(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4833849号
(P4833849)
(45)発行日　平成23年12月7日(2011.12.7)　(24)登録日　平成23年9月30日(2011.9.30)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330B
G09C 1/00 (2006.01)　　G09C 1/00 640E

請求項の数 24　(全 22 頁)

(21)出願番号　特願2006-536584 (P2006-536584)
(86)(22)出願日　平成16年7月29日 (2004.7.29)
(65)公表番号　特表2007-519077 (P2007-519077A)
(43)公表日　平成19年7月12日 (2007.7.12)
(86)国際出願番号　PCT/US2004/024370
(87)国際公開番号　WO2005/045579
(87)国際公開日　平成17年5月19日 (2005.5.19)
審査請求日　平成19年6月29日 (2007.6.29)
(31)優先権主張番号　10/693,172
(32)優先日　平成15年10月23日 (2003.10.23)
(33)優先権主張国　米国(US)

前置審査

(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　110001243
特許業務法人　谷・阿部特許事務所
(74)復代理人　100115624
弁理士　濱中　淳宏
(74)復代理人　100145388
弁理士　藤原　弘和

最終頁に続く

(54)【発明の名称】アイデンティティの認識のための方法およびシステム

(57)【特許請求の範囲】
【請求項１】
開始システムから意図された受信システムにアイデンティティ情報文書を送信するコンピュータ実施方法であって、
前記開始システムは、処理ユニットおよびメモリを含み、
前記アイデンティティ情報文書は、前記開始システムを使用する当事者についてのアイデンティティ情報の一部または全部から成り、該アイデンティティ情報は、該当事者に関する情報の集合および該情報の集合の用途を含み、
前記処理ユニットが実施する前記方法は、
第１のアイデンティティ情報文書および第２のアイデンティティ情報文書に含める情報を選択するために、前記開始システムに含まれている自己アイデンティティ情報ストアから前記開始システムを使用する当事者についてのアイデンティティ情報のリストを示すステップであって、前記第１のアイデンティティ情報文書は、第１の意図された受信システム用に生成され、前記第２のアイデンティティ情報文書は、第２の意図された受信システム用に生成され、前記第１の意図された受信システムは、前記第２の意図された受信システムとは異なり、前記アイデンティティ情報のリストを選択のために示すステップは、前記当事者に前記第１および第２の意図された受信システムへのアイデンティティ情報の開示を制御することを可能にさせる、ステップと、
前記第１のアイデンティティ情報文書に含めるために、前記メモリに格納されている、前記自己アイデンティティ情報ストアからのアイデンティティ情報のリストから前記アイ

デンティティ情報の第１の選択を受信するステップであって、選択された第１のアイデンティティ情報は、前記自己アイデンティティ情報ストアの前記当事者に関連するアイデンティティ情報の第１のサブセットを含み、前記アイデンティティ情報の第１のサブセットは、前記第１の意図された受信システムに固有のものである、ステップと、

前記第２のアイデンティティ情報文書に含めるために、前記メモリに格納されている、前記自己アイデンティティ情報ストアからのアイデンティティ情報のリストから前記アイデンティティ情報の第２の選択を受信するステップであって、選択された第２のアイデンティティ情報は、前記自己アイデンティティ情報ストアの前記当事者に関連するアイデンティティ情報の第２のサブセットを含み、前記アイデンティティ情報の第２のサブセットは、前記第２の意図された受信システムに固有のものであり、かつ前記アイデンティティ情報の第１のサブセットとは異なる、ステップと、

前記開始システムに含まれている自己アイデンティティ情報ストアから前記選択された第１および第２のアイデンティティ情報を読み取るステップと、

前記選択された第１のアイデンティティ情報および少なくとも第１のキーを含めるために、前記第１のアイデンティティ情報文書における前記第１のキーに関連付けられた第２のキーを使用してサインされた前記第１のアイデンティティ情報文書を生成するステップと、

前記第１のアイデンティティ情報文書を前記第１の意図された受信システムに送信するステップと

を含むことを特徴とする方法。

【請求項２】

前記アイデンティティ情報の第１の選択を受信するステップは、グラフィカルユーザインタフェース（ＧＵＩ）からのユーザ入力に基づいて前記自己アイデンティティ情報ストアからアイデンティティ情報の第１のサブセットの選択を受信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】

前記アイデンティティ情報の第１の選択を受信するステップは、前記自己アイデンティティ情報ストアから所定の情報のサブセットの選択を受信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４】

前記第１のアイデンティティ情報文書を生成するステップは、拡張可能マークアップ言語（ＸＭＬ）文書における前記選択された第１のアイデンティティ情報を符号化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５】

前記選択された第１のアイデンティティ情報は、前記第１のアイデンティティ情報文書を発信する当事者のアイデンティティ主張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】

前記選択された第１のアイデンティティ情報は、前記アイデンティティ情報の内容を使用することができる用途を規定するための使用法ポリシーを含むことを特徴とする請求項１に記載の方法。

【請求項７】

開始システムからのアイデンティティ情報文書を受信システムが受信するコンピュータ実施方法であって、

前記受信システムは、処理ユニットおよびメモリを含み、

前記アイデンティティ情報文書は、前記開始システムを使用する当事者についてのアイデンティティ情報の一部または全部から成り、該アイデンティティ情報は、該当事者に関する情報の集合および該情報の集合の用途を含み、

前記処理ユニットが実施する前記方法は、

前記開始システムからサインされた第１のアイデンティティ情報文書を第１の受信シス

テムにて受信するステップであって、前記第１のアイデンティティ情報文書は、前記当事者に関連し、かつ前記開始システムに含まれている自己アイデンティティ情報ストアから選択されるアイデンティティ情報の第１のサブセットを含む選択されたアイデンティティ情報を含み、前記アイデンティティ情報の第１のサブセットは、前記第１の受信システムに固有のものであり、前記アイデンティティ情報の第１のサブセットは、アイデンティティ情報の第２のサブセットとは異なり、前記アイデンティティ情報の第２のサブセットは、第２の受信システムを対象とした第２のアイデンティティ情報に含まれる、ステップと、

前記第１のアイデンティティ情報文書におけるアイデンティティ情報の第１のサブセットが信頼できるかどうかを判定するステップと、

前記アイデンティティ情報の第１のサブセットが信頼できると判定された場合、前記第１の受信システムに置かれ、かつ前記メモリに格納されている認識済みアイデンティティ情報ストアに前記アイデンティティ情報の第１のサブセットを保存するステップと、

前記アイデンティティ情報の第１のサブセットが信頼できないと判定された場合、前記アイデンティティ情報の第１のサブセットを検証するか否かを判定するステップと、

前記アイデンティティ情報の第１のサブセットが信頼できないと判定された場合、前記アイデンティティ情報の第１のサブセットが信頼できないことを示すフラグとともに、前記第１の受信システムにおいて、前記認識済みアイデンティティ情報ストアに前記アイデンティティ情報の第１のサブセットを保存するステップと

を含むことを特徴とする方法。

【請求項８】

前記アイデンティティ情報の第１のサブセットを検証する判定に応じて、前記第１のアイデンティティ情報文書の開始システムからアイデンティティ認識番号（ＩＲＮ）を検索するステップと、前記ＩＲＮが正しいかどうかを判定するステップと、前記ＩＲＮが正しいことに応じて、前記アイデンティティ情報の第１のサブセットを前記認識済みアイデンティティ情報ストアに保存するステップと

をさらに含むことを特徴とする請求項７に記載の方法。

【請求項９】

前記アイデンティティ情報の第１のサブセットが信頼できるかどうかを判定するステップは、グラフィカルユーザインタフェースを介したユーザ入力に基づいて行われることを特徴とする請求項７に記載の方法。

【請求項１０】

前記アイデンティティ情報の第１のサブセットを検証するか否かを判定するステップは、グラフィカルユーザインタフェースを介したユーザ入力に基づいて行われることを特徴とする請求項７に記載の方法。

【請求項１１】

アイデンティティ情報文書を送信するシステムであって、

前記アイデンティティ情報文書は、当事者についてのアイデンティティ情報の一部または全部から成り、該アイデンティティ情報は、該当事者に関する情報の集合および該情報の集合の用途を含み、

前記システムは、

プロセッサと、

前記プロセッサに接続された通信チャネルと、

前記プロセッサに結合され、かつ前記プロセッサによって読取り可能なメモリと

を備え、

前記メモリは、前記プロセッサによって実行された場合、前記プロセッサに、

第１のアイデンティティ情報文書に含めるために、開始システムに含まれている自己アイデンティティ情報ストアからアイデンティティ情報を選択するステップであって、前記選択されたアイデンティティ情報は、前記自己アイデンティティ情報ストアの当事者に関連するアイデンティティ情報の所定の第１のサブセットを含み、前記アイデンティティ情

報の所定の第１のサブセットは、第１の意図された受信システムに固有のものであり、かつ前記第１のアイデンティティ情報文書に含めるために自動的に選択され、前記自己アイデンティティ情報ストアの当事者に関連するアイデンティティ情報の所定の第２のサブセットは、第２の意図された受信システムに固有のものであり、前記アイデンティティ情報の第２のサブセットは、前記アイデンティティ情報の第１のサブセットとは異なる、ステップと、

前記開始システムに含まれている前記自己アイデンティティ情報ストアから前記アイデンティティ情報の第１のサブセットを読み取るステップと、

前記アイデンティティ情報の第１のサブセットおよび少なくとも第１のキーを含めるために、前記第１のキーと対になった第２のキーを使用してサインされた前記第１のアイデンティティ情報文書を生成するステップと、

前記第１のアイデンティティ情報文書を前記通信チャネルに接続された前記第１の意図された受信システムに送信して該第１の受信システムにて前記受信者のアイデンティティを確立するステップと

を行わせる一連の命令を含むことを特徴とするシステム。

【請求項１２】

第１のアイデンティティ情報文書に含めるために、アイデンティティ情報を選択するステップは、グラフィカルユーザインタフェース（ＧＵＩ）からのユーザ入力に基づいて前記自己アイデンティティ情報ストアからアイデンティティ情報の第１のサブセットを選択するステップを含むことを特徴とする請求項１１に記載のシステム。

【請求項１３】

前記第１のアイデンティティ情報文書を生成するステップは、拡張可能マークアップ言語（ＸＭＬ）文書において前記アイデンティティ情報の第１のサブセットを符号化するステップを含むことを特徴とする請求項１１に記載のシステム。

【請求項１４】

前記アイデンティティ情報の第１のサブセットは、前記第１のアイデンティティ情報文書を発信する当事者のアイデンティティ主張を含むことを特徴とする請求項１１に記載のシステム。

【請求項１５】

前記アイデンティティ情報の第１のサブセットは、前記アイデンティティ情報の第１のサブセットの内容を使用することができる用途を規定するための使用法ポリシーを含むことを特徴とする請求項１１に記載のシステム。

【請求項１６】

当事者の将来の認識において使用するために開始システムからアイデンティティ情報文書を受信するシステムであって、

前記アイデンティティ情報文書は、前記開始システムを使用する当事者についてのアイデンティティ情報の一部または全部から成り、該アイデンティティ情報は、該当事者に関する情報の集合および該情報の集合の用途を含み、

前記システムは、

プロセッサと、

前記プロセッサに接続された通信チャネルと、

前記プロセッサに結合され、かつ前記プロセッサによって読取り可能なメモリと

を備え、

前記メモリは、前記プロセッサによって実行された場合、前記プロセッサに、

前記開始システムからサインされた第１のアイデンティティ情報文書を第１の受信システムにて受信するステップであって、選択されたアイデンティティ情報を含む前記サインされた第１のアイデンティティ情報文書は、前記開始システムに含まれている自己アイデンティティ情報ストアの当事者に関連するアイデンティティ情報の第１のサブセットを含み、前記アイデンティティ情報の第１のサブセットは、前記第１の受信システムに固有のものであり、自己アイデンティティ情報ストアの当事者に関連するアイデンティティ情報

の第２のサブセットは、第２の意図された受信システムに固有のものであり、前記第２の意図された受信システムは、前記第１の意図された受信システムとは異なり、前記アイデンティティ情報の第２のサブセットは、前記アイデンティティ情報の第１のサブセットとは異なる、ステップと、

前記第１のアイデンティティ情報文書におけるアイデンティティ情報の第１のサブセットが信頼できるかどうかを判定するステップと、

前記アイデンティティ情報の第１のサブセットが信頼できない場合、前記アイデンティティ情報の第１のサブセットを検証するかどうかを判定するステップと、

前記アイデンティティ情報の第１のサブセットが信頼できると判定された場合、前記第１の受信システムに置かれている認識済みアイデンティティ情報ストアに前記アイデンティティ情報の第１のサブセットを保存するステップと、

前記アイデンティティ情報の第１のサブセットが信頼できない場合、前記アイデンティティ情報の第１のサブセットが信頼できないことを示すフラグとともに、前記第１の受信システムにおいて、前記認識済みアイデンティティ情報ストアに前記アイデンティティ情報の第１のサブセットを保存するステップであって、前記認識済みアイデンティティ情報ストアは、前記当事者の将来の認識のために使用される、ステップと

を行わせる一連の命令を含む、ことを特徴とするシステム。

【請求項１７】

前記アイデンティティ情報の第１のサブセットを検証する判定に応じて、前記第１のアイデンティティ情報文書の開始システムからアイデンティティ認識番号（ＩＲＮ）を受信するステップと、前記ＩＲＮが正しいかどうかを判定するステップと、前記ＩＲＮが正しいことに応じて、前記アイデンティティ情報の第１のサブセットを前記認識済みアイデンティティ情報ストアに保存するステップと

をさらに含むことを特徴とする請求項１６に記載のシステム。

【請求項１８】

前記アイデンティティ情報の第１のサブセットが信頼できるかどうかを判定するステップは、グラフィカルユーザインタフェースを介したユーザ入力に基づいて行われることを特徴とする請求項１７に記載のシステム。

【請求項１９】

前記アイデンティティ情報の第１のサブセットを検証すべきかどうかを判定するステップは、グラフィカルユーザインタフェースを介したユーザ入力に基づいて行われることを特徴とする請求項１７に記載のシステム。

【請求項２０】

アイデンティティ認識のコンピュータプロセスを実行するためのコンピュータプログラムを含むコンピュータ読み取り可能な記憶媒体であって、前記コンピュータプログラムは、処理ユニットおよびメモリを含むコンピュータによって実行される場合に、前記コンピュータプロセスを前記処理ユニットに実行させ、前記コンピュータプロセスは、

第１のアイデンティティ情報文書および第２のアイデンティティ情報文書に含める情報を選択するために、前記開始システムに含まれている自己アイデンティティ情報ストアから前記開始システムを使用する当事者についてのアイデンティティ情報のリストを示すステップであって、該第１および第２のアイデンティティ情報文書は、前記開始システムを使用する当事者についてのアイデンティティ情報の一部または全部から成り、該アイデンティティ情報は、該当事者に関する情報の集合および該情報の集合の用途を含み、前記第１のアイデンティティ情報文書は、第１の意図された受信システム用に作成され、前記第２のアイデンティティ情報文書は、第２の意図された受信システム用に作成され、前記第１の意図された受信システムは、前記第２の意図された受信システムとは異なり、前記アイデンティティ情報のリストを選択のために示すステップは、前記当事者に前記第１および第２の意図された受信システムへのアイデンティティ情報の開示を制御することを可能にさせる、ステップと、

前記第１のアイデンティティ情報文書に含めるために、前記メモリに格納されている、

前記自己アイデンティティ情報ストアからのアイデンティティ情報のリストから前記アイデンティティ情報の第１の選択を受信するステップであって、選択された第１のアイデンティティ情報は、前記自己アイデンティティ情報ストアの前記当事者に関連するアイデンティティ情報の第１のサブセットを含み、前記アイデンティティ情報の第１のサブセットは、前記第１の意図された受信システムに固有のものである、ステップと、

前記第２のアイデンティティ情報文書に含めるために、メモリに格納されている、前記自己アイデンティティ情報ストアからのアイデンティティ情報のリストから前記アイデンティティ情報の第２の選択を受信するステップであって、選択された第２のアイデンティティ情報は、前記自己アイデンティティ情報ストアの前記当事者に関連するアイデンティティ情報の第２のサブセットを含み、前記アイデンティティ情報の第２のサブセットは、前記第２の意図された受信システムに固有のものであり、かつ前記アイデンティティ情報の第１のサブセットとは異なる、ステップと、

前記開始システムに含まれている自己アイデンティティ情報ストアから前記選択された第１および第２のアイデンティティ情報を読み取るステップと、

前記選択された第１のアイデンティティ情報および少なくとも公開鍵を含めるために、前記第１のアイデンティティ情報文書における前記公開鍵に関連付けられた秘密鍵を使用してサインされた前記第１のアイデンティティ情報文書を生成するステップと、

前記第１のアイデンティティ情報文書を前記第１の受信システムに送信し、前記第１の受信システムにて前記当事者のアイデンティティを確立するステップと、

選択された前記第２のアイデンティティ情報およびデジタルシグネチャを含むように前記第２のアイデンティティ情報文書を生成するステップと、

前記第２のアイデンティティ情報文書を前記第２の受信システムに送信し、前記第２の受信システムにて前記当事者のアイデンティティを確立するステップと

を含むことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項２１】

前記アイデンティティ情報の第１の選択を受信するステップは、グラフィカルユーザインタフェース（ＧＵＩ）からのユーザ入力に基づいて前記自己アイデンティティ情報ストアからアイデンティティ情報の第１のサブセットを受信するステップを含むことを特徴とする請求項２０に記載のコンピュータ読み取り可能な記憶媒体。

【請求項２２】

前記第１のアイデンティティ情報文書を生成するステップは、拡張可能マークアップ言語（ＸＭＬ）文書において前記選択された第１のアイデンティティ情報を符号化するステップを含むことを特徴とする請求項２０に記載のコンピュータ読み取り可能な記憶媒体。

【請求項２３】

前記選択された第１のアイデンティティ情報は、前記第１のアイデンティティ情報文書を発信する当事者のアイデンティティ主張を含むことを特徴とする請求項２０に記載のコンピュータ読み取り可能な記憶媒体。

【請求項２４】

前記選択された第１のアイデンティティ情報は、前記アイデンティティ情報の内容を置くことができる用途を規定する使用法ポリシーを含むことを特徴とする請求項２０に記載のコンピュータ読み取り可能な記憶媒体。

【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およびネットワークセキュリティの分野に関する。より詳細には、本発明は、異種コンピュータシステム間のユーザ制御アイデンティティ情報の交換に関する。

【背景技術】

【０００２】

資源を共有すべきコンピュータの表現を有しないネットワーク上でコンピュータの資源

をユーザと共有することがしばしば望まれる。たとえば、企業、大学、または他の組織は従業員、学生、または他の個人が使用するために何らかのタイプのネットワークに接続される１つまたは複数のサーバを有することがある。個人を含む様々なエンティティはインターネットまたは他のネットワーク上で情報または資源を共有する。有線および無線ネットワークは家庭で使用するために一般的になりつつあり、パーソナルコンピュータから家庭用機器までの広い範囲のデバイスはこれらのネットワークに接続され、アクセス可能になる。より広い範囲の資源へのより容易なアクセスが利用可能になるにつれて、これらの資源の安全な（ｓｅｃｕｒｅ）共有およびそれらの間の共同作業がより重要になる。

【０００３】

これらの資源の安全な共有およびそれらの間の共同に対する１つの障害は、与えられた資源にアクセスしようと試みる様々なエンティティを認識および認証することに関する。言い換えれば、コンピュータ上の資源にアクセスしようと試みるエンティティが、それがあると主張するエンティティであり、それらの資源にアクセスするために必要な許可を有することを確認および保証するように注意を払わなければならない。エンティティを認識し、許可を与える様々な方法が使用されている。

【０００４】

エンティティを認識し、許可を与える１つの方法は、セキュリティドメインを規定するためにセットアップされるアカウントおよびパスワードのシステムを含む。たとえば、企業は、セキュリティドメインがその企業のあらゆる常勤従業員からなるサーバまたはネットワークのためのセキュリティドメインを生成することを望むことがある。システムアドミニストレータなどのセキュリティドメインを実行しているものは、一般にユーザ名およびパスワード含むアカウントを各従業員に与え、これらのアカウントを介して資源へのアクセスを制御するポリシーをセットアップする。ひとたびセキュリティドメインが所定の位置にくると、アカウントのない物を排除しながらドメインメンバに資源へのアクセスを与えることができる。

【０００５】

しかしながら、ユーザが様々なユーザ名およびパスワードを憶える必要があるアカウントのシステムに基づくセキュリティドメインは面倒なことがある。さらに、アカウントのシステムに基づくセキュリティドメインはインターネットなどのネットワーク上で情報または資源を共有することを望む個人にとって良いモデルではない。加えて、様々なビジネス上の理由で、旧来の閉セキュリティドメインを拡張し、さらにはインターネット上から選択された個人と交換する必要があることがある。たとえば、従業員、外部コントラクタ、および他の個人またはエンティティが、共有される文書、コミュニティ、および他の資源にアクセスする仮想チームの一員になりうるプロジェクトをセットアップする必要があることがある。

【発明の開示】

【発明が解決しようとする課題】

【０００６】

資源にアクセスするための有効なユーザ名およびパスワードをもつアカウントを使用する誰かがそのアカウントの所有者であると仮定することは比較的容易であるが、旧来の閉セキュリティドメインの一員でないアイデンティティ（身元情報と称することがある）を認識することは極めて困難であった。エンティティを識別および認証する方法としてパブリックキーインフラストラクチャが使用されてきた。パブリックキーインフラストラクチャは証明または推薦機関とこれらのシステムのユーザとの間の信頼関係に基づく。しかしながら、これらのインフラストラクチャは理解、ブートストラップ、および管理が複雑である。したがって、パブリックキーインフラストラクチャは簡単で使いやすい、様々なタイプのエンティティに適用可能なアイデンティティ認識システムを提供しないので、コンピュータユーザを認識する主流技術にはならなかった。これらの考察および他の物に関して本発明はなされたのである。

【課題を解決するための手段】

【０００７】
上記および他の問題は、受信者によって送信者をアイデンティティ認識するため、および送信者によってサインされたアイデンティティ情報を利用してアイデンティティ情報を交換するためのシステムおよび方法によって解決される。当事者に関する選択されたアイデンティティ情報はコンピュータシステム間で交換することができ、当事者の認識に使用することができるアイデンティティ情報文書に含まれる。アイデンティティ認識は許可を含まない。本発明では、送信者の許可、すなわちアイデンティティ認識と、受信者の資源にアクセスする送信者の許可は分けられる。
【０００８】
さらに他の態様によれば、本発明は、アイデンティティ情報文書に含めるために自己アイデンティティ情報ストアからアイデンティティ情報を選択するステップを含むアイデンティティ情報文書を送信する方法に関する。選択されたアイデンティティ情報を自己アイデンティティ情報ストアから読み取り、選択されたアイデンティティ情報およびパブリックキーなどの少なくとも第１のキーを含むためにアイデンティティ情報文書を生成する。アイデンティティ情報文書は、アイデンティティ情報文書に含まれる第１のキーに関連付けられたプライベートキーなどの第２のキーを使用して送信者がサインしたデジタルシグナチャを有する。次いでアイデンティティ情報文書を受信者に送信する。本発明の別の態様によれば、アイデンティティ情報文書を受信する方法は、サインされたアイデンティティ情報文書を発信者または送信者から受信するステップを含む。アイデンティティ情報文書で運ばれるアイデンティティ情報が信頼できるかどうかに関して判定を行う。アイデンティティ情報が信頼できると判定された場合、アイデンティティ情報を認識済みアイデンティティ情報ストアに保存する。認識済みアイデンティティ情報ストアは、発信者が再び受信者のコンピュータシステムに接続しようと試みた場合に発信者の将来の認識および認証のために使用される。
【０００９】
さらに他の態様によれば、本発明は、アイデンティティ情報文書を送信するシステムに関する。システムは、プロセッサと、プロセッサに接続された通信チャネルと、プロセッサに結合され、プロセッサによって読取り可能なメモリとを含む。メモリは、プロセッサによって実行された場合、プロセッサに、アイデンティティ情報文書に含めるために自己アイデンティティ情報ストアからアイデンティティ情報を選択させる一連の命令を含む。選択されたアイデンティティ情報は自己アイデンティティ情報ストアから読み取られ、選択されたアイデンティティ情報および少なくとも第１のキーを含めるためにアイデンティティ情報文書は生成される。アイデンティティ情報文書はアイデンティティ情報文書に含まれる第１のキーと対になった第２のキーを使用してサインされたデジタルシグナチャを有する。次いでアイデンティティ情報文書は通信チャネルに接続された受信者に送信される。
【００１０】
さらに他の態様によれば、本発明は、アイデンティティ情報文書を受信するシステムに関する。システムは、プロセッサと、プロセッサに接続された通信チャネルと、プロセッサに結合され、プロセッサによって読取り可能なメモリとを含む。メモリは、プロセッサによって実行された場合、プロセッサに、発信者または送信者からサインされたアイデンティティ情報文書を受信させる一連の命令を含む。アイデンティティ情報文書によって運ばれるアイデンティティ情報が信頼できるかどうかに関して判定が行われる。アイデンティティ情報が信頼できると判定された場合、アイデンティティ情報は認識済みアイデンティティ情報ストアに保存される。認識済みアイデンティティ情報ストアは、発信者が受信者のコンピュータシステムに接続しようと試みた場合、発信者の将来の認識および認証に使用される。
【００１１】
本発明は、コンピュータプロセス、コンピューティングシステムとして、またはコンピュータプログラム製品またはコンピュータ読取り可能媒体などの製造物品として実施する

ことができる。コンピュータ読取り可能媒体は、コンピュータシステムによって読取り可能であり、コンピュータプロセスを実行するための命令のコンピュータプログラムを符号化するコンピュータ記憶媒体とすることができる。コンピュータ読取り可能媒体は、コンピュータシステムによって読取り可能であり、コンピュータプロセスを実行するための命令のコンピュータプログラムを符号化する搬送波上の伝搬信号とすることができる。

【００１２】

本発明を特徴付けるこれらおよび様々な他の特徴ならびに利点は以下の詳細な説明を読むことおよび関連する図面を見ることから明らかになろう。

【発明を実施するための最良の形態】

【００１３】

本発明の様々な実施形態を説明する前に、本説明を通して使用するいくつかの用語を定義する。

【００１４】

「アイデンティティ情報」は、当事者またはその代理人が、どのような情報が受信デバイスに伝えられるかを制御することができ、かつ当該情報の意図された用途を示すことができる、アイデンティティ情報システムにおける当事者に関する情報の集合である。

【００１５】

「アイデンティティ情報文書」は、受信デバイスが、当該アイデンティティ情報文書の発信者を示すことができ、かつ当該発信者が開始または応答したデジタルイベントをその後認識することができるように、あるデバイスから別のデバイスに送信された当事者についてのアイデンティティ情報のサブセットである。

【００１６】

「当事者」とは、デジタル的に行動することが可能な何らかのエンティティである。当事者は、個人、家庭、組織、明示的グループ、および共通の役割にある人々、またはある種の属性およびこれらの個人がそれによって行動する様々な電子デバイスを共有する人々を意味する個々の人々、グループ、あるいは人々の集合である。

【００１７】

図１は本発明の一実施形態によるアイデンティティ認識のためのシステムを概念レベルで示す。この例はネットワーク１１１または他のチャネルを介して接続された開始システム１０１および受信システム１０６を示す。明らかになるように、たいていのデバイスは様々な時刻に開始システム１０１としても受信システム１０６としても機能する。しかしながら、簡単のために、これらの機能はここでは別々に示されている。加えて、ネットワーク１１１は、インターネットを含む何らかのタイプのネットワークとすることができ、または開始システム１０１と受信システム１０６の間に通信を確立するのに適したある他のタイプのチャネルとすることができる。

【００１８】

開始システム１０１は自己アイデンティティ情報１０２のセットを維持する。自己アイデンティティ情報１０２は、開始システム１０１によって表されるかまたはそれを使用する当事者に関する様々な情報を含むことができる。この情報は、たとえば、名前、電子メールアドレス、ウェブサイトＵＲＬ、および他の個人情報、ならびにこの情報がどのように使用することができるかを記載した使用法ポリシーを含むことができる。これらの異なる識別要素を本明細書ではアイデンティティ主張と呼ぶ。

【００１９】

自己アイデンティティ情報１０２の一部または全部を含むアイデンティティ情報文書１０５が作成される。一実施形態において、アイデンティティ情報文書１０５は受信システム１０６からの要求に応じて作成される。したがって、開始システム１０１によって表されるかまたはそれを使用する当事者が受信システム１０６などの他のシステムにアイデンティティ情報を送信したい場合、ユーザは自己アイデンティティ情報１０２から送信すべき情報を選択する。言い換えれば、当事者はアイデンティティ情報文書１０５を生成する場合に自己アイデンティティ情報１０２からの情報の開示を制御する能力を有する。した

がって、当事者は異なる受信者へのアイデンティティデータの異なるサブセットを選択的に開示し、開示情報をどのように使用することができるかに関してその意志を表わすことができる。さらに、これにより「漸進的開示」が可能になり、当事者は情報をほとんど含まない第１のアイデンティティ情報文書を送信し、それを行う理由がある場合にある後の時点でより多くの情報を漏らすこともできる。

【００２０】

特定の一実施形態において、全アイデンティティ情報文書は、アイデンティティ情報文書が生成された場合にアイデンティティ情報文書を発信した当事者のプライベートキーを使用してデジタルシグナチャでサインされる。したがって、アイデンティティ情報文書は自己サインされていると呼ばれる。別の実施形態において、全アイデンティティ情報文書は、アイデンティティ情報文書が生成された場合にアイデンティティ情報文書を発信した当事者に対してアイデンティティ主張を発行した組織のプライベートキーでサインされたデジタルシグナチャを有する。この場合、アイデンティティ情報文書は組織によってサインされていると呼ばれる。同様に、既に共有されているアイデンティティ情報文書または漸進的開示の更新は、元々共有されていたアイデンティティ情報をサインするために使用されたプライベートキーを使用してサインされることになる。サインするプライベートキーと対になったパブリックキーはアイデンティティ情報文書の一部として含む様々な様式で分配することができる。あるいは、パブリック／プライベートキーシステム以外のキー構成を使用することができる。たとえば、一連のプライベートキーを使用することができる。

【００２１】

開始システム１０１は自己アイデンティティ情報１０２から、サインされたアイデンティティ情報文書１０５を生成し、それをネットワーク１１１を介して受信システムに送信する。一実施形態によれば、アイデンティティ情報は、受信システム１０６にチャネルを使用して送信することができる拡張可能マークアップ言語（ＸＭＬ）ファイルまたはテキストファイルを含むことができる。アイデンティティ情報文書１０５の１つの可能なフォーマットの詳細については図６を参照しながら以下で述べる。しかしながら、一般的に言えば、アイデンティティ情報文書１０５は様々なタイプのチャネル上の異種システム間で情報を転送するのに適したフォーマットとすることができる。上述のように、アイデンティティ情報文書１０５を開始システム１０１から受信システム１０６に転送するために使用されるチャネルは様々な可能な媒体のいずれかとすることができる。たとえば、電子メール、インスタントメッセージング、ビーミング、専用回線および多くの他の機構をチャネルとして使用することができる。さらに、チャネルは安全であることもあり、安全でないこともある。

【００２２】

受信システム１０６は着信したアイデンティティ情報文書１０５を読み取り、それを受諾または拒否する。一般的なシナリオにおいて、アイデンティティ情報文書１０５は既知の当事者から発信し、受信システム１０６はアイデンティティ情報文書１０５の認証の極めて優れた審判となる。しかしながら、アイデンティティ情報文書１０５が未知の当事者から到着した場合、または詐欺師がアイデンティティ情報文書１０５を開き、変更または偽造するのに十分な動機を有する恐れがある場合、受信システム１０６はアイデンティティ情報文書１０５を拒否するか、またはそれの真正性のさらなる検証を求めることができる。この検証の詳細については図３～６を参照しながら以下で説明する。

【００２３】

ひとたびアイデンティティ情報文書が受諾されると、それが含んでいる情報は受信システム１０６の認識済みアイデンティティ情報１０７に加えられる。ひとたびアイデンティティ情報文書１０５が認識済みアイデンティティ情報１０７のリストに加えられると、受信システム１０６は次いでそれが含んでいる情報を使用して、将来開始システム１０１を認証し、さもなければ信頼することができないその当事者と対話するチャネルを使用することができる。次いでアイデンティティ情報文書１０５によって表される当事者に、たと

えば、カレンダや文書など、受信システム１０６上の資源へのアクセスを与えることができる。あるいは、当事者は課題を与えられ、課題が満足された場合、受信システム上の資源へのアクセスを許可されることもある。逆に、受信システム１０６によって受諾されたアイデンティティ情報文書を提供しなかった識別されていないシステム１１０によって表されるかまたはそれを使用する識別されていない当事者は受信システム１０６の資源から排除することができる。同様に、受信システム１０６によって受諾されたアイデンティティ情報文書を提供した識別されたシステム１１０によって表されるかまたはそれを使用する識別された当事者は受信システム１０６の資源から意図的に排除することができる。

【００２４】

アイデンティティ情報１０５の使用およびアイデンティティ情報を認識済みアイデンティティ情報リスト１０７にインポートすることによる当事者の認識は受信システム１０６またはそれへのアクセスに関する資格をその当事者に自動的に提供しない。それは将来当事者を認識および認証するための受信システム１０６の能力を提供するだけである。認識または認証はファイル共有の許可、暗号化されたメールの送信、以前に共有されていたアイデンティティ情報の自動更新などの可能性を提供する。誰でも認識することができる。認識とは、受信システム１０６が誰を扱っているのかを受信システム１０６が知ることを暗示し、アクセス権が当事者に与えられることは暗示しない。当事者を認識することは、彼らに何かへのアクセスを与えることを暗示しない。彼らには認証後またはそうすることが有用または安全（ｓａｆｅ）である場合にアクセスを与えることができる。

【００２５】

したがってアイデンティティ認識は一方向に働く。したがってアイデンティティ認識がいずれかの方向に効果的に働くために開始システム１０１と受信システム１０６の間のアイデンティティ情報の二方向交換を要求することが必要である。開始システム１０１から受信システム１０６へのアイデンティティ情報文書１０５の一方向交換は、開始システム１０１によって表されるかまたはそれを使用して当事者を識別し、適宜その当事者を扱うために受信システム１０６にとって十分である。

【００２６】

アイデンティティ情報文書１０５および認識されたアイデンティティリスト１０７に基づいて受信システム１０６の資源へのアクセスを許すことは、当事者のアイデンティティを認識することができず、アクセスを適宜付与または拒否することができる場合、または追加の許可プロセスを要求することができる場合、安全を損なわない。さらに、認識されていない当事者を排除することができる。

【００２７】

図２は本発明の実施形態を実施することができる適切なコンピューティングシステム環境の例を示す。このシステム２００は開始システムおよび／または上述のような受信システムとして働くために使用することができる物を代表する。その最も基本的な構成において、システム２００は一般に少なくとも１つ処理ユニット２０２およびメモリ２０４を含む。コンピューティングデバイスの正確な構成およびタイプに応じて、メモリ２０４を揮発性（ＲＡＭなど）、不揮発性（ＲＯＭ、フラッシュメモリなど）または２つのある組合せとすることができる。この最も基本的な構成を図２に破線２０６で示す。加えて、システム２００はまた追加フィーチャ／機能を有することができる。たとえば、デバイス２００はまた、限定はしないが、磁気または光ディスクまたはテープを含む追加のストレージ（取外し可能および／または取外し不能）を含むことができる。そのような追加のストレージを図２に取外し可能ストレージ２０８および取外し不能ストレージ２１０で示す。コンピュータ記憶媒体はコンピュータ読取り可能命令、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記憶のための方法または技術で実施された揮発性および不揮発性、取外し可能および取外し不能媒体を含む。メモリ２０４、取外し可能ストレージ２０８および取外し不能ストレージ２１０はすべてコンピュータ記憶媒体の例である。コンピュータ記憶媒体は、限定はしないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル汎用ディスク（ＤＶＤ）または他の

光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージまたは他の磁気記憶デバイス、または所望の情報を記憶するために使用することができ、システム２００がアクセスすることができる他の媒体を含むことができる。そのようなコンピュータ記憶媒体はシステム２００の一部とすることができる。

【００２８】

システム２００はまたシステムが他のデバイスと通信することを可能にする通信接続２１２を含むことができる。通信接続２１２は通信媒体の例である。通信媒体は一般にコンピュータ読取り可能命令、データ構造、プログラムモジュール、または搬送波や他の輸送機構などの変調データ信号の他のデータを実施し、情報配布媒体を含む。「変調データ信号」という用語は、信号中の情報を符号化するような様式で設定または変更されたそれの特性の１つまたは複数を有する信号を意味する。限定ではなく例として、通信媒体は有線ネットワークや直接有線接続などの有線媒体、および音響、ＲＦ、赤外などの無線媒体および他の無線媒体を含む。本明細書で使用するコンピュータ読取り可能媒体という用語は記憶媒体と通信媒体の両方を含む。

【００２９】

システム２００はまたキーボード、マウス、ペン、ボイス入力デバイス、タッチ入力デバイスなどの入力デバイス２１４を含む。ディスプレイ、スピーカ、プリンタなどの出力デバイス２１６も含むことができる。すべてのこれらのデバイスは当技術分野でよく知られており、本明細書では長く述べる必要はない。

【００３０】

システム２００などのコンピューティングデバイスは一般に少なくとも何らかの形態のコンピュータ読取り可能媒体を含む。コンピュータ読取り可能媒体はシステム２００がアクセスできる利用可能な媒体である。限定ではなく例として、コンピュータ読取り可能媒体はコンピュータ記憶媒体および通信媒体を備えることがある。

【００３１】

図３は本発明の一実施形態によるアイデンティティ認証のためのシステムの主ソフトウェア構成要素を示す。この例は、図１に示す例と同様、チャネル３０６によって接続された開始システム３０１と受信システム３０９を示す。また、上述のように、システムは様々な時刻に開始システム３０１と受信システム３０９の両方として機能することができる。しかしながら、簡単のために、これらの機能を本明細書では別々に示す。

【００３２】

開始システム３０１は自己アイデンティティ情報ストア（自己アイデンティティ情報記憶手段）３０２、自己アイデンティティ情報制御モジュール３０３、アイデンティティ情報処理ユニット３０４、アイデンティティ認識番号（ＩＲＮ）処理モジュール３０５を含む。自己アイデンティティ情報ストア３０２はデータベース、リスト、または開始システム３０１によって表されるかまたはそれを使用する当事者に固有の情報の他の集合を備える情報を記憶することができる。自己アイデンティティ情報ストア３０２は当事者の名前、電子メールアドレス、パブリックキーおよび／または証明書、および以下で説明するようにアイデンティティ情報文書において使用することができる他の個人化情報などの情報を記憶することができる。

【００３３】

自己アイデンティティ情報制御モジュール３０３は自己アイデンティティ情報ストア３０２からアイデンティティ情報を読み取る。当事者はアイデンティティ情報を別のシステムに送信したい場合、自己アイデンティティ情報制御モジュール３０３を介して自己アイデンティティ情報ストア３０２から送信すべき情報を選択する。たとえば、当事者がアイデンティティ情報文書を送信したい場合、当事者がその自己アイデンティティ情報ストア３０２から送信すべき情報を選択する自己アイデンティティ情報制御モジュール３０３によってグラフィカルユーザインタフェース（ＧＵＩ）を提示することができる。

【００３４】

自己アイデンティティ情報制御モジュール３０３はアイデンティティ情報文書３０７を

生成する場合に自己アイデンティティ情報ストア３０２からの情報の開示を制御する能力を当事者に提供する。ＧＵＩを介して提示された場合、自己アイデンティティ情報を様々な読みやすく、使いやすいフォーマットで提示することができる。たとえば、アイデンティティ情報文書に含めることを示すために、チェックマーク、さもなければ選択するよう、情報のリストをユーザに対して提示することができる。したがって自己アイデンティティ情報制御モジュール３０３は当事者が異なる受信システム３０９に対してアイデンティティ情報の異なるサブセットを選択的に開示し、開示情報をどのように使用することができるかに関して当事者の意志を表わすことを可能にする。さらに、自己アイデンティティ情報制御モジュール３０３により「漸進的開示」が可能になり、当事者は情報をほとんど含まない第１のアイデンティティ情報文書を送信し、それを行う理由がある場合にある後の時点でより多くの情報を漏らすこともできる。

【００３５】

アイデンティティ情報処理ユニット３０４は自己アイデンティティ情報制御モジュール３０３によって提供された情報からアイデンティティ情報文書３０７を生成し、それをチャネル３０６を介して受信システム３０９に送信する。一実施形態によれば、アイデンティティ情報文書３０７は、受信システム３０９にいずれかのチャネルを使用して送信することができるＸＭＬファイルまたはテキストファイルを含むことができる。アイデンティティ情報の１つの可能なフォーマットの詳細は以下で図６を参照しながら述べる。しかしながら、一般的に言えば、アイデンティティ情報３０７は異種システム間で情報を転送するのに適したフォーマットであるべきである。

【００３６】

開始システム３０１から受信システム３０９にアイデンティティ情報文書３０７を転送するために使用されるチャネル３０６は様々な可能な媒体のいずれかとすることができる。たとえば、電子メール、インスタントメッセージング、ビーミング、専用回線および多くの他の機構をチャネル３０６として使用することができる。チャネル３０６は安全であることもあり、安全でないこともある。

【００３７】

受信システム３０９はアイデンティティ情報処理ユニット３１２、受信済みアイデンティティ情報制御モジュール３１１、認識済みアイデンティティ情報ストア（認識済みアイデンティティ情報）３１０およびＩＲＮ処理モジュール３１４を含む。受信システム３０９のアイデンティティ情報処理ユニット３１２はチャネル３０６から着信アイデンティティ情報３０７を受信する。アイデンティティ情報処理ユニット３１２はアイデンティティ情報文書３０７からのアイデンティティ情報を受信済みアイデンティティ情報制御モジュール３１１に渡す。

【００３８】

受信済みアイデンティティ情報制御モジュール３１１はアイデンティティ情報文書３０７を受諾すべきか拒否すべきかを判定する。いくつかの場合、この判定は、受信済み情報を受諾すべきか拒否すべきかに関してＧＵＩを介してユーザを待ち行列化することに基づくことができる。ＧＵＩを介して提示された場合、アイデンティティ情報文書からのアイデンティティ情報は様々な読みやすいフォーマットで提示することができる。たとえば、アイデンティティ情報は情報の迅速で容易なレビューが可能なローロデックス（ｒｏｌｏｄｅｘ）または「コンタクト」エントリの形態で提示することができる。

【００３９】

アイデンティティ情報文書３０７が既知の当事者から発信した場合、受信システム３０９はアイデンティティ情報文書３０７の認証の極めて優れた審判となる。しかしながら、アイデンティティ情報が未知の当事者から発信した場合、または詐欺師がメールを開き、変更するのに十分な動機をもっている恐れがある場合、受信システム３０９はアイデンティティ認識番号（ＩＲＮ）処理モジュール３１４を使用してアイデンティティ情報文書３０７を検証する。

【００４０】

アイデンティティ情報文書３０７は様々な媒体上で交換することができる。媒体によっては他の媒体よりも詐欺にかかりやすい物もある。アイデンティティ情報文書３０７が電子メールのような詐欺にかかりやすい媒体上で交換される場合またはアイデンティティ情報文書３０７が別段に疑わしい場合、アイデンティティ情報文書３０７が詐欺または中心人物の攻撃を受けていないことを保証するためにアイデンティティ情報文書３０７の完全性の域外検証を行うことが有益である。域外検証が要求される程度は、どのようにアイデンティティ情報が獲得されるか、および送信側と共有されることが意図される情報の機密性によって異なる。

【００４１】

当事者へのアイデンティティ情報文書３０７の結合の域外検証をサポートするために、アイデンティティ認識番号（ＩＲＮ）を使用することができる。ＩＲＮはアイデンティティ情報文書に含められる読取り可能ストリングとして与えるために適切な変換機能をもつ当事者のパブリックキーのハッシュである。この変換機能を介したＩＲＮは一連の容易に読取り可能で覚えやすい番号によって示すことができる。たとえば、ＩＲＮは電話番号と同様とすることができる。

【００４２】

域外検証を行うために、受信システム３０９のＩＲＮ処理モジュール３１４はアイデンティティ情報文書３０７のＩＲＮを計算し、表示する。受信システムまたはそのユーザは次いで電話でまたはインスタントメッセージング（ＩＭ）を介して発信者を呼び出すなど、代替チャネル３０８によって発信者に連絡し、発信者にそのＩＲＮを確認するよう尋ねる。ＩＲＮ処理モジュール３１４は次いで、確認されたＩＲＮが受信済みアイデンティティ情報文書３０７に基づいて受信者端で計算された物と一致することを検証することができる。

【００４３】

中心人物の攻撃が送信者をだますためにパブリックキー情報を代用することによって受信システム３０９によって受信されたアイデンティティ情報文書３０７をいたずらした場合、計算されたＩＲＮは域外検証プロセスにおいて明白になるであろう真の送信者のＩＲＮに一致しないであろう。ＩＲＮはパブリックキーから計算された際にパブリック情報になることができ、したがって人のアイデンティティに対する注意としてビジネスカードなどのような物に含めるのに適していることに注意されたい。

【００４４】

ひとたびアイデンティティ情報文書３０７が受諾されると、それが含んでいる情報は認識済みアイデンティティ情報ストア（認識済みアイデンティティ情報記憶手段）１０７に追加される。アイデンティティ情報文書３０７を発信する当事者には次いで受信システム３０９上の資源へのアクセスが与えられる。将来、当事者がその資源へのアクセスを試みた場合、その人のコンピュータにはアイデンティティ情報文書３０７においてパブリックキーに関連付けられたプライベートキーの知識を証明するための課題が与えられる。当事者が真正である場合、コンピュータはこの知識の証拠を提供し、資源に対する認識および許可を生じることができる。

【００４５】

あるいは、拒否されたアイデンティティ情報でも認識済みアイデンティティ情報ストア１０７に入れることができる。たとえば、アイデンティティ情報の所与のセットが拒否されたとしても、それは将来の参照のために記憶し、信頼できない物としてマーキングされる。この認識済みであるが信頼できないアイデンティティ情報は、認識済みアイデンティティ情報ストアの特別な部分に記憶することによって、あるいは何らかの様式でタグ付けまたはフラグ付けすることなどによってマーキングすることができる。そのような情報は信頼できないアイデンティティ情報の将来の識別において有用であることがある。

【００４６】

加えて、認識済みアイデンティティ情報ストア１０７のアイデンティティ情報は、受信システムのユーザによるレビューのために、恐らくはＧＵＩによってアクセス可能なこと

がある。ＧＵＩを介して提示された場合、認識済みアイデンティティ情報ストア１０７からのアイデンティティ情報は様々な読みやすいフォーマットで提示することができる。たとえば、アイデンティティ情報は情報の迅速で容易なレビューが可能なローロデックスまたは「コンタクト」エントリの形態で提示することができる。

【００４７】

図３に示すシステムを使用すると、アイデンティティ情報の漸進的開示のプロセスを利用することによって、その主題（サブジェクト）ついての機密情報を含むアイデンティティ情報文書の交換を安全に行うことができる。このプロセスにおいて、発信者および受信者はまず、たとえばＸ５０９ｖ３証明書などの証明書、およびアイデンティティ情報文書を介した最低限必要なアイデンティティ主張（ｉｄｅｎｔｉｔｙ　ｃｌａｉｍ）にカプセル化することができるパブリックキーを交換する。両当事者は次いで情報の受信者のパブリックキーで暗号化された残りの開示された属性の全セットを交換する。これにより機密データは意図した受信者のみが見ることができ、他の誰にも見ることができなくなる。もちろん、漸進的開示方法を使用するためにアイデンティティ情報文書の交換が必要とされることは必須ではない。漸進的開示は同じく一方向共有に使用することができる。漸進的開示交換は無国籍で非同期に行うことができ、セッションによって覆い隠す必要も、特定のプロトコルに束縛する必要もない。

【００４８】

本発明の様々な実施形態の論理オペレーションは、（１）コンピュータ実施行為またはコンピューティグシステム上で実行するプログラムモジュールのシーケンスとして、および／または（２）コンピューティグシステム内の相互接続された機械論理回路または回路モジュールとして実施される。実施は、本発明を実施するコンピューティグシステムの性能用件に依存する選択の問題である。したがって、本明細書で説明する本発明の実施形態を構成する論理オペレーションはオペレーション、構造デバイス、行為またはモジュールと様々に呼ばれる。これらのオペレーション、構造デバイス、行為およびモジュールは本明細書に添付された特許請求の範囲に記載の本発明の趣旨および範囲から逸脱せずに、ソフトウェア、ファームウェア、特殊目的デジタル論理、およびその任意の組合せで実施することができることを当業者なら認識するであろう。

【００４９】

図４は本発明の一実施形態によるアイデンティティ情報の交換を開始するステップを示すフローチャートである。ここで処理は選択オペレーション４０５から始まる。選択オペレーション４０５は、アイデンティティ情報文書に含まれる自己アイデンティティ情報ストアからアイデンティティ情報を選択するステップを含む。選択オペレーションは、アイデンティティ情報の事前選択されたセットがいくつかの状況に対して識別されている場合、ＧＵＩを介してまたは自動的にユーザ入力に基づいてアイデンティティ情報文書に含めるためにアイデンティティ情報を選択する。制御は次いで読取りオペレーション４１０に渡る。

【００５０】

読取りオペレーション４１０は自己アイデンティティ情報ストアから選択されたアイデンティティ情報を読込むステップを含む。読取りオペレーションは選択されたアイデンティティ情報を位置特定し、自己アイデンティティ情報ストアから情報を検索する。制御は次いで生成オペレーション４１５に渡る。

【００５１】

生成オペレーション４１５は自己アイデンティティ情報ストアから選択され、読み取られた情報を含むアイデンティティ情報文書を生成するステップを含む。生成オペレーション４１５は選択された情報からアイデンティティ情報文書を構築する。以下で説明するように、アイデンティティ情報文書はＸＭＬファイルを含むことができる。あるいは、アイデンティティ情報文書は様々な媒体上で異種システムに情報を転送するのに適した形態とすることができる。加えて、アイデンティティ情報文書は、場合によっては証明書にカプセル化された１つまたは複数のパブリックキーなどの少なくとも第１のキーを含む。アイ

デンティティ情報文書は、アイデンティティ情報文書に含まれるパブリックキーの１つと対になったプライベートキーなどの第２のキーを使用してデジタルシグナチャでサインすることができる。制御は次いで送信オペレーション４２０に渡る。

【００５２】

送信オペレーション４２０はチャネルを介してアイデンティティ情報文書を受信システムに送信するステップを含む。送信オペレーションはアイデンティティ情報文書を受信システムに出力信号で伝送し、通信または送信する。上述のように、チャネルは安全であることもあり、安全でないこともある。アイデンティティ情報文書を送信することができるチャネルの例としては、限定はしないが、電子メール、インスタントメッセージング、ビーミング、専用回線などがある。

【００５３】

図５は本発明の一実施形態によるアイデンティティ情報を受信するステップを示すフローチャートである。この例において、処理は受信オペレーション５０５で始まる。受信オペレーション５０５は上述のようなチャネルからアイデンティティ情報文書を受信するステップを含む。受信オペレーションは着信信号からのアイデンティティ情報文書を回復するために開始システムからの着信信号を処理する。制御は次いで問合せオペレーション５１０に渡る。

【００５４】

問合せオペレーション５１０はアイデンティティ情報文書で受信されたアイデンティティ情報が信頼できるかどうかを判定するステップを含む。問合せオペレーションは情報をどのように受信したかに関係するいくつかの状況に基づいてアイデンティティ情報の認証をテストする。ある場合には、真正性の判定は、情報を受諾すべきか拒否すべきかに関してＧＵＩを介してユーザに問い合わせるステップに単に依拠することがある。他の場合には、ヒューリスティックスのアルゴリズムを使用して、情報を転送するために使用される媒体、情報の機密性、および任意の数の他の基準に基づいて自動的に判定を行うことができる。情報が信頼できると判定された場合、制御は保存オペレーション５３０に渡り、アイデンティティ情報文書で受信されたアイデンティティ情報が認識済みアイデンティティ情報ストアに保存される。保存オペレーションがアイデンティティ情報を認識済みアイデンティティ情報ストアに書き込んだ後、オペレーションフローは主プログラムフローに戻る。

【００５５】

問合せオペレーション５１０において、アイデンティティ情報が信頼できると判定されなかった場合、制御は問合せオペレーション５１５に渡る。問合せ検証オペレーション５１５はアイデンティティ情報文書を検証しようと試みたかどうかを判定するステップを含む。問合せ検証オペレーションは検証プロセスを行うべきかどうかを決定することである。この判定はデフォルトで自動的に行われるか、ＧＵＩを介したユーザ入力に基づくか、またはユーザよってプログラム可能ないくつかの他の基準に基づくことができる。問合せオペレーション５１５において、アイデンティティ情報を検証しないという判定がなされた場合、それ以上の処理は行われず、オペレーションフローは主プログラムフローに戻る。しかしながら、アイデンティティ情報の検証を試みるという判定がなされた場合、制御は検索オペレーション５２０に渡る。

【００５６】

ＩＲＮ検索オペレーション５２０は開始システムまたは発信者からＩＲＮを検索するステップを含む。検索オペレーションは代替チャネルによって開始システムまたは発信者に連絡するよう受信システムにコマンドを出すか、または受信システムのユーザにプロンプトを出す。たとえば、ユーザは電話で発信者を呼び出すか、またはＩＭ（インスタントメッセージング）を送信し、発信者にそのＩＲＮを確認するよう尋ねることもある。

【００５７】

ＩＲＮ生成オペレーション５２３はアイデンティティ情報文書で受信されたパブリックキーに基づいて受信局でＩＲＮを再生成する。ＩＲＮでＩＲＮを計算するために、生成オ

ペレーション５２３はアイデンティティ情報文書で送信されたパブリックキーをハッシュする。あるいは、発信者のディスプレイ名（図６）をパブリックキーと組み合わせ、次いでその組合せをハッシュすることができる。次いでハッシュオペレーションの結果をマスキングアルゴリズムにかけて、‘Ａ’を英数字を示すとしてＡＡＡ－ＡＡ－ＡＡ－ＡＡＡの形態の英数字シグナチャを生成する。ＩＲＮ生成オペレーション５２３によって計算されたＩＲＮは７３２－ＡＢ－５Ｈ－ＸＶＱのように見えることもある。次いで２つのＩＲＮをＩＲＮテストオペレーション５２５によって比較する。

【００５８】

ＩＲＮテストオペレーション５２５はＩＲＮが正しいかどうかを判定するステップを含む。ＩＲＮテストオペレーション５２５は受信局で生成された計算済みＩＲＮを開始システムから検索された検索済みＩＲＮと比較する。中心人物の攻撃が送信者を欺くためにパブリックキー情報を代用することによって受信者によって受信されたアイデンティティ情報をいたずらした場合、計算済みＩＲＮは発信者または開始システム、すなわち真の送信者からの検索済みＩＲＮと一致しないであろう。

【００５９】

ＩＲＮが正しいと判断された場合、制御は保存オペレーション５３０に渡る。保存オペレーション５３０は認識済みアイデンティティ情報ストアのアイデンティティ情報文書で受信されたアイデンティティ情報を保存または記憶する。オペレーションフローは次いで受信システムの主制御プログラムに戻る。

【００６０】

あるいは、拒否されたアイデンティティ情報さえも認識済みアイデンティティ情報ストアに入れることができる。たとえば、アイデンティティ情報の所与のセットが拒否されたとしても、それは将来の参照のために記憶し、信頼できない物としてマーキングすることができる。この認識済みであるが信頼できないアイデンティティ情報は、認識済みアイデンティティ情報ストアの特別の部分に記憶することによって、あるいは何らかの様式でタグ付けまたはフラグ付けすることなどによってマーキングすることができる。そのような情報は信頼できないアイデンティティ情報の将来の識別において有用であることがある。

【００６１】

図６は本発明の一実施形態によるアイデンティティ情報文書のための例示的なフォーマットを示す。データ構造として、アイデンティティ情報文書６００は、キーに結合され、埋め込まれた使用法ポリシーによって支配されるアイデンティティ主張および他の属性／特性主張の集合である。ＸＭＬはアイデンティティ情報のための符号化言語として使用されることになる。しかしながら、他のフォーマットも等しく適切と考えられる。アイデンティティ情報文書６００の要素はまた、アイデンティティ情報文書６００がその機密性が維持されなければならない機密情報を含んでいる場合、場合によっては暗号化することができる。

【００６２】

アイデンティティ情報文書６００内のデータは２つのカテゴリに分けることができる。これらのカテゴリは論理構成要素６０１のセットおよび属性タグ６０８のセットを含む。アイデンティティ情報文書は６つの当事者論理構成要素、すなわち、１）アイデンティティ情報主題識別子６０２、２）主題の１つまたは複数のアイデンティティ主張６０３、３）主題のディスプレイ名および０または複数の選択的に開示された属性６０４、４）任意の容認できるフォーマット（たとえばＸ５０９ｖ３証明書のパブリックキー）で包囲される主題のための１つまたは複数のキー６０５、５）主題のプライバシー要件を表わす使用法ポリシー６０６、６）データの完全性を保護し、アイデンティティ情報更新の場合に送信者を認証するアイデンティティ情報の全内容にわたるデジタルシグナチャ６０７を有する。これら６つの論理構成要素６０１の各々について以下で述べる。

【００６３】

主題識別子６０２は、名前識別子として表わされるそのアイデンティティ主張の１つによって識別されるエンティティとしてアイデンティティ情報の主題を表わす。アイデンテ

ィティ情報主題の好ましい名前識別子またはアイデンティティ主張は、主題タイプが人間である場合、電子メールアドレスである。

【００６４】

アイデンティティ主張６０３は、アイデンティティ情報文書の主題を一意に識別する構造化情報を含む。アイデンティティ主張は、所与の時間期間中に単一の当事者を識別するために所与のタイプの当局によって割り当てられる値である。アイデンティティ情報文書におけるアイデンティティ主張は様々な名前空間における当事者を識別し、ディスプレイ名および物理メーリングアドレスなどの他の開示情報は、当事者が識別された後に当事者に対してさらなるコンテキストを供給する。

【００６５】

ディスプレイ名６０４は探索およびオペレーション中に受信者のシステムで使用することができる。しかしながら、それは一意である必要はない。ディスプレイ名および他の開示情報（物理メーリングアドレスなど）は、当事者がアイデンティティ情報の主題仕様を介して識別された後に当事者に対して追加のコンテキストを供給する。開示情報は主題に関する説明的情報からなる。これは特性のセットとして表わされる。いくつかの特性は標準化することができ、拡張機構があることがある。

【００６６】

キー６０５は、場合によっては証明書フォーマット（たとえばＸ５０９ｖ３証明書）内にカプセル化される１つまたは複数のキーを含む。キー６０５はパブリックキーとすることができ、アイデンティティ情報の主題のための認識情報としてアイデンティティ情報に含めることができる。証明書を使用する場合、自己サインするか、または証明書当局によって発行することができる。

【００６７】

使用法ポリシー６０６は、アイデンティティ情報の内容を置くことができる使用者に関して発信者の命令を受信者に伝達する。たとえば、それはアイデンティティ情報の内容を他人に漏らすべきではないことを示すことがある。認識済みアイデンティティ情報ストアは当事者を規定する情報の残部とともに使用法ポリシーを記憶し、ユーザが、たとえば、共有することを意図しない当事者をコピーしようと試みた場合、システムは発信者の意図を示す警告をユーザに対して表示することになる。

【００６８】

デジタルシグナチャ６０７はアイデンティティ情報文書内にシグナチャデータを提供する。ＸＭＬシグナチャは、シグナチャを文書に関係させる３つの方法、すなわちエンベロープ化、エンベロープ済み、および消去を有する。本発明の一実施形態によれば、アイデンティティ情報文書は、アイデンティティ情報内容をサインする場合にＸＭＬエンベロープ済みシグナチャを使用する。

【００６９】

アイデンティティ情報文書６００は、１）アイデンティティ情報ＩＤ６０９、２）大バージョン６１０、３）小バージョン６１１、４）主題タイプ６１２、５）情報タイプ６１３、および６）発行インスタント６１４を含む、６つの属性タグ６０８を持つことができる。これらの属性タグ６０８の各々について以下で述べる。

【００７０】

アイデンティティ情報ＩＤ６０９はアイデンティティ情報文書の識別子である。それはシグナチャなどの文書の他の部分からアイデンティティ情報文書を参照することができる識別子を提供する。

【００７１】

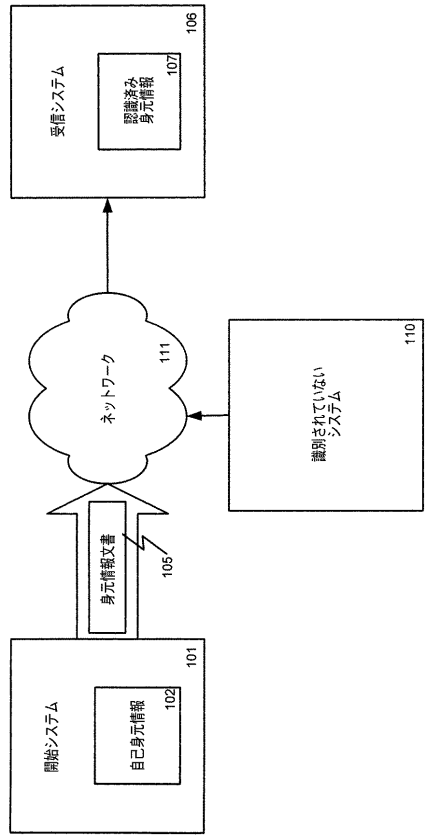
大バージョン６１０はこのアイデンティティ情報文書の大バージョン番号である。小バージョン６１１はこのアイデンティティ情報文書の小バージョン番号である。

【００７２】

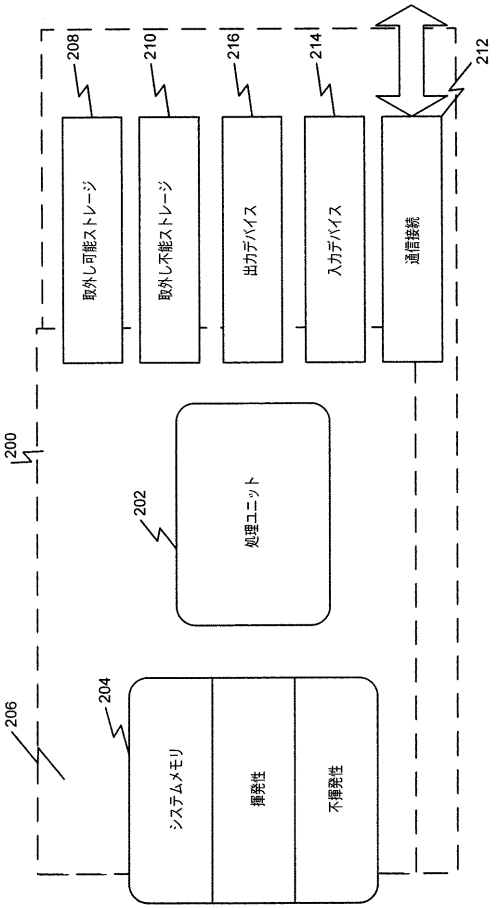
主題タイプ６１２は、このアイデンティティ情報文書の主題である当事者のタイプである。人間、コンピュータ、組織など、様々なタイプの当事者がありうる。

【００７３】
情報タイプ６１３はこのアイデンティティ情報のタイプである。たとえば、新しい当事者を生成するために「新しい」アイデンティティ情報を認識済みアイデンティティ情報ストアにインポートすることができ、また「更新」アイデンティティ情報を使用して、より最近の変更をもつ既存の当事者を改善することができる。
【００７４】
発行インスタント属性６１４は、アイデンティティ情報が発行または生成された場合にＵＴＣで表わされる時間インスタントである。更新アイデンティティ情報上のこのタイムスタンプは、アイデンティティ情報の主題の既存の表現が時期外れであるかより新しいかを判定するために使用することができる。
【００７５】
本発明についてコンピュータ構造フィーチャ、方法論的行為に固有の言語でコンピュータ読取り可能媒体によって説明したが、添付の特許請求の範囲で規定された本発明は必ずしも記載されている特定の構造、行為または媒体に限定されないことを理解されたい。一例として、識別情報を符号化するためにＸＭＬ以外の異なるフォーマットを使用することができる。したがって、特定の構造フィーチャ、行為および媒体は特許請求の範囲に記載の発明を実施する例示的な実施形態として開示されている。
【００７６】
上述の様々な実施形態は例示のために提供した物にすぎず、本発明を限定するものと解釈すべきではない。当業者は本明細書に例示および説明した例実施形態および適用例に従うことなく、また添付の特許請求の範囲に記載の本発明の真の趣旨および範囲から逸脱することなく、本発明に対してなすことができる様々な改変および変更を容易に認識するであろう。
【図面の簡単な説明】
【００７７】
【図１】本発明の一実施形態によるアイデンティティ認識のためのシステムを概念レベルで示す図である。
【図２】本発明の実施形態を実施することができる適切なコンピューティングシステム環境の例を示す図である。
【図３】本発明の一実施形態によるアイデンティティ認識のための例示的なソフトウェア構成要素を示す図である。
【図４】本発明の一実施形態によるアイデンティティ情報の交換を開始するステップを示すフローチャートである。
【図５】本発明の一実施形態によるアイデンティティ情報を受信するステップを示すフローチャートである。
【図６】本発明の一実施形態によるアイデンティティ情報文書のための例示的なフォーマットを示す図である。

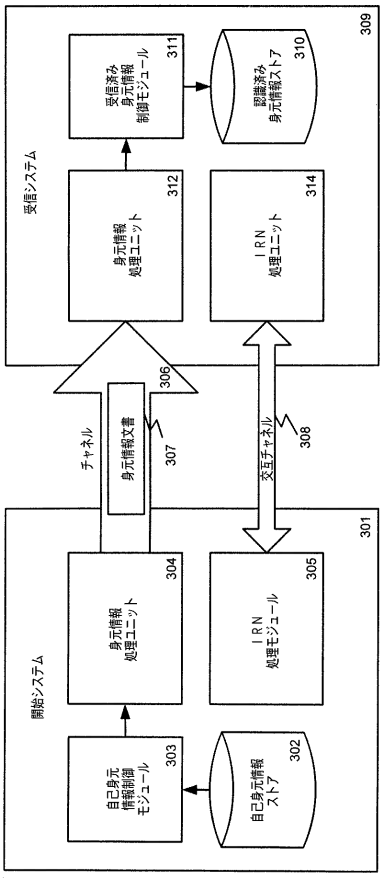
【図１】


受信システム
106
既識別済み身元情報
107
ネットワーク
111
識別されていないシステム
110
身元情報文書
105
開始システム
101
自己身元情報
102

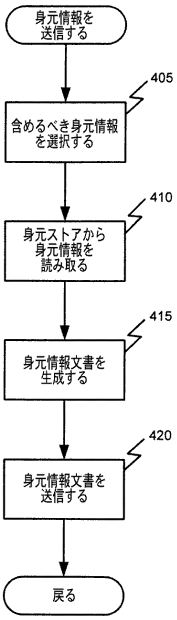
【図２】


208
210
216
214
212
取外し可能ストレージ
取外し不能ストレージ
出力デバイス
入力デバイス
通信接続
200
202
処理ユニット
206
204
システムメモリ
揮発性
不揮発性

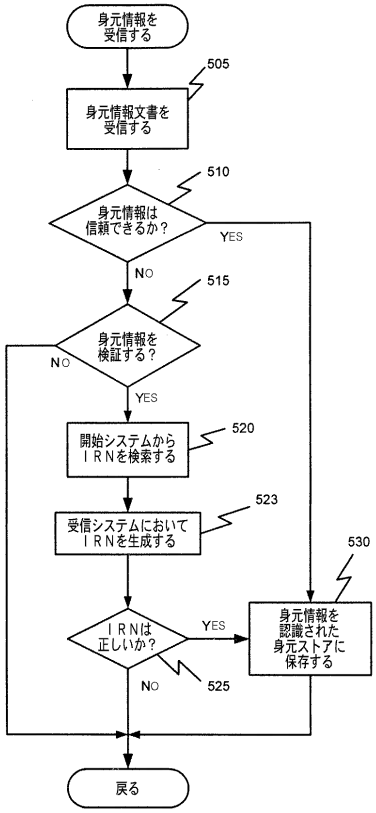
【図３】


309
受信システム
受信済み身元情報制御モジュール
311
既識別済み身元情報ストア
310
身元情報処理ユニット
312
IRN処理ユニット
314
306
チャネル
身元情報文書
307
交互チャネル
308
301
開始システム
身元情報処理ユニット
304
IRN処理モジュール
305
自己身元情報制御モジュール
303
自己身元情報ストア
302

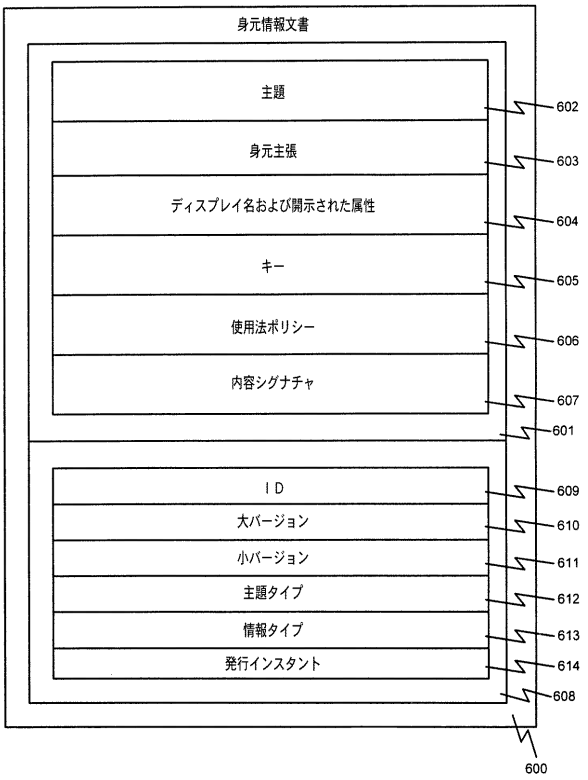
【図４】


身元情報を送信する
405
含めるべき身元情報を選択する
410
身元ストアから身元情報を読み取る
415
身元情報文書を生成する
420
身元情報文書を送信する
戻る

【図５】


身元情報を受信する
505
身元情報文書を受信する
510
身元情報は信頼できるか？
YES
NO
515
身元情報を検証する？
NO
YES
520
開始システムからＩＲＮを検索する
523
受信システムにおいてＩＲＮを生成する
530
ＩＲＮは正しいか？
YES
NO
525
身元情報を認識された身元ストアに保存する
戻る

【図６】


身元情報文書
主題
602
身元主張
603
ディスプレイ名および開示された属性
604
キー
605
使用法ポリシー
606
内容シグナチャ
607
601
ＩＤ
609
大バージョン
610
小バージョン
611
主題タイプ
612
情報タイプ
613
発行インスタント
614
608
600

フロントページの続き

(72)発明者　キム　キャメロン
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　コーポレーション内
(72)発明者　アラン　ナンダ
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　コーポレーション内
(72)発明者　ドナルド　ジェイ．　アシェル
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　コーポレーション内
(72)発明者　マーリ　サタゴパン
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　コーポレーション内
(72)発明者　スチュアート　クワン
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　コーポレーション内
(72)発明者　コリン　ブレイス
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　コーポレーション内
(72)発明者　ウォルター　スミス
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　コーポレーション内
(72)発明者　メリッサ　ダン
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　コーポレーション内

審査官　和田　財太

(56)参考文献　国際公開第０３／０３８５５７（WO，Ａ２）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/20
G06Q　10/00-50/00
G09C　1/00