【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成24年2月23日(2012.2.23)

【公開番号】特開2006-236349(P2006-236349A)
【公開日】平成18年9月7日(2006.9.7)
【年通号数】公開・登録公報2006-035
【出願番号】特願2006-45612(P2006-45612)
【国際特許分類】
*Ｇ０６Ｆ　21/20　　(2006.01)*
*Ｇ０９Ｃ　 1/00　　(2006.01)*
*Ｇ０６Ｆ　13/00　　(2006.01)*
【ＦＩ】
Ｇ０６Ｆ　15/00　　３３０Ａ
Ｇ０９Ｃ　 1/00　　６６０Ｅ
Ｇ０６Ｆ　13/00　　３５１Ａ

【誤訳訂正書】
【提出日】平成24年1月10日(2012.1.10)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【特許請求の範囲】
【請求項１】
コンピュータに一つの方法を実行させるコンピュータ実行可能命令を含む１つまたは複数のコンピュータ読取可能な記録媒体であって、前記方法は、
ａ）ノード識別子をピアツーピアネットワークの第１のノードに割り当てるステップと、
ｂ）前記第１のノードで、キー／値ペアを格納するステップであって、前記キー／値ペアのキーは第１の登録キーを含み、前記キー／値ペアの値はペイロードおよびアクセスリストを含み、前記アクセスリストは前記ペイロードの取出しを許可されたユーザに関連する第１の検索識別子を含むステップと、
ｃ）前記第１のノードで、検索メッセージを受信するステップであって、前記検索メッセージは第２の登録キーおよび第２の検索識別子を含むステップと、
ｄ）前記第１の検索識別子を前記第２の検索識別子と比較するステップと、
ｅ）前記第２の検索識別子が前記第１の検索識別子とマッチしない場合はエラーメッセージを送信するステップと
を備えることを特徴とする１つまたは複数のコンピュータ読取可能な記録媒体。
【請求項２】
前記検索メッセージは起点標識を含み、前記方法は、前記第１のノードが前記起点標識を検証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１つまたは複数のコンピュータ読取可能な記録媒体。
【請求項３】
前記起点標識はテキスト文字列からなる署名を含み、前記起点標識を検証するステップは前記テキスト文字列からなる前記署名を検証するステップを含むことを特徴とする請求項２に記載の１つまたは複数のコンピュータ読取可能な記録媒体。
【請求項４】
前記第２の検索識別子は前記第２の検索識別子に関連するユーザの公開キーを含み、前

記署名を検証するステップは前記公開キーを用いて前記テキスト文字列を復号するステップを含むことを特徴とする請求項３に記載の１つまたは複数のコンピュータ読取可能な記録媒体。
【請求項５】
前記第１の検索識別子を前記第２の検索識別子と比較するステップは、前記第２の検索識別子をハッシュするステップと、前記ハッシュされた第２の検索識別子を前記第１の検索識別子と比較するステップとを含み、前記方法は、前記ハッシュされた第２の検索識別子が前記第１の検索識別子とマッチする場合に、前記ペイロードを第３のノードに送信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１つまたは複数のコンピュータ読取可能な記録媒体。
【請求項６】
前記第１の検索識別子は、前記第１の検索識別子に関連する第１のユーザの公開キーのハッシュ値を含むことを特徴とする請求項５に記載の１つまたは複数のコンピュータ読取可能な記録媒体。
【請求項７】
第２のノードでグループキーを生成するステップと、前記グループキーを用いて前記第１のノードからの前記ペイロードを暗号化するステップとをさらに備え、前記格納するステップは、前記第２のノードから送信されたペイロードおよびグループキーを含む前記キー／値ペアを格納することを特徴とする請求項１に記載の１つまたは複数のコンピュータ読取可能な記録媒体。
【請求項８】
前記第１の検索識別子に関連する第１のユーザの公開キーを用いて前記グループキーを暗号化するステップと、前記暗号化されたグループキーを前記第１の検索識別子と関連づけるステップとをさらに備えることを特徴とする請求項７に記載の１つまたは複数のコンピュータ読取可能な記録媒体。
【請求項９】
前記第１のノードで、前記登録キーおよび第２の検索識別子を含む検索メッセージを第３のノードから受信するステップと、前記第２の検索識別子が前記第１の検索識別子に対して検証された場合は、前記暗号化されたペイロードおよび前記暗号化されたグループキーを前記第３のノードに送信するステップと、前記第３のノードで、前記暗号化されたグループキーを秘密キーを用いて復号するステップと、前記暗号化されたペイロードを前記復号されたグループキーを用いて復号するステップとをさらに備えることを特徴とする請求項８に記載の１つまたは複数のコンピュータ読取可能な記録媒体。
【請求項１０】
ピアツーピアネットワークにおいて、取出しノードの検索プロセスとストレージノードの検索モジュールとの間で通信を行う方法であって、
ａ）前記検索プロセスによって、登録キーおよび検索識別子を含めた複数のメッセージパラメータを含む検索メッセージを発行するステップと、
ｂ）前記検索モジュールによって、前記検索メッセージを受信し前記検索メッセージを構文解析して前記パラメータを取り出すステップと、
ｃ）前記登録キーが格納されたキー／値ペアのキーにマッチし、かつ前記ペイロードの取出しを許可されたユーザに関連する前記検索識別子が前記キー／値ペアに関連するアクセスリストに含まれている場合は、前記検索モジュールによってキー検出メッセージを発行するステップであって、前記キー検出メッセージは前記キー／値ペアの前記値の少なくとも一部を含むステップと
を備えることを特徴とする方法。
【請求項１１】
前記値の前記少なくとも一部はグループキーを用いて暗号化され、前記グループキーは前記検索プロセスにとって既知であることを特徴とする請求項１０に記載の方法。
【請求項１２】

前記キー検出メッセージは前記グループキーの暗号化されたものを含むことを特徴とする請求項１１に記載の方法。
【請求項１３】
前記検索識別子は前記検索識別子に関連する第１のユーザの公開キーのハッシュを含むことを特徴とする請求項１０に記載の方法。
【請求項１４】
前記検索モジュールは、前記検索識別子にハッシュを実施した後で前記アクセスリストと比較することを特徴とする請求項１０に記載の方法。
【請求項１５】
コンピュータを、
ａ）第１の登録キー、ペイロード、第１の検索識別子、およびグループキーを含む登録メッセージを受信するための登録モジュールであって、前記グループキーは前記ペイロードの復号に適したものであるモジュール、および
ｂ）第２の登録キーおよび第２の検索識別子を含む検索メッセージを受信する検索モジュールであって、前記第２の検索識別子が前記ペイロードの取出しを許可されたユーザに関連する前記第１の検索識別子にマッチするかどうか、および前記第１の登録キーが前記第２の登録キーにマッチするかどうかを判定することによって前記検索メッセージを検証し、前記検索メッセージが検証された場合は、前記ペイロードを前記第２の検索識別子に関連するピアツーピアネットワークのノードに送信し、前記検索メッセージが検証できなかったことに応答してエラーメッセージを送信する検索モジュール
として機能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１６】
前記検索メッセージは起点標識をさらに含み、前記検索モジュールは前記第２の検索識別子を使用して前記起点標識を検証し、前記起点標識を検証できなかったことに応答して前記エラーメッセージを送信することを特徴とする請求項１５に記載のコンピュータプログラム。
【請求項１７】
前記第２の検索識別子と前記第１の検索識別子がマッチするかどうかの判定は、前記第２の検索識別子のハッシュを前記第１の検索識別子と比較することを含むことを特徴とする請求項１５に記載のコンピュータプログラム。
【請求項１８】
前記登録モジュールは、ピアツーピアネットワーク上の前記登録モジュールを一意に識別するノード識別子に前記第１の登録キーが類似しているかどうかを判定するためのものであり、また前記登録モジュールは、前記ペイロードに関連する前記第１の登録キー、前記第１の検索識別子、および前記グループキーを格納するためのものであることを特徴とする請求項１５に記載のコンピュータプログラム。
【請求項１９】
前記検索モジュールは、前記検索メッセージが検証された場合に、前記グループキーの暗号化されたものを前記ピアツーピアネットワークの前記ノードに送信するためのものであり、前記グループキーは前記ピアツーピアネットワークの前記ノードにとって既知の暗号キーを使用して暗号化されることを特徴とする請求項１５に記載のコンピュータプログラム。
【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【発明の詳細な説明】
【発明の名称】ピアツーピアネットワーク情報
【技術分野】

【０００１】
本発明は、ピアツーピアネットワークに関する。
【発明の開示】
【発明が解決しようとする課題】
【０００２】
オーバレイネットワークを使用して、ピアツーピアネットワークにおいて、ノード群に関する様々な情報を格納しかつ／または通信することができる。格納された情報を、キー値ペアとして、キーに関係づけて格納することができる。典型的なピアツーピアネットワークでは、ピアツーピアネットワークのユーザはだれでもキーおよびそのキーに関連する値の検索を要求することができる。しかし、格納されたオーバレイネットワークの情報を、安全な状態にし、保護し、かつ／または分配する必要がある場合が存在するが、ピアツーピアネットワークにおいては、要求ユーザを認証しかつ／またはネットワーク上での攻撃を阻止して、キー値ペアの情報に対するセキュリティ、プライバシー等を保護するための中央サーバは存在しない。
【発明が解決するための手段】
【０００３】
上述した課題を解決するために、本発明は、以下を方法と媒体を備える。
本発明の一態様によれば、本発明に係る１つまたは複数のコンピュータ読取可能な記録媒体は、コンピュータに一つの方法を実行させるコンピュータ実行可能命令を含む１つまたは複数のコンピュータ読取可能な記録媒体であって、前記方法は、ａ）ノード識別子をピアツーピアネットワークの第１のノードに割り当てるステップと、ｂ）前記第１のノードで、キー／値ペアを格納するステップであって、前記キー／値ペアのキーは第１の登録キーを含み、前記キー／値ペアの値はペイロードおよびアクセスリストを含み、前記アクセスリストは前記ペイロードの取出しを許可されたユーザに関連する第１の検索識別子を含むステップと、ｃ）前記第１のノードで、検索メッセージを受信するステップであって、前記検索メッセージは第２の登録キーおよび第２の検索識別子を含むステップと、ｄ）前記第１の検索識別子を前記第２の検索識別子と比較するステップと、ｅ）前記第２の検索識別子が前記第１の検索識別子とマッチしない場合はエラーメッセージを送信するステップとを備える。
【０００４】
本発明の他の態様によれば、本発明に係る方法は、ピアツーピアネットワークにおいて、取出しノードの検索プロセスとストレージノードの検索モジュールとの間で通信を行う方法であって、ａ）前記検索プロセスによって、登録キーおよび検索識別子を含めた複数のメッセージパラメータを含む検索メッセージを発行するステップと、ｂ）前記検索モジュールによって、前記検索メッセージを受信し前記検索メッセージを構文解析して前記パラメータを取り出すステップと、ｃ）前記登録キーが格納されたキー／値ペアのキーにマッチし、かつ前記ペイロードの取出しを許可されたユーザに関連する前記検索識別子が前記キー／値ペアに関連するアクセスリストに含まれている場合は、前記検索モジュールによってキー検出メッセージを発行するステップであって、前記キー検出メッセージは前記キー／値ペアの前記値の少なくとも一部を含むステップとを備える。
【０００５】
本発明の他の態様によれば、本発明に係るコンピュータプログラムは、コンピュータを、ａ）第１の登録キー、ペイロード、第１の検索識別子、およびグループキーを含む登録メッセージを受信するための登録モジュールであって、前記グループキーは前記ペイロードの復号に適したものであるモジュール、およびｂ）第２の登録キーおよび第２の検索識別子を含む検索メッセージを受信する検索モジュールであって、前記第２の検索識別子が前記ペイロードの取出しを許可されたユーザに関連する前記第１の検索識別子にマッチするかどうか、および前記第１の登録キーが前記第２の登録キーにマッチするかどうかを判定することによって前記検索メッセージを検証し、前記検索メッセージが検証された場合は、前記ペイロードを前記第２の検索識別子に関連するピアツーピアネットワークのノー

ドに送信し、前記検索メッセージが検証できなかったことに応答してエラーメッセージを送信する検索モジュールとして機能させる。

【発明を実施するための最良の形態】

【０００６】

本発明の前述の態様および付随する利点の多くは、以下の詳細な説明を添付の図面と併せて参照することによってより良く、また、より容易に理解できるようになるであろう。

【０００７】

［例示的動作環境］

図１および以下の議論は、ピアツーピアネットワークストレージシステムのノードを実装することができる適切なコンピュータ環境の、簡潔で一般的な説明を提供することを意図したものである。図１の動作環境は適切な動作環境の一例に過ぎず、動作環境の使用または機能の範囲について何らかの制限を示唆することを意図したものではない。本明細書で説明するノードとしての使用に適した他の周知のコンピュータシステム、環境、および／または構成の例には、パーソナルコンピュータ、ハンドヘルドまた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、プログラマブル家電、ネットワークパーソナルコンピュータ、ミニコンピュータ、メインフレームコンピュータ、上記システムまたは装置のいずれかを含む分散コンピュータ環境などが含まれるが、これらに限られるものではない。

【０００８】

必須ではないが、ピアツーピアノードおよびピアツーピアストレージシステムは、１つまたは複数のコンピュータまたは他の装置によって実行される、プログラムモジュールなどのコンピュータ実行可能な命令の一般的な状況で説明される。一般に、プログラムモジュールには、特定のタスクを実施するか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、データ構造などが含まれる。一般に、プログラムモジュールの機能は、必要に応じて様々な環境に組み合わせること、または様々な環境に分散させることができる。

【０００９】

図１を参照すると、ピアツーピアノードを実装するための例示的システムには、コンピュータ装置１００などのコンピュータ装置が含まれる。その最も基本的な構成では、コンピュータ装置１００は一般に、少なくとも１つの処理ユニット１０２およびメモリ１０４を含む。コンピュータ装置の正確な構成や種類に応じて、メモリ１０４は（ＲＡＭなどの）揮発性、（ＲＯＭ、フラッシュメモリなどの）不揮発性、またはその両者の組合せであってもよい。この最も基本的な構成は、図１の破線１０６によって示されている。さらに、装置１００は追加の機構および／または機能を備えることもできる。例えば、装置１００は磁気または光ディスクあるいはテープなど、（例えば、リムーバブルおよび／または固定の）追加の記憶装置を含むこともできるが、これらに限られるものではない。このような追加の記憶装置は、図１ではリムーバブル記憶装置１０８および固定記憶装置１１０によって示されている。コンピュータ記憶媒体には、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、その他のデータなどの情報を記憶するための任意の方法または技術で実装された、揮発性および不揮発性、リムーバブルおよび固定の媒体が含まれる。メモリ１０４、リムーバブル記憶装置１０８、固定記憶装置１１０など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には、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリその他のメモリ技術製品、ＣＤ－ＲＯＭ、ＤＶＤ（ｄｉｇｉｔａｌ ｖｅｒｓａｔｉｌｅ ｄｉｓｋ）その他の光学記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置その他の磁気記憶装置、あるいは所望の情報を格納するために使用することができ、装置１００によってアクセス可能な他の任意の媒体が含まれるが、これらに限られるものではない。このようなコンピュータ記憶媒体はいずれも、装置１００の一部であってもよい。

【００１０】

装置１００は通信接続（群）１１２を含むこともできる。この通信接続により、装置１

００はピアツーピアネットワーク２１１内の他のノードなど、他の装置と通信することができるようになる。通信接続（群）１１２は通信媒体の一例である。通信媒体は一般に、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、その他のデータなどを搬送波や他の伝送機構など被変調データ信号の形で実施するとともに、いずれかの情報伝達媒体を含む。「被変調データ信号」という用語は、情報を信号中に符号化するような方法で設定または変更された、１つまたは複数の信号特性を含む信号を意味する。限定の意味ではなく例として、通信媒体には有線ネットワークまたは直接有線接続などの有線媒体、ならびに音響、無線電波、赤外、その他の無線媒体が含まれる。本明細書で使用するコンピュータ可読媒体という用語は、記憶媒体と通信媒体の両方を含むものとする。

【００１１】

装置１００はまた、キーボード、マウス、ペン、音声入力装置、タッチ入力装置、レーザレンジファインダ、赤外線カメラ、ビデオ入力装置、および／または他の任意の入力装置などの入力装置（群）１１４を含むこともできる。表示器、スピーカ、プリンタ、および／または他の任意の出力装置などの出力装置（群）１１６を含むこともできる。

【００１２】

［ピアツーピアネットワーク］

ピアツーピアネットワークは一般に、コンピュータの自己管理されたネットワークと見なされており、そのネットワーク内にはネットワークの維持を担当するサーバまたはコントローラはまったく存在しない。ピアツーピアネットワークおよびアプリケーションを生成するために、いくつかの異なるアーキテクチャを使用することができる。このようなアーキテクチャの１つがオーバレイネットワークである。一般に、オーバレイネットワークは、インターネットプロトコル（ＩＰ）アドレスなどの従来のネットワークアドレスの上に副次的なレベルを提供する。

【００１３】

ピアツーピアネットワーク用のオーバレイネットワークに関して現在知られている例には、カリフォルニア大学バークレー校でＢｅｎ　Ｙ．Ｚｈａｏらによって開発されたＴａｐｅｓｔｒｙ、マサチューセッツ工科大学で開発されたＣｈｏｒｄ、本件特許出願人と様々な大学とで開発されたＰａｓｔｒｙなどがある。Ｔａｐｅｓｔｒｙ、Ｃｈｏｒｄ、およびＰａｓｔｒｙは、分散システム構築のためのツールキットである。ＣＡＮ、Ｋａｄｅｍｌｉａ、Ｓｋｉｐｎｅｔ、およびＶｉｃｅｒｏｙは、類似の他のシステムである。新しいオーバレイ設計も頻繁に発表されている。

【００１４】

図２は代表的なオーバレイネットワークを示す。ネットワークの各ノード２１０、２３０は、図１の例示的コンピュータ装置１００によって実装することができる。オーバレイネットワークに属するノード２１０、２３０は、下位層のネットワーク媒体２１１を介した通信媒体を用いて相互にメッセージをルーティングする。下位層のネットワーク媒体は、特定のコンピュータ間でメッセージを直接ルーティングするための情報および機能を有しているが、一般にオーバレイネットワークは部分的なルーティング情報だけを維持しており、中間ノードを介した逐次転送を利用してメッセージを意図した最終的な宛先に送達する。

【００１５】

ピアツーピアネットワークでは、ネットワークの各アクティブノードにノード識別子を割り当てることができる。ノード識別子は、ピアツーピアネットワークに接続されたアクティブノードの一意の識別子である。ノード識別子は、マシンに対して永続させること、および／またはユーザの特定のセッションに対して設定することができる。ノード識別子は、ネットワークプロトコルによって定義される任意のサイズとすることができる。また、そのサイズは、ネットワークの予想されるユーザ数、システムのセキュリティ、衝突回避に対する要望などに応じて決定することができる。例えば、Ｐａｓｔｒｙのピアツーピアネットワークプロトコルは１２８ビットのノード識別子を定義しており、任意のサイズの識別子を許容することができる。ノードの識別子を任意の適切な方法で割り当てること

ができる。例えば、ランダムに割り当てることができる。あるいはユーザは、シードを選択し、それを日付、時間など任意選択の他のデータを用いてハッシュしてノード識別子を形成することもできる。一例として、永続的なノード識別子は、ユーザのピアツーピアネットワークへの初期登録時に信頼できる第三者機関によって提供され、かつ／または認証されたマシンのキー証明書に基づくものであってもよい。ノードの割当てを任意の適切な方法で実施することができる。例えば、ノードの割当てを、１つまたは複数の信頼できる認証局によって実施することができる。認証局は、ノード識別子がノード識別子空間からランダムに選択されることを保証し、各ノードがノード識別子を偽造することを阻止することができる。認証局はオフラインとし、かつオーバレイネットワークの通常の動作に関与させないようにして攻撃から保護することができる。

【００１６】

ピアツーピアネットワークに参加するために、各ノードは、ピアツーピアネットワーク内の既知の他のノードについてのノード識別子および／またはルーティング情報を含むルーティングテーブルを生成することができる。ルーティングテーブルを、任意の適切な方法で、ピアツーピアネットワークプロトコルに従って生成することができる。例えばユーザは、ネットワーク内の少なくとも１人の既知で既存のユーザを一連のノード識別子にわたって照会することができる。このユーザは一般に、ルーティングテーブルの「最初の行」に格納されている。次に、この新しいユーザは、その新しいユーザのノード識別子に最も近いノードの一部を照会して、そのユーザ自身のノード識別子に近接しかつ／または類似した追加のノード識別子を発見することができる。ルーティングテーブルの最下行または最後の行は、そのルーティングテーブルを格納するユーザノードのノード識別子に最も近いノード識別子、例えばピアツーピアネットワークにおけるユーザノードの隣接ノードを含むことができる。このようにして、ルーティングテーブルの最下行は、ユーザノードのノード識別子に最も近いノード識別子からなるリーフセット（ｌｅａｆ　ｓｅｔ）を形成することができる。ピアツーピアネットワークに復帰するユーザノードは、永続的ルーティングテーブル内のエントリを更新し、かつ／または検証することができる。各ノードのルーティングテーブルは完全である必要はなく、例えばルーティングテーブルは部分的なルーティングテーブルでもよいことを理解されたい。例えば、ノード識別子が見つからないか、または存在しないために、ルーティングテーブルを完全に埋めることができないこともある。

【００１７】

オーバレイネットワークを使用して、様々な情報を格納しかつ／または通信することができる。例えば、ピアツーピアネットワークは、アドレス解決（例えば、ピア名前解決プロトコル（ＰＮＲＰ））のための名前、分散データベースなどのデータファイル、暗号化キー、リッチプレゼンスデータなどを提供することができる。データは登録メッセージのペイロードとして登録し、ピアツーピアネットワークのメンバーである１つまたは複数のストレージノードの分散ハッシュテーブルに格納することができる。全体のハッシュテーブルの記憶はピアツーピアネットワークの様々なノード間に分散されるので、どの単一のノードも全体のハッシュテーブルを格納することはない。正確に言えば、様々なストレージノードがハッシュテーブルの様々な部分を格納することができる。

【００１８】

ペイロードデータを格納するために、ハッシュテーブルは登録キーをある値と関連づける。値はペイロードを含みかつ／またはペイロードを表す。このように、ノードによって格納されたハッシュテーブルの各部分はキー／値ペアを格納する。各登録キーは、その値に含まれかつ／またはその値によって表されたペイロードに関連するキー識別子のハッシュであってもよい。例えば、キー識別子は、ピアツーピアネットワークのユーザの一意の個人識別子、またはペイロードに含まれるファイルもしくは他のデータの識別子などであってもよい。インスタントメッセンジャアプリケーションの例では、キー識別子は、ユーザ名、インターネットプロトコルアドレス、公開または秘密キー、および／またはアプリケーション標識を含むことができる。このようにして、登録キーの衝突を減少させること

ができる。衝突が発生した場合は、登録キーを相互に区別するために登録キーに関連する値を使用することができる。登録キーを形成するキー識別子のハッシュは、任意の適切なハッシュアルゴリズム（例えば、ＭＤ５ハッシュ）の使用に基づいて実施することができる。図２を参照すると、１つまたは複数の暗号サービスモジュール２７０は、ピアツーピアネットワークのノードに、暗号化、復号、ハッシングなどのサービスを提供することができる。

【００１９】

キー識別子のハッシュすなわち登録キーは、ピアツーピアネットワークのどのノードが登録キーに関連するペイロードを格納しているかを識別する。一例では、ノード識別子は登録キーの番号空間に関係づけることができる。例えば、ノード識別子が番号１～８の場合は、各ノードには登録キーの番号空間の８分の１を割り当てることができる。他の例では、キー／値ペアの登録キーとノード識別子は同じバイトサイズを有し、同じベース、例えばベース１０、ベース１６、ベース５などを有することができる。ペイロードを格納するために、ペイロードの登録キーに最も近いノード識別子を有するユーザノードを選択することができる。単一点障害、例えば単一のノードがペイロードを格納することを回避するために、キー／値ペアを複製し、登録キーの識別子に類似したノード識別子を有する複数のストレージノードに格納することができる。このようにして、複製によってストレージノードのルーティングテーブルにおけるリーフセットの少なくとも一部を活用することができる。複写ファクタはユーザノードがピアツーピアクラウド（ｐｅｅｒ－ｔｏ－ｐｅｅｒ　ｃｌｏｕｄ）の内部に滞在する平均時間、ユーザノードがクラウドを離れる確率、所望される情報の信頼性などに依存して決定することができる。

【００２０】

ペイロードを登録するために、ユーザノードは登録メッセージを構成することができる。登録メッセージを構成するために、ユーザノードはピアツーピアネットワークストレージシステムのコンピュータ実行可能命令を実装することができる。その一例が、図２のノード２３０に示されている。ユーザノードは登録プロセス２４０、例えば登録アプリケーションインタフェース（ＡＰＩ）などにアクセスして登録メッセージを構成し、通信媒体を使用して登録メッセージを送信することができる。ユーザノードは、例えば登録ＡＰＩなどによって登録キーを決定してペイロードと関係づけることができる。上述のように、キー／値ペアのキーは周知の識別子、例えば個人識別子および／またはアプリケーションデータから構成された文字列などのハッシュである。ユーザノードは、例えばローカルアプリケーション２８０および／または登録プロセス２４０など、任意の適切な方法を用いてキー／値ペアの値であるペイロードを作成することができる。例えば、インスタントメッセンジャアプリケーションでは、ペイロードは、ユーザの使い易い名前、ユーザの現在のエンドポイントアドレス、および／またはローカルアプリケーションのプレゼンスデータを含むことができる。ピアツーピアネットワーク２００のどのノード２１０がペイロードを格納するのかを決定するために、ユーザノードは、ルーティングテーブル２６５で、関連するペイロードのキーに最も近いノード識別子を有すると指示されたノードに、クラウド２１１を介し通信媒体を使用して登録メッセージを送信することができる。ユーザノードは、キー／値ペアのキーにより類似したノード識別子を有する他のノードに登録メッセージをルーティングすることもできる。このプロセスは、ピアツーピアネットワークプロトコルの下で、登録メッセージの登録キーに最も近いノード識別子を有するストレージノードのハッシュテーブル部分２６０にキー／値ペアが格納されるまで繰り返すことができる。

【００２１】

例えば、受信ノードは、登録モジュール２９０を使用して登録メッセージを受信することができる。登録モジュールは登録要求を構文解析して登録キーを取り出し、そのキーをその受信ノードに割り当てられたノード識別子と比較することができる。登録キーが同一かまたは類似している場合（例えば、受信ノードのルーティングテーブルのそのリーフセットに含まれる場合）は、受信ノードは登録メッセージから構文解析されたキー／値ペア

を格納することができる。
【００２２】
オーバレイネットワークは、あるノードのＩＤが他のどのノードのＩＤよりもキーに近いときに通知できるような十分な情報をそのルーティングテーブル内に維持する。次に、その最も近いノードは、そのハッシュテーブル２６０内にドキュメントを格納し、指示されたキー／値ペアを求める照会に応答する役割を果たすことになる。上述のように、登録メッセージを複製し、ネットワークプロトコルに従って追加のノードの分散ハッシュテーブル内に格納することもできる。
【００２３】
代表的なピアツーピアネットワークでは、ピアツーピアネットワークのユーザはだれでもキーおよびその関連する値の検索を要求することができる。このように、キー／値ペアの値は代表的ピアツーピアネットワーク内の任意の人によってアクセスすることができる。格納されたキー／値ペアの値の情報セキュリティは、ピアツーピアネットワークへのエントリを管理し、メッセージをルーティングする際にユーザのルーティングテーブルの認証性を検証することなどによって管理することができる。あるノードが、例えば情報の誤用など「不正行為を行った」場合は、そのノードのハッシュテーブル内に格納された情報を提供することを拒絶し、かつ／または他のノードメンバーにメッセージを転送することを拒絶して、そのノードのノード識別子を無効にすることができる。しかし、代表的なピアツーピアネットワークの内部では、任意のノードによって全ての情報を取り出すことができる。
【００２４】
場合によっては、キー／値ペアを登録したユーザは、すべてのユーザまたはピアツーピアネットワークのユーザの一部が、そのキー／値ペアにアクセスしかつ／またはそれを取り出すことを望まないことがある。例えば、インスタントメッセンジャアプリケーションでは、ユーザは、ネットワークに接続しビデオゲームで遊んでいることや、インターネットを閲覧していることを上司に見つかることを望まないこともある。ピアツーピアネットワークにおいては、要求ユーザを認証しかつ／またはネットワーク上での攻撃を阻止して、キー／値ペアの情報に対するセキュリティ、プライバシー等を保護するための中央サーバは存在しない。
【００２５】
［ピアツーピアネットワークセキュリティ］
分散ハッシュテーブルに登録されたキー／値ペアの格納および／または取出しは、制限することができる。一例では、キー／値ペアの値を暗号化してその情報を保護することができる。キー／値（例えば、キー識別子のハッシュ）を照会する他のユーザは、その情報を復号できない場合でも、その値を取り出すことができる場合がある。しかし、情報が暗号化されている場合であっても、照会ユーザがあるデータを取り出したという単なる事実だけで何らかの情報が提供され、プライバシーまたは他のセキュリティ事項が侵害される恐れがある。例えば、インスタントメッセンジャの環境では、識別されたユーザがオンラインでない場合は、キー／値ペアが登録されないことがある。したがって、何らかの値を受信した照会ユーザは、その値が暗号化されている場合でも、他のユーザがオンラインであることを確認することができる。
【００２６】
情報へのアクセスを管理し、かつ／またはピアツーピアネットワークのハッシュテーブル内に格納された情報を保護するために、上記の登録メッセージを修正することができる。図３は、分散ハッシュテーブル、例えばピアツーピアネットワークの分散ハッシュテーブルなどに格納されるように情報を登録する方法３００の一例を示す。
【００２７】
ユーザは任意の適切な方法でピアツーピアネットワークに参加することができる。例えば、３１４で、ネットワークプロトコルに従って、ユーザにノード識別子を割り当てることができる。３０２で、ユーザは図２の登録プロセス２４０などによって、ペイロードに

関連づけられる登録キーを決定することができる。上述のように、キー／値ペアの登録キーは既知のキー識別子、例えば個人識別子および／またはアプリケーションデータから構成された文字列などのハッシュである。次にユーザは、ローカルアプリケーションおよび／または登録プロセスなどによる任意の適切な方法を使用して、３０４で、キー／値ペアの値の一部であるペイロードを作成することができる。上述のように、ペイロードは登録キーに関連づけられる任意の情報であってよく、例えばリッチプレゼンスデータ、ストレージファイル、および／または通信アドレスなどであってもよい。

【００２８】

ペイロード情報へのアクセスを制限するために、３０６で、ユーザノードはアクセスリストを決定することができる。登録メッセージのアクセスリストは、図２の登録プロセス２４０および／またはローカルアプリケーション２８０によって構成することができる。アクセスリストは、登録ユーザがペイロード情報を取り出す権限を持つことを望むユーザに関連する１つまたは複数の適切な検索識別子を含むことができる。インスタントメッセンジャの例では、アクセスリストは、登録ノード２３０のインスタントメッセンジャコンタクトリストに関連する検索識別子を含むことができる。データストレージの例では、アクセスリストは、登録されたファイルへのアクセスが許可されたユーザの検索識別子を含むことができる。アクセスリストの検索識別子は、ペイロード情報へのアクセスを許可するために検証できる任意の適切な識別子であってもよい。アクセスリストの検索識別子は、ユーザの暗号化されていない識別子であってもよいし、あるいはユーザの識別子を暗号化またはハッシュしたものであってもよい。例えば、ユーザの検索識別子は、ピアツーピアネットワーク内のユーザノードの個人識別子、例えばＩＰアドレスなどであってもよい。他の例では、ユーザの検索識別子は、取出し権限を有するユーザに関する公開／秘密キーペアの公開または秘密キーのハッシュであってもよい。

【００２９】

登録ユーザは、３０８で、図２の登録プロセス２４０などによって、登録メッセージを構成することができる。登録メッセージは、決定された登録キー、ペイロードを含む値、およびアクセスリストから構成することができる。他の例では、キー／値ペアの値は、ペイロードとアクセスリストの組合せまたは連結によって形成することができる。登録ノードは、３１０で、ピアツーピアネットワークのネットワークプロトコルに従って通信媒体を使用し、適切なノード（群）に登録メッセージを送信することができる。

【００３０】

登録メッセージを受信するノードには、３１６で、ネットワークプロトコルに従ってノード識別子を割り当てることができる。受信ノードは、図２の登録モジュール２９０などを使用して登録メッセージを受信することができる。登録モジュールは登録メッセージを構文解析して登録キーを取り出すことができる。また、登録モジュールは、割り当てられたノード識別子を登録メッセージの登録キーと比較して、キー／値ペアを格納すべきかどうかを決定することができる。受信ノードに割り当てられたノード識別子が登録メッセージの登録キーに最も近い場合、または登録キーが受信ノードのルーティングテーブルにおけるその受信ノードのリーフセット内に存在している場合は、受信ノードはキー／値ペアをそのハッシュテーブルに格納し、そのキー／値ペアのストレージノードになることができる。図２の例を参照すると、受信ノードの登録モジュール２９０は、登録メッセージから解析されたキー／値ペアをハッシュテーブル２６０に送って格納することができる。

【００３１】

登録されたキー／値ペアを格納するハッシュテーブル、例えば図２のノード２３０のハッシュテーブル２６０は、ストレージノードのメモリ内にある任意の適切なデータストアに格納することができる。任意の適切なフォーマットの任意の適切なデータストアを使用して、ハッシュテーブル情報を取出し、ノードに格納し、かつ／またはそのノードと通信できることを理解されたい。データストアとしては、リレーショナルデータベース、オブジェクト指向データベース、非構造化データベース、インメモリデータベース、シーケンシャルメモリ、その他のデータストアなどが使用できる。ストレージアレイはフラットフ

ァイルシステム、例えばＡＳＣＩＩテキスト、バイナリファイル、通信ネットワークを介して送信されたデータ、他の任意のファイルシステムなどを使用して構成することができる。前述のデータストアについてのこれらの可能な実装にもかかわらず、本明細書で使用するデータストアおよびストレージアレイという用語は、コンピュータによってアクセス可能な任意の方法で収集され格納された任意のデータを意味する。

【００３２】

時には、ピアツーピアネットワーク内の他のノードが、キー／値ペアとしてハッシュテーブルに格納されたペイロード情報を取り出し、かつ／またはアクセスしたいと望むこともある。ペイロード情報を取り出すために、取出しユーザノードは検索メッセージを構成し、その検索メッセージをストレージノードに宛てに送ることができる。検索メッセージを、図２のノード２３０における検索プロセス２５０などの検索ＡＰＩによって構成することができる。

【００３３】

図４は、格納された情報を、検索メッセージを使用してピアツーピアネットワークから取り出すための例示的方法４００を示す。格納されたデータをピアツーピアネットワークから取り出すために、取出しユーザノードは、４０２で、所望の情報に対する適切な登録キーを決定することができる。登録メッセージの登録キーを決定するのと同様に、検索メッセージを作成する取出しユーザノードは、例えば図２の検索プロセス２５０および／またはローカルアプリケーション２８０を使用して、格納された情報に対する適切なキー識別子を決定することができる。キー識別子には、個人識別子および登録ユーザのアプリケーション情報を含めることができる。登録キーを形成するために、キー識別子をハッシュすることができる。例えば、キー識別子は、図２の検索プロセス２５０および／または暗号化サービスモジュール２７０を使用してハッシュすることができる。

【００３４】

次に、取出しユーザノードは、４０４で、取出しノードの検索識別子を決定することができる。上述のように、検索識別子は、格納されたキー／値ペアへのアクセスを許可されたユーザの任意の適切な識別子であってもよい。例えば、ＰＫＩシステムでは、検索識別子は取出しユーザの公開キーであってもよい。図２を参照すると取出しノードは、検索プロセス２５０および／または暗号化サービスモジュール２７０を使用して検索識別子を形成することができる。

【００３５】

取出しユーザノードは、検索メッセージを構成して、登録キーおよび検索識別子を含めることもできる。取出しノードは、４０６で、ピアツーピアネットワークの適切なノード、例えば検索メッセージのキーに最も近いノード識別子を有するノードに検索メッセージを送信することができる。例えば、図２を参照すると、検索プロセス２５０はルーティングテーブル２６５にアクセスして、決定された登録キーに最も近い既知のノード識別子を決定し、通信媒体を使用しネットワーククラウド２１１を介して検索メッセージをそのノードに送信することができる。

【００３６】

受信ノードは検索メッセージを受信し、図２の検索モジュール２９５など任意の適切なプロセスを使用してその検索メッセージを構文解析し、登録キーを取り出すことができる。図４を参照すると受信ノードは、４０８で、図２の検索モジュール２９５などによって検索メッセージを検証することができる。例えば、受信ノードは、検索メッセージで提供された登録キーが、受信ノードのハッシュテーブル内に格納された登録キーのいずれかに正確にマッチするかどうかを判定することができる。ノードにそのような登録されたキーが存在しない場合は、４１０で、ノードは取出しユーザノードにエラーメッセージを返すことができる。エラーメッセージは、「指定されたキーは存在しません」または「アクセスは拒否されました」など任意の適切なエラーメッセージとすることができる。

【００３７】

構文解析された登録キーが受信ノードに存在している場合には、４１２で、受信ノード

は取出しユーザを検証することができる。取出しユーザを任意の適切な方法で検証することができる。例えば、受信ノードは、検索モジュール２９５を用いて検索メッセージを構文解析することなどによって、検索メッセージ内の検索識別子を取り出すことができる。受信ノードは、検索メッセージの検索識別子を、指示されたキー／値ペアのアクセスリストにリストアップされた１つまたは複数の検索識別子と比較することができる。検索メッセージからの検索識別子が、例えば取出しユーザのＩＰアドレスや公開キーなどのようにハッシュされていない場合には、受信ノードは検索識別子をハッシュした後でアクセスリストと比較することができる。検索メッセージの指示された検索識別子が、アクセスリストのどの検索識別子にもマッチしていない場合は、４１４で、受信ノードはエラーメッセージを返すことができる。このエラーメッセージは、４１０で返されるエラーメッセージと同一でも異なっていてもよい。エラーメッセージが同一の場合は、取出しノードは、登録されたキー／値ペアへのアクセスが拒絶された場合でも、登録されたキー／値ペアが存在するかどうかを判定できない場合がある。

【００３８】

ユーザが検証された場合は、４１６で、受信ノードはキー検出メッセージを作成することができる。このメッセージは、登録キーおよびメッセージペイロードにマッチするハッシュテーブルの行を含むことができる。ネットワークプロトコルおよび／またはアクセスリスト特権に従って、アクセスリストそのものはペイロードと共にユーザに返すこともあるし、返さないこともある。キー検出メッセージは任意の適切なプロセス、例えば図２の検索モジュール２９５および／またはキー検出ＡＰＩなどのキー検出プロセス（図示せず）を使用して構成することができる。次に、４１８で、受信ノードは通信媒体を使用してキー検出メッセージを取出しノードに送信することができる。

【００３９】

取出しユーザノードに関する追加の検証を実装することもできる。例えば、取出しノードによって構成された検索メッセージはまた、起点証明標識を含むこともできる。起点証明標識は、その取出しノードが検索メッセージを生成したことを指示することができる。起点標識は、どのノードがメッセージを生成したかを指示するために検証することができる任意の適切な標識であってもよい。図４の取出し方法を参照すると、４２０で、この取出しノードは図２の検索プロセス２５０など任意の適切なプロセスによって起点標識を決定することができる。例えば、取出しノードは、現在の世界時標識などのテキスト文字列に取出しユーザの秘密キーを用いて署名することによって起点標識を決定することができる。上述のように、１つまたは複数の暗号サービスモジュール、例えば図２の暗号サービスモジュール２７０は、ピアツーピアネットワークの取出しノードに暗号化サービスを提供することができる。起点標識を検索メッセージに追加して、４０６で、受信ノードに送信することができる。

【００４０】

４１２で、取出しユーザを検証するとき、受信ノードは、図２の検索モジュール２９５など任意の適切なプロセスを使用して起点標識を検証することができる。一例では、受信ノードは取出しユーザの公開キーを用いて起点標識の署名を検証することができる。署名サービスを図２に示された暗号サービスモジュール２７０によって提供することもできる。公開キーは検索メッセージから構文解析すること、あるいは適切なキー取出しシステムから取り出すことができる。例えば、取出しキーは取出しユーザノードの公開キーであってもよい。このようにして、構文解析された取出しキーを使用して検索メッセージの起点標識を検証することができる。起点標識が受信ノードで検証できなかった場合は、受信ノードは４１４でエラーメッセージを返すことができる。このエラーメッセージは、４１０で返されるエラーメッセージと同一であっても、異なっていてもよい。場合によっては、起点署名の検証は、検索識別子検証より多くのプロセッサパワーを必要とすることがある。したがって、起点標識は、検索識別子を検証した後で検証することができる。

【００４１】

起点標識をさらに検証するために、受信ノードは起点標識のコンテンツを検査すること

ができる。例えば、署名されたコンテンツは追加の検証規準を提供することができる。例えば、起点標識は、世界時および世界時の署名を含むことができる。受信ノードは、図２の検索モジュール２９５などによって、構文解析された世界時と現在の時刻の差を検証閾値と比較することもできる。時間の差が閾値を越えた場合は、例えばメッセージがタイムアウトしており、４１４で、受信ノードはエラーメッセージを返すことができる。このエラーメッセージは、４１０で返されたエラーメッセージと同一でも、異なっていてもよい。起点標識が検証された場合は、４１６に移り、受信ノードは上述のキー検出メッセージを作成することができる。

【００４２】

場合によっては、例えば信頼できるドメインでは、格納されたキー／値ペアの暗号化されていないペイロードでも十分にセキュアなことがある。より詳細には、暗号化されていないペイロード情報を格納するストレージノード（群）は、データに対するリスクが十分に低いものと見なすことができる。例えば、多数のユーザを有する大規模ネットワークにおいては、特定のデータのためのストレージノードとして攻撃者が選択される可能性は極めて低い可能性がある。この場合、暗号化されていないペイロード情報の保護には、ある部分、ハッシュテーブルのその部分に格納されるペイロード情報に対するストレージノードの無関心さを利用することができる。

【００４３】

ある場合には、ペイロード情報を暗号化して、例えばストレージノードおよび／または攻撃者による無許可のアクセスに対する保護を提供することができる。図３の方法３００を参照すると、３１２で、登録ノードはペイロードを暗号化することができる。ペイロードを暗号化するためには、登録ノードは、ペイロードを暗号化しその復号を可能にするのに適した任意の適切な暗号化技術を使用することができる。暗号化技術には、これらに限定されるものではないが、対称暗号化キー、非対称暗号化キー、公開／秘密キーペアの一方などを使用することができる。上述のように、暗号化サービスは、図２に示した１つまたは複数の暗号サービスモジュール２７０によって提供することができる。

【００４４】

３１２でペイロードを暗号化する方法の一例が図５に示されている。５０２で、登録ノードはグループキーを生成することができる。グループキーは、例えばランダムまたは所定の、対称または非対称の任意の適切な暗号化キーとすることができる。次に、５０４で、登録ノードは生成されたグループキーを使用してペイロードを暗号化することができる。

【００４５】

アクセスリストで識別された取出しユーザがペイロードを復号できることを保証するために、登録ノードは登録メッセージ中にグループキーを含めることができる。グループキーは、ピアツーピアネットワークのストレージノードに格納されたキー／値ペアの値の一部として含めるなど、任意の適切な方法で登録メッセージに含めることができる。しかし、グループキーを、暗号化されたペイロードと同じ記憶位置（例えば、キー／値ペア）に含めることにより、リスクが許容レベルを越えて増大する可能性がある。より詳細には、ペイロードの暗号化は、ペイロードの復号に使用できるグループキーと共に格納された場合にはセキュアでなくなることがある。

【００４６】

グループキーを保護するために、５０６で、登録ユーザは任意の適切な暗号化技術および任意の適切な暗号キーを使用して、グループキーを暗号化することができる。図２を参照すると、暗号サービスモジュール２７０を使用してグループキーを暗号化することができる。一例では、グループキーを、アクセスリストで識別されたユーザの個人公開キーを使用して暗号化することができる。次に、この暗号化されたグループキーは、５０８で、アクセスリストに含まれたそのユーザの検索識別子と関連づけることができる。アクセスリストで複数のユーザが識別された場合は、この方法は５０６に戻り、リスト中で識別された各ユーザの公開キーを用いてグループキーを暗号化し、暗号化されたグループキーを

各対応するユーザと関連づけることができる。各暗号化されたグループキーを、５１０で、アクセスリストのその対応するユーザに関連する登録メッセージ中に含めることができる。

【００４７】

インスタントメッセンジャアプリケーションをサポートするピアツーピアネットワークは、ピアツーピアネットワークに情報を登録し、その情報を取り出す場合の一例である。ピアツーピアネットワークのプロトコルに従って、各アクティブノードにノード識別子が割り当てられる。参加ユーザ、例えばＪａｎｅ　Ｄｏｅは、自分の登録識別子をピアツーピアネットワークに登録して、自分の通信アドレスおよび／またはリッチプレゼンスデータを使用可能にすることができる。Ｊａｎｅ　Ｄｏｅのノードは登録メッセージを構成することができる。登録メッセージ６００の一部を示す概略図の例が図６に示されている。登録メッセージ６００は、値６２０に関連する登録キー６１０を含むことができる。インスタントメッセンジャの例における登録キー６１０を、インターネット電子メールアドレスなどの個人識別子や「オンライン」の指示などのアプリケーションデータのハッシュとして形成することができる。この場合、Ｊａｎｅ　Ｄｏｅの登録キー６１０を、ＳＨＡ（ｊａｎｅ．ｄｏｅ@ｍｉｃｒｏｓｏｆｔ．ｃｏｍ－ｏｎｌｉｎｅ）として表すことができる。値６２０は、ペイロード６２４、アクセスリスト６２６、および／または１つまたは複数のグループキー６２８などの１つまたは複数の部分からなる組合せとすることができる。

【００４８】

値のペイロード部分６２４をローカルアプリケーション、例えばインスタントメッセンジャローカルアプリケーションなどからアクセスすることができる。インスタントメッセンジャの例におけるペイロード６２４には、使い易い名前（例えば、Ｊａｎｅ　Ｄｏｅ－ＧＩ　Ｊａｎｅ！）、現在の活動標識（例えば、Ｑｕａｋｅ動作中）、および／またはＩＰアドレス（例えば、１．２．３．４．５０３０）などのＪａｎｅ　Ｄｏｅの現在のメッセンジャエンドポイントなどを含めることができる。

【００４９】

キー／値ペアを格納することができるノード、および／または他の無許可ノードからペイロードデータへのアクセスを制限するために、Ｊａｎｅのノードはグループキー（ＧＫ）６２８を生成し、そのグループキーを用いてペイロードデータを暗号化することができる。暗号化されたペイロードデータは、｛ＧＫ｝（Ｊａｎｅ　Ｄｏｅ－ＧＩ　Ｊａｎｅ，‘ｐｌａｙｉｎｇ　Ｑｕａｋｅ’，１．２．３．４．５０３０）と表すことができる。

【００５０】

ピアツーピアネットワークに格納されるペイロードデータへのアクセスを制限するために、Ｊａｎｅ　Ｄｏｅは、彼女のペイロードデータにアクセスすることができるピアツーピアネットワークメンバーの１人または複数のユーザからなるアクセスリスト６２６を形成することができる。キー／値ペアへのアクセスが許可されたユーザは、検索識別子６３０によって識別することができる。例えばＪａｎｅは、彼女の母親Ｊｏａｎ　Ｄｏｅおよび夫Ｊｏｈｎ　Ｄｏｅが、彼女のペイロードデータ、例えばインスタントメッセンジャアプリケーションのコンタクトおよび／またはプレゼンスデータにアクセスすることを望むことがある。したがって、ＪａｎｅはＪｏａｎ　Ｄｏｅに対する検索識別子とＪｏｈｎ　Ｄｏｅに対する検索識別子を含むアクセスリストを生成することができる。

【００５１】

アクセスリスト６２６およびグループキー（群）６２８の一例を示すテーブルが図７に示されている。図７の例示のテーブル６２６において、このアクセスリストテーブルは２つの列７１０、７２０を含むことができる。第１の列７１０は、検索識別子を含むことができる。この検索識別子は、登録されたキー／値ペアにアクセスすることが許可されたノードおよび／または人の識別子のハッシュであってもよい。図示の例では、第１の列７１０はＪｏａｎ　Ｄｏｅの個人識別子のハッシュ７１２、およびＪｏｈｎ　Ｄｏｅの個人識別子のハッシュ７１４を含むことができる。より詳細には、Ｊｏａｎ　ＤｏｅおよびＪｏ

ｈｎ　Ｄｏｅの検索識別子はそれぞれ、各ユーザの公開キーＰＫのハッシュ、例えばＳＨＡ（ＰＫJoan）およびＳＨＡ（ＰＫJohn）とすることができる。テーブル７００の第２列７２０は図６の暗号化されたグループキーＧＫ６２８を含むことができる。このグループキーは、関連するユーザの公開キーを用いて暗号化することができる。図７に示された例では、グループキー７２２はＪａｎｅの公開キーＰＫJoanによって暗号化されたグループキー６２８とすることができ、グループキー７２４はＪｏｈｎの公開キーＰＫJohnによって暗号化されたグループキー６２８とすることができる。このようにして、暗号化されたグループキー７２２は検索識別子７１２と関連づけることができ、同様に暗号化されたグループキー７２４は検索識別子７１４と関連づけることができる。

【００５２】

次に、Ｊａｎｅはキー／値ペアをピアツーピアネットワークに登録することができる。より詳細には、メッセージを、キー／値ペアの登録キーに最も近いノード識別子が割り当てられたピアツーピアネットワークのノードにルーティングしかつ格納することができる。また、キー／値ペアを複製し、キー／値ペアの登録キーの識別子に隣接するかまたは類似する追加のノード、例えばストレージノードのリーフセットに格納することができる。

【００５３】

Ｊａｎｅにインスタントメッセージを送信するために、ユーザは検索メッセージを生成して、Ｊａｎｅのコンタクト情報および／またはピアツーピアネットワーク内でのステータスを確認することができる。図８は検索メッセージ８００の一例を示す概略図である。ユーザは値６２０を登録するために使用される登録キー６１０を指定することができる。より詳細には、ユーザはユーザ識別子およびアプリケーションデータのハッシュを指定することができる（例えば、ＳＨＡ（ｊａｎｅ．ｄｏｅ@ｍｉｃｒｏｓｏｆｔ．ｃｏｍ－ｏｎｌｉｎｅ））。ユーザはまた、検索識別子８１０を提供することもできる。例えば、Ｊｏａｎ　Ｄｏｅが検索メッセージ８００を構成している場合は、検索識別子は公開キーのハッシュ、例えばＳＨＡ（ＰＫJoan）とすることができる。他の例では、取出しユーザによって提供される検索識別子８１０は、そのユーザのハッシュされていない公開キーとすることもできる。取出しユーザはまた、起点標識８２０を提供することもできる。例えば、起点標識はＪｏａｎの秘密キーを用いて暗号化された世界時、例えばＰＶJoan（世界時）とすることができる。ユーザは、ピアツーピアネットワーククラウドを介して、指示された登録キーに最も近いノード識別子を有するノードに検索メッセージを転送することができる。

【００５４】

受信ノードは登録キー６１０を構文解析し検査して、そのキーがそのノードに登録されているかどうかを判定することができる。登録されていない場合は、受信ノードはエラーメッセージを送信することができる。登録キーが見つかった場合には、受信ノードは検索識別子８１０を、格納されているキー／値ペアについての図６のアクセスリスト６２６と比較することができる。検索識別子８１０がハッシュされておらず、アクセスリストの検索識別子がハッシュされている場合は、受信ノードは、検索識別子８１０をハッシュしてからアクセスリストと比較することができる。検索識別子８１０がアクセスリスト６２６に存在しない場合は、受信ノードはエラーメッセージを送信することができる。

【００５５】

検索識別子が存在する場合は、受信ノードは検索メッセージの起点標識を検証することができる。より詳細には、受信ノードは取出しユーザの公開キーを使用して起点標識８２０の署名を検証することができる。上述のように、起点標識を取出しユーザの秘密キーを用いて署名することができる。署名を検証するために、取出しユーザの公開キーは、任意の適切なプロセスを用いて、検索メッセージ、取出しユーザ、サードパーティなどから取り出すことができる。秘密キーによって署名されたコンテンツは有効な世界時であることを検証することができる。さらに、提供された世界時は、検索メッセージに対する時間境界閾値を越えないことを検証することができる。起点標識が有効でない場合は、受信ノードはエラーメッセージを送信することができる。起点標識が有効な場合、受信ノードは、

提供された検索識別子に関連する登録キー６１０、暗号化されたペイロード６２４、および暗号化されたグループキー６２８を含むキー検出メッセージを構成することができる。取出しユーザ、ここではＪｏａｎ　Ｄｏｅは、キー検出メッセージを受信し、暗号化されたペイロードおよび暗号化されたグループキーを構文解析することができる。Ｊｏａｎ　Ｄｏｅのノードは、彼女の秘密キー（ＰＶJoan）を用いて、グループキー６２８を復号する（グループキー６２８は、上述の例ではＪｏａｎの公開キー（例えば、ＰＫJoan）を用いて暗号化されている）。次に、Ｊｏａｎのノードは、グループキー６２８を使用して、ペイロード６２４を復号し、ペイロードを取り出すことができる。例えば、彼女の娘Ｊａｎｅのコンタクト情報およびプレゼンスデータを確認することができる。

【００５６】

ときおり、登録ユーザはキー／値ペアのアクセスリストを修正することができる。任意の適切な方法を使用してアクセスリストを修正することができる。例えば、登録ユーザは、キー／値ペアを登録解除し、更新されたアクセスリストを用いてキー／値ペアを再登録することができる。例えば、Ｊａｎｅがアクセスリストから彼女の母を削除した場合は、Ｊｏａｎ　Ｄｏｅがピアツーピアネットワーク内で彼女の娘を検索しようと試みた際に、彼女は、例えば「キーが見つかりません」などのエラーメッセージを受信することがある。キー／値ペアを登録解除する要求は、アクセス制限される場合がある。例えば、登録ユーザノードだけがキー／値ペアの登録解除を実施することができる。他の例では、アクセスリストで識別されたユーザに、キー／値ペアの登録解除を実施する権限を与えることができる。登録解除アクセスリストは、上で論じた取出しアクセスリストと同一であっても異なっていてもよい。

【００５７】

ピアツーピアネットワークにデータを登録し、そのデータを取り出すための上記の方法は、あるレベルの情報セキュリティを提供する。あるキー／値ペアに対するアクセスリストを知っているユーザは、登録ノードとストレージノード（群）である。アクセスリストは公開キーを含むことはできるが、コンタクト情報を含むことはできないので、アクセス権を有するユーザの識別の確定を困難にすることができる。アクセスを許可されたユーザの識別は、ユーザ識別子のハッシュである検索識別子を生成することによってさらに隠蔽することもできる。

【００５８】

登録されたキー／値ペアを格納するためのストレージノードとして攻撃者が選択される確率は、特にかなり大規模なネットワークにおいては低いものと考えられる。例えば、登録メッセージがストレージノードにルーティングされるとき、ｌｏｇ（Ｎ）台のノードがそのメッセージを受信する可能性がある。ただし、Ｎはピアツーピアネットワーク内のノードの数である。ｋ台のノードがこのキー／値ペアの登録を格納できるものとする。ただし、ｋはピアツーピアネットワークの複製ファクタによって決まる１以上の数である。このとき、攻撃者がストレージのための登録を受信する可能性は（ｌｏｇ（Ｎ）＋ｋ）／Ｎになる。ノードの数が５，０００，０００ユーザ、底が１０、登録が４ノード間で複製される場合は、攻撃者が登録を受信する（したがって、登録ユーザがオンライン中であることを知る）確率は、ほぼ０．００００３である。

【００５９】

ストレージノードは、ハッシュテーブルのその部分に格納されたキー／値ペアを公開することにより、宛先不定の攻撃を提供する可能性がある。ストレージノードが格納されたデータのいずれにも関心がない場合でも、キー／値ペアを公開することによって、他の攻撃者がそれらを取り出すことが可能になり、格納されたデータおよび／または登録ユーザへの間接的な攻撃が生成されることになる。上述の方法は、ペイロード情報を暗号化することによって宛先不定の攻撃の影響を低減することができる。詳細には、宛先不定の攻撃者は、登録されたユーザがオンラインかどうかを単に登録の存在だけで判断することができるが、コンタクト情報や他のリッチプレゼンスデータは、登録ユーザのプライバシーを保護するためにグループキーを用いて暗号化することができる。さらに、ピアツーピアネ

ットワーク内部でのユーザの認証によって宛先不定の攻撃を阻止することもできる。あるノードが（例えば、キー／値ペアを公開するなど）ネットワーク運営の規則を破った場合には、ピアツーピアネットワークに参加するためのノードの証明書を無効にすることができる。攻撃を受けたユーザノードまたは情報の完全性が失われたユーザノードに新しい識別情報、例えばノード識別子および／または個人識別子を提供することによって、攻撃を阻止することもできる。

【００６０】

上述のストレージシステムを、ハッシュテーブルのキー／値ペアの全体または一部に対する特権メンバーのアクセスを許可するように修正することができる。より詳細には、特権メンバーに、キー／値ペアの全てまたは一部へのアクセスを許可することができる。一例では、特権メンバーの識別子を、要求されたキー／値ペアへのアクセス権を有する有効なユーザとしてストレージノードによって常に検証することができる。例えば、受信ノードは提供された検索識別子と、登録されたキー／値ペアに関連するアクセスリストおよび全てのキー／値ペアへのアクセス権を有する特権メンバーの検索識別子を含むネットワークの特権メンバーのアクセスリストとを比較することができる。他の例では、特権メンバーの識別子を、ピアツーピアネットワークに登録されたキー／値ペアのアクセスリストのすべて、または少なくとも一部に追加することができる。例えば、特権メンバーの検索識別子は、ピアツーピアネットワークに登録された各アクセスリストに自動的に追加することができる。一例では、登録ユーザを、そのユーザによって登録される任意のメッセージのアクセスリストに自動的に追加することができる。

【００６１】

アクセスリストが検索識別子を含んでいない（例えば、登録ユーザによって許可ユーザが提供されていない）場合は、ピアツーピアストレージシステムは任意の適切なデフォルトの動作をとることができる。例えば、アクセスリストが提供されていない場合には、すべての取出しユーザを有効にして関連する格納されたキー／値ペアを取り出せるようにすることができる。あるいは、アクセスリストが提供されていない場合は、登録ユーザおよび／または特権メンバーだけを有効ユーザとして検証して、格納されたキー／値ペアを取り出せるようにすることができる。

【００６２】

本明細書に記載の本発明の実施形態は、１つまたは複数のコンピュータシステムにおける論理ステップとして実装することができる。本発明の論理動作を、（１）１つまたは複数のコンピュータシステムで実行される一連のプロセッサ実装されたステップとして、また（２）１つまたは複数のコンピュータシステム内部で相互接続されたマシンモジュールとして実装することができる。実装は、本発明を実装するコンピュータシステムの性能要件に応じて選択されるものである。したがって、本明細書に記載の本発明の実施形態を構成する論理動作は、オペレーション、ステップ、オブジェクト、モジュールなどと様々に呼ばれている。

【００６３】

上記の明細、例、およびデータは、本発明の例示的実施形態の構造および使用についての完全な記述を提供するものである。本発明の趣旨および範囲を逸脱することなく、本発明の多数の実施形態を構成し得るので、本発明は添付の特許請求の範囲によって定められるものとする。

【図面の簡単な説明】

【００６４】

【図１】ピアツーピアネットワークのノードを実装するためのコンピュータシステムの一例を示す概略図である。

【図２】ピアツーピアネットワークおよびピアツーピアネットワークストレージシステムの一例を示す概略図である。

【図３】ピアツーピアネットワークにデータを登録する方法の一例を示す流れ図である。

【図４】ピアツーピアネットワークのデータを取り出す方法の一例を示す流れ図である。

【図５】図３の登録データのペイロードを暗号化する方法の一例を示す流れ図である。
【図６】ピアツーピアネットワークの登録メッセージの一例を示す概略図である。
【図７】図６のアクセスリストの一例としてのテーブルを示す図である。
【図８】ピアツーピアネットワークにおける検索メッセージの一例を示す概略図である。
【００６５】
１０２　処理ユニット
１０４　システムメモリ、揮発性、不揮発性
１０６　破線
１０８　リムーバブル記憶装置
１１０　固定記憶装置
１１２　通信接続
１１４　入力装置（群）
１１６　出力装置（群）
２１１　ネットワーク
２１０　ノード
２１１　ネットワーク
２３０　ノード
２４０　登録プロセス
２５０　検索プロセス
２６０　ハッシュテーブル
２６５　ルーティングテーブル
２７０　暗号化サービスモジュール
２８０　ローカルアプリケーション
２９０　登録モジュール
２９５　検索モジュール
３００　方法
３０２　登録キーを決定する
３０４　ペイロードを作成する
３０６　アクセスリストを決定する
３０８　登録メッセージを構成する
３１０　登録メッセージを送信する
３１２　ペイロードを暗号化する
３１４　ノード識別子を割り当てる
３１６　ノード識別子を割り当てる
４００　例示的方法
４０２　キーを決定する
４０４　検索識別子を決定する
４０６　検索メッセージを送信する
４０８　検索メッセージは検証されたか？
４１０　エラーメッセージを送信する
４１２　取出しユーザは検証されたか？
４１４　エラーメッセージを送信する
４１６　キー検出メッセージを作成する
４１８　キー検出メッセージを送信する
４２０　起点標識を決定する
５０２　グループキーを生成する
５０４　ペイロードを暗号化する
５０６　グループキーを暗号化する
５０８　暗号化されたグループキーをユーザと関連づける
５１０　暗号化されたグループキーを登録メッセージに含める

６００　登録メッセージ
６１０　登録キー
６２４　ペイロード
６２６　アクセスリスト
６２８　グループキー（群）
６３０　検索識別子
６２６　アクセスリスト
６２８　グループキー
７００　テーブル
７１０　第１の列
７１２　検索識別子
７１４　検索識別子
７２０　第２列
７２２　グループキー
７２４　グループキー
８００　検索メッセージ
６１０　登録キー
８１０　検索識別子
８２０　起点標識