの方法の有効性を確認するための実装を行う。

文　献

(1)TREND MICRO インターネット脅威年間レポート 2012 年度
http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20121218094256.html

インストール時の特性を利用したワーム検出の一手法

名城大学　理工学部
早川顕太，鈴木秀和，渡邊晃

Watanabe Lab.

研究背景

- インターネットの普及に伴い，コンピュータウイルスによる被害が深刻になっている
- 近年，流行しているコンピュータウイルス
  - ワーム
    - 自ら他のPCへ感染する機能を持つ
  - ボット
    - 攻撃者の命令に応じて活動
    - 大規模な攻撃を行うために，ワームと同様に他PCへ感染する機能を持つことが多い
- この研究ではワームの検出手法を提案する

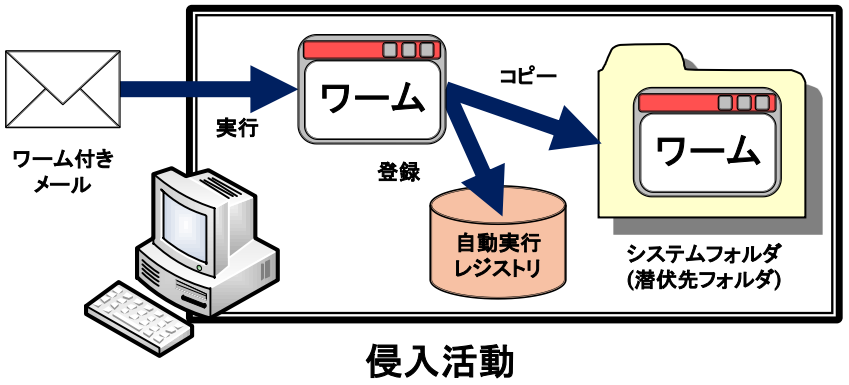
ワームの振る舞い

- 独立したプログラムとして存在し，次の一連の活動を行う

侵入活動

システムに駐在するため，

- システムフォルダ内に自身のコピーを作成
- それを，OS起動時に自動実行するように登録

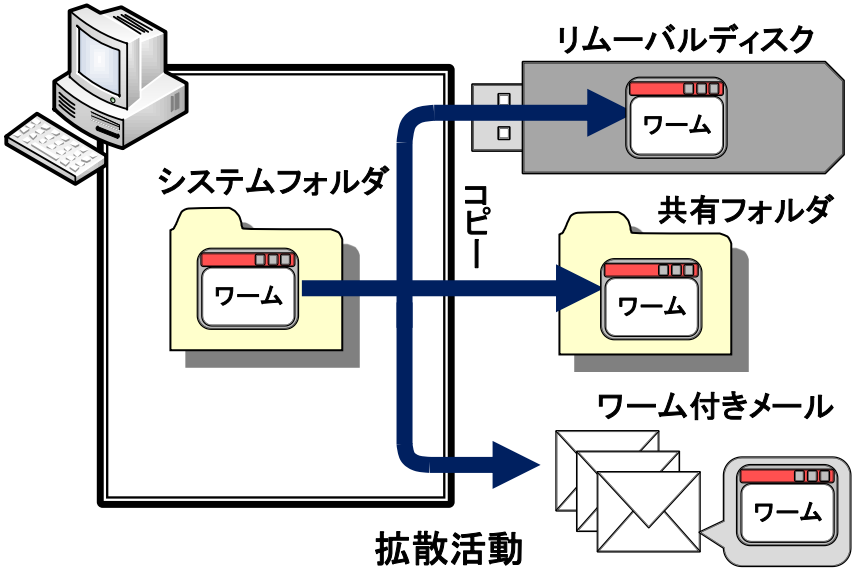


侵入活動

拡散活動

侵入後，他のPCに感染するため，

- USBや共有フォルダ，メールに自身のコピーを作成



拡散活動

既存技術

- パターンマッチング方式
  - ウイルスの特徴的なバイナリパターンを定義し，静的に検出
- 静的ヒューリスティック法
  - ウイルスの特徴的な振る舞いを定義し，静的に検出
- ビヘイビア法
  - ウイルスの特徴的な振る舞いを定義し，動的に検出

各方式の比較

	未知ウイルス	暗号型ウイルス
パターンマッチング方式	×	×
静的ヒューリスティック法	○	×
ビヘイビア法	○	○

ビヘイビア法を用いた既存のワーム検出技術

自己ファイルREADの検出による未知ワームの検知方式

検出する振る舞い: 「自身の実行ファイルをREAD」

- 理由：ワームは侵入時や拡散時に自身のコピーを作成するため
- 課題：自プロセスのメモリ上に存在するコードをREADするワーム

侵入挙動の反復性を用いたボット検知方式

検出する振る舞い: 「侵入活動の反復」

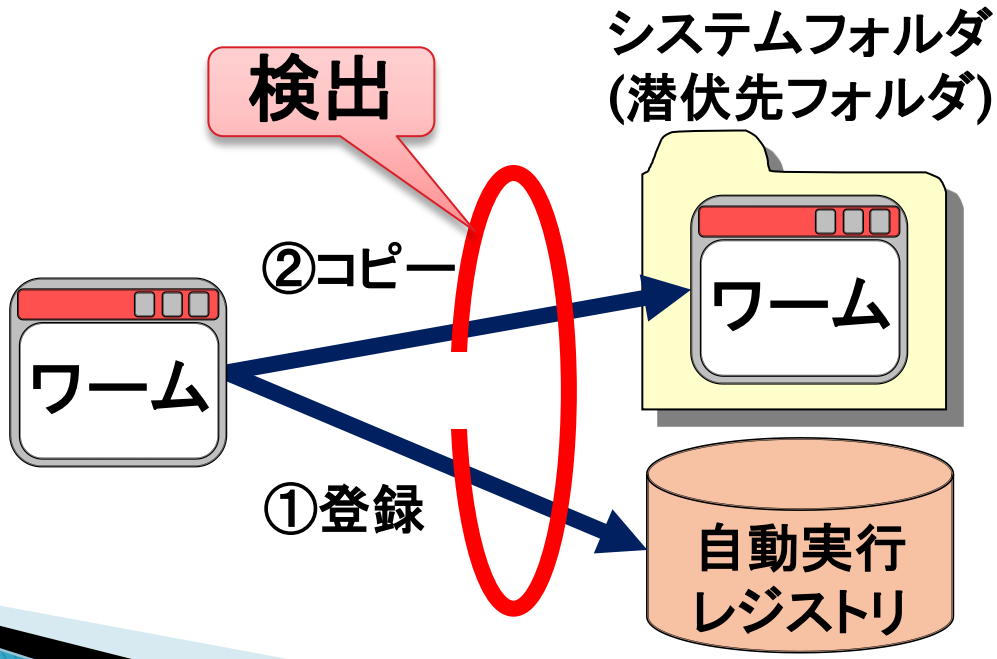
- 発現方法：侵入後のプログラムを侵入前の実行環境に戻し，再実行
- 課題：ボットの実行ファイル内に，侵入済みであるかどうかのフラグを用意し，それにより侵入活動を行うかを判断するボット

- 松本隆明ほか，自己ファイルREADの検出による未知ームの検知方式，情報処理学会論文誌，Vol.48，No.9，pp3174-3182，(2007).
- 酒井崇裕ほか，侵入挙動の反復性を用いたボット検知方式，情報処理学会論文誌，Vol.51，No.9，pp1591-1599，(2010).

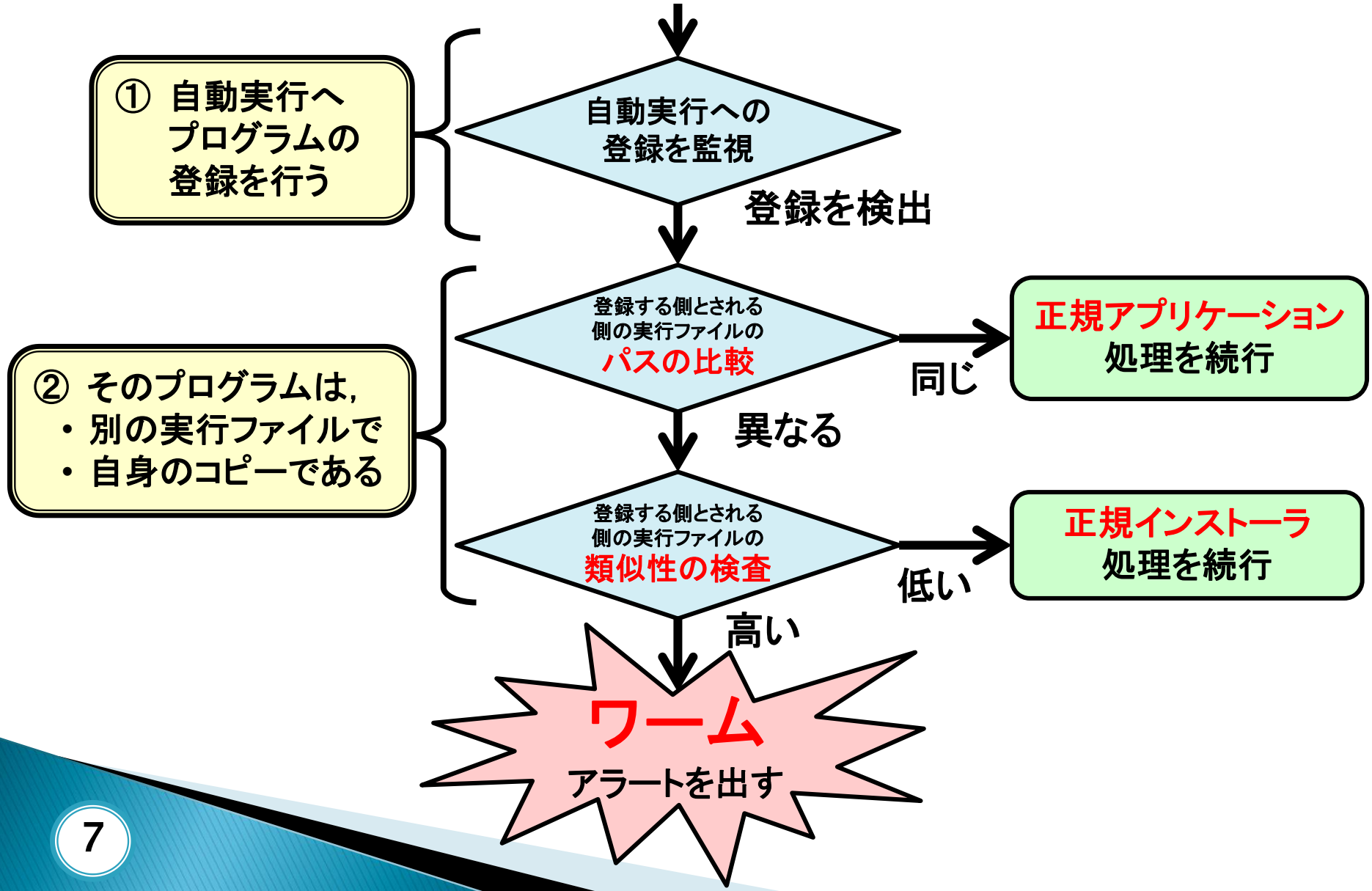
提案方式

- ビヘイビア法を適用
  - ワームの侵入活動を次のように定義し，検出する

① ワームは自動実行へプログラムの登録を行う
② そのプログラムは別の実行ファイルで自身のコピーである



提案方式のフローチャート



検証実験

検証実験を行い，提案方式の有用性の評価を行う．

- 実験環境
  - 仮想マシンVMware上の「Windows XP SP3」

- 検知実験に使用したワームの検体
  - マルウェア配布サイト「Offensive　Computing」から独自に入手したマルウェア
  - その内，WindowsXP上で実行可能で，Symantec社の検出種別がワームであった19体を使用

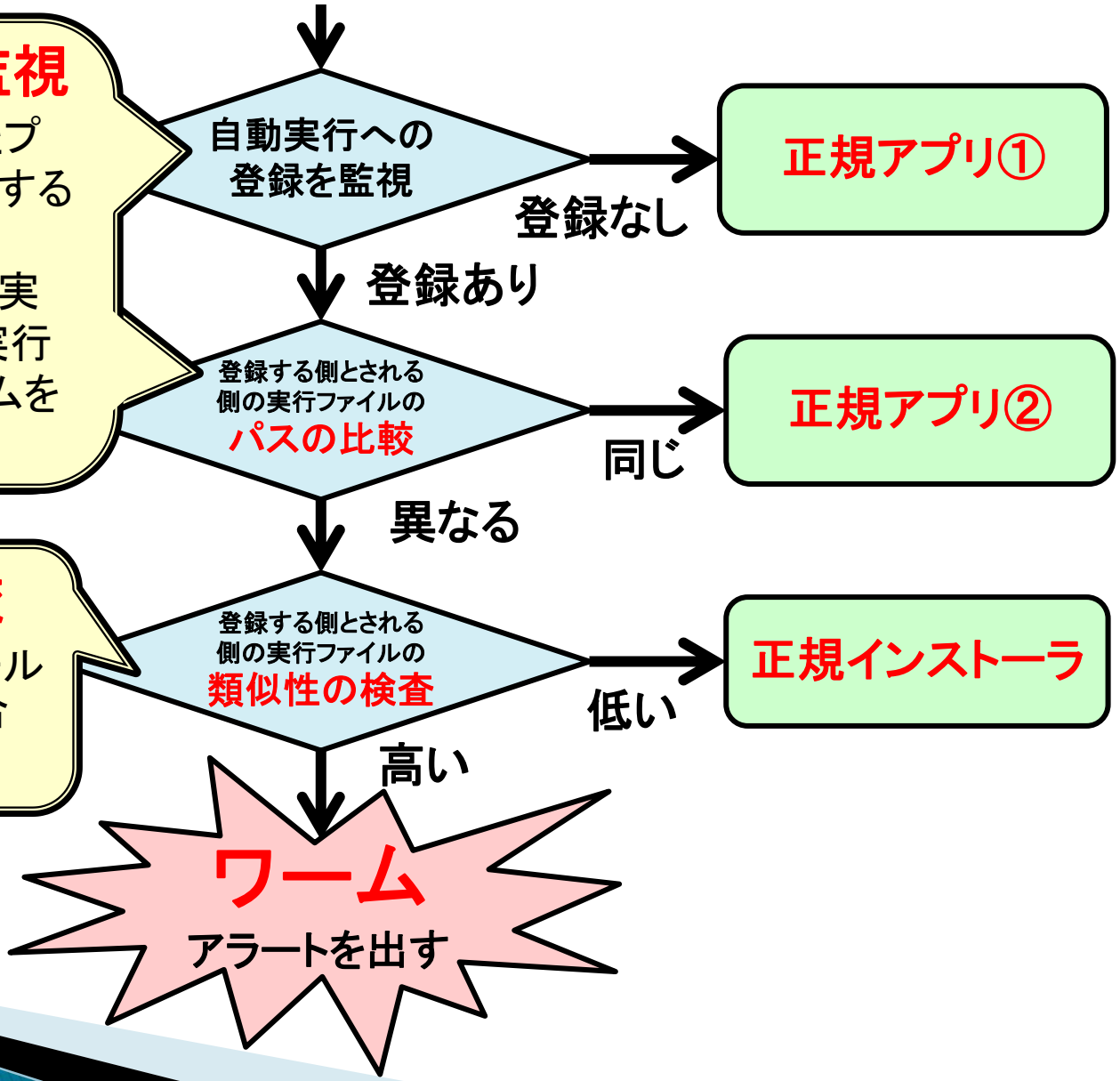
実験方法

Autorunsによる監視

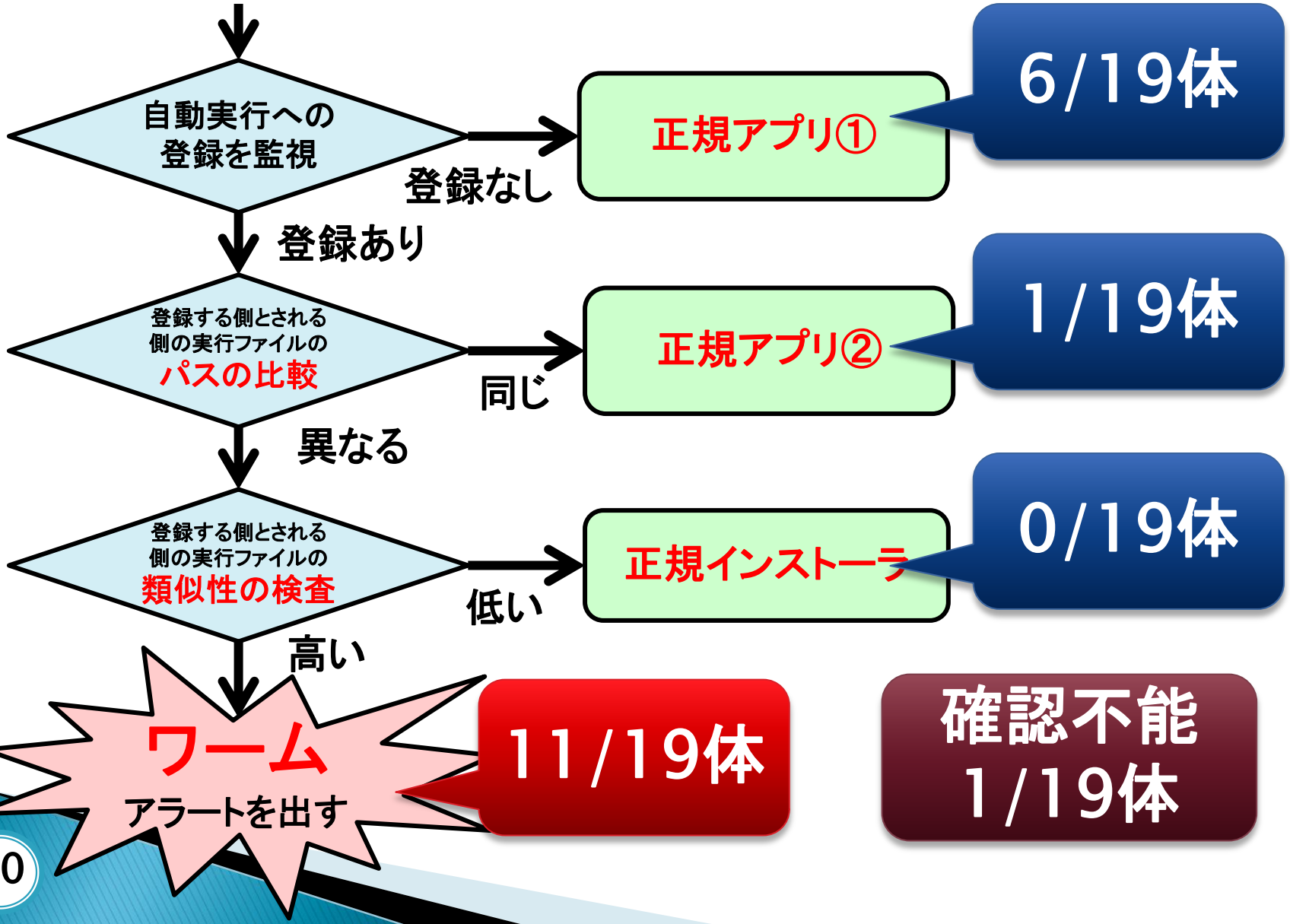
- 自動実行に登録されたプログラムの一覧を表示するツール
- 検査対象プログラムの実行前後で新たに自動実行に追加されたプログラムを探す.

ヘッダ情報の比較

実行に関する重要なフィールドの一致率が100%の場合ワームと判定.



ワーム19体に対する検出結果



提案方式の評価

- 評価
  自動起動への登録が観測されないワームについて
  未検知が存在する（6/19体）

- 自動実行へ登録を行わないワームの考察
  - 再起動がめったに行われないサーバなどへの感染を目的としたワーム
  - 既存の自動実行するプログラムを改造し，そのプログラムから自身のコピーを実行させるタイプのワーム
  - 仮想環境内で実行したため，それを検知され活動を行わなかった

提案方式の課題

- ワームの侵入活動の振る舞い定義の見直し
  - 提案方式は自動実行への登録をトリガーとして動く
    ⇒自動実行へ登録を行わないワームを検出できない
  - システムフォルダへの実行ファイル作成をトリガーとして動くように改良
    ⇒自動実行へ登録を行わないワームも検出できる可能性がある

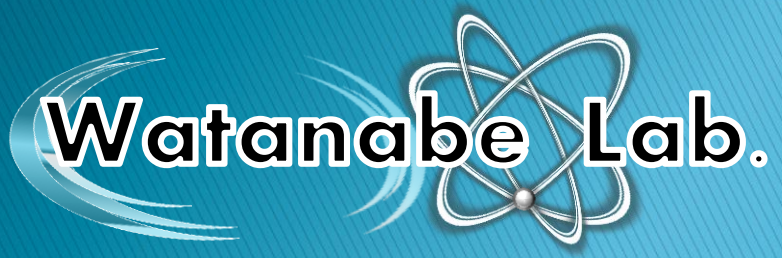
まとめ

- ワームの振る舞いを考察し，ワーム特有のインストール特性を利用したワーム検出手法を提案した
- 検知実験や，誤検知実験を行い提案方式の有用性や問題点を示した
- 今後は，検出率を上げるため提案方式の改善や，実装を行う予定である

参考文献

- TREND MICRO ～2012年度インターネット脅威年間レポート～
  - http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20121218094256.html
- マルウェア配布サイト「Offensive Computing」
  - http://www.offensivecomputing.net/
- 松本隆明ほか，自己ファイルREADの検出による未知ームの検知方式，情報処理学会論文誌，Vol.48，No.9，pp3174-3182，(2007).
- 酒井崇裕ほか，侵入挙動の反復性を用いたボット検知方式，情報処理学会論文誌，Vol.51，No.9，pp1591-1599，(2010).

補足資料



誤検知実験

- 自動実行へ登録が行われる3体の正規インストーラについて，誤検知がないか実験を行った.

- 誤検知実験の結果
  いずれもヘッダ情報の一致率は0%で誤検知はない.

インストーラ	誤検出	判定結果
Skype	○	「正規インストーラ」と判定
Dropbox	○	「正規インストーラ」と判定
Rainlendar （スケジュール管理ツール）	○	「正規インストーラ」と判定