Vol.2010-CSEC-50 No.40
2010/7/2

自動実行登録に基づく マルウェアの分類に関する検討

名坂康平[†]　酒井崇裕[†]　山本匠[††]
竹森敬祐[†††]　西垣正勝[††]

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，その第一歩として，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うことを試みる．

A study on classification of malware based on automatic execution set-up

KOHEI NASAKA[†]　T AKAHIRO SAKAI[†]
T AKUMI YAMAMOTO[††]　KEISUKE　TAKEMORI[†††]
MASAKATSU NISHIGAKI[††]

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 further commands from the attacker. In other words, for almost all malwares, intrusion into 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, it has been difficult to find all the malwares only by one scheme due to vast diversity of malwares. Hence it is important to categorize all variety of malwares based on some appropriate manner, and use a suitable detection scheme 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.

[†]静岡大学大学院情報学研究科，〒432-8011 浜松市中区城北 3-5-1，
Graduate school of Informatics, Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan
[††]静岡大学創造科学技術大学院，〒432-8011 浜松市中区城北 3-5-1，
Graduate School of Science and Technology, Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan
[†††]株式会社KDDI研究所，〒356-8502 埼玉県ふじみ野市大原2-1-15，
KDDI R&D Laboratories, Inc. 2-1-15 Ohara, Fujimino, Saitama, 356-8502 JAPAN

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．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 章で本稿をまとめる．

2. 既存研究

本章では，自動実行登録の挙動に着目したビヘイビアブロッキング法として，侵入挙動の反復性によるボット検知方式[3]について説明する．

ボットは，初めて PC に潜りこむ際に，自身の潜伏環境を整えるために，自分自身

の実行ファイルを OS の自動実行リストに登録するなどの「侵入挙動」を示す．そしてシステムに侵入した後，C&C サーバからの指令に従って様々な「攻撃挙動」を行う．このような侵入挙動と攻撃挙動の一連の挙動は，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．我々は，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た検知方式を提案している[3].

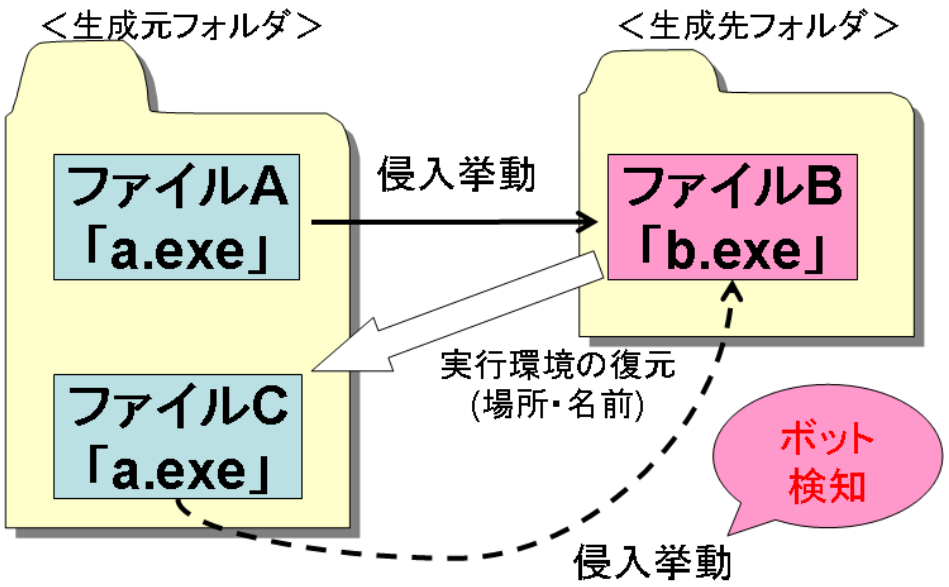

図 1　侵入挙動の反復性
Figure 1 Repetitiveness of intrusion

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，すべてのマルウェアを検知するためには，単一の方式だけでは不十分であり，マルウェアのタイプごとに適した検知方式を検討する必要がある．

3.　自動実行登録方法の分類

本章では，マルウェアの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う．

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．よって本研究では，「自動実行登録されるマルウェア」を検知対象とする．

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，今回どのような 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．

2 章の冒頭で述べたように，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．

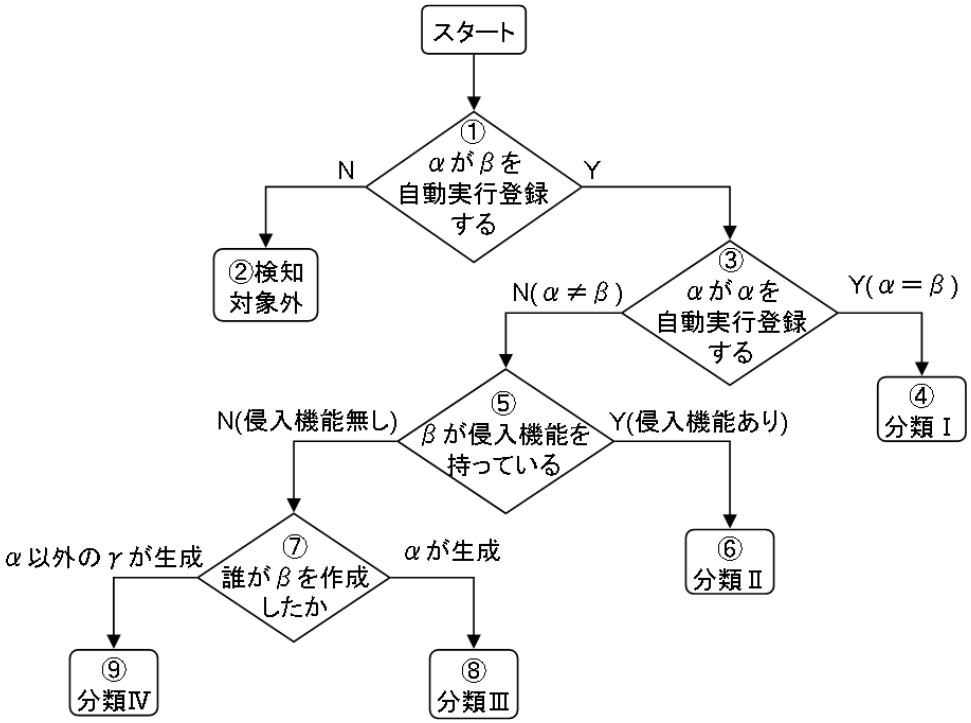

図 2 マルウェアの分類
Figure 2 Classification of malware

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．

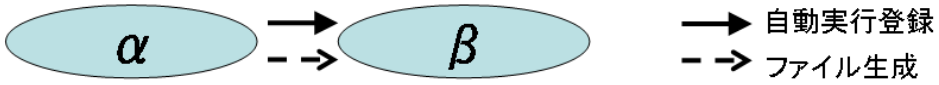

図 3 分類 III のマルウェア
Figure 3 Malware in category III

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．

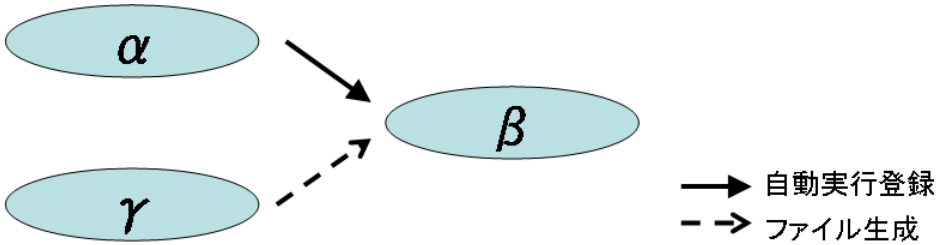

図 4 分類 IV のマルウェア
Figure 4 Malware in category IV

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[4][5]，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}（≠α）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．

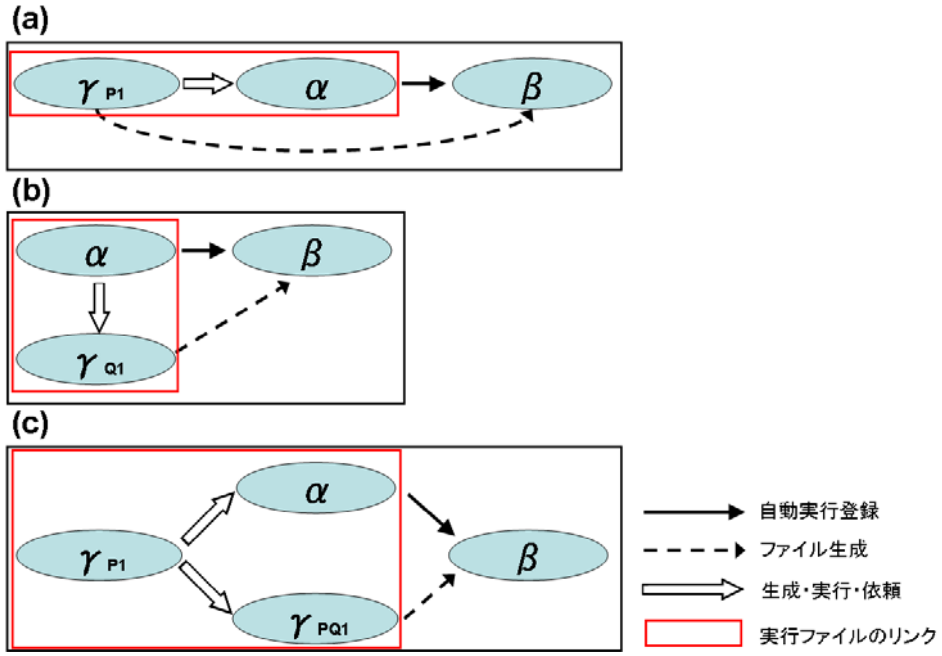

図 5　実行ファイルのリンクによる分類 III の拡張
Figure 5 Malware in category III with consideration of execution link

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．

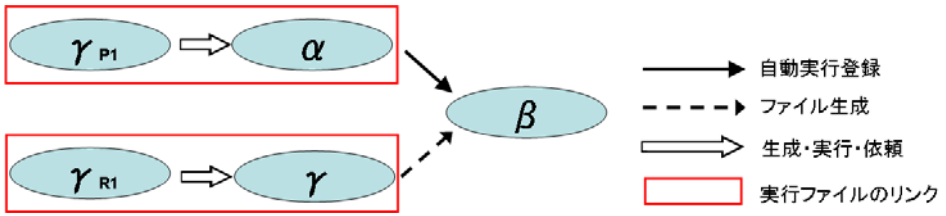

図 2　実行ファイルのリンクによる分類 IV の拡張
Figure 6 Malware in category IV with consideration of execution link

4. 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．今後は，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調査していく．また，既存方式では検知することができないマルウェアに対しては，その検知方式を検討していきたい．今回の分類の際にマルウェアの特徴を定式化することができたと考えている．よって，既存方式では検知不可能なマルウェアに対する検知方式を検討するにあたっては，今回の分類作業を通じて獲得された知識を役立てることができるのではないかと期待している．

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）

Vol.2010-CSEC-50 No.40
2010/7/2

[4] 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）
[5] 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）