(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5510937号
(P5510937)
(45)発行日　平成26年6月4日(2014.6.4)　(24)登録日　平成26年4月4日(2014.4.4)

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

請求項の数 22 (全 22 頁)

(21)出願番号　特願2011-516546(P2011-516546)
(86)(22)出願日　平成21年6月23日(2009.6.23)
(65)公表番号　特表2011-527046(P2011-527046A)
(43)公表日　平成23年10月20日(2011.10.20)
(86)国際出願番号　PCT/US2009/048328
(87)国際公開番号　WO2010/002638
(87)国際公開日　平成22年1月7日(2010.1.7)
審査請求日　平成24年6月25日(2012.6.25)
(31)優先権主張番号　12/165,599
(32)優先日　平成20年6月30日(2008.6.30)
(33)優先権主張国　米国(US)

早期審査対象出願

(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】エンティティのレピュテーションスコアの簡易化された伝達

(57)【特許請求の範囲】
【請求項１】
ユーザにエンティティの評判（レピュテーション）を伝達する、コンピュータにより実施される方法であって、
複数のクライアントに関連付けられた、前記クライアントの信頼性の評価を表す衛生スコアであって、前記クライアントにおけるマルウエア検出の頻度に基づき決定された衛生スコアを特定するステップと、
複数のクライアントのうちの１つがエンティティに遭遇したことの通知を受信するステップであって、前記エンティティはファイル、プログラム又はウェブサイトを含む、ステップと、
前記クライアントの前記衛生スコアに基づいて、少なくとも閾値レベルの信頼性を示す衛生スコアを有する、信頼できるクライアントのセットを識別するステップと、
前記エンティティのレピュテーションスコアを計算するステップであって、前記レピュテーションスコアは、前記エンティティを使用したことのあるすべてのユーザに対する、前記エンティティを使用したことのある信頼できるクライアントの比率の測定を含み、前記レピュテーションスコアは、前記エンティティに悪意があるか否かの評価を表すステップと、
前記エンティティに遭遇した前記クライアントに前記レピュテーションスコアを提示するステップであって、前記レピュテーションスコアは、前記レピュテーションスコアが信頼できると考えられる他のクライアントに基づくことを示すメッセージが付随するステッ

プとを含む、方法。
【請求項２】
前記レピュテーションスコアは、前記エンティティを使用したことのあるクライアントセットの前記衛生スコアの数学的変換を更に含む、請求項１に記載の方法。
【請求項３】
前記メッセージは、１つまたは複数の信頼できるクライアントによる前記エンティティの使用についての統計を含む、請求項１に記載の方法。
【請求項４】
前記エンティティはファイルであり、前記エンティティの遭遇は、前記エンティティをダウンロードするステップ、または前記エンティティをダウンロードしようとするステップを含む、請求項１に記載の方法。
【請求項５】
前記エンティティはウェブサイトであり、前記エンティティの遭遇は、前記ウェブサイトを見るステップ、または前記ウェブサイトを見ようとするステップを含む、請求項１に記載の方法。
【請求項６】
エンティティの評判（レピュテーション）をユーザに伝達する、コンピュータにより実施される方法であって、前記方法は、
クライアントがエンティティに遭遇するステップであって、前記エンティティはファイル、プログラム又はウェブサイトを含む、ステップと、
クライアントが遭遇したエンティティに悪意があるか否かの評価を表すレピュテーションスコアを受信するステップであって、前記レピュテーションスコアは、前記エンティティを使用したことのあるすべてのユーザに対する、前記エンティティを使用したことのある信頼できるクライアントの比率の測定を含み、信頼できるクライアントは閾値を超える衛生スコアを有するクライアントであり、衛生スコアは、前記クライアントの信頼性の評価を表すと共に、前記クライアントにおけるマルウエア検出の頻度に基づき決定される、ステップと、
前記クライアントの出力装置を介して前記レピュテーションスコアを前記ユーザに伝達するステップと、
前記クライアントの前記出力装置を介して、前記レピュテーションスコアが信頼できるクライアントに基づくことを示すメッセージを前記ユーザに伝達するステップとを含む、方法。
【請求項７】
前記レピュテーションスコアは、前記エンティティを使用したことのあるクライアントセットの前記衛生スコアの数学的変換を含む、請求項６に記載の方法。
【請求項８】
前記メッセージは、１つまたは複数の信頼できるクライアントによる前記エンティティの使用についての情報を含む、請求項６に記載の方法。
【請求項９】
前記エンティティはファイルであり、前記エンティティに遭遇するステップは、前記エンティティをダウンロードするステップ、または前記エンティティをダウンロードしようとするステップを含む、請求項６に記載の方法。
【請求項１０】
前記エンティティはウェブサイトであり、前記エンティティに遭遇するステップは、前記ウェブサイトを見るステップ、または前記ウェブサイトを見ようとするステップを含む、請求項６に記載の方法。
【請求項１１】
エンティティの評判（レピュテーション）をユーザに伝達するためのコンピュータプログラムであって、コンピュータに、
複数のクライアントに関連付けられた衛生スコアを特定するステップであって、前記衛

生スコアは前記クライアントの信頼性の評価を表し、前記クライアントにおけるマルウエア検出の頻度に基づき決定される、ステップと、
複数のクライアントのうちの１つがエンティティに遭遇したことの通知を受信するステップであって、前記エンティティはファイル、プログラム又はウェブサイトを含む、ステップと、
前記クライアントの前記衛生スコアに基づいて信頼できるクライアントのセットを特定するステップであって、信頼できるクライアントは少なくとも信頼性の閾値を超える衛生スコアを有する、ステップと、
前記エンティティのレピュテーションスコアを計算するステップであって、前記計算されたレピュテーションスコアは、前記エンティティを使用したことのあるすべてのユーザに対する、前記エンティティを使用したことのある信頼できるクライアントの比率の測定を含み、前記レピュテーションスコアは、前記エンティティに悪意があるか否かの評価を表すステップと、
前記エンティティに遭遇した前記クライアントに前記レピュテーションスコアを提示するステップであって、前記レピュテーションスコアは、前記レピュテーションスコアが信頼できると考えられる他のクライアントに基づくことを示すメッセージが付随するステップと、
を実行させるためのコンピュータプログラム。
【請求項１２】
前記レピュテーションスコアは、前記エンティティを使用したことのあるクライアントセットの前記衛生スコアの数学的変換を含む、請求項１１に記載のコンピュータプログラム。
【請求項１３】
前記メッセージは、１つまたは複数の信頼できるクライアントによる前記エンティティの使用についての統計を含む、請求項１１に記載のコンピュータプログラム。
【請求項１４】
前記エンティティはファイルであり、前記エンティティの遭遇は、前記エンティティをダウンロードするステップ、または前記エンティティをダウンロードしようとするステップを含む、請求項１１に記載のコンピュータプログラム。
【請求項１５】
前記エンティティはウェブサイトであり、前記エンティティの遭遇は、前記ウェブサイトを見るステップ、または前記ウェブサイトを見ようとするステップを含む、請求項１１に記載のコンピュータプログラム。
【請求項１６】
エンティティの評判（レピュテーション）をユーザに伝達するためのコンピュータプログラムであって、コンピュータに、
クライアントにおいてエンティティに遭遇するステップであって、前記エンティティはファイル、プログラム又はウェブサイトを含む、ステップと、
クライアントが遭遇したエンティティに悪意があるか否かの評価を表すレピュテーションスコアを受信するステップであって、前記レピュテーションスコアは、前記エンティティを使用したことのあるすべてのユーザに対する、前記エンティティを使用したことのある信頼できるクライアントの比率の測定を含み、信頼できるクライアントは閾値を超える衛生スコアを有するクライアントであり、衛生スコアは、前記クライアントの信頼性の評価を表すと共に、前記クライアントにおけるマルウエア検出の頻度に基づき決定される、ステップと、
前記クライアントの出力装置を介して前記レピュテーションスコアを前記ユーザに伝達するステップと、
前記クライアントの前記出力装置を介して、前記レピュテーションスコアが信頼できるクライアントに基づくことを示すメッセージを前記ユーザに伝達するステップと、
を実行させるためのコンピュータプログラム。

【請求項１７】
前記レピュテーションスコアは、前記エンティティを使用したことのあるクライアントセットの前記衛生スコアの数学的変換を含む、請求項１６に記載のコンピュータプログラム。
【請求項１８】
前記メッセージは、１つまたは複数の信頼できるクライアントによる前記エンティティの使用についての情報を含む、請求項１６に記載のコンピュータプログラム。
【請求項１９】
前記エンティティはファイルであり、前記エンティティに遭遇するステップは、前記エンティティをダウンロードするステップ、または前記エンティティをダウンロードしようとするステップを含む、請求項１６に記載のコンピュータプログラム。
【請求項２０】
前記エンティティはウェブサイトであり、前記エンティティに遭遇するステップは、前記ウェブサイトを見るステップ、または前記ウェブサイトを見ようとするステップを含む、請求項１６に記載のコンピュータプログラム。
【請求項２１】
クライアントにおけるマルウエアは、前記クライアント上での既知のマルウエアのシグネチャとのデータの照合により検出される、
請求項１に記載の方法。
【請求項２２】
クライアントにおけるマルウエアは、前記クライアント上での既知のマルウエアのシグネチャとのデータの照合により検出される、
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】
関連出願の相互参照
本願は、参照によりその全体が援用される２００６年１２月２９日に出願された「Ｈｙｇｉｅｎｅ－Ｂａｓｅｄ　Ｃｏｍｐｕｔｅｒ　Ｓｅｃｕｒｉｔｙ」という名称の米国特許出願第１１／６１８，２１５号明細書に関する。
【０００２】
本発明は、一般にはコンピュータセキュリティに関し、特に、潜在的にコンピュータを損なう恐れがあるコンピュータファイル、ウェブサイト、および／または他のエンティティにより呈される評価リスクの程度をユーザに提供することに関する。
【背景技術】
【０００３】
近代のコンピュータを攻撃可能な多種多様な悪意のあるソフトウェア（マルウェア）が存在する。マルウェアの脅威としては、コンピュータウィルス、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、およびフィッシングウェブサイトが挙げられる。近代のマルウェアは多くの場合、攻撃者に金融的な利益を提供するように設計される。例えば、マルウェアは、ログイン、パスワード、銀行口座識別子、およびクレジットカード番号等の重要な情報を不正に捕捉することができる。同様に、マルウェアは、攻撃者が侵入先のコンピュータにアクセスし制御できるようにする隠れたインタフェースを提供することができる。
【０００４】
昔のマルウェアは通常、多くのコンピュータに大量配信されたが、近代のマルウェアは多くの場合、比較的少数のみのコンピュータを標的として送出される。トロイの木馬プログラムは、特定の企業の特定の部門のコンピュータを標的とするように設計し得る。同様に、偽の電子メールが、特定の銀行または特定の電子商取引サイトの顧客のみに向けられ

たフィッシング攻撃を含み得る。

【０００５】

大量配信されるマルウェアは多くの場合、従来のセキュリティソフトウェアにより検出し無効化することができる。セキュリティソフトウェアは、シグネチャスキャンおよび挙動監視ヒューリスティック等の技法を使用して、マルウェアを検出する。しかし、これら技法は、的を絞った脅威の検出にはあまり有効ではない。その理由は、同じマルウェアのインスタンス数が少なく、セキュリティソフトウェアがそのマルウェアを認識するように構成されない場合があるためである。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

さらに、大量配信されるマルウェアであっても検出がより難しくなりつつある。悪意のあるウェブサイトは、数人の訪問者毎に新しい悪意のあるコードを自動的に生成し得る。その結果、マルウェアは広範囲に配信されるが、少数のユーザのみが厳密に同じコードを有し、そのコードを検出するシグネチャを生成すること（およびシグネチャスキャンに基づく技法を使用すること）が非実用的になる。バージョンの異なるマルウェアが異なる機能を実行することがあり、これによっても、ヒューリスティックおよび他の技法を通してのマルウェアの検出が難しくなる。したがって、当分野では、マルウェアを検出する新しい方法が必要である。

【０００７】

さらに、シグネチャ、ヒューリスティック、およびマルウェアを検出する他の技法を開発するためにマルウェアを解析するセキュリティ企業は多数のマルウェア提出を受ける。セキュリティ企業は、提出されたマルウェアにより課される脅威を効率的に測定する方法を有さないことがある。例えば、セキュリティ企業は、提出されたソフトウェアが本当に悪意のあるものであるか否かまたは特定のマルウェアがどの程度広く蔓延しているかを知らない場合がある。その結果、セキュリティ企業は最大の脅威を構成する提出の解析に集中するためにマルウェア提出をランク付けまたは優先順位付けすることに手こずる。

【０００８】

当分野では、潜在的なマルウェアにより課される脅威を査定し、それら脅威をユーザに効率的に伝達する方法が必要である。２００６年１２月２９日に出願された米国特許出願第１１／６１８，２１５号明細書に記載のような評判（レピュテーション）に基づくシステムの場合、ソフトウェアアプリケーションまたは他のエンティティの評判（レピュテーション）が、ユーザコミュニティの使用パターンに基づいて送出される。次に、別の人がエンティティの評判（レピュテーション）を使用して、そのエンティティを使用すべきか否かについて判断することができる（ユーザにより手動で、またはユーザのクライアントシステムにより自動的に）。しかし、効率的に伝達されない場合、レピュテーションスコアは、助けようとしているユーザを混乱させる恐れがある。したがって、アプリケーションまたは他のエンティティの評判（レピュテーション）をユーザに対して、ユーザが明確に理解できるように提示する必要がある。

【課題を解決するための手段】

【０００９】

特別なユーザ（例えば、「パワーユーザ」、「コンピュータ上級者」、または信頼されるべきユーザを含意する他の呼び方）の概念を使用して、本発明の実施形態は、平均ユーザよりも信頼されるべき安全なまたはベテランのコンピュータユーザとの関連付けを詳述することにより、エンティティの評判（レピュテーション）を効率的に伝達する。エンティティは、ユーザがダウンロードもしくはインストールした、またはユーザがダウンロードもしくはインストールしようとしているアプリケーションまたは他のファイルであり得、したがって、エンティティの評判（レピュテーション）は、ファイルが他の特別なユーザからどの程度信頼されるかの尺度である。あるいは、エンティティは、クライアントシステムが対話でき、マルウェアの脅威を課し得るコンピュータ利用環境内のウェブサイト

または他の任意のエンティティであり得る。伝達される評判（レピュテーション）により、ユーザは、ユーザ自身のクライアント上で、エンティティを信頼すべきか否かについて判断することができる。

【００１０】

一実施形態では、複数のクライアントのそれぞれの衛生スコア（ｈｙｇｉｅｎｅ　ｓｃｏｒｅ）が特定され、衛生スコアは、クライアントの信頼性の評価を表す。クライアントのうちの１つがあるエンティティに遭遇した場合、そのエンティティのレピュテーションスコアが計算され、クライアントに提供される。レピュテーションスコアは、閾値を超える衛生スコアを有するクライアントのみに応じて計算し得る。計算されたレピュテーションスコアは、高い衛生スコアを有するクライアントを有する特別なユーザの観点からの、エンティティに悪意があるか否かの評価を表す。エンティティに遭遇したクライアントは次に、レピュテーションスコアが良好な衛生スコアを有する他の信頼できるクライアントに基づくことを示すメッセージと共に、レピュテーションスコアをユーザに提示する。このようにして、良好な衛生を有する信頼できるクライアントがエンティティと対話したことのある程度についての情報を使用して、エンティティの評判（レピュテーション）がユーザに通知される。

【００１１】

エンティティが実行可能なプログラムコードを含む場合、ユーザがそのエンティティをダウンロードする際、またはユーザのクライアントにインストールしようとする際に、そのエンティティのレピュテーションスコアがユーザに提示され得る。エンティティがウェブサイトである場合、ユーザがそのウェブサイトを開く際、またはユーザのクライアント上のブラウザがウェブサイトにナビゲートする前に、レピュテーションスコアがユーザに提示され得る。レピュテーションスコアにより提供される情報を用いて、ユーザは、ユーザのクライアントによるエンティティとの対話を許可すべきか否かについて、より情報に通じた判断を下し得る。

【図面の簡単な説明】

【００１２】

【図１】一実施形態によるコンピュータ利用環境の高レベルブロック図である。

【図２】レピュテーションサーバまたはクライアントとして使用される典型的なコンピュータを示す高レベルブロック図である。

【図３】一実施形態によるクライアントのセキュリティモジュールの詳細図を示す高レベルブロック図である。

【図４】一実施形態によるレピュテーションサーバの詳細図を示す高レベルブロック図である。

【図５】一実施形態による、セキュリティをクライアントに提供するためにセキュリティモジュールにより実行されるステップを示すフローチャートである。

【図６】一実施形態によるレピュテーションサーバにより実行されるステップを示すフローチャートである。

【図７】一実施形態による、提出されたマルウェアの優先度を決定するためにレピュテーションサーバにより実行されるステップ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】

【００１３】

これら図は、単なる例示として本発明の様々な実施形態を示す。以下の考察から、本明細書に示される構造および方法の代替の実施形態を、本明細書に開示される本発明の原理から逸脱せずに利用し得ることを当業者は容易に認識するであろう。

【００１４】

図１は、一実施形態によるコンピュータ利用環境１００の高レベルブロック図である。図１は、ネットワーク１１４により接続されたレピュテーションサーバ１１０および３つのクライアント１１２を示す。説明を簡潔かつ明確にするために、３つのみのクライアント１１２が図１に示される。コンピュータ利用環境１００の実施形態は、ネットワーク１

１４に接続された数千または数百万のクライアント１１２を有し得る。
【００１５】
図１およびその他の図は、同様の参照番号を使用して同様の要素を識別する。「１１２Ａ」等の参照番号の後の文字は、テキストがその特定の参照番号を有する要素を特に指すことを示す。「１１２」等の後に続く文字のないテキスト内の参照番号は、その参照番号を有する図中の要素のうちの任意またはすべての要素を指す（例えば、テキスト中の「１１２」は図中の参照番号「１１２Ａ」、「１１２Ｂ」、および／または「１１２Ｃ」を指す）。
【００１６】
レピュテーションサーバ１１０は、ネットワーク１１４を介してクライアント１１２と対話する。一実施形態では、レピュテーションサーバ１１０は、クライアント１１２の衛生スコアを受信する。クライアントの衛生スコアは、クライアント１１２の信頼性の評価を表す。この文脈の中での「信頼性」は、マルウェアおよび他のコンピュータ関連脅威に感染するクライアントの傾向の尺度を指し、感染した頻度が高いクライアント１１２ほど、信頼性は低い。「信頼性」は、脅威を回避するユーザの能力にも相当する。いくつかの実施形態では、レピュテーションサーバ１１０は、クライアント１１２から受信されるデータに基づいて自身の衛生スコアを計算する。さらに、レピュテーションサーバ１１０は、クライアント上に存在する、ダウンロードされた、インストールされた、または実行されたファイル、クライアントが訪れたウェブサイト、およびクライアント１１０上で検出されたマルウェア等のクライアント１１２の状態を記述するデータを受信する。
【００１７】
一実施形態では、レピュテーションサーバ１１０は、クライアントの衛生スコアを考慮してクライアント１１２の集合的な状態を解析し、クライアントが遭遇した特定のプログラム、ファイル、ウェブサイト、および他のコンピュータ関連エンティティのレピュテーションスコアを計算する。レピュテーションスコアは、エンティティに悪意がある（例えば、コンピュータ関連脅威である）危険性の評価である。例えば、低い衛生スコアを有するクライアント１１２が主に遭遇する特定のファイルの場合、そのファイルを使用する大半のユーザはコンピュータの脅威を回避することに不得手であるため、そのファイルに悪意がある危険性が高い。したがって、そのファイルは低いレピュテーションスコアを受ける可能性が高い。同様に、高い衛生スコアを有するクライアント１１２が頻繁に訪れるウェブサイトは、コンピュータの脅威を回避することに優れたユーザが頻繁に訪れているため、高いレピュテーションスコアを受ける可能性が高い。レピュテーションサーバ１１０は、レピュテーションスコアをクライアント１１２に提供し、クライアント（およびクライアントのユーザ）は、スコアを使用して、特定の動作を実行すべきか否かに関しての挙動をガイドする。例えば、クライアント１１２は、閾値を下回るレピュテーションスコアを有するファイルのダウンロードを阻止するように構成することができる。同様に、ユーザは、ファイルの低いレピュテーションスコアを見た上で、そのファイルのインストールまたは実行を断ることができる。
【００１８】
一実施形態では、クライアント１１２は、ファイルのダウンロード、インストール、および／または実行ならびにネットワーク１１４上のウェブサイトの閲覧を含む動作を実行するために、１人または複数のユーザにより使用されるコンピュータである。クライアント１１２は、例えば、ユーザがウェブサーバまたはネットワーク１１４上の他のコンピュータからコンテンツを検索し表示できるようにするウェブブラウザを実行するパーソナルコンピュータであり得る。他の実施形態では、クライアント１１２は、個人情報端末（ＰＤＡ）、携帯電話、ページャ、テレビジョン「セットトップボックス」等のコンピュータ以外のネットワーク対応装置である。この説明では、用語「クライアント」は、マルウェアまたは他の脅威を構成し得るファイルまたは他のエンティティに遭遇するサーバおよびゲートウェイ等のコンピュータも含む。例えば、クライアント１１２は、企業ネットワークとインターネットとの間に配置されるネットワークゲートウェイであり得る。クライア

ント１１２は、他のクライアントがアクセス可能なファイルを記憶するメールサーバまたはウェブサーバでもあり得る。

【００１９】

一実施形態では、クライアント１１２は、クライアントの状態を監視するセキュリティモジュール１１６を実行する。状態は、インストールされたファイル、実行されたファイル、およびダウンロードされたファイル、訪れたウェブサイト等のクライアント上で実行される動作を含む。さらに、セキュリティモジュール１１６の実施形態は、クライアント１１２でのマルウェア検出も監視する。セキュリティモジュール１１６は、状態を記述するデータをレピュテーションサーバ１１０に提供する。

【００２０】

さらに、セキュリティモジュール１１６の実施形態は、状態に基づいてクライアントの衛生スコアを計算し、このスコアをレピュテーションサーバ１１０に提供する。多くの場合、衛生スコアには大きな差がある。ティーンエイジャー等の特定のタイプのユーザは、他のユーザよりも危険性の高いオンライン挙動をとる可能性がはるかに高い。例えば、ティーンエイジャーおよび他の若年の人々は、ピアツーピアネットワークおよびマルウェアが見つけることが多い他の場所からファイルをダウンロードする可能性がより高い。これら動作は、マルウェア検出の増大に繋がり、その結果、そのようなユーザが使用するクライアントは低い衛生スコアを有することが多い。他のユーザは、危険性の高い挙動をとらず、マルウェアに遭遇することは希である。それら後者のユーザのクライアント１１２は高い衛生スコアを受ける。

【００２１】

さらに、セキュリティモジュール１１６は、レピュテーションサーバ１１０からレピュテーションスコア１１６を受信する。一実施形態では、セキュリティモジュール１１６は、例えば、レピュテーションスコアを閾値と比較するか、またはレピュテーションスコアに基づいてユーザにメッセージを表示することにより、エンティティのレピュテーションスコアを査定する。セキュリティモジュール１１６は、任意に、査定の結果に応答して、動作をキャンセルするか、またはエンティティが関わる別の動作を実行する。セキュリティモジュール１１６は、査定の結果として実行される動作の説明をレピュテーションサーバ１１０に提供する。

【００２２】

このようにして衛生スコアおよびレピュテーションスコアを使用することにより、脅威を回避するユーザの能力と、ユーザの遭遇したコンピュータ関連エンティティに関して特定の動作をとる判断とが関連付けられる。この手法は、エンティティに関連するリスクを正確に測定する、レピュテーションスコアのファイル、ウェブサイト、および他のエンティティへの割り当てにユーザの集合的な知性を活用する。レピュテーションスコアは、ユーザがエンティティを明示的に査定または判断する必要なく計算される。さらに、レピュテーションスコアは、ファイル、ウェブサイト、または他の潜在的に悪意を有するエンティティの高度な解析を必要とせずに計算される。したがって、この手法は、従来のシグネチャスキャンおよび／またはヒューリスティック技法を使用して識別されない場合がある相当量のマルウェアまたは他の脅威が存在するコンピュータ利用環境によく適する。

【００２３】

ネットワーク１１４は、レピュテーションサーバ１１０とクライアント１１２との間の通信経路を表す。一実施形態では、ネットワーク１１４はインターネットである。ネットワーク１１４は、必ずしもインターネットの部分であるとは限らない専用通信リンクまたは私設通信リンクを使用してもよい。一実施形態では、ネットワーク１１４は、標準通信技術および／またはプロトコルを使用する。したがって、ネットワーク１１４は、イーサネット（登録商標）、８０２．１１、統合サービスデジタル網（ＩＳＤＮ）、デジタル加入者回線（ＤＳＬ）、非同期転送モード（ＡＴＭ）等の技術を使用するリンクを含み得る。同様に、ネットワーク１１４に使用されるネットワーク化プロトコルは、伝送制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）、ハイパーテキスト転送プロトコル

（ＨＴＴＰ）、簡易メール転送プロトコル（ＳＭＴＰ）、ファイル転送プロトコル（ＦＴＰ）等を含み得る。ネットワーク１１４を介して交換されるデータは、ハイパーテキストマークアップ言語（ＨＴＭＬ）、拡張可能マークアップ言語（ＸＭＬ）等を含む技術および／またはフォーマットを使用して表し得る。さらに、リンクのうちのすべてまたはいくつかは、セキュアソケットレイヤ（ＳＳＬ）、セキュアＨＴＴＰ、および／または仮想私設ネットワーク（ＶＰＮ）等の従来の暗号技術を使用して暗号化し得る。別の実施形態では、エンティティは、上述したものの代替または追加として、カスタムおよび／または専用のデータ通信技術を使用し得る。

【００２４】

図２は、レピュテーションサーバ１１０またはクライアント１１２として使用される典型的なコンピュータ２００を示す高レベルブロック図である。バス２０４に結合されたプロセッサ２０２が示される。バス２０４には、メモリ２０６、記憶装置２０８、キーボード２１０、グラフィックスアダプタ２１２、ポインティングデバイス２１４、およびネットワークアダプタ２１６も結合される。ディスプレイ２１８が、グラフィックスアダプタ２１２に結合される。

【００２５】

プロセッサ２０２は、ＩＮＴＥＬｘ８６互換性ＣＰＵ等の任意の汎用プロセッサであり得る。記憶装置２０８は、一実施形態では、ハードディスクドライブであるが、書き込み可能コンパクトディスク（ＣＤ）またはＤＶＤ、あるいは固体状態メモリ装置等のデータを記憶可能な他の任意の装置であってもよい。メモリ２０６は、例えば、ファームウェア、読み取り専用メモリ（ＲＯＭ）、不揮発性ランダムアクセスメモリ（ＮＶＲＡＭ）、および／またはＲＡＭであり得、プロセッサ２０２により使用される命令およびデータを保持する。ポインティングデバイス２１４は、マウス、トラックボール、または他の種類のポインティングデバイスであり得、キーボード２１０と併せて使用されて、データをコンピュータ２００に入力する。グラフィックスアダプタ２１２は、画像および他の情報をディスプレイ２１８に表示する。ネットワークアダプタ２１６は、コンピュータ２００をネットワーク１１４に結合する。

【００２６】

当該技術分野において既知のように、コンピュータ２００は、コンピュータプログラムモジュールを実行するように構成される。本明細書において使用される用語「モジュール」は、指定された機能を提供するコンピュータプログラム論理および／またはデータを指す。モジュールは、ハードウェア、ファームウェア、および／またはソフトウェアで実施し得る。一実施形態では、モジュールは記憶装置２０８に記憶され、メモリ２０６にロードされ、プロセッサ２０２により実行される。

【００２７】

図１のエンティティが使用するコンピュータシステム２００のタイプは、実施形態およびエンティティが使用する処理能力に応じて様々であり得る。例えば、携帯電話であるクライアント１１２は通常、限られた処理能力を、小型ディスプレイ２１８を有し、ポインティングデバイス２１４を有さない場合がある。逆に、レピュテーションサーバ１１０は、協働して、本明細書において説明される機能を提供する複数のブレードサーバを備え得る。

【００２８】

図３は、一実施形態によるクライアント１１２のセキュリティモジュール１１６の詳細図を示す高レベルブロック図である。いくつかの実施形態では、セキュリティモジュール１１６は、クライアント１１２上で実行中のオペレーティングシステム内に組み込まれる一方で、他の実施形態では、セキュリティモジュールは独立したアプリケーションまたは別の製品の部分である。図３に示されるように、セキュリティモジュール１１６自体が複数のモジュールを含む。セキュリティモジュール１１６の他の実施形態が、ここで説明されるモジュールと異なるモジュールおよび／または他のモジュールを有してもよいこと、および機能を異なる様式でモジュールに分散させてもよいことを当業者は認識するであろ

う。

【００２９】

マルウェア検出モジュール３１０は、クライアント１１２上でのマルウェアの存在を検出する。上述したように、「マルウェア」は、コンピュータウィルス、ワーム、トロイの木馬プログラム、およびこれらと同様のもの等のソフトウェアを含む。この説明では、「マルウェア」は、ユーザを騙して機密情報を暴露させようとする「フィッシング」サイト等の悪意のあるウェブサイトも含む。一実施形態では、マルウェア検出モジュール３１０は、既知のタイプのマルウェアを記述したシグネチャデータベースを含む。マルウェア検出モジュール３１０は、エミュレーションおよびシグネチャスキャン等の技法を使用して、データベース内のシグネチャをクライアント１１２上のファイルおよび／または他のデータと照合する。一致が発生した場合、一致したデータはマルウェアであると想定される。さらに、マルウェア検出モジュール３１０の実施形態は、ヒューリスティック技法および他の技法を使用して、以前は未知であったマルウェアを検出する。いくつかの実施形態では、マルウェア検出モジュール３１０は、マルウェアによるクライアント１１２の破損の阻止およびマルウェアの削除等のタスクを実行する追加の機能を含む。

【００３０】

さらに、マルウェア検出モジュール３１０の実施形態は、続けて解析するために、検出されたファイルまたは他のエンティティをレピュテーションサーバ１１０に提出する。時には、マルウェア検出モジュール３１０は、ヒューリスティック技法または他の技法を通して以前は未知であったマルウェアを識別することになる。これらの状況では、マルウェアをレピュテーションサーバ１１０に提出して、レピュテーションサーバ１１０に関連付けられた専門家がマルウェアを解析できるようにすることが望ましいことが多い。この解析は、マルウェアを検出し無効化し、マルウェアに感染したクライアント１１２を修復し、誤検出量を低減する技術の改良に繋がり得る。

【００３１】

状態監視モジュール３１２は、クライアント１１２の状態を監視して、クライアント１１２とクライアントの衛生スコアまたはエンティティのレピュテーションスコアに関連するファイルおよびウェブサイト等のエンティティとの遭遇を検出する。このために、状態監視モジュール３１２の実施形態は、クライアントの記憶装置２０８に存在するファイルおよびクライアントのメモリ２０６内に存在するプロセスを識別する。さらに、状態監視モジュール３１２は、クライアントの衛生スコアまたはエンティティのレピュテーションスコアに関連するクライアント１１２で実行される動作を監視する。一実施形態では、状態監視モジュール３１２により実行される監視のタイプは、ユーザ構成可能なパラメータに基づいて制限される。例えば、ユーザは、プライバシーまたは他のタイプの懸念により、特定のタイプの監視をディセーブルし得る。さらに、状態監視モジュール３１２の実施形態は動作を一時的に中止して、その動作をキャンセルする機会を提供し得る。

【００３２】

より具体的には、状態監視モジュール３１２の実施形態は、クライアント１１２に導入されるか、または実行されるファイルが関わる動作を監視する。例えば、監視される動作としては、ネットワーク１１４上のウェブサイトおよび／または他のロケーションからのファイルのダウンロード、リムーバブル媒体を介するクライアント１１２へのファイルのロード、クライアントへのファイルのインストール、およびクライアントでのファイルの実行が挙げられる。それぞれの場合において、状態監視モジュール３１２は、実行された動作およびその動作に関わった１つまたは複数のファイルの識別情報を記録する。一実施形態では、状態監視モジュール３１２は、ファイルを一意に識別するハッシュを生成することにより、ファイルを識別する。さらに、状態監視モジュール３１２のいくつかの実施形態は、マルウェアが存在する危険がある実行可能ファイルのみ、または他のファイルタイプのみを監視し識別する。

【００３３】

状態監視モジュール３１２の実施形態は、ネットワーク１１４を介して行われるウェブ

閲覧および／または他の動作に関わる動作を監視する。状態監視モジュール３１２の一実施形態は、ネットワーク通信を監視し、クライアント１１２が閲覧するウェブサイトおよび／またはウェブサイトのタイプ（例えば、セックスまたはギャンブルのウェブサイト）を特定する。さらに、状態監視モジュール３１２は、ウェブサイトに埋め込まれた特定のプログラムおよび他のコード等の、クライアント１１２が閲覧するウェブサイトに存在するエンティティも識別する。さらに、状態監視モジュール３１２は、ウェブサイトがクライアントブラウザ内にポップアップウィンドウを生成するか否か等の訪れたウェブサイトの特徴を監視する。状態監視モジュール３１２の別の実施形態は、クライアント側ウェブブラウザにより保持されるファイルキャッシュを調べて、ブラウザを使用して訪れたサイトを特定する。

【００３４】

衛生計算モジュール３１４は、測定項目のセットに応答して、クライアント１１２の衛生スコアを計算する。一実施形態では、測定項目は、マルウェア検出モジュール３１０によるマルウェア検出および状態監視モジュール３１２により監視されるクライアント状態を含む。一実施形態では、衛生計算モジュール３１４は、測定項目を構成するデータをレピュテーションサーバ１１０に送信し、サーバはクライアントの衛生スコアを計算する。

【００３５】

一実施形態では、衛生計算モジュール３１４は、マルウェア検出等の特定のイベントの発生頻度に基づく測定項目を使用する。例えば、測定項目は、１週間、１ヶ月、または３ヶ月の間隔等の時間期間中に観察されるマルウェア検出数を含み得る。同様に、測定項目は、クライアント１１２にダウンロードされ、かつ／またはインストールされたファイル数に相対する測定マルウェア検出数を含み得る。同様に、測定項目が基づく動作は、一定の時間間隔中に測定されるか、または合計訪問ウェブサイト数に相対する、ユーザが既知の悪意のある、または芳しくないウェブサイト（セックス／ギャンブルサイト、多くのポップアップウィンドウを有するサイト、またはフィッシング攻撃をホストすることが分かっているサイト等）を閲覧する頻度を含み得る。測定項目により測定されるイベントの頻度が変更した場合、クライアント１１２の衛生スコアも経時変化し得る。

【００３６】

一実施形態では、衛生スコアは、複数のクライアントの衛生スコアを直接比較できるようにする、０および１等の所与の範囲内に正規化された数値である。例えば、ゼロのスコアは最も不良な衛生を表す一方で、１のスコアは最良の衛生を表し得る。他の実施形態では、衛生スコアは、限られた値のセットのうちの１つに定量化される。例えば、可能な衛生スコアは０および１のみである。

【００３７】

レピュテーション査定モジュール３１６は、レピュテーションサーバ１１０からファイル、プログラム、ウェブサイト、および／または他のエンティティのレピュテーションスコアを受信する。一実施形態では、レピュテーション査定モジュール３１６は、状態監視モジュール３１２と協働して、クライアント１１２がレピュテーションスコアを有するエンティティに遭遇するときを検出する。これら遭遇は、ユーザの知らないうちに自動的に実行される動作およびユーザの指示で行われる動作を含み得る。例えば、モジュール３１６は、クライアントのウェブブラウザがウェブサーバからファイルをダウンロードしようとするとき、ファイルをクライアント１１２にインストールしようとするとき、およびユーザがファイルを実行しようとするときを検出する。一実施形態では、レピュテーション査定モジュール３１６は、エンティティの識別情報（例えば、実行可能ファイルのハッシュまたはウェブサイトのＵＲＬ）をレピュテーションサーバ１１０に送信し、その引き替えとして、レピュテーションスコアを受信する。別の実施形態では、レピュテーション査定モジュール３１６は、特定のプログラムのレピュテーションスコアのキャッシュを保持し、レピュテーションサーバ１１０と交信する前に（またはレピュテーションサーバ１１０との交信に代えて）、キャッシュを調べて、スコアがキャッシュ内に含まれるか否かを判断する。さらに、レピュテーション査定モジュール３１６の実施形態は、レピュテーシ

ョン査定モジュールが査定する必要がないファイルまたは他のエンティティを識別する除外セットを保持する。それら除外されるエンティティは、ファイルのデジタルシグネチャ付きのハッシュを使用して、かつ／または他の技法を介して識別される。

【００３８】

一実施形態では、状態監視モジュール３１２は、レピュテーション査定モジュール３１６がエンティティのレピュテーションスコアを取得する間、エンティティが関わる動作を中止する。レピュテーション査定モジュール３１６は、レピュテーションスコアを査定し、スコアに応じて、中止していた動作をキャンセルする。一実施形態では、レピュテーション査定モジュール３１６は、レピュテーションスコアをレピュテーション閾値と突き合わせて査定し、スコアが閾値を下回る場合には動作をキャンセルする（かつ／またはスコアが閾値を上回る場合、動作を許可する）。例えば、レピュテーションモジュール３１６は、ブラウザがメールサーバまたはウェブサイトからダウンロードしようとしているファイルが、閾値を下回るレピュテーションスコアを有すると判断し得、したがって、ファイルは悪意のあるものである危険性が高いため、ダウンロードをキャンセルし得る。一実施形態では、閾値はユーザにより設定される。他の実施形態では、閾値は、クライアント１１２の管理者またはレピュテーションサーバ１１０により設定される。

【００３９】

一実施形態では、レピュテーション査定モジュール３１６は、レピュテーションスコアを説明するメッセージをユーザに表示し、それにより、スコアに応じて動作をキャンセルする機会をユーザに提供する。この表示は、レピュテーションスコアがレピュテーション閾値を下回る（または別の閾値を下回る）場合に行われ得る。例えば、レピュテーション査定モジュール３１６は、ユーザが実行しようとしているファイルが低いレピュテーションスコアを有することを検出し、レピュテーションスコアまたは警告メッセージをユーザに表示して、ユーザに潜在的な脅威を査定させる。

【００４０】

いくつかの実施形態では、ユーザに表示されたレピュテーションスコアは、数値として表される一方で、他の実施形態では、テキスト説明またはグラフィックスアイコン（例えば、５つ星のうちの４つ星）等の他の技法を使用して表される。例えば、レピュテーション査定モジュール３１６の実施形態は、ユーザがファイルを実行しようとする際、ファイルのレピュテーションスコアをダイアログボックスまたは他のユーザインタフェース（ＵＩ）要素内に表示する。同様に、レピュテーション査定モジュール３１６の実施形態は、ユーザがサイトを閲覧しようとする際、ウェブサイトのレピュテーションスコアを記述するグラフィックスアイコンを提供する。レピュテーション査定モジュール３１６により表される表示は、例えば、「このプログラムの評判（レピュテーション）は悪いです。本当にインストールしたいですか？」、「良好な衛生の多くの人々がこのプログラムをインストールしました。そのため、使用しても安全であるはずです」、または「このプログラムを試したユーザはごく少数であり、評判（レピュテーション）は未知です。このプログラムをテストしたいですか？」のようなメッセージを有するダイアログボックスを含み得る。

【００４１】

レピュテーション査定モジュール３１６は、レピュテーションスコアを、ユーザが理解する可能性がより高いフォーマットに変換し得る。一実施形態では、レピュテーションスコアは、「信頼できる」クライアントのセットに基づき、信頼できるクライアントは、クライアントの衛生スコアに基づいて識別される。一実施形態では、信頼できるクライアントは、所定の閾値を上回る衛生スコアを有するクライアントのセットとして定義される。したがって、特定のエンティティのレピュテーションスコアは、エンティティを使用したことのある信頼できるクライアントに応じて計算し得る。このようにして、レピュテーションスコアは、エンティティに遭遇した可能性のある信頼できるクライアントの観点から、エンティティに悪意があるか否かの評価を表す。レピュテーションスコアが計算されると、エンティティに遭遇しているユーザに対し、クライアント上にそれが提示される。ユ

ーザがこのレピュテーションスコアの意味を理解するのを助けるために、クライアントは、レピュテーションスコアが信頼できると考えられる他のクライアントに基づくことを示すメッセージもユーザに提示する。レピュテーションスコアおよび付随するメッセージは、様々な形態をとり得る。

【００４２】

一実施形態では、レピュテーションスコアは、すべてのクライアントに対する、エンティティを使用したことのある信頼できるクライアントの割合として、または信頼できるクライアントとして定義され、エンティティを使用したことのあるクライアントの割合として計算される。このレピュテーションスコアおよび付随するメッセージはこうして、新しいエンティティに遭遇した新しいユーザに、同じエンティティに遭遇したことのある他のクライアントの全般的な信頼性について通知する。付随するメッセージは、「このアプリケーションをインストールした９４５人の他のユーザのうち、６４％のユーザがパワーユーザです。」のようなものであり得る。メッセージは、ユーザが平均ユーザよりも信頼できることを効率的に伝える様々な方法で、信頼できるユーザを参照し得る。これらは、「パワーユーザ」、「コンピュータ上級者」、「信頼できるユーザ」、または同じまたは同様の意味を伝える他の任意の用語を含み得る。

【００４３】

別の実施形態では、レピュテーションスコアは、エンティティを使用する信頼できるクライアントの数として計算される。したがって、このレピュテーションスコアおよび付随するメッセージは、新しいエンティティに遭遇した新しいユーザに、何人の信頼できるユーザがそのエンティティをすでに使用したかについて通知する。付随するメッセージは、「１２５０人の信頼できるユーザがこのプログラムをダウンロードしインストールしました」のようなものであり得る。このメッセージを見た場合、ユーザは、何人の信頼できるユーザがすでに行ったかに基づいて、エンティティを使用する先例に続くべきか否かについて、情報に通じた判断を下し得る。

【００４４】

別の実施形態では、レピュテーションスコアは、エンティティを使用したクライアントの衛生スコアの数学的な直接変換として計算される。単純な例では、レピュテーションスコアは、エンティティに遭遇したことがあり、エンティティを使用したことのあるすべてのクライアントの衛生スコアの平均である。この種のレピュテーションスコアは、エンティティを使用する典型的なクライアントの構成についての情報を新しいユーザに提供する。マルウェアは、「良好な衛生」のクライアントでは見つかる可能性がより低いため、スコアが高いことによって、エンティティが信頼できることがユーザに伝えられる。この実施形態では、付随するメッセージは、「このアプリケーションに対するコンピュータ上級者のスコアは５つ星中の４．３です」のようなものであり得る。このメッセージを見ているユーザが、このメッセージがどのように計算されたのか理解しない場合であっても、メッセージは、アプリケーションが信頼できるユーザ（例えば、「コンピュータ上級者」または「パワーユーザ」）により信頼される程度に基づいて、アプリケーションが信頼できるはずであることを効率的に伝える。

【００４５】

一実施形態では、レピュテーション査定モジュール３１６により提示される表示は、動作をキャンセルする機会もユーザに提供する。したがって、モジュール３１６により提示されるダイアログボックスは、ユーザにファイルのインストールまたは実行をキャンセルまたは確認させる１組の「Ｙｅｓ／Ｎｏ」または「ＯＫ／キャンセル」ボタンを含み得る。レピュテーション査定モジュール３１６は、表示されたレピュテーションスコアに対するユーザの応答を記憶し、ユーザが動作を実行する都度、必ずしもレピュテーションスコアを表示するとは限らない。上述したように、状態監視モジュール３１２の実施形態は、レピュテーションスコアに対するユーザの応答、特に、ユーザがレピュテーションスコアに鑑みて動作の継続を選択するか、それともキャンセルを選択するかを監視する。状態監視モジュール３１２は、レピュテーションサーバ１１０にユーザの応答を通知する。サー

バ１１０は、その応答を使用して、エンティティのレピュテーションスコアを改良または調整することができる。

【００４６】

サーバ通信モジュール３１８は、ネットワーク１１４を介してレピュテーションサーバ１１０と通信する。一実施形態では、サーバ通信モジュール３１８は、クライアント１１２についての情報を提供する報告をサーバ１１０に送信する。情報は、クライアントの衛生スコア、クライアント１１２とエンティティとの間で監視されたすべての遭遇の記述、および潜在的なマルウェアの提出を含む。一実施形態では、サーバ通信モジュール３１８は、衛生スコアが変更した場合、または一定の間隔等の所定の時間に衛生スコアをレピュテーションサーバ１１０に報告する。別の実施形態では、サーバ通信モジュール３１８は、クライアントがエンティティに遭遇する都度、および／またはマルウェアである恐れがあるエンティティを検出または提出する都度、衛生スコアをレピュテーションサーバ１１０に報告する。例えば、サーバ通信モジュール３１８は、レピュテーション査定モジュール３１６がエンティティのレピュテーションスコアを要求する都度、衛生スコアおよびエンティティの識別子を含むタプルをレピュテーションサーバ１１０に送信する。いくつかの実施形態は、報告内に、レピュテーションサーバ１１０が特定の報告を、その報告を生成したクライアントに関連付け、複製報告を検出できるようにする一意のクライアント識別子または他のデータを含む。さらに、サーバ通信モジュール３１８の実施形態は、クライアント１１２にセキュリティを提供するために使用される情報をレピュテーションサーバ１１０から受信する。受信される情報は、エンティティのレピュテーションスコア、マルウェアの定義、およびセキュリティモジュール１１６への他の更新を含む。

【００４７】

図４は、一実施形態によるレピュテーションサーバ１１０の詳細図を示す高レベルブロック図である。一実施形態では、レピュテーションサーバ１１０は、セキュリティモジュール１１６をクライアント１１２に提供する同じエンティティにより操作される。図４に示されるように、レピュテーションサーバ１１０はいくつかのモジュールを含む。レピュテーションサーバ１１０の他の実施形態が、ここに説明されるものと異なるモジュールおよび／または他のモジュールを有してもよいこと、および機能を異なる様式でモジュールに分散させてもよいことを当業者は認識するであろう。さらに、レピュテーションサーバ１１０に帰する機能を複数のサーバで実行してもよい。

【００４８】

クライアント通信モジュール４１０は、ネットワーク１１４を介してクライアント１１２と通信する。一実施形態では、クライアント通信モジュール４１０は、衛生スコア、監視された状態、マルウェア提出、および他の情報を記述したデータをクライアント１１２から受信する。さらに、クライアント通信モジュール４１０の実施形態は、ファイル、ウェブサイト、および他のエンティティのレピュテーションスコアをクライアント１１２に提供する。

【００４９】

衛生キャッシュモジュール４１２は、クライアント１１２から受信した衛生スコアを記憶する。衛生スコアが（衛生スコア、エンティティ識別子）タプルで受信される実施形態では、衛生キャッシュモジュール４１２は、スコアを関連するエンティティとスコアとを関連付けるテーブルまたは他のデータ構造にスコアを記憶する。衛生スコアがクライアント１１２の識別子と共に受信される別の実施形態では、衛生キャッシュモジュール４１２は、スコアとクライアントとを関連付けるテーブルまたは他のデータ構造にスコアを記憶する。レピュテーションサーバ１１０が衛生スコアを計算する実施形態では、衛生キャッシュモジュール４１２は、上述した衛生計算モジュール３１４に帰する機能を実行する。

【００５０】

状態情報モジュール４１４は、クライアント１１２において状態監視モジュール３１２により監視された動作および他の状態情報を記述するデータを記憶する。一実施形態では、記憶されるデータは、クライアント１１２とエンティティとの遭遇を記述する。これら

遭遇は、クライアント１１２に存在するファイル、クライアント１１２にダウンロードされたファイル、クライアント１１２にインストールされたファイル、および／またはクライアント１１２により実行されるファイル、クライアントが訪れたウェブサイト等を、これらの動作を実行しようとするあらゆる試行を含めて含む。状態情報モジュール４１４は、ユーザが、プログラムのレピュテーションスコアを説明したメッセージを見た後に特定のファイルを実行したか否か等、クライアント１１２において実行されるレピュテーションスコア査定に応答して実行される動作を記述するデータも記憶する。一実施形態では、状態情報モジュール４１４は、動作を、動作（および遭遇）が発生したクライアントの衛生スコアに関連付ける。別の実施形態では、状態情報モジュール４１４は、動作を、動作が発生したクライアント１１２の識別子に関連付ける。

【００５１】

一実施形態では、衛生キャッシュ４１２および状態情報モジュール４１４の機能は、エンティティ識別子およびそのエンティティに遭遇したクライアント１１２の衛生スコアを記憶する結合モジュールにより実行される。さらに、衛生スコアは、ヒストグラムまたは別の効率的な様式で表される。例えば、特定のエンティティについて、結合モジュールは、高い衛生スコアを有する５つのクライアントおよび低い衛生スコアを有する２５のクライアントがエンティティに遭遇したことを記録する。モジュールは、エンティティに遭遇した特定のクライアント１１２の識別子を必ずしも記憶するとは限らない。

【００５２】

レピュテーション計算モジュール４１６は、衛生キャッシュ４１２および／または状態情報４１４モジュール内のデータに基づいて、ファイル、ウェブサイト、および／または他のエンティティのレピュテーションスコアを計算する。一実施形態では、レピュテーションスコアは、衛生スコアと同様の数値である。レピュテーションスコアは、異なるエンティティのレピュテーションスコアを直接比較できるように、０および１等の所与の範囲内に正規化される。例えば、０のスコアは最低の評判（レピュテーション）を表す一方で、１のスコアは最高の評判（レピュテーション）を表し得る。他の実施形態では、レピュテーションスコアは限られた値のセットのうちの１つに定量化される。

【００５３】

ファイルまたは他のエンティティのレピュテーションスコアは主に、エンティティに遭遇したクライアント１１２の衛生スコアに基づく。例えば、高い衛生スコアを有するクライアント１１２により頻繁にインストールされ、かつ／または実行されるファイルは、高いレピュテーションスコアを受ける可能性が高い。逆に、低い衛生スコアを有するクライアント１１２のみに頻繁にインストールまたは実行されるファイルは、低いレピュテーションスコアを受ける可能性が高い。

【００５４】

レピュテーション計算モジュール４１６の一実施形態は、データのクロス混合に基づいてレピュテーションスコアを計算する。例えば、マルウェアがクライアントで頻繁に検出されるため、クライアント１１２のセットが低い衛生スコアを受けると想定する。レピュテーション計算モジュール４１６は、そのセット内のクライアントが頻繁に訪れるウェブサイトに低いレピュテーションスコアを割り当てることができる。したがって、モジュール４１６は、そのウェブサイトがマルウェアに直接関連がない場合であっても、レピュテーションスコアをウェブサイトに割り当てるためにマルウェア検出を活用する。

【００５５】

一実施形態では、レピュテーション計算モジュール４１６は、重みを特定のクライアントに割り当て、次に、その重みを使用して、クライアントが遭遇したファイル、ウェブサイト、および他のエンティティのレピュテーションスコアに影響を与えることにより、レピュテーションスコアを計算する。特別なプログラムに入会し、かつ／または他の基準を満たす非常に高い衛生スコアを有する特定のクライアントは、「スーパークライアント」として指定され、それらクライアントからのデータは、遭遇するエンティティのレピュテーションスコアに対して大きな影響を及ぼす。例えば、１つまたは複数のスーパークライ

アントが特定のファイルを実行するか、または特定のウェブサイトを訪れる場合、それらファイルまたはウェブサイトが正当な（すなわち、悪意のない）ものである可能性が非常に高いため、レピュテーション計算モジュール４１６は、高いレピュテーションスコアをファイルまたはウェブサイトに割り当てる。

【００５６】

エンティティに割り当てられたレピュテーションスコアは、時間の経過に伴って進化し得る。一実施形態はまず、以前に未知のファイル、ウェブサイト、または他のエンティティに低いレピュテーションスコアを割り当てる。この初期低スコアは、真の評判（レピュテーション）を評価するのに十分なクライアントがエンティティに遭遇するまで、エンティティが潜在的に悪意のあるものとして扱われる「審査期間」を表す。したがって、初期レピュテーションスコアは、このエンティティに遭遇するクライアント１１２の数が増大するにつれて変更される可能性が高い。初期低レピュテーションスコアを有するファイルは、高い衛生スコアを有するクライアントによりインストールされ実行される場合、より高いレピュテーションスコアを受けることができる。実際に、高い衛生スコアを有するクライアント１１２のユーザが、低いレピュテーションスコアを有することを示すダイアログボックスを見た後にファイルのインストールを選択する場合、これは、そのファイルがより高いレピュテーションスコアに値することの強力な信号である。レピュテーション計算モジュール４１６の実施形態は、これらの種類の動作を観察し、エンティティのレピュテーションスコアを常時更新する。

【００５７】

マルウェア受信モジュール４１８は、クライアント１１２においてマルウェア検出モジュール３１０により提出された潜在的なマルウェアを記憶する。いくつかの実施形態では、マルウェア受信モジュール４１８は、ネットワーク１１４上でクライアント１１２からの多数の提出を受信する。多くの提出があるため、それぞれが表すおおよそのリスク量により提出をランク付けすることが望ましい。このランク付けにより、セキュリティ専門家は、提出に優先度を付け、最も危険なものから最初に解析することができる。

【００５８】

したがって、マルウェア受信モジュール４１８の実施形態は、少なくとも部分的にマルウェアのレピュテーションスコアおよび／または使用頻度に基づいて提出をランク付ける。低いレピュテーションスコアを有し、多くのクライアント１１２が遭遇した提出ファイルは、比較的少数のクライアントが遭遇するファイルよりも高い優先度を有する。良好なレピュテーションスコアを有する提出ファイルには、低いランクが割り当てられ、かつ／または効率的に無視される。

【００５９】

図５は、一実施形態による、クライアント１１２にセキュリティを提供するためにセキュリティモジュール１１６により実行されるステップを示すフローチャートである。他の実施形態は、示されているステップを異なる順序で実行し、かつ／または異なるもしくは追加のステップを実行する。さらに、ステップのうちのいくつかまたはすべては、セキュリティモジュール１１６以外のモジュールにより実行することができる。

【００６０】

セキュリティモジュール１１６は、マルウェア検出のためにクライアント１１２の状態、記憶装置２０８に存在するファイル、および／または特定の芳しくないウェブサイトの閲覧等の動作を監視する（５１０）。セキュリティモジュール１１６は、監視される状態に基づいてクライアント１１２の衛生スコアを計算する（５１２）。例えば、多くのマルウェア検出が所与の時間期間内に発生する場合、クライアント１１２は低い衛生スコアを受ける可能性が高い。セキュリティモジュール１１６は、別個の報告またはサーバへの別の報告の部分として、衛生スコアをレピュテーションサーバ１１０に提供する。

【００６１】

ある時点で、セキュリティモジュール１１６は、クライアント１１２が遭遇したエンティティのレピュテーションスコアを取得する（５１４）。例えば、セキュリティモジュー

ル１１６が、記憶装置２０８に記憶された特定のファイルを識別するか、またはクライアントブラウザがウェブサイトからファイルをダウンロードしようとするかもしれない。セキュリティモジュール１１６は、ファイルのハッシュ等の識別子を使用して遭遇したエンティティを識別し、その識別子をレピュテーションサーバ１１０に送信し、応答として、エンティティのレピュテーションスコアを受信する。セキュリティモジュール１１６は、例えば、レピュテーションスコアを閾値と比較し、かつ／またはそれについてのメッセージをユーザに表示することにより、レピュテーションスコアを査定する（５１６）。いくつかの実施形態では、セキュリティモジュール１１６は、、エンティティのレピュテーションスコアを取得し査定している間、そのエンティティが関わる動作を任意に中止する。セキュリティモジュール１１６またはユーザは、査定の結果に基づいて動作を任意にキャンセルし、かつ／または別の動作を実行する。セキュリティモジュール１１６は、エンティティとの遭遇、エンティティ識別子、および査定の結果（例えば、ユーザがエンティティが関わる動作をキャンセルしたか否か）をレピュテーションサーバ１１０に報告する（５１８）。一実施形態では、報告は、クライアント１１２の衛生スコアを含み、サーバ１１０が、査定の結果として実行されたあらゆる動作に基づいて、エンティティのレピュテーションスコアをさらに改良できるようにする。

【００６２】

一実施形態では、セキュリティモジュール１１６は、エンティティとの遭遇をレピュテーションサーバ１１０に報告するが、それに応答して、レピュテーションスコアを必ずしも受信するとは限らない。例えば、セキュリティモジュール１１６は、記憶装置２０８上の静的ファイル等のクライアント１１２が遭遇したエンティティをレピュテーションサーバ１１０に報告して、クライアント１１２（およびその衛生スコア）とクライアント１１２が遭遇したエンティティとの関連付けを作成する。この技法を使用して、環境１００に種を播き、エンティティの初期レピュテーションスコアを作成することができる。

【００６３】

図６は、一実施形態によるレピュテーションサーバ１１０により実行されるステップを示すフローチャートである。レピュテーションサーバ１１０の実施形態が、複数のクライアント１１２と同時に通信し、複数のエンティティのレピュテーションスコアを計算することを当業者は認識するであろう。したがって、レピュテーションサーバ１１０の実施形態は、図６のステップの複数のインスタンスを同時に実行し得る。他の実施形態は、示されるステップを異なる順序で実行し、かつ／または異なるもしくは追加のステップを実行する。さらに、ステップのうちのいくつかまたはすべては、レピュテーションサーバ１１０以外のサーバにより実行することができる。

【００６４】

レピュテーションサーバ１１０は、クライアント１１２から衛生スコアを受信する（６１０）。上述したように、衛生スコアは、クライアントの信頼性の評価を表す。レピュテーションサーバ１１０は、監視されたクライアント状態を記述するデータも受信する（６１２）。これらデータは、ファイル、プログラム、およびウェブサイト等のエンティティとの遭遇を記述する。例えば、データは、クライアントにダウンロードされたファイル、インストールされたファイル、および／または実行されたファイル、ならびにクライアントが訪れたウェブサイトを記述することができる。

【００６５】

レピュテーションサーバ１１０は、クライアント１１２が遭遇したエンティティのレピュテーションスコアを計算する（６１４）。レピュテーションスコアは、クライアント１１２の衛生スコアに基づく。サーバ１１０は、高い衛生スコアを有するクライアント１１２が頻繁に遭遇するファイルには、高いレピュテーションスコアを計算し得る。同じ趣旨で、サーバ１１０は、低い衛生スコアを有するクライアント１１２が最も頻繁に遭遇するファイルには、低いレピュテーションスコアを計算し得る。

【００６６】

レピュテーションサーバ１１０は、エンティティのレピュテーションスコアをクライア

ント１１２に提供する（６１６）。例えば、レピュテーションサーバ１１０は、ハッシュにより識別されたファイルのレピュテーションスコア要求を受信し、それに応答して、スコアを提供し得る。クライアント１１２および／またはクライアントのユーザは、スコアを査定して、エンティティが正当なものであるか否かを判断する。一実施形態では、レピュテーションサーバ１１０は、遭遇および結果査定に基づいてレピュテーションスコアを常時更新する。

【００６７】

図７は、一実施形態による提出エンティティに優先度を決定するためにレピュテーションサーバ１１０により実行されるステップを示すフローチャートである。他の実施形態は、示されたステップを異なる順序で実行し、かつ／または異なるもしくは追加のステップを実行する。さらに、ステップのうちのいくつかまたはすべては、レピュテーションサーバ１１０以外のサーバにより実行することができる。

【００６８】

レピュテーションサーバ１１０は、マルウェアが検出されたか、またはマルウェアの疑いのあるファイルを有するクライアント１１２から提出を受信する（７１０）。これら提出は、悪意のあるソフトウェアを有するファイルおよび誤検出または他の理由により正当なソフトウェアを有するファイルを含み得る。レピュテーションサーバは、レピュテーションスコアに基づいて提出の優先度を決定する（７１２）。低いレピュテーションスコアを有し、かつ／またはクライアント１１２が頻繁に遭遇する提出ファイルは一般に、高い優先度を受ける。逆に、高いレピュテーションスコアを有し、かつ／またはクライアント１１２が希に遭遇する提出ファイルは一般に、より低い優先度を受ける。セキュリティ専門家は、優先度を使用して、提出ファイルをランク付け、どの提出を解析するかを判断する。

【００６９】

本発明の実施形態の上記説明は、説明のために提示され、網羅的である、すなわち本発明を開示された厳密な形態に限定する意図はない。上記開示に照らして多くの変更および変形が可能なことを当業者は理解することができる。

【００７０】

この説明のいくつかの部分には、情報に対する動作のアルゴリズムおよび象徴的表現に関して本発明の実施形態が説明される。これらアルゴリズム的な説明および表現は一般に、他の当業者に作業の実質を効率的に伝えるために、データ処理の分野の当業者により使用される。これら動作は、機能的、計算的、または論理的に説明されるが、コンピュータプログラムまたは同等の電気回路、マイクロコード等により実施されると理解される。さらに、一般性を失わずに、これら動作構成をモジュールと呼ぶことが場合により都合のよいことも証明されている。説明された動作および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、またはこれらの任意の組み合わせで具現し得る。

【００７１】

本明細書において説明される任意のステップ、動作、またはプロセスは、単独で、または他の装置と組み合わせて、１つまたは複数のハードウェアまたはソフトウェアモジュールで実行または実施し得る。一実施形態では、ソフトウェアモジュールは、コンピュータプロセッサにより実行されると、説明されるステップ、動作、またはプロセスのうちの任意のものまたはすべてを実行するコンピュータプログラムコードを含むコンピュータ可読媒体を備えたコンピュータプログラム製品を使用して実施される。

【００７２】

本発明の実施形態は、本明細書における動作を実行する装置にも関し得る。この装置は、要求される目的に向けて特に構築してもよく、かつ／またはコンピュータに記憶されたコンピュータプログラムにより選択的にアクティブ化または再構成される汎用計算装置を備えてもよい。そのようなコンピュータプログラムは、有形のコンピュータ可読記憶媒体または電子命令の記憶に適し、コンピュータシステムバスに結合された任意の種類の媒体に記憶し得る。さらに、本明細書において参照される任意の計算システムは、単一のプロ

セッサを含んでもよく、または計算能力を高めるために複数のプロセッサ設計を利用したアーキテクチャであってもよい。

【００７３】

本発明の実施形態は、搬送波に具現されるコンピュータデータ信号にも関し得、コンピュータデータ信号は、コンピュータプログラム製品の任意の実施形態または本明細書において説明される他のデータの組み合わせを含む。コンピュータデータ信号は、有形の媒体で提示される製品であるか、または搬送波であり、搬送波に変調もしくはその他の様式で符号化され、有形であり、任意の適した伝送方法に従って伝送される。

【００７４】

最後に、本明細書において使用される用語は主に、読みやすさおよび説明のために選択されており、本発明の主旨を明確に説明するため、または限定するために選択されていない場合もある。したがって、本発明の範囲は、この詳細な説明により限定されず、むしろ、本明細書に基づいて出願上で発行される任意の請求項により限定されることが意図される。したがって、本発明の実施形態の本開示は、以下の特許請求の範囲に記載される本発明の範囲の限定ではなく説明を意図される。

【図１】

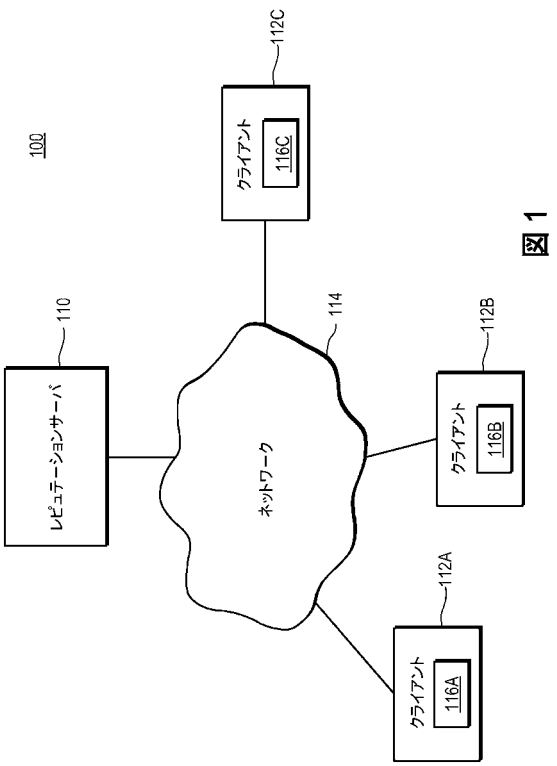

図１

【図２】

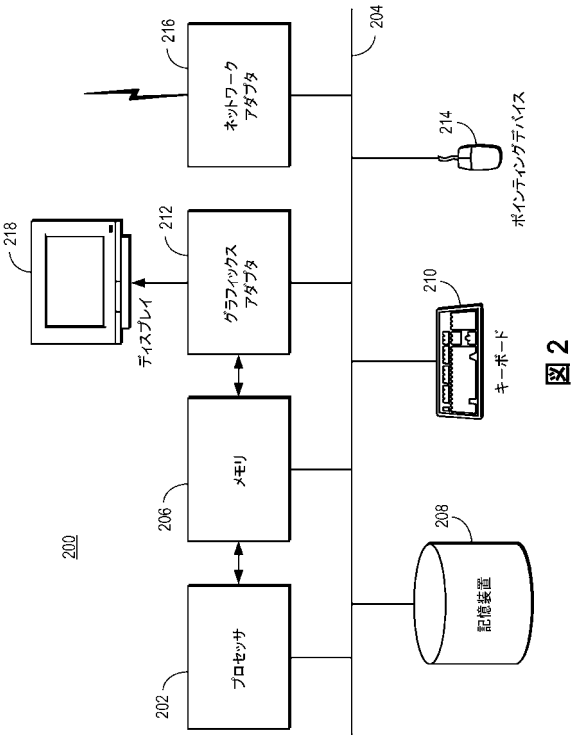

図２

【図３】

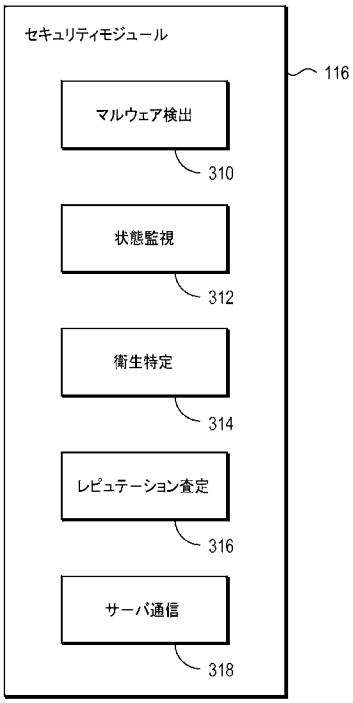

図３

【図４】

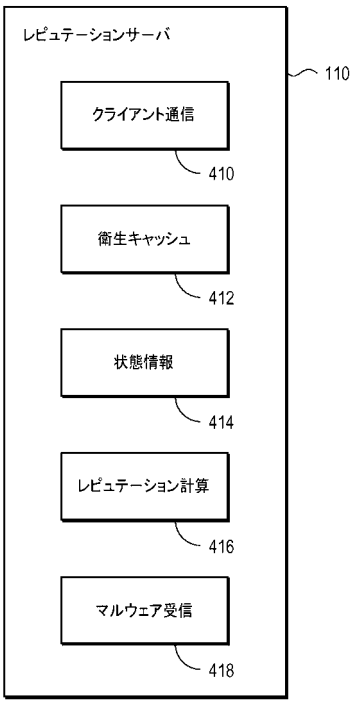

図４

【図５】

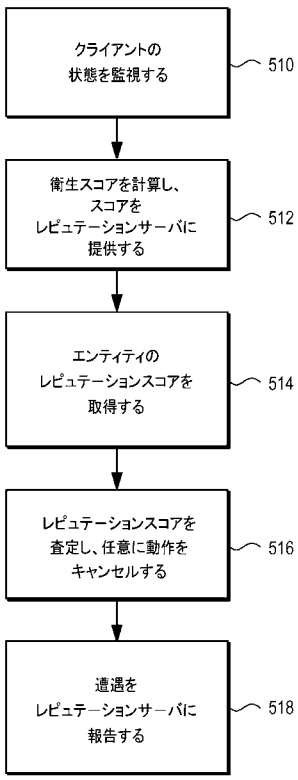

図５

【図６】

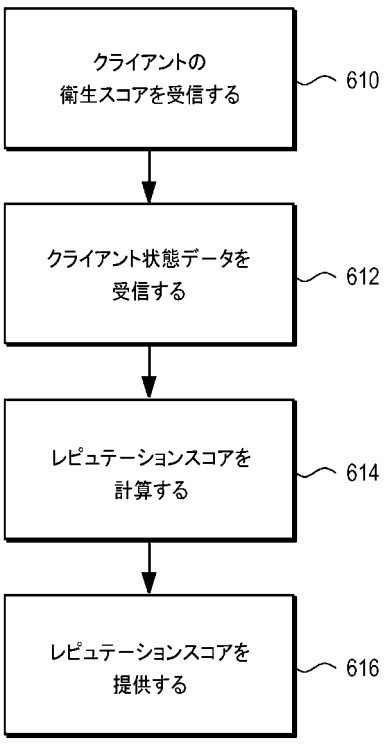

図６

【図７】

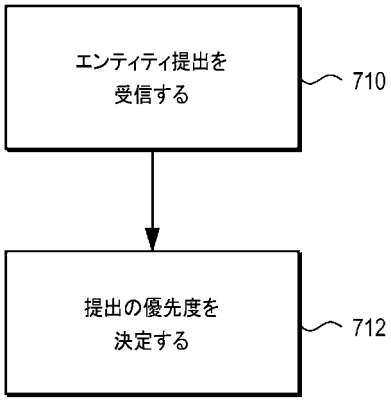

図７

フロントページの続き

(72)発明者　キャリー・エス・ナッチェンバーグ
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　シマンテック・コーポレーション内

審査官　宮司　卓佳

(56)参考文献　特開２００６－２４４００７（ＪＰ，Ａ）
特開２００４－３６１９９６（ＪＰ，Ａ）
特開２００４－０７０６７４（ＪＰ，Ａ）
特開２００８－１５８９５９（ＪＰ，Ａ）
特開２００６－３１８２８６（ＪＰ，Ａ）
米国特許出願公開第２００６／０２５３５８３（ＵＳ，Ａ１）
米国特許出願公開第２００８／０２６３６７７（ＵＳ，Ａ１）
米国特許出願公開第２００８／０２５５９７７（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５６