(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2009-534940
(P2009-534940A)
(43)公表日　平成21年9月24日(2009.9.24)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5B089
G06F 13/00	(2006.01)	G06F	13/00	351A	5J104

審査請求 未請求　予備審査請求 未請求　（全 18 頁）

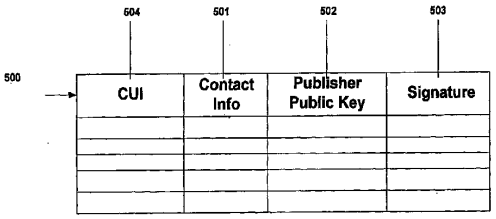
(21)出願番号　特願2009-506645 (P2009-506645)
(86)(22)出願日　平成19年4月23日 (2007.4.23)
(85)翻訳文提出日　平成20年11月26日 (2008.11.26)
(86)国際出願番号　PCT/US2007/010092
(87)国際公開番号　WO2007/124180
(87)国際公開日　平成19年11月1日 (2007.11.1)
(31)優先権主張番号　11/408,894
(32)優先日　平成18年4月21日 (2006.4.21)
(33)優先権主張国　米国 (US)

(71)出願人　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　100140109
弁理士　小野　新次郎
(74)代理人　100089705
弁理士　社本　一夫
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100080137
弁理士　千葉　昭男
(74)代理人　100096013
弁理士　富田　博行

最終頁に続く

(54)【発明の名称】ピアツーピアコンタクト情報交換

(57)【要約】
【解決手段】
本システムは、公的に入手可能なインデックスストア内に、認証されたコンタクト情報を発行可能であって、コンタクト情報をリトリーブし、それを検証できる。本発明の方法及びシステムは、クライアントベースであって、サーバを任意とする発行方法を提供できる。公的に入手可能なインデックスストアは、ピアツーピアネットワークにおいて使用される分散ハッシュテーブルであり得る。本システムは、サーバが有効であり得ないか又はサーバの信用が最小限であり得る別のセキュアなディレクトリサービスアプリケーションにおいて使用され得る。
【選択図】図５



【特許請求の範囲】
【請求項１】
セキュアな発行システムのために、公的に入手可能なインデックスストアを使用する方法であって、
公開鍵に対して統計的に固有な暗号的に固有な識別子を提供するステップと、
発行元の秘密鍵を用いてメッセージに署名するステップであって、前記メッセージが、前記発行元公開鍵を含むものと、
前記メッセージを公的に入手可能なインデックスストアに挿入するステップであって、前記メッセージが、前記暗号的に固有な識別子によってインデックス付けられるものと、
前記暗号的に固有な識別子に基づいてエントリーをリトリーブするステップと、
前記暗号的に固有な識別子が、前記公開鍵に関連するか決定するステップと、
前記メッセージが、前記公開鍵に対応する秘密鍵によって署名されているか決定するステップと、を含む方法。
【請求項２】
更に、前記メッセージが、期待された形式及び構文を有するか決定するステップ、を含む請求項１記載の方法。
【請求項３】
前記インデックスストアが、分散ハッシュテーブル及びディレクトリサーバのうちの１つであること、を特徴とする請求項１記載の方法。
【請求項４】
前記暗号的に固有な識別子が、ハッシュ関数を使用して前記ユーザの公開鍵から生成されること、を特徴とする請求項１記載の方法。
【請求項５】
更に、前記暗号的に固有な識別子が前記公開鍵に関連することと、前記メッセージが前記公開鍵に対応する秘密鍵によって署名されていることと、前記メッセージが期待された形式及び構文を有することと、を決定したとき、前記リトリーブを実行する計算機の前記公開鍵の使用を可能にするステップ、を含む請求項１記載の方法。
【請求項６】
前記メッセージが更に、暗号強度に比例する期間パラメタを含むこと、を特徴とする請求項１記載の方法。
【請求項７】
更に、期間パラメタによって示される期間が経過していないことと、暗号的に固有な識別子が前記公開鍵に関連することと、前記メッセージが前記公開鍵に対応する秘密鍵によって署名され、前記メッセージが期待された形式及び構文を有することと、を決定したとき、前記リトリーブするステップを実行する計算機の前記公開鍵の使用を可能にするステップ、を含む請求項６記載の方法。
【請求項８】
前記暗号的に固有な識別子が、グループ公開鍵を含むこと、を特徴とする請求項１記載の方法。
【請求項９】
前記暗号的に固有な識別子が、少なくとも第１のユーザの暗号的に固有な識別子及び第２のユーザの暗号的に固有な識別子から形成されること、を特徴とする請求項１記載の方法。
【請求項１０】
ピアツーピアネットワークを形成する複数のピアノードと、
前記ピアツーピアネットワークの分散ハッシュテーブルと、
第１のピアノードの公開鍵に統計的に固有な暗号的に固有な識別子を生成し、前記公開鍵を含んでいて前記公開鍵に対応する秘密鍵によって署名されたメッセージを前記暗号的に固有な識別子によってインデックス付けられる前記分散ハッシュテーブルに挿入する、前記第１のピアノードと、

前記暗号的に固有な識別子に基づいて前記メッセージをリトリーブし、前記暗号的に固有な識別子が前記公開鍵に関連するか決定し、前記メッセージが前記公開鍵に対応する前記秘密鍵によって署名されているか決定し、前記メッセージが期待された形式及び構文を有するか決定する、第２のノードと、を含む計算機システム。

【請求項１１】

前記暗号的に固有な識別子が前記公開鍵に関連することと、前記署名が前記公開鍵に対応する前記秘密鍵によって署名されていることと、前記メッセージが期待された形式及び構文を有することとを決定したとき、前記第２のノードが、前記第１のノードと通信するために前記公開鍵を使用すること、を特徴とする請求項１０記載のシステム。

【請求項１２】

前記暗号的に固有な識別子が、前記第１のノードに関連する第１の暗号的に固有な識別子と前記第２のノードに関連する第２の暗号的に固有な識別子との組み合わせを含むこと、を特徴とする請求項１０記載のシステム。

【請求項１３】

前記メッセージが、前記第２のノードの公開鍵を使用し暗号化されていること、を特徴とする請求項１２記載のシステム。

【請求項１４】

前記メッセージが、期間パラメタを含み、該期間パラメタが、前記公開鍵と該公開鍵に対応する前記秘密鍵とを生成するために使用される暗号化アルゴリズムの強度に比例すること、を特徴とする請求項１０記載のシステム。

【請求項１５】

前記期間パラメタによって示される期間が経過していないことと、前記暗号的に固有な識別子が前記公開鍵に関連していることと、前記メッセージが前記公開鍵に対応する前記秘密鍵によって署名されていることと、前記メッセージが期待された形式及び構文を有することとを決定したとき、前記第２のノードが、前記メッセージを承認することを特徴とする請求項１４記載のシステム。

【請求項１６】

公開鍵から暗号的に固有な識別子を生成するステップと、

前記暗号的に固有な識別子に基づいてインデックスストアのエントリーをリトリーブするステップであって、前記エントリーが公開鍵に対応する秘密鍵によって、共に署名されているメッセージ及び前記公開鍵を含むものと、

前記暗号的に固有な識別子が、前記公開鍵に関連するか決定するステップと、

前記メッセージ及び公開鍵が、前記秘密鍵によって署名されているか決定するステップと、を含む動作を実行するための計算機実行可能命令を有する計算機可読媒体。

【請求項１７】

更に、前記メッセージが、期待された形式及び構文を有するか決定するステップ、を含む請求項１６記載の計算機可読媒体。

【請求項１８】

更に、前記メッセージの期間パラメタが経過したか決定するステップ、を含む請求項１６記載の計算機可読媒体。

【請求項１９】

前記期間パラメタによって示される期間が、前記公開及び秘密鍵を生成するために使用される暗号レベルに比例すること、を特徴とする請求項１８記載の計算機可読媒体。

【請求項２０】

前記暗号的に固有な識別子が、第１の暗号的に固有な識別子と第２の暗号的に固有な識別子とを結合することによって形成されることと、前記メッセージが、前記第２の暗号的に固有な識別子に関連する計算機の公開鍵を使用し暗号化されることと、を特徴とする請求項１６記載の計算機可読媒体。

【発明の詳細な説明】

【背景技術】

【０００１】
ディレクトリサービスは、通常ネットワークサーバを使用し提供され得る。ディレクトリサービスを利用するためにユーザは、サーバに接続することと、ディレクトリサービスにアクセスするためのユーザアカウントを有することを要求され得る。更にユーザは、データ完全性及びデータ認証を提供するためのサーバを信用する必要がある。ディレクトリサービスが、接続された実体のより小さなグループ、例えばアドホックネットワークに対して意図される場合、そのアドホックネットワーク用にディレクトリサーバを作成し、セットアップすることは、非効率であり得る。例えばアドホックネットワークは、通常、本質上一時的であり、短期間、少数のユーザのための専用サーバをセットアップすることは、管理者の時間、（いくつかのサーバが再割り当てされるか又は追加されなければならない）設備リソース容量、（ユーザがアカウント生成及びセットアップにかかわり得る）ユーザの時間に関して、非常に高価であり得る。加えてサーバベースシステムが普通であるが、ピアツーピアネットワークなどの、新しいサーバが不要なシステムは、通信を容易にするために専用サーバを要求しないので、アドホックネットワークを作成するためのより大きな柔軟性を提供できる。しかし、既存の暗号化プロセスを使用し、これらのアドホックネットワーク上でセキュア通信を可能にするために、サーバベースモデルに頼らない公開鍵の交換を容易にするためのディレクトリサービスが要求される。
【特許文献１】米国特許出願第１０／８８２０７９号
【発明の開示】
【課題を解決するための手段】
【０００２】
本システムは、公的に入手可能なインデックスストアに、認証されたコンタクト情報を発行できる。また本システムは、コンタクト情報をリトリーブし、それを検証する方法も提供できる。本発明の方法及びシステムは、サーバを任意とするクライアントベースであり得る。公的に入手可能なインデックスストアは、ピアツーピアネットワークにおいて使用される分散ハッシュテーブルであり得る。本システムは、サーバが有効であり得ないか又はサーバの信用が最小限であり得る別のセキュアなディレクトリサービスアプリケーションにおいて使用され得る。
【発明の効果】
【０００３】
一実施形態においては、本システムは、一般的なメッセージ発行システムとして使用され得る。別の実施形態においては、本システムは、意図する受信者だけによって、投稿されたレコードがリトリーブされ得、読まれ得る選択的な発行を提供するために使用され得る。
【発明を実施するための最良の形態】
【０００４】
以下の文章は、多くの異なる実施形態の詳細記述を説明しているが、記載の法的範囲が本開示の終わりに説明される請求項の語句によって定義されることが理解されよう。詳細な記述は、例示的に過ぎないと理解されるべきであって、あらゆる可能な実施形態を記述するのは不可能でないにしても非実用的なので、あらゆる可能な実施形態については記述しない。本明細書の出願日以降、最新技術又は開発技術のいずれかを使用した本発明の範囲内の多数の代替実施形態が実施され得る。
【０００５】
また、以下理解されるべきことは、用語が「本明細書に使用される用語’‘は、・・・を意味するために定義される」という文章か又は同様な文章を使用し、本明細書に明確に定義されていない場合、そのわかりやすさ又は普通の意味を越えて明白に又は意味によるいずれかによってその用語の意味を限定する意図は全くなく、（請求項の言語以外の）本明細書におけるいかなる項目のいかなる記述を基にした範囲内で限定されると解釈してはいけないことである。本明細書の終わりの請求項において、復唱されるいかなる用語も単一の意味を持つ一貫した方法で本明細書において参照されるという点は、読者を混乱させ

ないように明確にするだけのためになされるのであって、意味によるか又は別の単一のその意味に限定することによってその用語を請求する意図はない。請求項目がいかなる構造の詳説を伴わず、最終的に「手段」及び機能という語句の列挙による定義がされていない場合、いかなる請求項目範囲も米国特許法３５のセクション１１２の第６パラグラフの適用に基づいた解釈がされることを意図しない。

【０００６】

図１は、本発明群の方法及び装置のためのシステムを実施し得る最適な計算システム環境（１００）の一例を示す。計算システム環境（１００）は、最適な計算環境の一例に過ぎず、本発明の方法及び装置の使用又は機能性の範囲に関して、いかなる制限も提示することを意図しない。計算環境（１００）は、例示的な動作環境（１００）において示される任意の一コンポーネント又はコンポーネントの組み合わせに関していかなる依存性も要求も有しないものとして解釈されるべきである。

【０００７】

一連の請求の方法及び装置は、いくつもの別の汎用的又は特定用途の計算システム環境又は構成と共に作動する。請求の方法及び装置を用いて使用に適し得る周知の計算システム、環境及び／又は構成の例は、パーソナルコンピュータ、サーバコンピュータ、携帯用又はラップトップ装置、マルチプロセッサシステム、マイクロプロセッサベースシステム、セットトップボックス、プログラマブル家電、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、前述のシステム又は装置などのいくつかを含む分散計算環境を含むが、これらに限定されない。

【０００８】

一連の請求の方法及び装置は、計算機によって実行されるプログラムモジュールなどの一般的な計算機実行可能命令の文脈で記述され得る。一般に、プログラムモジュールは、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んでいて、特定のタスクを実行又は特定の抽象データ型を実現する。また本方法及び装置は、通信ネットワークを介し接続されるリモートプロセッシング装置によってタスクを実行する分散計算環境において実施され得る。分散計算環境においては、メモリ記憶装置を含むローカル及びリモート計算機記憶媒体双方においてプログラムモジュールが配置され得る。

【０００９】

図１を参照し、一連の請求の方法及び装置を実施するための例示的なシステムは、計算機（１１０）の形式の汎用計算装置を含む。計算機（１１０）のコンポーネントは、処理ユニット（１２０）、システムメモリ（１３０）及びシステムメモリを含む多様なシステムコンポーネントを処理ユニット（１２０）に接続するシステムバス（１２１）を含むが限定されない。システムバス（１２１）は、メモリバス又はメモリコントローラを含むいくつかの任意のタイプのバス構造、周辺機器用バス及び様々なバスアーキテクチャのうちいくつかを使用するローカルバスであり得る。制限ではなく例として、そのようなアーキテクチャは、業界標準アーキテクチャ（ＩＳＡ）バス、マイクロチャネルアーキテクチャ（ＭＣＡ）バス、拡張ＩＳＡ（ＥＩＳＡ）バス、ビデオ機器に関する標準化団体（ＶＥＳＡ）ローカルバス及びメザニンバスとして知られる周辺機器相互接続（ＰＣＩ）バスを含む。

【００１０】

計算機（１１０）は、一般に様々な計算機可読媒体を含む。計算機可読媒体は、計算機（１１０）によってアクセスされ得る使用可能ないくつかの媒体であり得、揮発性及び不揮発性双方の媒体及び取り外し可能及び取り外し不可能な双方の媒体を含む。制限ではなく例として、計算機可読媒体は、計算機記憶媒体及び通信媒体を含む。計算機記憶媒体は、計算機可読命令、データ構造、プログラムモジュール又は他のデータなどの情報の記憶に関する任意の方法又は技術にて実装される揮発性及び不揮発性双方の取り外し可能及び取り外し不可能な媒体を含む。計算機記憶媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ又は他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）又は他の光ディスク記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置又は他の

磁気記憶装置又は所望の情報をストアするために使用され得、計算機（１１０）によってアクセスされ得る他の任意の媒体を含むが、これらに限定されない。通信媒体は一般に、搬送波又は別の移送手段などの変調データ信号で計算機可読命令、データ構造、プログラムモジュール又は他のデータを具現化したものであって、任意の情報伝達媒体を含む。用語「変調データ信号」は、１つ以上の特徴の組を有する信号又は信号中の情報を符号化する方法によって変更された信号を意味する。通信媒体は、制限ではなく例として、有線ネットワーク又は直接有線接続のようなワイヤード媒体並びに音響、無線（ＲＦ）、赤外線及び他の無線媒体のようなワイヤレス媒体を含む。前述のいくつかの組み合わせもまた、計算機可読媒体の範囲内に含む必要がある。

【００１１】

システムメモリ（１３０）は、読み出し専用メモリ（ＲＯＭ）（１３１）及びランダムアクセスメモリ（ＲＡＭ）（１３２）などの揮発性及び／又は不揮発性メモリ形式の計算機記憶媒体を含む。基本入出力システム（ＢＩＯＳ）（１３３）は、起動の間などに計算機（１１０）のエレメントの間の情報送信を支援する基本ルーチンを含んでいて通常ＲＯＭ（１３１）にストアされる。ＲＡＭ（１３２）は通常、データ及び／又はプログラムモジュールを含んでいて、処理ユニット（１２０）によって、即時アクセス可能及び／又は現在作動している。制限ではなく例として、図１は、オペレーティングシステム（１３４）、アプリケーションプログラム（１３５）、他のプログラムモジュール（１３６）及びプログラムデータ（１３７）を示す。

【００１２】

また計算機（１１０）は、別の取り外し可能／取り外し不可能、揮発性／不揮発性の計算機記憶媒体も含み得る。例に過ぎないが、図１は、取り外し不可能、不揮発性磁気媒体から読み出すか又はそれに書き込むハードディスクドライブ（１４０）、取り外し可能、不揮発性磁気ディスク（１５２）から読み出すか又はそれに書き込む磁気ディスクドライブ（１５１）、ＣＤ－ＲＯＭ又は他の光媒体などの取り外し可能、不揮発性光ディスク（１５６）から読み出す又はそれに書き込む光ディスクドライブ（１５５）を示す。例示的な動作環境において使用され得る別の取り外し可能／取り外し不可能、揮発性／不揮発性計算機記憶媒体は、限定しないが、磁気テープカセット、フラッシュメモリカード、デジタル多用途ディスク、デジタルビデオテープ、半導体ＲＡＭ、半導体ＲＯＭ等を含む。ハードディスクドライブ（１４１）は通常、インタフェース（１４０）などの取り外し不可能メモリインタフェースを介し、システムバス（１２１）と接続され、磁気ディスクドライブ（１５１）及び光ディスクドライブ（１５５）は通常、インタフェース（１５０）などの取り外し可能メモリインタフェースによってシステムバス（１２１）と接続される。

【００１３】

前述の図１に例示されるドライブ及びそれらに関連する計算機記憶媒体は、計算機（１１０）に計算機可読命令、データ構造、プログラムモジュール及び他のデータの記憶装置を提供する。図１において、例えばハードディスクドライブ（１４１）は、オペレーティングシステム（１４４）、アプリケーションプログラム（１４５）、他のプログラムモジュール（１４６）及びプログラムデータ（１４７）をストアするように示される。これらのコンポーネントは、オペレーティングシステム（１３４）、アプリケーションプログラム（１３５）、他のプログラムモジュール（１３６）及びプログラムデータ（１３７）と同等か又は異なるどちらかであり得ることに留意されたい。オペレーティングシステム（１４４）、アプリケーションプログラム（１４５）、他のプログラムモジュール（１４６）及びプログラムデータ（１４７）は、異なる複製物であることを最小限に示すために本明細書においては所与の異なる番号を付与する。ユーザは、キーボード（１６２）などの入力装置及びマウス、トラックボール又はタッチパッドのような一般に呼ばれるポインティング装置（１６１）を介し、計算機（２０）にコマンド及び情報を入力できる。（図示されない）別の入力装置は、マイクロフォン、ジョイスティック、ゲームパッド、衛星放送受信アンテナ、スキャナ又はその他を含み得る。多くの場合、これら及び他の入力装置は、システムバスに接続されるユーザ入力インタフェース（１６０）を介し、処理ユニッ

ト（１２０）と接続されるが、パラレルポート、ゲームポート又はユニバーサルシリアルバス（ＵＳＢ）のような別のインタフェース及びバス構造によっても接続され得る。モニタ（１９１）又は別のタイプの表示装置もまた、ビデオインタフェース（１９０）などのインタフェースを介し、システムバス（１２１）に接続される。更にまた、モニタ、計算機は、スピーカ（１９７）及びプリンタ（１９６）などの他の周辺出力装置も含み得、これらは出力周辺インタフェース（１９０）介し接続され得る。

【００１４】

計算機（１１０）は、リモートコンピュータ（１８０）などの１つ以上のリモート計算機との論理的な接続を使用するネットワーク環境において作動し得る。リモートコンピュータ（１８０）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、ピア装置又は一般的な他のネットワークノードであり得、図１にはメモリ記憶装置（１８１）だけが例示されているが、通常、前述の計算機（１１０）に関連するエレメントの多数又はすべてを含む。図１に示される論理的な接続は、ローカルエリアネットワーク（ＬＡＮ）（１７１）及び広域ネットワーク（ＷＡＮ）（１７３）を含むが、別のネットワークもまた含み得る。そのようなネットワーク環境は、オフィス、企業全体の計算機ネットワーク、イントラネット及びインターネットにおいて一般的である。

【００１５】

計算機（１１０）は、ＬＡＮネットワーク環境において使用されるとき、ネットワークインターフェース又はアダプタ（１７０）を介し、ＬＡＮ（１７１）に接続される。計算機（１１０）は通常、ＷＡＮネットワーク環境において使用されるとき、インターネットなどのＷＡＮ（１７３）において通信を確立するためのモデム（１７２）又は別の手段を含む。内蔵又は外付けであり得るモデム（１７２）は、ユーザ入力インタフェース（１６０）又は適切な別の装置を介し、システムバス（１２１）に接続され得る。ネットワーク環境においては、計算機（１１０）又はその一部に関連して表示されるプログラムモジュールは、リモートのメモリ記憶装置にストアされ得る。制限ではなく例として、図１は、メモリ装置（１８１）に常駐するようなリモートアプリケーションプログラム（１８５）を示す。例示されたネットワーク接続は例示的であって、計算機の間の通信リンクを確立する他の手段が使用され得ることが十分理解されよう。

【００１６】

ピアツーピア（Ｐ２Ｐ）システムは、分散的な方法によって、例えばセントラルサーバの支援なしに相互通信するネットワークノードを使用する。ピアツーピアネットワークにおける各ノード（例えばアプリケーション又は装置）は、直接的な接続を介しネットワーク上の別のノードと通信可能か、又は、各ノードは、意図するノードに通信を中継するための１つ以上の仲介ノードを使用し間接的に通信可能である。

【００１７】

図２は、Ｐ２Ｐシステム（２００）の上位レベルの図を例示する。本システム（２００）は、ピア実体（２０２～２１２）の集合を含む。ピア実体（２０２～２１２）は、ネットワーク又はネットワーク（複数）の組み合わせを介し共に接続されるパーソナルコンピュータ装置であり得る。図２は、ピア実体それぞれ（２０２～２１２）が、他のピア実体すべて（２０２～２１２）に接続される一例を例示する。他の場合においては、１つ以上のピア実体（２０２～２１２）は、１つ以上の仲介の参加者（２０２～２１２）を介し他のピア実体（２０２～２１２）に接続され得る。しかし、ピアツーピアネットワーク上でセキュアな通信を提供するために、ピアノードの間のセキュアな接続が、最初に確立される必要があり得る。

【００１８】

接続セキュリティは、本技術分野において一般的に知られ得るような対称鍵暗号化プロセスを基本とする。しかし、この暗号セキュリティを実施するために、ピア実体は、セキュアな接続を最初に確立可能にする証明書及び／又は公開鍵をまず交換することを必要とし得る。図３に例示されているようないくつかの既存システムにおいて、この交換は、セントラルディレクトリサーバ（３００）を使用し容易にされ得、そこではユーザ（３０１

）、（３０２）、（３０３）が、自分の証明書（３０４）、（３０５）、（３０６）及び／又は公開鍵をディレクトリサーバ（３００）上に投稿可能である。ディレクトリサービス（３０７）は、鍵（３０９）として使用されるユーザ名又は別の識別子の下でインデックス付けられた証明書及び／又は公開鍵のレコード（３０８）を含むデータベーステーブルであり得る。ディレクトリサーバ（３００）に接続可能であって、ディレクトリサービス（３０７）へのアクセスを認められたユーザは、対象ユーザの識別子を使用し対象ユーザを検索し、対象ユーザの対応する公開鍵を取得できる。このアプローチは、サーバ（３００）への接続性と、ディレクトリサーバ（３００）を用いた明示的な署名による登録と、ディレクトリサーバ（３００）の信用と、を要求する。更に誰かがサーバなどのホスティング費用を負う必要がある。ユーザ（３０３）がリモートから接続しているとき、インターネット接続性（３１０）が更に要求され得る。サーバ登録プロセスは、ディレクトリサーバ（３００）の信用を促すために使用されるユーザアカウントに関連する。例えば任意のユーザがサーバ（３００）にアクセス可能な場合、特に公開鍵などのセキュリティ情報が投稿され、交換される場合、サーバ（３００）は、より危険にさらされ、影響されやすいと見なされ得る。更に、アドホックであって一時的なネットワークのためのディレクトリサーバを作成することは、これらのネットワークの一時的な性質と、ディレクトリサーバをセットアップする際の苦労と、のために非実用的であり得る。アドホックなピアツーピアネットワークのための可能な次善策は、電子メールを介するか又は証明書／公開鍵を含むディスケットを対象メンバーに物理的に送信又は郵送するような非ネットワークプロセスを介し公開鍵を交換することであり得る。これによって、ピア実体はサーバに依存しないセキュアなリンクを確立できる。しかし、これは厄介で間違いが発生し得る。

【００１９】

本発明のサーバに依存しないインデックスプロセスの一実施形態は、図４に例示される分散ハッシュテーブル（ＤＨＴ）（４００）などのサーバが不要なインデックスストアを使用し得る。この分散ハッシュテーブル（４００）は、ピアツーピアネットワーク（４０５）を形成するピア実体（４０１～４０４）のグループに渡って保持され得る。分散ハッシュテーブルにおけるエントリーは、例えばハッシュ関数を使用し、論理的に分割又は分類され得る。ハッシュ関数は、いくつかの組織化方法によってレコードを共に凝集でき、その結果、リトリーブをより効率的にする。ＤＨＴは２つの主な特性：１）複数のノード（例えばノード（４０１～４０４））に渡るテーブル（例えばテーブル（４００））の配布及び２）レコードを発行しリトリーブするための方法を提供する（図示されない）ルーティング機構を有し得る。ルーティング機構及び配布は、Chord、PNRP、Pastry、Tapestryなどのようなオーバレイプロトコルによって管理され得る。ＤＨＴは、本発明の一実施形態によるインデックスストアを提供するために使用され得るが、ここでは、ピア実体のグループによって容易にアクセスされ得る任意のインデックスストアが、サーバベースの複数のインデックスを含んで使用され得ることを強調する。サーバベースの複数のインデックスの場合、本発明システムは、セキュアでないインデックスストアに要求されるレベルのセキュリティを提供できるので、本発明システムは、サーバ単体から要求される信用レベルを低減できる。

【００２０】

本発明のサーバに依存しないインデックスプロセスの一実施形態は、図５に例示されるような特定のレコード形式を使用し得る。図５は、発行元がコンタクト情報（５０１）、発行元の公開鍵（５０２）及び発行元の秘密鍵を使用したコンタクト情報の署名（５０３）を含むレコード（５００）をインデックスストアに投稿できることを例示する。代替として署名は、コンタクト情報と公開鍵との組み合わせに関するものがあり得る。このレコードは、レコード鍵（５０４）によってインデックス付けされ得る。一実施形態においては、レコードのレコード鍵（５０４）は、暗号的に固有な識別子（ＣＵＩ）であり得る。ＣＵＩは、２つの主な特性を有し得る。第１にＣＵＩは、統計的に特有であり得、第２にＣＵＩは、発行元公開鍵（５０２）などの特定ユーザの公開鍵に対応できる。一般的なデータベースインデックススキームと同様に、レコード鍵は、実体エントリーの複製を防ぐ

ために固有であることを必要とする。従ってＣＵＩは、それが特定の状況又はアプリケーションに対し固有である高い可能性があるように生成されるものの１つであり得る。例えば数人だけのメンバーのピアグループにおいて、暗号的に固有な識別子が同一の会員公開鍵から生成され得る可能性がそのグループの規模にしては起こりそうもない場合、ＣＵＩは統計的に固有であり得る。

【００２１】

ＣＵＩは、公開鍵からハッシュ又は暗号化アルゴリズムなどのアルゴリズムを使用し生成され得る。ＣＵＩは、アルゴリズムを使用してその公開鍵と対応するか又は一致することを検証され得る。一実施形態においては、ＣＵＩは、「コールサイン（Callsigns）」と題する米国出願特許番号１０／８８２０７９に記載されたＰ２Ｐシステムにおいて使用されるピア名などのより短くユーザ管理がより可能な形式によって、公開鍵などのより長いユーザ識別子を表すために使用され得る。

【００２２】

図５のレコードは、図４のＤＨＴ（４００）などのインデックスストアにコンタクト情報を発行するために使用され得る。ＣＵＩ鍵（５０４）は、各レコード（５００）を検索し、コンタクト情報（５０１）及び公開鍵（５０２）をリトリーブするために使用され得る。この実施形態においては、発行済み情報は公的であり得、すなわち発行済み情報は、署名以外暗号化されない。しかし後述の別の実施形態は、発行済みの情報の一部を暗号化し得る。またこの実施形態は公開鍵（５０２）の交換を容易にするためにレコード（５００）を使用することを例示するが、ここで固有のメッセージ発行が使用され得る任意のアプリケーションにおいて、本システムが使用され得ることを強調する。コンタクト情報（５０１）の代わりに例えば、任意のメッセージがユーザＣＵＩ（５０４）に対して投稿され得る。

【００２３】

図６は、本発明の実施形態による一般的な発行プロセスを例示する。ＣＵＩは、ハッシュ関数などのアルゴリズムを使用し所与のユーザの公開鍵（６０１）に対して生成され得る。ここで使用され得るアルゴリズムは何であれＣＵＩは、それを生成するために使用される公開鍵に対応することを検証され得ること、に留意することが重要である。コンタクト情報又は他のメッセージデータ及び発行元の公開鍵のレコードが構築され（６０２）、コンタクト情報及び／又は発行元の公開鍵が、（公開鍵に対応し得る）発行元の秘密鍵によって署名され得る（６０３）。コンタクト情報、公開鍵及び署名を含むレコードが、公的に入手可能なインデックスに挿入される（６０４）。レコードは、発行元公開鍵に対応するＣＵＩによってインデックス付けられ得る。

【００２４】

図７は、本発明の実施形態によるリトリーブプロセスを例示する。第２のピアとの接続を所望するユーザは、第２のピアのＣＵＩを取得できる（７０１）。ＣＵＩは、電子メール又は（例えば普通郵便、口頭でのやりとり、名刺などの）非ネットワークプロセスのいずれかを介し帯域外から取得され得る。ＣＵＩは、インデックスストアのＣＵＩにマップされたレコードを検索するために使用され得る（７０２）。前述のようにレコードは、鍵、いくつかのメッセージ情報（コンタクト情報）及び署名を含み得る。

【００２５】

次にユーザは、ＣＵＩに基づくレコードをリトリーブするためにインデックスストアに質問できる（７０３）。ＣＵＩが一旦リトリーブされるとＣＵＩは、それらが相互に対応するか確認するためにレコードに含まれる公開鍵を使用し検証され得る（７０４）。このプロセスのブロックは、レコードがＣＵＩに対応することを検証するために使用され得る。ＣＵＩは、様々な方法によって公開鍵に対し統計的に固有に生成され得る。一実施形態においては、ピア通信システムは、例えば広く認められたハッシュ関数を使用し、一般的なマッピングプロセスを事前準備し得る。この初期の検証プロセスは、レコードが所与のＣＵＩに実際に対応し得ることを確認することを支援する。

【００２６】

ＣＵＩが適切にマッピングする場合、レコードの署名は、発行元の対応する秘密鍵によって署名が署名されているか決定するために使用され得る（７０５）。これによって発行元が暗号化のために使用された公開鍵に対応する秘密鍵を所有するとみなされ得るので、メッセージが発行元から発せられたという証拠を提供することによってメッセージを認証できる。

【００２７】

レコード／メッセージが適切に署名されている場合、メッセージの形式及び／又は構文チェックが、レコードのコンタクト情報において実行され得る（７０６）。これは、例えばメッセージが署名に一致させるように不正侵入されなかったことを確認するために使用され得る。暗号化された署名に一致させるように不正侵入されたメッセージを提供することは、統計的に困難であり得るが、不可能でないかもしれない。しかし不正侵入することは、意図された又は期待された形式に従わないメッセージをもたらし得る。こうしてメッセージの第１のチェックは、メッセージ形式が期待された形式に従うか決定するためになされ得る。例えばコンタクト情報が通信される所においては、コンタクト情報は１０文字形式を必要とし得る。レコード形式がこの１０文字形式を提供しない場合、何者か又は何かがそのメッセージを改ざんした可能性がある（７１１）。

【００２８】

代替として又は更に、メッセージのセマンティクスがチェックされ得る。例えばコンタクト情報は、オプションリストとそれらのオプションの間の特定の関係とに限定され得る。したがって、本形式が２つのエントリーを要求し、第１のエントリーは、第２のエントリー（意味）に関連し、それらがこの期待された形式に一致しない場合、何者か又は何かがメッセージを改ざんした可能性がある（７１１）。

【００２９】

検証プロセスすべて（７０４）、（７０５）、（７０６）が首尾よく完了した場合、そのレコードは認証され得（７０７）、次に使用され得、例えば公開鍵は、通信リンクを確立するために使用され得る。検証ステップ（７０４）、（７０５）、（７０６）のいずれかが失敗した場合、何者か又は何かがメッセージを改ざんした可能性がある（７１１）。公開鍵交換システムの場合は、接続が拒否される。

【００３０】

図８に図示される別の実施形態においては、期間パラメタ（８０１）が、レコード（８００）に含まれ得る。この期間パラメタ（８０１）は、記載の認証プロセスにおいて使用される暗号レベルに対応し得る。例えば、暗号化レベルは、本発明システムにおいて使用される公開鍵／秘密鍵の組を生成するために使用される暗号強度に相当し得る。暗号強度が高い場合、期間は長期であり得、逆もまた真である。期間パラメタ（８０１）は、レコードに対する有効期間を示し得る。こうして図９に例示されるように期間パラメタ（８０１）は、リトリーブプロセスにおいて使用され得る。図９は、ブロック（９０９）を追加した図７の同一のプロセスを例示していて、期間パラメタ（８０１）によって示される期間（９０１）は、期間が経過したか決定するためにチェックされる。期間パラメタ（８０１）が経過した場合、レコードは信用できなくなり得る（９１１）。そうでない場合、レコードは有効であり得る（９０７）。

【００３１】

図１０～１２は別の実施形態を例示し、そこでは第１のユーザによって、第２の対象ユーザだけがリトリーブできるデータを発行できる選択的な発行が使用される。この選択的な発行の実施形態においては、図１０に例示されるようにレコード（１００１）が使用され得る。レコード（１００１）は、２つのＣＵＩ（１００３）、（１００４）の組み合わせから形成される鍵（１００２）を含み得る。第１のＣＵＩ（１００３）は、第１のユーザと関連し得、第２のＣＵＩ（１００４）は、第２のユーザと関連し得る。組み合わせは、第１のＣＵＩに第２のＣＵＩを単純に追加することによって形成され得る。このレコードは、メッセージ部分（１００５）及び期間パラメタ（１００６）を含み得る。メッセージ（１００５）は、発行元のコンタクト情報におけるデータ、発行元公開鍵及び署名を含

み得る。

【００３２】

図１１は、図１０のレコード（１００１）を使用する選択的な発行プロセスを例示する。発行元は、公開鍵から自分のＣＵＩを生成し（１１０１）、選択する受信者のＣＵＩを取得し（１１０２）、メッセージを構築し（１１０３）、発行元の秘密鍵を使用してメッセージに署名し（１１０４）、ＣＵＩの組み合わせ鍵（１１０１）に基づくインデックスにメッセージを挿入できる（１１０５）。更に、メッセージは、意図する受信者の公開鍵を使用し暗号化される（１１０６）。

【００３３】

図１２は、選択的な発行プロセスのためのリトリーブプロセスを例示していて、ブロック（１２０１）、（１２０２）、（１２０３）を追加した図７と同様である。発行されたレコードのリトリーブを所望する受信者は、最初に発行元のＣＵＩを取得し得（１２０１）、次に結合されたＣＵＩ鍵の下でインデックスストアのレコードを検索する（１２０２）。更に改良された実施形態においては、メッセージは、受信者の公開鍵を使用し暗号化され得る。こうして受信者だけが意図するデータを複号化できる。ＣＵＩの組み合わせ鍵を使用したメッセージのリトリーブ（１２０２）後、受信者は、最初にレコードを解読するために、その秘密鍵を使用し（１２０３）、その後、図７の検査及び検証プロセスが続く。この選択的発行の実施形態においては、（レコードを暗号化するために使用される）受信者の公開鍵は、組み合わせ鍵を生成するために発行元が使用した受信者ＣＵＩから決定され得る。

【００３４】

前術の実施形態の別の改良においては、鍵はグループ公開鍵であり得、ピアグループによって所有される。この実施形態においては、グループの任意メンバーがグループ公開鍵の下でレコードを検索し認証プロセスを実行する。ユーザグループは、レコードへのアクセスを有し得、投稿されたメッセージの受信のための明確な対象とされ得る。

【００３５】

ここで前述の特定の実施形態は、公開鍵交換ディレクトリに関連し得るが、コンタクト情報が別のデータを表し得ることも強調しなければならない。コンタクト情報の代わりに、例えばレコードは一般的メッセージの投稿があり得る。こうして本発明システムは、任意の公的にアクセス可能なインデックスストアにおける一般発行システムとして使用され得る。また本発明システムは、公開鍵検索以外のディレクトリサービスを提供するためにも使用され得る。本発明システムは、分散ハッシュテーブルなどの既存の分散インデックスストアがサーバを頼らずにセキュアなディレクトリサービスが働くように機能させ得る。

【００３６】

更に、本発明システムは、サーバセキュリティが最小限であり得、それによって本発明システムによって提供される認証プロセスを必要とする既存のサーバベースディレクトリ上で使用され得る。ピアグループ及びピアツーピアネットワークなどのアドホックシステムにおいては、サーバが不要な公開鍵発行及びリトリーブプロセスによってディレクトリサービスを提供するためにホスティングされる専用サーバの必要性を減らすことにより、ネットワークなどの作成をより効率的にし得る。また本発明の方法及びシステムは、公開鍵／秘密鍵の暗号化プロセスが、ユーザによるサーバへの明示的な登録の必要性を排除できるので、ユーザの関与を最小化できる。

【図面の簡単な説明】

【００３７】

【図１】本発明に従って作動可能な計算システムのブロック図を例示する。

【図２】一般的なピアツーピアネットワークを例示する。

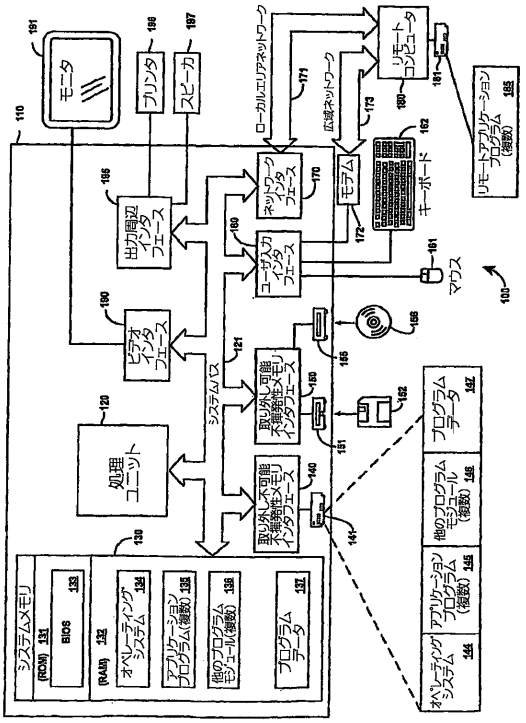
【図３】一般的なディレクタサーバ及びサービスを例示する。

【図４】分散ハッシュテーブルを例示する。

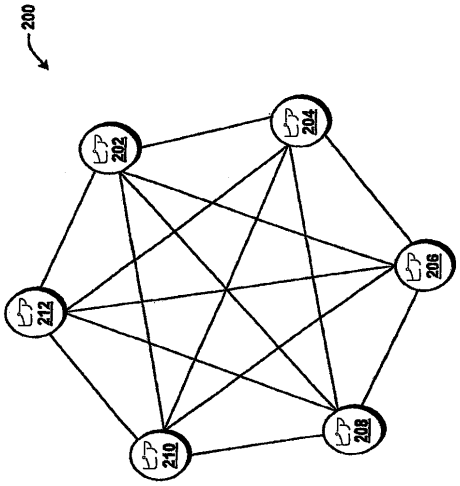
【図５】本発明の実施形態において使用されるレコードを例示する。

【図６】発行プロセスの実施形態を例示する。
【図７】リトリーブプロセスの実施形態を例示する。
【図８】期間パラメタを含む変更されたレコードを例示する。
【図９】期間パラメタを使用する別の検証プロセスを例示する。
【図１０】選択的な発行のための変更されたレコードを例示する。
【図１１】選択的な発行のための発行プロセスの実施形態を例示する。
【図１２】選択的な発行のためのリトリーブプロセスの実施形態を例示する。

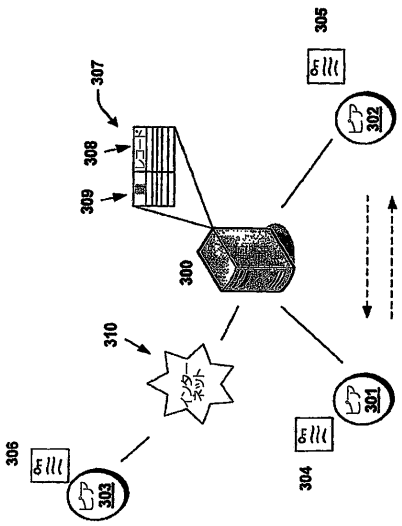
【図１】



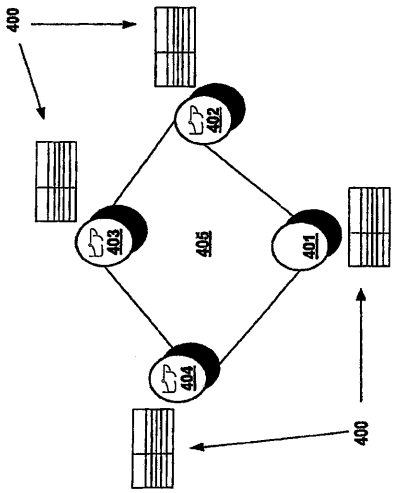
【図２】



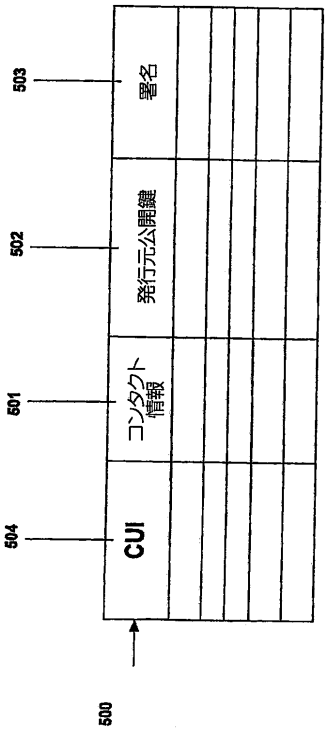
【図３】


305
307
308
309
300
310
インターネット
306
303
304
301
302

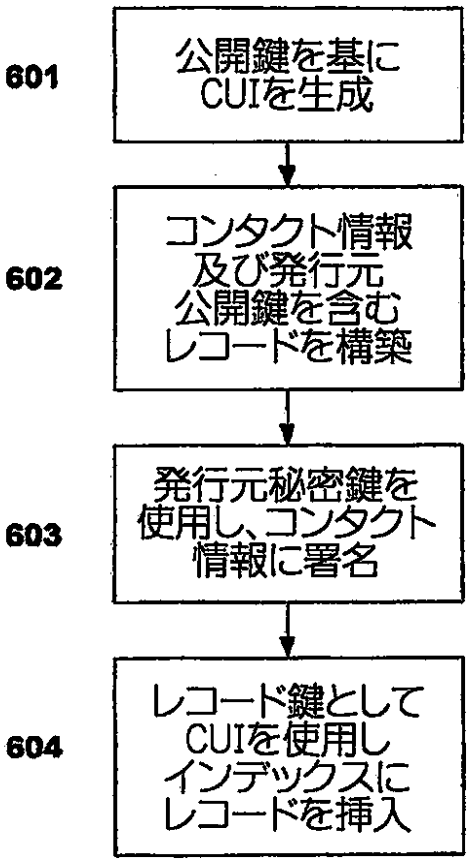
【図４】


400
402
403
405
401
404
400

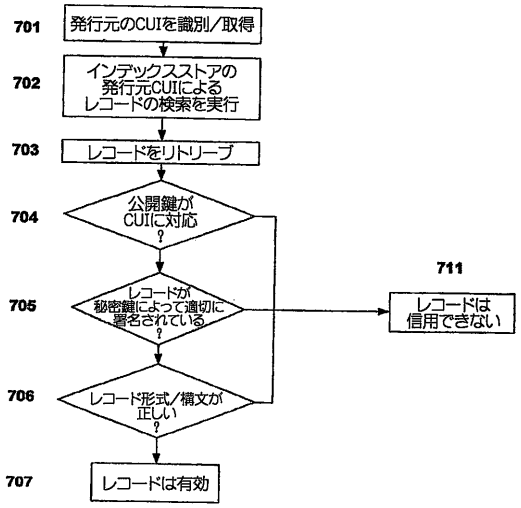
【図５】


503
署名
502
発行元公開鍵
501
コンタクト情報
504
CUI
500

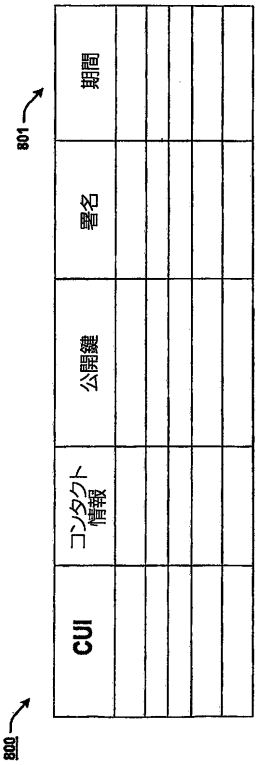
【図６】


601
公開鍵を基にCUIを生成
602
コンタクト情報及び発行元公開鍵を含むレコードを構築
603
発行元秘密鍵を使用し、コンタクト情報に署名
604
レコード鍵としてCUIを使用しインデックスにレコードを挿入

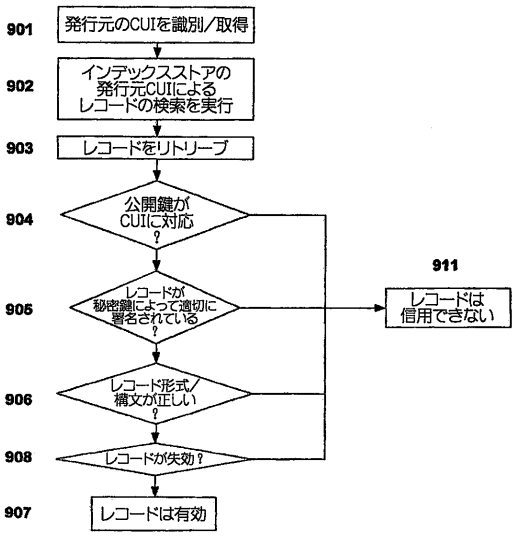
【図７】


701
発行元のCUIを識別/取得
702
インデックスストアの発行元CUIによるレコードの検索を実行
703
レコードをリトリーブ
704
公開鍵がCUIに対応？
705
レコードが秘密鍵によって適切に署名されている？
711
レコードは信用できない
706
レコード形式/構文が正しい？
707
レコードは有効

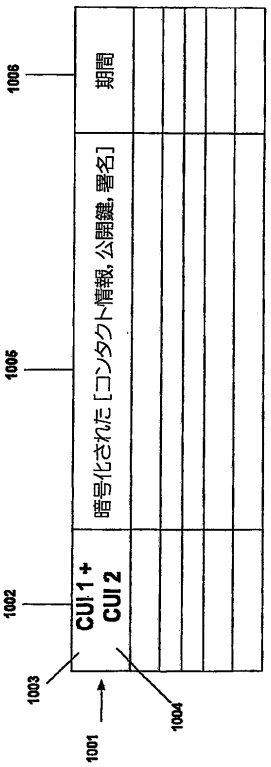
【図８】


801
期間
署名
公開鍵
コンタクト情報
CUI
800

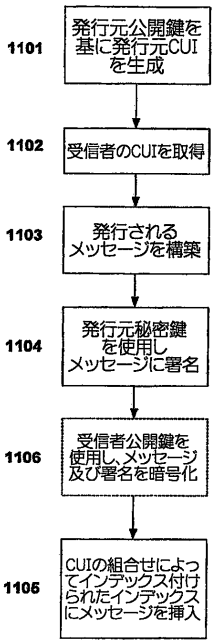
【図９】


901
発行元のCUIを識別/取得
902
インデックスストアの発行元CUIによるレコードの検索を実行
903
レコードをリトリーブ
904
公開鍵がCUIに対応？
905
レコードが秘密鍵によって適切に署名されている？
911
レコードは信用できない
906
レコード形式/構文が正しい？
908
レコードが失効？
907
レコードは有効

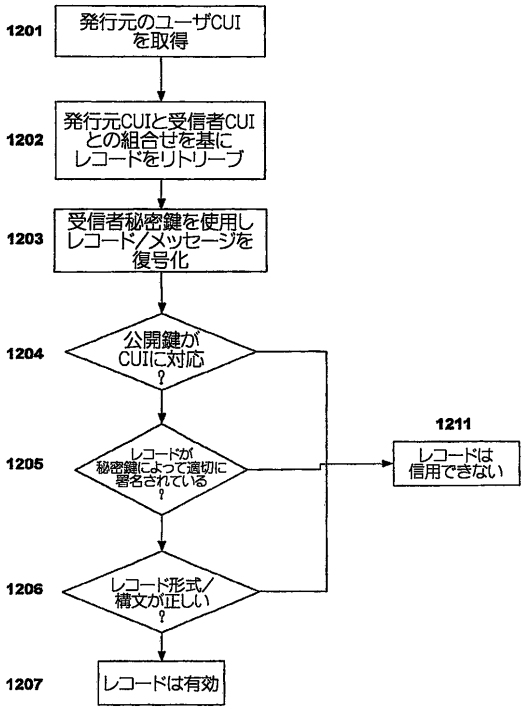
【図１０】


1006
期間
1005
暗号化された[コンタクト情報, 公開鍵, 署名]
1002
CUI 1 + CUI 2
1003
1004
1001

【図１１】


1101
発行元公開鍵を基に発行元CUIを生成
1102
受信者のCUIを取得
1103
発行されるメッセージを構築
1104
発行元秘密鍵を使用しメッセージに署名
1106
受信者公開鍵を使用しメッセージ及び署名を暗号化
1105
CUIの組合せによってインデックス付けられたインデックスにメッセージを挿入

【図１２】


1201
発行元のユーザCUIを取得
1202
発行元CUIと受信者CUIとの組合せを基にレコードをリトリーブ
1203
受信者秘密鍵を使用しレコード/メッセージを復号化
1204
公開鍵がCUIに対応？
1205
レコードが秘密鍵によって適切に署名されている？
1211
レコードは信用できない
1206
レコード形式/構文が正しい？
1207
レコードは有効

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2007/010092

A. CLASSIFICATION OF SUBJECT MATTER

G06F 15/16(2006.01)i, G06F 17/00(2006.01)i, H04L 9/30(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 8 : G06F, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models since 1975
Japanese Utility models and applications for Utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKIPASS(KIPO internal) "peer to peer", "distributed hash table". "public key", "index", "store"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20040064693 A1(KULDIPSINGH A.PABLA et al.) 1 April 2004 See abstract.	1-20
A	US 5005200 A(ADDISON M. FISCHER) 2 April 1991 See abstract; figures 2-4.	1-20
A	US 20050135381 A1(CEZARY DUBNICKI et al.) 23 January 2005 See figures 1-28.	1-20
A	US 20030028585 A1(WILLIAM J. YEAGER et al.) 6 Feburary 2003 See abstract.	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 OCTOBER 2007 (12.10.2007)	**15 OCTOBER 2007 (15.10.2007)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer HAN, Seon Kyoung Telephone No. 82-42-481-8523

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2007/010092

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 20040064693 A1	01.04.2004	US 7206934 B2	17.04.2007
US 5005200 A	02.04.1991	AT 113429 E	15.11.1994
		AT 150605 E	15.04.1997
		AU 4242589 A1	13.09.1990
		AU 620291 B2	13.02.1992
		CA 2000400 AA	07.09.1990
		CA 2000400 C	08.10.1996
		DE 69013541 C0	01.12.1994
		DE 69013541 T2	09.03.1995
		DE 69030268 T2	26.06.1997
		DK 386867 T3	03.04.1995
		EP 386867 A2	12.09.1990
		EP 386867 TD	29.04.1993
		EP 386867 B1	26.10.1994
		EP 386867 A3	10.06.1992
		EP 586022 A1	09.03.1994
		EP 586022 B1	19.03.1997
		ES 2036978 T1	16.06.1993
		ES 2036978 T3	01.01.1995
		ES 2098651 T3	01.05.1997
		GR 93300050 T1	30.06.1993
		JP 2291043 A2	30.11.1990
		JP 3520081 B2	19.04.2004
		US 5214702 A	25.05.1993
US 20050135381 A1	23.01.2005	None	
US 20030028585 A1	06.02.2003	EP 1282289 A2	05.02.2003
		EP 1282289 A3	20.09.2006
		US 7222187 B2	22.05.2007

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．ＥＥＰＲＯＭ

(74)代理人 100153028
弁理士 上田 忠
(72)発明者 シド，ガーシャラン・エス
アメリカ合衆国ワシントン州９８０５２，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，インターナショナル・パテンツ
(72)発明者 ホートン，ノア
アメリカ合衆国ワシントン州９８０５２，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，インターナショナル・パテンツ
(72)発明者 シンハル，サンディープ・ケイ
アメリカ合衆国ワシントン州９８０５２，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，インターナショナル・パテンツ

Ｆターム(参考) 5B089 GA21 KA17 KC58
5J104 AA07 AA08 JA21 KA02 KA05 LA03 LA06 NA02 NA05 NA12
NA37 NA38 PA07