(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5610451号
(P5610451)
(45)発行日　平成26年10月22日(2014.10.22)　(24)登録日　平成26年9月12日(2014.9.12)

(51)Int.Cl.　F I
G06F 21/56 (2013.01)　G06F 21/00 156A

請求項の数 20 (全 19 頁)

(21)出願番号	特願2012-528934 (P2012-528934)
(86)(22)出願日	平成22年9月10日 (2010.9.10)
(65)公表番号	特表2013-504824 (P2013-504824A)
(43)公表日	平成25年2月7日 (2013.2.7)
(86)国際出願番号	PCT/US2010/048475
(87)国際公開番号	WO2011/034792
(87)国際公開日	平成23年3月24日 (2011.3.24)
審査請求日	平成25年8月29日 (2013.8.29)
(31)優先権主張番号	12/560,261
(32)優先日	平成21年9月15日 (2009.9.15)
(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　100107456
弁理士　池田　成人
(74)代理人　100148596
弁理士　山口　和弘
(74)代理人　100123995
弁理士　野田　雅一

最終頁に続く

(54)【発明の名称】コンピュータファイルの評判スコアの個別有効期間

(57)【特許請求の範囲】
【請求項１】
ファイルの評判スコアの個別有効期間（ＴＴＬ）を生成する、コンピュータに実装される方法であって、前記評判スコアは、ファイルが悪意を有するか否かを判定するために利用され、前記方法は、
セキュリティシステムにおいて、クライアントシステムから要求を受信するステップであって、前記要求は、前記クライアントシステムにより識別されたファイルの識別子を有する、ステップと、
複数のクライアントシステムから受信した前記ファイルの評判情報に基づいて、前記ファイルの評判スコアを生成するステップであって、前記評判スコアは、前記ファイルの信頼度の評価を表している、ステップと、
複数のクライアントシステムから受信した前記ファイルの評判情報に基づいて、前記評判スコアの確信度スコアを判定するステップであって、前記確信度スコアは、前記評判スコアが前記ファイルの実際の信頼度を反映している尤度を示している、ステップと、
前記セキュリティシステムにおいて、複数のクライアントシステムから受信した前記ファイルの評判情報及び前記確信度スコアに基づいて前記評判スコアのＴＴＬを演算するステップであって、前記ＴＴＬは、前記評判スコアの有効期間を表しており、高い確信度スコアと関連する評判スコアのＴＴＬによって表される有効期間は、低い確信度スコアと関連する評判スコアのＴＴＬによって表される有効期間よりも長い、ステップと、
前記要求に応答して前記評判スコア及び前記ＴＴＬを前記クライアントシステムに送信

するステップと、
を含む、コンピュータに実装される方法。
【請求項２】
その範囲の両端部に位置した評判スコア又はその範囲の両端との差が所定の閾値以下の評判スコアの前記確信度スコアは、前記端部に位置してはいない評判スコアの前記確信度スコアよりも高い請求項１に記載の、コンピュータに実装される方法。
【請求項３】
前記評判スコアの前記確信度スコアを判定するステップは、
前記ファイルの年齢を判定するステップであって、老年ファイルと関連する評判スコアの前記確信度スコアは、若年ファイルと関連する評判スコアの前記確信度スコアよりも高い、ステップ
を含む請求項１に記載の、コンピュータに実装される方法。
【請求項４】
前記評判スコアの前記確信度スコアを判定するステップは、
クライアントシステム間における前記ファイルの普及度を判定するステップであって、普及しているファイルと関連する評判スコアの前記確信度スコアは、あまり普及していないファイルと関連する評判スコアの前記確信度スコアよりも高い、ステップ
を含む請求項１に記載の、コンピュータに実装される方法。
【請求項５】
前記評判スコアは、前記ＴＴＬによって表された前記有効期間中において、前記ファイルが悪意を有しているかどうかを判定するべく、前記クライアントシステムによって利用される請求項１に記載の、コンピュータに実装される方法。
【請求項６】
ファイルの評判スコアの個別有効期間（ＴＴＬ）を生成するコンピュータシステムであって、前記評判スコアは、ファイルが悪意を有するか否かを判定するために利用され、前記コンピュータシステムは、
セキュリティシステムにおける、クライアントシステムから要求を受信する通信手段であって、前記要求は、前記クライアントシステムにより識別されたファイルの識別子を有する、通信手段と、
複数のクライアントシステムから受信した前記ファイルの評判情報に基づいて、前記ファイルの評判スコアを生成する評判スコア生成手段であって、前記評判スコアは、前記ファイルの信頼度の評価を表している、評判スコア生成手段と、
複数のクライアントシステムから受信した前記ファイルの評判情報に基づいて、前記評判スコアの確信度スコアを判定する確信度判定手段であって、前記確信度スコアは、前記評判スコアが前記ファイルの実際の信頼度を反映している尤度を示している、確信度判定手段と、
複数のクライアントシステムから受信した前記ファイルの評判情報及び前記確信度スコアに基づいて前記評判スコアのＴＴＬを演算するＴＴＬ判定手段であって、前記ＴＴＬは、前記評判スコアの有効期間を表しており、高い確信度スコアと関連する評判スコアのＴＴＬによって表される有効期間は、低い確信度スコアと関連する評判スコアのＴＴＬによって表される有効期間よりも長い、ＴＴＬ判定手段と、
を有し、
前記通信手段は、前記要求に応答して前記評判スコア及び前記ＴＴＬを前記クライアントシステムに送信するべく更に構成されている、コンピュータシステム。
【請求項７】
その範囲の両端部に位置した評判スコア又はその範囲の両端との差が所定の閾値以下の評判スコアの前記確信度スコアは、前記端部に位置してはいない評判スコアの前記確信度スコアよりも高い請求項６に記載のコンピュータシステム。
【請求項８】
前記確信度判定手段は、

前記ファイルの年齢を判定する手段であって、老年ファイルと関連する評判スコアの前記確信度スコアは、若年ファイルと関連する評判スコアの前記確信度スコアよりも高い、手段を含む、
請求項６に記載のコンピュータシステム。
【請求項９】
前記確信度判定手段は、
クライアントシステム間における前記ファイルの普及度を判定する手段であって、普及しているファイルと関連する評判スコアの前記確信度スコアは、あまり普及していないファイルと関連する評判スコアの前記確信度スコアよりも高い、手段を含む、
請求項６に記載のコンピュータシステム。
【請求項１０】
前記評判スコアは、前記ＴＴＬによって表された前記有効期間中において、前記ファイルが悪意を有しているかどうかを判定するべく、前記クライアントシステムによって利用される請求項６に記載のコンピュータシステム。
【請求項１１】
ファイルの評判スコアの個別有効期間（ＴＴＬ）を生成する、コンピュータにより実行可能なコンピュータプログラムであって、前記評判スコアは、ファイルが悪意を有するか否かを判定するために利用され、前記コンピュータプログラムは、
コンピュータに、
セキュリティシステムにおいて、クライアントシステムから要求を受信するステップであって、前記要求は、前記クライアントシステムにより識別されたファイルの識別子を有する、ステップと、
複数のクライアントシステムから受信した前記ファイルの評判情報に基づいて、前記ファイルの評判スコアを生成するステップであって、前記評判スコアは、前記ファイルの信頼度の評価を表している、ステップと、
複数のクライアントシステムから受信した前記ファイルの評判情報に基づいて、前記評判スコアの確信度スコアを判定するステップであって、前記確信度スコアは、前記評判スコアが前記ファイルの実際の信頼度を反映している尤度を示している、ステップと、
前記セキュリティシステムにおいて、複数のクライアントシステムから受信した前記ファイルの評判情報及び前記確信度スコアに基づいて前記評判スコアのＴＴＬを演算するステップであって、前記ＴＴＬは、前記評判スコアの有効期間を表しており、高い確信度スコアと関連する評判スコアのＴＴＬによって表される有効期間は、低い確信度スコアと関連する評判スコアのＴＴＬによって表される有効期間よりも長い、ステップと、
前記要求に応答して前記評判スコア及び前記ＴＴＬを前記クライアントシステムに送信するステップと、
を実行させる、コンピュータプログラム。
【請求項１２】
その範囲の両端部に位置した評判スコア又はその範囲の両端との差が所定の閾値以下の評判スコアの前記確信度スコアは、前記端部に位置してはいない評判スコアの前記確信度スコアよりも高い請求項１１に記載の、コンピュータプログラム。
【請求項１３】
前記評判スコアの前記確信度スコアを判定するステップは、
前記ファイルの年齢を判定するステップであって、老年ファイルと関連する評判スコアの前記確信度スコアは、若年ファイルと関連する評判スコアの前記確信度スコアよりも高い、ステップ
を含む請求項１１に記載の、コンピュータプログラム。
【請求項１４】
前記評判スコアの前記確信度スコアを判定するステップは、
クライアントシステム間における前記ファイルの普及度を判定するステップであって、普及しているファイルと関連する評判スコアの前記確信度スコアは、あまり普及していな

いファイルと関連する評判スコアの前記確信度スコアよりも高い、ステップ
を含む請求項１１に記載のコンピュータプログラム。
【請求項１５】
前記ＴＴＬは、前記ファイルの異なる評判スコアを生成できるような追加情報を収集するのに要する時間の長さの評価を表す、
請求項１に記載のコンピュータに実装される方法。
【請求項１６】
前記ＴＴＬを演算するステップは、評判スコア及び確信度スコアの与えられた値に基づきＴＴＬの値を特定する表から、ＴＴＬを選択することを含む、
請求項１に記載のコンピュータに実装される方法。
【請求項１７】
前記クライアントシステムは、前記セキュリティシステムから送信されたＴＴＬを受信し、前記クライアントシステムのローカルなセキュリティポリシに基づき、前記セキュリティシステムから受信された前記ＴＴＬを変更するように構成されている、
請求項１に記載のコンピュータに実装される方法。
【請求項１８】
前記セキュリティシステムは、前記クライアントシステムから前記ＴＴＬを受信しない、
請求項１に記載のコンピュータに実装される方法。
【請求項１９】
前記セキュリティシステムは、前記クライアントシステムから前記ＴＴＬを受信しない、
請求項６に記載のコンピュータシステム。
【請求項２０】
前記セキュリティシステムは、前記クライアントシステムから前記ＴＴＬを受信しない、
請求項１１に記載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】
本開示は、一般に、コンピュータセキュリティの分野に関し、更に詳しくは、コンピュータファイルが悪意を有しているかどうかの判定に関する。
【背景技術】
【０００２】
現代のコンピュータは、悪意を有する様々なソフトウェア（マルウェア）の攻撃を受ける可能性がある。マルウェアの脅威には、コンピュータウイルス、ワーム、トロイの木馬プログラム、スパイウェア、アドウェア、クライムウェア、及びフィッシングウェブサイトが含まれる。悪意を有するエンティティは、しばしば、その悪意を有するエンティティ自体の利益のために使用可能な秘密又は機密データを保存するサーバーを攻撃する。ホームコンピュータを含むその他のコンピュータも、同様に、ユーザーがその他の人々と電子メールを介して通信する際に、ユーザーが新しいプログラム又はプログラムアップデートをダウンロードする際に、並びに、多くのその他の状況において送信されうる悪意を有するソフトウェアから、常時保護されなければならない。悪意を有するエンティティがコンピュータ上における攻撃のために利用することができる様々な選択肢及び方法は、多数に上る。
【０００３】
署名ストリングのスキャニングなどのマルウェアを検出する従来の技法は、その有効性を失いつつある。現代のマルウェアは、しばしば、相対的に少数のコンピュータのみをターゲットとし、且つ、それらに対してのみ供給される。例えば、トロイの木馬プログラムは、特定の企業の特定の部署内のコンピュータをターゲットにするように設計可能である

。このようなマルウェアにセキュリティアナリストが遭遇することは絶対にないであろうし、従って、セキュリティソフトウェアが、このようなマルウェアを検出するための署名によって構成されることも絶対にないであろう。一方、大量配布されるマルウェアの場合には、マルウェアのすべてのインスタンスを一意にする多形性を包含可能である。この結果、マルウェアのすべてのインスタンスを確実に検出する署名ストリングを開発することが困難である。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

マルウェアを検出するための新しい技法は、評判システムの使用を必要としている。評判システムは、ファイルがマルウェアである尤度を評価するべく、コンピュータ上において遭遇したファイルの評判を判定可能である。ファイルの評判を生成する1つの方法は、そのファイルが存在しているネットワークに接続されたコンピュータからレポートを収集し、且つ、そのレポートに含まれている情報に基づいて評判を生成するというものである。ファイルの評判は、収集されるレポートが増えるのに伴って、時間と共に変化可能である。評判スコアを使用してマルウェアを検出しているネットワークに接続されたコンピュータ及びその他のエンティティに対して変化する評判スコアを効率的に提供する方法に対するニーズが存在している。

【課題を解決するための手段】

【０００５】

本開示の実施形態は、コンピュータファイルの評判スコアの個別の有効期間（Ｔｉｍｅ－Ｔｏ－Ｌｉｖｅ：ＴＴＬ）を生成及び利用する方法（並びに、これに対応したシステム及びコンピュータプログラムプロダクト）を含む。

【０００６】

本開示の一態様は、ファイルの評判スコアの個別有効期間（ＴＴＬ）を生成するコンピュータ実装方法であり、この方法は、クライアントシステムから要求を受信するステップであって、要求は、ファイルの識別子を有する、ステップと、ファイルの評判スコアを生成するステップであって、評判スコアは、ファイルの信頼度の評価を表している、ステップと、評判スコアに基づいて評判スコアのＴＴＬを判定するステップであって、ＴＴＬは、評判スコアの有効期間を表している、ステップと、要求に応答して評判スコア及びＴＴＬをクライアントシステムに送信するステップと、を有する。

【０００７】

本開示の別の態様は、ファイルの評判スコアの個別有効期間（ＴＴＬ）を生成するコンピュータシステムであり、このコンピュータシステムは、クライアントシステムから要求を受信する通信モジュールであって、要求は、ファイルの識別子を有する、通信モジュールと、ファイルの評判スコアを生成する評判スコア生成モジュールであって、評判スコアは、ファイルの信頼度の評価を表している、評判スコア生成モジュールと、評判スコアに基づいてその評判スコアのＴＴＬを判定するＴＴＬ判定モジュールであって、ＴＴＬは、評判スコアの有効期間を表している、ＴＴＬ判定モジュールと、のための実行可能なコンピュータプログラムコードを有するコンピュータ可読ストレージ媒体を有し、通信モジュールは、要求に応答して評判スコア及びＴＴＬをクライアントシステムに送信するべく更に構成されている。

【０００８】

本開示の更に別の態様は、ファイルの評判スコアの個別有効期間（ＴＴＬ）を生成する実行可能なコンピュータプログラムコードによって符号化されたコンピュータ可読ストレージ媒体であり、コンピュータプログラムコードは、クライアントシステムから要求を受信するステップであって、要求は、ファイルの識別子を有する、ステップと、ファイルの評判スコアを生成するステップであって、評判スコアは、ファイルの信頼度の評価を表している、ステップと、評判スコアに基づいて評判スコアのＴＴＬを判定するステップであって、ＴＴＬは、評判スコアの有効期間を表している、ステップと、要求に応答して評判

スコア及びＴＴＬをクライアントシステムに送信するステップと、のためのプログラムコードを有する。

【０００９】

本明細書に記述されている特徴及び利点は、それらのすべてを網羅したものではなく、且つ、具体的には、図面、本明細書、及び特許請求の範囲の観点において、多くの更なる特徴及び利点が当業者に明らかとなろう。更には、本明細書に使用されている言語は、基本的に、可読性及び教育的な目的のために選択されたものであり、従って、開示されている主題を線引き又は制限するべく選択されたものではない場合があることに留意されたい。

【図面の簡単な説明】

【００１０】

【図１】本開示の一実施形態による演算環境のハイレベルブロック図である。

【図２】本開示の一実施形態による図１に示されている演算環境において使用されるコンピュータの一例を示すハイレベルブロック図である。

【図３】本開示の一実施形態によるセキュリティモジュール内のモジュールを示すハイレベルブロック図である。

【図４】本開示の一実施形態によるセキュリティシステム内のモジュールを示すハイレベルブロック図である。

【図５】本開示の一実施形態による評判スコア及びその評判スコアの個別有効期間（ＴＴＬ）に基づいてコンピュータファイルが悪意を有しているかどうかを判定するプロセスを示すフローチャートである。

【図６】本開示の一実施形態によるコンピュータファイルの現在の評判スコア及びその評判スコアの付随する個別ＴＴＬを連続的に生成するプロセスを示すフローチャートである。

【発明を実施するための形態】

【００１１】

図面及び以下の説明は、特定の実施形態を一例として表したものに過ぎない。当業者であれば、以下の説明から、本明細書に記述されている原理を逸脱することなしに、本明細書に示されている構造及び方法の代替実施形態を利用することも可能であることを容易に認識するであろう。以下、例が添付図面に示されているいくつかの実施形態を詳細に参照することとする。可能な場合には常に、類似の又は同一の参照符号が、図中において使用されると共に、類似の又は同一の機能を示すことになるということに留意されたい。

【００１２】

システム環境

図１は、本開示の一実施形態によるコンピュータファイルの評判スコアの個別有効期間（ＴＴＬ）を生成及び利用するための演算環境１００を示すハイレベルブロック図である。図示のように、演算環境１００は、ネットワーク１３０を通じて接続されたクライアントシステム１１０と、セキュリティシステム１２０と、を含む。以下の説明をわかりやすく且つ明瞭なものにするべく、それぞれのエンティティごとに、１つのみが示されている。演算環境１００内には、その他のエンティティも同様に存在可能である。

【００１３】

クライアントシステム１１０は、悪意を有するソフトウェアをホスティング可能な電子装置である。一実施形態において、クライアントシステム１１０は、例えば、Ｍｉｃｒｏｓｏｆｔ Ｗｉｎｄｏｗｓ互換オペレーティングシステム（ＯＳ）、Ａｐｐｌｅ ＯＳ Ｘ、及び／又はＬｉｎｕｘディストリビューションを実行する従来のコンピュータシステムである。別の実施形態においては、クライアントシステム１１０は、パーソナルデジタルアシスタント（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔ：ＰＤＡ）、携帯電話機、ビデオゲームシステムなどのコンピュータ機能を具備した別の装置である。クライアントシステム１１０は、通常、悪意を有するソフトウェアをホスティング可能な多数のコンピュータファイルを保存する。

【００１４】
しばしば、「マルウェア」とも呼ばれる悪意を有するソフトウェアは、一般に、クライアントシステム１１０上において秘密裏に実行される又はなんらかの秘密の機能を具備したソフトウェアとして規定される。マルウェアは、正規のファイルに付着する寄生ウイルス、コンピュータに感染すると共にその他のコンピュータにも拡散するべくコンピュータのセキュリティの脆弱性を活用するワーム、正規のもののように見えるが、実際には隠蔽された悪意を有するコードを含むトロイの木馬プログラム、及び機密情報を取得するか又は広告を表示するべくコンピュータ上におけるキーストローク及び／又はその他の動作を監視するスパイウェアなどの多数の形態を有することができる。
【００１５】
クライアントシステム１１０は、マルウェアの存在を検出するセキュリティモジュール１１５を実行する。セキュリティモジュール１１５は、例えば、コンピュータのＯＳに内蔵することも可能であり、或いは、別個の包括的なセキュリティパッケージの一部であってもよい。一実施形態においては、セキュリティモジュール１１５は、セキュリティシステム１２０を運営しているエンティティによって提供される。セキュリティモジュール１１５は、ネットワーク１３０を介してセキュリティシステム１２０と通信可能である。
【００１６】
一実施形態において、セキュリティモジュール１１５は、ファイルの評判スコアに対する要求をセキュリティシステム１２０に送信し、且つ、その返信として評判スコア及び関連するＴＴＬを受信する。セキュリティモジュール１１５は、ＴＴＬによって規定された（有効期間と呼ばれる）期間中において、受信した評判スコアと、ファイルの振る舞いの観察結果などのその他の要因と、に基づいて、そのファイルが悪意を有しているかどうかを判定し、且つ、その後に、評判スコアを破棄する。
【００１７】
評判スコアは、関連するファイルの信頼度の評価を表している。例えば、評判スコアは、０～１の範囲の連続した値であってよく、０のスコアは、非常に低い信頼度（例えば、ファイルが悪意を有していること）を示し、且つ、１のスコアは、非常に高い信頼度（例えば、ファイルが正規のものであること）を示す。
【００１８】
ＴＴＬは、関連する評判スコアが有効である期間を規定する。実施形態に応じて、ＴＴＬは、規定されたイベントの後の時間の長さとして規定することも可能であり（例えば、評判スコアは、クライアントシステム１１０がそのスコアを受信した後に１週間にわたって有効である）、明示的な日付として規定することも可能であり（例えば、評判スコアは、２０１２年７月１日まで有効である）、或いは、更に別の方式によって規定することも可能である。
【００１９】
セキュリティシステム１２０は、クライアントシステム１１０及びその他の供給源からコンピュータファイルに関する情報（例えば、その振る舞い）を受信し、それらのファイルの評判スコアを生成すると共に、評判スコア及びその評判スコアに対する確信度に基づいて関連するＴＴＬを判定するべく構成されたハードウェア装置及び／又はソフトウェアプログラムである。また、セキュリティシステム１２０は、特定のファイルの評判スコアに対する要求をクライアントシステム１１０から受信し、且つ、それに応答して、それらの現在の評判スコア及びＴＴＬを提供する。セキュリティシステム１２０の一例は、セキュリティモジュール１１５がクライアントシステム１１０上のマルウェアを検出及び除去できるようにするセキュリティソフトウェア及びサービスを提供するウェブに基づいたシステムである。
【００２０】
セキュリティシステム１２０は、ファイルの信頼度と相関した関係にある属性に基づいてファイルの評判スコアを生成する。例えば、セキュリティシステム１２０は、数例を挙げると、ファイルの１つ又は複数の供給源の評判（例えば、ファイルが評判の良いウェブ

サイトから又は評判の良くないウェブサイトからダウンロードされたかどうか）を分析可能であり、ファイルがデジタル署名によって署名されているかどうか（例えば、評判の良いエンティティによってデジタル署名されたファイルは、評判の良くないエンティティによって署名されたファイル又はデジタル署名を伴わないファイルよりも信頼することができる）を分析可能であり、且つ、ファイルがクライアントシステム１１０の間において普及しているかどうかを分析可能である。

【００２１】

セキュリティシステム１２０は、生成された評判スコアの確信度スコアを判定する。確信度スコアは、セキュリティシステム１２０が評判スコアに対して具備している確信度（即ち、基礎をなすファイル（ｕｎｄｅｒｌｙｉｎｇ　ｆｉｌｅ）の真の信頼度を評判スコアが反映している尤度）を示す。例えば、確信度スコアは、０～１の範囲の連続的な値であってよく、０のスコアは、非常に低い確信度（例えば、評判スコアの通知値が非常に小さいこと）を示し、且つ、１のスコアは、非常に高い確信度（例えば、基礎をなすファイルの真の信頼度を評判スコアがほとんど確実に反映していること）を示す。

【００２２】

セキュリティシステム１２０は、評判スコアの値、基礎をなすファイルの年齢（即ち、セキュリティシステム１２０がそのファイルについて認知している期間の長さ）、及びセキュリティシステム１２０のユーザーベースにおけるファイルの普及度などの、生成された評判スコアに対する確信度に相関した関係を有する属性に基づいて確信度スコアを判定する。

【００２３】

セキュリティシステム１２０は、ファイルの信頼度（即ち、評判スコア）及びその評判スコアの確信度スコアに相関した関係を有する属性に基づいてＴＴＬを演算する。一般に、セキュリティシステム１２０は、高い確信度スコアを有する評判スコアに対しては、長期のＴＴＬを設定し、且つ、低い確信度スコアを有する評判スコアに対しては、短期のＴＴＬを設定する。即ち、ＴＴＬは、セキュリティシステム１２０がそのファイルの実質的に異なる評判スコアを生成できるようにする十分な追加的関連情報を収集するためにセキュリティシステム１２０が所要した時間の長さの評価を表している。ファイルの信頼度の評価が長期間にわたって変化する可能性が低い場合には、ＴＴＬは、長くなり、且つ、さもなれば、短くなる。高い確信度スコアを有する評判スコアに対して長期のＴＴＬを設定することにより、クライアントシステム１１０は、セキュリティシステム１２０に対してアップデートを要求する前に、その評判スコアに長期間にわたって依存することになる。

【００２４】

また、セキュリティシステム１２０の機能のうちの１つ又は複数のものは、クライアントシステム１１０上又はクラウド演算環境内において実行することも可能である。本明細書に使用されているクラウド演算とは、動的にスケーラブルであると共に多くの場合に仮想化されているリソースがインターネット上においてサービスとして提供されるスタイルの演算を意味している。従って、クラウド演算の顧客は、一般に、対象のソフトウェアプラットフォームに対するホストとして機能する物理的なインフラストラクチャを所有する代わりに、第三者のプロバイダからリソースを借りて使用しており、これらのリソースをサービスとして消費し、且つ、使用したリソースについてのみ対価を支払う。

【００２５】

ネットワーク１３０より、クライアントシステム１１０とセキュリティシステム１２０は、通信可能である。一実施形態において、ネットワーク１３０は、標準的な通信技術及び／又はプロトコルを使用している。即ち、ネットワーク１３０は、Ｅｔｈｅｒｎｅｔ、８０２．１１、ＷｉＭＡＸ（Ｗｏｒｌｄｗｉｄｅ　Ｉｎｔｅｒｏｐｅｒａｂｉｌｉｔｙ　ｆｏｒ　Ｍｉｃｒｏｗａｖｅ　Ａｃｃｅｓｓ）、３Ｇ、ＤＳＬ（Ｄｉｇｉｔａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｌｉｎｅ）、ＡＴＭ（Ａｓｙｎｃｈｒｏｎｏｕｓ　Ｔｒａｎｓｆｅｒ　Ｍｏｄｅ）、ＩｎｆｉｎｉＢａｎｄ、ＰＣＩ　Ｅｘｐｒｅｓｓ　Ａｄｖａｎｃｅｄ　Ｓｗｉｔｃｈｉｎｇなどの技術を使用したリンクを包含可能である。同様に、ネットワーク１

３０上において使用されるネットワーキングプロトコルは、ＭＰＬＳ（Ｍｕｌｔｉｐｒｏｔｏｃｏｌ Ｌａｂｅｌ Ｓｗｉｔｃｈｉｎｇ）、ＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）、ＵＤＰ（Ｕｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ）、ＨＴＴＰ（Ｈｙｐｅｒｔｅｘｔ Ｔｒａｎｓｐｏｒｔ Ｐｒｏｔｏｃｏｌ）、ＳＭＴＰ（Ｓｉｍｐｌｅ Ｍａｉｌ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）、ＦＴＰ（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）などを包含可能である。ネットワーク１３０上において交換されるデータは、ＨＴＭＬ（ＨｙｐｅｒＴｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）やＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）などを含む技術及び／又はフォーマットを使用して表現可能である。更には、リンクのすべて又は一部は、ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ）、ＴＬＳ（Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）、ＶＰＮ（Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）、及びＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ ｓｅｃｕｒｉｔｙ）などの従来の暗号化技術を使用して暗号化可能である。別の実施形態においては、エンティティは、前述のものの代わりに又はそれらに加えて、カスタム及び／又は専用データ通信技術を使用可能である。また、実施形態に応じて、ネットワーク１３０は、インターネットなどのその他のネットワークに対するリンクを包含することも可能である。

【００２６】

コンピュータアーキテクチャ

図１に示されているエンティティは、１つ又は複数のコンピュータを使用して実装される。図２は、例示用のコンピュータ２００を示すハイレベルブロック図である。コンピュータ２００は、チップセット２０４に結合された少なくとも１つのプロセッサ２０２を含む。チップセット２０４は、メモリコントローラハブ２２０と、入出力（Ｉ／Ｏ）コントローラハブ２２２と、を含む。メモリ２０６及びグラフィックスアダプタ２１２は、メモリコントローラハブ２２０に結合されており、且つ、グラフィックスアダプタ２１２には、ディスプレイ２１８が結合されている。ストレージ装置２０８、キーボード２１０、ポインティング装置２１４、及びネットワークアダプタ２１６は、Ｉ／Ｏコントローラハブ２２２に結合されている。コンピュータ２００のその他の実施形態は、異なるアーキテクチャを有する。

【００２７】

ストレージ装置２０８は、ハードドライブ、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｋ Ｒｅａｄ－Ｏｎｌｙ Ｍｅｍｏｒｙ）、ＤＶＤ、又は半導体メモリ装置などのコンピュータ可読ストレージ媒体である。メモリ２０６は、プロセッサ２０２によって使用される命令及びデータを保持する。ポインティング装置２１４は、マウス、トラックボール、又はその他のタイプのポインティング装置であり、且つ、データをコンピュータシステム２００に入力するべく、キーボード２１０との組合せにおいて使用される。グラフィックスアダプタ２１２は、画像及びその他の情報をディスプレイ２１８上に表示する。ネットワークアダプタ２１６は、コンピュータシステム２００を１つ又は複数のコンピュータネットワークに結合する。

【００２８】

コンピュータ２００は、本明細書に記述されている機能を提供するコンピュータプログラムモジュールを実行するべく適合されている。本明細書に使用されている「モジュール」という用語は、規定された機能を提供するべく使用されるコンピュータプログラムロジックを意味している。従って、モジュールは、ハードウェア、ファームウェア、及び／又はソフトウェアに実装可能である。一実施形態において、プログラムモジュールは、ストレージ装置２０８上に保存され、メモリ２０６内に読み込まれ、且つ、プロセッサ２０２によって実行される。

【００２９】

図１のエンティティによって使用されるコンピュータ２００のタイプは、実施形態と、そのエンティティが必要としている処理能力とに応じて、変化可能である。例えば、セキ

ュリティシステム１２０は、本明細書に記述されている機能を提供するべく協働する複数のブレードサーバーを有してもよい。別の例として、クライアントシステム１１０は、限られた処理能力を有する携帯電話機を有してもよい。コンピュータ２００が、キーボード２１０、グラフィックスアダプタ２１２、及びディスプレイ２１８などの前述のコンポーネントのうちのいくつかを欠くことも可能である。

【００３０】

セキュリティモジュールのアーキテクチャ例の概要

図３は、一実施形態によるセキュリティモジュール１１５内のモジュールの詳細な図を示すハイレベルブロック図である。セキュリティモジュール１１５のいくつかの実施形態は、本明細書に記述されているものとは異なる及び／又はそれら以外のモジュールを有する。同様に、機能も、その他の実施形態によれば、本明細書に記述されているものとは異なる方式により、モジュール間において分散させることができる。図示のように、セキュリティモジュール１１５は、ファイルモニタモジュール３１０と、セキュリティ分析エンジン３２０と、通信モジュール３３０と、データストア３４０と、を含む。

【００３１】

ファイルモニタモジュール３１０は、クライアントシステム１１０内のコンピュータファイルを継続的に監視し、且つ、それらの供給源（例えば、それらのファイルがダウンロードされた元のウェブサイト）、デジタル署名、振る舞い、並びに、生成日付及び最新の変更日付などのシステムプロパティなどの関連情報を収集する。このような関連情報は、関連ファイルの「メタデータ」と集合的に呼称される。

【００３２】

セキュリティ分析エンジン３２０は、これらのメタデータ及び評判スコアなどの要因に基づいて、監視対象のファイルが悪意を有しているかどうかを判定する。一実施形態において、セキュリティ分析エンジン３２０は、疑わしい振る舞い（例えば、システムレジストリに対する書き込みの試み）が、あるファイルについて観察された際に、そのファイルに関する判定を実行する。例えば、セキュリティ分析エンジン３２０は、レジストリへの書き込みを試みる良好な評判（即ち、高い評判スコア）を有する第１ファイルは、恐らくは、マルウェアではなく、且つ、レジストリへの書き込みを試みる不良な評判（即ち、低い評判スコア）を有する第２ファイルは、恐らくは、マルウェアであると判定可能である。

【００３３】

ファイルが評判スコアを具備していない場合、又はファイルの評判スコアが失効している（即ち、そのＴＴＬがそのように示している）場合には、セキュリティ分析エンジン３２０は、通信モジュール３３０との間において調整を行い、現在の評判スコア及び関連するＴＴＬをセキュリティシステム１２０に対して要求する。あるいは、ファイルが有効な評判スコアと関連付けられている（例えば、有効期間が終了していない）場合には、セキュリティ分析エンジン３２０は、評判スコア及びメタデータなどのその他の要因に基づいて、そのファイルが悪意を有しているかどうかを判定する。

【００３４】

一実施形態において、セキュリティ分析エンジン３２０は、悪意を有すると判定されたファイルのブラックリストと、正規のものであると判定されたファイルのホワイトリストと、を生成する。例えば、以降の評判スコアの変化に起因してファイルの判定内容（即ち、ファイルが悪意を有するかどうか）が変化した場合には、セキュリティ分析エンジン３２０は、ブラックリスト及び／又はホワイトリストを相応して更新する。

【００３５】

通信モジュール３３０は、監視対象のファイルの評判スコア及び対応するＴＴＬを判定するべくセキュリティシステム１２０と通信する。通信モジュール３３０は、ファイルの識別子（例えば、デジタル指紋）及び関係する情報（例えば、メタデータ）をセキュリティシステム１２０に送信し、且つ、これに応答して評判スコア及び付随するＴＴＬを受信する。一実施形態においては、識別子の代わりに又はこれに加えて、ファイル自体をセキ

ュリティシステム１２０に送信可能である。通信モジュール３３０は、ファイルのその他の関連情報と共に、評判スコア及びＴＴＬをデータストア３４０内に保存する。

【００３６】

データストア３４０は、クライアントシステム１１０によって使用されるデータを保存する。このようなデータの例には、クライアントシステム１１０上に存在しているコンピュータファイルの識別子及びそれらのメタデータ、評判スコア及び関連するＴＴＬ、並びに、セキュリティシステム１２０に関する情報（例えば、ＩＰアドレス）が含まれる。データストア３４０は、リレーショナルデータベース又は任意のその他のタイプのデータベースであってよい。

【００３７】

セキュリティシステムのアーキテクチャ例の概要

図４は、一実施形態によるセキュリティシステム１２０内のモジュールの詳細な図を示すハイレベルブロック図である。セキュリティシステム１２０のいくつかの実施形態は、本明細書に記述されているものとは異なるモジュール及び／又はそれら以外のモジュールを有する。同様に、機能も、その他の実施形態によれば、本明細書に記述されているものとは異なる方式により、モジュール間において分散させることができる。図示のように、セキュリティシステム１２０は、通信モジュール４１０と、評判スコア生成モジュール４２０と、確信度判定モジュール４３０と、ＴＴＬ判定モジュール４４０と、データストア４５０と、を含む。

【００３８】

通信モジュール４１０は、クライアントシステム１１０上において稼働しているセキュリティモジュール１１５から問合せを受信し、且つ、セキュリティモジュール１１５に応答を提供する。問合せは、コンピュータファイルの識別子を含み、且つ、そのファイルのメタデータを包含してもよい。応答は、識別されたファイルの評判スコアと、その評判スコアのＴＴＬと、を含む。相応して、通信モジュール４１０は、現在の評判スコア及び関連するＴＴＬについて評判スコア生成モジュール４２０及びＴＴＬ判定モジュール４４０にコンタクトする。また、通信モジュール４１０は、コンピュータファイルに関係する情報をクライアントシステム１１０及びその他のリソースから受信し、且つ、受信した情報をデータストア４５０内に保存する。

【００３９】

評判スコア生成モジュール４２０は、コンピュータファイルの評判スコアを生成する。前述のように、評判スコアとは、関連するファイルの信頼度の評価である。評判スコア生成モジュール４２０は、ファイルの信頼度に相関した関係を有する属性に基づいて評判スコアを生成する。このような属性の例には、例えば、セキュリティシステム１２０のユーザーベース間におけるファイルの普及度（又は、人気）、そのファイルの供給源の評判、そのファイルを有する同一クライアントシステム１１０上に存在するその他のファイルの評判スコア、及びそのファイルの振る舞いの観察結果が含まれる。一実施形態においては、評判スコア生成モジュール４２０は、コンピュータファイルに関する要求及び情報がクライアントシステム１１０及びその他の供給源から受信されるのに伴って、評判スコアを連続的に生成する。

【００４０】

確信度判定モジュール４３０は、評判スコア生成モジュール４２０によって生成された評判スコアの確信度スコアを判定する。前述のように、確信度スコアは、生成された評判スコアに対してセキュリティシステム１２０が具備している確信度を示している。確信度判定モジュール４３０は、生成された評判スコアに対する確信度に相関した関係を有する属性に基づいて確信度スコアを判定する。このような属性の例には、評判スコアの値、ファイルの年齢（即ち、セキュリティシステム１２０がそのファイルについて認知している期間の長さ）、及びセキュリティシステム１２０のユーザーベース間におけるそのファイルの普及度が含まれる。

【００４１】

範囲の端部又はその近傍に位置した評判スコアは、時間に伴って大幅に変化する可能性が低いため、評判スコアに対する高い確信度の通知として機能する。例えば、評判スコアが、範囲の下端である０に近い場合には、これは、関連するファイルがほとんど確実に悪意を有していることを通知しており、評判スコアが時間に伴って大幅に変化する可能性はゼロに近い。一実施形態においては、評判スコアは、極度（０．９５超過又は０．０５未満）、決定的（０．９５と０．８の間又は０．０５と０．２の間）、かろうじて決定的（０．７と０．８の間又は０．２と０．３の間）、及び非決定的（０．３と０．７の間）という各評判帯域に分類される。

【００４２】

セキュリティシステム１２０がファイルについて認知している時間の長さは、ファイルの評判スコアに対する確信度の別のインジケータである。ファイルが、セキュリティシステム１２０にとって相対的に新しいものである場合には、セキュリティシステム１２０が、恐らくは、その信頼度の良好な評価を実施するための十分な情報をまだ収集していないことから、評判スコアの確信度は低い。ファイルがセキュリティシステム１２０にとって慣れ親しんだものとなるのに伴って、セキュリティシステム１２０は、相対的に多くの情報を収集している可能性が高く、従って、相対的に良好な評価を実施可能であるため、評判スコアに対する確信度が上昇する。更には、セキュリティシステム１２０が長期間にわたってファイルについて認知している場合には、評判スコアを大幅に変更することになる新しい情報が近い将来に現れる可能性が小さい。一実施形態においては、ファイルの年齢は、老年（６ヶ月超過）、中年（６ヶ月以下、３ヶ月超過）、若年（３ヶ月以下、１．５ヶ月超過）、非常に若年（１．５ヶ月以下）という各年齢帯域に分類される。

【００４３】

セキュリティシステム１２０のユーザーベースにおけるファイルの普及度も、ファイルの評判スコアに対する確信度のインジケータである。相対的に普及しているファイルは、セキュリティシステム１２０によって相対的に十分に認知されている傾向を有し、且つ、その結果、セキュリティシステム１２０は、それらの普及したファイルに関する相対的に多くの情報を有する傾向を有し、この結果、それらの評判スコアの確信度が上昇する。一実施形態においては、ファイルの普及度は、非常に高い（５００００マシン超過）、高い（５００００以下、２５０００超過）、中程度（２５０００以下、１００００超過）、低い（１００００以下、１０００超過）、非常に低い（１０００以下）という各普及度帯域に分類される。

【００４４】

確信度判定モジュール４３０は、前述のものなどの複数の確信度インジケータを総合的に考慮することにより、確信度スコアを判定する。例えば、確信度判定モジュール４３０は、次表を検討することにより、確信度スコアを判定可能である。

【００４５】

【表１】

普及度	年齢	評判	確信度スコア
中程度	老年	非決定的	非常に高い
非常に高い	老年	極度	非常に高い
高い	老年	決定的	非常に高い
中程度	中年	かろうじて決定的	高い
高い	若年	かろうじて決定的	低い
低い	若年	極度	低い
非常に低い	非常に若年	かろうじて決定的	低い
非常に低い	非常に若年	極度	低い
非常に低い	非常に若年	かろうじて決定的	非常に低い
非常に低い	非常に若年	非決定的	非常に低い

【００４６】
確信度判定モジュール４３０は、ファイルの属性がそれぞれのカテゴリにおいて規定されているものを満足又は超過している表中の（上から下への方向において）第１の行からそのファイルの評判スコアの確信度スコアを取得可能である。単純化すると、上述の表を使用して判定される確信度スコアは、非常に高い、高い、低い、及び非常に低いという４つの値のうちの１つを有する。
【００４７】
ＴＴＬ判定モジュール４４０は、評判スコア生成モジュール４２０によって生成された評判スコアのＴＴＬを判定する。前述のように、ＴＴＬは、その関連する評判スコアの有効期間を表している。ＴＴＬ判定モジュール４４０は、関連する評判スコア及びその評判スコアについて判定された確信度スコアに基づいてＴＴＬを判定する。前述の例を継続すれば、ＴＴｌ判定モジュール４４０は、同様の方式により、次表を検討することにより、ＴＴＬを判定可能である。
【００４８】
【表２】

評判	確信度スコア	TTL
決定的	**非常に高い**	**１年**
かろうじて決定的	**高い**	**１ヶ月**
かろうじて決定的	**低い**	**１週間**
非決定的	**非常に低い**	**１日**

【００４９】
単純化すると、上述の表を使用して判定されるＴＴＬは、１年、１ヶ月、１週間、及び１日という４つの値のうちの１つを有する。
【００５０】
データストア４５０は、セキュリティシステム１２０によって使用されるデータを保存する。このようなデータの例には、例えば、コンピュータファイル（例えば、デジタル指紋などの識別子、メタデータ、過去／現在の評判スコア及びＴＴＬ）、ウェブサイト、デジタル署名、及びクライアントシステム１１０に関連した情報が含まれる。ファイルに関連した情報をファイル識別子によって１つにグループ化及びインデックス付けし、迅速な検索を促進することも可能である。データストア３４０と同様に、データストア４５０は、リレーショナルデータベース又は任意のその他のタイプのデータベースであってよい。
【００５１】
セキュリティモジュール用の方法の概要
図５は、一実施形態による評判スコア及びその評判スコアの個別ＴＴＬに基づいてコンピュータファイルが悪意を有しているかどうかを判定するためのセキュリティモジュール１１５用のプロセス５００を示すフローチャートである。その他の実施形態は、異なる順序においてプロセス５００の各ステップを実行可能である。更には、その他の実施形態は、本明細書に記述されているものとは異なる及び／又は更なるステップを包含可能である。
【００５２】
まず、クライアントシステム１１０上において稼働しているセキュリティモジュール１１５は、セキュリティ検査のために、コンピュータファイルを識別する（５１０）。例えば、セキュリティモジュール１１５は、システム１１０上に存在するファイルを監視し、監視対象のファイルのうちの１つによる疑いのある活動の実行の試みを観察し、且つ、セキュリティ検査のために、そのファイルを識別する（５１０）。
【００５３】
セキュリティモジュール１１５は、利用可能な有効な評判スコアを識別されたファイル

が具備しているかどうかを判定する（５２０）。例えば、セキュリティモジュール１１５は、識別されたファイルと関連する評判スコア及び付随するＴＴＬの存在について、データストア３４０内をサーチする。そのような評判スコアが存在しないか又は利用可能な評判スコアが既に失効している（ＴＴＬがそのように示している）場合には、セキュリティモジュール１１５は、有効な評判スコアが利用不能な状態にあると判定する（５２０）。あるいは、識別されたファイルの評判スコアがデータストア３４０内に存在しており、且つ、付随するＴＴＬによって規定された有効期間が終了していない場合には、セキュリティモジュール１１５は、その評判スコアが、その識別されたファイルの信頼度の有効な評価であると仮定し、且つ、その識別されたファイルが、利用可能な有効な評判スコアを具備していると判定する（５２０）。

【００５４】

セキュリティモジュール１１５が、その識別されたファイルの利用可能な有効な評判スコアを具備している場合には、セキュリティモジュール１１５は、評判スコアと、その識別されたファイルの振る舞いの観察結果などのその他の要因とに基づいて、そのファイルが悪意を有しているかどうかを判定する（５５０）。セキュリティモジュール１１５は、ファイルが悪意を有していると判定されたかどうかに基づいて、その識別されたファイルによる疑いのある活動の実行の試みを許容するかどうかを更に判定可能である。

【００５５】

有効な評判ファイルが利用不能な状態にある場合には、セキュリティモジュール１１５は、その識別されたファイルの評判スコアをセキュリティシステム１２０に対して要求する（５３０）。例えば、セキュリティモジュール１１５は、ファイルの識別子（例えば、デジタル指紋）を含む要求をセキュリティシステム１２０に送信する。また、セキュリティモジュール１１５は、セキュリティシステム１２０に対して、要求と共に、その識別されたファイルのメタデータ（例えば、振る舞いの観察結果）を送信してもよい。その結果、セキュリティモジュール１１５は、要求５３０に応答して、セキュリティシステム１２０から評判スコア及び付随するＴＴＬを受信する（５４０）。セキュリティモジュール１１５がセキュリティシステム１２０から評判スコアを受信したら、セキュリティモジュール１１５は、前述のように、そのファイルが悪意を有しているかどうかを判定する（５５０。

【００５６】

セキュリティシステム用の方法の概要

図６は、一実施形態によるコンピュータファイルの現在の評判スコア及びその評判スコアの付随する個別ＴＴＬを連続的に生成するためのセキュリティシステム１２０用のプロセス６００を示すフローチャートである。その他の実施形態は、本明細書に記述されているものとは異なるステップ及び／又は更なるステップを包含可能である。

【００５７】

セキュリティシステム１２０は、コンピュータファイルに関連した情報を受信する（６１０）。関連した情報の例には、例えば、コンピュータファイルの識別子（例えば、デジタル署名）、振る舞いの観察結果、１つ又は複数の供給源、普及度（例えば、そのファイルをホスティングしているクライアントシステム１１０）、及び年齢（例えば、ファイルが特定のクライアントシステム１１０上に存在している期間の長さ）が含まれる。セキュリティシステム１２０は、クライアントシステム１１０上において稼働しているセキュリティモジュール１１５、データストア４５０、及びその他の供給源などの供給源から情報を受信する（６１０）。セキュリティシステム１２０は、セキュリティモジュール１１５から受信した関連情報をデータストア４５０内に保存する。

【００５８】

セキュリティシステム１２０は、受信した情報に基づいて、そのファイルの現在の評判スコアを生成し（６２０）、生成した評判スコアの確信度スコアを判定し（６３０）、且つ、評判スコア及び確信度スコアを含む要因に基づいて、生成された評判スコアのＴＴＬを判定する（６４０）。この評判スコアは、そのコンピュータファイルの現在の評判スコ

アとして、ＴＴＬ及び確信度スコアと共に、データストア４５０内に保存可能である。
【００５９】
プロセス６００は、ファイルの新しく受信された関連情報を反映した更新済みの評判スコア及びＴＴＬを生成するべく継続的に反復される。セキュリティシステム１２０は、新しい関連情報が受信された際に、ファイルの現在の評判スコア及びＴＴＬに対する要求を受信した際に、或いは、既定の時間間隔において、プロセス６００を反復可能である。例えば、セキュリティシステム１２０は、ファイルの評判スコアに対する要求をそのファイルのメタデータと共にセキュリティモジュール１１５から受信し（６１０）、その受信したメタデータを考慮して評判スコアを生成し（６２０）、且つ、確信度スコア及びＴＴＬを判定し（６３０、６４０）、評判スコア及びＴＴＬをセキュリティモジュール１１５に対して返す。
【００６０】
この方法は、評判スコアに対する確信度を反映したファイルの属性に基づいて特定のファイルの評判スコアの個別ＴＴＬをインテリジェントに判定している。この結果、良好である又は不良である可能性が非常に高いファイル（即ち、確信度が高い評判スコアを有するファイル）についてセキュリティモジュール１１５がセキュリティシステム１２０に対して送信する要求の数が低減され、且つ、従って、クライアントシステム１１０及びセキュリティシステム１２０の性能が改善される。従って、この方法は、個別ＴＴＬを利用することにより、有利には、満足のゆくリアルタイムセキュリティのクライアントシステム１１０に対する提供と、バックエンド性能及びスケーラビリティの維持と、の間におけるトレードオフを実現している。
【００６１】
更なる実施形態
一実施形態においては、クライアントシステム１１０がコンピュータファイルの評判スコア及びＴＴＬをローカルに生成し、それらのＴＴＬが失効する時点まで評判スコアを再生成しないように、セキュリティシステム１２０の少なくとも一部をクライアントシステム１１０上において稼働するセキュリティモジュール１１５内において実装可能である。
【００６２】
別の実施形態においては、セキュリティシステム１２０によって提供されるＴＴＬを、クライアントシステム１１０により、そのローカルなセキュリティポリシーに基づいて更にカスタマイズ可能である。例えば、クライアントシステム１１０が（例えば、インターネットカフェ内のコンピュータなどのように）低レベルのセキュリティポリシーを実施している場合には、クライアントシステム１１０は、既定の且つカスタマイズされた倍率だけ、評判スコアのＴＴＬを延長可能である。その一方で、クライアントシステム１１０が厳格なローカルセキュリティポリシーを実施している場合には、クライアントシステム１１０は、セキュリティシステム１２０によって提供されるＴＴＬを低減してもよい。
【００６３】
上述の説明のいくつかの部分は、アルゴリズム的なプロセス又は動作の観点において実施形態を表している。これらのアルゴリズム的な記述及び表現は、一般に、当業者が自身の研究内容を当業者に対して効率的に伝達するべく、データ処理分野の当業者によって使用されるものである。これらの動作は、機能的に、演算的に、又は論理的に記述されているが、これらは、プロセッサ又は等価な電気回路による実行のための命令を有するコンピュータプログラム、マイクロコード、又はこれらに類似したものによって実装されるものと理解されたい。更には、しばしば、一般性を失うことなしに、これらの機能的な動作の集合体をモジュールと呼称することが便利であることが証明されている。記述されている動作及びそれらの関連するモジュールは、ソフトウェア、ファームウェア、ハードウェア、又はこれらの任意の組合せとして実施可能である。
【００６４】
本明細書に使用されている「一実施形態」又は「実施形態」に対する参照は、その実施形態との関連において記述されている特定の要素、特徴、構造、又は特性が少なくとも１

つの実施形態に含まれていることを意味している。本明細書の様々な箇所における「一実施形態において」という文言の出現は、必ずしも、それらのすべてが同一の実施形態を参照するものではない。

【００６５】

いくつかの実施形態は、「結合された」及び「接続された」という表現をこれらの表現の派生物と共に使用することによって記述されている場合がある。これらの用語は、互いの同義語として意図されてはいないことを理解されたい。例えば、いくつかの実施形態は、複数の要素が相互の間において直接的な物理的又は電気的接触状態にあることを示すべく、「接続された」という用語を使用して記述される場合がある。別の例においては、いくつかの実施形態は、複数の要素が直接的な物理的又は電気的接触状態にあることを示すべく、「結合された」という用語を使用して記述される場合がある。但し、「結合された」という用語は、複数の要素が相互の間における直接的な接触状態にはないが、依然として、相互に協働又は相互作用することを意味している場合もある。実施形態は、この文脈に限定されるものではない。

【００６６】

本明細書に使用されている「含む／（ｃｏｍｐｒｉｓｅｓ、ｃｏｍｐｒｉｓｉｎｇ）」、「含む（ｉｎｃｌｕｄｅｓ、ｉｎｃｌｕｄｉｎｇ）」、「有する（ｈａｓ，ｈａｖｉｎｇ）」、又はこれらの任意のその他の変形は、非排他的な包含を意味するように意図されている。例えば、要素のリストを有するプロセス、方法、物品、又は装置は、必ずしも、それらの要素にのみ限定されるものではなく、明示的に列挙されていない又はそのようなプロセス、方法、物品、又は装置に固有のその他の要素をも含む場合がある。更には、明示的に特記されていない限り、「又は」は、包含的論理和を意味しており、且つ、排他的論理和を意味してはいない。例えば、条件Ａ又はＢは、Ａが真であり（又は、存在し）、且つ、Ｂが偽である（又は、存在しない）と、Ａが偽であり（又は、存在していない）、且つ、Ｂが真である（又は、存在している）と、Ａ及びＢの両方が真である（又は、存在している）と、といううちの任意のものによって満足される。

【００６７】

更には、本明細書においては、実施形態の要素及びコンポーネントを表すべく、「１つの（ａ又はａｎ）」が使用されている。これは、利便のために、且つ、開示の一般的な意味を付与するべく、行われているものに過ぎない。この表現は、１つ又は少なくとも１つを含むと判読することを要し、且つ、単数形は、そうでないことが明白に意味されていない限り、複数形をも含む。

【００６８】

当業者は、本開示を参照した際に、コンピュータファイルの評判スコアの個別ＴＴＬを生成及び利用するシステム及びプロセスの更なる構造的及び機能的代替設計について理解するであろう。従って、以上においては、特定の実施形態及び用途が図示及び説明されているが、本発明は、本明細書に記述されている構造及びコンポーネントそのままに限定されるものではなく、且つ、添付の請求項に規定されている精神及び範囲を逸脱することなしに、本明細書に開示されている方法及び装置の構成、動作、及び詳細において、当業者に明らかな様々な変更、修正、及び変形を実施可能であることを理解されたい。

【図１】

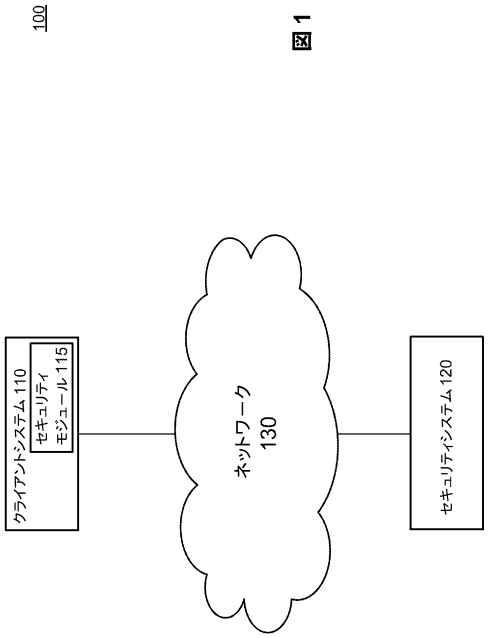

図 1

【図２】

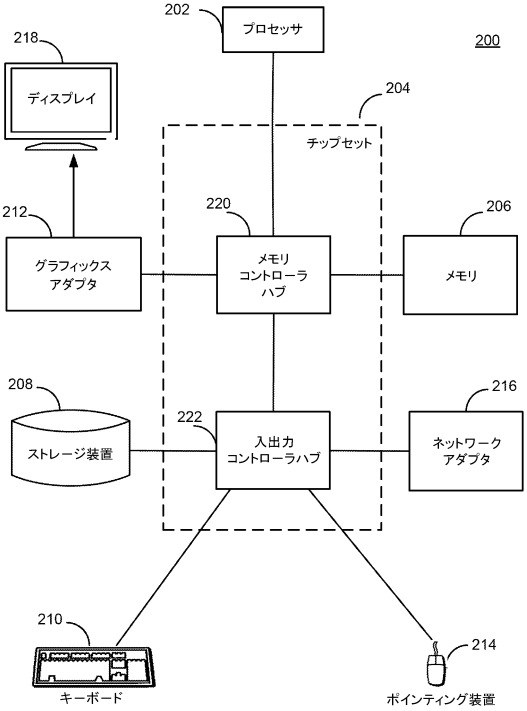

図 2

【図３】

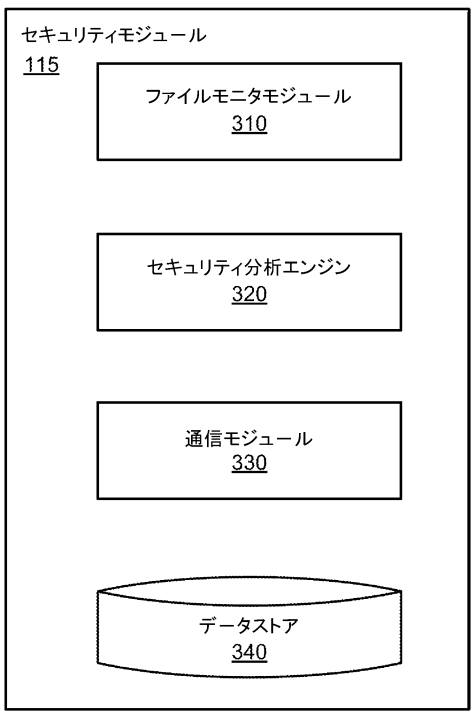

図 3

【図４】

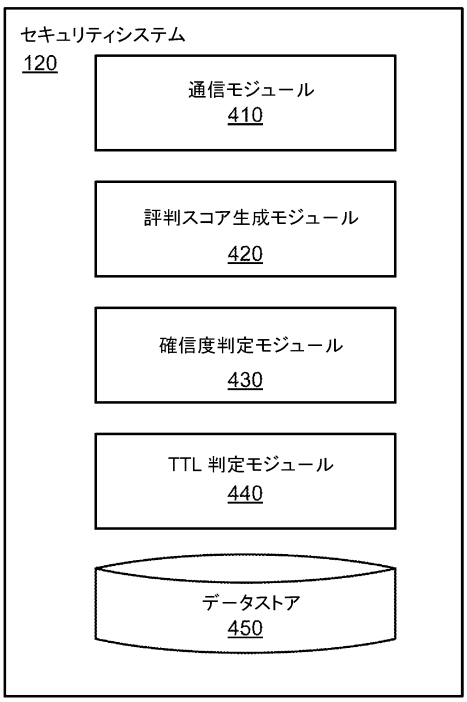

図 4

【図５】

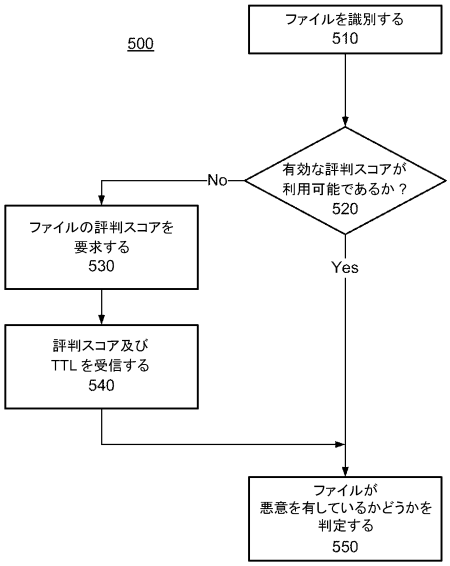
500
ファイルを識別する
510
有効な評判スコアが
利用可能であるか？
520
No
Yes
ファイルの評判スコアを
要求する
530
評判スコア及び
TTL を受信する
540
ファイルが
悪意を有しているかどうかを
判定する
550

図 5

【図６】

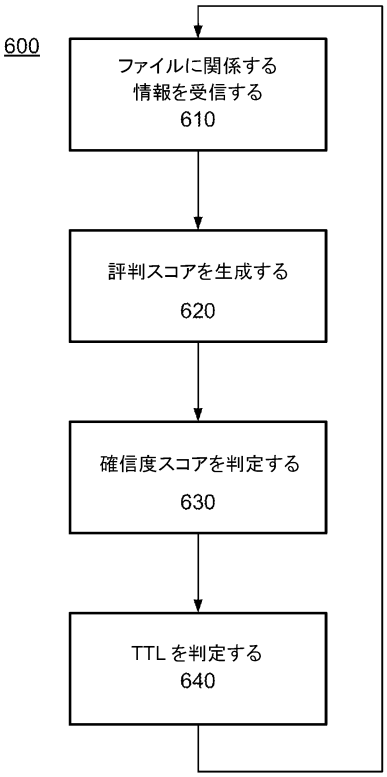
600
ファイルに関係する
情報を受信する
610
評判スコアを生成する
620
確信度スコアを判定する
630
TTL を判定する
640

図 6

フロントページの続き

(72)発明者　ヴィジェイ・セシャドリ
アメリカ合衆国　カリフォルニア州　９４０４３　マウンテン・ヴュー　エリス・ストリート　３５０　シマンテック　コーポレイション内
(72)発明者　ズルフィカール・ラムザン
アメリカ合衆国　カリフォルニア州　９４０４３　マウンテン・ヴュー　エリス・ストリート　３５０　シマンテック　コーポレイション内
(72)発明者　ジェームズ・ホーグランド
アメリカ合衆国　カリフォルニア州　９４０４３　マウンテン・ヴュー　エリス・ストリート　３５０　シマンテック　コーポレイション内
(72)発明者　アダム・エル・グリック
アメリカ合衆国　カリフォルニア州　９４０４３　マウンテン・ヴュー　エリス・ストリート　３５０　シマンテック　コーポレイション内
(72)発明者　アダム・ライト
アメリカ合衆国　カリフォルニア州　９４０４３　マウンテン・ヴュー　エリス・ストリート　３５０　シマンテック　コーポレイション内

審査官　戸島　弘詩

(56)参考文献　特表２０１０－５２１７４９（ＪＰ，Ａ）
特表２００８－５００６５３（ＪＰ，Ａ）
国際公開第２００８／１１３０５９（WO，Ａ１）
米国特許出願公開第２００９／０１８７４４２（ＵＳ，Ａ１）
米国特許出願公開第２００８／０２５６６２２（ＵＳ，Ａ１）
米国特許出願公開第２００６／０２５３５８４（ＵＳ，Ａ１）
米国特許出願公開第２００８／０１４７６１２（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／００－２１／８８
Ｇ０６Ｆ１３／００
Ｇ０６Ｑ１０／００，３０／００，５０／００，９０／００
Ｈ０４Ｌ１２／００