(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-79901
(P2010-79901A)
(43)公開日　平成22年4月8日(2010.4.8)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/22	(2006.01)	G06F	9/06	660N	5B276

審査請求 未請求　請求項の数 20　ＯＬ　（全 15 頁）

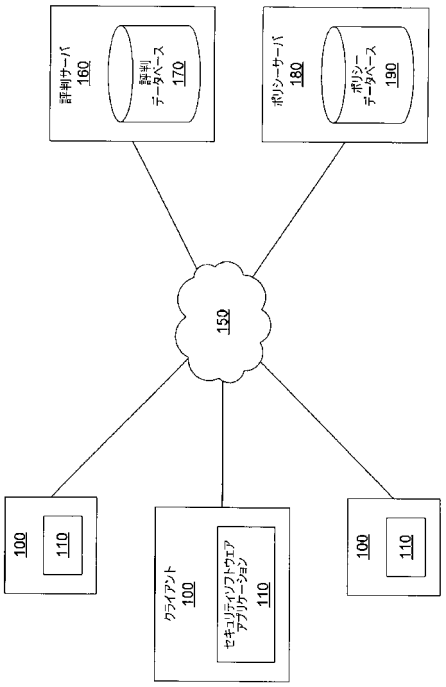
(21)出願番号　特願2009-217767 (P2009-217767)
(22)出願日　平成21年9月18日 (2009.9.18)
(31)優先権主張番号　12/238300
(32)優先日　平成20年9月25日 (2008.9.25)
(33)優先権主張国　米国 (US)

(71)出願人　504206263
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９５０１４　クパチーノ，スティーブンズ・クリーク・ブルバード，２０３３０
(74)代理人　100077539
弁理士　飯塚　義仁
(74)代理人　100114742
弁理士　林　秀男
(74)代理人　100125265
弁理士　貝塚　亮平

最終頁に続く

(54)【発明の名称】アプリケーションの評判に応じて段階的に制限を実施する方法およびそのコンピュータプログラム

(57)【要約】　（修正有）
【課題】合法なソフトウェアが作動し、クライアントのリソースを使用するのを可能としつつ、マルウェアからクライアントを守る。
【解決手段】クライアント１００上のセキュリティソフトウェアアプリケーション１１０は、クライアント１００上のアプリケーションからのリソースの要求を監視し、そのアプリケーションの評判を決定する。アプリケーションの評判は、遠隔の評判サーバ１６０から取得された評判スコアにより測定される。セキュリティソフトウェアアプリケーション１１０は、アプリケーションの評判に基づくアプリケーションのための可能なアクセスポリシーの段階的セットから１つのアクセスポリシーを決定する。セキュリティソフトウェアアプリケーション１１０は、アプリケーションのリソースの要求にアクセスポリシーを適用する。
【選択図】図１



【特許請求の範囲】
【請求項１】
アプリケーションの評判に応じてアプリケーション制限を実施する方法であって、
クライアント上のアプリケーションからのリソースの要求を監視するステップと、
前記アプリケーションに関連した評判の基準を決定するステップと、
前記アプリケーションに関連した評判の基準の少なくとも一部に基づいて、３つ以上の可能なアクセスポリシーのセットから１つのアクセスポリシーを選択するステップと、
前記アプリケーションからのリソースの要求に対して前記選択されたアクセスポリシーを実施するステップと
を含むことを特徴とする方法。
【請求項２】
前記アプリケーションに関連した評判の基準を決定するステップは、ネットワークを介して評判サーバから評判スコアを検索するステップを含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記可能なアクセスポリシーのセットは、
前記リソースを要求するアプリケーションが第１の閾値より大きい評判を有するならば、いずれかのリソース要求を可能にするアクセスポリシーと、
前記リソースを要求するアプリケーションが第２の閾値未満の評判を有するならば、いずれのリソースの要求も拒むアクセスポリシーと、
前記リソースを要求するアプリケーションが前記第１の閾値よりも低く且つ前記第２の閾値よりも高い範囲の評判を有するならば、いくつかのリソースの要求を許可するとともに、その他のリソースの要求を拒む少なくとも１つのアクセスポリシーと
を備えることを特徴とする請求項１に記載の方法。
【請求項４】
前記３つ以上の可能なアクセスポリシーのセットは、前記アプリケーションの評判スコアの機能として、クライアントリソースへのアクセスレベルの連続的スケールを含むことを特徴とする請求項１に記載の方法。
【請求項５】
前記アクセスポリシーを選択するステップは、アクセスポリシーへの評判スコアの予め定められたマッピングを参考にするステップを含むことを特徴とする請求項１に記載の方法。
【請求項６】
前記アクセスポリシーは、ネットワークを介してポリシーサーバから取得されることを特徴とする請求項１に記載の方法。
【請求項７】
前記アクセスポリシーは、前記アプリケーションが前記クライアントのリソースのサブセットにアクセスするのを可能にすることを特徴とする請求項１に記載の方法。
【請求項８】
前記選択されたアクセスポリシーを実施するステップは、アプリケーション／リソース仮想化、アプリケーションネットワークファイアウォール、ネットワークアクセス制御、サンドボックス、および阻止動作ポリシー実施ポイント技術の１つ以上を用いるステップを含むことを特徴とする請求項１に記載の方法。
【請求項９】
アプリケーションの評判に応じてアプリケーション制限を実施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、クライアント上のアプリケーションに関連した評判の基準を決定する手順を実行させるための評判モジュールと、
コンピュータに、前記評判モジュールによって決定された前記アプリケーションに関連した評判の基準を取得し、該アプリケーションに関連した評判の基準の少なくとも一部に

基づく３つ以上のアクセスポリシーのセットから１つのアクセスポリシーを選択する手順を実行させるためのポリシーモジュールと、
コンピュータに、前記ポリシーモジュールによって選択されたアクセスポリシーを取得し、前記アプリケーションからのクライアントのリソースの要求に対して前記選択されたアクセスポリシーを実施する手順を実行させるためのセキュリティモジュールと
を含むことを特徴とするコンピュータプログラム。
【請求項１０】
前記評判モジュールは、コンピュータに、ネットワークを介して前記評判サーバから評判スコアを検索することにより、前記アプリケーションに関連した評判の基準を決定する手順を実行させるように構成されることを特徴とする請求項９に記載のコンピュータプログラム。
【請求項１１】
前記可能なアクセスポリシーのセットは、
前記リソースを要求するアプリケーションが第１の閾値より大きい評判を有するならば、いずれかのリソースの要求を可能にするアクセスポリシーと、
前記リソースを要求するアプリケーションが第２の閾値未満の評判を有するならば、いずれのリソースの要求も拒むアクセスポリシーと、
前記リソースを要求するアプリケーションが前記第１の閾値よりも低く且つ前記第２の閾値よりも高い範囲の評判を有するならば、いくつかのリソースの要求を可能にするとともに、その他のリソース要求を拒む少なくとも１つのアクセスポリシーと
を備えることを特徴とする請求項９に記載のコンピュータプログラム。
【請求項１２】
前記３つ以上の可能なアクセスポリシーのセットは、前記アプリケーションの評判スコアの機能として、クライアントリソースへのアクセスレベルの連続的スケールを含むことを特徴とする請求項９に記載のコンピュータプログラム。
【請求項１３】
前記ポリシーモジュールは、コンピュータに、アクセスポリシーへの評判スコアの予め定められたマッピングを参考にすることにより、前記アクセスポリシーを選択する手順を実行させるように構成されることを特徴とする請求項９に記載のコンピュータプログラム。
【請求項１４】
前記ポリシーモジュールは、コンピュータに、ネットワークを介してポリシーサーバから前記アクセスポリシーを取得する手順を実行させるように構成されることを特徴とする請求項９に記載のコンピュータプログラム。
【請求項１５】
前記アクセスポリシーは、前記アプリケーションが前記クライアントのリソースのサブセットにアクセスするのを可能にすることを特徴とする請求項９に記載のコンピュータプログラム。
【請求項１６】
前記セキュリティモジュールは、コンピュータに、アプリケーション／リソース仮想化、アプリケーションネットワークファイアウォール、ネットワークアクセス制御、サンドボックス、および阻止動作ポリシー実施ポイント技術の１つ以上を用いて、前記選択されたアクセスポリシーを実施する手順を実行させるように構成されることを特徴とする請求項９に記載のコンピュータプログラム。
【請求項１７】
実体の評判に応じてアプリケーション制限を実施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、
クライアント上のリソースを使用する実体による試みを監視する手順と、
前記実体の評判スコアを取得する手順と、
少なくとも前記実体の評判スコアの一部に基づく前記実体の前記リソースへのアクセス

レベルを前記リソースへのフルアクセスの許可からアクセスの不許可の間で決定する手順と、
前記決定されたアクセスレベルに応じて、前記実体による前記リソースの制限された使用を可能にする手順と
を実行させることを特徴とするコンピュータプログラム。
【請求項１８】
前記実体は、前記クライアント上で実行しているアプリケーションを含むことを特徴とする請求項１７に記載のコンピュータプログラム。
【請求項１９】
前記実体はウェブサイトを含むことを特徴とする請求項１７に記載のコンピュータプログラム。
【請求項２０】
前記評判スコアは、ネットワークを介して評判サーバから取得されることを特徴とする請求項１７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】
本発明は、一般にコンピュータセキュリティソフトウェアに関し、より詳細には、アプリケーションの評判に基づいてアプリケーションの制限を実施することに関する。
【背景技術】
【０００２】
現代のコンピュータを攻撃可能な種々の悪意のあるソフトウェア（マルウェア）がある。マルウェアの脅威は、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、およびフィッシングウェブサイトを含む。現代のマルウェアは、しばしば、攻撃者に金融的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などの重要な情報を不正に取り込むことができる。同様に、マルウェアは、攻撃者が危険に曝されたコンピュータにアクセスし、それを制御することを可能にする隠れたインタフェースを提供することができる。
【０００３】
古典的なマルウェアは通常多くのコンピュータに大量に配布されていたが、現代のマルウェアは、しばしば、比較的一握りのコンピュータのみをターゲット（標的）として送られる。例えば、特定の企業の特定の部門のコンピュータをターゲットにするようにトロイの木馬プログラムを設計することができる。同様に、偽電子メールは、ある銀行や他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むことができる。大量に配布されたマルウェアは、しばしば、マルウェアを検出するためのサイン（署名）スキャニングや挙動監視発見解決法（挙動監視ヒューリスティックス）などの技術を用いる従来のセキュリティソフトウェアにより検出され、無能力化され得る。しかしながら、同じマルウェアの実例が少なく、セキュリティソフトウェアがそれを認識するように構成されていないので、これらの技術はターゲットとなる脅威を検出するのにあまり効果的ではない。
【０００４】
大量に配布されたマルウェアでさえ検出するのがさらに難しくなってきている。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。結果として、マルウェアは広く配布（分散）されるが、少数のユーザのみが全く同じコードを有する。このため、マルウェアを検出するためには、署名を生成し、サインスキャニングベースの技術を用いることは非現実的となる。ときには、異なるバージョンのマルウェアは、発見的方法や他の技術を通してマルウェアを検出するのを困難にする異なる機能を実行する。
【０００５】
また、マルウェアを検出するための署名、発見的方法および他の技術を開発するために

、マルウェアを解析するセキュリティ会社は、多くのマルウェアの発信を受信する。セキュリティ会社は、ときには、発信されたマルウェアにより提起される脅威を効果的に測定する方法を持っていない。例えば、セキュリティ会社は、発信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、マルウェアの特定部分がどの程度広く配布されたかを知り得ない。結果として、セキュリティ会社は、最大の脅威を継続する発信を解析することに集中するために、マルウェアの発信を格付けしあるいは優先順位を付けるための困難な時間を必要とする。

【０００６】

これらの問題は、疑わしいマルウェアをブロック（遮断）するためにブラックリストを用い、あるいは、是認されたクリーンなソフトウェアのみを許可するためにホワイトリスト（優良ソフトウェアのリスト）を用いる評判ベースのシステムに影響を与えていた。ブラックリスト化方法は、積極的に突然変異し、急激に増殖するマルウェアを識別するために現在必要とされる莫大な量のフィンガープリント（はっきりとした特徴）により破綻してしまう。同様に、ホワイトリストポリシーは、公知の優良なソフトウェアが起動することのみを許可するものであるが、あまりにも不完全であり、そのため、顧客の環境（ほとんどの企業環境でさえ）にとってはあまりにも限定的である。公知の優良なアプリケーションの純粋なホワイトリストデータベースの保守および適時の配布は、正規のソフトウェアの配布と歩調を合わせることができず、結果として、ホワイトリストデータベースが時代遅れであるため、あまりにも多くの合法なソフトウェアがブロックされてしまう。したがって、ブラックリストおよびホワイトリスト解決法はともに、新しいマルウェアと合法なソフトウェアが開発される速い割合のために、これらのシステムが新しい未知のコードを適切に取り扱えないような経験をする。

【０００７】

いくつかの以前のシステムは、未知のサイトがシステムリソースの仮想コピー上で動作することを可能にするために、アプリケーション仮想化と類似する仮想サンドボックスを用いていた。他のシステムは、未知のアプリケーションにより修正されるとき敏感なリソースの複写コピーを作成するために提供するアプリケーションを用いていた。しかしながら、これらの解決法は、単に二値的であり、アプリケーションは、そのアプリケーションがシステムにとって公知であるか未知であるかに基づいて、実際のリソースかコピーのいずれかへのアクセスを提供される。そのため、合法なソフトウェアが作動し、クライアントのリソースを使用するのを可能としつつ、マルウェアからクライアントを守る新しい方法が当該技術分野において必要である。

【発明の概要】

【０００８】

以前の解決手法と対照的に、本発明の実施形態は、評判スケールに応じてアプリケーションに与えられる信頼度に従って、クライアントのリソースへの段階的アクセスをそのアプリケーションに提供する。アプリケーションの信頼レベルとクライアントのリソースへのアクセスレベルとの間のそのような二値ではないマッピングは、そのアプリケーションがクライアントのリソースにアクセスしようと試みるとき自動的に、ユーザに意識させないで適用されればよい。一実施形態では、評判ベースのシステムは、段階的信頼スケールと、アクセスなしからフルアクセスまでの段階的スケールに沿ったリソース双方向性のためのアプリケーション機能を制限しあるいは許可するポリシー実施機構とを利用する。これは、以前のブラックリスト化とホワイトリスト化のアプローチの合理的な妥協案を考慮に入れる。ここでは、未知のアプリケーションは、（ブラックリスト化の場合のような）フルアクセスを与えられるか、（ホワイトリスト化の場合のような）アクセスを完全に禁じられるかのいずれかであろう。

【０００９】

本発明の一実施形態では、クライアント上のアプリケーションからのリソース要求を監視して、そのクライアント上のセキュリティソフトウェアは、そのアプリケーションの評判の基準を決定する。アプリケーションの評判は、遠隔の評判サーバから取得され得る評

判スコアによって測定されてもよい。そして、セキュリティソフトウェアは、アプリケーションの評判に基づいてアプリケーションのアクセスポリシーを選択する。ここで、アクセスポリシーは、アプリケーションが公知であるか未知であるかに基づく単なる２値ではない。例えば、アクセスポリシーは、３つ以上のアクセスポリシーのセットから選択されればよく、セキュリティポリシーは、フルアクセスの許可とアクセスの不許可との間のアプリケーションのアクセスレベルを要求されたリソースに単に提供すればよい。一度このアクセスポリシーを決定すると、セキュリティソフトウェアは、例えば、アクセスを許可しもしくは許可しないために、あるいは制限されたアクセスを許可するために、アクセスポリシーの制限をリソース要求に適用する。

【００１０】

本発明の実施形態は、アプリケーションの制限を適用することに限定されず、その代わりに、クライアントのリソースにアクセスしようと試みるあらゆる実体の制限を適用してもよい。例えば、これらの実体は、ウェブサイト、ネットワークを介してクライアントに接続される他のコンピュータシステム、周辺装置、および、クライアントのリソースにアクセスするように試み得るその他のハードウェアもしくはソフトウェア実体を含めばよい。

【図面の簡単な説明】

【００１１】

【図１】本発明の一実施形態におけるコンピュータ環境の高度ブロック図である。

【図２】本発明の一実施形態における評判サーバまたはクライアントとして用いられる典型的なコンピュータを示す高度ブロック図である。

【図３】本発明の一実施形態におけるセキュリティソフトウェアアプリケーションの図である。

【図４】本発明の一実施形態におけるアプリケーション制限を実施するための方法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】

【００１２】

添付図面は、単に例示の目的のために本発明の種々の実施形態を描写する。当業者は、本明細書に例示の構造および方法の代わりの実施形態が開示される本発明の原理を逸脱することなく利用され得ることを以下の記述から容易に認識するであろう。

【００１３】

図１は、クライアント１００において悪意のあるソフトウェアを検出してブロックするためのユーザ支援セキュリティシステムを含むネットワーク図を示す。一実施形態では、クライアント１００は、ファイルをダウンロードしたり、インストールしたり、あるいは実行したり、また、ネットワーク１５０上のウェブサイトを閲覧（ブラウジング）したりすることを含む活動（アクティビティ）を実行するために一人以上のユーザにより用いられるコンピュータである。クライアント１００は、例えば、ユーザがネットワーク１５０を介してウェブサーバまたは他のコンピュータからコンテンツを検索および表示するのを可能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ればよい。他の実施形態では、クライアント１００は、携帯情報端末（ＰＤＡ：personal digital assistant）、携帯電話、ポケットベル、テレビジョン「セットトップボックス」、またはあらゆる他の適当な計算装置などのコンピュータ以外のネットワーク対応装置である。また、本明細書において、用語「クライアント」は、悪意のあるコードまたは他の脅威を構成し得るファイルあるいは他の実体（エンティティ）に遭遇するサーバやゲートウェイなどのコンピュータを含む。例えば、クライアント１００は、企業ネットワークとインターネットの間にあるネットワークゲートウェイであればよい。また、クライアント１００は、他のクライアントがアクセス可能なファイルを格納するメールサーバまたはウェブサーバであってもよい。

【００１４】

セキュリティシステムは、評判サーバ１６０およびポリシーサーバ１８０をさらに備え

ていてもよい。評判サーバ１６０は、評判データベース１７０を含むか、あるいは別の方法で評判データベース１７０に接続される。評判データベース１７０は、評判の基準が追跡されるアプリケーションや他の実体の評判スコアを保持する。評判サーバ１６０は、評判データベース１７０内の評判スコアへのアクセスを提供される。ポリシーサーバ１８０は、ポリシーデータベース１９０を含むか、あるいは別の方法でポリシーデータベース１９０に接続される。ポリシーデータベース１９０は、本発明の実施形態によりサポートされるアプリケーションや他の実体のポリシーセットを保持する。ポリシーサーバ１８０は、ポリシーデータベース１９０内のポリシーへのアクセスを提供する。以下、評判サーバ１６０およびポリシーサーバ１８０の動作・機能をより詳細に説明する。

【００１５】

ネットワーク１５０は、クライアント１００、評判サーバ１６０およびポリシーサーバ１８０間の通信経路を表す。一実施形態では、ネットワーク１５０はインターネットである。また、ネットワーク１５０は、必ずしもインターネットの一部ではない専用または私用通信リンクを用いることもできる。一実施形態では、ネットワーク１５０は標準的な通信技術やプロトコルを利用する。そして、ネットワーク１５０は、イーサネット(登録商標)、８０２．１１、統合サービスデジタル通信網（ＩＳＤＮ）、デジタル加入者線（ＤＳＬ）、非同期転送モード（ＡＴＭ）などの技術を用いるリンクを含むことができる。同様に、ネットワーク１５０上で用いられるネットワーキングプロトコルは、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）などを含むことができる。ハイパーテキストマークアップ言語（ＨＴＭＬ）、拡張マークアップ言語（ＸＭＬ）などを含む技術あるいはフォーマットを用いて、ネットワーク１５０上で交換されるデータを表現することができる。さらに、セキュアソケットレイヤー（ＳＳＬ）、セキュアＨＴＴＰ、仮想私設通信網（ＶＰＮｓ）などの従来の暗号化技術を用いて、すべてまたはいくつかのリンクを暗号化してもよい。別の実施形態では、実体は、上述のものに代わり、あるいはそれに加えて、カスタムあるいは専用データ通信技術を用いることができる。

【００１６】

図２は、典型的なコンピュータ２００を示す高度ブロック図である。コンピュータ２００は、クライアント１００、評判サーバ１６０およびポリシーサーバ１８０の少なくともいずれかとして用いられればよい。バス２０４に接続されるプロセッサ２０２を示す。また、メモリ２０６、記憶装置２０８、キーボード２１０、グラフィックアダプタ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もバス２０４に接続される。ディスプレイ２１８はグラフィックアダプタ２１２に接続される。プロセッサ２０２は、インテル（ＩＮＴＥＬ）ｘ８６互換ＣＰＵなどのいずれかの汎用プロセッサであればよい。一実施形態では、記憶装置２０８は、ハードディスク装置であるが、書き込み可能なコンパクトディスク（ＣＤ）またはＤＶＤ、あるいはソリッドステートメモリ装置などのデータを格納可能なあらゆる他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、読出し専用メモリ（ＲＯＭ）、不揮発性ランダムアクセスメモリ（ＮＶＲＡＭ）、あるいはＲＡＭであればよく、プロセッサ２０２により用いられる指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、その他のポインティングデバイスであればよく、コンピュータ２００にデータを入力するためのキーボード２１０と協力して用いられる。グラフィックアダプタ２１２は、画像（イメージ）および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２００をネットワーク１５０に接続させる。

【００１７】

当技術分野で周知のように、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。本明細書で用いられるように、用語「モジュール」とは、コンピュータに読み取り可能な記憶媒体に格納され、あるいはコンピュータ２００の演算処理装置によりアクセスすることができる、特定の機能を提供するためのコンピュータ

プログラムロジックあるいはデータをいう。モジュールは、ハードウェア、ファームウェア、あるいはソフトウェアで実行されてもよい。一実施形態では、モジュールは、記憶装置２０８に格納され、メモリ２０６にロードされ、プロセッサ２０２により実行される。

【００１８】

図１の実体により用いられるタイプのコンピュータシステム２００は、実施形態およびその実体により用いられる処理パワーによって変更することができる。例えば、携帯電話であるクライアント１００は、典型的に制限された処理パワーおよび小さいディスプレイ２１８を有し、ポインティングデバイス２１４を有さない。逆に、評判サーバ１６０またはポリシーサーバ１８０は、本明細書に記述される機能を提供するために、協働する複数のブレードサーバを備えていてもよい。

【００１９】

一実施形態では、クライアント１００は、クライアント１００を監視するセキュリティソフトウェアアプリケーション１１０を実行する。一実施形態では、セキュリティソフトウェアアプリケーション１１０は、クライアント１００上で実行している処理を監視する。ここで、このような処理は悪意のあるコードを含んでもよい。例えば、セキュリティソフトウェアアプリケーション１１０は、クライアント１００のディスプレイにアイテムを表示するために、グラフィック機能の呼出などのクライアント１００上の行動を監視すればよい。セキュリティソフトウェアアプリケーション１１０に加えて、クライアント１００は、クライアント１００上の１つ以上の他のソースアプリケーションを格納し、実行してもよい。ソースアプリケーションは、実行可能なあらゆるタイプのファイル、（ＤＬＬのような）ライブラリ、マークアップ言語を含むドキュメント、あるいは実行可能なコードもしくは他の指令を含むクライアント１００上のその他のファイルを含んでもよい。

【００２０】

クライアント１００は、ネットワーク１５０を介して評判サーバ１６０と通信する。また、評判サーバ１６０は、例えば、クライアントコンピュータシステムが相互作用し得る種々のアプリケーションおよび他のソフトウェア実体の評判を追跡するためのユーザのオンラインコミュニティを維持するために、ネットワーク１５０を介して他の多くのクライアントコンピュータシステムと通信すればよい。２００６年１２月２９日に出願された米国特許出願第１１／６１８，２１５号は、クライアントの信憑性の評価を表す、種々のクライアントコンピュータシステムのためのクライアント予防措置スコアを用いて、実体の評判スコアを計算する方法およびシステムを開示する。この米国特許出願は参照により本出願に組み込まれる。これに関連して、クライアントの信憑性は、悪意のあるコードに感染するクライアントの傾向、他のコンピュータ関連の脅威、およびその脅威を避けるユーザの能力の少なくとも１つを参照すればよい。その代わりに、アプリケーションの評判スコアは、その他の所望の方法に従って計算されてもよい。その方法は、そのアプリケーションを利用するクライアントのセットの予防措置スコアに基づいてもよく、基づかなくてもよい。

【００２１】

他のユーザのコミュニティに基づく評判スコアを用いることは、遭遇するコンピュータ関連の実体を含むある活動に従事するという決定と、脅威を避けるユーザの能力とを関連付ける。このアプローチは、ファイル、ウェブサイト、およびその実体に関連したリスクを実際に測定する他の実体に評判スコアを割り当てるために、ユーザの集合的な情報（知力）を活用する。評判スコアは、明確に実体を評価または判断することをユーザに要求することなく計算されてもよい。また、評判スコアは、ファイル、ウェブサイト、または他の潜在的に悪意のある実体の最新の分析を要求することなく計算されてもよい。そのため、そのアプローチは、従来のサイン（署名）スキャニングや発見的方法技術を用いて識別され得ない相当量のマルウェアもしくは他の脅威があるコンピュータ環境に十分に適している。

【００２２】

図３は、クライアント１００により格納され、実行されるセキュリティソフトウェアア

プリケーション１１０の一実施形態を示す。セキュリティソフトウェアアプリケーション１１０は、評判モジュール３１０と、ポリシーモジュール３２０と、ポリシーデータベース３３０と、セキュリティモジュール３４０とを備える。以下に記述するように、セキュリティソフトウェアアプリケーション１１０の実施形態は、クライアント上のアプリケーションの対応する評判に応じて、クライアント上のアプリケーション制限の段階的実施を提供する。実施された制限は、クライアントのリソースへのアクセスを完全に許可しあるいは許可しなくてもよく、フルアクセスとアクセスなしの間のあるアクセス制限量を提供してもよい。

【００２３】

図４は、クライアント上のアプリケーションの対応する評判に応じてクライアントのアプリケーション制限の段階的実施を提供する処理を示す。図４に記述する動作は、クライアント１００上のセキュリティソフトウェアアプリケーション１１０により実行されてもよい。しかしながら、それらの動作は、ある実体またはソフトウェアモジュールによってすべてが実行される必要はない。セキュリティソフトウェアアプリケーション１１０の機能性を実行するために、ソフトウェアモジュールのあらゆる組み合わせが用いられてもよい。また、それらのいくつかは、クライアント１００と通信するクライアント１００以外のシステムにより実行されてもよい。

【００２４】

一実施形態では、セキュリティソフトウェアアプリケーション１１０は、クライアント上で起動している別のアプリケーションからのリソース要求を監視する（ステップ４１０）。例えば、セキュリティソフトウェアアプリケーション１１０は、クライアント１００上で現在起動しているある種類のまたはすべての処理を監視すればよい。これらの処理は、例えば、クライアントのディスプレイにアイテムを表示するグラフィック機能の呼出、クライアントのメモリの特定のエリアからの読み出しもしくはそこへの書き込み、ネットワークを介してクライアント外部との通信用の特定のポートの使用を含んでいればよい。これらは、単に、アプリケーションがクライアント１００のリソースを要求する処理の例であり、多くの変形や可能性が存在する。また、クライアントのメモリ、表示能力およびネットワークインタフェースなどの要求され得るクライアント１００の特定のリソースは大きく変化する。一実施形態では、セキュリティソフトウェアアプリケーション１１０は、疑わしいと決定されたクライアントリソースの特定のセット（メモリのある部分やあるＣＯＭポート（通信ポート）など）のみの要求を監視するように構成される。

【００２５】

一度、セキュリティソフトウェアアプリケーション１１０が特定のアプリケーションからのクライアントリソースの要求を監視したならば（ステップ４１０）、評判モジュール３１０は、アプリケーションの評判を決定する（ステップ４２０）。一実施形態では、アプリケーションの評判は評判スコアにより表現される。この評判スコアは、低い評判から高い評判（または信憑性）までの所定のスケール内の数値から構成されればよい。特定のアプリケーションの評判スコアは、評判ベースのシステムにより決定されるようなアプリケーションの信憑性の基準である。一実施形態では、評判モジュール３１０は、評判サーバ１６０からアプリケーションの評判スコアを取得する。評判サーバ１６０は、上述のような複数のアプリケーションの評判スコアを保持する。

【００２６】

そして、評判モジュール３１０は、アプリケーションの評判スコアをポリシーモジュール３２０に渡す。また、ポリシーモジュール３２０は、この評判スコアを用いて、アプリケーションのリソース要求に適用されるべきアクセスポリシーを選択する（ステップ４３０）。ポリシーモジュール３２０は、ポリシーデータベース３３０から選択されたアクセスポリシーを取得する。ポリシーデータベース３３０は、クライアント１００上に存在するか、クライアント１００と通信可能に接続される。ポリシーモジュール３２０がポリシーデータベース３３０からアクセスポリシーを直接取得するならば、ポリシーモジュール３２０は、そのアプリケーションにおける可能な評判スコアのセットと可能なアクセスポ

リシーの対応するセットの間のマッピングを定義するリファレンスを参考にしてもよい。このマッピングは、例えば、評判スコアと対応するアクセスポリシーとのテーブルにより実行されればよい。ここで、ポリシーモジュール３２０は、アプリケーションの評判スコアに対応するアクセスポリシーを単に選択する（ステップ４３０）。その代わりに、評判とアクセスポリシーの間のマッピングは、入力として評判スコアを与えられることに基づいてアクセスポリシーの連続的スケールを提供する機能を含むあらゆる他の適切な機構を備えていてもよい。

【００２７】

別の実施形態では、ポリシーモジュール３２０は、ネットワーク１５０を介して評判スコアをポリシーサーバ１８０に転送することによりアクセスポリシーを選択する。そして、ポリシーサーバ１８０は、アプリケーションのリソース要求に適用するアクセスポリシーを決定するために、（例えば、上述のような）適当なアクセスポリシーに評判スコアをマッピングする（関連付ける）。ポリシーサーバ１８０は、ポリシーデータベース１９０からこのアクセスポリシーを取得してもよい。そして、ポリシーサーバ１８０は、選択されたアクセスポリシーをポリシーモジュール３２０に送信する。

【００２８】

原則として、アプリケーションは、二値的なものよりもむしろ段階的スケールで、クライアントのリソースへのより多くのアクセスを与えられる。そのため、あるアプリケーションがより高い評判を有するほど、クライアントのリソースへのアクセスレベルが比較的高く許容される傾向にある。しかしながら、評判とアクセスの間のマッピングは、要求を作成しあるいはリソースを要求するアプリケーションに応じて異なる評判要求を効果的に課す異なるアプリケーションまたは異なるリソース要求によって異なってもよい。例えば、周知のソフトウェアプロバイダにより製造された第１のアプリケーションは、未知のソフトウェアプロバイダにより製造された第２のアプリケーションの評判スコアが第１のアプリケーションの評判スコアよりも高いとしても、第２のアプリケーションよりもクライアントのリソースへのより多いアクセスを与えられればよい。これは、段階的アプリケーション制限を設定することにおけるより多くの柔軟性を可能にする。

【００２９】

特定のアプリケーションのための可能なアクセスポリシーのセットは、多くの異なる方法において段階的制限を提供してもよい。アクセスポリシーと評判の間のマッピングは、高度に設定可能であってもよく、多くの異なる種類のマッピングが可能である。１つの分かりやすい例では、周知の優良なアプリケーションには制限がなく、周知の不良なアプリケーションは、どのリソースへのアクセスも許可されず、未知のアプリケーションは、敏感なリソースの仮想コピーを有する堅いサンドボックス内でのみ起動するのを許可される。この単純なポリシーは、部分的なアクセスのいくつかの段階がアプリケーションの評判に応じて存在するように、ソフトウェアの評判に基づくサンドボックス制限の段階的緩和で強化されてもよい。

【００３０】

また、アクセスポリシーのセットにより定義される制限は、特定のクライアントリソースにとって特有であってもよい。例えば、アクセスポリシーは、アプリケーションが利用し得る出力ポートを制限してもよい。高度に信頼されたアプリケーションは、あらゆる出力ポートを利用可能であるのに対し、中間的評判レベルのアプリケーションは、あるいくつかのポートのみを利用することが許されてもよく、非常に低い信頼レベルの別のアプリケーションは、どの出力ポートも利用することができなくてもよい（したがって、クライアントの外部にメッセージを送信することができない）。別の例では、アクセスポリシーは、システムメモリの部分と、読み出し、書き込みまたはそれらの部分の両方を行う能力とを定義する。アプリケーションがより信頼されればされるほど、このアプリケーションは、メモリのより多くの部分にアクセスすることができ、より適当にそれらの部分から読み出したり、そこに書き込んだりすることができる。さらに別の例では、アクセスポリシーは、所定の時間特定のリソースへのアクセスを提供してもよい。ここで、その時間は評

判スコアの機能である。そして、より高い評判スコアを有するアプリケーションは、低い評判スコアを有するアプリケーションほど頻繁にリソースへのリースを要求する必要がないだろう。大量のクライアントリソースおよびそれらのリソースに適用され得る可能な制限があるので、上記で提供される例は、本発明の実施形態で用いられ得るよりも単に可能なアクセスポリシーの小さいセットである。

【００３１】

一度アクセスポリシーがアプリケーションのために選択されると（ステップ４３０）、上述のように、ポリシーモジュール３２０は、セキュリティモジュール３４０へアクセスポリシーを伝達する。そして、セキュリティモジュール３４０は、そのアプリケーション上のアクセスポリシーを実施する（ステップ４４０）。このアプリケーションは、クライアントのリソースの１つ以上のためのアプリケーションの要求を制限したり、否定したりすることを含んでもよい。セキュリティモジュール３４０は、クライアントのリソースへのアプリケーションのアクセスを制限するための様々な公知の機構のいずれかを用いて、アクセスポリシーを実施してもよい（ステップ４４０）。これらの技術は、限定するものではないが、アプリケーション／リソース仮想化、アプリケーションネットワークファイアウォール、ネットワークアクセス制御、サンドボックス、および阻止動作ポリシー実施ポイント技術を含んでもよい。これらの技術は、アプリケーションがどの動作を実行可能とされているか、あるいはクライアント内のどのリソース（もしくは、どのリソースの仮想コピー）を制限して、所望のアプリケーション抑制の微細制御を提供してもよい。

【００３２】

サンドボックスを用いる一実施形態では、サンドボックスの制限は、種々の適当な技術のいずれかを用いて達成されればよく、それに適した多くの周知の技術がある。特に、本発明の実施形態は、いずれも商業的に利用可能な、アルティリス社（Altiris, Inc.）からのソフトウェア仮想化ソリーション（ＳＶＳ：Software Virtualization Solution）アプリケーション、シマンテック（Symantec）社からのノートンインターネットセキュリティ（ＮＩＳ）のアプリケーションファイアウォール、ＳＮＡＣサンドボックス（ウィンドウズ(登録商標)ステーション制御およびリソース仮想化）、あるいは、種々の発見的方法、阻止動作ポリシー実施ポイント構成、およびルール指定エンジンの仮想階層化機能性を利用すればよい。これらの技術により、セキュリティシステムは、信頼できないアプリケーション（すなわち、低い評判を有するアプリケーション）に重大なシステムリソースのコピーを選択的に提示し、インターネット活動を選択的に許可または否定し、いくつかの種類のアクセス（例えば、ＨＴＴＰ）を許可するが、その他（例えば、ＦＴＰ）を否定し、遠隔のおよび周知のサイトへのアクセスを許可するが、内部個人サイトへのアクセスを否定もしくは限定し、プログラムが同じ信頼レベルで他のプログラムと相互作用するのを許可するが、より高いレベル（もしくは他のレベル）では許可せず、並びに、クライアントのリソースにアクセスしてそれを利用するアプリケーションの能力の種々の他の制限を達成することができてもよい。

【００３３】

したがって、本発明の実施形態は、セキュリティソフトウェアシステムがアプリケーションの評判に応じてアプリケーション制限を実施するのを可能にする。しかしながら、クライアントのリソースを用いて公知の信頼できないアプリケーションを否定する単なるブラックリストやそれらのリソースを用いて公知の信頼できるアプリケーションのみを承認するホワイトリストよりもむしろ、本発明の実施形態は、セキュリティソフトウェアがアプリケーションの評判に基づくクライアントリソースへの複数のアクセスレベルを提供することができる段階的スケールを利用可能にする。これは、評判ベースのシステム内のセキュリティを維持しつつ、純粋なブラックリスト化またはホワイトリスト化アプローチの弱点の多くを避けるものである。

【００３４】

別の実施形態では、多くの場合、アプリケーションの評判が時間とともに変化し得るので、アプリケーションの評判が変化するにつれて、セキュリティソフトウェアアプリケー

ション１１０は、クライアントのリソースへの変化するアクセスレベルを提供する。図４に戻って、アプリケーションの評判が調整された後（ステップ４５０）、セキュリティソフトウェアアプリケーション１１０は、ステップ４１０～４４０を再度実行し、新しい評判スコアを反映させてもよい。これにより、評判が増加したか減少したかに応じて、多くのまたは少ないアクセスのいずれかを許可するクライアントのリソースのためのアプリケーションの要求に適用される異なるアクセスポリシーをもたらしてもよい。

【００３５】

新しいアプリケーションがリリースされると、例えば、アプリケーションについてのわずかなデータポイントしかないので、そのアプリケーションは高い評判を有し得ない。特に、良い予防措置または信頼性を有すると考えられるユーザは、そのアプリケーションをあまりインストールして使用しないかもしれない。そのため、初期段階では、セキュリティソフトウェアの実施形態は、完全にブロックするわけではないが、新しいアプリケーションのクライアントリソースへのアクセスを制限してもよい。有益に、これは、ユーザがアプリケーションの機能性の全部または一部のいずれかを未だにできる限り使用可能にしつつ、低い評判の新しいアプリケーションによる攻撃に対して、ユーザにある保護レベルを提供する。多くのユーザが新しいアプリケーションをインストールして使用し、それを信頼し始めるにつれて、アプリケーションの評判が上昇する傾向にあるだろう。これにより、新しいアプリケーションに対してより小さい制限的アクセスポリシーをセキュリティソフトウェアの実施形態に順次実施させる傾向があるだろう。このように、セキュリティソフトウェアは、クライアントシステムで起動する合法なソフトウェアを過度に制限することなく、このクライアントシステムを保護する目的で、種々のアプリケーションの変化する評判に動的および自動的に順応すればよい。

【００３６】

アプリケーションの制限の実施に関して説明したが、本発明の実施形態は、アプリケーションの制限を適用することのみに限定されない。その代わりに、本発明の実施形態は、クライアントのリソースにアクセスしようと試みるあらゆる実体への制限を適用してもよい。これらの実体は、限定するものではないが、クライアントがアクセス可能なウェブサイト、ネットワークを介してクライアントと通信可能な他のコンピュータシステム、クライアントに取り付け可能な周辺装置、および、クライアントのリソースへのアクセスを要求し、または他の方法でそのアクセスを得ようと試みることができるあらゆる他のハードウェアもしくはソフトウェア実体を含めばよい。これらの実体の評判は、上述のような評判サーバを用いて追跡されればよい。ここで、あるウェブサイトは、そのＵＲＬ、ネットワークネームもしくは製造番号アドレスによる別のコンピュータシステム、およびＭＡＣアドレスもしくはその一部による周辺装置によって識別されればよい。

【００３７】

本発明の実施形態の上記記述は、例証の目的で提示されたものであり、網羅的なものではなく、開示された正確な形式に本発明を限定するものでもない。関連技術の当業者は、上記開示を考慮して、多くの修正や変更が可能であることを認識することができる。

【００３８】

この記述のいくつかの部分は、情報の動作のアルゴリズムおよび記号的表現によって本発明の実施形態を記述する。これらのアルゴリズム的記述および表現は、データ処理技術の当業者によって通常用いられ、他の技術分野の当業者にそれらの作業の内容を伝達する。機能的に、計算機的に、あるいは論理的に記述されるが、これらの動作は、コンピュータプログラムもしくは同等の電気回路、マイクロコードなどにより実行され得ることを理解されたい。また、一般性の喪失なく、作用のこれらの配置（配列）をモジュールとして言及することは、ときには都合のよいものであると立証されている。記述された動作およびそれらの関連モジュールは、ソフトウェア、ファームウェア、ハードウェア、またはそれらのあらゆる組み合わせで具体化されればよい。

【００３９】

１つ以上のハードウェアまたはソフトウェアモジュールで、単独であるいは他の装置と

協働して、本実施形態に記述したステップ、動作あるいは処理のいずれかを実行してもよい。一実施形態では、ソフトウェアモジュールは、いずれかのあるいはすべての記述したステップ、動作もしくは処理を実行するためのコンピュータプロセッサにより実行可能なコンピュータプログラムコードを含むコンピュータに読み取り可能な媒体を備えるコンピュータプログラムで実行される。

【００４０】

また、本発明の実施形態は、ここで開示の動作を実行するための装置に関するものであってもよい。この装置は、要求される目的のために特別に構成されてもよく、あるいは、コンピュータに格納されたコンピュータプログラムによって選択的に活性化し、または再構成した汎用の計算装置を備えていてもよい。そのようなコンピュータプログラムは、コンピュータに読み取り可能な有形の記憶媒体もしくは電子的指令を格納するのに適したあらゆるタイプの媒体に格納されてもよく、コンピュータシステムバスに接続されてもよい。また、本明細書において言及されるいずれかのコンピュータシステムは、シングルプロセッサ（１つのプロセッサ）を含んでいてもよく、増加された計算能力のために複数のプロセッサデザインを用いるアーキテクチャであってもよい。

【００４１】

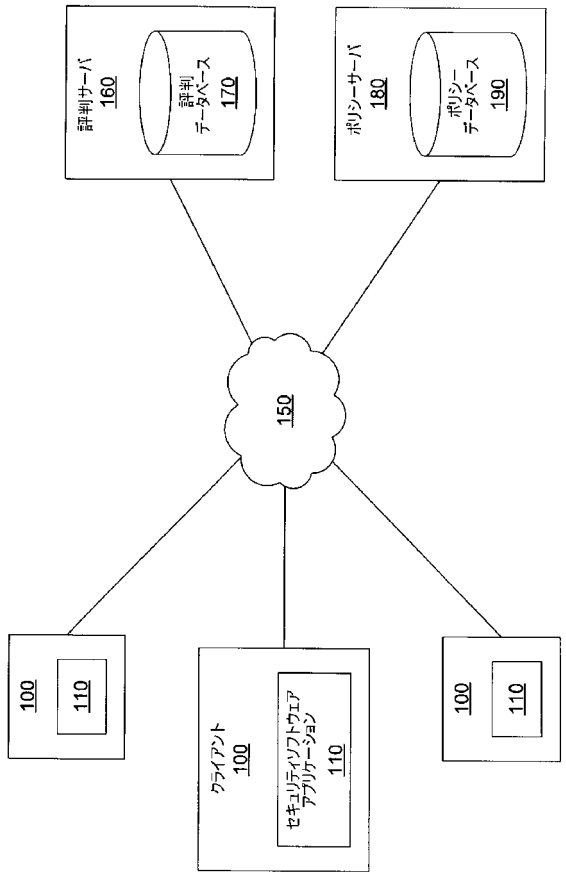
最後に、明細書中で用いられる用語は、主として、読みやすさおよび教育的目的のために選択されたものであり、本発明の主題の範囲を定めたり、限定したりするために選択されたものではない。そのため、本発明の範囲はこの詳細な記述により限定されるものではなく、この記述に基づいて本明細書に由来する特許請求の範囲のいずれかの請求項によって限定されるように意図する。したがって、本発明の実施形態の開示は、限定するものではないが、添付の特許請求の範囲に記載された本発明の範囲の例証となるように意図したものである。

【符号の説明】

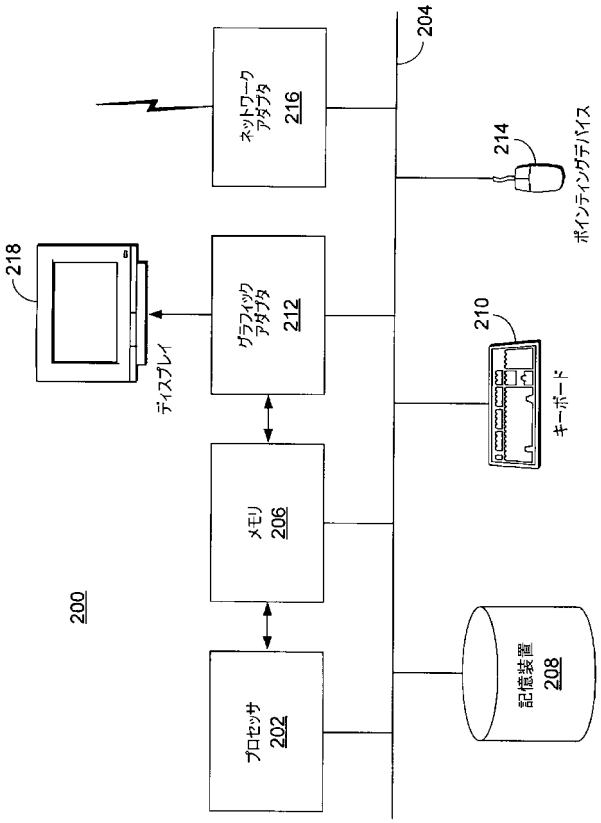
【００４２】

１００　クライアント
１１０　セキュリティソフトウェアアプリケーション
１５０　ネットワーク
１６０　評判サーバ
１７０　評判データベース
１８０　ポリシーサーバ
１９０　ポリシーデータベース
２００　コンピュータ（コンピュータシステム）
２０２　プロセッサ
２０４　バス
２０６　メモリ
２０８　記憶装置
２１０　キーボード
２１２　グラフィックアダプタ
２１４　ポインティングデバイス
２１６　ネットワークアダプタ
２１８　ディスプレイ
３１０　評判モジュール
３２０　ポリシーモジュール
３３０　ポリシーデータベース
３４０　セキュリティモジュール

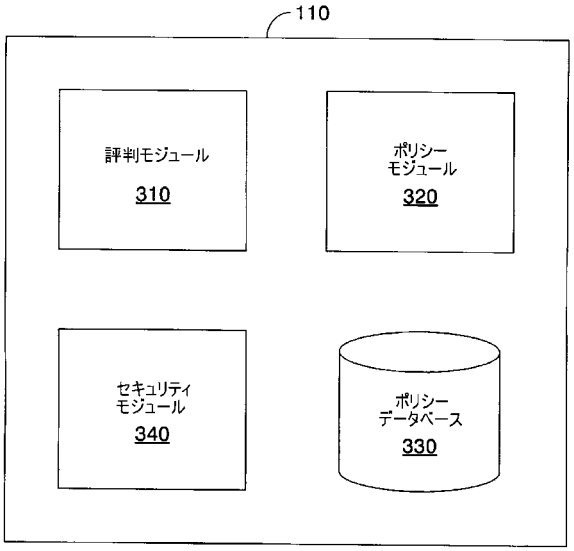
【図１】


評判サーバ
160
評判
データベース
170
ポリシーサーバ
180
ポリシー
データベース
190
150
100
110
クライアント
100
セキュリティソフトウェア
アプリケーション
110
100
110

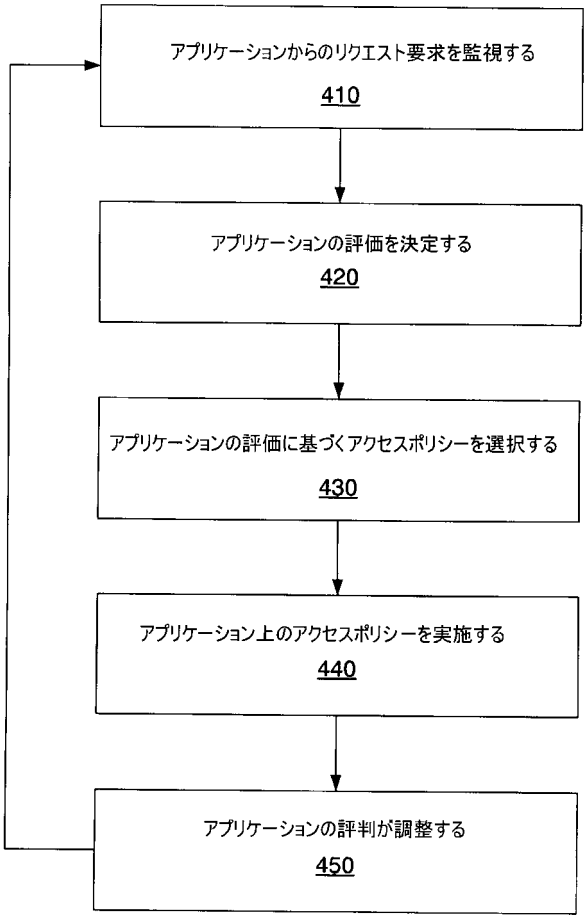
【図２】


204
ネットワーク
アダプタ
216
214
ポインティングデバイス
218
ディスプレイ
グラフィック
アダプタ
212
210
キーボード
メモリ
206
200
プロセッサ
202
記憶装置
208

【図３】


110
評判モジュール
310
ポリシー
モジュール
320
セキュリティ
モジュール
340
ポリシー
データベース
330

【図４】


アプリケーションからのリクエスト要求を監視する
410
アプリケーションの評価を決定する
420
アプリケーションの評価に基づくアクセスポリシーを選択する
430
アプリケーション上のアクセスポリシーを実施する
440
アプリケーションの評判が調整する
450

フロントページの続き

(72)発明者　ケネス　シュナイダー
アメリカ合衆国　カリフォルニア　９５０１４，クパチーノ，スティーブンス　クリーク　ブールバード　２０３３０，　シマンテック　コーポレーション内
(72)発明者　ブルース　マッコーケンデール
アメリカ合衆国　カリフォルニア　９５０１４，クパチーノ，スティーブンス　クリーク　ブールバード　２０３３０，　シマンテック　コーポレーション内

Ｆターム(参考) 5B276 FD08