自己複製挙動に着目した未知ワーム検出手法の提案

110430052　神谷 早紀
渡邊研究室

1. はじめに

遠隔操作，DDos 攻撃，情報窃取などを行うボットが流行し問題になっている．ボットは，ボットネットを構成し攻撃するため，ワームの自己増殖する機能を持っており感染が拡大している．

一般的にマルウェア（ワーム）検出は，マルウェアのシグネチャを記録した定義ファイルを用いるパターンマッチングで行われている．しかし，この方法はパッカーなどのコード難読化を用いるマルウェアやポリモーフィックなどの複製の度に自己改変するステルス技術に対応できていない．また，ボット作成キットが出回るなどにより亜種マルウェアが増大しており，シグネチャの生成が間に合わないという課題がある．そこで，マルウェアらしい「挙動」を検出するビヘイビア法が注目されている．

本稿ではワームが必ず行う，自己複製という挙動に着目したワーム検出手法を提案する．

2. 既存研究

ビヘイビア法によるワーム検出に関する既存研究として以下のような研究がある [1][2]．文献 [1] は，ワームが複製を作成する時に観測される「自身のファイルを全て READ する」挙動を検出する．しかし，正規プログラムでもこの挙動が起こるため，誤検知が発生する．文献 [2] は，ワームが「侵入挙動を繰り返す」という挙動を検出する．ここで言う侵入挙動とは，ファイルを作成する事と，自動実行されるようレジストリに登録する事である．この手法は反復性を検出するために，PC 環境を復元する，再実行するなどの処理を行う必要があり，処理が重い．

3. 提案方式

ワームは，PC 内で実行されると，自分自身の複製を作成し，その複製を自動実行のレジストリに登録するなどの侵入活動を行う．これにより，ワームは PC の再起動後も PC 内に駐在できるようになる．その後，他の PC への拡散活動を行ったり，その他攻撃活動を開始する．

このように，ワームは PC 内に侵入した際まず自己複製を行う．この挙動に着目し，自己複製を検出する事により攻撃活動を開始する前にワームを検出する事ができる．ワームの中には，複製の度に暗号化の鍵を変えて自己改変するポリモーフィック型も存在する．しかし，実行可能ファイルのヘッダ部分は改変が難しい．Windows の実行ファイルは PE 形式に従っている．PE ヘッダの中でもファイルごとに固有かつ改変が難しい項目を比較することで複製かどうかを判定する．これに該当する項目として，ImportTable フィールドと，AddressOfEntryPoint フィールドが挙げられる．ヘッダにより複製を判定するためポリモーフィック型も検出できるという利点がある．

図 1 に提案方式の概要を示す．ファイルへの書き込みを監視し，書き込みが行われた場合，書き込みを行ったプロセスの実行ファイル A と，書き込まれたファイル B のヘッダを比較し自己複製挙動を検出する．

提案方式の誤検知の可能性を調査するため，正規プログラムにおいても自己複製挙動が検出されるかどうかを検証した．その結果，インストーラとアンインストーラの一部で，自己複製挙動が検出された．そこで，自己複製を検出した際にインストールもしくはアンインストール中かどうかをユーザーに問い合わせるダイアログを出す事でワームかどうか判定する事とした．

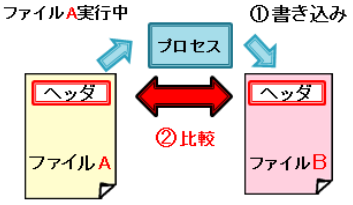


図 1: 提案方式の概要

4. 検知実験と課題

提案方式の有用性を検証するため，プロセスの処理を監視できる ProcessMonitor と，2 つのファイルを比較する CompFile を用いて実験を行った．実験環境は，仮想マシン VMware 上の Windows7 SP3 で，ネットワーク環境はホストオンリーとした．使用した検体は，マルウェア配布サイトから独自に入手したマルウェアの内，Symantec 社の検出種別がワームである 25 体である．

Symantec 社のマルウェアに関するレポート [3] によると，21/25 体が自分自身（実行ファイル）をコピーするとある．実際に仮想環境で実験を行った結果，11/25 体の検体を検出できた．検出率減少の原因は，ワームが他プロセスに複製を委託するなど，巧妙な手法で複製を作成したことが考えられる．また，インターネットに接続されていない環境である事や，耐解析機能を持ち仮想環境で実行されていることを検知して挙動を変えた可能性，あるいは実行環境がワームの想定する OS のバージョンと異なるなどの環境要因により動作しなかった事などが考えられる．

ユーザーモードの API フックを用いて提案方式を実装し，一部のワームを検出できることを確認した．しかし，子プロセスに複製を委託したり，CodeInjection を行うなど，複製元を隠すワームを検出できないことも明らかになった．今後これらのワームに対処できるよう提案方式を改善したい．

5. まとめ

本稿は，ワームが自己複製をした時に実行可能ファイルのヘッダ部分は変更できない点に注目し，ワームを検出する方法を提案した．監視ツールを用いた基礎実験から提案方式の有用性を確認し，実装方法について検討した．

参考文献

[1] 松本. 他：自己ファイル READ の検出による未知ワームの検知方式, 情報処理学会論文誌, Vol.48,No.9, pp.31743182,Sep2007.

[2] 酒井. 他：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,pp.1591-1599,Sep2010.

[3] http://www.symantec.com/ja/jp/security_response/landing/azlisting.jsp

自己複製挙動に着目した未知ワーム検知手法の提案

渡邊研究室
110430052　神谷早紀

Watanabe Lab.

研究背景

- **マルウェアの爆発的な増加**
  - マルウェア作成キットなどにより簡単にマルウェアを作成できる
  - 1分に307個マルウェアが出現

- 流行しているマルウェア
  - **ボット**
    - 遠隔操作により，攻撃者の命令に従って活動
    - ボットに感染したコンピュータ群によりボットネットを構成するため，ワームと同等の拡散機能を持つ
  - **ワーム**
    - **独立して動作し，PCへ侵入して自身を拡散する機能を持つマルウェア**

ワームを検出する手法を提案

従来のマルウェア検出手法

- パターンマッチング法
  - 個々のマルウェアそれぞれに特徴的なシグネチャを定義し，検査対象と比較し一致するものを検出
    →未知マルウェア検出不可

- ビヘイビア法
  - 実行されているプログラムの動作を監視し，事前に定義したマルウェアらしい特有の挙動を検出
    →未知マルウェア検出可能

未知のワーム検出可能なビヘイビア法に着目

既存研究

- 検出挙動：自己ファイルREAD
  - **検出方法**：自分のファイルを読み込む挙動を検出
    - ワームの性質上，自分自身を複製する
    - 複製時，自分のファイルを読み込む
  - **課題**：誤検知が起こる
    - 正規プログラムで自己ファイルREADが起こる

- 検出挙動：侵入挙動の反復性
  - **検出方法**：侵入挙動検知後，実行環境を復元し再実行
    - 侵入挙動：複製作成，自動実行リストへ登録
    - 未感染環境では常に侵入活動を行う　→反復
  - **課題**：処理が重い
    - 実行環境を復元，再度実行する必要がある

- 松本. 他：自己ファイルREAD の検出による未知ワームの方式，情報処理学会論文誌, Vol.48,No.9, pp.3174-3182,Sep2007.
- 酒井. 他：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,pp.1591-1599,Sep2010.

ワームの挙動

- ①侵入活動
  - PC内に常駐するためにまず侵入活動を行う
    →自身を複製し，複製を自動実行リストへ登録
- ②拡散活動
  - 自己増殖し拡散，他のPCへの侵入を試みる
    →リムーバルディスクや共有フォルダなどに自身の複製を作成

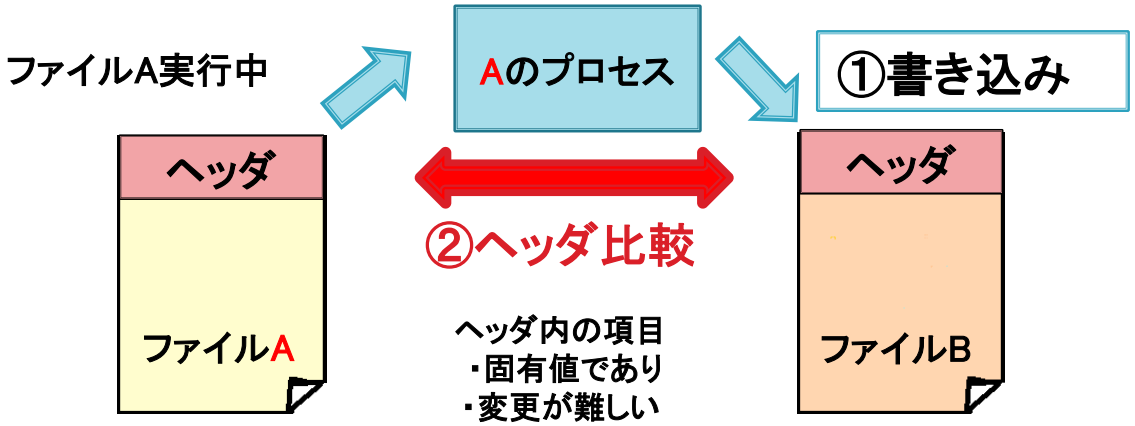
自分の複製を生成する　＝　自己複製挙動　を検出

→ワームを検出

提案方式

- **検出挙動：自己複製挙動**
- **検出方法：**
  - **①　ファイルへの書き込みを検査**
  - **②　ヘッダ比較　→　複製判定**

書き込まれたファイルと，
書き込みを行ったプロセスの実行ファイルのヘッダを比較する



- 変異型ワーム

  複製のたびに自己改変する
  →ヘッダは改変が難しく，変化しない
  →ヘッダを比較することで自己複製を検出

提案方式のフローチャート

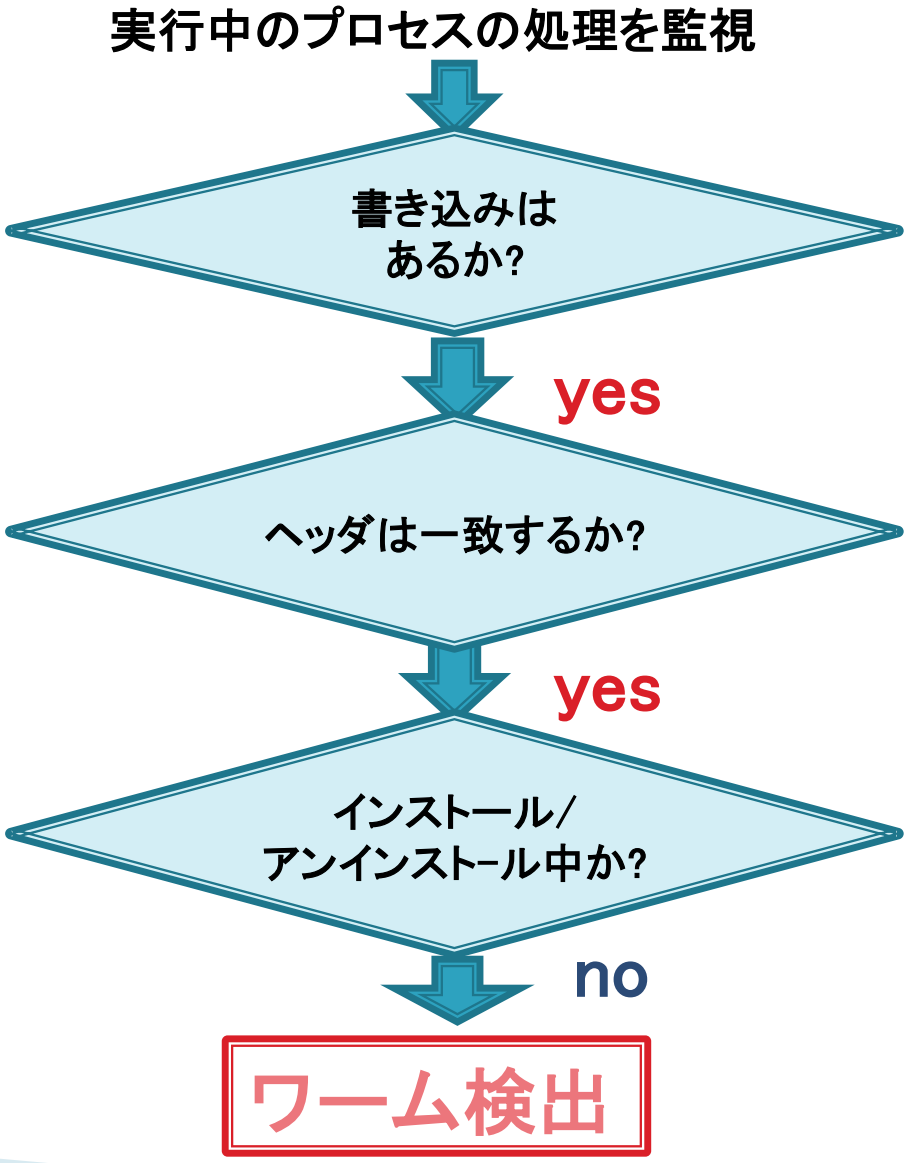
- **誤検知回避**
  インストーラ/
  アンインストーラは
  自己複製挙動を行う事がある

  ↓

  ユーザに問い合わせる

  ↓

  正規プログラムと
  マルウェアを区別



実装方法

- **APIフック**

  アプリケーションのAPI呼び出しを横取り(フック)し独自処理を行う技術

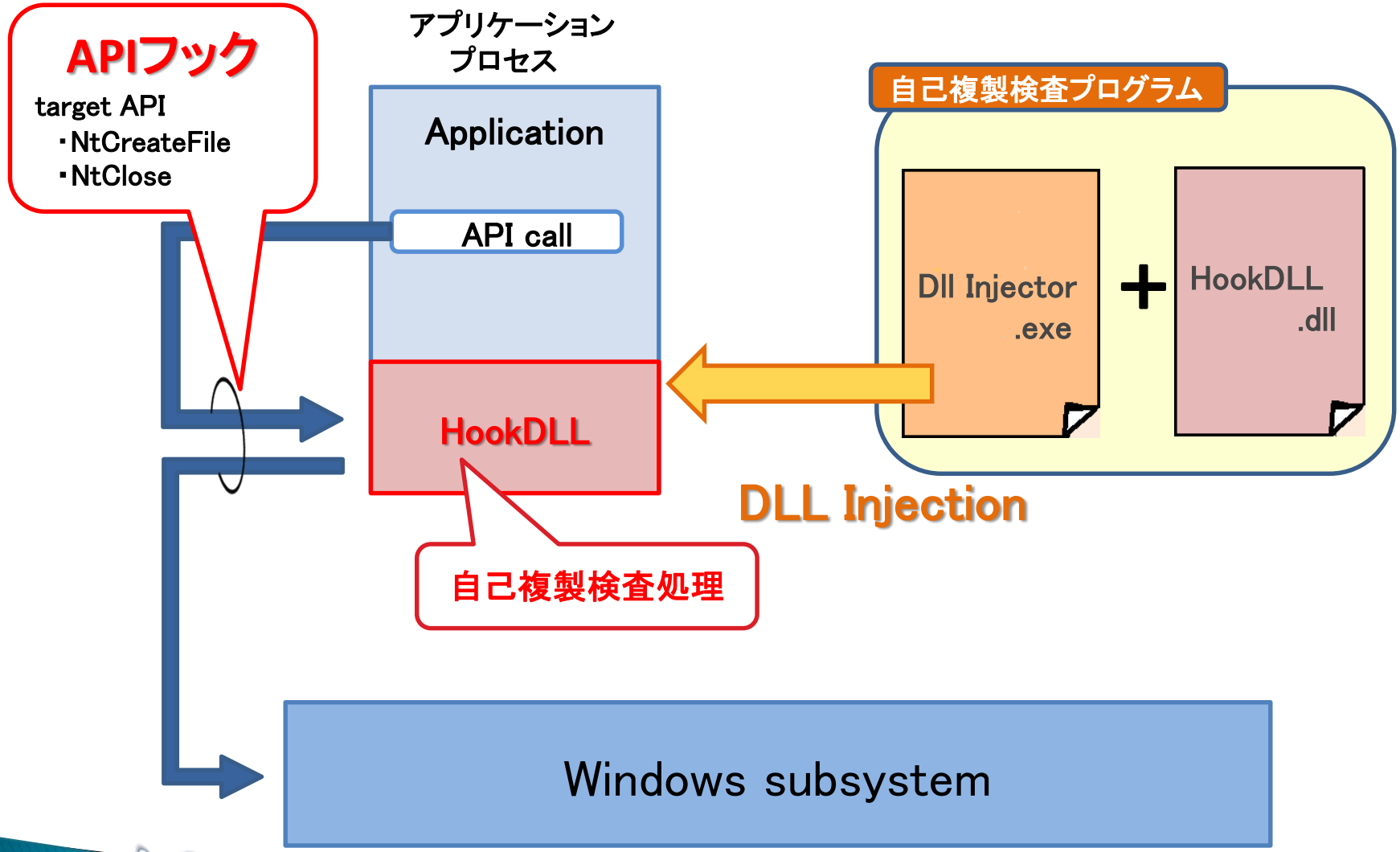
  - Detours Library
    - Microsoft Research が提供するAPIフック用のライブラリ
    - フック対象APIの先頭命令をJMP命令に変更→制御を横取り

- **DLL Injection**
  - DLLをプロセスに強制的にロードさせる技術
  - **自己複製検査処理　←DLLに実装**

    ①NtCreateFile API , NtClose APIをフックし書き込み操作を検査

    ②ヘッダを比較して複製の判定

検査プログラムの動作概要



検知実験

- 実験内容
  1. **Symantec社のレポートによる調査**
  2. **ツールによる検知実験**
     - ProcessMonitor
       プロセスの行った処理をリアルタイムに表示できるツール
     - CompFile
       2つのファイルを比較できるツール
  3. **検査プログラムによる検知実験**

- 実行環境
  - 仮想環境VMware上 「Windows7 SP3」（管理者権限で実行）

- 使用したワーム検体
  - 下記サイト独自に入手したマルウェアの内，
    Symantec社の種別がワームであるもの25体
    - Offensie Computinghttp://www.offensivecomputing.net/）
    - VX Vault（http://vxvault.siri-urz.net/）

実験結果

マルウェア名	発見日	Symantec社レポート	ツールによる検知実験	検査プログラムによる検知実験
W32.Cridex	2012/1/20	○	○	○
W32.Yimfoca	2010/5/2	○	○	○
W32.Koobface	2008/8/3	○	○	○
W32.Koobface.B	2008/8/3	○	○	○
W32.Badday.A	2007/10/3	○	○	○
W32.SillyDC	2006/10/4	○	○	○
W32.Mytob.BE@mm	2005/4/21	○	○	○
W32.Mydoom.F@mm	2004/2/20	○	○	○
W32.Klez.gen@mm	2004/2/18	○	○	○
W32.Mimail.Q@mm	2004/1/7	○	○	○
W32.IRCBot.NG	2011/4/7	○	△	×複製有
W32.Pilleuz!gen2	2010/2/25	○	△	×複製有
W32.Pilleuz	2009/9/29	○	△	×複製有
W32.Fubalca.E	2007/4/1	○	△	×複製有
W32.Changeup!gen20	2012/11/27	○	×	×
W32.Changeup!gen23	2012/8/22	○	×	×
W32.Disttrack	2012/8/16	○	×	×
W32.Buzus	2009/12/10	○	×	×
W32.Ircbrute	2008/6/20	○	×	×
W32.SillyFDC	2007/2/27	○	×	×
W32.Evaman.C@mm	2004/8/3	○	?	○
W32.Feebs.J@mm	2006/1/16	×	○	×
W32.Zimuse	2010/1/23	×	×	×
W32.Waledac	2008/12/23	×	×	×
W32.Downadup	2008/11/21	×	×	×

- **レポート**
  21/25体，自己複製
  - 4/25体：実行ファイル形式でないマルウェアなど
- **検知実験**
- **検査プログラムにより11体，検出（○）**
  提案方式の有用性を確認
- **6体，複製無し（×）**
  - 耐解析機能（仮想環境を検知）
  - OSのバージョン

  →環境要因による挙動の変化
- **4体，他プロセスに複製を委託（△）**
  - 他のプロセスに処理を委託
    - 子プロセスを生成
    - CordInjection
  - →処理を追いかけて複製元を正しく把握する必要

まとめ

- ビヘイビア法によるワーム検出手法を提案
- 自己複製挙動を検出するプログラムを実装し，
  実際に自己複製を行うワームを検出することに成功

- 今後の予定
  - 他プロセスを介して複製を作成するワームへの対策として，
    処理を追いかける方法を検討し，提案方式を改善する

ご清聴ありがとうございました

補足資料

比較項目について

Windowsの実行ファイルは
PE（Portable Executable）フォーマットに従っている

- Address Of EntryPoint
  - プログラムの開始位置を示す値
- Import table
  - インポートテーブルへのアドレス
  - プログラムが使用するDLLの情報を格納

項目名	一致率(%)
Import Table	0.02
Address Of Entry Point	0.09
Time Date Stamp	0.14
Size Of Code	0.63
Import Address Table	0.92
Resource Table	1.09
Size Of Initialized Data	1.14
Size Of Image	1.67
Base Of Data	3.32
Check Sum	19.6

中谷直司，小池竜一，厚井裕司，吉田等明. メール型未知ウイルス感染防御ネットワークシステムの提案.情報処理学会論文誌, Vol.45, No.8,pp.1908-1920, Aug.2004.

正規プログラムの挙動
-自己複製挙動調査-

ツールを用いて自己複製挙動があるかどうかを調査した

- インストーラで3/9体
- アンインストーラで4/9体

自己複製挙動が観測された

検体	Installer	Uninstaller
WireShark	あり	あり
DropBox	なし	あり
AdobeReader	なし	あり
GoogleChrome	あり	なし
iTunes	なし	なし
Lhaplus	あり	なし
LINE	なし	あり
Skype	なし	なし
サクラエディタ	なし	なし

APIフックによる自己複製挙動の検出

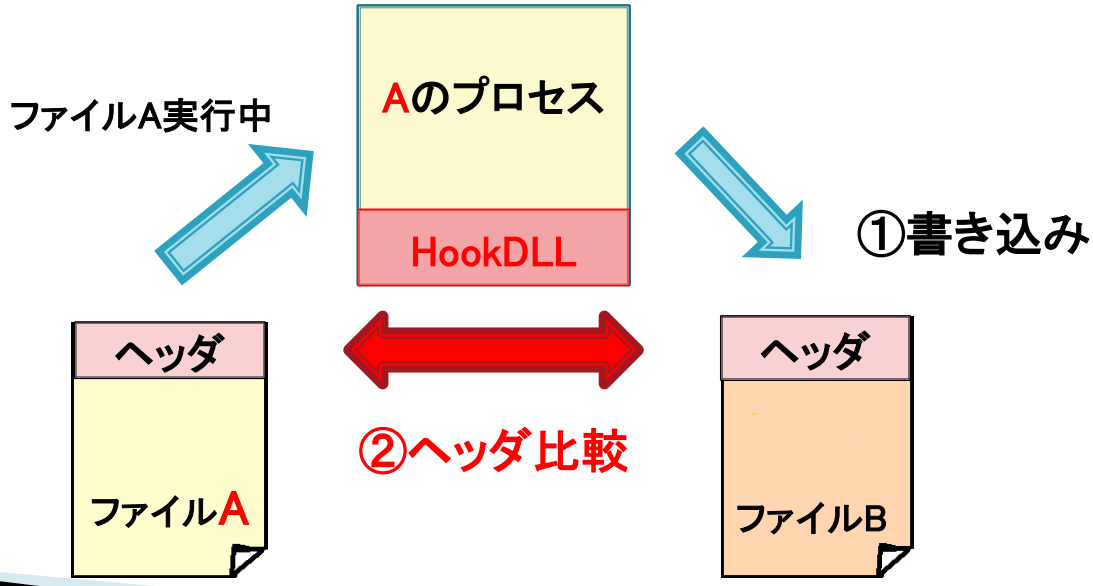
- **書き込みを監視する**
  NtCreateFileと，NtCloseにAPIフックを仕掛け，プロセスの処理を監視

書き込み動作

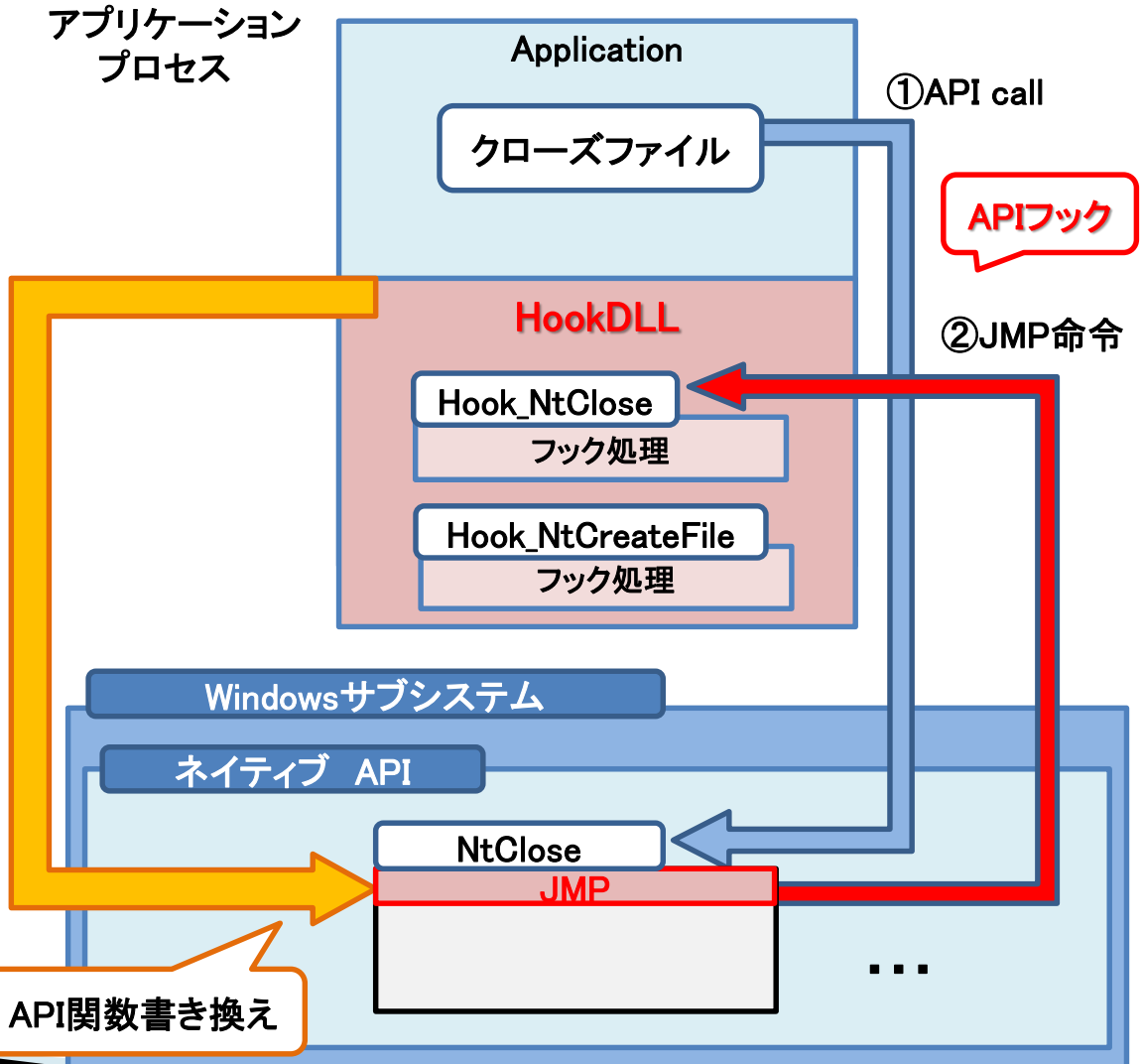
1.ファイルを開く　→NtCreateFile　API　呼び出し
→書き込み権限をチェック

2.書き込む

3.ファイルを閉じる（書き込み終了）　→NtClose　API　呼び出し
→ヘッダを比較



Detoursフックの仕組み



検知実験結果
-OSバージョンの違いによる挙動の変化-

マルウェア名	発見日	Windows XP	Windows 7
W32.Mimail.Q@mm	2004/1/7	○	○
W32.Cridex	2012/1/20	○	○
W32.Koobface	2008/8/3	○	○
W32.Koobface.B	2008/8/3	○	○
W32.SillyDC	2006/10/4	○	○
W32.Mydoom.F@mm	2004/2/20	○	○
W32.Klez.gen@mm	2004/2/18	○	○
W32.Mytob.BE@mm	2005/4/21	○	○
W32.Feebs.J@mm	2006/1/16	×	○
W32.Badday.A	2007/10/3	○	○
W32.Fubalca.E	2007/4/1	△(Explorer)	△(Internet Explorer)
W32.IRCBot.NG	2011/4/7	△(?)	△(Explorer)
W32.Pilleuz!gen2	2010/2/25	△(?)	△(?)
W32.Ircbrute	2008/6/20	△(Explorer)	×
W32.SillyFDC	2007/2/27	○	×
W32.Disttrack	2012/8/16	×	×
W32.Waledac	2008/12/23	×	×
W32.Downadup	2008/11/21	×	×
W32.Evaman.C@mm	2004/8/3	?	?

ワーム以外のマルウェアに対する検知実験

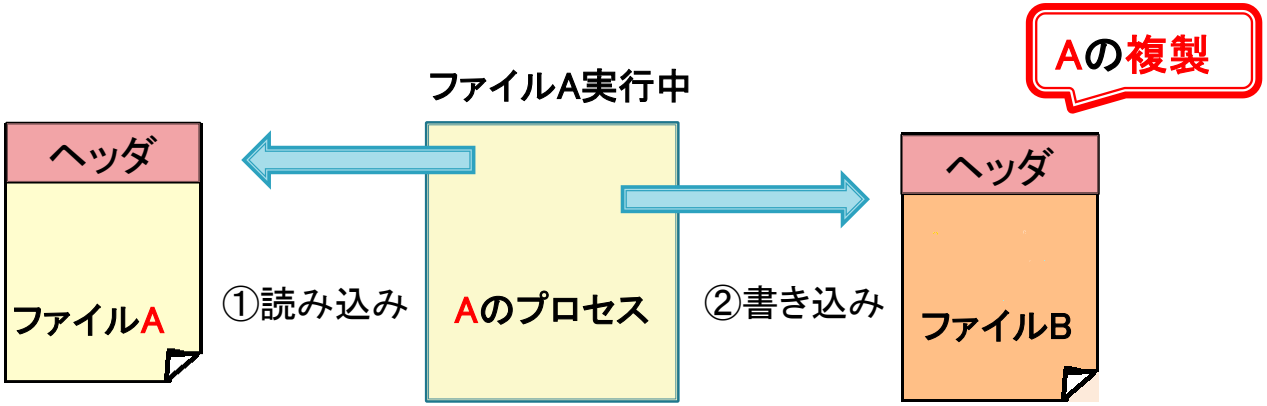
マルウェア名	種別	発見日	ツールによる検知実験
W32.Netsky.D@mm	Virus Worm	2004/3/1	○
W32.Grum.A	Virus	2007/3/30	×
W32.IRCBot	Trojan Worm	2002/7/8	○
W32.IRCBot.Gen	Trojan Worm	2008/10/27	×
W32.Dozer	Trojan Worm	2009/7/8	×
W32.Shadesrat	Trojan Worm	2011/2/22	×
W32.Ckbface!gen1	Trojan Virus	2011/1/27	○
Backdoor.IRC.Bot	Trojan	2003/5/2	○
Trojan.Packed.NsAnti	Trojan	2007/5/30	○
Trojan.FakeAV	Trojan	2007/10/10	○
Backdoor.Spakrab	Trojan	2008/4/7	○
Trojan.Zbot	Trojan	2010/1/10	○
Trojan.Spyeye	Trojan	2010/2/2	○
Trojan.Gen	Trojan	2010/2/19	○
Backdoor.Cycbot!gen3	Trojan	2011/3/3	○
Trojan.Klovbot	Trojan	2011/10/18	○

- 種別がワーム以外のマルウェアに対する，ツールを用いた検知実験
- Windows　XP
- 12/16体が自己複製

既存研究①　-自己ファイルREAD-

- 検出方法
  ワームは自身を拡散する性質がある
  →他のコンピュータに感染時，自身の複製を作成する
  →自分自身のファイルを全てREADする
  自身のファイルを全てREADするという挙動を検出する

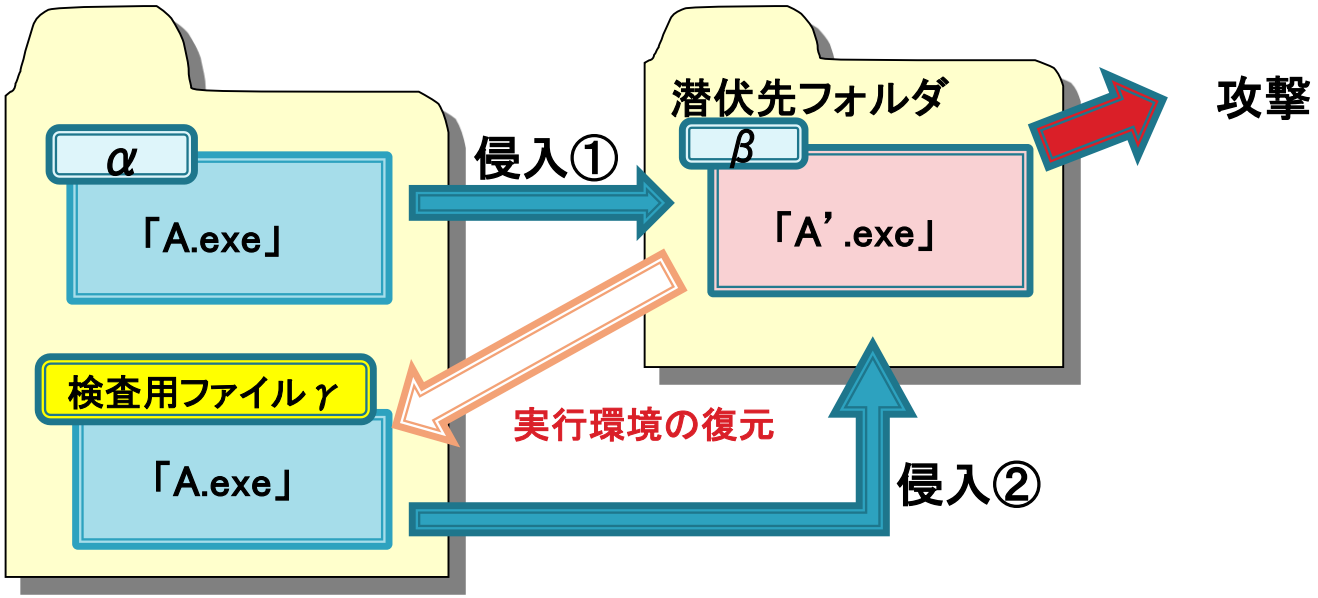
- **課題**
  - 自己ファイルREADは，正規プログラム（WireShark）でも起こる
    →誤検知が起こる



既存研究②　–侵入挙動の反復性–

- **検出方法**
  - ワーム（ボット）はPC内に常駐するために，
    自己複製をし，自動実行リストへ登録する（侵入挙動）
    →PC環境を未感染状態に復元し再実行すると，再び侵入挙動を行う

- 課題：拡散挙動は検出不可，処理が重い



定性評価

- 既存研究と提案方式の定性評価

評価項目	自己ファイルREAD	侵入挙動の反復性	提案方式
変異型ワーム	○	○	○
侵入挙動の検出	○	○	○
拡散挙動の検出	○	×	△
誤検知	×	○	△
処理の重さ	○	×	○