自動実行登録に基づくマルウェアの分類に関する検討と評価

名坂康平† 酒井崇裕† 山本匠†† 竹森敬祐††† 西垣正勝††

†静岡大学大学院情報学研究科，432-8011 静岡県浜松市中区城北 3-5-1

††静岡大学創造科学技術大学院，432-8011 静岡県浜松市中区城北 3-5-1

†††株式会社 KDDI 研究所，356-8502 埼玉県ふじみ野市大原 2-1-15

あらまし 近年のマルウェアの目的から，PC起動時に自らが自動的に実行される環境を整えることは非常に重要なアクションとなっている．著者らはこの自動実行登録に注目したマルウェアの検知方式を提案しているが，マルウェアは多種多様であり，1つの方式ですべてのマルウェアを検知することは難しい．そのため，適切なアプローチに基づいてマルウェアを分類し，それぞれを検知できる方式を組み合わせることによって，網羅的にすべてのマルウェアを検知することが重要である．本稿では自動実行登録という挙動に着目してマルウェアの分類を行い，CCCDataSet2010を用いて評価を行った．

Study and evaluation on classification of malware based on automatic execution set-up

Kohei Nasaka† Takahiro Sakai† Takumi Yamamoto††
Keisuke Takemori††† Masakatsu Nishigaki††

†Graduate school of Informatics, Shizuoka University,
3-5-1 Johoku, Naka, Hamamatsu,Shizuoka, 432-8011 Japan
††Graduate School of Science and Technology, Shizuoka University,
3-5-1 Johoku, Naka, Hamamatsu,Shizuoka, 432-8011 Japan

Abstract. Today's malwares, such as bots, are remotely controlled by commands sent through the Internet from an attacker. This means that these malwares have to stay alive themselves in PC so that they can await for future commands from the attacker. In other words, for almost all malwares, intrusion into operating system directory and registration themselves to auto run list are key functions which they should equip. This motivated us to study a malware detection scheme based on the action with respect to automatic execution set-up, however, due to vast diversity of malwares, it has been difficult to find all the malwares by one scheme only. Hence it is important to categorize all variety of malwares based on some appropriate manner, and use a suitable detection scheme respectively for each category of malwares. That is, to enumerate every possible detection schemes is necessary for coping with today's malwares. Therefore, in this paper, as the first step to the goal, we try to categorize malwares based on a behavior with respect to automatic execution set-up. Then, we evaluate the validity of the proposed classification by using CCC DATAset2010.

1　はじめに

近年，ボットやスパイウェアなどに代表される金銭目的のマルウェアの被害が増大している[1]．その対策として，これまでに様々なマルウェア検知手法が提案されてきているが，著者らは，未知のマルウェアを効果的に検知することが可能であるという観点から，ビヘイビアブロッキング法[2]に注目している．ビヘイビアブロッキング法では，システム上で動作しているプロセスの動きを監視し，マルウェアによく見受けられる挙動を検出することによって検知を行う．

金銭目的のマルウェアの場合，マルウェアがその目的を達成するためには，感染 PC 内に長期間潜伏・常駐し続けることが非常に重要である．そのため，システムフォルダ内に侵入し，自身を OS の自動実行リスト（レジストリ，スタートアップフォルダ，サービスプロセスなど）に登録するという一連の挙動は必須のビヘイビアであると考えられる．

著者らは，この自動実行登録の挙動に注目したマルウェアの検知方式を提案している[3]．しかしながら，マルウェアは感染手順だけを見ても多種多様であり，1 つの方式ですべてのマルウェアを検知することは難しい．そのため，自動実行登録という観点からマルウェアを分類し，複数の方式を組み合わせて，網羅的にすべてのマルウェアを検知することが重要である．

そこで本稿では，自動実行登録という挙動に着目し，マルウェアの分類を行うことを試みる[4]．今後，本稿で行ったマルウェアの分類結果を礎として，どういうタイプのマルウェアがどのタイプの既存方式で検知できるのか，どういうタイプのマルウェアが既存方式では検知できないのかを検討することが可能となると期待できる．

以下 2 章で既存研究について紹介し，3 章で自動実行登録に基づいたマルウェアの分類を行う．4 章で実際に検体を用いて分類の検討を行い，5 章で本稿をまとめる．

2　既存研究

自動実行登録の挙動に注目したマルウェアの検知方式はすでにいくつか提案されている．

「Windows API の監視による 不正インストール検出手法の検討」[5]は，Windows API を介したレジストリの変更を監視し，変更があった場合にアラートを上げる方式である．自動実行登録の多くはレジストリの追加・変更によって行なわれるため，この方式を適用することにより自動実行登録を行うようなマルウェアを検知することができる．しかし，レジストリの変更はインストーラ等の正規プログラムも数多く行なうため，正規プログラムを誤って検知してしまう可能性が高い．

著者らは，このような誤検知を避ける手法として「侵入挙動の反復性によるボット検知方式」[3]を提案している．この方式では，ボットは侵入挙動（自身の潜伏環境を整える挙動）と攻撃挙動（実際に被害を与える挙動）の両機能を併せ持つという特徴と，ボットは実行環境によって挙動を変化させるという特徴に基づいた「侵入挙動の反復性」を利用してボットを検知する．以下に，その具体的な説明をする．

ボットは，初めて PC に潜りこむ際に侵入挙動を行い，その後，C&C サーバからの指令に従って様々な攻撃挙動を行う．このような侵入と攻撃の一連の挙動は，ボットが自身の目的を達成するために不可欠なものである．よって，ボットは基本的には侵入・攻撃の両機能を単一の検体の中に有していることが期待される．

これを逆に捉えれば，侵入・攻撃の両機能を有しているボットは，PC 内で初めて実行された時には必ず侵入挙動を行うということを意味する．このため，実行環境に応じて侵入挙動と攻撃挙動を使い分けるボットにおいては，図 1 のように，自動実行登録された実行ファイルの実行環境を感染初期の状態に戻してやることによって，侵入挙動が再び観測される．この方式ではこの「侵入挙動が繰り返される」というボット特有の挙動を利用している．

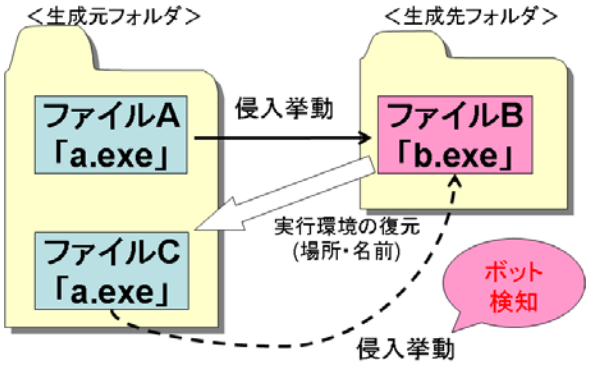

図 1 侵入挙動の反復性

この方式は，侵入機能と攻撃機能を併せ持つタイプのボットに対しては有効であり，かつ，正規のインストーラを誤検知することもないという特長を有する．

しかし，マルウェアは多種多様であり，「ダウンローダ」と呼ばれるタイプのボットのように，侵入機能のみを有する検体と攻撃機能のみを有する検体が別々に存在し，前者は後者を OS の自動実行リストに登録する作業のみを担う場合もありうる．この場合は，「自動実行登録された攻撃機能のみを有する検体の実行環境」を「自動実行登録を行った侵入挙動のみを有する検体の初期環境」に復元したとしても，侵入挙動が再び観測されることは無い．

このように，この方式は検知対象は絞られるが誤検知無くマルウェアを検出することに成功している．したがって，この他にもこのような誤検知の無い検知方式を種々検討し，それら複数の方式を併用することによって，すべてのマルウェアを誤検知なく検知することが可能であると期待できる．ただし，それぞれの方式で検知可能なマルウェアの性質は当然のことながら異なる．よって効率よくすべてのマルウェアを検知するためには，マルウェアの分類を行い，分類ごとにマルウェアの本質を捉えた検知方式を検討していくことが望ましい．本稿ではこの目的を達成するための第 1 段階として，マルウェアの自動実行登録に関する挙動に着目し，マルウェアの分類図を作成する[4].

3 自動実行登録の方法に基づくマルウェアの分類

3.1 分類図の作成

ボット等のマルウェアは，その目的を達成するために，感染 PC 内に長期間潜伏・常駐し続けることが非常に重要となる．よって本論文では，マルウェアの「感染 PC に自分自身を自動実行登録する」という挙動に着目して，マルウェアの分類を行う[4].

図 2 に分類図を示す．本検知方式においては，ある実行ファイル α によって実行ファイル β が自動実行リストに登録されたイベントを基点に，検査が開始される（図 2 の①）．自動実行登録を行わないマルウェアとして，寄生型，メモリ常駐型などがあるが，今回は対象外である（図 2 の②）．

自動実行登録された実行ファイル β の分類を考えた場合（図 2 の③），$\beta = \alpha$ であるか，$\beta \neq \alpha$ のいずれかである．$\beta = \alpha$ の場合（図 2 の④）は，α が α 自身を自動実行登録したことを意味する．この場合，自動実行登録を行った α（すなわち，侵入機能を有するマルウェア）そのものが自動実行登録されたため，自動実行登録された β（$= \alpha$）を実行した場合，再び侵入挙動が観測される．よって，図 2 の④に分類されるマルウェアは文献[3]の方法で検知可能である．

$\beta \neq \alpha$（図 2 の⑤）の場合は，α が α 自身とは異なる β を自動実行登録したことを意味する．そこで次に，どのような β が自動実行登録されたかという観点に着目して分類を続ける．β の機能の分類を考えた場合，β は侵入機能を有するか否かのいずれかである．β が侵入機能を有する場合（図 2 の⑥），自動実行登録された β を実行した場合に再び侵入挙動が観測される．よって，図 2 の⑥に分類されるマルウェアは文献[3]の方法で検知可能である．

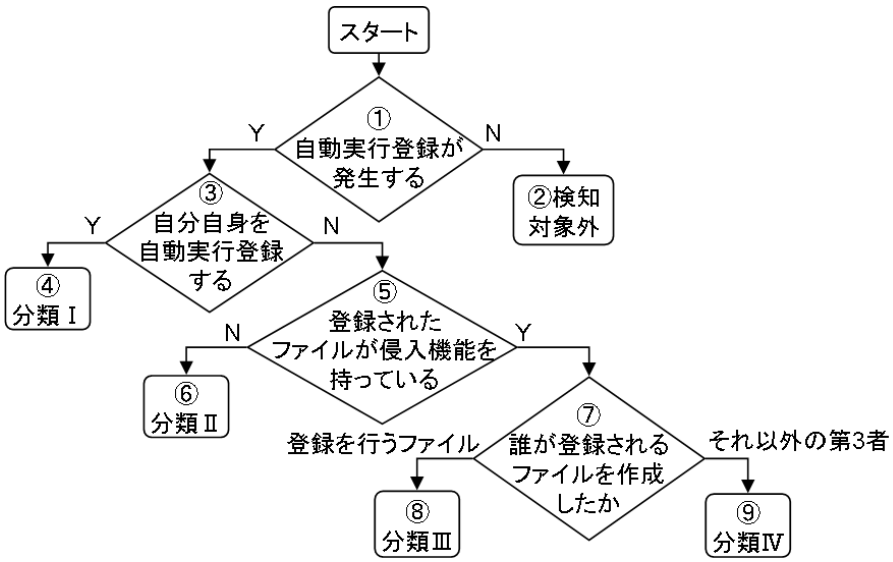

図 2 自動実行登録に基づくマルウェアの分類

2 章で述べたように，侵入挙動と攻撃挙動がマルウェアの本質的な挙動であるといえる．よって，β が侵入機能を所持しない場合（図 2 の⑦）とは，「侵入機能のみを有するマルウェア（α）が，攻撃挙動のみを有するマルウェア（β）を自動実行リストに登録する」という機能分化・連携型のマルウェアの感染を意味している．そこで更に，β が誰に作成されたかという観点に着目して分類を続ける．β を作成したエンティティを考えた場合，α が β を生成したか（図 2 の⑧），α 以外の実行ファイル γ が β を生成したか（図 2 の⑨）のいずれかである．

以上の分類によって，マルウェアは分類 I（図 2 の④），分類 II（図 2 の⑥），分類 III（図 2 の⑧），分類 IV（図 2 の⑨）に分けられる．

3.2 実行ファイルのリンク

分類 III（図 2 の⑧）のマルウェアは，「侵入機能を有するマルウェア α が，攻撃機能を有するマルウェア β を生成した上で β を自動実行リストに登録する」というタイプのマルウェアである．この様子を模式的に図示したものを図 3 に示す．

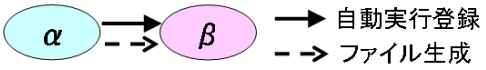

図 3 分類 III のマルウェア

一方，分類 IV（図 2 の⑨）のマルウェアは「攻撃機能を有するマルウェア β を生成する第三のマルウェア γ が存在しており，侵入機能を有するマルウェア α がこれを利用して β を自動実行リストに登録する」というタイプのマルウェアである．この様子を模式的に図示したものを図 4 に示す．

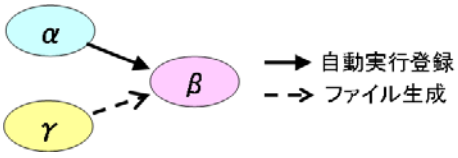

図 4 分類 IV のマルウェア

最近になって，複数のマルウェアが連携して 1 台の PC を狙って感染してくる例が報告されてはいるものの[6][7]，複数のマルウェアによる連携感染は（単体のマルウェアによる感染と比べて）マルウェアの数が多い分だけ，その制御が難しくなる．例えば，仮に，α と γ を別の経路で感染させるような方法を採るマルウェアがあった場合，そのマルウェアは複数の脆弱性（感染ルート）が存在する PC にしか感染することができない．よって，分類 IV における 2 つのマルウェア α と β は，通常，1 系統の制御によって稼動していることのほうが多いのではないかと推測される．これを「実行ファイルのリンク」という概念で模式的に表したものが図 5 である．

図 5(a)は，局所的には「γ_{P1}（$\neq \alpha$）が生成した β を，α が自動実行リストに登録している」ように見えるが，実際には，α は γ_{P1} によって生成されており，その制御の担い手は γ_{P1} 一人である．よって，この場合，γ_{P1} と α を一つのグループとして捉えれば，図 5(a)は図 3 のモデルに帰着することになる．すなわち，図 5(a)は分類 III のマルウェアと見なせる．なお，$\gamma_{P1} \Rightarrow \gamma_{P2} \Rightarrow \cdots \Rightarrow \alpha$ というように，複数のリンクが存在していても同様である．

図 5(b)は，局所的には「γ_{Q1}（$\neq \alpha$）が生成した β を，α が自動実行リストに登録している」ように見えるが，実際には，α が γ_{Q1} を生成しており，その制御の担い手は α 一人である．よって，この場合，α と γ_{Q1} を一つのグループとして捉えれば，図 5(b)は図 3 のモデルに帰着することになる．すなわち，図 5(b)は分類 III のマルウェアと見なせる．なお，$\alpha \Rightarrow \cdots \Rightarrow \gamma_{Q2} \Rightarrow \gamma_{Q1}$ というように，複数のリンクが存在していても同様である．

図 5(a)と図 5(b)をまとめると図 5(c)のように表すことができる．図 5(c)は，局所的には「γ_{PQ1}（$\neq \alpha$）が生成した β を，α が自動実行リストに登録している」ように見えるが，実際には，γ_{P1} が α と γ_{PQ1} を生成しており，その制御の担い手は γ_{P1} 一人である．図 5(c)も図 3 のモデルに帰着し，分類 III のマルウェアと見なされる．

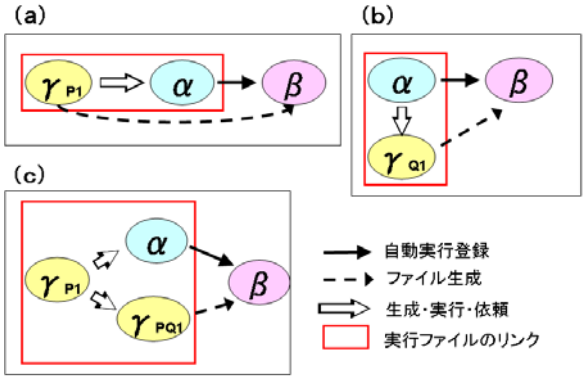

図 5 実行ファイルのリンクによる分類 III の拡張

以上より，実行ファイルのリンクを辿ったとしても，やはり α と γ の制御が異なるタイプのマルウェアのみが分類 IV（図 2 の⑨）に残ることになる．このタイプのマルウェアのモデルを図 5(c)に合わせた形で図示

すると，図 6 のようになる．図 6 のマルウェアは，局所的には「γ（$\neq\alpha$）が生成したβを，αが自動実行リストに登録している」ように見え，実際に，αの起源となっているγ_{P1}とγの起源となっているγ_{R1}の間に制御関係の依存はない．

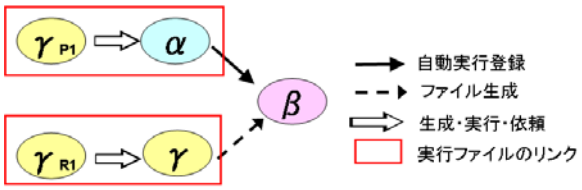

図 6 実行ファイルのリンクによる分類Ⅳの拡張

4 検証

CCC DATAset2010[8]のマルウェア検体 50 体に対し，提案した自動実行登録方法の分類を適用し，分類図の妥当性について検証を行った．自動実行リストへの登録に関しては，自動実行リスト上のプログラムを一覧表示するモニタツールである Autoruns[9]を用いて確認した．また，ファイル生成や実行ファイルのリンクに関しては，プロセスのファイルアクセスを監視可能なモニタツールである ProcMon[10]を用いて確認を行った．

本実験は物理的に隔離されたネットワーク上で行った．実験に使用したマシンの OS は Windows XP Professional SP2 である．

4.1 分類結果

CCC DATAset2010 に含まれる検体の分類結果を表 1 に示す．なお，CCC DATAset2010 のマルウェア検体は 50 体であったが，本実験の実験環境において実行不可能（実行すると，エラーが表示されプロセスが終了する）な検体が 2 体存在したため，実行可能であった 48 検体に対して検討を進めた．

表 1 分類結果

分類	合計
検知対象外	21
分類Ⅰ	1
分類Ⅱ	19
分類Ⅲ	2
分類Ⅳ	0
その他	5

表 1 の「検知対象外」は，実行ファイルの自動実行登録を行わなかった検体である．CCC DATAset2010 の中には，このような検体が 21 体存在した．検知対象外の検体を除くと，文献[3]の方式で検知が可能である分類Ⅰ，分類Ⅱの検体が大半を占めていることがわかる．分類Ⅲの検体も 2 体存在した．分類Ⅳにおいては，該当する検体が存在しなかった．分類Ⅳについては，今回の実験では，検体を一つずつ実行して検証を行ったため，複数のファイルが協力して自動実行登録を行うという動作は観測されなかったと考えられる．

なお，「その他」の検体は，実行ファイルが自動実行リストに登録されたが，登録されたファイルの所在が見つからない（Explorer 上からアクセスできない）もの，自分自身で自動実行登録した実行ファイルを削除してしまうものなどである．なお，このように自動実行登録された実行ファイルが存在しない検体に対しては，文献[3]の方法による検知を行うことはできない．

4.2 考察

今回の検体においては，検知対象外の検体が約半数存在したが，その中には接続先の C&C サーバが存在しないために動作を終了していると見受けられる検体も含まれていた．今回の実験は物理的に隔離されたネットワーク上で行っており，マルウェアが完全に動作するには不十分な実験環境であったために自動実行登録が観測されなかった可能性もある．そのため，これらの検体は環境を適切に整えて実験を行うことによって自動実行登録が観測され，分類を行うことができる可能性がある．環境を整えても自動実行登録を行わない検体に関しては，自動実行登録という以外の観点から，今後分類を検討していく必要がある．

「その他」と判断された検体は，自動実行登録されたファイルを何らかの方法でアクセス不可能，あるいは削除するため，図 2 の⑤の判定（登録されたファイルが侵入機能を持っているか）を行うことができず，正しく分類を行うことができなかった．ただし，これらの検体はすべて自身が生成した実行ファイルを自動実行登録していたため，分類Ⅱまたは分類Ⅲのいずれかに含まれる検体であるということは確認できた．これらの検体についても正確な分類ができるよう，観測の精度を高めることが今後の課題となる．なお，このような「ファイルの存在を隠す」というと

いう挙動は，検知や解析を回避するためのマルウェア特有の動きであり，それ自体に特徴があると考えられる．そのため，この特徴を分類の観点に組み入れることによって，新たな分類図を生成することも可能となる．

分類Ⅲと判定された 2 つの検体は，どちらも自動実行登録されたファイルが侵入機能を持っていなかった．自動実行登録という挙動のみを考えた場合，分類Ⅲのマルウェアは正規のインストーラとの区別がつかない．よって，分類Ⅲに含まれる検体については，マルウェアと正規プログラムの判別をするために，さらに細かく分類を行っていく必要がある．そこで，今回分類Ⅲに分類された 2 つの検体の動作を詳細に解析してみた．

1 つ目の検体は，バッチファイルを生成・実行し，その中で 2 つの実行ファイルを生成・自動実行登録していた．ここで，この 2 つの実行ファイルは，バッチファイルの実行の中でバッチファイルを生成した検体自身に引数を与えて実行させることにより生成されていた．自分自身を再実行するような動作はマルウェア特有の特徴的な挙動であると考えられる．よって，このような「実行のリンク」に注目することで，分類Ⅲのマルウェアを更に分類することができる可能性がある．

2 つ目の検体は，実行するたびに異なるファイル名の実行ファイルを生成・自動実行登録していた．自動実行登録される実行ファイル名を毎回変更するような動作はマルウェア特有の特徴的な挙動であると考えられる．よって，このような「生成ファイル名」に着目することで，分類Ⅲのマルウェアを更に分類することができる可能性がある．

5　まとめ

本稿では，マルウェアの自動実行登録という挙動に着目し，マルウェアの分類を行った．さらに CCC DATAset2010 に対し，本稿で行ったマルウェアの分類を適用し，その分類結果を考察した．

自動実行登録という挙動のみを考えた場合，分類Ⅲのマルウェアは正規のインストーラとの区別がつかない．よって，今後は分類Ⅲに含まれる検体を更に詳細に分類していく方法を検討していく必要がある．

参考文献

[1] サイバークリーンセンター，“平成 20 年度サイバークリーンセンター(CCC)活動報告”，https://www.ccc.go.jp/report/h20ccc_report.pdf

[2] 情報処理推進機構，″未知ウイルス検出技術に関する調査″，http://www.ipa.go.jp/security/fy15/reports/uvd/index.html

[3] 酒井崇裕，竹森敬祐，安藤類央，西垣正勝，“侵入挙動の反復性によるボット検知方式”，コンピュータセキュリティシンポジウム 2009 論文集，pp.781-786(2009.10)

[4] 名坂康平，酒井崇裕，山本匠，竹森敬祐，西垣正勝，“自動実行登録に基づくマルウェアの分類に関する検討”，情報処理学会研究報告，2010-CSEC-50-40，pp.1-5(2010.7)

[5] 三根 健司，鈴木秀和，渡邊晃，“Windows API の監視による不正インストール検出手法の検討”，2007 年電気関係学会東海支部連合大会講演論文集，論文番号 O-372(2007.9)

[6] 竹森敬祐，酒井崇裕，西垣正勝，安藤類央，三宅優，“マルウェア通信活動抑制のためのネットワーク制御”，コンピュータセキュリティシンポジウム 2009 論文集，pp.409-414(2009.10)

[7] 桑原和也，菊池浩明，寺田真敏，藤原将志，“パケットキャプチャーから感染種類を判定する発見的手法について”，コンピュータセキュリティシンポジウム 2009 論文集，pp.397-402(2009.10)

[8]畑田充弘，他：マルウェア対策のための研究用データセット～MWS 2010 Datasets～，MWS2010 (2010.10)

[9] Microsoft TechNet，"ProcMon"，http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx

[10] Microsoft TechNet，"Autoruns"，http://technet.microsoft.com/ja-jp/sysinternals/bb963902.aspx