(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5882542号
(P5882542)
(45)発行日　平成28年3月9日(2016.3.9)　(24)登録日　平成28年2月12日(2016.2.12)

(51)Int.Cl.　F I
G06F 21/56 (2013.01)　G06F 21/56 360

請求項の数 14 (全 16 頁)

(21)出願番号	特願2015-525646(P2015-525646)
(86)(22)出願日	平成25年8月26日(2013.8.26)
(65)公表番号	特表2015-523668(P2015-523668A)
(43)公表日	平成27年8月13日(2015.8.13)
(86)国際出願番号	PCT/US2013/056562
(87)国際公開番号	WO2014/035857
(87)国際公開日	平成26年3月6日(2014.3.6)
審査請求日	平成27年1月28日(2015.1.28)
(31)優先権主張番号	13/973,229
(32)優先日	平成25年8月22日(2013.8.22)
(33)優先権主張国	米国(US)
(31)優先権主張番号	201210310462.4
(32)優先日	平成24年8月28日(2012.8.28)
(33)優先権主張国	中国(CN)

早期審査対象出願

(73)特許権者　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　110000028
特許業務法人明成国際特許事務所

最終頁に続く

(54)【発明の名称】マルウェアプロセスの検出

(57)【特許請求の範囲】
【請求項１】
マルウェアプロセスを検出するためのシステムであって、
１つ以上のプロセッサと、
前記１つ以上のプロセッサに結合され、前記１つ以上のプロセッサに命令を提供するように構成された１つ以上のメモリと、を備え、
前記１つ以上のプロセッサは、
プロセスの起動を監視し、
前記プロセスの前記起動の完了に対応して、前記プロセスの実行より前に、前記プロセスに関係付けられたベースアドレスを決定し、前記プロセスに関係付けられた前記ベースアドレスは、そこから命令が読み出されて実行されるメモリブロックに関係付けられ、
前記ベースアドレスに関係付けられた前記メモリブロックの許可を決定し、前記メモリブロックの許可は、読み出し及び書き込みのうち少なくとも１つが前記メモリブロックにおいて許可されたかどうかに関係付けられ、
前記メモリブロックの前記決定された許可に少なくとも部分的に基づいて、前記プロセスがマルウェアプロセスに関係付けられている可能性があるかどうかを決定し、
前記メモリブロックの前記許可が読み出し専用許可を含む場合に、
前記プロセスが前記マルウェアプロセスに関係付けられている可能性がないことを決定し、
前記プロセスの前記実行を許可し、

前記メモリブロックの前記許可が前記読み出し専用許可を含まない場合に、
前記プロセスに関係付けられたメモリ画像に含まれるポータブル実行可能ヘッダコードが指定のコードに一致するかどうかを決定し、
前記プロセスに関係付けられた前記メモリ画像に含まれる前記ポータブル実行可能ヘッダコードが前記指定のコードに一致するかどうかに少なくとも部分的に基づいて、前記プロセスが前記マルウェアプロセスに関係付けられている可能性があるかどうかを決定し、
前記プロセスに関係付けられた前記メモリ画像に含まれる前記ポータブル実行可能ヘッダコードが前記指定のコードに一致するかどうかに少なくとも部分的に基づいて、前記プロセスの前記実行を防ぐことを決定する、ように構成される、システム。

【請求項２】
請求項１に記載のシステムであって、
前記ベースアドレスは、前記プロセスに対応する拡張指示ポインタ情報に関係付けられた戻りアドレスに少なくとも部分的に基づいて決定される、システム。

【請求項３】
請求項１に記載のシステムであって、
前記ベースアドレスは、オペレーティングシステムによって記録される、システム。

【請求項４】
請求項１に記載のシステムであって、
前記読み出し専用許可を含まない前記許可は、書き込みを許可する、システム。

【請求項５】
請求項４に記載のシステムであって、
前記メモリブロックの前記許可が前記読み出し専用許可を含まない場合に、前記１つ以上のプロセッサは、さらに、前記マルウェアプロセスに関係付けられた警告メッセージを、ユーザインターフェースにおいて提示するように構成される、システム。

【請求項６】
請求項１に記載のシステムであって、
前記プロセスに関係付けられた前記ポータブル実行可能ヘッダコードが前記指定のコードに一致する場合に、前記１つ以上のプロセッサは、さらに、前記プロセスが前記マルウェアプロセスに関係付けられている可能性があると決定し、前記プロセスの前記実行を防ぐように構成される、システム。

【請求項７】
請求項６に記載のシステムであって、
前記プロセスに関係付けられた前記ポータブル実行可能ヘッダコードが前記指定のコードに一致しない場合に、前記１つ以上のプロセッサは、さらに、前記プロセスが前記マルウェアプロセスに関係付けられていないと決定し、前記プロセスの前記実行を許可するように構成される、システム。

【請求項８】
マルウェアプロセスを検出するための方法であって、
プロセスの起動を監視することと、
前記プロセスの前記起動の完了に対応して、前記プロセスの実行より前に、１つ以上のプロセッサを使用して、前記プロセスに関係付けられたベースアドレスを決定することであって、前記プロセスに関係付けられた前記ベースアドレスは、そこから命令が読み出されて実行されるメモリブロックに関係付けられる、ベースアドレスの決定と、
前記ベースアドレスに関係付けられた前記メモリブロックの許可を決定することであって、前記メモリブロックの前記許可は、読み出し及び書き込みのうち少なくとも１つが前記メモリブロックにおいて許可されたかどうかに関係付けられる、前記メモリブロックの許可の決定と、
前記メモリブロックの前記決定された許可に少なくとも部分的に基づいて、前記プロセスがマルウェアプロセスに関係付けられている可能性があるかどうかを決定することと、

前記メモリブロックの前記許可が読み出し専用許可を含む場合に、
前記プロセスが前記マルウェアプロセスに関係付けられている可能性がないことを決定することと、
前記プロセスの前記実行を許可することと、
前記メモリブロックの前記許可が前記読み出し専用許可を含まない場合に、
前記プロセスに関係付けられたメモリ画像に含まれるポータブル実行可能ヘッダコードが指定のコードに一致するかどうかを決定することと、
前記プロセスに関係付けられた前記メモリ画像に含まれる前記ポータブル実行可能ヘッダコードが前記指定のコードに一致するかどうかに少なくとも部分的に基づいて、前記プロセスが前記マルウェアプロセスに関係付けられている可能性があるかどうかを決定することと、
前記プロセスに関係付けられた前記メモリ画像に含まれる前記ポータブル実行可能ヘッダコードが前記指定のコードに一致するかどうかに少なくとも部分的に基づいて、前記プロセスの前記実行を防ぐかどうかを決定することと、を含む、方法。

【請求項９】
請求項８に記載の方法であって、
前記ベースアドレスは、前記プロセスに対応する拡張指示ポインタ情報に関係付けられた戻りアドレスに少なくとも部分的に基づいて決定される、方法。

【請求項１０】
請求項８に記載の方法であって、
前記読み出し専用許可を含まない前記許可は、書き込みを許可する、方法。

【請求項１１】
請求項１０に記載の方法であって、
前記メモリブロックの前記許可が前記読み出し専用許可を含まない場合に、さらに、前記マルウェアプロセスに関係付けられた警告メッセージを、ユーザインターフェースにおいて提示することを含む、方法。

【請求項１２】
請求項８に記載の方法であって、
前記プロセスに関係付けられた前記ポータブル実行可能ヘッダコードが前記指定のコードに一致する場合に、さらに、前記プロセスが前記マルウェアプロセスに関係付けられている可能性があると決定し、前記プロセスの前記実行を防ぐことを含む、方法。

【請求項１３】
請求項８に記載の方法であって、
前記プロセスに関係付けられた前記ポータブル実行可能ヘッダコードが前記指定のコードに一致しない場合に、さらに、前記プロセスが前記マルウェアプロセスに関係付けられていないと決定し、前記プロセスの前記実行を許可することを含む、方法。

【請求項１４】
マルウェアプロセスを検出するためのコンピュータプログラムであって、コンピュータを使用して、
プロセスの起動を監視する機能と、
前記プロセスの前記起動の完了に対応して、前記プロセスの実行より前に、前記プロセスに関係付けられたベースアドレスを決定するための機能であって、前記プロセスに関係付けられた前記ベースアドレスは、そこから命令が読み出されて実行されるメモリブロックに関係付けられる、ベースアドレスの決定機能と、
前記ベースアドレスに関係付けられた前記メモリブロックの許可を決定する機能であって、前記メモリブロックの許可は、読み出し及び書き込みのうち少なくとも１つが前記メモリブロックにおいて許可されたかどうかに関係付けられる、前記メモリブロックの許可決定機能と、
前記メモリブロックの前記決定された許可に少なくとも部分的に基づいて、前記プロセスがマルウェアプロセスに関係付けられている可能性があるかどうかを決定する機能と、

前記メモリブロックの前記許可が読み出し専用許可を含む場合に、
前記プロセスが前記マルウェアプロセスに関係付けられている可能性がないことを決定し、
前記プロセスの前記実行を許可し、
前記メモリブロックの前記許可が前記読み出し専用許可を含まない場合に、
前記プロセスに関係付けられたメモリ画像に含まれるポータブル実行可能ヘッダコードが指定のコードに一致するかどうかを決定し、
前記プロセスに関係付けられた前記メモリ画像に含まれる前記ポータブル実行可能ヘッダコードが前記指定のコードに一致するかどうかに少なくとも部分的に基づいて、前記プロセスが前記マルウェアプロセスに関係付けられている可能性があるかどうかを決定し、
前記プロセスに関係付けられた前記メモリ画像に含まれる前記ポータブル実行可能ヘッダコードが前記指定のコードに一致するかどうかに少なくとも部分的に基づいて、前記プロセスの前記実行を防ぐかどうかを決定する、
機能と、を実現するための、コンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

［関連出願の相互参照］

本出願は、２０１２年８月２８日に出願され「Ａ　ＴＲＯＪＡＮ　ＨＯＲＳＥ　ＤＥＴＥＣＴＩＯＮ　ＭＥＴＨＯＤ　ＡＮＤ　ＤＥＶＩＣＥ（トロイの木馬を検出する方法及び機器）」と題された中国特許出願第２０１２１０３１０４６２．４号の優先権を主張する。該出願は、あらゆる目的のために、参照によって本明細書に組み込まれる。

【０００２】

本出願は、通信技術の分野に関し、特に、マルウェアプロセスを検出するための技術に関する。

【背景技術】

【０００３】

インターネット技術の更なる普及に伴って、ネットワークセキュリティの問題がいっそう目立ってきた。特に、トロイの木馬タイプのマルウェアプロセスは、重要な情報の盗用及び破壊を招いてきた。トロイの木馬は、疑いを持たないユーザの機器にダウンロードされ、オペレーティングシステムへの特権的アクセスを得る及び／又は悪性コードを機器にインストールするタイプのマルウェアである。多くの場合、トロイの木馬は、悪意を持つ者にユーザ機器への不正アクセスを提供する。悪意を持つ者は、そのような不正アクセスを悪用して情報を盗む及び／又はそれ以外の形でユーザ機器に危害を加える。

【０００４】

従来タイプのトロイの木馬検出技術の１つは、以下のとおりである。即ち、トロイの木馬に関係しているとまだ決定されていないプロセスからサンプルコードを抽出し、そのサンプルコードを、トロイの木馬特徴データベースに保存されている既知のトロイの木馬プロセス特徴コードに関係付けられた１つ以上の特徴コードと比較し、もし、一致を見つけられたならば、そのプロセスをトロイの木馬プロセスに関係していると決定する。

【０００５】

上述された従来のトロイの木馬検出方法では、信頼できる署名情報を有するプロセス（例えば、いずれの既知のトロイの木馬プロセスに関係付けられた特徴コードにも一致しないサンプルコードを伴うプロセス）又はホワイトリストに載っている信頼できるプロセス（例えば、既知の非マルウェアプロセスに関係付けられた特徴コードに一致するサンプルコードを伴うプロセス）は、トロイの木馬検出を受けないのが一般的である。しかしながら、このような検出技術は、インジェクション型トロイの木馬を検出しない恐れがある。インジェクション型トロイの木馬プロセスは、実行されるときに、先ず、プロセスを起動させる。このプロセスは、既知のマルウェアプロセスに関係付けられた特徴コードに及び

／又はマルウェアプロセスであると決定されなかったいずれのプロセスに関係付けられた特徴コードにも一致せず、その代わり、ホワイトリストに含まれるプロセスに関係付けられた特徴コードに一致するゆえに、マルウェアプロセスであると決定されない、あらゆるプロセスでありうる。このプロセスの起動が完了する前に、インジェクション型トロイの木馬プロセスは、プロセスを休止させ、プロセスに関係付けられたメモリ画像に自身の悪性コードを書き込む。インジェクション型トロイの木馬プロセスは、次いで、プロセスの起動を再開させる。このようにして、インジェクション型トロイの木馬は、従来のトロイの木馬検出技術を巧みに回避する。

【０００６】

一具体例では、インジェクション型トロイの木馬プロセスは、ノードパッドプロセス（notepad.exe）のプロセスを起動させるだろう。このノードパッドプロセスは、信頼できる署名情報を有する（例えば、そのコードのサンプルが、ホワイトリストに載っているコードに一致しえる）ゆえに、マルウェアプロセスであると見なされない。このノードパッドプロセスの起動が完了する前に、インジェクション型トロイの木馬プロセスは、このノードパッドプロセスを休止させ、ノードパッドプロセスのメモリ画像に自身の悪性コードを書き込む。インジェクション型トロイの木馬プロセスは、次いで、ノードパッドプロセスの起動を再開させる。

【０００７】

ノードパッドプロセスの起動が完了した後、このノードパッドプロセスは、トロイの木馬プロセスに関係付けられたものになり、また、信頼できる署名情報を有しているゆえに、従来のトロイの木馬検出技術によってマルウェアを検出することができないだろう。したがって、ノードパッドプロセスは、操り人形型のプロセスであるインジェクション型トロイの木馬プロセスに変容する。インジェクション型トロイの木馬プロセスは、従来のトロイの木馬検出技術を回避するために、悪性プロセスを隠す覆いを外側に纏っているのに等しい振る舞いをする。

【図面の簡単な説明】

【０００８】

以下の詳細な説明及び添付の図面において、本発明の様々な実施形態が開示される。

【０００９】

【図１】マルウェアプロセスを検出するためのシステムの一実施形態を示した図である。

【００１０】

【図２】マルウェアプロセスを検出するためのプロセスの一実施形態を示したフローチャートである。

【００１１】

【図３】マルウェアプロセスを検出するためのプロセスの一実施形態を示したフローチャートである。

【００１２】

【図４】マルウェアプロセスを検出するためのシステムの一実施形態を示した図である。

【発明を実施するための形態】

【００１３】

本発明は、プロセス、装置、システム、合成物、コンピュータ読み取り可能記憶媒体に実装されたコンピュータプログラム製品、並びに／又は結合先のメモリに記憶された命令及び／若しくは結合先のメモリによって提供される命令を実行するように構成されたプロセッサなどのプロセッサのような、数々の形態で実現することができる。本明細書では、これらの実現形態、又は本発明がとりえるその他のあらゆる形態が、技術と称されてよい。一般に、開示されるプロセスの各段階の順番は、本発明の範囲内で変更されてよい。別途明記されない限り、タスクを実施するように構成されるものとして説明されるプロセッサ又はメモリなどのコンポーネントは、所定時にタスクを実施するように一時的に構成された汎用コンポーネントとして、又はタスクを実施するように製造された特殊コンポーネントとして実装されてよい。本明細書で使用される「プロセッサ」という用語は、コンピ

ュータプログラム命令などのデータを処理するように構成された１つ以上の機器、回路、並びに／又は処理コアを言う。

【００１４】

本発明の原理を例示した添付の図面とともに、以下で、本発明の１つ以上の実施形態の詳細な説明が提供される。本発明は、このような実施形態との関わりのもとで説明されるが、いずれの実施形態にも限定されない。本発明の範囲は、特許請求の範囲によってのみ限定され、本発明は、数々の代替形態、変更形態、及び均等物を包含している。以下の説明では、本発明の完全な理解を与えるために、数々の具体的詳細が明記されている。これらの詳細は、例示を目的として提供されるものであり、本発明は、これらの詳細の一部又は全部を伴わずとも、特許請求の範囲にしたがって実施されえる。明瞭を期するために、本発明に関係した技術分野においてで知られる技工物は、本発明が不必要に不明瞭にされないように、詳細な説明を省略されている。

【００１５】

本明細書において、マルウェアプロセス検出の実施形態が説明される。プロセスの起動は、監視される。一部の実施形態では、プロセスは、マルウェアプロセス若しくは非マルウェアプロセスのいずれであるかをまだ決定されておらず、既知のマルウェアプロセスに関係付けられた特徴コードに一致せず、及び／又はホワイトリストに含まれるプロセスに関係付けられた特徴コードに一致している。様々な実施形態において、「ホワイトリスト」は、マルウェアではないと見なされている及び／又は事前に決定されたプロセスを挙げたリストである。プロセスの起動が完了した後、プロセスに関係付けられたベースアドレスに関係付けられたメモリブロックの許可が決定される。例えば、許可は、読み出し専用、書き込み専用、並びに／又は読み出し及び書き込み許容のいずれかであってよい。非マルウェアプロセスのベースアドレスに関係付けられたメモリブロックは、一般に、読み出し専用許可に関係付けられていると想定される。しかしながら、トロイの木馬プロセスは、通常は、悪性コードを書き込むために書き込みを許容する許可を持つメモリブロックを探す必要がある。したがって、様々な実施形態において、もし、プロセスの起動の完了に続いて、プロセスのベースアドレスに関係付けられたメモリブロックが読み出し専用ではない（例えば、書き込み専用や、読み出し及び書き込みの）許可に関係付けられていると決定されたならば、そのプロセスは、トロイの木馬プロセスに関係付けられている可能性があること、及びプロセスの起動中に、トロイの木馬プロセスは、プロセスのベースアドレスを、トロイの木馬プロセスが（例えば、悪性コードを）書き込むことを許可されたメモリブロックに関係付けられるものに変更したことが決定される。しかしながら、もし、プロセスのベースアドレスに関係付けられたメモリブロックが読み出し専用許可に関係付けられていると決定されたならば、プロセスは、トロイの木馬プロセスに関係付けられていないと決定される。

【００１６】

図１は、マルウェアプロセスを検出するためのシステムの一実施形態を示した図である。この例では、システム１００は、機器１０２と、ネットワーク１０４と、第三者システム１０６とを含む。ネットワーク１０４は、様々な高速ネットワーク及び／又は電気通信ネットワークを含む。

【００１７】

機器１０２は、ラップトップとして示されているが、機器１０２は、デスクトップコンピュータ、モバイル機器、スマートフォン、タブレット端末、及び／又は任意の計算機器であってよい。機器１０２には、ソフトウェアアプリケーション及び／又は物理的コンポーネントがインストールされてよく、これは、機器１０２ではなく、マルウェアプロセスである可能性があるプロセスを検出するために機器１０２のオペレーティングシステム及び／又はメモリへのアクセスを有するその他のどこかにインストールされてもよい。マルウェアプロセスの一例は、トロイの木馬プロセスである。例えば、もし、トロイの木馬プロセスなどのマルウェアプロセスが機器１０２にインストールされることになると、第三者システム１０６を使用している悪意あるユーザは、機器１０２に記憶されている情報を

トロイの木馬プロセスを通じて盗もうとする及び／又はそれ以外の形で危害を加えようとするだろう。損なわれたプロセスは、トロイの木馬プロセスによって書き込まれた悪性コードを実行するかもしれないゆえに、トロイの木馬プロセスがいつ機器１０２にインストールされた可能性があるかを検出し、そのトロイの木馬に関係付けられたプロセスの更なる実行をブロックすることが望ましいとされる。マルウェアプロセス検出のためのソフトウェアアプリケーション及び／又は物理的コンポーネントは、機器１０２において起動するプロセスを監視するように構成される。プロセスの起動の完了を受けて、プロセスに関係付けられたベースアドレスが決定される。ベースアドレスに関係付けられた機器１０２に関係付けられたメモリブロックが見つけられ、そのメモリブロックに関係付けられた読み出し及び／又は書き込み許可が決定される。以下で更に説明されるように、プロセスがマルウェアプロセス（例えば、トロイの木馬プロセス）に関係付けられている可能性があるかどうかは、そのプロセスのベースアドレスにおけるメモリブロックに関係付けられた許可のタイプに少なくとも部分的に基づいて決定される。もし、プロセスが、マルウェアプロセスに関係付けられていると決定されたならば、そのプロセスは、悪意あるユーザから機器１０２が遠隔攻撃を受ける可能性を防ぐために、更なる実行が行われないように停止されるだろう。

【００１８】

図２は、マルウェアプロセスを検出するためのプロセスの一実施形態を示したフローチャートである。一部の実施形態では、プロセス２００は、図１の機器１０２において実行に移される。

【００１９】

２０２では、プロセスの起動が監視される。例えば、プロセスは、ユーザによる選択を受けて、又はソフトウェアアプリケーションの実行を受けて起動されてよい。一部の実施形態では、プロセスは、マルウェアプロセス若しくは非マルウェアプロセスのいずれであるかをまだ決定されておらず、既知のマルウェアプロセスに関係付けられた特徴コードに一致せず、及び／又はホワイトリストに含まれるプロセスに関係付けられた特徴コードに一致している。

【００２０】

２０４では、プロセスの起動の完了を受けて、プロセスに関係付けられたベースアドレスが決定される。プロセスが起動を終了させた後に、プロセスに関係付けられたベースアドレスが決定される。様々な実施形態において、「ベースアドレス」は、プロセスに関係付けられたメモリブロックの先頭のメモリアドレスを言う。ベースアドレスは、そこから命令が読み出されて実行される、プロセスの先頭のメモリブロックを指している。

【００２１】

一般に、プロセスが機器（例えば、コンピュータ）において起動されるときは、ディスクに保存されている対応するプログラムにしたがって、先ず、ディスク画像が生成される必要がある。ディスク画像は、メモリ（例えば、ランダムアクセスメモリ（ＲＡＭ））内へマッピングされ、それによって、プロセスに関係付けられたメモリ画像が生成される。プロセスが実行されているときは、該実行は、メモリ内へマッピングされたメモリ画像に含まれるプロセスの先頭アドレスから開始する。この先頭アドレスは、プロセスのベースアドレスとして言及される。ベースアドレスの厳密な位置は、オペレーティングシステムに依存する。例えば、Windows（登録商標）オペレーティングシステムにおいて、もし、動的アドレス機能（例えば、アドレス空間配置の無作為化、即ち略称ＡＳＬＲ）がアクティブにされないならば、特定のプロセスのベースアドレスは、特定のアドレス（例えば、０ｘ４０００００００）に固定されるのが一般的である。しかしながら、ＡＳＬＲ機能がアクティブにされるときは、プロセスのベースアドレスは、メモリ内において動的に移動されてよく、したがって、特定のアドレスに固定されない（例えば、ＡＳＬＲがアクティブにされると、プロセスのベースアドレスは、必ずしも常に０ｘ４０００００００であるとは限らない）。

【００２２】

インジェクション型トロイの木馬プロセスが正常プロセスを起動させるときに、前者は、後者のプロセスのメモリ画像の生成を、それが完全に行われる前に休止させ、書き込みを許可しているメモリ内のメモリブロックに自身の悪性コードを書き込む。もし、プロセスの初期ベースアドレスが、書き込みを許可しない（例えば、読み出し専用許可に関係付けられた）メモリブロックに関係付けられているならば、トロイの木馬プロセスは、悪性コードを書き込むための異なるメモリブロック、即ち書き込みを許可しているメモリブロック（例えば、書き込み専用の、又は読み出し及び書き込み許容のメモリブロック）を探す。一部の実施形態では、プロセスの起動が停止されている間に、トロイの木馬プロセスは、トロイの木馬が悪性コードを書き込んだメモリブロックのアドレスを、プロセスに対応する拡張指示ポインタ（ＥＩＰ）情報に関係付けられた戻りアドレスとして設定する。一部の実施形態では、プロセスに対応する戻りアドレス（ＥＩＰ）情報は、次いで、プロセスの新しいベースアドレスとして記録される。次いで、インジェクション型トロイの木馬プロセスは、新しいベースアドレス、即ちトロイの木馬プロセスによって書き込まれた悪性コードに関係付けられたアドレスから、プロセスの起動を再開させる。このようにして、プロセスの初期ベースアドレスは、インジェクション型トロイの木馬プロセスによって、トロイの木馬が悪性コードを書き込んだメモリブロックの先頭アドレスに変更されている。もし、プロセスが実行されると、該プロセスは、初期ベースアドレスに関係付けられたメモリブロックに含まれていた初期機能を実行するのではなく、トロイの木馬プロセスによって戻された変更後のベースアドレスに関係付けられたメモリブロックに含まれる悪性コードに対応する機能を実行する。

【００２３】

一部の実施形態では、プロセスのベースアドレスは、機器のオペレーティングシステムによって記録される。したがって、プロセスのベースアドレスは、オペレーティングシステムから決定されて、対応するメモリブロックを見つけるために使用されてよい。

【００２４】

２０６では、ベースアドレスに関係付けられたメモリブロックの許可が決定される。メモリブロックの許可は、任意の既知の技術を使用して決定されてよい。様々な実施形態において、メモリブロックの許可は、読み出し専用、書き込み専用、又は読み出し及び書き込み許容であってよい。

【００２５】

２０８では、決定された許可に少なくとも部分的に基づいて、プロセスがマルウェアプロセスに関係付けられている可能性があるかどうかが決定される。様々な実施形態において、プロセスのベースアドレスに関係付けられたメモリブロックの許可が読み出し専用である場合は、プロセスはマルウェアプロセスに関係付けられていないと決定される。もし、プロセスがマルウェアプロセスに関係付けられていないならば、これ以上の更なる行為はとられない、及び／又はプロセスは実行を許可される。様々な実施形態において、プロセスのベースアドレスに関係付けられたメモリブロックの許可が読み出し専用ではない何かである（例えば、メモリブロックの許可が書き込みを許可している）場合は、プロセスはマルウェアプロセスに関係付けられている可能性があると決定される。一部の実施形態では、具体的なマルウェアプロセスは、トロイの木馬プロセスである。一部の実施形態では、プロセスのベースアドレスに関係付けられたメモリブロックの許可が、読み出し専用ではない何かである場合に、プロセスは、それがマルウェアプロセス（例えば、トロイの木馬プロセス）に関係付けられているかどうかを決定するために、更なるテストを経る。

【００２６】

プロセスのベースアドレスに関係付けられたメモリブロックの許可は、通常は読み出し専用である。インジェクション型トロイの木馬は、メモリブロックに悪性コードを書き込む必要があるので、悪性コードを書き込むための許可を有するメモリブロックを探し、プロセスに関係付けられたベースアドレスを、読み出し専用ではない許可を有するメモリブロックに関係付けられるように変更する。こうして、変更後のベースアドレスは、書き込みを許可するメモリブロックを指すことになる。したがって、もし、メモリブロックの許

可が読み出し専用であるならば、プロセスのベースアドレスは、トロイの木馬プロセスによって変更されていないと想定される。しかしながら、もし、メモリブロックの許可が書き込みを許可しているならば、プロセスのベースアドレスは、トロイの木馬プロセスによって変更されていると想定される。プロセスは、トロイの木馬プロセスに関係付けられている可能性があると決定された場合は、更なる実行からブロックされるだろう、及び／又は機器上で実行されているトロイの木馬プロセスの存在についての警告がユーザに対して提示されるだろう。更に、プロセスがトロイの木馬プロセスに関係付けられていると決定された場合は、その事象からログが生成されて、将来の照会／分析に備えて保存されてよい。

【００２７】

一部の実施形態では、読み出し専用ではない許可に関係付けられたメモリブロック内に位置するベースアドレスを有する特殊プロセスがある。特殊プロセスは、そのベースアドレスが読み出し専用ではない許可に初期から関係付けられているものの、必ずしもトロイの木馬プロセスに関係付けられているとは限らない。一部の実施形態では、特殊プロセスは、通常プロセスのメモリ画像に含まれるポータブル実行可能ファイルヘッダ（ＰＥヘッダ）コードとは異なるＰＥヘッダに基づいて、通常プロセスから区別されるだろう。プロセスのＰＥヘッダは、プロセスに関係付けられたメモリ画像内で見つけられる。したがって、プロセスがトロイの木馬プロセスに関係付けられていると決定される偽陽性率を下げるためには、もし、プロセスのベースアドレスに関係付けられたメモリブロックに関係付けられた許可が読み出し専用ではない何かであると決定されたならば、そのプロセスがトロイの木馬プロセスに関係付けられている可能性があると決定する前に、そのプロセスのメモリ画像に含まれるＰＥヘッダコードが通常プロセス（非特殊プロセス）に関係付けられた指定のコードに一致するかどうかもチェックされる。例えば、読み出し専用ではない許可を有するメモリブロックに関係付けられたベースアドレスを持つプロセスがトロイの木馬プロセスに関係付けられたプロセスであるかどうかを決定するために、通常プロセスのメモリ画像に含まれるＰＥヘッダコードに対応する指定のコードを挙げた所定のリストが使用される。したがって、この追加のチェックを実施することによって、ベースアドレスに関係付けられたメモリブロックの許可が読み出し専用はない何かであるがそのＰＥヘッダコードは指定のコードに一致しないプロセスが、トロイの木馬プロセスに関係付けられた通常プロセスではなく、特殊プロセスであると見なされる。

【００２８】

図３は、マルウェアプロセスを検出するためのプロセスの一実施形態を示したフローチャートである。一部の実施形態では、プロセス３００は、図１の機器１０２において実行に移される。一部の実施形態では、図２のプロセス２００は、プロセス３００を使用して実現される。

【００２９】

３０２では、プロセスの起動が監視される。

【００３０】

３０４では、プロセスの起動の完了を受けて、プロセスに関係付けられたベースアドレスが決定される。

【００３１】

３０６では、ベースアドレスに関係付けられたメモリブロックが読み出し専用許可に関係付けられているかどうかが決定される。メモリブロックが読み出し専用許可に関係付けられている場合は、制御は３０８に移される。メモリブロックが読み出し専用ではない許可に関係付けられている場合は、制御は３１０に移される。

【００３２】

３０８では、プロセスはマルウェアプロセスに関係付けられていないと決定される。一部の実施形態では、これ以上の行為はなされない。

【００３３】

３１０では、プロセスのメモリ画像に含まれるＰＥヘッダコードが指定のコードに一致

するかどうかが決定される。一部の実施形態では、ヘッダコードは、通常（非特殊）プロセスの指定のコードを挙げた所定のリストに突き合わされる。ＰＥヘッダコードが指定のコードに一致する場合は、制御は３１２に移される。ＰＥヘッダコードが指定のコードに一致しない場合は、制御は３０８に移される。

【００３４】

３１２では、プロセスはマルウェアプロセスに関係付けられている可能性があると決定される。例えば、マルウェアプロセスは、トロイの木馬プロセスである。プロセスは、対応するメモリブロックが読み出し専用ではない許可に関係付けられたベースアドレスを有し、これは、トロイの木馬プロセスがプロセスの初期ベースアドレスを、トロイの木馬プロセスが悪性コードを書き込むことができたメモリブロックに関係付けられるように変更した可能性が高いことを意味し、また、プロセスは、特殊プロセスであると決定されていないので、プロセスは、トロイの木馬プロセスに関係付けられている可能性があると決定される。一部の実施形態では、プロセスのベースアドレスに関係付けられたメモリブロックの許可が読み出し専用ではない何かである場合に、プロセスは、それがトロイの木馬プロセスに関係付けられているかどうかを決定するために更なるテストを経る。

【００３５】

３１４では、ユーザインターフェースにおいて警告メッセージが提示される。一部の実施形態では、トロイの木馬プロセスに関係付けられている可能性があるプロセスの検出に関する警告メッセージをユーザに対して提示することに加えて、プロセスは、更なる実行からブロックもされる。

【００３６】

図４は、マルウェアプロセスを検出するためのシステムの一実施形態を示した図である。この例では、システム４００は、監視モジュール４０２と、評価モジュール４０４と、処理モジュール４０６とを含む。

【００３７】

モジュールは、１つ以上の汎用プロセッサ上で実行されるソフトウェアコンポーネントとして、又は本発明の実施形態で説明される方法を（パソコン、サーバ、ネットワーク装置などの）計算機器に実行させるための幾つかの命令を含み尚且つ（光ディスク、フラッシュ記憶装置、モバイルハードディスクなどの）不揮発性の記憶媒体に記憶させることができるソフトウェア製品の形で具現化することができる要素であるように設計されたプログラム可能論理装置及び／若しくは特殊用途向け集積回路などのハードウェアとして、実装することができる。モジュールは、１つの機器に実装されてよい、又は複数の機器に分散されてよい。

【００３８】

監視モジュール４０２は、起動されたプロセスを監視するように、及びプロセスの起動が完了したときにプロセスのベースアドレスに関係付けられたメモリブロックを決定するように構成される。例えば、プロセスのベースアドレスは、オペレーティングシステムによって記録される。

【００３９】

評価モジュール４０４は、監視モジュール４０２によって決定されたメモリブロックの許可が読み出し専用であるかどうかを評価するように構成される。

【００４０】

処理モジュール４０６は、評価モジュール４０４がメモリブロックの許可が読み出し専用であると決定した場合に、そのプロセスはトロイの木馬プロセスに関係付けられていないと決定するように構成される。処理モジュール４０６は、評価モジュール４０４がメモリブロックの許可が読み出し専用ではない何かであると決定した場合に、そのプロセスをトロイの木馬プロセスに関係付けられている可能性があると決定するように構成される。一部の実施形態では、処理モジュール４０６は、更に、プロセスがトロイの木馬プロセスに関係付けられている可能性があると決定した場合に、プロセスを更なる実行からブロックするように構成される。

【００４１】
一部の実施形態では、監視モジュール４０２は、更に、起動されたプロセスのベースアドレスを記録するように、及び該記録されたベースアドレスを使用して、ベースアドレスに関係付けられたメモリブロックを見つけるように構成される。
【００４２】
一部の実施形態では、監視モジュール４０２は、更に、プロセスの起動の停止中に戻りアドレスＥＩＰ情報に含まれるアドレスを、そのプロセスのベースアドレスとして記録するように構成される。
【００４３】
一部の実施形態では、処理モジュール４０６は、更に、記録されたプロセスのベースアドレスに関係付けられたメモリブロックの許可が読み出し専用ではない何かであると決定した場合に、プロセスのメモリ画像に含まれるＰＥヘッダコードが通常プロセスに対応する指定のコードに一致するかどうかを決定するように構成される。プロセスのメモリ画像に含まれるＰＥヘッダコードが通常プロセスに対応する指定のコードに一致する場合は、処理モジュール４０６は、そのプロセスはトロイの木馬プロセスに関係付けられている可能性があると決定するように構成される。しかしながら、プロセスのメモリ画像に含まれるＰＥヘッダコードが通常プロセスに対応する指定のコードに一致しない場合は、処理モジュール４０６は、そのプロセスは（例えば、そのプロセスはＰＥヘッダコードが通常プロセスのそれに一致しないゆえに実際は特殊プロセスであるだろうゆえに、）トロイの木馬プロセスに関係付けられていないと決定するように構成される。
【００４４】
処理モジュール４０６は、更に、プロセスがトロイの木馬プロセスに関係付けられている可能性があると決定した場合に、トロイの木馬プロセスの検出に関係付けられた警告メッセージをユーザインターフェースにおいて提示するために生成するように構成される。
【００４５】
当業者ならば、本出願を、本発明の趣旨及び範囲から逸脱することなく変更する及び多様化することができる。したがって、もし、本出願のこれらの変更形態及び多様化形態が、本出願の特許請求の範囲及びそれらの等価技術の範囲内であるならば、本出願は、これらの変更形態及び多様化形態もまた、その範囲内に含むことを意図する。当業者ならば、本出願の実施形態が、方法、システム、又はコンピュータソフトウェア製品として提供可能であることがわかるはずである。したがって、本出願は、完全にハードウェアで構成される実施形態、完全にソフトウェアで構成される実施形態、及びソフトウェアとハードウェアとを組み合わせた実施形態の形態をとることができる。また、本出願は、コンピュータ動作可能なプログラムコードを含む１つ以上のコンピュータ動作可能な記憶媒体（磁気ディスク記憶装置、ＣＤ－ＲＯＭ、及び光記憶装置を含むがこれらに限定はされない）に実装されたコンピュータプログラム製品の形態をとることができる。
【００４６】
以上の実施形態は、理解を明瞭にする目的で幾らか詳細に説明されているが、本発明は、与えられた詳細に限定されない。本発明を実現するには、多くの代替的手法がある。開示される実施形態は、例示的であり、非限定的である。
本発明は、たとえば、以下のような態様で実現することもできる。

適用例１：
マルウェアプロセスを検出するためのシステムであって、
１つ以上のプロセッサと、
前記１つ以上のプロセッサに結合され、前記１つ以上のプロセッサに命令を提供するように構成された１つ以上のメモリと、
を備え、
前記１つ以上のプロセッサは、
プロセスの起動を監視し、

前記プロセスの前記起動の完了を受けて、前記プロセスに関係付けられたベースアドレスを決定し、
前記ベースアドレスに関係付けられたメモリブロックの許可を決定し、及び
前記決定された許可に少なくとも部分的に基づいて、前記プロセスがマルウェアプロセスに関係付けられている可能性があるかどうかを決定する、ように構成される、システム。

適用例２：
適用例１のシステムであって、
前記ベースアドレスは、前記プロセスに対応する拡張指示ポインタ（ＥＩＰ）情報に関係付けられた戻りアドレスに少なくとも部分的に基づいて決定される、システム。

適用例３：
適用例１のシステムであって、
前記ベースアドレスは、オペレーティングシステムによって記録される、システム。

適用例４：
適用例１のシステムであって、
前記許可が書き込みを許可していると決定された場合に、前記１つ以上のプロセッサは、更に、前記プロセスは前記マルウェアプロセスに関係付けられている可能性があると決定するように構成される、システム。

適用例５：
適用例４のシステムであって、
前記１つ以上のプロセッサは、更に、前記マルウェアプロセスに関係付けられた警告メッセージを、ユーザインターフェースにおいて提示するように構成される、システム。

適用例６：
適用例４のシステムであって、
前記１つ以上のプロセッサは、更に、前記プロセスの更なる実行をブロックするように構成される、システム。

適用例７：
適用例１のシステムであって、
前記許可が読み出し専用であると決定された場合に、前記１つ以上のプロセッサは、更に、前記プロセスは前記マルウェアプロセスに関係付けられていないと決定するように構成される、システム。

適用例８：
適用例１のシステムであって、
前記許可が書き込みを許可していると決定された場合に、前記１つ以上のプロセッサは、更に、前記プロセスに関係付けられたメモリ画像に含まれるポータブル実行可能（ＰＥ）ヘッダコードが指定のコードに一致するかどうかを決定するように構成される、システム。

適用例９：
適用例８のシステムであって、
前記プロセスに関係付けられた前記ＰＥヘッダコードが前記指定のコードに一致する場合に、前記１つ以上のプロセッサは、更に、前記プロセスは前記マルウェアプロセスに関係付けられている可能性があると決定するように構成される、システム。

適用例１０：
適用例８のシステムであって、
前記プロセスに関係付けられた前記ＰＥヘッダコードが前記指定のコードに一致しない場合に、前記１つ以上のプロセッサは、更に、前記プロセスは前記マルウェアプロセスに関係付けられていないと決定するように構成される、システム。

適用例１１：
マルウェアプロセスを検出するための方法であって、
プロセスの起動を監視することと、
前記プロセスの前記起動の完了を受けて、１つ以上のプロセッサを使用して、前記プロセスに関係付けられたベースアドレスを決定することと、
前記ベースアドレスに関係付けられたメモリブロックの許可を決定することと、
前記決定された許可に少なくとも部分的に基づいて、前記プロセスがマルウェアプロセスに関係付けられている可能性があるかどうかを決定することと、
を備える方法。

適用例１２：
適用例１１の方法であって、
前記ベースアドレスは、前記プロセスに対応する拡張指示ポインタ（ＥＩＰ）情報に関係付けられた戻りアドレスに少なくとも部分的に基づいて、決定される、方法。

適用例１３：
適用例１１の方法であって、更に、
前記許可が書き込みを許可していると決定された場合に、前記プロセスは前記マルウェアプロセスに関係付けられている可能性があると決定することを備える方法。

適用例１４：
適用例１３の方法であって、更に、
前記マルウェアプロセスに関係付けられた警告メッセージを、ユーザインターフェースにおいて提示することを備える方法。

適用例１５：
適用例１３の方法であって、更に、
前記プロセスの更なる実行をブロックすることを備える方法。

適用例１６：
適用例１１の方法であって、更に、
前記許可が読み出し専用であると決定された場合に、前記プロセスは前記マルウェアプロセスに関係付けられていないと決定することを備える方法。

適用例１７：
適用例１１の方法であって、更に、
前記許可が書き込みを許可していると決定された場合に、前記プロセスに関係付けられたメモリ画像に含まれるポータブル実行可能（ＰＥ）ヘッダコードが、指定のコードに一致するかどうかを決定することを備える方法。

適用例１８：
適用例１７の方法であって、更に、
前記プロセスに関係付けられた前記ＰＥヘッダコードが前記指定のコードに一致する場

合に、前記プロセスは前記マルウェアプロセスに関係付けられている可能性があると決定することを備える方法。

適用例１９：
適用例１７の方法であって、更に、
前記プロセスに関係付けられた前記ＰＥヘッダコードが前記指定のコードに一致しない場合に、前記プロセスは前記マルウェアプロセスに関係付けられていないと決定することを備える方法。

適用例２０：
マルウェアプロセスを検出するためのコンピュータプログラム製品であって、非一時的なコンピュータ読み取り可能記憶媒体に実装され、
プロセスの起動を監視するためのコンピュータ命令と、
前記プロセスの前記起動の完了を受けて、前記プロセスに関係付けられたベースアドレスを決定するためのコンピュータ命令と、
前記ベースアドレスに関係付けられたメモリブロックの許可を決定するためのコンピュータ命令と、
前記決定された許可に少なくとも部分的に基づいて、前記プロセスがマルウェアプロセスに関係付けられている可能性があるかどうかを決定するためのコンピュータ命令と、
を備えるコンピュータプログラム製品。

【図１】

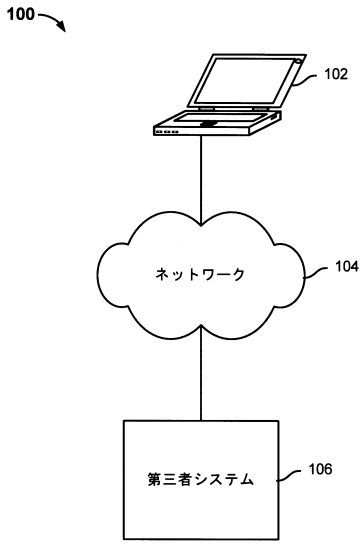

FIG. 1

【図２】

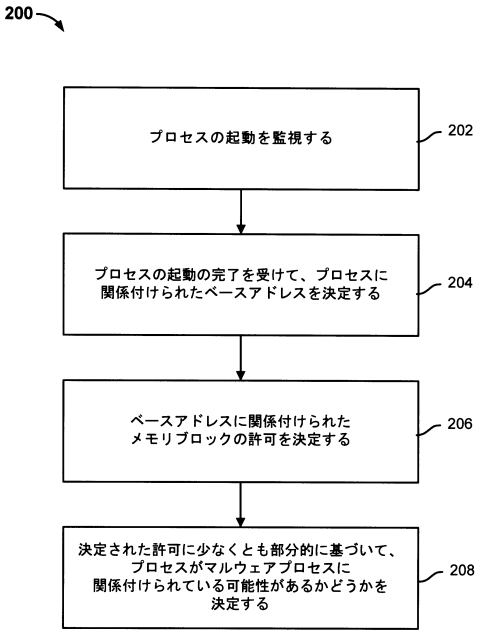

FIG. 2

【図３】

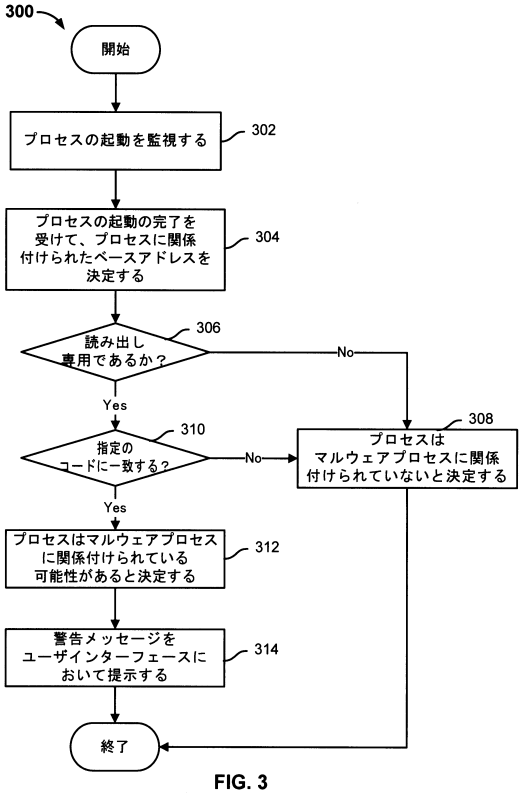

FIG. 3

【図４】

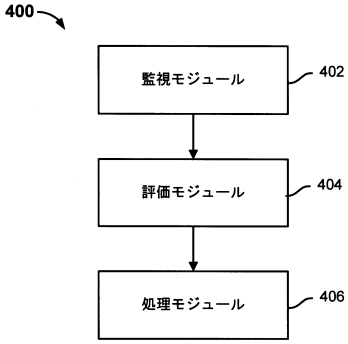

FIG. 4

フロントページの続き

(72)発明者　ニエ・ワンチュエン
中華人民共和国　ハンチョウ，ワーナー・ロード，ザ・ウエスト・レイク・インターナショナル・プラザ・オブ・エス　アンド　ティー，ビルディング　エー，１０階，ナンバー３９１，アリババ・グループ・リーガル・デパートメント内

審査官　中里　裕正

(56)参考文献　特開２０１１－２３３１２６（ＪＰ，Ａ）
米国特許出願公開第２０１０／００４３０７２（ＵＳ，Ａ１）
国際公開第２０１１／０７６４６４（WO，Ａ１）
MICHAEL SIKORSKI, PRACTICAL MALWARE ANALYSIS, [ONLINE], ２０１２年　2月２９日, P253-259, ＵＲＬ, http://www.safaribooksonline.com

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５６
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ　Ｘｐｌｏｒｅ