(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5976020号
(P5976020)
(45)発行日　平成28年8月23日(2016.8.23)　(24)登録日　平成28年7月29日(2016.7.29)

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

請求項の数 15　(全 26 頁)

(21)出願番号	特願2013-558142 (P2013-558142)
(86)(22)出願日	平成24年3月14日 (2012.3.14)
(65)公表番号	特表2014-508363 (P2014-508363A)
(43)公表日	平成26年4月3日 (2014.4.3)
(86)国際出願番号	PCT/US2012/029101
(87)国際公開番号	WO2012/125744
(87)国際公開日	平成24年9月20日 (2012.9.20)
審査請求日	平成26年11月18日 (2014.11.18)
(31)優先権主張番号	13/048,380
(32)優先日	平成23年3月15日 (2011.3.15)
(33)優先権主張国	米国(US)

(73)特許権者　501113353
シマンテック　コーポレーション
Ｓｙｍａｎｔｅｃ　Ｃｏｒｐｏｒａｔｉｏｎ
アメリカ合衆国，カリフォルニア州　９４０４３，マウンテン　ビュー，エリス　ストリート　３５０
(74)代理人　100147485
弁理士　杉村　憲司
(74)代理人　100134119
弁理士　奥町　哲行
(72)発明者　ソーベル・ウィリアム　イー
アメリカ合衆国　カリフォルニア州　９１９３５　ジャムール　アルタローマドライブ　３５９２

最終頁に続く

(54)【発明の名称】アンチマルウェアメタデータのルックアップを行うためのシステム及び方法

(57)【特許請求の範囲】
【請求項１】
サーバ側のアンチマルウェアメタデータのルックアップを行うためのコンピュータ実施方法であって、前記方法の少なくとも一部は、少なくとも１つのプロセッサを含むコンピュータデバイスによって行われ、
第１のコンピュータシステム上でクライアント側の複数の実行可能オブジェクトを識別するステップであって、前記クライアント側の複数の実行可能オブジェクトには実行前にマルウェアのスキャンが行われ、マルウェアのスキャンに使用されるサーバ側のアンチマルウェアメタデータの待機は、前記クライアント側の複数の実行可能オブジェクトへのアクセスの待ち時間をもたらすステップと、
前記クライアント側の複数の実行可能オブジェクト内のクライアント側の各実行可能オブジェクトに関して、前記クライアント側の実行可能オブジェクトの実行の危急性を評価することによって、前記サーバ側のアンチマルウェアメタデータがいつ必要とされるかを予測するステップと、
前記第１のコンピュータシステムから離れた第２のコンピュータシステム上で、前記クライアント側の複数の実行可能オブジェクト内のクライアント側の各実行可能オブジェクトに対応する前記サーバ側のアンチマルウェアメタデータを識別するステップと、
前記評価に基づいて、前記クライアント側の複数の実行可能オブジェクトに対応する前記サーバ側のアンチマルウェアメタデータの検索順序の優先順位を決定するステップと、
前記検索順序に基づいて、前記第２のコンピュータシステムから、前記クライアント側

の複数の実行可能オブジェクト内の対応するクライアント側の実行可能オブジェクトを起動する前に、前記サーバ側のアンチマルウェアメタデータを検索するステップと、
対応する前記クライアント側の実行可能オブジェクトを起動する際に利用できるように、検索された前記アンチマルウェアメタデータをクライアント側のアンチマルウェアシグネチャキャッシュ中に保存し、前記サーバ側のアンチマルウェアメタデータの検索に起因するアクセスの待ち時間を減少させるステップと、
を含む方法。
【請求項２】
前記クライアント側の複数の実行可能オブジェクトを識別するステップは、システム構成情報を用いて、自動起動されるクライアント側の実行可能オブジェクトセットを識別するステップを含み、前記システム構成情報は、前記自動起動されるクライアント側の実行可能オブジェクトセット中の自動起動されるクライアント側の実行可能オブジェクトの各々がいつ起動される可能性が高いかを示す、請求項１に記載のコンピュータ実施方法。
【請求項３】
前記自動起動されるクライアント側の実行可能オブジェクトセットを識別するステップは、オペレーティングシステムのブート処理中に起動される少なくとも１つのクライアント側の実行可能オブジェクトを識別するステップを含む、請求項２に記載のコンピュータ実施方法。
【請求項４】
前記自動起動されるクライアント側の実行可能オブジェクトセットを識別するステップは、
サービスと、
ドライバと、
ログイン時に実行されるように構成されたクライアント側の実行可能オブジェクトと、
タスクスケジューラに従って実行されるように構成されたクライアント側の実行可能オブジェクトと、
の内の少なくとも１つを識別するステップを含む、請求項２に記載のコンピュータ実施方法。
【請求項５】
前記クライアント側の複数の実行可能オブジェクトを識別するステップは、ユーザによって起動される可能性の高いクライアント側の実行可能オブジェクトセットを識別するステップを含む、請求項１に記載のコンピュータ実施方法。
【請求項６】
前記ユーザによって起動される可能性の高い前記クライアント側の実行可能オブジェクトセットを識別するステップは、
前記ユーザが所有するデスクトップ上の実行可能オブジェクトと、
前記ユーザが所有するダウンロードフォルダ内の実行可能オブジェクトと、
の内の少なくとも１つを識別するステップを含む、請求項５に記載のコンピュータ実施方法。
【請求項７】
前記クライアント側の複数の実行可能オブジェクトを識別するステップは、
前記クライアント側の複数の実行可能オブジェクト内の第１のクライアント側の実行可能オブジェクトを識別するステップと、
前記第１のクライアント側の実行可能オブジェクトが第２のクライアント側の実行可能オブジェクトに依存することを示す依存情報を識別するステップと、
前記クライアント側の複数の実行可能オブジェクト内に前記第２のクライアント側の実行可能オブジェクトを包含させるステップと、
を含む、請求項１に記載のコンピュータ実施方法。
【請求項８】
前記クライアント側の複数の実行可能オブジェクトを識別するステップは、

前記クライアント側の複数の実行可能オブジェクト内の第１のクライアント側の実行可能オブジェクトを識別するステップと、
前記第１のクライアント側の実行可能オブジェクトに対する拡張として動作する第２のクライアント側の実行可能オブジェクトを識別するステップと、
を含む、請求項１に記載のコンピュータ実施方法。
【請求項９】
前記クライアント側の実行可能オブジェクトの実行の前記危急性を評価するステップは、
前記クライアント側の実行可能オブジェクトの作成時間を識別するステップと、
前記作成時間と現在の時間との距離に伴って、前記クライアント側の実行可能オブジェクトの危急の実行の予想を単調に増大させるステップと、
を含む、請求項１に記載のコンピュータ実施方法。
【請求項１０】
前記サーバ側のアンチマルウェアメタデータを検索するステップは、リモートストレージシステムからアンチマルウェアシグネチャを検索するステップを含む、請求項１に記載のコンピュータ実施方法。
【請求項１１】
サーバ側のアンチマルウェアメタデータのルックアップを行うためのシステムであって、
識別モジュールであって、
第１のコンピュータシステム上でクライアント側の複数の実行可能オブジェクトを識別するようにプログラムされ、ここで、前記クライアント側の複数の実行可能オブジェクトには実行前にマルウェアのスキャンが行われ、マルウェアのスキャンに使用されるサーバ側のアンチマルウェアメタデータの待機は、前記クライアント側の複数の実行可能オブジェクトへのアクセスの待ち時間をもたらすものであり、
前記第１のコンピュータシステムから離れた第２のコンピュータシステム上で、前記クライアント側の複数の実行可能オブジェクト内のクライアント側の各実行可能オブジェクトに対応する前記サーバ側のアンチマルウェアメタデータを識別するようにプログラムされた識別モジュールと、
前記クライアント側の複数の実行可能オブジェクト内のクライアント側の各実行可能オブジェクトに関して、前記クライアント側の実行可能オブジェクトの実行の危急性を評価することによって、前記サーバ側のアンチマルウェアメタデータがいつ必要とされるかを予測するようにプログラムされた予測モジュールと、
前記評価に基づいて、前記クライアント側の複数の実行可能オブジェクトに対応する前記サーバ側のアンチマルウェアメタデータの検索順序の優先順位を決定するようにプログラムされた優先順位決定モジュールと、
前記検索順序に基づいて、前記第２のコンピュータシステムから、前記クライアント側の複数の実行可能オブジェクト内の対応するクライアント側の実行可能オブジェクトを起動する前に、少なくとも１つのサーバ側のアンチマルウェアメタデータを検索するようにプログラムされた検索モジュールと、
対応する前記クライアント側の実行可能オブジェクトを起動する際に利用できるように、検索された前記アンチマルウェアメタデータをクライアント側のアンチマルウェアシグネチャキャッシュ中に保存し、前記サーバ側のアンチマルウェアメタデータの検索に起因するアクセスの待ち時間を減少させるようにプログラムされた保存モジュールと、
前記識別モジュール、前記予測モジュール、前記優先順位決定モジュール、及び前記検索モジュールを実行するように構成された少なくとも１つのハードウェアプロセッサと、
を含むシステム。
【請求項１２】
前記識別モジュールは、自動起動されるクライアント側の実行可能オブジェクトセットを識別するためのシステム構成情報を用いて、前記クライアント側の複数の実行可能オブ

ジェクトを識別するようにプログラムされ、前記システム構成情報は、前記自動起動されるクライアント側の実行可能オブジェクトセット中の自動起動されるクライアント側の実行可能オブジェクトの各々がいつ起動される可能性が高いかを示す、請求項１１に記載のシステム。

【請求項１３】

前記識別モジュールは、

サービスと、

ドライバと、

ログイン時に実行されるように構成されたクライアント側の実行可能オブジェクトと、

タスクスケジューラに従って実行されるように構成されたクライアント側の実行可能オブジェクトと、

の内の少なくとも１つを識別することにより、前記自動起動されるクライアント側の実行可能オブジェクトセットを識別するようにプログラムされる、請求項１２に記載のシステム。

【請求項１４】

前記識別モジュールは、ユーザによって起動される可能性の高いクライアント側の実行可能オブジェクトセットを識別することにより、前記クライアント側の複数の実行可能オブジェクトを識別するようにプログラムされる、請求項１１に記載のシステム。

【請求項１５】

コンピュータデバイスの少なくとも１つのプロセッサによって実行されると、前記コンピュータデバイスに、

第１のコンピュータシステム上におけるクライアント側の複数の実行可能オブジェクトの識別であって、前記クライアント側の複数の実行可能オブジェクトには実行前にマルウェアのスキャンが行われ、マルウェアのスキャンに使用されるサーバ側のアンチマルウェアメタデータの待機は、前記クライアント側の複数の実行可能オブジェクトへのアクセスの待ち時間をもたらす識別と、

前記クライアント側の複数の実行可能オブジェクト内のクライアント側の各実行可能オブジェクトに関して、前記クライアント側の実行可能オブジェクトの実行の危急性の評価をすることによる、前記サーバ側のアンチマルウェアメタデータがいつ必要とされるかの予測と、

前記第１のコンピュータシステムから離れた第２のコンピュータシステム上における、前記クライアント側の複数の実行可能オブジェクト内のクライアント側の各実行可能オブジェクトに対応する前記サーバ側のアンチマルウェアメタデータの識別と、

前記評価に基づく、前記クライアント側の複数の実行可能オブジェクトに対応する前記サーバ側のアンチマルウェアメタデータの検索順序の優先順位の決定と、

前記検索順序に基づく、前記第２のコンピュータシステムから、前記クライアント側の複数の実行可能オブジェクト内の対応するクライアント側の実行可能オブジェクトを起動する前における、前記サーバ側のアンチマルウェアメタデータの検索と、

対応する前記クライアント側の実行可能オブジェクトを起動する際に利用できるように、検索された前記アンチマルウェアメタデータをクライアント側のアンチマルウェアシグネチャキャッシュ中に保存させ、前記サーバ側のアンチマルウェアメタデータの検索に起因するアクセスの待ち時間の減少と、

を行わせる１つまたは複数のコンピュータ実行可能命令を含む、コンピュータ可読ストレージ媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本開示は、概して、アンチマルウェアメタデータのルックアップを行うためのシステム及び方法に関する。

【背景技術】

【０００２】
アンチウイルス及びアンチスパイウェアソリューションは、一般的に、従来のスキャンに基づく技術を用いて、エンドポイントデバイスに対するウイルス、ワーム、トロイの木馬、スパイウェア、及び他のマルウェアを識別する。一般的なアンチウイルス及びアンチスパイウェアソリューションは、既知の脅威の特徴（例えばアンチマルウェアシグネチャ）に関してファイルをチェックすることにより、これらの脅威を検出することができる。脅威が検出されるとすぐに、一般的にはそれを削除または隔離することによって、ソリューションがそれを修正することができる。
【０００３】
マルウェアの脅威の数が増加するにつれて、これらの脅威を識別するシグネチャデータベースの大きさも増加する。しかしながら、大型のアンチマルウェアシグネチャデータベースは、ディスクフットプリントの増加により、クライアントデバイスにとって望ましくない場合がある。サーバ側のルックアップは、アンチマルウェアシグネチャの保存に関連する問題を軽減し得るが、アプリケーションの起動の許可前にアンチマルウェアシグネチャを待つ間、アプリケーションへのアクセスが遅れる場合がある。従って、本開示は、アンチマルウェアシグネチャのルックアップを行うためのさらなる改良されたシステム及び方法の必要性を見出した。
【発明の概要】
【課題を解決するための手段】
【０００４】
以下により詳細に説明するように、本開示は、概して、アンチマルウェアメタデータのルックアップを行うためのシステム及び方法に関する。本明細書に記載のシステム及び方法は、アンチマルウェアメタデータがいつ必要とされるかを予測し、この予測に基づいて、アンチマルウェアメタデータのルックアップの優先順位を決定し得る。例えば、ある方法は、実行前にマルウェアのスキャンが行われる複数の実行可能オブジェクトを識別するステップを包含し得る。この方法は、複数の実行可能オブジェクト内の各実行可能オブジェクトに関して、実行可能オブジェクトの実行の危急性を評価するステップも包含し得る。この方法は、評価に基づいて、複数の実行可能オブジェクトに対応するアンチマルウェアメタデータの検索順序の優先順位を決定するステップと、検索順序に基づいて、複数の実行可能オブジェクト内の実行可能オブジェクトに対応するアンチマルウェアメタデータを検索するステップとをさらに包含し得る。
【０００５】
本明細書に記載のシステムは、様々なソースの何れからでも複数の実行可能オブジェクトを識別することができる。例えば、これらのシステムは、システム構成情報を用いて、自動起動される実行可能オブジェクトセットを識別することができる。システム構成情報は、自動起動される実行可能オブジェクトセット中の自動起動される実行可能オブジェクトの各々がいつ起動される可能性が高いかを示し得る。この例では、自動起動される実行可能オブジェクトセットを識別するステップは、オペレーティングシステムのブート処理中に起動されるように構成された少なくとも１つの実行可能オブジェクトを識別するステップを包含し得る。追加的または代替的に、自動起動される実行可能オブジェクトセットを識別するステップは、サービス、ドライバ、ログイン時に実行されるように構成された実行可能オブジェクト、及び／またはタスクスケジューラに従って実行されるように構成された実行可能オブジェクトを識別するステップを包含し得る。
【０００６】
一部の実施例では、複数の実行可能オブジェクトを識別するステップは、ユーザによって起動される可能性の高い実行可能オブジェクトセットを識別するステップを包含し得る。例えば、実行可能オブジェクトセットは、ユーザが所有するデスクトップ上の実行可能オブジェクト及び／またはユーザが所有するダウンロードフォルダ内の実行可能オブジェクトを包含し得る。
【０００７】

本明細書に記載のシステムは、複数の実行可能オブジェクト内の第１の実行可能オブジェクトを識別するステップと、第１の実行可能オブジェクトが第２の実行可能オブジェクトに依存することを示す依存情報を識別するステップと、複数の実行可能オブジェクト内に第２の実行可能オブジェクトを包含させるステップとによっても、複数の実行可能オブジェクトを識別することができる。追加的または代替的に、複数の実行可能オブジェクトを識別するステップは、複数の実行可能オブジェクト内の第１の実行可能オブジェクトを識別するステップと、第１の実行可能オブジェクトに対する拡張として動作する第２の実行可能オブジェクトを識別するステップとを包含し得る。一部の実施例では、複数の実行可能オブジェクトを識別するステップは、実行を目的として起動された実行可能オブジェクト及び／または実行中の実行可能オブジェクトを識別するステップを包含し得る。

【０００８】

実行可能オブジェクトの実行の危急性を評価するステップは、実行可能オブジェクトが識別された状況を調べるステップを包含し得る。一部の実施例では、実行可能オブジェクトの実行の危急性を評価するステップは、実行可能オブジェクトの作成時間を識別するステップ及び作成時間と現在の時間との距離に伴って実行可能オブジェクトの危急の実行の予想を単調に増大させるステップも包含し得る。

【０００９】

検索順序の優先順位を決定するステップは、複数の実行可能オブジェクト内の少なくとも１つの実行可能オブジェクトに関連するアンチマルウェアメタデータを検索するために優先順位決定情報をリモートコンピュータシステムから受信するステップを包含し得る。一部の実施例では、本明細書に記載のシステムは、実行可能オブジェクトの計画された起動前の実行可能オブジェクトのスキャンに間に合うように、アンチマルウェアメタデータを検索することができる。様々な実施例において、本明細書に記載のシステムは、リモートストレージシステムからアンチマルウェアシグネチャを検索することができる。

【００１０】

上記の実施形態の何れかの特徴を、本明細書に記載の一般原理に従って互いに組み合わせて使用することができる。上記及び他の実施形態、特徴、及び利点は、添付の図面及び特許請求の範囲と併せて以下の詳細な説明を読めば、より完全に理解されるであろう。

【００１１】

添付の図面は、複数の例示的な実施形態を図示し、本明細書の一部である。以下の記載と共に、これらの図面は、本開示の様々な原理を明示及び説明する。

【図面の簡単な説明】

【００１２】

【図１】アンチマルウェアメタデータのルックアップを行うためのシステム例のブロック図である。

【図２】アンチマルウェアメタデータのルックアップを行うためのシステム例のブロック図である。

【図３】アンチマルウェアメタデータのルックアップを行うための方法例のフロー図である。

【図４】実行可能ファイルに関する依存性チャート例のブロック図である。

【図５】アンチマルウェアメタデータのルックアップを行うためのシステム例のブロック図である。

【図６】本明細書に記載及び／または図示される実施形態の内の１つまたは複数の実施が可能なコンピュータシステム例のブロック図である。

【図７】本明細書に記載及び／または図示される実施形態の内の１つまたは複数の実施が可能なコンピュータネットワーク例のブロック図である。

【発明を実施するための形態】

【００１３】

図面を通して、同一の参照文字及び記述は、類似するが、必ずしも同一ではない要素を示す。本明細書に記載の例示的な実施形態は、様々な変更形態及び代替形態が可能である

が、具体的な実施形態を図面に例として示しており、本明細書において詳細に説明する。しかしながら、本明細書に記載の例示的な実施形態は、開示される特定の形態に限定されることを意図していない。より正確に言えば、本開示は、添付の請求項の範囲に入る全ての変更形態、均等物、及び代替形態を含める。

【００１４】

以下により詳細に説明するように、本開示は、概して、アンチマルウェアメタデータのルックアップを行うためのシステム及び方法に関する。本明細書に記載のシステム及び方法は、アンチマルウェアメタデータが必要な時を予測し、これらの予測に基づいて、アンチマルウェアメタデータのルックアップの優先順位を決定することができる。アンチマルウェアメタデータのルックアップの優先順位を決定することにより、これらのシステム及び方法は、実行可能ファイルを起動させるユーザによって認識される待ち時間を少なくして、アンチマルウェアシステムが起動前にアンチマルウェアメタデータの検索及び実行可能ファイルのスキャンを行うことを可能にできる。

【００１５】

図１、図２及び図４を参照して、アンチマルウェアメタデータのルックアップを行うためのシステム例の詳細な説明を以下に示す。図３に関連して、対応するコンピュータ実施方法の詳細な説明も示す。実行可能ファイルに関する依存性チャート例の詳細な説明を図４に関連して示す。さらに、図６及び図７にそれぞれ関連して、本明細書に記載の実施形態の内の１つまたは複数の実施が可能なコンピュータシステム及びネットワークアーキテクチャ例の詳細な説明を示す。

【００１６】

図１は、アンチマルウェアメタデータのルックアップを行うためのシステム例１００のブロック図である。この図に図示されるように、システム例１００は、１つまたは複数のタスクを行うための１つまたは複数のモジュール１０２を包含し得る。例えば、以下により詳細に説明するように、システム例１００は、実行前にマルウェアのスキャンが行われる複数の実行可能オブジェクトを識別するようにプログラムされた識別モジュール１０４を包含し得る。システム例１００は、複数の実行可能オブジェクト内の各実行可能オブジェクトに関して、実行可能オブジェクトの実行の危急性を評価するようにプログラムされた予測モジュール１０６も包含し得る。システム例１００は、評価に基づいて、複数の実行可能オブジェクトに対応するアンチマルウェアメタデータの検索順序の優先順位を決定するようにプログラムされた優先順位決定モジュール１０８をさらに包含し得る。

【００１７】

さらに、以下により詳細に示されるように、システム例１００は、検索順序に基づいて、複数の実行可能オブジェクト内の１つの実行可能オブジェクトに対応するアンチマルウェアメタデータを検索するようにプログラムされた検索モジュール１１０を包含し得る。別個の要素として図示されているが、図１のモジュール１０２の内の１つまたは複数は、単一のモジュールまたはアプリケーションの一部でもよい。

【００１８】

特定の実施形態では、図１のモジュール１０２の内の１つまたは複数は、コンピュータデバイスによって実行されると、コンピュータデバイスに１つまたは複数のタスクを行わせることのできる１つまたは複数のソフトウェアアプリケーションまたはプログラムでもよい。例えば、以下により詳しく説明するように、モジュール１０２の内の１つまたは複数は、図２に図示されるデバイス（例えばコンピュータシステム２０２及び／またはアンチマルウェアサーバ２０６）、図６のコンピュータシステム６１０、及び／または図７のネットワークアーキテクチャ例７００の一部等の１つまたは複数のコンピュータデバイス上に保存され、かつ実行されるように構成されたソフトウェアモジュールでもよい。図１のモジュール１０２の内の１つまたは複数は、１つまたは複数のタスクを行うように構成された１つまたは複数の専用コンピュータの全体または一部でもよい。

【００１９】

図１のシステム例１００は、様々な形で配置することができる。例えば、システム例１

００の全体または一部は、図２に図示されるシステム例２００の一部でもよい。図２に示されるように、システム２００は、ネットワーク２０４を介してアンチマルウェアサーバ２０６と通信するコンピュータシステム２０２を包含し得る。ある実施形態では、以下により詳細に説明するように、コンピュータシステム２０２は、識別モジュール１０４、予測モジュール１０６、優先順位決定モジュール１０８、及び検索モジュール１１０を包含し得る。

【００２０】

識別モジュール１０４は、実行前にマルウェアのスキャンが行われる実行可能オブジェクト２１０を識別するようにプログラムされ得る。予測モジュール１０６は、実行可能オブジェクト２１０の各々に関して、実行の危急性を評価するようにプログラムされ得る。優先順位決定モジュール１０８は、評価に基づいて、実行可能オブジェクト２１０に対応するアンチマルウェアメタデータの検索順序２１２の優先順位を決定するようにプログラムされ得る。検索モジュール１１０は、検索順序に基づいて、複数の実行可能オブジェクト内の１つの実行可能オブジェクトに対応するアンチマルウェアメタデータ（例えば、アンチマルウェアサーバ２０６に保存されたアンチマルウェアシグネチャ２１４（１～ｎ）の内の１つまたは複数）を検索するようにプログラムされ得る。

【００２１】

コンピュータシステム２０２は、一般的に、コンピュータ実行可能命令を読み取り可能ないかなる種類または形態のコンピュータデバイスを意味する。コンピュータシステム２０２の例には、ラップトップ、デスクトップ、サーバ、携帯電話、パーソナルデジタルアシスタント（ＰＤＡ）、マルチメディアプレーヤー、埋め込み式システム、これらの内の１つまたは複数の組み合わせ、図６のコンピュータシステム例６１０、または他の任意の適切なコンピュータデバイスが包含されるが、これらに限定されない。

【００２２】

アンチマルウェアサーバ２０６は、一般的に、ルックアップの試みに応答してアンチマルウェアメタデータを任意の提供可能な種類または形態のコンピュータデバイスを意味する。アンチマルウェアサーバ２０６の例には、様々なデータベースサービスの提供及び／または特定のソフトウェアアプリケーションの実行を行うように構成されたアプリケーションサーバ及びデータベースサーバが包含されるが、これらに限定されない。

【００２３】

ネットワーク２０４は、一般的に、通信またはデータ転送を促進可能な媒体またはアーキテクチャを意味する。ネットワーク２０４の例には、イントラネット、広域ネットワーク（ＷＡＮ）、ローカルエリアネットワーク（ＬＡＮ）、パーソナルエリアネットワーク（ＰＡＮ）、インターネット、電力線通信（ＰＬＣ）、セルラーネットワーク（例えばＧＳＭネットワーク）（「ＧＳＭ」は登録商標）、または図７のネットワークアーキテクチャ例７００等が包含されるが、これらに限定されない。ネットワーク２０４は、無線または有線接続を用いた通信またはデータ転送を促進することができる。ある実施形態では、ネットワーク２０４は、コンピュータシステム２０２とアンチマルウェアサーバ２０６との通信を促進することができる。

【００２４】

図３は、アンチマルウェアメタデータのルックアップを行うためのコンピュータ実施方法例３００のフロー図である。図３に示されるステップは、任意の適切なコンピュータ実行可能コード及び／またはコンピュータシステムによって行うことができる。一部の実施形態では、図３に示されるステップは、図１のシステム１００及び／または図２のシステム２００のコンポーネントの内の１つまたは複数によって行うことができる。

【００２５】

図３に図示されるように、ステップ３０２において、本明細書に記載のシステムの内の１つまたは複数は、実行前にマルウェアのスキャンが行われる複数の実行可能オブジェクトを識別することができる。例えば、ステップ３０２において、識別モジュール１０４は、図２のコンピュータシステム２０２の一部として、実行可能オブジェクト２１０を識別

することができる。

【００２６】

本明細書においては、「実行可能オブジェクト」という言葉は、実行可能命令の任意の集まりを意味し得る。実行可能ファイルの例には、ポータブル実行可能ファイル、ネイティブ実行可能ファイル、ライブラリファイル（ダイナミックリンクライブラリやダイナミックシェアードオブジェクト等）、インタプリタ内で実行されるバイトコードファイル、及び／またはスクリプトファイルが包含される。

【００２７】

識別モジュール１０４は、適切な状況における複数の実行可能オブジェクトを識別することができる。例えば、複数の実行可能オブジェクトは、実行可能オブジェクトの実行及び／または実行を目的としたロードが許可される前に、システム上の各実行可能オブジェクトのスキャン及び／または検証を行うように構成されたシステムに存在し得る。一部の実施例では、システムは、マルウェアに関して各実行可能オブジェクトをスキャンするように構成されてもよい。追加的または代替的に、システムは、各実行可能オブジェクトからマルウェアの妥当性及び／またはマルウェアが存在しないことを確認するように構成されてもよい。例えば、システムは、ホワイトリストに照らして、既知のマルウェアの変種に照らして、及び／またはコミュニティ評判スコアに関して各実行可能オブジェクトのチェックを行うように構成されてもよい。

【００２８】

識別モジュール１０４は、様々なソースの何れからも複数の実行可能ファイルを識別することができる。一部の実施例では、識別モジュール１０４は、システム構成情報を用いて、自動起動される実行可能オブジェクトセットを識別することができる。システム構成情報は、自動起動される実行可能オブジェクトセットにおける自動起動される各実行可能オブジェクトがいつ起動される可能性が高いかを示すことができる。システム構成情報は、絶対時間、現在の時間と比較した時間、１つまたは複数のイベントと比較した時間の観点から、１つまたは複数のイベントと比較した順序（１つまたは複数の実行可能オブジェクトの実行との比較を包含する）等で、自動起動される各実行可能オブジェクトがいつ起動される可能性が高いかを示すことができる。

【００２９】

一部の実施例では、自動起動される実行可能オブジェクトセットの識別には、オペレーティングシステムのブート処理中に起動されるように構成された少なくとも１つの実行可能オブジェクトの識別が包含され得る。例えば、識別モジュール１０４は、ＭＩＣＲＯＳＯＦＴ　ＷＩＮＤＯＷＳ　ＰＲＥＦＥＴＣＨ（「ＷＩＮＤＯＷＳ」は登録商標、以下同じ）及び／またはＭＩＣＲＯＳＯＦＴ　ＷＩＮＤＯＷＳ　ＳＵＰＥＲＦＥＴＣＨからデータを得ることにより、ブート処理中に起動するように構成された１つまたは複数の実行可能オブジェクトを識別すること、及び／または他の一般的に使用されるアプリケーションを識別することができる。識別モジュール１０４は、追加的または代替的に、ＢｏｏｔＥｘｅｃｕｔｅレジストリ情報からデータを得てもよい。例えば、識別モジュール１０４は、

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲Ｓｙｓｔｅｍ╲ＣｕｒｒｅｎｔＣｏｎｔｒｏｌＳｅｔ╲Ｃｏｎｔｒｏｌ╲Ｓｅｓｓｉｏｎ　Ｍａｎａｇｅｒ╲ＢｏｏｔＥｘｅｃｕｔｅ

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲Ｓｙｓｔｅｍ╲ＣｕｒｒｅｎｔＣｏｎｔｒｏｌＳｅｔ╲Ｃｏｎｔｒｏｌ╲Ｓｅｓｓｉｏｎ　Ｍａｎａｇｅｒ╲ＳｅｔｕｐＥｘｅｃｕｔｅ

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲Ｓｙｓｔｅｍ╲ＣｕｒｒｅｎｔＣｏｎｔｒｏｌＳｅｔ╲Ｃｏｎｔｒｏｌ╲Ｓｅｓｓｉｏｎ　Ｍａｎａｇｅｒ╲Ｅｘｅｃｕｔｅの内の何れかまたは全てからデータを得ることができる。

【００３０】

識別モジュール１０４は、自動起動される実行可能オブジェクトセットの識別の一部として、サービスを識別することもできる。例えば、識別モジュール１０４は、自動的に開

始するように構成された登録サービスを識別することができる。追加的または代替的に、識別モジュール１０４は、ドライバを識別することができる。例えば、識別モジュール１０４は、

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲Ｓｙｓｔｅｍ╲ＣｕｒｒｅｎｔＣｏｎｔｒｏｌＳｅｔ╲Ｓｅｒｖｉｃｅｓからデータを得ることができる。

【００３１】

一部の実施例では、識別モジュール１０４は、ウィンソックプロバイダ及び／またはレイヤードサービスプロバイダを識別することができる。追加的または代替的に、識別モジュール１０４は、ログイン時に実行されるように構成された実行可能オブジェクトを識別することができる。例えば、識別モジュール１０４は、ログイン構成設定からデータを得ることができる。一例として、識別モジュール１０４は、

・Ｃ：╲Ｕｓｅｒｓ╲［ｕｓｅｒ］╲ＡｐｐＤａｔａ╲Ｌｏｃａｌ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ　Ｓｉｄｅｂａｒ（「Ｗｉｎｄｏｗｓ」は登録商標、以下同じ）╲Ｓｅｔｔｉｎｇｓ．ｉｎｉ

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲ＳＯＦＴＷＡＲＥ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｒｕｎ

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲ＳＯＦＴＷＡＲＥ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ　ＮＴ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｗｉｎｌｏｇｏｎ╲Ｕｓｅｒｉｎｉｔ

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲ＳＯＦＴＷＡＲＥ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲ＲｕｎＯｎｃｅＥｘ

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲ＳＯＦＴＷＡＲＥ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲ＲｕｎＯｎｃｅ

・Ｃ：╲ＰｒｏｇｒａｍＤａｔａ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ╲Ｓｔａｒｔ　Ｍｅｎｕ╲Ｐｒｏｇｒａｍｓ╲Ｓｔａｒｔｕｐ

・Ｃ：╲Ｕｓｅｒｓ╲［ｕｓｅｒ］╲ＡｐｐＤａｔａ╲Ｒｏａｍｉｎｇ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ╲Ｓｔａｒｔ　Ｍｅｎｕ╲Ｐｒｏｇｒａｍｓ╲Ｓｔａｒｔｕｐ

・ＨＫＥＹ＿ＣＵＲＲＥＮＴ＿ＵＳＥＲ╲Ｓｏｆｔｗａｒｅ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ　ＮＴ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｗｉｎｄｏｗｓ╲Ｌｏａｄ

・ＨＫＥＹ＿ＣＵＲＲＥＮＴ＿ＵＳＥＲ╲Ｓｏｆｔｗａｒｅ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｐｏｌｉｃｉｅｓ╲Ｅｘｐｌｏｒｅｒ╲Ｒｕｎ

・ＨＫＥＹ＿ＣＵＲＲＥＮＴ＿ＵＳＥＲ╲Ｓｏｆｔｗａｒｅ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｒｕｎ

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲Ｓｙｓｔｅｍ╲ＣｕｒｒｅｎｔＣｏｎｔｒｏｌＳｅｔ╲Ｃｏｎｔｒｏｌ╲Ｔｅｒｍｉｎａｌ　Ｓｅｒｖｅｒ╲Ｗｄｓ╲ｒｄｐｗｄ╲ＳｔａｒｔｕｐＰｒｏｇｒａｍｓ

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲ＳＯＦＴＷＡＲＥ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ　ＮＴ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｗｉｎｌｏｇｏｎ╲ＡｐｐＳｅｔｕｐ

・ＨＫＥＹ＿ＣＵＲＲＥＮＴ＿ＵＳＥＲ╲Ｓｏｆｔｗａｒｅ╲Ｐｏｌｉｃｉｅｓ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ╲Ｓｙｓｔｅｍ╲Ｓｃｒｉｐｔｓ╲Ｌｏｇｏｎ

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲Ｓｏｆｔｗａｒｅ╲Ｐｏｌｉｃｉｅｓ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ╲Ｓｙｓｔｅｍ╲Ｓｃｒｉｐｔｓ╲Ｌｏｇｏｎ

・ＨＫＥＹ＿ＣＵＲＲＥＮＴ＿ＵＳＥＲ╲Ｓｏｆｔｗａｒｅ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｐｏｌｉｃｉｅｓ╲Ｓｙｓｔｅｍ╲Ｓｈｅｌｌ
・ＨＫＥＹ＿ＣＵＲＲＥＮＴ＿ＵＳＥＲ╲ＳＯＦＴＷＡＲＥ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ　ＮＴ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｗｉｎｌｏｇｏｎ╲Ｓｈｅｌｌ
・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲ＳＯＦＴＷＡＲＥ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ　ＮＴ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｗｉｎｌｏｇｏｎ╲ＧｉｎａＤＬＬ
・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲ＳＯＦＴＷＡＲＥ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ　ＮＴ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｗｉｎｌｏｇｏｎ╲Ｔａｓｋｍａｎ
・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲ＳＯＦＴＷＡＲＥ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ　ＮＴ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｗｉｎｌｏｇｏｎ╲Ｎｏｔｉｆｙの内の何れかまたは全てからデータを得ることができる。

【００３２】

識別モジュール１０４は、タスクスケジューラに従って実行されるように構成された実行可能オブジェクトを識別することもできる。この例では、識別モジュール１０４は、タスクスケジューラの構成ファイルからデータを得ることにより、実行可能オブジェクトを識別することができる。

【００３３】

一部の実施例では、識別モジュール１０４は、別の実行可能オブジェクトの代わりに、及び／または別の実行可能オブジェクトと同時に自動的にロード及び／または実行されるように構成された実行可能オブジェクトを識別することができる。例えば、識別モジュール１０４は、ある実行可能ファイルを別の実行可能ファイルの代わりに実行させる画像ハイジャック構成を識別することができる（例えば、実行可能ファイルを直接実行する代わりに、実行可能ファイルをロードするように構成されたデバッガ）。追加的または代替的に、識別モジュール１０４は、１つまたは複数のアプリケーションを用いてライブラリを自動的にロードさせるコンポーネント導入構成を識別することができる。一例として、識別モジュール１０４は、

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲ＳＯＦＴＷＡＲＥ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ　ＮＴ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｗｉｎｄｏｗｓ╲Ａｐｐｉｎｉｔ＿Ｄｌｌｓ
・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲Ｓｏｆｔｗａｒｅ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ　ＮＴ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｉｍａｇｅ　Ｆｉｌｅ　Ｅｘｅｃｕｔｉｏｎ　Ｏｐｔｉｏｎｓの一方または両方からデータを得ることができる。

【００３４】

複数の実行可能オブジェクトの識別の一部として、識別モジュール１０４は、ユーザによって起動される可能性の高い実行可能オブジェクトセットを識別することもできる。例えば、識別モジュール１０４は、ユーザが所有するデスクトップ上の実行可能オブジェクトを識別することができる。追加的または代替的に、識別モジュール１０４は、ユーザが所有するダウンロードフォルダ（例えば、リモートソースからダウンロードされたファイルのデフォルトターゲット位置として構成されたフォルダ）内の実行可能オブジェクトを識別することができる。一部の実施例では、識別モジュール１０４は、アプリケーション起動メニュー内の実行可能オブジェクトのリスト（例えば、最近起動されたアプリケーションのリスト）を識別することができる。追加的または代替的に、識別モジュール１０４は、１つまたは複数のユーザインタフェース要素の状態を調べることにより、実行可能オブジェクトを識別することができる。例えば、識別モジュール１０４は、ユーザによって

現在反転表示されている、及び／またはマウス及び／またはキーボードフォーカスが置かれた実行可能オブジェクトに対するリンクを識別することができる。追加的または代替的に、識別モジュール１０４は、実行可能オブジェクトのディレクトリの内容を表示する開かれたウィンドウ内の実行可能オブジェクトを識別することができる。

【００３５】

一部の実施例では、識別モジュール１０４は、識別された実行可能オブジェクトが実行を目的として依存する１つまたは複数の実行可能オブジェクトを識別することによって、複数の実行可能オブジェクトを拡張することができる。例えば、識別モジュール１０４は、複数の実行可能オブジェクト内の第１の実行可能オブジェクトを識別し、第１の実行可能オブジェクトが第２の実行可能オブジェクトに依存することを示す依存情報を識別し、次に、複数の実行可能オブジェクト内に第２の実行可能オブジェクトを包含させてもよい。例えば、識別モジュール１０４は、第１の実行可能オブジェクト内のインポートテーブルを調べ、インポートテーブル内で参照される第２の実行可能オブジェクトを識別することができる。図４は、実行可能ファイルに関する依存性チャート例４００のブロック図である。図４に図示されるように、実行可能ファイル４０２は、実行可能ファイル４０４に先立つ実行を必要とし、実行可能ファイル４０４は、実行可能ファイル４０６に先立つ実行を必要とし得る（例えば、ブート処理の一部として）。実行可能ファイル４０６は、実行可能ファイル４０８（例えば、実行可能ファイル４０６のインポートテーブルにおいて参照されるライブラリ）に依存し得る。従って、識別モジュール１０４は、ブート処理の一部として、実行可能ファイル４０２、４０４、及び４０６を識別し得る。識別モジュール１０４は、次に、実行可能ファイル４０６が実行可能ファイル４０８に依存することから、実行可能ファイル４０８を識別し得る。一部の実施例では、識別モジュール１０４は、複数の実行可能オブジェクト間の依存情報を収集及び／またはマッピング（例えば、図４に図示するように）することができる。例えば、識別モジュール１０４は、予測モジュール１０６に依存情報を提供することができる。

【００３６】

一部の実施例では、識別モジュール１０４は、識別された実行可能オブジェクトに対する拡張として動作する１つまたは複数の実行可能オブジェクトを識別することによって、複数の実行可能オブジェクトを拡張することができる。例えば、識別モジュール１０４は、複数の実行可能オブジェクト内の第１の実行可能オブジェクトを識別し、第１の実行可能オブジェクトに対する拡張として動作する第２の実行可能オブジェクトを識別することができる。例えば、第１の実行可能オブジェクトは、ブラウザを包含し、第２の実行可能オブジェクトは、ブラウザに対する拡張を包含し得る。追加的または代替的に、第１の実行可能オブジェクトは、ＭＩＣＲＯＳＯＦＴ　ＷＩＮＤＯＷＳ　ＥＸＰＬＯＲＥＲを包含し、第２の実行可能オブジェクトは、シェル拡張を包含し得る。一例として、識別モジュール１０４は、

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲ＳＯＦＴＷＡＲＥ╲Ｃｌａｓｓｅｓ╲Ｐｒｏｔｏｃｏｌｓ╲Ｆｉｌｔｅｒ

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲Ｓｏｆｔｗａｒｅ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｅｘｐｌｏｒｅｒ╲ＳｈｅｌｌＥｘｅｃｕｔｅＨｏｏｋｓ

・ＨＫＥＹ＿ＣＵＲＲＥＮＴ＿ＵＳＥＲ╲Ｓｏｆｔｗａｒｅ╲Ｃｌａｓｓｅｓ╲＊╲ＳｈｅｌｌＥｘ╲ＣｏｎｔｅｘｔＭｅｎｕＨａｎｄｌｅｒｓ

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲Ｓｏｆｔｗａｒｅ╲Ｃｌａｓｓｅｓ╲＊╲ＳｈｅｌｌＥｘ╲ＰｒｏｐｅｒｔｙＳｈｅｅｔＨａｎｄｌｅｒｓ

・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲Ｓｏｆｔｗａｒｅ╲Ｃｌａｓｓｅｓ╲Ｄｉｒｅｃｔｏｒｙ╲Ｓｈｅｌｌｅｘ╲ＣｏｐｙＨｏｏｋＨａｎｄｌｅｒｓ

・ＨＫＥＹ＿ＣＵＲＲＥＮＴ＿ＵＳＥＲ╲Ｓｏｆｔｗａｒｅ╲Ｃｌａｓｓｅ

s╲Ｆｏｌｄｅｒ╲ＳｈｅｌＥｘ╲ＤｒａｇＤｒｏｐＨａｎｄｌｅｒｓ
・ＨＫＥＹ＿ＬＯＣＡＬ＿ＭＡＣＨＩＮＥ╲Ｓｏｆｔｗａｒｅ╲Ｗｏｗ６４３２Ｎｏｄｅ╲Ｍｉｃｒｏｓｏｆｔ╲Ｗｉｎｄｏｗｓ╲ＣｕｒｒｅｎｔＶｅｒｓｉｏｎ╲Ｅｘｐｌｏｒｅｒ╲ＳｈｅｌｌＩｃｏｎＯｖｅｒｌａｙＩｄｅｎｔｉｆｉｅｒｓの内の何れかまたは全てからデータを得ることができる。

【００３７】

識別モジュール１０４は、実行時及び／または実行後に１つまたは複数の実行可能オブジェクトを識別することもできる。例えば、識別モジュール１０４は、実行を目的として起動された実行可能オブジェクト及び／または実行中の実行可能オブジェクトを識別することができる。一部の実施例では、識別モジュール１０４は、アプリケーションの実行パターンを監視することによって、頻繁に実行される実行可能オブジェクト及び／または特定の順序及び／または特定のパターンに従って実行される可能性の高い実行可能オブジェクトを識別することができる。

【００３８】

図５は、アンチマルウェアメタデータのルックアップを行うためのシステム例５００を図示する。一例として図５を使用して、識別モジュール１０４は、図４の実行可能ファイルを識別することができる（例えばシステム構成情報５１０を用いる）。

【００３９】

図３に戻り、ステップ３０４において、本明細書に記載のシステムの内の１つまたは複数は、複数の実行可能オブジェクト内の各実行可能オブジェクトに関して、実行可能オブジェクトの実行の危急性を評価することができる。例えば、ステップ３０４において、予測モジュール１０６は、図２のコンピュータシステム２０２の一部として、実行可能オブジェクト２１０の各々の実行の危急性を評価することができる。追加の例として図５を用いて、ステップ３０４において、予測モジュール１０６は、複数の実行可能オブジェクト内の各実行可能オブジェクトの実行の危急性を評価することができる。

【００４０】

予測モジュール１０６は、様々な方法で実行可能オブジェクトの実行の危急性を評価することができる。例えば、予測モジュール１０６は、実行可能オブジェクトが所定の時間内に実行される可能性を評価することができる。例えば、予測モジュール１０６は、実行可能オブジェクトに関するアンチマルウェアメタデータの検索及び／またはアンチマルウェアメタデータを有する実行可能オブジェクトのスキャンにかかる時間内に実行可能オブジェクトが実行される可能性を評価することができる。追加的または代替的に、予測モジュール１０６は、実行可能オブジェクトが次に実行される実行可能オブジェクトである可能性が最も高いか否かを評価することができる。一部の実施例では、予測モジュール１０６は、実行可能オブジェクトの重要性－例えば、ユーザの経験にとって実行可能オブジェクトのタイムリーな実行がどれ程重要であるか（例えば、核となる機能性及び／または非インタラクティブなバックグラウンドタスクに対してユーザインタフェース要素を提供する実行可能オブジェクトの優先順位を決定する）、何個の実行可能オブジェクトがその実行可能オブジェクトに依存しているか等と共に、実行可能オブジェクトの実行の危急性を評価することができる。

【００４１】

予測モジュール１０６は、様々な情報を用いて実行可能オブジェクトの実行の危急性を評価することができる。例えば、予測モジュール１０６は、実行可能オブジェクトが識別された状況を包含する、識別モジュール１０４によって集められた情報を用いることができる。例えば、予測モジュール１０６は、ブート処理が進行中である場合及び／または実行可能オブジェクトが間もなく実行されることをブート依存情報が示す場合、この実行可能オブジェクトの実行が危急であると決定し得る。追加的または代替的に、予測モジュール１０６は、オペレーティングシステムがサービス及び／またはドライバをロードする寸

前である場合及び自動的にロードされるように構成された登録サービス及び／またはドライバを実行可能オブジェクトが包含する場合、この実行可能オブジェクトの実行が危急であると決定し得る。一部の実施例では、予測モジュール１０６は、現在のデスクトップが実行可能オブジェクトへのリンクを表示する場合、この実行可能オブジェクトの実行が危急である可能性が高いと決定し得る。実行可能オブジェクトに依存する別の実行可能オブジェクトの実行が危急であると予測モジュール１０６が決定した場合にも、予測モジュール１０６は、この実行可能オブジェクトの実行が危急であると決定し得る。

【００４２】

一部の実施例では、予測モジュール１０６は、実行可能オブジェクトの作成時間を識別することができる。予測モジュール１０６は、作成時間と現在の時間との距離に伴って、実行可能オブジェクトの危急の実行の予想を単調に高め得る。例えば、予測モジュール１０６は、古い実行可能オブジェクトに関する危急性の格付けを下げ得る、及び／または新しい実行可能オブジェクトに関する危急性の格付けを上げ得る。

【００４３】

予測モジュール１０６は、様々な測定基準、データ構造、及び／またはアルゴリズムを用いて、実行可能オブジェクトの実行の危急性を評価することができる。例えば、予測モジュール１０６は、実行可能オブジェクトに関する危急性の格付け及び／またはスコアを生成してもよい。追加的または代替的に、予測モジュール１０６は、実行可能オブジェクトを包含する依存性チャートを生成することができる。一般的に、予測モジュール１０６は、少なくとも部分的に複数の実行可能オブジェクトを順序付け得るアルゴリズムを用いてもよい。一部の実施例では、予測モジュール１０６は、危急性の格付けを生成するアルゴリズムに対してハードコードされた、及び／または明確に構成された重み及び／または入力を用いてもよい。例えば、予測モジュール１０６は、ブート処理中に、ブート処理依存情報に対して大きな重みを与えるように構成されてもよい。別の例として、予測モジュール１０６は、デスクトップ上の実行可能オブジェクトの存在に対して、この実行可能オブジェクトの予定された実行時間を示すタスクスケジューラの構成に対するよりも小さな重みを与えるように構成されてもよい。追加的または代替的に、予測モジュール１０６は、過去の経験に基づいて、アルゴリズムに対する重み及び／または入力を自動的に調整するように構成されてもよい。例えば、実行が危急であったことを示したアルゴリズムによって認識された入力にもかかわらず、予測モジュール１０６が、実行可能オブジェクトの実行を予測し損なう場合、予測モジュール１０６は、入力の重みを増加させ得る。

【００４４】

一例として図４を用いて、予測モジュール１０６は、ブート処理中に、実行可能オブジェクトの実行の可能性の高い順序を示す依存性チャート４００を生成することができる。例えば、実行可能ファイル４１０及び４１２は共に、実行可能ファイル４０６の後にのみ実行され得る。実行可能ファイル４１４は、実行可能ファイル４１０の後にのみ実行され、さらに、実行可能ファイル４１６及び４１８に依存し得る。実行可能ファイル４２０は、実行可能ファイル４１４及び４１２の後にのみ実行され得る。同様に、実行可能ファイル４２２は、実行可能ファイル４１２の後にのみ実行され得る。実行可能ファイル４２４、４２６、及び４２８は、実行可能ファイル４２０に対するプラグインを表し得る。

【００４５】

図３に戻り、ステップ３０６において、本明細書に記載のシステムの内の１つまたは複数は、評価に基づいて、複数の実行可能オブジェクトに対応するアンチマルウェアメタデータの検索順序の優先順位を決定することができる。例えば、ステップ３０６において、優先順位決定モジュール１０８は、図２のコンピュータシステム２０２の一部として、実行可能オブジェクト２１０に対応するアンチマルウェアシグネチャ２１４（１）～（ｎ）の内の１つまたは複数に関する検索順序２１２を生成することができる。追加例として図５を用い、ステップ３０６において、優先順位決定モジュール１０８は、キュー５２０内で図４の実行可能ファイルに対応するアンチマルウェアサーバ５０６からのアンチマルウェアメタデータの検索順序の優先順位を決定することができる。

【００４６】
本明細書においては、「アンチマルウェアメタデータ」という言葉は、実行可能オブジェクトがマルウェアの脅威を包含する、及び／またはもたらすか否かを決定するために使用される任意のデータを指し得る。従って、ある実行可能オブジェクトに「対応する」アンチマルウェアメタデータは、その実行可能オブジェクトがマルウェアの脅威を包含する、及び／またはもたらすか否かを決定するために使用されるアンチマルウェアメタデータを指し得る。一般的に、「アンチマルウェアメタデータ」は、ファイルのスキャン、検証、及び／またはチェックを行う過程でアンチマルウェアシステムが使用し得る任意のデータを指し得る。例えば、アンチマルウェアメタデータは、アンチマルウェアシグネチャを包含し得る。本明細書においては、「アンチマルウェアシグネチャ」という言葉は、指紋、ハッシュ、及び／または他の任意の表現、またはマルウェアの変種、ファミリー、及び／または型の特徴の識別を指し得る。アンチマルウェアメタデータの別の例には、ホワイトリストシグネチャが包含され得る。ホワイトリストシグネチャには、指紋、ハッシュ、及び／または他の任意の表現、または既知の正常なファイルの特徴の識別が包含され得る。アンチマルウェアメタデータの追加例には、ファイルの評判情報が包含され得る。

【００４７】
「評判情報」という用語は、本明細書においては、一般的に、実行可能ファイル、ソフトウェア発行者、及び／またはファイルソース（ウェブドメインまたはダウンロードリンク等）の信頼性または正当性に関するある特定のコミュニティ（セキュリティソフトウェア発行者のユーザ基盤等）の意見を伝える情報を指す。評判情報の例には、評判スコア（例えば、高い評判スコアは、ファイル、ソフトウェア発行者、またはファイルソースがコミュニティ内で一般的に信用されており、低い評判スコアは、ファイル、ソフトウェア発行者、またはファイルソースがコミュニティ内で一般的に信用されていないことを示す）、普及率情報（例えば、（１）特定のファイルのインスタンス、（２）特定のソフトウェア発行者によって提供されたファイル、及び／または（３）ウェブドメイン等の特定のファイルソースから得られたファイルを含むコミュニティ内のユーザデバイスのパーセンテージ数を識別する情報）、またはファイル、ソフトウェア発行者、及び／またはファイルソースの信頼性または正当性に関するコミュニティの意見を識別するために使用され得る他の任意の情報が包含されるが、これらに限定されない。

【００４８】
優先順位決定モジュール１０８は、任意の適切な方法で、検索順序の優先順位を決定することができる。例えば、優先順位決定モジュール１０８は、予測モジュール１０６によって生成された任意のスコア、格付け、及び／または依存性チャートを用いて、検索順序の決定を行ってもよい。一部の実施例では、優先順位決定モジュール１０８は、アンチマルウェアメタデータの検索を行う間に１つまたは複数の実行可能ファイルの実行を遅延させることによって生じる予測される待ち時間を最小限に抑えるように、検索順序の優先順位を決定することができる。

【００４９】
一部の実施例では、優先順位決定モジュール１０８は、継続的に検索順序を修正することができる。例えば、ＭＩＣＲＯＳＯＦＴ　ＷＩＮＷＯＲＤのアンチマルウェアメタデータのルックアップの期限が切れ、ユーザがより頻繁にＭＩＮＥＳＷＥＥＰＥＲよりもＭＩＣＲＯＳＯＦＴ　ＷＩＮＷＯＲＤにアクセスする場合、優先順位決定モジュール１０８は、ＭＩＮＥＳＷＥＥＰＥＲよりもＭＩＣＲＯＳＯＦＴ　ＷＩＮＷＯＲＤのルックアップを優先し得る。

【００５０】
一例として図５を用いると、優先順位決定モジュール１０８は、予測モジュール１０６によって生成された依存性チャート４００に基づいて、キュー５２０を生成及び／または修正することができる。例えば、実行可能ファイル４０２が依存性チャート４００のルートに存在するので、優先順位決定モジュール１０８は、実行可能ファイル４０２をキュー５２０の先頭に配置し得る。同様に、依存性チャート４００において実行可能ファイル４

０４が実行可能ファイル４０２に続くので、優先順位決定モジュール１０８は、キュー５２０内で実行可能ファイル４０４を次に配置し得る。実行可能ファイル４０６は、実行可能ファイル４０４に続くが、実行可能ファイル４０８に依存するので、優先順位決定モジュール１０８は、依存性チャート４００内で実行可能ファイル４０８及び４０６を次に配置し得る。一部の実施例では、実行可能ファイル４２０及び４２２は、インタラクティブ実行可能オブジェクト（例えば、ユーザインタフェースを提示する実行可能オブジェクト）を意味し得る。従って、優先順位決定モジュール１０８は、インタラクティブ実行可能オブジェクトのロードにとって最短経路をたどれる様に、キュー５２０内で、実行可能ファイル４１０の前に実行可能ファイル４１２及び４２２を配置し得る。優先順位決定モジュール１０８は、次に、キュー５２０中に、実行可能ファイル４１８、４１６、４１４、４２０、４２４、４２６、及び４２８を配置することにより、依存性チャート４００における他の経路を完了することができる。

【００５１】

一部の実施例では、優先順位決定モジュール１０８は、リモートコンピュータシステムから、複数の実行可能オブジェクト内の少なくとも１つの実行可能オブジェクトに関連するアンチマルウェアメタデータを検索するために優先順位決定情報も受信し得る。例えば、モジュール１０２のインスタンスは、他のクライアントシステム上で実行され、実行可能ファイルの依存性、実行可能ファイルの起動パターン、及びユーザの実行可能ファイルの好みに関するデータを収集し得る。これらの他のクライアントシステムは、収集したデータをセントラルサーバに提供し、今度は、セントラルサーバが、データを集約し、様々なクライアントシステム上で実行中の優先順位決定モジュール１０８の様々なインスタンスを使用するためにデータを配布し得る。

【００５２】

図３に戻ると、ステップ３０８において、本明細書に記載のシステムの内の１つまたは複数は、検索順序に基づいて、複数の実行可能オブジェクト内のある実行可能オブジェクトに対応するアンチマルウェアメタデータを検索することができる。例えば、ステップ３０８において、検索モジュール１１０は、図２のコンピュータシステム２０２の一部として、検索順序２１２に基づいて、実行可能オブジェクト２１０に対応するアンチマルウェアシグネチャ２１４（１）～（ｎ）の少なくとも１つを検索し得る。追加例として図５を用い、ステップ３０８において、検索モジュール１１０は、キュー５２０に基づいて、アンチマルウェアサーバ５０６からアンチマルウェアメタデータを検索し得る。

【００５３】

一部の実施例では、検索モジュール１１０は、実行可能オブジェクトの計画された起動前の実行可能オブジェクトのスキャンに間に合うように、アンチマルウェアメタデータを検索することができる。一例として図５を用いると、アンチマルウェアメタデータの検索後に、検索モジュール１１０は、アンチマルウェアシグネチャキャッシュ５３０中にアンチマルウェアメタデータを保存してもよい。アンチマルウェアシステム５４０は、次に、実行可能ファイルの起動の試みを検出し得る。アンチマルウェアシステム５４０は、アンチマルウェアサーバ５０６から必要とされるアンチマルウェアメタデータを検索するのではなく、アンチマルウェアシグネチャキャッシュ５３０からアンチマルウェアメタデータを用いて実行可能ファイルを単純にスキャンしてもよい。一部の実施例では、検索モジュール１１０は、リモートストレージシステムからアンチマルウェアメタデータ（例えばアンチマルウェアシグネチャ）を検索してもよい。例えば、アンチマルウェアサーバ５０６は、複数の実行可能オブジェクトに対応するアンチマルウェアメタデータを保存するクラウドストレージサービスを包含し得る。従って、実行可能オブジェクトの実行前に直接アンチマルウェアサーバ５０６からアンチマルウェアメタデータを検索することにより、アンチマルウェアシグネチャキャッシュ５３０からアンチマルウェアメタデータを検索することとは対照的に、不要な待ち時間が生じ得る。ステップ３０８の後に、方法３００は終了し得る。

【００５４】

一部の実施例では、本明細書に記載のシステムは、アンチマルウェアメタデータを用いて、実行可能オブジェクトに対してアンチマルウェアスキャンを行うこともできる。本明細書に記載のシステムは、次に、実行可能オブジェクトが安全であることをアンチマルウェアスキャンが示す場合には実行可能オブジェクトを起動させ、あるいは、実行可能オブジェクトが安全でないことをスキャンが示す場合には、実行可能オブジェクトの実行を阻止することができる。

【００５５】

アンチマルウェアメタデータのルックアップの優先順位を決定することによって、本明細書に記載のシステム及び方法は、アンチマルウェアシステムがアンチマルウェアメタデータを検索し、実行可能ファイルを起動させるユーザによって認識される待ち時間を少なくして、起動前に実行可能ファイルをスキャンすることを可能にできる。

【００５６】

図６は、本明細書に記載及び／または図示される実施形態の内の１つまたは複数を実施可能なコンピュータシステム例６１０のブロック図である。コンピュータシステム６１０は、コンピュータ可読命令を実行可能な任意のシングルまたはマルチプロセッサコンピュータデバイスまたはシステムを広く意味する。コンピュータシステム６１０の例には、ワークステーション、ラップトップ、クライアント側端末、サーバ、分散コンピュータシステム、ハンドヘルドデバイス、または他の任意のコンピュータシステムまたはデバイスが包含されるが、これらに限定されない。最も基本的な構成では、コンピュータシステム６１０は、少なくとも１つのプロセッサ６１４及びシステムメモリ６１６を包含し得る。

【００５７】

プロセッサ６１４は、一般的に、データの処理または命令の解釈及び実行が可能な任意の種類または形態の処理装置を意味する。特定の実施形態では、プロセッサ６１４は、ソフトウェアアプリケーションまたはモジュールから命令を受信し得る。これらの命令は、本明細書に記載及び／または図示された実施形態例の内の１つまたは複数の機能をプロセッサ６１４に行わせることができる。例えば、プロセッサ６１４は、単体または他の要素と一緒に、本明細書に記載の識別、使用、評価、増大、優先順位の決定、受信、及び／または検索ステップの内の１つまたは複数を行い得る、及び／またはそれらを行うための手段となり得る。プロセッサ６１４は、本明細書に記載及び／または図示された他のステップ、方法、またはプロセスも行い得る、及び／またはそれを行うための手段ともなり得る。

【００５８】

システムメモリ６１６は、一般的に、データ及び／または他のコンピュータ可読命令を保存可能な任意の種類または形態の揮発性または不揮発性ストレージデバイスまたは媒体を意味する。システムメモリ６１６の例には、ランダムアクセスメモリ（ＲＡＭ）、読み出し専用メモリ（ＲＯＭ）、フラッシュメモリ、または他の任意の適切なメモリデバイスが包含されるが、これらに限定されない。必須ではないが、特定の実施形態では、コンピュータシステム６１０は、揮発性記憶装置（例えば、システムメモリ６１６等）及び不揮発性ストレージデバイス（例えば、以下に詳細に説明するようなプライマリストレージデバイス６３２等）の両方を包含し得る。ある実施例では、図１のモジュール１０２の内の１つまたは複数が、システムメモリ６１６にロードされ得る。

【００５９】

特定の実施形態では、コンピュータシステム例６１０は、プロセッサ６１４及びシステムメモリ６１６に加えて、１つまたは複数のコンポーネントまたは要素も包含し得る。例えば、図６に図示されるように、コンピュータシステム６１０は、メモリコントローラ６１８、入出力（Ｉ／Ｏ）コントローラ６２０、及び通信インタフェース６２２を包含し、これらの各々は、通信インフラ６１２を介して相互接続され得る。通信インフラ６１２は、一般的に、コンピュータデバイスの１つまたは複数のコンポーネント間の通信を促進可能な任意の種類または形態のインフラを意味する。通信インフラ６１２の例には、通信バス（ＩＳＡ、ＰＣＩ、ＰＣＩｅ、または同様のバス等）及びネットワークが包含されるが

、これらに限定されない。

【００６０】

メモリコントローラ６１８は、一般的に、メモリまたはデータの取り扱いが可能な、あるいは、コンピュータシステム６１０の１つまたは複数のコンポーネント間の通信の制御が可能な任意の種類または形態のデバイスを意味する。例えば、特定の実施形態では、メモリコントローラ６１８は、通信インフラ６１２を介して、プロセッサ６１４、システムメモリ６１６、及びＩ／Ｏコントローラ６２０間の通信を制御し得る。特定の実施形態では、メモリコントローラ６１８は、単体または他の要素と一緒に、識別、使用、評価、増大、優先順位の決定、受信、及び／または検索等の本明細書に記載及び／または図示されるステップまたは特徴の内の１つまたは複数を行い得る、及び／またはそれらを行うための手段となり得る。

【００６１】

Ｉ／Ｏコントローラ６２０は、一般的に、コンピュータデバイスの入力及び出力の機能を調整及び／または制御可能な任意の種類または形態のモジュールを意味する。例えば、特定の実施形態では、Ｉ／Ｏコントローラ６２０は、プロセッサ６１４、システムメモリ６１６、通信インタフェース６２２、ディスプレイアダプタ６２６、入力インタフェース６３０、及びストレージインタフェース６３４等のコンピュータシステム６１０の１つまたは複数の要素間のデータ転送の制御または促進を行い得る。Ｉ／Ｏコントローラ６２０を用いて、例えば、単体または他の要素と一緒に、本明細書に記載の識別、使用、評価、増大、優先順位の決定、受信、及び／または検索ステップの内の１つまたは複数を行い得る、及び／またはそれらを行うための手段となり得る。Ｉ／Ｏコントローラ６２０を用いることにより、本開示に記載の他のステップ及び特徴も行い得る、及び／またはそれらを行うための手段ともなり得る。

【００６２】

通信インタフェース６２２は、コンピュータシステム例６１０と、１つまたは複数の追加のデバイスとの通信の促進が可能な任意の種類または形態の通信デバイスまたはアダプタを広く意味する。例えば、特定の実施形態では、通信インタフェース６２２は、コンピュータシステム６１０と、追加のコンピュータシステムを包含するプライベートまたはパブリックネットワークとの通信を促進し得る。通信インタフェース６２２の例には、有線ネットワークインタフェース（ネットワークインタフェースカード等）、無線ネットワークインタフェース（無線ネットワークインタフェースカード等）、モデム、及び他の任意の適切なインタフェースが包含されるが、これらに限定されることはない。少なくとも１つの実施形態において、通信インタフェース６２２は、インターネット等のネットワークへの直接リンクを介したリモートサーバへの直接接続を提供し得る。通信インタフェース６２２は、このような接続を、例えば、ローカルエリアネットワーク（イーサネットネットワーク等）（「イーサーネット」は登録商標、以下同じ）、パーソナルエリアネットワーク、電話またはケーブル網、携帯電話接続、衛星データ接続、または他の任意の適切な接続を用いて間接的に提供することもできる。

【００６３】

特定の実施形態では、通信インタフェース６２２は、外部バスまたは通信チャネルを介した、コンピュータシステム６１０と、１つまたは複数の追加のネットワークまたはストレージデバイスとの通信を促進するように構成されたホストアダプタを意味する場合もある。ホストアダプタの例には、ＳＣＳＩホストアダプタ、ＵＳＢホストアダプタ、ＩＥＥＥ１３９４ホストアダプタ、ＳＡＴＡ及びｅＳＡＴＡホストアダプタ、ＡＴＡ及びＰＡＴＡホストアダプタ、ファイバチャネルインタフェースアダプタ、またはイーサネットアダプタ等が包含されるが、これらに限定されない。通信インタフェース６２２により、コンピュータシステム６１０が、分散またはリモートコンピューティングに携わることも可能となり得る。例えば、通信インタフェース６２２は、リモートデバイスから命令を受信する、あるいは、実行を目的としてリモートデバイスに命令を送信することができる。特定の実施形態では、通信インタフェース６２２は、単体または他の要素と一緒に、本明細書

に開示される識別、使用、評価、増大、優先順位の決定、受信、及び／または検索ステップの内の１つまたは複数を行い得る、及び／またはそれらを行うための手段となり得る。通信インタフェース６２２を用いることにより、本開示に記載の他のステップ及び特徴も行い得る、及び／またはそれらを行うための手段ともなり得る。

【００６４】

図６に図示されるように、コンピュータシステム６１０は、ディスプレイアダプタ６２６を介して通信インフラ６１２に接続される少なくとも１つのディスプレイデバイス６２４も包含し得る。ディスプレイデバイス６２４は、一般的に、ディスプレイアダプタ６２６によって転送された情報を視覚的に表示することが可能な種類または形態のデバイスを意味する。同様に、ディスプレイアダプタ６２６は、一般的に、ディスプレイデバイス６２４上での表示を目的に、通信インフラ６１２から（あるいは、当該分野で公知のようにフレームバッファから）グラフィックス、テキスト、及び他のデータを転送するように構成された任意の種類または形態のデバイスを意味する。

【００６５】

図６に図示されるように、コンピュータシステム例６１０は、入力インタフェース６３０を介して通信インフラ６１２に接続された少なくとも１つの入力デバイス６２８も包含し得る。入力デバイス６２８は、一般的に、コンピュータまたは人間によって生成された入力をコンピュータシステム例６１０に提供することが可能な任意の種類または形態の入力デバイスを意味する。入力デバイス６２８の例には、キーボード、ポインティングデバイス、音声認識装置、または他の任意の入力デバイスが包含されるが、これらに限定されない。少なくとも１つの実施形態では、入力デバイス６２８は、単体または他の要素と一緒に、本明細書に開示される識別、使用、評価、増大、優先順位の決定、受信、及び／または検索ステップの内の１つまたは複数を行い得る、及び／またはそれらを行うための手段となり得る。入力デバイス６２８を使用することにより、本開示に記載の他のステップ及び特徴も行い得る、及び／またはそれらを行うための手段ともなり得る。

【００６６】

図６に図示されるように、コンピュータシステム例６１０は、ストレージインタフェース６３４を介して通信インフラ６１２に接続されるプライマリストレージデバイス６３２及びバックアップストレージデバイス６３３も包含し得る。ストレージデバイス６３２及び６３３は、一般的に、データ及び／または他のコンピュータ可読命令の保存が可能な種類または形態のストレージデバイスまたは媒体を意味する。例えば、ストレージデバイス６３２及び６３３は、磁気ディスクドライブ（例えば、いわゆるハードドライブ）、フロッピーディスクドライブ（「フロッピー」は登録商標、以下同じ）、磁気テープドライブ、光ディスクドライブ、またはフラッシュドライブ等でもよい。ストレージインタフェース６３４は、一般的に、ストレージデバイス６３２及び６３３と、コンピュータシステム６１０の他のコンポーネントとのデータの転送を行う種類または形態のインタフェースまたはデバイスを意味する。

【００６７】

特定の実施形態では、ストレージデバイス６３２及び６３３は、コンピュータソフトウェア、データ、または他のコンピュータ可読情報を保存するように構成されたリムーバブルストレージ装置から読み取る、及び／またはそれに書き込むように構成され得る。適切なリムーバブルストレージ装置の例には、フロッピーディスク、磁気テープ、光ディスク、またはフラッシュメモリデバイス等が包含されるが、これらに限定されない。ストレージデバイス６３２及び６３３は、コンピュータソフトウェア、データ、または他のコンピュータ可読命令をコンピュータシステム６１０にロードすることが可能な他の類似の構造またはデバイスも包含し得る。例えば、ストレージデバイス６３２及び６３３は、ソフトウェア、データ、または他のコンピュータ可読情報の読み書きを行うように構成され得る。ストレージデバイス６３２及び６３３は、コンピュータシステム６１０の一部でもよく、あるいは、他のインタフェースシステムを介してアクセスされた別個のデバイスでもよい。

【００６８】
特定の実施形態では、ストレージデバイス６３２及び６３３を用いて、例えば、単体または他の要素と一緒に、本明細書に開示される識別、使用、評価、増大、優先順位の決定、受信、及び／または検索ステップの内の１つまたは複数を行い得る、及び／またはそれらを行うための手段となり得る。ストレージデバイス６３２及び６３３を用いることにより、本開示に記載の他のステップ及び特徴も行い得る、及び／またはそれらを行うための手段ともなり得る。
【００６９】
複数の他のデバイスまたはサブシステムをコンピュータシステム６１０に接続することができる。逆に、図６に図示される全てのコンポーネント及びデバイスは、本明細書に記載及び／または図示される実施形態を実施するために必ずしも存在する必要はない。上記で言及したデバイス及びサブシステムは、図６に示される形とは異なる形で相互接続されてもよい。コンピュータシステム６１０は、任意の数のソフトウェア、ファームウェア、及び／またはハードウェア構成を用いてもよい。例えば、本明細書に開示される実施形態例の内の１つまたは複数は、コンピュータ可読媒体のコンピュータプログラム（コンピュータソフトウェア、ソフトウェアアプリケーション、コンピュータ可読命令、またはコンピュータ制御論理とも呼ばれる）としてコード化され得る。「コンピュータ可読媒体」という言葉は、一般的に、コンピュータ可読命令の保存または搬送が可能な形態のデバイス、キャリア、または媒体を指す。コンピュータ可読媒体の例には、搬送波等の伝送型媒体や、磁気ストレージ媒体（例えば、ハードディスクドライブ及びフロッピーディスク）等の物理的媒体、光ストレージ媒体（例えば、ＣＤ－ＲＯＭまたはＤＶＤ－ＲＯＭ）、電子ストレージ媒体（例えば、ソリッドステートドライブ及びフラッシュ媒体）、及び他の配布システムが包含されるが、これらに限定されない。
【００７０】
コンピュータプログラムを含むコンピュータ可読媒体は、コンピュータシステム６１０にロードされ得る。コンピュータ可読媒体に保存されたコンピュータプログラムの全てまたは一部は、次に、システムメモリ６１６及び／またはストレージデバイス６３２及び６３３の様々な部分に保存され得る。プロセッサ６１４によって実行されると、コンピュータシステム６１０にロードされたコンピュータプログラムにより、プロセッサ６１４が、本明細書に記載及び／または図示される実施形態例の内の１つまたは複数の機能を行い得る、及び／またはそれらを行うための手段となり得る。追加的または代替的に、本明細書に記載及び／または図示される実施形態例の内の１つまたは複数は、ファームウェア及び／またはハードウェアにおいて実施され得る。例えば、コンピュータシステム６１０は、本明細書に開示される実施形態例の内の１つまたは複数を実施するように適合させた特定用途向け集積回路（ＡＳＩＣ）として構成されてもよい。
【００７１】
図７は、クライアントシステム７１０、７２０、及び７３０と、サーバ７４０及び７４５とが、ネットワーク７５０に接続され得るネットワークアーキテクチャ例７００のブロック図である。クライアントシステム７１０、７２０、及び７３０は、一般的に、図６のコンピュータシステム例６１０等の、任意の種類または形態のコンピュータデバイスまたはシステムを意味する。一例として、クライアントシステム７１０は、図１のシステム１００を包含し得る。
【００７２】
同様に、サーバ７４０及び７４５は、一般的に、様々なデータベースサービスの提供及び／または特定のソフトウェアアプリケーションの実行を行うように構成された、アプリケーションサーバまたはデータベースサーバ等のコンピュータデバイスまたはシステムを意味する。ネットワーク７５０は、一般的に、例えば、イントラネット、広域ネットワーク（ＷＡＮ）、ローカルエリアネットワーク（ＬＡＮ）、パーソナルエリアネットワーク（ＰＡＮ）、またはインターネットを包含する任意の通信またはコンピュータネットワークを意味する。

【００７３】
図７に図示されるように、１つまたは複数のストレージデバイス７６０（１）～（Ｎ）は、サーバ７４０に直接接続され得る。同様に、１つまたは複数のストレージデバイス７７０（１）～（Ｎ）は、サーバ７４５に直接接続され得る。ストレージデバイス７６０（１）～（Ｎ）及びストレージデバイス７７０（１）～（Ｎ）は、一般的に、データ及び／または他のコンピュータ可読命令の保存が可能な種類または形態のストレージデバイスまたは媒体を意味する。特定の実施形態では、ストレージデバイス７６０（１）～（Ｎ）及びストレージデバイス７７０（１）～（Ｎ）は、ＮＦＳ、ＳＭＢ、またはＣＩＦＳ等の様々なプロトコルを用いてサーバ７４０及び７４５と通信するように構成されたネットワーク接続ストレージ（ＮＡＳ）デバイスを意味し得る。
【００７４】
サーバ７４０及び７４５は、ストレージエリアネットワーク（ＳＡＮ）ファブリック７８０に接続されてもよい。ＳＡＮファブリック７８０は、一般的に、複数のストレージデバイス間の通信の促進が可能な種類または形態のコンピュータネットワークまたはアーキテクチャを意味する。ＳＡＮファブリック７８０は、サーバ７４０及び７４５及び複数のストレージデバイス７９０（１）～（Ｎ）及び／またはインテリジェントストレージアレイ７９５間の通信を促進し得る。ＳＡＮファブリック７８０は、デバイス７９０（１）～（Ｎ）及びアレイ７９５が、クライアントシステム７１０、７２０、及び７３０にとってローカル接続されたデバイスとして見えるように、ネットワーク７５０及びサーバ７４０及び７４５を介して、クライアントシステム７１０、７２０、及び７３０及びストレージデバイス７９０（１）～（Ｎ）及び／またはインテリジェントストレージアレイ７９５間の通信も促進し得る。ストレージデバイス７６０（１）～（Ｎ）及びストレージデバイス７７０（１）～（Ｎ）と同様に、ストレージデバイス７９０（１）～（Ｎ）及びインテリジェントストレージアレイ７９５は、一般的に、データ及び／または他のコンピュータ可読命令の保存が可能な種類または形態のストレージデバイスまたは媒体を意味する。
【００７５】
特定の実施形態において、図６のコンピュータシステム例６１０を参照すると、図６の通信インタフェース６２２等の通信インタフェースを用いて、各クライアントシステム７１０、７２０、及び７３０と、ネットワーク７５０との接続性を提供することができる。クライアントシステム７１０、７２０、及び７３０は、例えばウェブブラウザまたは他のクライアントソフトウェアを用いて、サーバ７４０または７４５上の情報にアクセスすることができる。このようなソフトウェアにより、サーバ７４０、サーバ７４５、ストレージデバイス７６０（１）～（Ｎ）、ストレージデバイス７７０（１）～（Ｎ）、ストレージデバイス７９０（１）～（Ｎ）、またはインテリジェントストレージアレイ７９５がホストのデータにクライアントシステム７１０、７２０、及び７３０がアクセスすることが可能となり得る。図７は、データ交換を目的としたネットワーク（インターネット等）の使用を示すが、本明細書に記載及び／または図示される実施形態は、インターネットまたは何れの特定のネットワーク基盤の環境にも限定されない。
【００７６】
少なくとも１つの実施形態において、本明細書に開示される実施形態例の内の１つまたは複数の全てまたは一部は、コンピュータプログラムとしてコード化され、サーバ７４０、サーバ７４５、ストレージデバイス７６０（１）～（Ｎ）、ストレージデバイス７７０（１）～（Ｎ）、ストレージデバイス７９０（１）～（Ｎ）、インテリジェントストレージアレイ７９５、またはこれらの任意の組み合わせにロードされ、実行され得る。本明細書に開示される実施形態例の内の１つまたは複数の全てまたは一部は、コンピュータプログラムとしてコード化され、サーバ７４０に保存され、サーバ７４５によって実行され、ネットワーク７５０上でクライアントシステム７１０、７２０、及び７３０に配布されることも可能である。従って、ネットワークアーキテクチャ７００は、単体または他の要素と一緒に、本明細書に開示される識別、使用、評価、増大、優先順位の決定、受信、及び／または検索ステップの内の１つまたは複数を行い得る、及び／またはそれらを行うため

の手段となり得る。ネットワークアーキテクチャ７００を用いることにより、本開示に記載の他のステップ及び特徴も行い得る、及び／またはそれらを行うための手段ともなり得る。

【００７７】

上記に詳述したように、コンピュータシステム６１０及び／またはネットワークアーキテクチャ７００の１つまたは複数のコンポーネントは、単体または他の要素と一緒に、アンチマルウェアメタデータのルックアップを行うための方法例の１つまたは複数のステップを行い得る、及び／またはそれらを行うための手段となり得る。

【００７８】

上記の開示は、具体的なブロック図、フローチャート、及び実施例を用いて様々な実施形態を記載しているが、本明細書に記載及び／または図示されるそれぞれのブロック図コンポーネント、フローチャートステップ、動作、及び／またはコンポーネントは、広範囲のハードウェア、ソフトウェア、またはファームウェア（またはそれらの任意の組み合わせ）構成を用いて、個々に、及び／または集合的に実施され得る。さらに、他のコンポーネント内に含まれるコンポーネントのどのような開示も、多くの他のアーキテクチャを具現化することにより同じ機能性を達成することができるので、本質的に例示的であると見なされるべきである。

【００７９】

一部の実施例では、図１のシステム例１００の全てまたは一部は、クラウドコンピューティングまたはネットワーク基盤の環境の一部を表し得る。クラウドコンピューティング環境は、インターネットを介して様々なサービス及びアプリケーションを提供することができる。これらのクラウド基盤のサービス（例えば、サース（ｓｏｆｔｗａｒｅ ａｓ ａ ｓｅｒｖｉｃｅ）、パース（ｐｌａｔｆｏｒｍ ａｓ ａ ｓｅｒｖｉｃｅ）、イアース（ｉｎｆｒａｓｔｒｕｃｔｕｒｅ ａｓ ａ ｓｅｒｖｉｃｅ）等）は、ウェブブラウザまたは他のリモートインタフェースを介してアクセス可能となり得る。本明細書に記載の様々な機能は、リモートデスクトップ環境または他のクラウド基盤のコンピューティング環境によって提供され得る。

【００８０】

本明細書に記載及び／または図示されるステップの処理パラメータ及びシーケンスは、ほんの一例として提供されたものであり、要望に応じて変更可能である。例えば、本明細書に図示及び／または記載されたステップは、ある特定の順序で示される、あるいは、説明され得るが、これらのステップは、必ずしも図示または説明された順序で行われる必要はない。本明細書に記載及び／または図示された様々な方法例は、本明細書に記載または図示されたステップの内の１つまたは複数を省略する、あるいは、開示されたステップに加えて追加のステップを包含することも可能である。

【００８１】

完全に機能したコンピュータシステムの状況において、様々な実施形態を本明細書に記載及び／または図示したが、これらの実施形態例の内の１つまたは複数は、実際に配布を行うために使用される特定の種類のコンピュータ可読媒体とは無関係に、様々な形態でプログラム製品として配布され得る。本明細書に開示された実施形態は、特定のタスクを行うソフトウェアモジュールを用いて実施されてもよい。これらのソフトウェアモジュールには、コンピュータ可読ストレージ媒体またはコンピュータシステムに保存され得るスクリプト、バッチ、または他の実行可能ファイルが包含され得る。一部の実施形態では、これらのソフトウェアモジュールは、本明細書に開示された実施形態例の内の１つまたは複数を行うようにコンピュータシステムを構成することができる。

【００８２】

さらに、本明細書に記載のモジュールの内の１つまたは複数は、ある形態から別の形態へと、データ、物理的デバイス、及び／または物理的デバイスの表現を変換することができる。例えば、本明細書に記載のモジュールの内の１つまたは複数は、アンチマルウェアシステムを低遅延のアンチマルウェアシステムへと変換することができる。

【００８３】
上記の記載は、本明細書に開示される実施形態例の様々な態様を当業者が最も活用できるように提供されたものである。この例示的な記載は、網羅的であること、または開示された何れの正確な形態にも限定されることを意図したものではない。本開示の精神及び範囲から逸脱することなく、多くの変更形態及び変形形態が可能である。本明細書に開示された実施形態は、あらゆる面で例示的であるとみなされるものであり、限定的であるとみなされるものではない。本開示の範囲を決定する際には、添付の特許請求の範囲及びそれらの均等物が参照される必要がある。
【００８４】
特に断りのない限り、明細書及び特許請求の範囲に使用される「１つの」（「ａ」または「ａｎ」）という用語は、「少なくとも１つの」という意味であると解釈されるものである。さらに、使用を簡単にするために、明細書及び特許請求の範囲に使用される「包含する」（「ｉｎｃｌｕｄｉｎｇ」）及び「有する」（「ｈａｖｉｎｇ」）という語は、「含む」（「ｃｏｍｐｒｉｓｉｎｇ」）という語と代替可能に、同じ意味として使用される。

【図１】

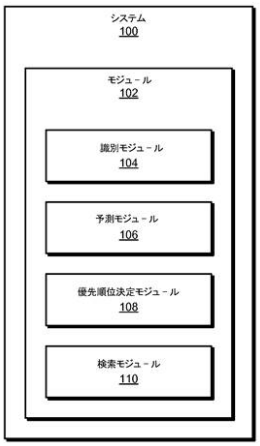

図１

【図２】

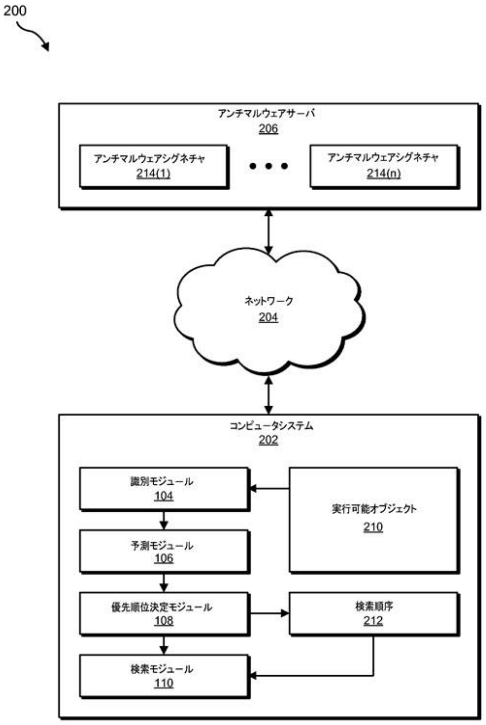

図２

【図３】

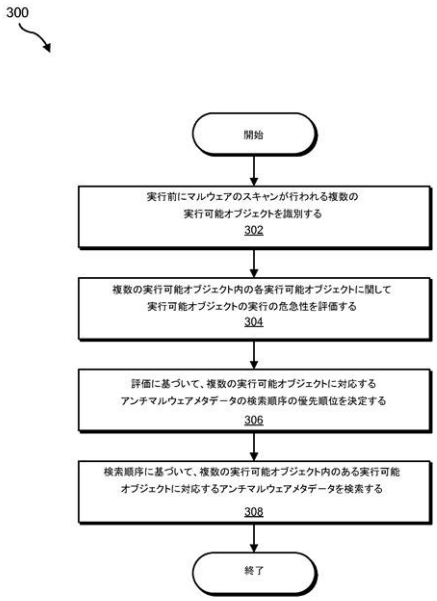

図３

【図４】

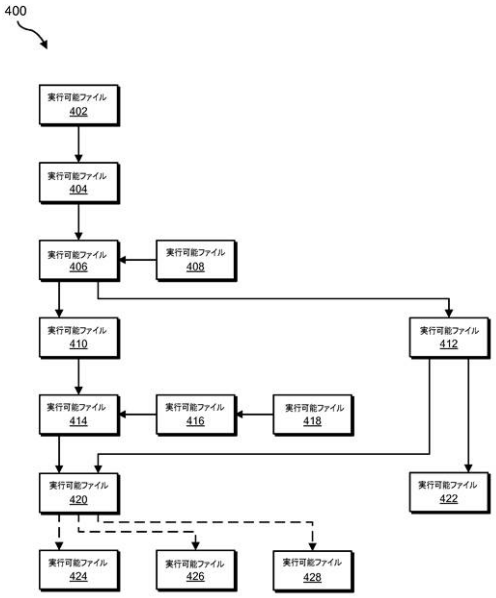

図４

【図５】

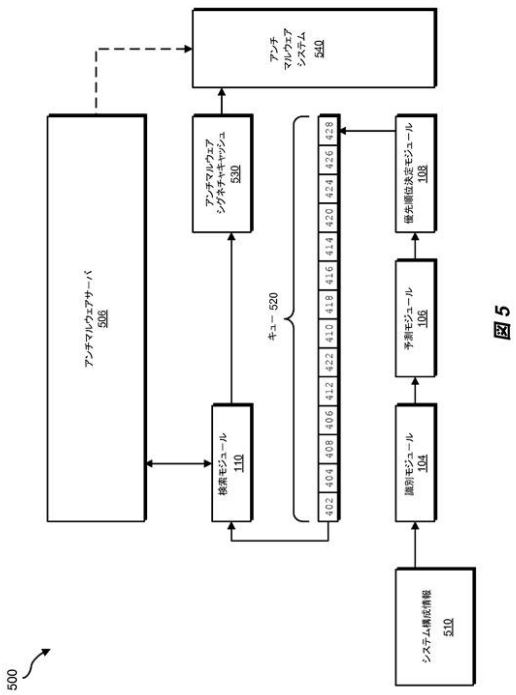

図５

【図６】

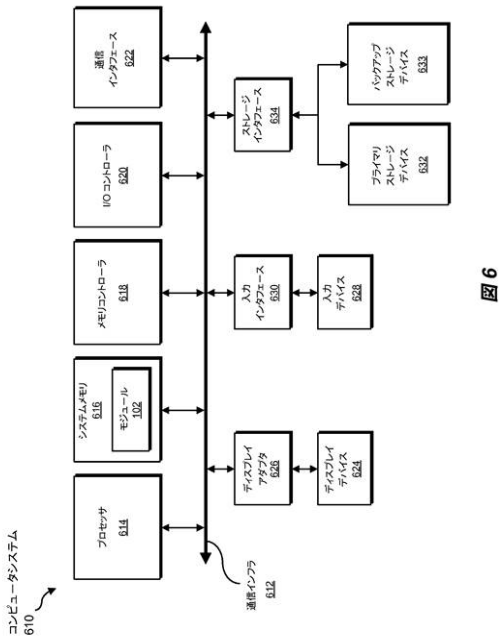

図６

【図７】

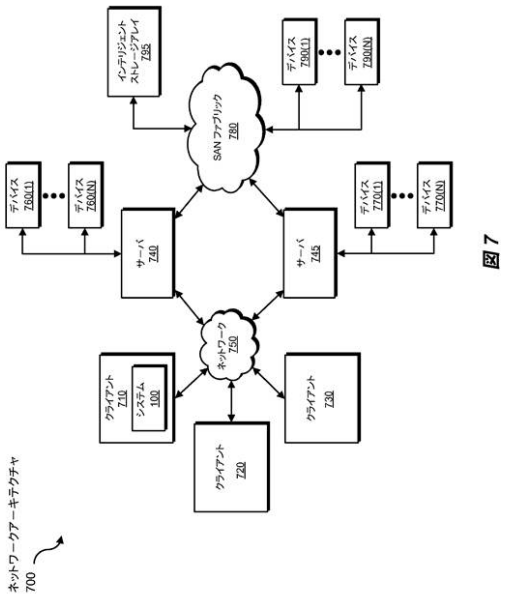
ネットワークアーキテクチャ
700
クライアント
Z10
システム
100
クライアント
Z20
クライアント
Z30
ネットワーク
Z50
サーバ
Z40
サーバ
Z45
SAN ファブリック
Z80
インテリジェント
ストレージアレイ
Z95
デバイス
Z60(1)
デバイス
Z60(N)
デバイス
Z70(1)
デバイス
Z70(N)
デバイス
Z90(1)
デバイス
Z90(N)

図７

フロントページの続き

(72)発明者　サティッシュ・ソーラブ
アメリカ合衆国　カリフォルニア州　９４５３６　フリーモント　ローラスコート　３７７９７

審査官　打出　義尚

(56)参考文献　米国特許出願公開第２００７／００７９３７７（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５６