(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5722337号
(P5722337)
(45)発行日　平成27年5月20日(2015.5.20)　(24)登録日　平成27年4月3日(2015.4.3)

(51)Int.Cl.　F I
G06F 21/62 (2013.01)　G06F 21/62 318

請求項の数 15 (全 15 頁)

(21)出願番号　特願2012-539924(P2012-539924)
(86)(22)出願日　平成22年10月29日(2010.10.29)
(65)公表番号　特表2013-511770(P2013-511770A)
(43)公表日　平成25年4月4日(2013.4.4)
(86)国際出願番号　PCT/US2010/054722
(87)国際公開番号　WO2011/062743
(87)国際公開日　平成23年5月26日(2011.5.26)
審査請求日　平成25年10月8日(2013.10.8)
(31)優先権主張番号　12/622,441
(32)優先日　平成21年11月20日(2009.11.20)
(33)優先権主張国　米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】リソースプロパティに基づくリソースアクセス制御

(57)【特許請求の範囲】
【請求項１】
コンピューティング環境において、
少なくとも一処理ユニットが、リソースから分離されたポリシーに基づいて前記リソースへのアクセスを決定するステップであって、アクセス要求に関連するユーザ要求に対して、前記リソースに関連するリソースラベルを評価することによるものを含み、前記リソースラベルは、前記リソースへのアクセスを決定するのに用いる前記リソースに関連する分類プロパティを含み、前記アクセス要求は前記ユーザ要求により要求されたリソースを特定する、前記リソースへのアクセスを決定するステップと、
前記ポリシーが前記リソースへのアクセスを認めるとの決定に応じて、前記少なくとも一処理ユニットが、前記リソースへのアクセスを許可するステップと、
前記ポリシーが前記リソースへのアクセスを認めないとの決定に応じて、前記少なくとも一処理ユニットが、前記リソースへのアクセスを拒絶するステップと
を備え、
前記ポリシーに基づいて前記リソースへのアクセスを決定するステップは、さらに、ユーザ要求に対して、前記リソースに関連するリソースラベルを評価した結果と、少なくとも一つの他のポリシー評価の結果とを論理的に組み合わせるステップをさらに含む
ことを特徴とする方法。
【請求項２】
一つまたは複数の分類ルールによって得られるリソース分類から前記リソースラベルを

得るステップをさらに備えること特徴とする請求項１に記載の方法。
【請求項３】
前記分類ルールは、あるリソースラベルをあるファイルへ割り当てる宣言型命令を備え、前記リソースは、ファイルであり、前記リソースラベルの各々を得ることは、
前記ファイルのコンテンツに対する変更、前記ファイルの一つまたは複数のラベルに対する変更、前記ファイルの他の属性に対する変更、前記ファイルの場所に対する変更、分類ルールに対する変更、もしくは一つまたは複数の分類ルールへの状態の変化、あるいは、
前記ファイルのコンテンツに対する変更、前記ファイルの一つまたは複数のラベルに対する変更、前記ファイルの他の属性に対する変更、前記ファイルの場所に対する変更、分類ルールに対する変更、もしくは一つまたは複数の分類ルールに対する状態の変化、の任意の組み合わせに基づいて、前記リソース分類を実行することを特徴とする請求項２に記載の方法。
【請求項４】
前記リソースに結合されたアクセス制御リストに基づいて、前記アクセスを決定するステップをさらに備えることを特徴とする請求項１に記載の方法。
【請求項５】
前記アクセス要求に関連する前記ユーザ要求に対して、前記リソースに関連する前記リソースラベルを評価することは、複合した条件を評価すること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】
前記ファイルに関連する前記リソースラベルをキャッシュするステップをさらに備えることを特徴とする請求項３に記載の方法。
【請求項７】
前記アクセス要求に関連する前記ユーザ要求に対して、前記リソースラベルを評価することは、前記ユーザ要求中のデータに対応するユーザのクリアランスレベル値が、前記リソースラベル中のデータに対応するリソースの機密性レベル値を満たすかどうかを評価することを含むことを特徴とする請求項１に記載の方法。
【請求項８】
コンピューティング環境における、
ポリシーに基づいてリソースへのアクセスの決定をする、前記ポリシー内の情報を使用して、アクセス要求に関連するユーザ要求に対して、前記リソースに関連するリソースラベルを評価する、前記リソースラベルは、前記リソースへのアクセスを決定するのに用いる前記リソースに関連する分類プロパティを含み、前記アクセス要求は、前記ユーザ要求により要求されたリソースを特定する、認証エンジン
を備え、
前記認証エンジンは、ユーザ要求に対して、前記リソースに関連するリソースラベルを評価した結果と、少なくとも一つの他のポリシー評価の結果とを論理的に組み合わせることにより、前記ポリシーに基づいて前記リソースへのアクセスの決定をする
システム。
【請求項９】
前記ポリシーはポリシーコンポーネントの組み合わせに基づく、または
前記ポリシーは前記リソースと独立して保持されて複数のリソースへ適用される、または
前記ポリシーはポリシーコンポーネントの組み合わせに基づくとともに前記ポリシーは前記リソースと独立して保持されて複数のリソースへ適用されることの両方である
ことを特徴とする請求項８に記載のシステム。
【請求項１０】
前記リソースはファイルを含み、
前記ファイルを分類することによって前記リソースラベルを提供する分類器をさらに備

えることを特徴とする請求項８に記載のシステム。
【請求項１１】
前記リソースはファイルを含み、前記リソースラベルは、前記ファイルの代替データストリームにキャッシュされることを特徴とする請求項８に記載のシステム。
【請求項１２】
コンピュータにより実行されると、前記コンピュータに、
アクセス要求を処理して、リソースへのアクセス関連の動作を承諾するか拒否するステップであって、前記リソースから分離されたポリシーを得ることを含む、ステップと、
前記ポリシーを使用して、前記アクセス関連の動作を承諾するか拒否するか決定するステップであって、前記アクセス要求に関連するユーザ要求に対して、前記リソースに関連するリソースラベルを評価することを含む、ステップと、
を実行させ、
前記リソースラベルは、前記リソースへのアクセスを決定するのに用いる前記リソースに関連する分類プロパティを含み、前記アクセス要求は、前記ユーザ要求により要求されたリソースを特定し、
前記ポリシーを使用して前記アクセス関連の動作を承諾するか拒否するかを決定するステップは、さらに、ユーザ要求に対して、前記リソースに関連するリソースラベルを評価した結果と、少なくとも一つの他のポリシー評価の結果とを論理的に組み合わせるステップをさらに含む
ことを特徴とするコンピュータプログラム。
【請求項１３】
前記リソースはファイルであり、
前記リソースラベルは前記ファイルに関連してキャッシュされ、
前記コンピュータに、さらに、
前記リソースラベルが有効かつ最新であるか決定するステップと、
前記リソースラベルが有効かつ最新でなければ、有効かつ最新のリソースラベルを得るステップと、
前記有効かつ最新のソースラベルを、前記ファイルと関連付けてキャッシュするステップと、
を実行させることを特徴とする請求項１２に記載のコンピュータプログラム。
【請求項１４】
複数のポリシーが適用可能であることを特徴とする請求項１２に記載のコンピュータプログラム。
【請求項１５】
少なくとも一つの他のポリシー評価は、アクセス制御リストベースの評価結果を含むことを特徴とする請求項１４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、リソースへのアクセスを制御する技術に関する。
【背景技術】
【０００２】
典型的な企業環境において、保持されて処理されるデータの量は莫大であり、その量は急速に増えている。ＩＴ（Information Technology）部門は、何百万、さらに何十億のファイルを、数十のフォーマットで扱わなくてはならない。さらに、この数は、著しい速度で（例えば、年間二桁で）増える傾向にある。
【０００３】
そのようなデータサイズと増加により、ＩＴ部門は、コンプライアンス、セキュリティ、および保管についても含めて、いくつかの複雑なシナリオを考える必要がある。これらのシナリオは、非構造化データ（例えば、ファイル）、半構造化データ（例えば、プロパ

ティレポジトリを有するファイル）、および構造化データ（例えば、データベース）に関連する。しばしば、これらのデータは積極的に管理されず、ファイル共有では構造化されていないフォームで保持される。

【０００４】

ファイルのようなリソース（オブジェクト）へのアクセスを管理するために、現在のセキュリティモデルは、認証されていないユーザのアクセスを制限しながら、正当なユーザがアクセスすることを許可する、オブジェクトについてのアクセス制御ポリシーを持つことに基づいている。しかしながら、データを含むリソースについてのＡＣＬ（access control list：アクセス制御リスト）によるビジネスポリシーに基づいてアクセスを守ることに加えて、企業は、コンテンツの機密性に基づいてデータを守ることに注意もしている。

【０００５】

例として、セキュリティグループ中の数百のユーザに読み出しアクセスを承諾するセキュリティポリシーを有するファイルについて考えてみる。ある時、ファイルのコンテンツが不注意で更新されて、そのファイルが顧客のレコードデータを晒したとすると、企業は、もはや、そのセキュリティグループ全体にそのようなアクセスを与えたがらないであろう。しかしながら、そのコンテンツの変更を検出し、そして、そのセキュリティポリシーを修正する自動的な仕組みは存在しない。

【０００６】

ファイル中で変更されるコンテンツは、企業がどのようにデータが扱われるのを望むかという別のことに密接に関連する場合がある。例えば、企業は、コンテンツに、機密データを加える変更をして、そのデータを含むファイルをＥメールに添付されないように、または携行可能な記憶デバイス（例えば、ＵＳＢデバイス）に平文でコピーされないようにするなど、どのようにデータが配布されるかを変えたい場合がある。

【０００７】

変更されたコンテンツの結果として、アクセスおよび／または配布を防止することは、既存のセキュリティモデルでは可能ではない。これは、意図しない情報の漏洩、およびデータの内部違反という結果となり、いくつかの企業などが直面する重大な問題であり、規制産業および公共部門においても同様である。

【発明の概要】

【０００８】

この概要は、さらに以下の詳細な説明に記載される、簡略化された形での代表的な概念の選択を導入するために提供される。この概要は、特許請求の主題の主要な特徴または本質的な特徴を識別することを意図されるものではなく、また、特許請求の主題の範囲を制限するいずれの方法によっても使用されることを意図されるものではない。

【０００９】

簡単に言えば、本明細書に記載される主題の様々な態様は、リソースへのアクセス要求に関連するユーザ要求（claim）に対して、そのリソースに関連するリソースラベルを評価するためのポリシーに基づいて、リソースへのアクセスを決定するための技術に向けられたものである。ある実装においては、そのポリシーはリソースから分離され、リソースから別々に／独立して保持されることで、同じポリシーを複数のリソースに適用する方法を提供する。

【００１０】

リソースは、ファイルであってもよく、リソースラベルは、そのファイルを分類プロパティに分類することで得られてもよい。このように、例えば、ファイルのコンテンツ変更は、そのリソースラベルを変更しうる再分類につながり、それにより、それらのそれぞれのユーザ要求に応じて、いずれのユーザがそのファイルへアクセスするかを変更する。

【００１１】

アクセスはポリシーから決定されてもよく、ポリシーは、ユーザ要求の評価に対するリソースラベルに単独で基づいて、または、１つまたは複数の評価結果と組み合わせて、ア

クセスを指定してもよい。例えば、ユーザトークンに対するアクセス制御リストの評価は、さらに、アクセスを承諾するか拒否するかを決定することに使用されうる。このように、例えば、ポリシーは、ユーザグループのメンバであり（ＡＣＬベースの評価)、リソースの秘密性レベルに対して十分なクリアランスレベルを有している（リソースラベルベースの評価）ユーザが、アクセスを得ることを指定しうる。他の例においては、ポリシーは、ユーザが、アクセスを得るために、ユーザグループのメンバであるか（ＡＣＬベースの評価）、あるプロジェクトのメンバとして識別されるか（リソースラベルベースの評価）、のいずれかを指定するようになっていてもよい。

【００１２】

他の利点は、以下の詳細な説明が図面とともに扱われることで、明白となるであろう。

【図面の簡単な説明】

【００１３】

【図１】ユーザ要求に対し、リソースラベルに基づいて、リソースアクセスを制御するためのコンピューティング環境におけるコンポーネントの例を示すブロック図である。

【図２】リソースへのアクセスの承諾において、セキュリティ認証によって実行されるステップを示すフロー図である。

【図３】本発明が組み込まれたコンピューティング環境の説明の例を表す。

【発明を実施するための形態】

【００１４】

本発明は、例として説明され、同様の参照符号が類似のエレメントを示す添付図面に限定されない。

【００１５】

本明細書に記載される技術の様々な態様は、概して、リソースを分類することで得られる分類プロパティセット（一つまたは複数の分類プロパティ）に基づいて、アクセスポリシーをリソースへ適用することに向けたものである。これは、リソースの現在のコンテンツを処理することで、分類プロパティセットの少なくとも一部を得ることに基づく。

【００１６】

リソースへのアクセスを決定するために使用される、リソースに関連する分類プロパティは、リソースラベルと呼ばれる。以下に説明されるように、リソースへのアクセスを要求するエンティティは、アクセス関連の動作を承諾するか拒否するかを決定する一つまたは複数のリソースラベルに対して評価される、一つまたは複数のユーザ要求を提供する。このように、例えば、ファイルのコンテンツが変化すると、そのファイルは再分類され、それによってリソースラベルが変化しうる。それにより、ファイルは、変化したリソースラベルに対して適切な一つまたは複数のユーザ要求を持たないユーザのアクセスを防止する。さらに詳細な例として、ファイルが変更されて、機密データを含むようになった場合、そのファイルは再分類され、ユーザにこのような機密データへアクセスすることを許可するユーザ要求を持たないこれらのユーザのアクセスを防止する、修正されたリソースラベルを作成する。

【００１７】

本明細書における例のいずれも非限定的なものであることを理解されたい。実際、説明の目的のため、本明細書においては、概して、ファイル形式のリソースへのアクセスが説明される。しかしながら、ファイルはリソースの一種にすぎない。つまり、他のリソースは、複数のファイルの一部分のような任意のデータの組、データベースの行および／または列、などを含んでいてもよく、さらに、コンピュータおよび周辺装置のような物理的エンティティ、および／またはアプリケーションロールのような仮想エンティティを含んでいてもよい。よって、本発明は、本明細書に記載されるいずれの特定の実施形態、態様、概念、構造、機能、および例にも限定されない。むしろ、本明細書に記載されるいずれの特定の実施形態、態様、概念、構造、機能、および例は、非限定的なものであり、本発明は、概して、コンピューティングおよびリソースアクセスにおいて、利益および利点をもたらす様々な方法によって使用されうる。

【００１８】
図１は、アクセス制御リスト（ＡＣＬ）１０４に関連するリソース１０２が分類器１０６により分類されて、少なくとも一つのリソースラベル１０８を含む分類プロパティセットを得るコンピューティング環境例を示す。分類によって、リソースに関連する多くの分類プロパティを含むプロパティセットを得ることになり、そのプロパティセットは複数のリソースラベルを含みうるが、図１では、簡潔化／説明のために、一つのリソースラベルのみ示されていることに留意されたい。ファイルリソースのため、そのリソースおよびＡＣＬは、リソースラベル１０８を含む分類プロパティをキャッシュするためにも使用可能な記憶装置１１０に保持される。
【００１９】
データ項目のコンテンツを処理することを含みうる分類（Classification）については、米国特許出願第１２／４２７，７５５号にさらに記載されており、参照により本明細書に組み込まれる。この技術は、分類プロパティを定義してファイルへ割り当てるとともに、これらのプロパティに基づいてファイルサーバ上のファイルに適用するアクションを指定するためのＦＣＩ（File Classification Infrastructure）として、マイクロソフトコーポレーションのＷｉｎｄｏｗｓ（登録商標）Ｓｅｒｖｅｒ２００８Ｒ２に実装されている。また、この技術は、ファイルサーバリソースマネージャ（ＦＳＲＭ）サーバロールの一部として利用可能である。
【００２０】
何らかの方法により、リソースラベル１０８は、リソースに関連付けられる。参照によりここに組み込まれる、“Alternate Data Stream Cache for File Classification”という題名の米国特許出願第１２／６０５，４５１号（米国特許出願公開第２０１１／００９９１５２号）に記載されるように、何らかの方法とは、自動的にあるルールによってリソースラベルをドキュメントに割り当てる宣言型（declarative）の分類ルールによって、分類プロパティのキャッシュへの参照ポインタによって、および／またはファイルリソースの代替データストリーム中のリソースラベルを格納することによって、などの方法である。リソースラベルは、分類ルールから推測されてもよく、必ずしも格納されないことに留意されたい。
【００２１】
概して、リソースラベル１０８は、ポリシーを適用するために、ユーザ要求とともに使用することが可能な情報を含む。しかしながら、キャッシュされているリソースラベルは、期限切れか、さもなければ無効である可能性がある。例えば、ファイルが修正される、または移動される場合（これにより、プロパティは期限切れとなる）、つまり、これはコンテンツ変更を含むが、および／またはファイルがリネームされる、またはファイルシステム内の別の場所に移動される場合（これらは、新しい場所に基づく分類の変更となりうる）を含み、キャッシュされるリソースラベルが期限切れになりうるいくつかの場合がある。キャッシュされるリソースラベルが無効となる他の場合は、以前の分類（classification）に使用される（米国特許出願第１２／４２７，７５５号に記載されている）分類ルールが修正されており、および／または、分類を決定する内部状態またはモジュールの構成が修正される場合である。例えば、分類ルールが変更されない場合でも、順番および／または２つ以上の分類ルールを組み合わせる方法は変化しうる。そして、このようないずれかの状態の変化は、異なるファイルプロパティ分類結果、および、それによって、無効なキャッシュされたリソースラベルという結果となる。
【００２２】
従って、ユーザ要求に対するリソースラベルを評価する前に、再分類が必要かどうかを決定するために、そのキャッシュされたリソースラベルの有効性および最新状態がチェックされる。もしそうであれば、前述した米国特許出願に記載されているように、再分類が実行される。キャッシュされるプロパティセットを更新するために、キャッシュされるプロパティセットの一部またはすべては有効性がチェックされ、および／または、リソースの一部またはすべては再分類されることに留意されたい。

【００２３】
リソースラベル対応セキュリティモデルによるポリシーの適用に向けると、リソース１０２へのアクセス要求１１２が（例えば、オペレーティングシステムに構築された）認証エンジン１１４によって受信されると、認証エンジン１１４は、その要求を処理して、アクセス要求１１２中で識別されるそのアクセス関連の動作が許可されるかどうかを確認する。ある実装においては、アクセス要求１１２は、一つまたは複数のポリシー１１８に依存してリソースのＡＣＬ１０４に対して評価されうる従来のアクセストークン１１６に関連付けられている。
【００２４】
知られているように、従来のＡＣＬベースのセキュリティは、トークン１１６に対して、リソースのＡＣＬを比較する。しかしながら、ＡＣＬベースのセキュリティは、基本的に静的であり、ドキュメント中のコンテンツ（例えば、データの機密性）に応じて変化しない。外部のエージェントにコンテンツの変化を監視させて、適切にＡＣＬを変更させることは可能である。しかしながら、それは重大な管理の複雑さを伴うため、実用的ではない。例えば、そのようなエージェントは、あらゆるポリシーの変更について、何百／何千のファイルのためにポリシーを監視しておそらくは変更しなければならない。
【００２５】
対照的に、本明細書に記載されるように、ユーザ要求１２０に対するリソースラベル１０８の評価は、ドキュメントの状態（例えば、その機密性、そのファイルが属するプロジェクト、など）と、これらのラベルを扱うポリシー１１８との間を分離する。ファイルの複数のラベルを保持する間、ポリシー変更は一元的に行うことができる。
【００２６】
従って、本明細書に記載されるように、一つのポリシー（または複数のポリシー）１１８に依存して、リソースの現在の状態に基づいて、リソースラベル１０８に対してユーザ要求１２０が評価され、アクセス関連の動作が許可されるかどうかを決定することができる。図１に表されるように、認証エンジン１１４のポリシー評価機構１２２（図２を参照して以下に例示される）は、セキュリティチェックを実行し、このセキュリティチェックは、ＡＣＬ１０４、および／または、ユーザ要求１２０を含むアクセストークン１１６に対してリソースラベル１０８を評価することを含む。ポリシー評価機構１２２は、この例において、アクセスを承諾または拒否する。
【００２７】
完全を期すために、ポリシー結合器１２４が図１に示される。概して、リソースアクセスのために、組織に渡って、および／またはビジネスオーナーによって定義される複数のグローバルポリシー、ドメイン固有のポリシー、ローカルポリシー、ディレクトリポリシー、などの複数のポリシーコンポーネントが存在してもよい。ポリシーの適用において一般的に知られているように、承継、オーバーライド、ブロッキング、などのような概念は、リソースに対して、結合されたポリシーを確立するために使用されうる。それにもかかわらず、複数のポリシーが、必要に応じて、このように複雑な場合があるため、ただ一つほどの簡単なポリシーは、本明細書に記載されている技術、例えば、リソースラベルおよびＡＣＬがアクセストークン／ユーザ要求によって合致する場合にアクセスを承諾する技術とともに使用されうる。同時に、このようなポリシーは、ポリシーが個々のリソースから分離しているため、変更することが容易である。
【００２８】
ある実装においては、認証エンジン１１４は、認証ランタイムが強化されたマイクロソフトコーポレーションのＷｉｎｄｏｗｓ（登録商標）７に基づく。Ｗｉｎｄｏｗｓ（登録商標）７のランタイムは、条件式言語（conditional expressions language）をサポートし、クレームベース（名前と値の組（name-value pairs）ベース）の同一性（identities）を用いて複雑なポリシーを指定する。
【００２９】
例として、以下のポリシー（セキュリティ記述子定義言語、またはＳＤＤＬ（security

descriptor definition language）に書き換えることが可能）は、ＸＹＺカンパニーのフルタイムの従業員は、承認額が１００００（ドル）未満であるため、承認することができる、ということを表している。

(XA;;APPROVE;;;WD;(member of {SG_ XYZ,SG_FTE} AND
ApprovalAmount < 10000)) .

【００３０】

本明細書に記載される、どのようにポリシーがラベルおよびユーザ要求を通じて適用されるかの例として、ファイルを提供する事業部などのような特定の環境において顧客機密データへアクセスすることが許可されている（セキュリティグループ中のメンバシップに表される）社員による、顧客機密データを有するドキュメントへのアクセスを許可したい企業を考えてみる。このポリシーのタイプは、「充足性」ではなく「必要性」を評価する。なぜならば、その目的は、その環境において、許可されている社員に、すべての顧客機密データへアクセスすることを許可することではないからである。すなわち、むしろ、アクセスは、そのように行うビジネス上のニーズがある時にのみ許可されるからである。この充足ポリシーは、そのドキュメントのビジネス上のニーズに応じて設定されるＡＣＬによって指示される。

【００３１】

この種の制限は、金融情報、顧客データ、およびビジネス上の重要データの漏洩を防止するために、金融、ヘルスケア、公共セクタなどの規制産業における政府規制によって要望され、または必要とされる。上記したように、現在のＡＣＬモデルを使用するポリシー強制は、実用的ではない。本明細書に記載の技術は、ポリシーをリソースに物理的に結びつけることなくポリシーを強制し、それにより、ビジネス上の機密データを有する一つまたは複数のコンピュータの集合体に対して、より弾力的で、容易に強制可能であり、分散型である。

【００３２】

リソースラベルに基づいて特定のユーザグループにアクセスを強制したい企業の例について続ける。グループ“SG ClearedPrnl”のメンバのみ、クレーム“customerData”を有するファイルを読み出すことができるが、そうでなければ、誰もが（そのリソースのＡＣＬのための別の適切なトークンとともに）そのようなデータ無しにファイルを読み出すことができることを指定するために、ポリシーとして以下が設定されうる。

(XA;;GR;;;WD;(resource.Exists(customerData) AND
member_of{SG_ClearedPrnl} OR NOT(resource.Exists(customerData)))

【００３３】

このように、ファイルが顧客データを含む場合、読み出しアクセスは、“SG ClearedPrnl”グループのメンバであるユーザのみに承諾される。ファイルが以前は顧客データを含まなかったが、その後、顧客データを含むように修正された場合、そのファイルは、（コンテンツの変更によって）再分類され、リソースラベルは、顧客データがそのファイルに存在することを示すファイルと関連付けられるであろう。従って、アクセスは、ファイルに顧客データが存在するかどうかに基づいて変化する。

【００３４】

他の例として、リソースラベルおよびユーザ要求は、その分類レベルに基づいてリソースへのアクセスを許可する、または許可しないことを比較する方法として使用されうる複数のレベルが、割り当てられうる。すなわち、以下の通りである。

(XA;;GR;;;WD;(user.clearanceLevel >= resource.sensitivityLevel)

【００３５】

リソースが最初に分類される時、その分類によってリソースラベルにおける機密性レベルが設定される。リソースの機密性レベル（リソースラベル中のデータに対応する値またはその他）は、ユーザのクリアランスレベル（ユーザ要求中のデータに対応する値またはその他）に対して比較されて、機密性レベルが満たされるかが決定される（それによって、アクセスが許可される）。もし、リソースが何らかの方法により変更され、その後、再

分類された場合、そのリソースラベルにおける機密性レベルは変更されうる。それにより、そのファイルへアクセスために必要とされるクリアランスレベルは上昇するか下降する。

【００３６】

他の例は、ユーザがファイルへアクセス可能なセキュリティグループの一員でない場合でも、ユーザのプロジェクトのため、ファイルへのアクセスを許容する例である。例えば、コンサルタントのような従業員でない者は、以下のポリシーによって、さもなければ従業員にのみアクセス可能であるファイルへのアクセスを許されうる。

(XA;;GR;;;WD;(user.projects OVERLAP resource.projects))

【００３７】

上記は、ユーザ要求、および遅延バインド解決（late binding resolution）を可能にするリソースラベルを含む複合した条件を評価するためのものであることに留意されたい。

【００３８】

図２は、どのようにユーザ要求に対してＡＣＬおよび／またはリソースラベルに基づいてリソースへのアクセスを決定するために、ポリシーが使用されうるかの簡潔な例を示す。図２では、ＡＣＬおよびリソースラベルを使用する、可能な２つのポリシーが例示されている。すなわち、ＡＣＬおよびリソースラベルの双方がアクセスのために必要とされるか（つまり、“ユーザグループのメンバであるか”ＡＮＤ“十分なクリアランスを有しているか”というようなＡＮＤ論理結合）、または、いずれかがアクセスを承諾するか（つまり、“ユーザグループのメンバであるか”ＯＲ“プロジェクトに関係すると確認されるか”というようなＯＲ論理結合）の場合である。ポリシーは、どのようにロジックが所与のリソースに適用されるかを設定し、容易に理解できるであろうが、より複雑な論理結合（ＮＯＴ、ＸＯＲ、など）が可能である。例えば、リソースラベルは、アクセスできるようになるために、複数グループ（複合したプリンシパル）中のユーザメンバシップを要求することが可能である。他の例では、リソースラベルは、一日のうちのある時間に、（どこかに記録される）一定量で、など、適切なユーザのみがリソースにアクセスできるような条件を含む。

【００３９】

ステップ２０２は、所与のリソースのために、リソースラベルがキャッシュされるかどうか、すなわち、以前、分類が実行されたかどうかを決定するステップを表す。もし、そうであれば、ステップ２０４は、概して、前述した“Alternate Data Stream Cache for File Classification”特許出願に記載されているように、リソースラベルが有効かつ最新であるかどうか、または再分類は必要であるかどうかを評価する。最初の分類（ステップ２０２）または再分類（ステップ２０４）が必要である場合には、ステップ２０６はリソースの分類、または再分類が実行される。ステップ２０８は、リソースラベルまたはラベルを含む分類プロパティを、その後の使用のためにキャッシュするステップを表す。

【００４０】

ステップ２１０は、リソースのＡＣＬに対するユーザのアクセストークンを評価するステップ、すなわち、従来のアクセスチェックを実行するステップを表す。アクセスが承諾される場合には、ステップ２１２は、この簡潔化された例において、それ自体で十分（ポリシーが“ＡＣＬアクセスＯＲリソースラベルアクセス”を表している）であるかどうかを評価する。すなわち、そうであれば、ステップ２２０に表されるように、アクセスは承諾される。これは、“プロジェクト”の例に対応し、例えば、ユーザは、（ＡＣＬに対する）ユーザグループクレーム“ＯＲ”（リソースラベルに対する）プロジェクトユーザ要求を有することで、アクセスを得ることができる。

【００４１】

“プロジェクト”の例において、アクセスを得るための他の方法は、ステップ２１０において、ＡＣＬがアクセスを承諾しない場合には、ステップ２１４において、ポリシーは“ＯＲリソースラベル”である。もしそうであれば、ステップ２１６は、ユーザ要求によ

って、リソースラベルに対するユーザアクセスを評価する。リソースラベルがアクセスを許可する場合には、ステップ２１６は、アクセスを許可するステップ２２０に分岐するか、もしくはステップ２１８によってアクセスは拒否される。

【００４２】

上記のように、図２のロジックは、“セキュリティグループに属することが必要ＡＮＤ機密データに対するクリアランスを有する”などのように、“ＡＮＤ”結合をも扱う。容易に理解できるであろうが、ステップ２１２および／またはステップ２１４の“ＡＮＤ”分岐に従って、アクセスは、ＡＣＬチェックが通過されること、およびリソースラベルが通過されることの両方を要求する。ステップ２１６が自動的に通過される（後で異なるように再分類されなければ）、例えば、機密性レベルがゼロであるためにすべての者が、さもなければ再分類されるまで、クリアランスを有するように、分類は、ファイルに対してリソースラベルを設定することができることに留意されたい。

【００４３】

リソースに対して要求されるアクセスに関する動作は、簡単な読み出し、または書き込み（または実行）アクセスよりも簡単なものでありうることに留意されたい。上記の例の一つを使用して、ユーザは、ファイルアクセスを要求して、ファイルを平文で携行可能な記憶デバイスに（例えば、直接、またはクリップボードを介して）コピーすることができる。アクセスポリシーの限界内（例えば、ドメインマシーン上）である時は、読み出しアクセスは許可されうるが、平文でテキストをコピーすることは、要求者のユーザ要求に対するリソースラベルに反映されるように、現在のファイルコンテンツに依存して許可されるか、または許可されないであろう。他の例において、他の要求されるアクセス関連の動作は、電子メールのメッセージにデータの一部を添付することであり、これも要求者のユーザ要求に対するリソースラベルに依存するであろう。そのようなポリシーは指定されて、好適に備えられる認証エンジン／オペレーティングシステムに実装されうる。

【００４４】

さらに、アクセスポリシーは、ファイルの代替データストリームなどにおいて、ファイルとともに移動しうる。例えば、ファイルのコンテンツの性質に基づいて、アクセスポリシーを尊守するデバイスに再びコピーし直される場合にポリシーが適用されるように、アクセスポリシーの限界外に移動する時には、アクセスポリシーをファイルとともにパッケージすることが望ましいであろう。この動作を強制するために、アクセスポリシーの境界を越える時は、ファイルは保護される（例えば、暗号化される）。

【００４５】

リソースプロパティに基づいたアクセスについての他のシナリオは、リポジトリにまたがってアクセスポリシーを保持することを含む。異なるマシンおよびリポジトリの間でファイルが移動する時（例えば、ファイルサーバからＳｈａｒｅＰｏｉｎｔ（登録商標）への移動）、ファイルがそのラベルを保持し、そのファイルが、分類ラベルが同じアクセスポリシーに参照される同じポリシードメインに留まる限り、そのアクセスポリシーは保持される。

【００４６】

このように、ファイルの分類プロパティに基づいて、アクセスポリシーをファイルへ適用することを含む、リソースラベルに対してユーザ要求に基づくアクセスポリシーを強制する機能が提供される。ユーザ要求およびリソースラベルは、クリアランス／機密性レベル、および／または他の論理結合のような複雑な条件セットで使用されうる。これは、現在、既知のシステムでは使用可能ではない、複合したプリンシパルおよび他の条件を含む、柔軟で複雑なポリシーを容易に可能とする。

【００４７】

（動作環境例）

図３は、図１および図２の例が実施されうる好適なコンピューティングおよびネットワーキング環境３００の例を示す。コンピューティングシステム環境３００は、好適なコンピューティング環境の一例にすぎず、本発明の使用または機能の範囲について、いかなる

限定をも示唆することは意図されていない。コンピューティング環境３００は、例示的なオペレーティング環境３００に示されるコンポーネントのいずれか、または組み合わせについて、あらゆる依存性または要求を持つものと解釈されるべきではない。

【００４８】

本発明は、他の多数の一般的な目的または特別な目的のコンピューティングシステム環境または構成によって動作可能である。本発明との使用に好適な、よく知られたコンピューティングシステム、環境、および／または構成の例は、上記のシステムまたはデバイスなどのいずれかを含むパーソナルコンピュータ、サーバコンピュータ、ハンドヘルドまたはラップトップデバイス、タブレットデバイス、マルチプロセッサシステム、マイクロプロセッサベースのシステム、セットトップボックス、プログラム可能な民生用電子機器、電子ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータ、分散型コンピューティング環境を含むが、これに限定されない。

【００４９】

本発明は、コンピュータによって実行されるプログラムモジュールのような、コンピュータが実行可能な命令の一般的なコンテキストによって記載されうる。概して、プログラムモジュールは、特定のタスクまたは実行する、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。 本発明は、通信ネットワークを通してリンクされるリモート処理デバイスによってタスクが実行される分散型コンピューティング環境において実行されうる。分散型コンピューティング環境において、プログラムモジュールは、メモリ記憶デバイスを含むローカルおよび／またはリモートコンピュータ記憶媒体に配置されうる。

【００５０】

図３を参照し、本発明の様々な態様を実装するための例示的なシステムは、コンピュータ３１０の形式の汎用コンピューティングデバイスを含んでいてもよい。コンピュータ３１０のコンポーネントは、処理ユニット３２０、システムメモリ３３０、および、システムメモリを含む様々なシステムコンポーネントを処理ユニット３２０へ結合するシステムバス３２１を含んでいてもよいが、これに限定されない。システムバス３２１は、メモリバスまたはメモリコントローラ、周辺バス、および様々なバスアーキテクチャのいずれかを使用するローカルバスを含むいくつかのタイプのバス構造のいずれかであってよい。例として、そのようなアーキテクチャは、ＩＳＡ（Industry Standard Architecture）バス、ＭＣＡ（Micro Channel Architecture）バス、ＥＩＳＡ（Enhanced ISA）バス、ＶＥＳＡ（Video Electronics Standards Association）ローカルバス、Ｍｅｚｚａｎｉｎｅバスとしても知られるＰＣＩ（Peripheral Component Interconnect）バスを含むが、これらに限定されない。

【００５１】

コンピュータ３１０は、典型的には、様々なコンピュータ可読媒体を含む。コンピュータ可読媒体は、コンピュータ３１０がアクセス可能な、あらゆる利用可能な媒体であってよく、揮発性媒体および不揮発性媒体の両方、並びに、着脱可能な媒体および着脱不可能な媒体を含む。例として、コンピュータ可読媒体は、コンピュータ記憶媒体および通信媒体を含んでいてもよいが、これに限定されない。コンピュータ記憶媒体は、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータなどの情報の格納のために、あらゆる方法または技術で実装される揮発性媒体および不揮発性媒体、着脱可能な媒体および着脱不可能な媒体を含む。コンピュータ記憶媒体は、所望の情報を格納するために使用可能であり、コンピュータ３１０がアクセス可能な、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ、もしくは他のメモリ技術、ＣＤ－ＲＯＭ、ＤＶＤ（digital versatile disks）、もしくは他の光学式ディスク記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置、もしくは他の磁気記憶装置、または他の媒体を含むが、これに限定されない。通信媒体は、典型的には、搬送波または他の伝送機構のような変調されたデータ信号中のコンピュータ可読命令、データ構造、プログラムモジュール、または他のデータを具現化し、あらゆる情報配信媒体を含む。「変調されたデータ信号」という用語は

、一つまたは複数の文字セットを有し、または、その信号中の情報をエンコードするような方法で変更された信号を意味する。例として、通信媒体は、有線ネットワークまたは直接配線接続などの有線媒体、並びに、音響式、ＲＦ、赤外線、および他の無線媒体を含むが、これに限定されない。上記のいずれかの組み合わせも、コンピュータ可読媒体の範囲内に含まれうる。

【００５２】

システムメモリ３３０は、ＲＯＭ（read only memory）３３１、ＲＡＭ（random access memory）３３２のような揮発性メモリおよび／または不揮発性メモリの形のコンピュータ記憶媒体を含む。ＢＩＯＳ（basic input／output system）３３３は、スタートアップ中などに、コンピュータ３１０内のエレメント間で情報を伝送することを手助けする基本ルーチンを含み、典型的には、ＲＯＭ３３１に格納される。ＲＡＭ３３２は、典型的には、すぐにアクセス可能であり、および／または処理ユニット３２０によって実行されるデータおよび／またはプログラムモジュールを含む。例として、図３は、オペレーティングシステム３３４、アプリケーションプログラム３３５、他のプログラムモジュール３３６、およびプログラムデータ３３７が示されているが、これに限定されない。

【００５３】

コンピュータ３１０は、他のリムーバブル／非リムーバブルな揮発性／不揮発性コンピュータ記憶媒体をも含んでいてもよい。単なる例として、図３は、非リムーバブルから読み出す、並びにこれに書き込むハードディスクドライブ３４１、不揮発性磁気媒体、リムーバブルから読み出す、並びにこれに書き込む磁気ディスクドライブ３５１、不揮発性磁気ディスク３５２、およびリムーバブルから読み出す、並びにこれに書き込む光学式ディスクドライブ３５５、ＣＤ－ＲＯＭ、または他の光学式媒体のような不揮発性光学式ディスク３５６を示す。例示的なオペレーティング環境で使用することが可能な他のリムーバブル／非リムーバブルな揮発性／不揮発性コンピュータ記憶媒体は、磁気テープカセット、フラッシュメモリカード、ＤＶＤ（digital versatile disks）、デジタルビデオテープ、ソリッドステートＲＡＭ、ソリッドステートＲＯＭ、などを含むが、これに限定されない。ハードディスクドライブ３４１は、典型的には、インタフェース３４０のような非リムーバブルなメモリインタフェースを通してシステムバス３２１に接続される。そして、磁気ディスクドライブ３５１および光学式ディスクドライブ３５５は、典型的には、インタフェース３５０のようなリムーバブルメモリインタフェースによって、システムバス３２１に接続される。

【００５４】

上記されるとともに図３に示されるドライブおよびそれらの関連するコンピュータ記憶媒体は、コンピュータ可読命令の記憶領域、データ構造、プログラムモジュール、およびコンピュータ３１０のための他のデータを提供する。図３において、例えば、ハードディスクドライブ３４１は、オペレーティングシステム３４４、アプリケーションプログラム３４５、他のプログラムモジュール３４６、およびプログラムデータ３４７を格納するように示されている。これらのコンポーネントは、オペレーティングシステム３３４、アプリケーションプログラム３３５、他のプログラムモジュール３３６、およびプログラムデータ３３７と同じでも、異なっていてもよいことに留意されたい。オペレーティングシステム３４４、アプリケーションプログラム３４５、他のプログラムモジュール３４６、およびプログラムデータ３４７は、それらが、最低限、異なる複製物であることを示すために、本明細書では異なる符号が付されている。ユーザは、タブレットまたは電子デジタイザ（座標入力装置）３６４、マイクロフォン３６３、キーボード３６２、並びに、ポインティングデバイス３６１、俗に言うマウス、トラッキングボール、またはタッチパッドのような入力デバイスを介して、コマンドおよび情報をコンピュータ３１０に入力することができる。図３に示されない他の入力デバイスは、ジョイスティック、ゲームパッド、サテライトディッシュ（衛星テレビ受信用アンテナ）、スキャナ、などを含んでいてもよい。これらの、および他の入力デバイスは、しばしば、システムバスに結合されるユーザ入力インタフェース３６０を通して処理ユニット３２０に接続されるが、パラレルポート、

ゲームポート、またはＵＳＢ(universal serial bus）のような他のインタフェースおよびバス構造によって接続されてもよい。モニタ３９１または他のタイプの表示デバイスも、ビデオインタフェース３９０のようなインタフェースによってシステムバス３２１に接続される。モニタ３９１は、さらにタッチスクリーンパネルなどで統合されてもよい。モニタおよび／またはタッチスクリーンパネルは、タブレット型パーソナルコンピュータのように、コンピューティングデバイス３１０が組み入れられているハウジングに物理的に結合されてもよいことに留意されたい。さらに、コンピューティングデバイス３１０のようなコンピュータは、出力周辺インタフェース３９４などを通して接続されるスピーカ３９５およびプリンタ３９６のような他の周辺出力デバイスさらに含んでいてもよい。

【００５５】

コンピュータ３１０は、ネットワーク環境において、リモートコンピュータ３８０のような一つまたは複数のリモートコンピュータへの論理的接続を使用して動作してもよい。図３では、メモリ記憶デバイス３８１のみ示されているが、リモートコンピュータ３８０は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピアデバイス、または他の共有ネットワークノードであってもよく、典型的には、コンピュータ３１０に関して上記されるエレメントの多数またはすべてを含む。図３に描かれている論理的接続は、一つまたは複数のＬＡＮ（local area networks）３７１、および一つまたは複数のＷＡＮ（wide area networks）３７３を含むが、他のネットワークをも含んでいてもよい。そのようなネットワーキング環境は、オフィス、企業規模のコンピュータネットワーク、イントラネット、およびインターネットではありふれたものである。

【００５６】

ＬＡＮネットワーキング環境にて使用される時は、コンピュータ３１０は、ネットワークインタフェースまたはアダプタ３７０を通して、ＬＡＮ３７１に接続される。ＷＡＮネットワーキング環境にて使用される時は、コンピュータ３１０は、典型的には、インターネットのようなＷＡＮ３７３への接続を確立するために、モデム３７２または他の手段を含む。モデム３７２は、内部または外部に備えられ、ユーザ入力インタフェース３６０または他の適切なメカニズムを介して、システムバス３２１に接続されうる。インタフェースおよびアンテナを備えるような無線ネットワーキングコンポーネントは、アクセスポイントまたはピアコンピュータを通して、ＷＡＮまたはＬＡＮと結合されうる。ネットワーク化された環境において、コンピュータ３１０に関連して描かれるプログラムモジュールまたはその部分（portions）は、リモートメモリ記憶デバイスに格納されてもよい。例として、図３は、メモリデバイス３８１上に存在するリモートアプリケーションプログラム３８５を示しているが、これに限定されない。示されるネットワーク接続は例示であり、コンピュータ間の通信リンクを確立する他の手段が使用されてもよいことを理解されたい。

【００５７】

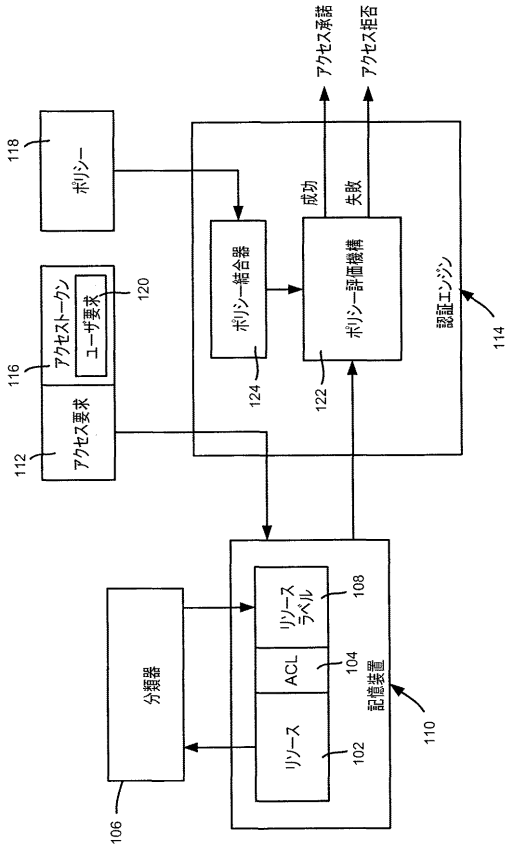
補助サブシステム３９９（例えば、コンテンツの補助ディスプレイ）は、ユーザインタフェース３６０を介して接続され、コンピュータシステムのメイン部分（portions）が低電力状態にある場合でも、プログラムコンテンツ、システム状態、およびイベントのようなデータがユーザへ提供されることを許容する。補助サブシステム３９９は、モデム３７２および／またはネットワークインタフェース３７０に接続され、メイン処理ユニット３２０が低電力状態にある間、これらのシステム間の接続を許容する。

【００５８】

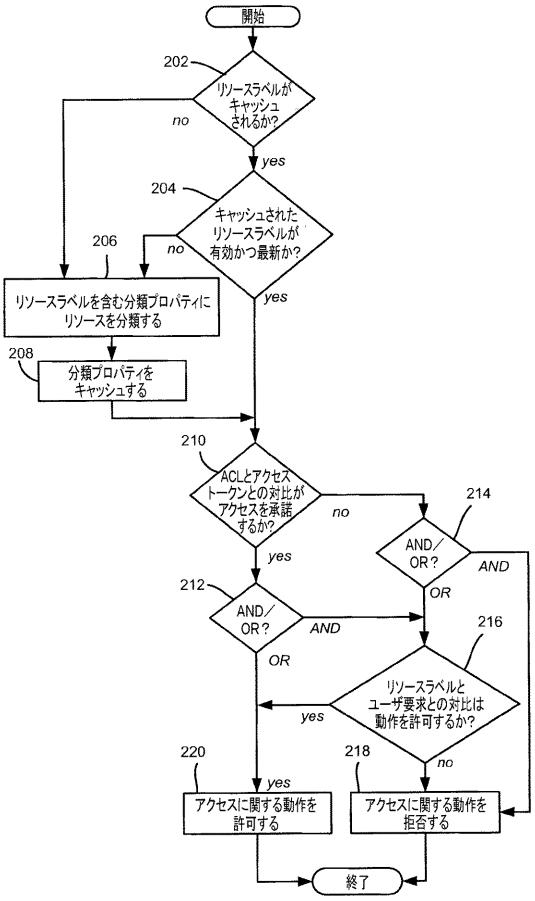
（むすび）

本発明は、様々な変更形態および代替構造を採用しうるが、その、ある例示された実施形態が図面に示され、上記に詳細に記載されている。しかしながら、本発明を、開示される特定の形式に限定する意図はなく、逆に、その意図は、本発明の主旨および範囲内にある、すべての変更形態、代替構造、および均等物をカバーすることである。

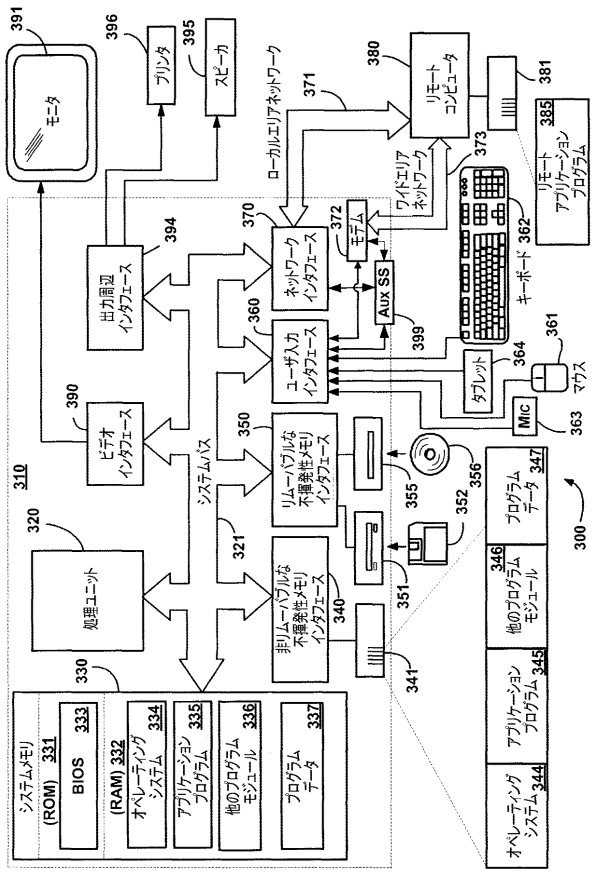
【図１】


ポリシー
アクセストークン
ユーザ要求
アクセス要求
ポリシー結合器
ポリシー評価機構
認証エンジン
成功
失敗
アクセス承諾
アクセス拒否
分類器
リソース
ACL
リソースラベル
記憶装置
118
120
116
112
124
122
114
108
104
102
110
106

【図２】


開始
リソースラベルがキャッシュされるか?
no
yes
キャッシュされたリソースラベルが有効かつ最新か?
no
yes
リソースラベルを含む分類プロパティにリソースを分類する
分類プロパティをキャッシュする
ACLとアクセストークンとの対比がアクセスを承諾するか?
no
yes
AND/OR?
AND
OR
AND/OR?
AND
OR
リソースラベルとユーザ要求との対比は動作を許可するか?
yes
no
アクセスに関する動作を許可する
アクセスに関する動作を拒否する
終了
202
204
206
208
210
212
214
216
218
220

【図３】


モニタ
プリンタ
スピーカ
ローカルエリアネットワーク
リモートコンピュータ
ワイドエリアネットワーク
リモートアプリケーションプログラム
出力周辺インタフェース
ネットワークインタフェース
モデム
AUX
SS
キーボード
ユーザ入力インタフェース
タブレット
マウス
Mic
ビデオインタフェース
システムバス
リムーバブルな不揮発性メモリインタフェース
処理ユニット
プログラムデータ
他のプログラムモジュール
アプリケーションプログラム
オペレーティングシステム
システムメモリ
(ROM)
BIOS
(RAM)
オペレーティングシステム
アプリケーションプログラム
他のプログラムモジュール
プログラムデータ
391
396
395
371
380
381
385
373
370
372
394
362
360
399
361
364
390
350
363
310
320
321
356
355
352
351
340
341
330
346
345
344
347
300
331
332
333
334
335
336
337

フロントページの続き

(72)発明者 ニール ベンーズヴィ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエーーインターナショナル パテンツ内
(72)発明者 ラジャ パザニベル ペルマル
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエーーインターナショナル パテンツ内
(72)発明者 アンダース サミュエルソン
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエーーインターナショナル パテンツ内
(72)発明者 ジェフリー ビー．ハンブリン
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエーーインターナショナル パテンツ内
(72)発明者 ラン カラチ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエーーインターナショナル パテンツ内
(72)発明者 ジークァン リー
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエーーインターナショナル パテンツ内
(72)発明者 マティアス エイチ．ウォルニク
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエーーインターナショナル パテンツ内
(72)発明者 クライド ロウ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエーーインターナショナル パテンツ内
(72)発明者 ポール エイドリアン オルテアン
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエーーインターナショナル パテンツ内

審査官 平井 誠

(56)参考文献 米国特許出願公開第２００７／０１５６６９４（ＵＳ，Ａ１）
米国特許出願公開第２００７／０１５６８９７（ＵＳ，Ａ１）
特開２００７－２９３６３０（ＪＰ，Ａ）
Michael Hart ET AL, More content-Less Control:Access Control in the Web 2.0, IEEE Web 2007, ２００７年 １月 １日, 1-3, （EPのサーチレポートでカテゴリXの文献）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ ２１