(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2012-518329
(P2012-518329A)
(43)公表日　平成24年8月9日(2012.8.9)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5J104
G06F 21/20	(2006.01)	G06F	21/20	131E	
G06F 21/24	(2006.01)	G06F	21/24	166A	

審査請求 未請求　予備審査請求 未請求　（全 39 頁）

(21)出願番号　特願2011-550169 (P2011-550169)
(86)(22)出願日　平成22年2月4日 (2010.2.4)
(85)翻訳文提出日　平成23年8月16日 (2011.8.16)
(86)国際出願番号　PCT/US2010/023239
(87)国際公開番号　WO2010/093558
(87)国際公開日　平成22年8月19日 (2010.8.19)
(31)優先権主張番号　61/152,956
(32)優先日　平成21年2月16日 (2009.2.16)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　12/491,403
(32)優先日　平成21年6月25日 (2009.6.25)
(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　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　ラウル　ブイ．オーラドカー
アメリカ合衆国　９８０５２－６３９９　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－インターナショナル　パテンツ内

最終頁に続く

(54)【発明の名称】信頼済みクラウドコンピューティングおよびサービスに関するフレームワーク

(57)【要約】
デジタルエスクローのパターンを、クラウドに記憶されるデータのための検索可能な暗号化技術を含むネットワークデータサービスに提供して、複数のエンティティにわたって信頼を分配して、単一点情報漏洩を回避する。一実施形態において、鍵ジェネレータ、暗号化技術プロバイダ、およびクラウドサービスプロバイダを、それぞれ別個のエンティティとして提供して、データの発行者が、秘密裏に（暗号化された）データをクラウドサービスプロバイダに発行すること、およびその後、暗号化されたデータを、そのデータを要求するサブスクライバに、サブスクライバの要求に応答して生成される鍵情報内に符号化されるサブスクライバ識別情報（例えばサブスクライバのロール）に基づき選択的に与えることを可能にする。

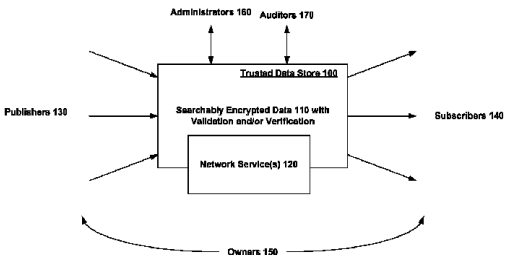


FIG. 1

【特許請求の範囲】
【請求項１】
少なくとも部分的に暗号化技術プロバイダにより分散される少なくとも１つの暗号化コンポーネント（４１０）であって、データの発行またはデータのサブスクライブの少なくとも一方のための鍵情報を生成する鍵ジェネレータ（４００）から独立して実装され、前記少なくとも１つの暗号化コンポーネント（４１０）は、前記鍵ジェネレータ（４００）により生成される前記鍵情報に基づき、少なくとも１つの検索可能な暗号化アルゴリズムまたは検索可能な復号アルゴリズムを実行するように構成される少なくとも１つのプロセッサを含む、暗号化コンポーネント（４１０）と、
ネットワークサービスプロバイダ（４２０）であって、前記鍵ジェネレータ（４００）および前記少なくとも１つの暗号化コンポーネント（４１０）から独立して実装され、前記少なくとも１つの暗号化コンポーネント（４１０）により暗号化されるデータに対してネットワークサービスを実装するように構成される少なくとも１つのプロセッサを含む、ネットワークサービスプロバイダ（４２０）と
を備えたことを特徴とするシステム。
【請求項２】
前記鍵情報は、前記少なくとも１つの暗号化コンポーネント（４１０）により暗号化されるデータに対するアクセス特権を定義する機能情報を備えたことを特徴とする請求項１に記載のシステム。
【請求項３】
前記機能情報を遅延バインドして、最新のアクセス特権を所与のサブスクライバに与えることを特徴とする請求項２に記載のシステム。
【請求項４】
前記ネットワークサービスプロバイダ（４２０）から、サブスクライバにより取り出されるデータ項目を検証して、前記ネットワークサービスから正しい項目を取り出したことを、サブスクライバに証明することを特徴とする請求項１に記載のシステム。
【請求項５】
前記ネットワークサービスプロバイダ（４２０）から、サブスクライバにより取り出される前記データ項目の内容を照合して、前記データ項目の内容に障害が無いことを、サブスクライバに証明することを特徴とする請求項１に記載のシステム。
【請求項６】
データサブスクライバ、またはデータの発行者は、匿名の認証情報に基づき、それぞれコンテンツをサブスクライブして、または発行して、個人情報を露出することなく特権が与えられるサブスクライバまたは発行者のロールを判定することを特徴とする請求項１に記載のシステム。
【請求項７】
前記ネットワークサービスプロバイダは、選択的にアクセス可能な暗号化されたデータ（１１０）を記憶する少なくとも１つのデータストア（１００）をさらに含み、少なくとも１つのサブスクライバ（１４０）は、前記暗号化されたデータ（１１０）の特定のサブセットをサブスクライブして、第１の独立エンティティ（４０１）は、少なくとも１つのサブスクライバに関連する識別情報に基づき暗号化鍵情報を生成して、第２の独立エンティティ（４１１）は、前記第１の独立エンティティ（４０１）により生成される暗号化鍵情報に基づき、前記特定のサブセットの復号を実行することを特徴とする請求項１に記載のシステム。
【請求項８】
前記少なくとも１つのサブスクライバ（１４０）は、前記暗号化されたデータのサブセットを監査する少なくとも１つの監査者であることを特徴とする請求項７に記載のシステム。
【請求項９】
前記少なくとも１つのサブスクライバ（１４０）は、前記暗号化されたデータに影響を

与える処理を管理または監視する少なくとも１つの管理者であることを特徴とする請求項７に記載のシステム。
【請求項１０】
データをサブスクライブする方法であって、
少なくとも１つのサブスクライバデバイスからの検索可能に暗号化されたデータのサブセットの要求に応答して、前記少なくとも１つのサブスクライバデバイスに関連する識別情報に基づき暗号化鍵情報を生成する鍵生成コンポーネントから、前記暗号化鍵情報を受信すること（３１０）と、
前記暗号化鍵情報において定義される少なくとも１つサブスクライバデバイスに与えられる特権の機能として、前記暗号化されたデータのサブセットを復号すること（３２０）と
を含む方法。
【請求項１１】
前記受信すること（３１０）は、前記少なくとも１つのサブスクライバデバイスのロールに基づいて前記暗号化鍵情報を生成する制御の別個の領域において操作する鍵生成コンポーネントから暗号化鍵情報を受信することを備えたことを特徴とする請求項１０に記載の方法。
【請求項１２】
前記受信すること（３１０）は、前記少なくとも１つのサブスクライバデバイスのロールを監査する機能として、暗号化鍵情報を受信することを備えたことを特徴とする請求項１１に記載の方法。
【請求項１３】
前記受信すること（３１０）は、前記少なくとも１つのサブスクライバデバイスの管理者のロールの機能として暗号化鍵情報を受信することを備えたことを特徴とする請求項１１に記載の方法。
【請求項１４】
暗号化されたデータのサブセットのデータ項目について取得可能性の証明の要求を、前記少なくとも１つのサブスクライバデバイスから受信すること（３０２０）と、
前記少なくとも１つのサブスクライバデバイスにより要求される前記暗号化されたデータのサブセット内の前記データ項目が正しいことを、前記サブスクライバデバイスに証明する情報を生成すること（３０１２）と、
をさらに備えたことを特徴とする請求項１０に記載の方法。
【請求項１５】
前記少なくとも１つのサブスクライバデバイスによる要求より前に、前記暗号化されたデータのサブセットは干渉されなかったという証明を求める要求を受信すること（２７２０）と、
前記少なくとも１つのサブスクライバデバイスによる要求より前に、前記暗号化されたデータのサブセットが干渉されなかったということをサブスクライバデバイスに証明する情報を生成すること（２７１２）と
をさらに備えたことを特徴とする請求項１０に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、信頼済みクラウドコンピューティングとデータサービスに関するフレームワークを参加者(単数または複数）に提供すること、およびフレームワークに基づく対応するシナリオに関する。
【背景技術】
【０００２】
ある従来のシステムに関する背景技術として、コンピュータデバイスは従来、デバイスにローカルなアプリケーションおよびデータサービスを実行してきた。そのような場合、

データがアクセス、処理、記憶、キャッシュなどされると、データは、ローカルバス、インターフェース、および他のデータ経路にわたって伝達され得るが、デバイスのユーザは、デバイスそのものが無くなったり盗まれたりする場合を除いて、ユーザのデータの干渉または露出を心配する必要は無かった。

【０００３】

しかし、オンラインおよびクラウドのサービスの発展と共に、アプリケーションおよびサービスは、ユーザのデバイスに代わっていくつかまたは全ての所与のサービスを実行するネットワークプロバイダにますます移行されてきている。そのような場合、ユーザのデータがサービスに対してアップロードされる時、サービスによって格納される時、またはサービスから検索される時に、ユーザのデータに誰がアクセス可能であるのか、または、より悪い可能性としては、干渉可能であるのか、についてユーザは懸念することになり得る。要するに、ユーザのデバイスのデータが、物理的所有の領域を出て、およびユーザから離れてネットワーク環境に入ると、ユーザの物理的所有から一旦出たデータを取り扱うことに対する懸念が自然に高じる。従って、クラウドサービスへの信頼、およびクラウドサービスに関連するデータの取り扱いを増大させることが望ましい。

【０００４】

今日のデバイスおよびクラウドサービスについての上述の欠陥は、単に従来のシステムのいくつかの問題の要旨を与えることを意図しており、および包括的であることは意図していない。最先端技術の他の問題、およびいくつかの種々の非制限的な実施形態の対応する利点が、以下の発明を実施するための形態を精査することによりさらに明らかになるであろう。

【発明の概要】

【０００５】

本明細書において簡略化された概要を提供して、より詳細な記述および添付の図面において記載される、例示の非制限的な実施形態の種々の態様についての基本的または一般的理解を可能にする助けとなる。しかし、本概要を、広範囲または包括的な要旨として意図しない。代わりに、本概要の唯一の目的は、例示の非制限的なある実施形態に関連するある概念を、以下に続く種々の実施形態のより詳細な説明に対する前置きとして、簡略化された形式で表すことである。

【０００６】

デジタルエスクローのパターンを、クラウドに記憶されるデータのための検索可能な暗号化技術を含むネットワークデータサービスに提供して、複数のエンティティにわたって信頼を分配して、単一点情報漏洩(single point of data compromise)を回避する。一実施形態において、鍵ジェネレータ、暗号化技術プロバイダ、およびクラウドサービスプロバイダを、それぞれ別個のエンティティとして提供して、データの発行者が、秘密裏に（暗号化された）データをクラウドサービスプロバイダに発行すること、および次いで、暗号化されたデータを、そのデータを要求するサブスクライバに、サブスクライバの要求に応答して生成される鍵情報内に符号化されるサブスクライバ識別情報に基づき選択的に与えることを可能にする。

【０００７】

信頼済みクラウドサービスのエコシステムに対する１組のシナリオが明らかになり、ならびにこれらのシナリオおよび種々の他の実施形態を、以下により詳細に記載する。

【図面の簡単な説明】

【０００８】

種々の非制限的な実施形態を、添付の図面を参照してさらに記載する。

【０００９】

【図１】実施形態に従う信頼済みクラウドサービスのフレームワークまたはエコシステムの例示の非制限的なブロック図である。

【図２】信頼済みクラウドサービスのエコシステムに従ってデータを発行する例示の非制限的な処理を示すフロー図である。

【図３】信頼済みクラウドサービスのエコシステムに従ってデータをサブスクライブする例示の非制限的な処理を示すフロー図である。
【図４】信頼済みエコシステムにおける、鍵生成センタ、暗号化技術プロバイダ、およびクラウドサービスプロバイダ４２０の分離を示す例示のエコシステムを示す図である。
【図５】企業のクラウドサービスを実行する信頼済みエコシステムのさらなる利点を示す別のアーキテクチャの図である。
【図６】信頼済みクラウドサービスのエコシステムに従う、ストレージ抽象化層６１０を介した異なるストレージプロバイダの適応を示す別のブロック図である。
【図７】種々のストレージプロバイダのストレージの詳細を抽象化するストレージ抽象化サービスに関連するストレージのさらなる態様を示す図である。
【図８】信頼済みクラウドサービスのエコシステムにおける種々の異なる参加者を示す別のブロック図である。
【図９】異なる要素を異なるエンティティまたは同じエンティティにより提供可能である信頼済みクラウドコンピューティングシステムの、例示の非制限的な実装のある層の代表的な図である。
【図１０】遅延バインドを用いてデータへの発行者制御の選択的なアクセスを提供できるように、デジタルセーフアプリケーションに文書を発行する、例示の非制限的な処理を示すフロー図である。
【図１１】遅延バインドを用いてデータへの発行者制御の選択的なアクセスを提供できるように、デジタルセーフアプリケーションに文書を発行する、例示の非制限的なシステムを示すブロック図である。
【図１２】デジタルセーフのシナリオに従ってデータをサブスクライブする、例示の非制限的な処理のフロー図である。
【図１３】デジタルセーフのシナリオに従ってデータをサブスクライブする、例示の非制限的なシステムのブロック図である。
【図１４】デジタルエスクローのパターンを使用して、１つまたは複数のデータセンタを介して企業の安全なエクストラネットを実装する、信頼済みクラウドサービスのエコシステムの例示の非制限的な実装を示す図である。
【図１５】クラウドサービスプロバイダにより記憶される暗号化されたデータへの選択的なアクセスがサブスクライバに与えられる、信頼済みクラウドサービスのエコシステムに基づく別の例示の非制限的なシナリオを示すフロー図である。
【図１６】アプリケーションの応答がユーザの認証情報に基づきサブスクライバに対して調整可能であることを示す別のフロー図である。
【図１７】単一の集団または複数の集団に対して実装可能な、安全なレコードアップロードのシナリオを示す別のフロー図である。
【図１８】信頼済みクラウドサービスのエコシステムにより可能にされた、例えば、単一の集団による自動検索のための、検索可能に暗号化されたデータストア全体にわたるロールベースのクエリの例示の非制限的な実装を示すさらに別のフロー図である。
【図１９】１つまたは複数のシナリオに従う、企業、鍵生成センタ、およびクラウドサービスプロバイダの間における信頼済みクラウドサービスエコシステムの実装のブロック図である。
【図２０】企業が、その暗号化されたデータのいくつかへのアクセスを外部の企業に提供する、複数の集団の共同のシナリオを示すフロー図である。
【図２１】複数の企業間における複数の集団の自動検索のシナリオを示すフロー図である。
【図２２】１つまたは複数のシナリオに従う、複数の企業、鍵生成センタ、およびクラウドサービスプロバイダの間における信頼済みクラウドサービスエコシステムの実装のブロック図である。
【図２３】信頼済みクラウドサービスに実装可能な例示の非制限的なエッジコンピュータネットワーク（ＥＣＮ）技術を示す図である。

【図２４】信頼済みクラウドサービスエコシステムに従う、鍵生成センタの１つまたは複数の任意選択的な態様を示すブロック図である。
【図２５】一実施形態において、検証、例えば、データ所有の証明を信頼済みデータサービスの提供に組み込むことを示す図である。
【図２６】一実施形態において、検証、例えば、データ所有の証明を信頼済みデータサービスの提供に組み込むことを示す図である。
【図２７】信頼済みサービスエコシステムに従う、データサービスのデータの例示の検証を示すブロック図である。
【図２８】一実施形態において、照合、例えば、取得可能性の証明を信頼済みデータサービスの提供に組み込むことを示す図である。
【図２９】一実施形態において、照合、例えば、取得可能性の証明を信頼済みデータサービスの提供に組み込むことを示す図である。
【図３０】信頼済みサービスエコシステムに従う、データサービスのデータの例示の検証を示すブロック図である。
【図３１】サービス自体の提供とは独立して、サービスの使用に適用可能な１組の異なる条件に基づき、発行者およびサブスクライバが使用する、複数の異なるオーバレイ業、またはデジタルエスクロー業(overlays or digital verticals)の提供を示すブロック図である。
【図３２】本明細書に記載される種々の実施形態を実装可能な例示の非制限的なネットワーク化された環境を表すブロック図である。
【図３３】本明細書に記載される種々の実施形態の１つまたは複数の態様を実装可能な例示の非制限的なコンピュータシステムまたは動作環境で表すブロック図である。
【発明を実施するための形態】
【００１０】
要旨
背景技術において検討したように、ネットワークサービスに送信されるデータは、プライバシー、改ざんの可能性等についての不安感をもたらす原因となり得、すなわち、データをユーザのデバイスからネットワークのアプリケーション、サービス、またはデータストアに送信する時、ユーザには、悪意のある第三者が害を及ぼすことはないという十分な確信が必要である。当然のことながら、ユーザはデータに対する制御を失う。従って、信頼を向上させて、データの発行者および／または所有者が、自身のデータについて物理的な制御を引き渡すことをいとわず、ネットワーク内において、発行者または所有者が、サブスクライバの識別に基づきサブスクライバに特権を与える場合を除いては、自身のデータが非公開で侵害されないままであることを信頼するようにすることが望ましい。
【００１１】
この点において、ネットワークサービスの従来の提供を取り囲む信頼に関する障壁を取り除くために、信頼済みクラウドコンピューティングおよびデータサービスのエコシステムまたはフレームワークを提供して、上記で確認した目的に加え、以下に記載する種々の実施形態において強調される他の利点を達成する。用語「クラウド」サービスは、一般に、サービスを、ユーザのデバイスからローカルに実行するのではなく、むしろ１つまたは複数のネットワークを介してアクセス可能な１つまたは複数のリモートデバイスから配信する概念を言う。ユーザのデバイスは、１つまたは複数のリモートデバイスで何が起きているのかについて詳細を理解する必要が無いので、ユーザのデバイスの観点から言えば、サービスが「クラウド」から配信されるように見える。
【００１２】
一実施形態において、システムには、データを発行またはサブスクライブする鍵情報を生成する鍵ジェネレータが含まれる。暗号化技術プロバイダは、鍵ジェネレータとは独立して実装され、鍵ジェネレータにより生成される鍵情報に基づく検索可能な暗号化／復号化アルゴリズム(単数または複数）を実装する。加えて、ネットワークサービスプロバイダは、鍵ジェネレータおよび暗号化技術プロバイダとは独立して実装され、暗号化技術プ

ロバイダにより暗号化されるデータについてのネットワークサービスを提供する。

【００１３】

検索可能な暗号化／復号化アルゴリズム(単数または複数）については、１つまたは複数の暗号化技術プロバイダにより実装される検索可能公開鍵暗号（ＰＥＫＳ）のスキームが、任意の所与のメッセージＷに対して、トラップドアＴＷを生成して、ＴＷは、所与の暗号文がＷの暗号化であるか否かのチェックを可能にして、ＴＷは平文についての任意の追加の情報を公開しないようにする。以下に記載する種々の実施形態に従って、ＰＥＫＳスキームを使用して、例えば、メッセージテキストなどのデータに含まれるキーワードに基づき、暗号化されたメッセージ等の暗号化データに優先順位をつけたり、フィルタリングしたりすることができる。従って、データの受信者には、対応するキーワード(単数または複数）に対する機能（暗号作成者により「トラップドア」と呼ばれることもある）を解除することにより、キーワード(単数または複数）に関連する暗号化されたデータの一部への選択されたアクセスを与えることができる。このようにして、暗号化されたデータをこれらのキーワードに対してチェックすることが可能であるが、サブスクライバの機能が許可するもの以外には、サブスクライバから取得されるものは無いことが保証される。

【００１４】

誤解を避けるために、本明細書における１つまたは複数の実施形態において、検索可能な暗号化を実装するアルゴリズムとしてＰＥＫＳを開示するが、検索可能な暗号化を達成する様々な代替のアルゴリズムが存在することは理解できるであろう。ＰＥＫＳに対するある例示の非制限的な代替には、例えば、Ｏｂｌｉｖｉｏｕｓ　ＲＡＭが含まれる。従って、用語「検索可能な暗号化」は、本明細書で使用される時、任意の１つの技術に制限されるべきではなく、および従って、広範囲の暗号化技術、または、暗号化されたデータ全体にわたる検索またはクエリの機能性に基づく、サブセットの暗号化されたデータの選択的なアクセスを許可する暗号化技術の組み合わせを言う。

【００１５】

任意選択的に、結果の検証および／または照合を、追加の利点として、エコシステムにおけるサブスクライバおよびデータの発行者に提供することができる。検証は、サブセットのデータを求めるサブスクリプション要求の結果として受信されるデータの項目が、正しいセットの項目であること、すなわち、受信されるべき正しいサブセットのデータを、実際に受信したということを検証する方法を提供する。暗号法における技術は、データ所有の証明(proof of data possession)（ＰＤＰ）であるが、誤解を避けるために、ＰＤＰは単に、実装可能な一実施例のアルゴリズムであり、および同一のまたは同様の目的を達成する他のアルゴリズムを使用することができる。データ所有を証明可能であることまたはデータ所有の証明（ＰＤＰ）は、ストレージサーバが、そのクライアントの潜在的に大きな外部委託されたデータを忠実に記憶しているということを、どのように頻繁に、効率的に、および安全に検証するかについての話題である。ストレージサーバを、セキュリティおよび信頼のどちらについても信頼できないものと仮定する。

【００１６】

結果の照合は、項目そのものの内容をチェックする追加の機構を提供して、すなわち、サブスクリプション要求に関連して受信される項目が、任意の認可されないエンティティにより改ざんされなかったということを確実にする。暗号法における照合の実施例には、データ所有の証明（ＰＤＰ）があるが、誤解を避けるために、ＰＤＰは単に、実装可能な一実施例のアルゴリズムであり、同一のまたは同様の目的を達成する他のアルゴリズムを使用することができる。暗号法において既知の別の技術には、取得可能性の証明(proof of retrievability)（ＰＯＲ）があるが、誤解を避けるために、ＰＯＲは単に、実装可能な一実施例のアルゴリズムであり、同一のまたは同様の目的を達成する他のアルゴリズムを使用することができる。クライアントは対象のファイルＦを完全に復元可能であり、および何の改ざんも発生していない、という意味では、ＰＯＲは、サービスプロバイダまたはデータのホスト（プルーバ）による、クライアント（ベリファイア）に対する、ファイルＦは完全なままであるという、コンパクトな証明である。

【００１７】
追加の選択肢として、エコシステムでは、匿名の認証情報の概念を実装することができ、それにより、発行者は、自身に関する情報を匿名での方法で、重要な詳細を露出させることなくアップロード可能であり、およびサブスクライバは、自身の機能により制限され得、重要な詳細を露出しないように、または発行者によりアップロードされる重要な詳細に対するアクセスを提供しないようにすることができる。このようにして、発行者またはサブスクライバは、第三者に対して望む範囲のみの情報を露出しつつ、システムと対話することができる。
【００１８】
従来のウェブサービスは、変化のないクライアントサーバの配置、およびウェブサービスのデータにアクセスする、変化なく定義されたユーザポリシに制限されてきた。しかし、多くの発行者およびサブスクライバを、絶えず変化しておよび発展している複雑なビジネスと他の関係に従って検討する時、そのような従来のウェブサービスモデルは、十分に柔軟性があり安全であるわけではない。従って、種々の実施形態において、遅延バインドを可能にして、発行者および／またはデータおよびコンテンツの所有者は、サブスクライバ(単数または複数）が誰であるのかに基づき、サブスクライバの機能(単数または複数）に基づき、およびサブスクライバが何を探しているのかに基づき、例えば、データを求める要求において採用されるキーワード(単数または複数）に基づき、暗号化されたコンテンツに対するアクセス特権を変更することができる。従って、サブスクライバの機能を、オンザフライで鍵ジェネレータにより提供される鍵情報内に符号化するので、サブスクライバが何に選択的にアクセス可能であるかは、発行者および／または所有者によるアクセス特権に対する変更と一致して動的に変化する。従って、サブスクライバの特権を、所与の要求に対して、その要求の鍵生成の時に定義して、および従って、常にサブスクライバからの要求について現在のポリシを反映する。
【００１９】
一実施形態において、選択的にアクセス可能な、例えば、検索可能な、暗号化されたデータを露出するデータストアを提供して、それにおいて、少なくとも１つの発行者が、リソース(単数または複数）を表すデータをデータストアに発行する。信頼の悪用の可能性を分散させる場合、第１の独立エンティティが、暗号化鍵情報の生成を実行する。第２の独立エンティティが次に、第１の独立エンティティにより生成された暗号化鍵情報に基づき、記憶する前に、発行されたデータの暗号化を実行する。次に、１組のネットワークサービスまたはクラウドサービスは、リソース(単数または複数）の発行者(単数または複数）または所有者(単数または複数）により与えられる遅延バインドされ選択された特権に基づき、ネットワークサービスに対する所与の要求のための暗号化されたデータに選択的にアクセスする。
【００２０】
他の実施形態において、データストアは、選択的にアクセス可能な暗号化されたデータを記憶して、それにおいて、サブスクライバ(単数または複数）は、指定されるサブセットの暗号化されたデータをサブスクライブする。第１の独立エンティティは、サブスクライバ(単数または複数）に関連する識別情報に基づき暗号化鍵情報を生成して、および第２の独立エンティティは、第１の独立エンティティにより生成される暗号化鍵情報に基づき、指定されるサブセットの復号を実行する。ネットワークサービス(単数または複数）は、サブスクライバ(単数または複数）による要求に応答して、および指定されるサブセットの発行者または所有者により与えられる遅延バインドされ選択された特権に基づき、暗号化されたデータに対する選択的なアクセスを提供する。
【００２１】
この点において、用語、発行者およびサブスクライバは一般に、信頼済みクラウドサービスのデータを、それぞれ発行またはサブスクライブする者を言う。しかし、実際には、信頼済みクラウドサービスのエコシステムおよびデジタルエスクローのパターンの業種、分野、および用途に応じて、発行者およびサブスクライバは、より多くの特定のロール（

役割）をとることができる。例えば、暗号化されたデータストアの監査人は、監査人のロールに基づき、電子メールストア内の一定の不快なキーワードを識別するが、不快なキーワードを含まない電子メールを読むことが禁止される機能等、一定の機能を有することができる。

【００２２】

同様に、信頼済みクラウドサービスのサーバの管理者に対して、サーバにより処理される動作およびデータトランザクションのログを監視することを許可することができるが、同様に任意の顧客の名前またはクレジットカードの情報を見ることを禁止することができる。従って、サブスクライバの識別は、サブスクライバがアクセス可能なデータの種類を制限する基礎とすることができる。

【００２３】

信頼済みエコシステムの種々の非制限的な実施形態を、クラウドサービスの信頼を築くための文脈において本明細書において示すが、本明細書において提供されるエコシステムの信頼の構築は、なおさら一般的なものであり、およびクラウドサービスへの適用に限定されない。むしろ、本明細書に記載される実施形態は、異なるサーバまたは企業のデータセンタ内の参加者に対して同様に適用可能である。従って、データが所与のエンティティを決して離れ得ない間は、本明細書に記載されるような信頼を構築する技術は、企業内の異なる処理が、制御の別個の領域において操作される場所で同様に適用可能である。全ての企業の処理にわたって可視性が無い場合は、参加者が企業の外部であるかのように、同様の不信な事柄が生じる。例えば、サーバが管理者の制御下にあっても、サーバは企業内において侵害され得、さもなければ、管理者が不注意の場合または悪意を持っている可能性がある。

【００２４】

本開示の種々の技術は、クラウドにおける暗号化されたデータに適用することに加えて、ラップトップまたは他の携帯用デバイス上に記憶されるデータに適用することもでき、ラップトップが無くなったり盗まれたりする場合に備えられる。そのような場合、デバイスは、最後には過度に興味深いまたは悪意のあるエンティティが所持していることがあるが、クラウドにおけるデータの保護に適用する、本明細書に記載される同じ技術を、サーバまたはラップトップ上のデータを保護することに適用することもできる。ローカルなデータを暗号化した場合、適切なサブスクライバの認証情報が無しで、データにアクセスするための適切なロールまたは機能を何も示すことができないローカルな暗号化されたデータを、窃盗犯は理解できないであろう。

【００２５】

さらに、これらおよび他の種々の例示の非制限的な実施形態およびシナリオの詳細を以下に提供する。

【００２６】

信頼済みクラウドサービスのエコシステム

前述のように、デジタルエスクローのパターンを、クラウドに記憶されるデータのための検索可能な暗号化技術を含むネットワークデータサービスに提供して、複数のエンティティにわたって信頼を分配して、1つのエンティティによる漏洩を回避する。一実施形態において、鍵ジェネレータ、暗号化技術プロバイダ、およびクラウドサービスプロバイダを、それぞれ別個のエンティティとして提供して、データの発行者が、秘密裏に（暗号化された）データをクラウドサービスプロバイダに発行すること、および暗号化されたデータを、そのデータを要求するサブスクライバに、サブスクライバの要求に応答して生成される鍵情報内に符号化されるサブスクライバ識別情報に基づき選択的に与えることを可能にする。

【００２７】

図１は、実施形態に従う信頼済みクラウドサービスのフレームワークまたはエコシステムのブロック図である。システムには、検索可能に暗号化されたデータ１１０を、検証および／または照合を受けるサブスクライバの要求の結果と共に記憶する信頼済みデータス

トア１００を含む。この点において、ネットワークサービス１２０を、安全なデータ１１０の上位に構築することができ、データの発行者は、例えば、ネットワークサービス(単数または複数）１２０を介して、データを要求するサブスクライバ１４０に対して与えられる機能全体の制御を保持する。発行者１３０はまた、サブスクライバ１４０とすることができ、逆の場合も同じである。同様に、データの所有者１５０は、発行者１３０および／またはサブスクライバ１４０とすることができる。定義可能な共通のロールおよび対応する機能のセットの実施例として、特殊化された種類の発行者１３０およびサブスクライバ１４０は、管理者１６０および監査人１７０である。

【００２８】

例えば、管理者１６０は、データ１１０全体にわたる許可の特殊化されたセットとすることができ、信頼済みデータストア１００の操作の維持を助け、および監査人エンティティ１７０は、監査の範囲内の一定のデータの整合性の維持を助けることができる。例えば、監査人１７０は、不快なキーワードを含むデータ１１０のメッセージをサブスクライブすることができ、その場合、監査人１７０は、与えられた機能に従って許可される場合は、データ１１０のメッセージがそのような不快なキーワードを含む時に警告を受けるが、他のメッセージは読むことはできない。この点において、発行者のデータをデジタルエスクローに置く能力に従って無数のシナリオを構築することができ、そのデータに対する選択的なアクセスを可能にする鍵を配布することができる。

【００２９】

例えば、発行者は、エコシステムに対して認証して、および１組の文書を指示してエコシステムに対してアップロードする。その文書を、検索可能な暗号化アルゴリズムに従って、暗号化鍵情報を生成する別個の鍵ジェネレータから受信される暗号化鍵情報に基づき、暗号化する。次に、暗号化されたデータを、暗号化されたデータのストレージのためにネットワークサービスプロバイダに転送して、要求デバイスに対して与えられた選択された特権の遅延バインドに従って、要求デバイスの識別情報に基づき、暗号化されたデータが選択的にアクセス可能になる。暗号化技術プロバイダを暗号化されたデータのストレージから切り離すことは、加えて、暗号化されたデータをさらなる漏洩から守ることである。

【００３０】

この点において、図２は、信頼済みクラウドサービスのエコシステムに従ってデータを発行する例示の非制限的な方法を示すフロー図である。２００にて、発行者は、システムに認証される（例えば、発行者は、ユーザ名とパスワード、Ｌｉｖｅ（ライブ）ＩＤ認証情報等を用いてログインする）。２１０にて、鍵情報を、１つまたは複数の実施形態にて以下に記載されるような鍵生成センタ等の、鍵ジェネレータにより生成する。２２０にて、別個の暗号化技術プロバイダが、鍵情報に基づき、１組の発行者の文書を暗号化する。２３０にて、暗号化された文書を、機能と共にネットワークサービスプロバイダ、例えば、ストレージサービスプロバイダに対してアップロードして、暗号化された文書(単数または複数）が、要求デバイス（サブスクライバ）の識別情報に基づき与えられる選択された特権の遅延バインドを用いて、選択的にアクセス可能になる。

【００３１】

サブスクライバ側では、例えば、サブスクライバは、エコシステムに対して認証して、およびデータのサブセットを求める要求、例えば、所与のキーワードまたは１組のキーワードを含む文書のサブセットを求めるクエリを指示する。少なくとも１つのサブスクライバデバイスから、検索可能に暗号化されたデータのサブセットを求める要求に応答して、鍵生成コンポーネントは、サブスクライバデバイスに関連する識別情報に基づき、暗号化鍵情報を生成する。次に、暗号化されたデータのサブセットを、暗号化鍵情報内に定義されるようなサブスクライバデバイスを許諾した特権の機能として復号する。

【００３２】

図３は、信頼済みクラウドサービスのエコシステムに従ってデータをサブスクライブする、例示の非制限的な方法を示すフロー図である。３００にて、データをサブスクライブ

する方法は、サブスクライバを認証するステップを含む（例えば、サブスクライバが、ユーザ名とパスワード、ＬｉｖｅＩＤ認証情報等を用いてログインする）。３１０にて、サブスクライバは、データを求める要求を行う。３２０にて、独立した鍵生成エンティティにより、サブスクライバの要求に基づき、鍵情報を生成して、ここで、サブスクライバの機能を鍵情報内に定義することができる。３３０にて、発行者のデータのサブセットを、鍵情報内に定義される機能に基づき復号する。例えば、ＣＳＰはデータを復号することが可能である。３４０にて、発行者のデータのサブセットを、サブスクライバに対してアクセス可能にして、例えば、サブスクライバは、所有者／発行者により与えられる動的に定義可能な機能に基づき、データのダウンロード、閲覧、処理、変更などを行うことができる。任意選択的に、暗号化、復号および鍵生成に使用される技術を、別個の暗号化技術プロバイダにより供給することができるが、任意の参加者により提供することができる。

【００３３】

一実施形態において、サブスクライバデバイスの識別情報は、サブスクライバのロールを含む。例えば、監査人のロール、または管理者のロール、または他の事前に指定されたロールを、検索可能に暗号化されたデータストアの種々の一部に対するアクセスを制限または許可する基礎として、発行者／所有者が使用することができる。

【００３４】

図４は、鍵生成センタ(center for key generation)（ＣＫＧ）４００、暗号化技術プロバイダ(cryptographic technology provider)（ＣＴＰ）４１０、およびクラウドサービスプロバイダ(cloud service provider)（ＣＳＰ）４２０を切り離し、それにより信頼済みエコシステム内の単一のエンティティによる漏洩の可能性を排除することを示す例示のエコシステムを示す。この点において、顧客(単数または複数）４３０は、データの発行者および／またはサブスクライバを含む。任意選択的に、ＣＫＧ４００を、例えば、ＣＴＰ４１０により提供される、参照ソフトウェア、オープンソースソフトウェア、および／またはソフトウェア開発キット(software development kit)（ＳＤＫ）に基づき構築することができ、そのようなコンポーネントを、それ自身で生成する集団のための構築のブロックを可能にし、または第３者のそのようなエコシステムのコンポーネントの実装を満足させることができる。一実施形態において、ＳＤＫを、ＣＴＰ４１０により提供して、および１つまたは複数の参加者により使用して、ＣＫＧ４００、以下により詳細に記載する計算・ストレージ抽象化(compute and storage abstraction)（ＣＳＡ）、および／または暗号化クライアントライブラリを提供または実装することができる。任意選択的に、ＳＤＫを、ＣＴＰ４１０からＣＫＧ４００を提供するエンティティに分配することができる。

【００３５】

一般に、ＣＫＧ４００、ＣＴＰ４１０またはＣＳＰ４２０のそれぞれを、所与の実装に応じてサブコンポーネントに再分割することができるが、全体的な分離を保ち、信頼を維持する。例えば、マスタ公開鍵(master public key)（ＭＰＫ）配信４０２、クライアントライブラリダウンローダ４０４、秘密鍵エクストラクタ４０６、信頼ベリファイア４０８、または他のサブコンポーネント等のＣＫＧエンティティ４０１を、別個に、サブセット内に、または一体化コンポーネントとして共に提供することができる。符号化および復号化用クライアントアプリケーション４１２、代替暗号化技術４１４、ＣＫＧとの対話のためのアプリケーション４１６、他の暗号構築ブロック４１８等のＣＴＰエンティティ４１１も、別個に、サブセット内に共に提供することができる。さらに、ＣＳＰ４２０を、ストレージサービス４２４およびサービスホスティング４２８をそれぞれ提供するＣＳＰ４２２、４２６等の多くの別個のサービスプロバイダとして考えることができ、またはそのようなサービスを共に提供することが可能である。

【００３６】

信頼済みエコシステムにおける１つまたは複数の参加者により提供されるＣＫＧ、またはＣＫＧインスタンス(単数または複数）は、単一のモノリシックなエンティティであることは必要ないことは十分に理解できるであろう。むしろ、ＣＫＧを、協働して鍵を生成

する多数の（冗長な）エンティティに分離することができ、小さいサブセットの参加者がオフラインである場合でも、操作を継続することができる。一実施形態において、小さなサブセットのこれらの参加者が攻撃相手により情報を漏洩され、またはそうでなければ利用不能もしくは信頼できなくなったとしても、任意選択的に、１組の参加者を全体として信頼できるものとすることができる。

【００３７】

図５は、企業５００のクラウドサービスを実行する信頼済みエコシステムの更なる利点を示す別のアーキテクチャの図である。例えば、企業５００は、異なる機関５０２、５０４、５０６、５０８を含むことができる。本図の異なる機関５０２、５０４、５０６、５０８は、機関が、システムを使用するポリシ、または鍵生成を実装することについての所有権を多くも少なくも持つことができることを示す。例えば、機関５０２は、独自のポリシ５１２を実装するが、集中型の鍵ジェネレータ５２２を使用する一方で、機関５０４は、独自の鍵ジェネレータ５２４を実装して、および独自のポリシ５１４を実装することを選択する。機関５０６もまた、独自のポリシを実装するが、第三者のＣＫＧ５２６に頼る一方、機関５０８は、第三者のポリシプロバイダ５１８、および独立したＣＫＧ５２８を頼ることを選択する。

【００３８】

この点において、データを発行するために、発行者５４０は、ＣＫＧ５２２からの出力に基づき、データ５３５を暗号化する公開パラメータを取得する。公開パラメータに基づき、独立した暗号化技術プロバイダを使用して、５４５にて発行者デバイス５４０により、データを暗号化する。暗号化されたデータを、ストレージ抽象化サービス５５０に対してアップロードする。ストレージ抽象化サービス５５０は、ＣＳＰ５７２、５７４、５７６、または５７８等の１つまたは複数のＣＳＰ５７０による、暗号化されたデータを記憶することに関連するストレージの動作を隠す。サブスクライバデバイス５６０では、データを求める要求は、ＣＫＧ５２２が提供しているプライベート秘密鍵５６５の生成をもたらす。プライベート秘密鍵５６５は、サブスクライバデバイス５６０が、５５５にてデータを復号することにより、検索可能に暗号化されたデータに選択的にアクセスすることを可能にする情報を含む。再度、ＣＳＰ５７０からデータを取得する動作を、ストレージ抽象化サービス５５０により隠す。また、サブスクライバデバイス５６０に与えられた特権は、発行者／所有者により与えられた機能の遅延バインドが原因で、現在の一連の特権となる。

【００３９】

複数のデータ所有者、すなわち企業または顧客が、本明細書に記載されるような信頼済みエコシステムに参加して、信頼済み関係を確立することができるということが、図５から十分理解できるであろう。そのような場合、各所有者は、自身が所有するＣＫＧ（例えば、機関５０４のＣＫＧ５２４）を提供または制御することができ、データを求める要求またはクエリを、対応するＣＫＧに転送して、要求されるデータの全ての共同所有者から必要な鍵を集めることができる。

【００４０】

図６は、ストレージ抽象化層６１０を介する異なるストレージプロバイダの適応を示す別のブロック図である。信頼済みエコシステムでは、クライアントアプリケーション６４０、６４２をそれぞれ有するデスクトップ６３０、６３２が、上述したようにデータを発行またはサブスクライブすることができ、鍵生成センタ６２０に対して、データの暗号化または復号に使用する鍵情報を求める要求を開始する。同様に、サービス６４４、６４６、６４８は、エコシステムにおいて、発行者および／またはサブスクライバとすることもできる。この点において、プライベートクラウドストア６００、ＳＱＬデータサービスストア６０２、または簡易ストレージウェブサービス６０４等のいずれかにより、データの記憶または抽出を行うために、ストレージ抽象化サービス６１０が、その名前が暗示するように、クライアントから離れた特定のストレージリポジトリまたはリポジトリについての仕様を抽象化する。

【００４１】
この点において、誤解を避けるために、図６は複数の状況を対象とする。１つの状況において、図６は、計算・ストレージ抽象化（ＣＳＡ）と呼ばれることもある、ストレージ抽象化サービスを介して、ストレージプロバイダの仲介機能を取り除く（ストレージプロバイダを個別に取り除く）場合を対象とする。加えて、図６は、同じタイプでも異なるタイプのものでもよい複数のバックエンドストレージプロバイダに、データを（例えば、冗長性のために）分割および／または展開(fan out)して、たとえ、１つ（または少数）のバックエンドストレージプロバイダが、偶然または故意にそのデータの自身のコピーを削除または変更したとしても、元データを再構成できるようにする、というシナリオも対象とする。

【００４２】
図７は、サーバＯＳ（オペレーティングシステム）７１４、およびストレージサービス７１２を含み、プライベートクラウドストア７００、ＳＱＬデータストア７０２、簡易ストレージウェブサービスストア７０４等のストレージの詳細を抽象化するストレージ抽象化サービス７１０に関連してストレージのさらなる態様を示す。クライアントは、クライアントアプリケーション７４０および７４２をそれぞれ有するデスクトップ７５０または７５２とすることができる。鍵生成センタ７２０は、サーバＯＳ７２４上で実行する鍵ジェネレータアプリケーション７２２を含むことができる。この点において、アクティブディレクトリ７３６、サーバＯＳ７３４、およびセキュリティトークンサービス(security token service)（ＳＴＳ）７３２を有する機関７３０は、エコシステムにおいて発行者またはサブスクライバとすることができる。この点において、ストレージ転送形式(storage transfer format)（ＳＴＦ）は、暗号化されたデータおよびメタデータをリポジトリ全体で交換するために使用することができる標準交換形式である。例えば、機関７３０が、電子メールデータをストレージサービスプロバイダ７００、７０２または７０４間で転送したい場合、ＳＴＦを使用することができる。

【００４３】
図８は、信頼済みエコシステム８２０における種々の異なる参加者を示す別のブロック図である。上述したように、有利なことに、企業８００は、大量のデータのストレージおよびメンテナンスを、オンサイトから、そのようなボリュームの処理に、より適したクラウドストレージサービスプロバイダにオフロードすることができる一方で、同時に、企業が、暗号化されたデータにわたって定義される機能全体の制御を維持するので、不正なサブスクライバに対してデータを復号することがないという安心感を維持する。例えば、機関８０２は、シェアポイント等の共同アプリケーション８１２を操作することができる。この点において、機関８０２は、シェアポイントのデータに対してデジタルエスクロー、つまり信頼済みドメインを設定することができる。ポリシ８３２およびＣＫＧ８３４を、第１のデータセンタ８３０により実装することができ、第１のデータセンタ８３０は、暗号化鍵情報を信頼済みドメインに対して定義することにより安全な空間を設定するように（８３５）操作する。

【００４４】
次に、別の機関８０４が、例えば、発行者８１４として機能して、ＣＫＧ８３４から取得される鍵情報に基づき、データを暗号化することができ、この時点で、第２のデータセンタ８４０のコンピュータ・ストレージ抽象化コンポーネント８４２は、検索可能に暗号化されたデータを、第３のデータセンタ８５０において、例えば、ＣＳＰ８５２に記憶することについての詳細を処理する。その一方で、機関８０４のサブスクライバ８１６がデータを要求すると、プライベート鍵情報または秘密鍵情報を、抽出８６５の一部としてサブスクライバ８１６に配信する。次に、サブスクライバに対して定義された機能を含むプライベート鍵情報に基づき、サブスクライバが特権を持つものと仮定してサブスクライバにより要求されるデータを、８７５にて復号して、および再度、抽象化層８４２は下層のストレージ８５２の詳細を処理する。

【００４５】

図９は、異なる要素を異なるエンティティまたは同じエンティティにより提供することができる信頼済みクラウドコンピューティングシステムの、例示の非制限的な実装のいくつかの層の代表的な図である。層スタックの底部には、暗号化／復号化アルゴリズムを実装するために使用される演算・暗号ライブラリ９８６がある。種々の暗号スキームの定義の抽象化を、中間層９８４として、詳述したライブラリ９８６と検索可能な暗号スキームの実際の実装９８２との間に提供することができる。層９８２、９８４および９８６をまとめて、より大きな暗号サービス層９８０を形成して、暗号サービス層９８０は、サービス型ソフトウェア（ＳａａＳ）アプリケーションエコシステムの抽象化層９６０と組み合わせられて、信頼済みデジタルエスクロー９７０およびそのストレージの実装の基礎を形成する。抽象化層９６０は、デジタルエスクローのパターン、すなわちSetUp()、Encrypt()、Extract()、Decrypt()等のコマンドの実装に使用される基本言語を含む。

【００４６】

抽象化層９６０の上部には、種々のより特殊なプラットフォーム技術（例えば、ＳＤＳ、Ａｚｕｒｅ、バックアップ／アーカイブ、ＲＭＳ、ＳＴＳ等）に結合する層９５０がある。種々の特殊なプラットフォーム技術に結合する層９５０の上部には、信頼済みデジタルエスクロー９００を使用する種々のＳａａＳアプリケーションがある。例示の非制限的な説明図は、デジタルエスクローアプリケーション９００を単一の会社９１０、またはパートナー９３０、またはその両者により実装することができることを示す。例えば、会社９１０は、高性能コンピューティング(high performance computing)（ＨＰＣ）、電子証拠開示および法定開示９１４、Ｌｉｖｅサービス９１６（例えば、ＤＢｏｘ）、サービス型バックアップ／アーカイブ９１８、監査ログ－ビジネスプロセスおよび監視９２０、または他のクラウドサービス９２２等のサービスを実装することができる。同様に、パートナー９３０は、電子信用状９３２、業種についてのサービス型ＨＰＣ９３４、ｅヘルスサービス、安全なエクストラネット９３８、コンプライアンス９４０、訴訟サポート９４２等のサービスを実装することができる。

【００４７】

信頼済みクラウドサービスのエコシステムに基づくシナリオ

図９の上半分では、鍵ジェネレータ、暗号プロバイダ、およびクラウドサービスプロバイダの分割に固有の増大した信頼によって、クラウドにおいて実現可能なアプリケーションの種類の外見を描く。この点において、そのような信頼済みクラウドサービスのエコシステムを可能にしたことにより、本明細書に記載される信頼済みエコシステムの１つまたは複数の利点を利用する、一連の豊富なサービスおよびシナリオを実現することができる。

【００４８】

例えば、図１０は、上述したように遅延バインドを用いてデータへの発行者制御の選択的なアクセスを与えることができるように、デジタルセーフアプリケーションに文書を発行する例示の非制限的な処理のフロー図である。１０００にて、デバイスを認証する（例えば、デバイスは、ユーザ名とパスワード、パスワード認証情報、生体認証情報、ＬｉｖｅＩＤ認証情報等でログインする）。１０１０にて、文書(単数または複数）をアップロードして、およびタグを入力する。タグを、１０２０にてエスクローエージェントに送信して、およびハッシュされたタグを、応答としてエスクローエージェントから受信する。この点において、タグを、上述したように供給することができ、または代替えとして、自動的にペイロード（レコード、文書）から、例えば、フルテキストインデックスを介して、抽出することができる。１０３０にて、クライアントは、発行者の鍵情報を用いて文書を暗号化して、および文書(単数または複数）を、安全なデジタルクラウドストレージプロバイダに、文書(単数または複数）に関するサブスクライバの機能と共に送信する。１０４０にて、安全なデジタルクラウドストレージプロバイダは、ストレージサービスに、例えば、ストレージ抽象化層に対して、暗号化されたブロブを送信する。

【００４９】

図１１は、図面においてラベル付けされる図１０の動作と共に、信頼済みエコシステム

における異なる参加者に照らして図１０を示す。この点において、クライアント１１１０の認証情報１１００と共に開始して、１０００が起きる。次に、１０１０が、クライアント１１１０にて起こる。次に、タグをエスクローエージェント１１２０に送信して、およびハッシュされたタグを受信するステップを、１０２０にて表す。次に、クライアント１１１０が文書を暗号化して、および１０３０にて示すように、デジタルセーフサービス１１３０に送信する。最後に、暗号化されたブロブを、１０４０により表されるようにストレージサービス１１４０に送信する。そして、文書(単数または複数）と共に送信され、または後でアップデートされる機能が許可する場合は、サブスクライバに、ユーザのサブセットに対するアクセスを許可することができる。

【００５０】

図１２は、デジタルセーフに置かれる素材をサブスクライブする例示の非制限的な処理のフロー図である。１２００にて、サブスクライバを認証して、および１２１０にて、クライアントデバイスが、エスクローエージェントにタグを送信して、エスクローエージェントは、ハッシュされたタグを１２１０にて応答して送り返す。次に、１２２０にて、クライアントは、ハッシュされたタグをデジタルセーフサービスに送信して、およびハッシュされたタグを解釈して、１２３０にて、クライアントが、全体としてまたは部分的に、その検索要求をストレージサービスにより実行させる権利が与えられるかどうかを理解する。

【００５１】

図１３は、図１１と同様に、参加者の上に重ねられる図１２の動作を表す。すなわち、動作１２００に対してクライアント１３１０およびその認証情報１３００、動作１２１０に対してクライアント１３１０およびエスクローエージェント１３２０、動作１２２０に対してクライアント１３１０およびデジタルセーフサービス１３３０、動作１２３０に対してデジタルセーフサービス１３３０およびストレージサービス１３４０である。

【００５２】

図１１および１３において、エスクローエージェント１１２０、１３２０は、ＣＫＧ、またはＣＫＧのコンポーネントとすることができる。あるいは、エスクローエージェント１１２０、１３２０は、別個の参加者により提供されるＣＫＧインスタンスとすることができ、それにより、エスクローエージェント１１２０、１３２０は、クライアントに代わって暗号化／復号化する信頼済みエンティティとなる。この点において、設計トレードオフおよび参加者間の関係が、エスクローエージェント１１２０、１３２０の機能および範囲に影響し得る。例えば、ローエンドのクライアントに対して、クライアントの機能を信頼済みプロキシサービスにオフロードすることが、重い処理を実行するためには必要とされる場合がある。

【００５３】

図１４は、デジタルエスクローのパターンを使用して、１つまたは複数のデータセンタを介して企業の安全なエクストラネットを実装する、信頼済みクラウドサービスの例示の非制限的な実装を示す。上述したように、信頼済みコンピューティングエコシステムは、暗号化技術プロバイダ（ＣＴＰ）１４１０から離れて実装される鍵生成センタ１４００を含むことができ、暗号化技術プロバイダ（ＣＴＰ）１４１０は、１つまたは複数のクラウドサービスプロバイダ（ＣＳＰ）１４２０から離れて実装される、エコシステムに準拠する暗号化技術を実装する際に使用する参照実装を提供する。安全なエクストラネットの例示の非制限的な実装において、１４８０は、共有されるリポジトリ１４７０（例えば、シェアポイント）、および共有されたリポジトリ１４７０内の文書に関連して使用する設計または分析のアプリケーションのリポジトリ１４６０、を企業が維持することを示す。ビジネスソフトウェア１４４０（例えば、Ｓｅｎｔｉｎｅｌ）は、デスクトップ１４５０を有するコンピュータに対するアプリケーションまたはサーバの性能などを監視することができる。

【００５４】

この点において、信頼済みクラウドサービスのエコシステムでは、デスクトップ１４５

０を使用するサブスクライバが、選択的にアクセス可能で、およびストレージから暗号化された情報を探す時、セキュリティトークンサービス１４３０は、何らかの情報を配信して、サブスクライバ１４８２を識別することが可能であり、およびＣＫＧ１４００を、１４８４により示される第１のデータセンタのＣＫＧ層１４０２のインターフェースを介して閲覧することができる。ＣＫＧ１４００は鍵情報を返し、その後、鍵情報を使用して、ストレージ抽象化サービス１４２２を介してデータサービス１４２４により保持される、１４８６により示されるようなデータに選択的にアクセスすることができる。従って、企業全体にわたって、および企業内のサブスクライバのロールに従って選択的に、任意のタイプのデータを共有することができる。

【００５５】

図１５は、サブスクライバに、例えば、企業内のＣＳＰにより記憶される暗号化されたデータへの選択的なアクセスを与える、信頼済みクラウドサービスのエコシステムに基づく別の例示の非制限的なシナリオを示すフロー図である。最初に、サブスクライバデバイスは、暗号化されたデータにアクセスする特権を獲得していない。しかし、いくつかまたは全ての暗号化されたデータを求める要求を行うことにより、例えば、１５００にてアプリケーションと対話することにより、１５１０にてアプリケーションが自動的に、請求を（暗合学の専門用語で）取得するために対応するＳＴＳと通信する。１５２０にて、アプリケーションはＣＫＧと通信して、サブスクライバに対する機能についての情報を符号化する鍵情報を取得する（機能は、暗号学の専門用語ではトラップドアと呼ばれることがあるが、用語機能は、用語トラップドアが一般的に現れる文脈に限定されない）。最後に、１５３０にて、アプリケーションは鍵情報をＣＳＰに提供し、これにより、暗号化されたデータ全体にわたる検索またはクエリが、サブスクライバの機能により許される範囲まで許可される。

【００５６】

図１６は、アプリケーションの応答が、サインイン情報に基づきサブスクライバに対して調整可能であることを示す別のフロー図である。例えば、１６００にて、ユーザＩＤ情報をアプリケーションによって受信する。１６１０にて、アプリケーションは関連のある請求をＳＴＳから取得する。１６２０にて、ユーザＩＤ情報に関連するユーザによりなされる１つまたは複数のロールに基づき、それらのロールに対する特権／制約に相応するように経験を調整することができる。例えば、会社の最高財務責任者に提示される、会社の暗号化されたデータを見るというユーザ経験は、郵便係りの従業員に与えられる、暗号化されたデータを見るということは異なるユーザ経験とすることができ、またそうすべきである。図１６は、単一または複数の集団のログインのシナリオに適用可能である。

【００５７】

図１７は、単一の集団または複数の集団に対して実装可能な、安全なレコードアップロードのシナリオを示す別のフロー図である。１７００にて、レコードおよびキーワードをアプリケーションによって受信して、例えば、デバイスのユーザにより、アプリケーションを用いて与えるかまたは指定する。１７１０にて、アプリケーションは、マスタ公開鍵（ＭＰＫ）を取得し、およびキーワード検索可能公開鍵暗号（ＰＥＫＳ）アルゴリズム(単数または複数）を適用する。ＭＰＫは、任意選択的に、アプリケーションによりキャッシュすることができる。１７２０にて、アプリケーションは、例えば、ストレージ抽象化層を介して、暗号化されたレコードをＣＳＰリポジトリに入力する。

【００５８】

図１８は、信頼済みクラウドサービスのエコシステムにより可能にされた、例えば、単一の集団による自動検索のための、検索可能暗号化データストア全体にわたるロールベースのクエリの例示の非制限的な実装を示すさらに別のフロー図である。１８００にて、結合(conjunctive)クエリを、アプリケーションにより受信または起動する。１８１０にてアプリケーションが、関連のある請求をＳＴＳから取得する。例えば、ＳＴＳは、ユーザのロール(単数または複数）を適切なクエリグループ(単数または複数）にマッピングし、および所与のロール(単数または複数）に適法なクエリセットを返す。１８２０にて、ア

プリケーションは、フィルタリングされた請求およびクエリをサブミットして、全ての請求(単数または複数）ではなく、クエリに対応する請求(単数または複数）を効率的にサブミットする。任意選択的に、ＣＫＧは、トラップドアの請求をアプリケーションに返す（または請求を拒否する）。１８３０にて、アプリケーションは、リモートインデックスでトラップドアの請求を実行する。リモートインデックスにわたる処理に基づき、結果を受信して、および結果を、アプリケーションにより、例えば、ユーザのロール(単数または複数）に基づきカスタムレンダリングを使用して、ユーザに対してレンダリングすることができる。

【００５９】

図１９は、企業１９２０、ＣＫＧ１９１０およびＣＳＰ１９００の間の信頼済みクラウドサービスエコシステムの実装のブロック図であり、上述の図１５から１８の動作を同じ参照番号で強調表示する。シナリオは、ユーザ１９２４が自身をアプリケーション１９２２に対して識別することで開始される。ＳＴＳ１９２６は、ＣＫＧ１９１０との間の情報の交換に関連して信頼１９３０を確立するよう動作し、およびシナリオの目的に応じてＣＳＰ１９００からのデータを暗号化または復号する時に使用する鍵情報をアプリケーション１９２２に返す。

【００６０】

図２０は、企業が、その暗号化されたデータのいくつかへのアクセスを外部の企業に提供する、複数の集団の共同のシナリオを示すフロー図である。例えば、製造業者は、信頼済みクラウドに記憶される製造業者のデータへのアクセスを供給業者に与えることができ、その逆も同様である。この点において、２０００にて、企業２のＳＴＳを、リソースプロバイダとして指定して、および、企業１のアプリケーションが次に、クラウド内においてリソースプロバイダにより提供されるリソースへのアクセスの請求を取得する。２０１０にて、企業１のＳＴＳを、識別プロバイダとして指定する。この点において、アプリケーションは、識別プロバイダにより容易にされるような、企業１においてサブスクライバにより定義されるロールまたはロールのセットへの請求を取得する。２０２０にて、請求を、企業２により制御され許容されるリソースに基づき、およびサブスクライブしているエンティティのロール（単数または複数）により定義される許可／機能に基づき、アプリケーションにより取り出す。なお、図２０において、１つのＳＴＳのみを示すが、デジタルエスクロー、すなわち、連合トラストオーバレイ(Federated Trust Overlay)には、複数の識別プロバイダＳＴＳおよび／または複数のリソースプロバイダＳＴＳが存在することができる。

【００６１】

図２１は、例えば、企業１と企業２などの複数の企業間など、複数の集団の自動検索のシナリオを示すフロー図である。２１００にて、結合クエリを、企業１のアプリケーションにより実行のために受信または起動する。２１１０にて、アプリケーションは、関連のある請求をリソースプロバイダ（企業２）のＳＴＳから取得する。リソースプロバイダを、任意選択的に、機関タグで指定することができる。ＳＴＳは、任意選択的に、ユーザのロールのマッピングを、クエリグループに対して実行し、適法なクエリセットをユーザのロールに返す。２１２０にて、アプリケーションは、フィルタリングされた請求およびクエリをユーザのロールに基づきサブミットする。全ての請求ではなく、クエリに対応する請求を、効率的にサブミットすることができる。任意選択的に、ＣＫＧは、機能（例えば、トラップドアの請求）をアプリケーションに返し、またはＣＫＧは請求を拒否する。２１３０にて、アプリケーションは、リモートインデックスでトラップドアの請求を実行する。リモートインデックスへの処理に基づき、結果を受信して、および結果を、アプリケーションにより、例えば、ユーザのロール(単数または複数）に基づきカスタムレンダリングを使用して、ユーザに対してレンダリングすることができる。

【００６２】

図１８および２１において、方法には、結合クエリを受信するステップ、あるいは、結合クエリを起動するステップが含まれる。この点において、任意選択的に、結合クエリを

暗号法的に保護して、トラップドア（または機能）の受信者は、クライアントもサービスプロバイダも、結合クエリを分解することも、その構成の一部を判定することもできないようにすることができる。

【００６３】

図２２は、企業２２２０、２２３０、ＣＫＧ２２１０、およびＣＳＰ２２００の間における信頼済みクラウドサービスエコシステムの実装のブロック図であり、上述の図２０から２１の動作を同一の参照番号で指定する。例えば、ユーザ２２２４は、自身をアプリケーション２２２２に対して識別することができる。企業２２２０のＳＴＳ２２２６、および企業２２３０のＳＴＳ２２３２とは、協働してＣＫＧ２２１０との間の情報の交換に関連して信頼２２３０を確立し、シナリオの目的に応じてＣＳＰ２２００からのデータを暗号化または復号する時に使用する鍵情報をアプリケーション２２２２に返す。

【００６４】

図２３は、信頼済みクラウドサービスに実装可能な例示の非制限的なエッジコンピュータネットワーク（ＥＣＮ）技術を示す。この点において、複数のダイナミックコンピュートノード２３７０、２３７２、２３７４、２３７６を、お互いに独立して操作する信頼済みクラウドコンポーネントのセットとの関連で計算処理能力に対して動的に割り当てる。例えば、鍵生成センタ２３２０、ストレージ抽象化サービス２３１０、機関２３３０、および機関２３４０を、図示するように実装して、上述したような複数機関のビジネスまたは他のシナリオを対象とする。鍵生成センタ２３２０は、鍵ジェネレータ２３２２、およびサーバＯＳ２３２４を含む。。ストレージ抽象化サービス２３１０は、ストレージサービスコンポーネント２３１２、およびサーバＯＳ２３１４を含む。機関２３３０は、ＳＴＳ２３３２、ＡＤ２３３６、およびサーバＯＳ２３３４を含む。機関２３４０は、ＳＴＳ２３３４、ＡＤ２３４６、およびサーバＯＳ２３４４を含む。サーバＯＳ２３１４、２３２４、２３３４、２３４４は、サーバ全体にわたって協働してＥＣＮを実装する。任意のストレージプロバイダまたは抽象化２３０２をデータの記憶のために使用することができ、例えば、ＳＱＬデータサービスを採用することができる。このようにして、１つまたは複数のデスクトップ２３５０、２３５２は、それぞれクライアントアプリケーション２３６０、２３６２を介して、データを発行またはサブスクライブすることが可能である。

【００６５】

図２４は、信頼済みクラウドサービスエコシステムに従う、鍵生成センタ２４１０の１つまたは複数の任意選択的態様を示すブロック図である。最初は、デスクトップ２４６０、２４６２、およびそれぞれのクライアントアプリケーション２４７０、２４７２、またはサービスもしくはサーバ２４７４、２４７６、２４７８、等の１組のコンピュータデバイスが、クラウドコンテンツ配信ネットワーク２４５０に対する潜在的な発行者および／またはサブスクライバである。しかし、１組のコンピュータデバイスのいずれかからの要求を遂行するのに先立って、まず、鍵生成センタは、公開鍵に基づきデータを暗号化し、およびその機能に基づき秘密鍵をデータのサブスクライバに配布する発行者に対する信頼の管理者(custodian)として動作する。

【００６６】

例示の非制限的な相互作用においては、最初に、コンピュータデバイスからの要求を提供して（２４００）、およびＣＫＧ２４１０の提供が、２４８０にて、ＣＫＧファクトリ２４０２からＣＫＧ２４１０のインスタンスを要求する。次に、２４８２にてユーザ認証２４０４を起動する。次に、ＣＫＧファクトリ２４０２の使用に対して任意の利用ごとの請求２４８４を、請求システム２４０６により適用する。次に、２４８６にて、テナントＣＫＧを、ＣＫＧファクトリ２４０２により実現して、ＣＫＧファクトリ２４０２は、ＭＰＫ配信コンポーネント２４１２、クライアントライブラリダウンローダ２４１４、秘密鍵エクストラクタ２４１６、およびトラストバリデータ／ベリファイア２４１８を含むことができる。

【００６７】

ＭＰＫ配信コンポーネント２４１２は、２４８８にてＭＰＫをＣＤＮ２４５０に配信す

る。クライアントライブラリダウンローダ２４１４は、デバイスにサブスクライブする、発行すべきデータを暗号化すること、またはデータを復号することに関連して使用され得る暗号文ライブラリを、要求クライアントにダウンロードする。次に、クライアントは、秘密鍵エクストラクタ２４１６から受信される鍵情報に基づき所与のセットの文書を抽出する要求をし、秘密鍵エクストラクタ２４１６は、トラストベリファイア２４１８と協働し、トラストベリファイア２４１８は、２４９４にて、サブスクライバのＳＴＳサムプリントを照合することに基づき、例えば、要求に関係する機関の異なるＳＴＳ２４２０、２４２２、２４２４、２４２６との通信に基づき、サブスクライバが特定の機能を有することを検証することが可能である。他の実施形態のように、ストレージ抽象化サービス２４４０を提供して、データベースサービス２４３０（例えば、ＳＱＬ）のストレージの詳細を抽象化することができる。

【００６８】

図２５は、ネットワークサービス２５２０の配信に関連して、検証および／または照合を有する、検索可能に暗号化されたデータ２５１０を含む信頼済みストア２５００の例示の非制限的な実施形態のブロック図である。本実施形態において、サブスクライバ２５４０、サブスクライバ２５４０により使用されるアプリケーションは、暗号化されたストア２５００の特定の部分へアクセスする要求の一部として、実際に受信される項目が、受信されるべき項目でもあることを検証する要求から返された項目にわたって、検証証明を実行することを要求することができる。この点において、図２５は、検索可能な暗号化技術と検証のための技術との組み合わせを示す。任意選択的に、システムを、本明細書において他の実施形態に記載される、請求ベースの識別およびアクセスの管理と統合することもできる。この点において、デジタルエスクローのパターンは、本明細書において種々の実施形態に記載されるように、連合トラストオーバレイとも呼ばれ、より従来的な請求ベースの認証システムとシームレスに統合させることができる。

【００６９】

図２５において、信頼済みデータストア２５００、またはデータストアのサービスプロバイダもしくはホストは、提供のステップを実行する一方で、データの所有者（例えば、サブスクライバデバイス）は検証を実行する。データストア２５００を信頼する理由は、データストア２５００が強力な保証を提供するということをユーザが信用しているためであるが、物理的なエンティティが実際にデータを提供すること、および完全には信頼できない参加者もいることを理解されたい。

【００７０】

図２６は、検証のステップを含むサブスクライブする例示の非制限的な処理を示すフロー図である。２６００にて、検索可能に暗号化されたデータのサブセットを、サブスクライバデバイスから受信する。２６１０にて、サブスクライバデバイスの識別情報に基づき、暗号化鍵情報を生成する鍵生成インスタンスから、暗号化鍵情報を生成する。２６２０にて、暗号化鍵情報において定義されるサブスクライバデバイスに与えられた機能の関数として、暗号化されたデータのサブセットを復号する。２６３０にて、サブセット内に表される項目を検証することができ（例えば、データ所有の証明）、および２６４０にてデータにアクセスする。

【００７１】

多くの場合、暗号化されたデータに対して、復号の必要無しにＰＤＰ／ＰＯＲを実行できることが望ましい。任意選択的に、ＰＤＰに必要な鍵情報を、検索可能な暗号化で保護されたメタデータ内に符号化することができる。これが、ＰＤＰ／ＰＯＲに使用される鍵を管理する効果的な方法である一方、クリアテキスト（暗号化されていないテキスト）のコンテンツにアクセスする必要無しに、ＰＤＰ／ＰＯＲを、暗号化されたデータに実行することができる多くの高価値のシナリオが存在することは留意されたい。

【００７２】

図２７は、ベリファイア２７００（例えば、データの所有者）が、暗号化チャレンジ２７２０をプルーバ２７１０（例えば、データサービスプロバイダ）に発行する、例示の非

制限的な検証チャレンジ／応答プロトコルを示す。チャレンジ２７２０の受信時、プルーバ２７１０は、データおよびチャレンジの関数として応答を計算する（２７１２）。そして、チャレンジ応答２７３０を、ベリファイア２７００に返して、ベリファイア２７００はその後計算を実行して、データが変更されていないことを検証または証明する（２７０２）。

【００７３】

図２７において概して例示される検証は、プライベートＰＤＰとして知られるが、「公開」バージョンも存在し、そこでは第三者に鍵（「公開」鍵）が提供され、第三者は、実際のデータについては何も知ることなく、同様のプロトコルに従ってベリファイアとして動作する。ＰＯＲは、照合の例であり、ＰＤＰは、データが取得できる（何らかの破損／変更があっても）という証明を提供する点で異なるが、図３０において以下に示すように、基本のプロトコルは同じであり、文書の構造および実際のアルゴリズムが異なる。本明細書の信頼済みエコシステムの種々の実装は、検索可能な暗号化とＰＯＲ／ＰＤＰとを結合させて、システムに利益もたらし、および信頼を強化する。この点において、データをサービスプロバイダにサブミットする前に、データを検索可能に暗号化して、およびデータの後処理にＰＯＲおよび／またはＰＤＰを含めることができる。

【００７４】

加えて、さらに強力な保証を提供する必要がある場合は、「データ分散」技術を、任意選択的に、上記の実施形態の内の任意の１つまたは複数の上に重ねることができる。データ分散では、任意の単一のサービスプロバイダにおける「非常に悪い挙動」すなわち壊滅的な損失に対する回復力のために、データをいくつかのサービスプロバイダに分配する。本明細書に記載される信頼の機構を使用して、この分散を、独立したサービスプロバイダが、共謀しておよびデータ破損させることを困難にすることができるような方法で実行する。これは、上述の分散ＣＫＧの実施形態と概念が同様である。

【００７５】

図２８は、ネットワークサービス２５２０の配信に関連して、検証および／または照合を有する検索可能に暗号化されたデータ２５１０を含む、信頼済みストア２５００の別の例示の非制限的な実施形態のブロック図である。具体的に、図２８は、サブスクライバ２５４０に返された項目が改ざんされなかったこと、あるいは不注意に変更されなかったことを照合する照合コンポーネント２８５０を示す。上述したＰＤＰは、照合の非制限的な実施例である。

【００７６】

図２９は、検証のステップを含むサブスクライブする例示の非制限的な処理を示すフロー図である。２９００にて、検索可能に暗号化されたデータのサブセットを、サブスクライバデバイスから受信する。２９１０にて、サブスクライバデバイスの識別情報に基づき暗号化鍵情報を生成する鍵生成インスタンスから、暗号化鍵情報を生成する。２９２０にて、暗号化鍵情報において定義されるサブスクライバデバイスに与えられた機能の関数として、暗号化されたデータのサブセットを復号する。２９３０にて、サブセット内に表される項目のコンテンツを照合することができ（例えば、取得可能性の証明）、２９４０にてデータにアクセスする。

【００７７】

図３０は、ベリファイア３０００（例えば、データ所有者）が、暗号化チャレンジ３０２０をプルーバ３０１０（例えば、データサービスプロバイダ）に発行する、例示の非制限的な照合チャレンジ／応答プロトコルを示す。チャレンジ３０２０の受信時、プルーバ３０１０は、データおよびチャレンジの関数として応答を計算する（３０１２）。そして、チャレンジ応答３０３０をベリファイア３０００に返し、ベリファイア３０００がその後計算を実行して、データが取得可能であることを照合または証明する（３００２）。

【００７８】

図３１は、複数の独立した連合トラストオーバレイ、またはデジタルエスクローが、並んで、または積層させる方法で重なり合って存在することができる、非制限的なシナリオ

を示すブロック図である。本シナリオにおいて、種々のネットワークサービス(単数または複数）３１２０が基礎を置くことができる、検索可能に暗号化されたデータ３１１０を有する信頼済みデータストア３１００が存在する。例えば、ネットワークサービス(単数または複数）３１２０は、クラウドサービスとして、ワードプロセシングソフトウェアの配信を含むことができる。地球的規模の配信の一部として、あるいは任意選択的に、それぞれが、異なるアプリケーション／業種／コンプライアンスの必要性／最高位のエンティティの要件、に対して調整される複数のオーバレイ／エスクロー３１３２、３１３４、３１３６を提供することが可能であり、発行者２５３０またはサブスクライバ３１５０は、例えば、司法権／居住地の要件または領域のセットに基づき、参加すべき正しいオーバレイ／エスクローを、暗黙的または明示的に選択するようにできる。従って、オーバレイは変更可能であるが、クラウドからのバックエンドサービスは、主要なサービス自体の配信を複雑にすることなく、同じままにできる。

【００７９】

本明細書において、信頼済みデータサービスの配信を示す、様々な例示の非制限的な実施形態を記載する。これらの実施形態は、単独ではなくむしろ、適切な場合はお互いに組み合わせることが可能である。加えて、上述の実施形態のいずれかを、多数の代替の方法で拡張することができる。例えば、一実施形態において、信頼済みデータサービスは、データへのアクセスについてのより強力なセキュリティのために、トラップドアまたは機能の有効期限や取り消しを提供する。別の任意選択的な実施形態において、権利管理層を、信頼済みデータサービスの提供に組み込み、例えば、暗号化／復号化の一部としてコンテンツに付加される権利を保護して、またはプレーンテキスト内でより簡単に認識可能または検出可能なデジタルエスクローにおける著作権のあるデータに対する動作を阻止する。従って、本明細書に記載される実施形態の任意の組み合わせまたは置き換えを、本開示の範囲内で検討する。

【００８０】

例示の非制限的な実装

デジタルエスクローのパターンの例示の実装を、連合トラストオーバレイ(Federated Trust Overlay)（ＦＴＯ）と呼ぶ。付録Ａで添付されるものは、ＦＴＯの実装についての一部の追加の非制限的な詳細である。

【００８１】

この点において、デジタルエスクローのパターンは、単に多くの可能性のあるパターンおよび変形の実施例である。さらに、本パターン（これには、発行者、サブスクライバ、管理者および監査人、ならびに場合により上述した他の専門のロールも、関与する）を、ＣＴＰ、ＣＳＰ、ＣＫＧ等の「政教」分離を実行して、信頼を維持する別の基礎となるＦＴＯのパターンの上に積層する。お互いを干渉し合うことなく、およびお互いの存在を知ることさえも無く共存することができる、複数の独立したＦＴＯおよびＤＥＰもある。また、クラウドストレージサービスプロバイダが共に操作することなく、またはこれらのパターン／オーバレイの存在について知るようになることさえも無く、ＤＥＰおよびＦＴＯのパターンをクラウドストレージにオーバレイすことが可能である。

【００８２】

さらに詳細には、ＦＴＯは、クラウド内のデータサービスからは独立したサービスのセットである。これらのサービスは、データサービスのオペレータ以外の集団により操作され、および機密性、改ざんの検出、およびクラウドサービスにより提供されるデータに対する否認防止を考慮した強力な保証を提供することができる。

【００８３】

任意のパートナー、例えば、仲介サービス、検証サービス、ストレージ抽象化サービス等、がこれらのオーバレイサービスを構築および提供することができる。これらのパートナーは、参照の実装を提供すること、または公に利用可能な形式およびプロトコルに基づき自身が所有する実装を構築することを選択することができる。

【００８４】

形式、プロトコル、および参照の実装の公の性質が原因で、ＦＴＯのオペレータおよびデータの所有者等の集団の間の制御の分離を維持することは単純であろう。

【００８５】

暗号化が本解決策の要素である一方、異なる集団にわたって連合されるサービスの組織化も解決策の一部である。従来の暗号化技術が多くのシナリオに対して有力である一方、それらは改ざんの検出、否認防止、複数の（信頼できない）サービスを組織化することによる信頼の形成、データリポジトリの検索等のシナリオのの多くを可能にすることを排除する。

【００８６】

補足の文脈

ある追加の非制限的な文脈に対して、上述したように、クラウドが提供する信頼のあるものは、信頼の上に構築するクラウドのためのアプリケーションエコシステムを可能にする。本明細書において使用される種々の用語には、ＣＫＧ－鍵生成センタが含まれ、これは、複数テナントの鍵生成センタを提供するエンティティであり、例えば，マイクロソフト（登録商標）、ベリサイン（登録商標）、フィディリティ、ソブリン(Sovereign)エンティティ、エンタープライズ、コンプライアンスエンティティ等はいずれも、ＣＫＧを提供することができる。この点において、複数テナントは任意選択的である（例えば、命令ではなく希望する場合）。他の用語には、ＣＴＰ－暗号文技術プロバイダを含み、これは、信頼済みエコシステムで使用する暗号化技術を提供するエンティティであり、例えば、シマンテック（登録商標）、サーティコム（登録商標）、ボルテージ、ＰＧＰ　Ｃｏｒｐ、ＢｉｔＡｒｍｏｒ、エンタープライズ、ガーディアン(Guardian)、ソブリン(Sovereign)エンティティ等はいずれも、ＣＴＰとすることができる会社の例である。

【００８７】

加えて、用語ＣＳＰ－クラウドサービスプロバイダは、ストレージを含むクラウドサービスを提供するエンティティである。様々な会社がそのようなデータサービスを提供することができる。ＣＩＶ(Cloud Index Validator)－クラウドインデックスバリデータは、返されるインデックスを検証する第２のリポジトリである。ＣＳＡ－計算・ストレージ抽象化は、ストレージのバックエンドを抽象化する。ＳＴＦ－ストレージ転送形式は、データ／メタデータをリポジトリ全体で伝送する共通の形式である。

【００８８】

この点において、上述したように、あり企業のシナリオ(単数または複数）は、データサービスの技術またはアプリケーションを使用する工学エクストラネット(engineering extranet)、設計・工学分析、製造者と供給者(単数または複数）との間のデータ関係の定義等を含む。従って、一意的なエコシステムを、複数のエンティティにわたって信頼を分配することにより、様々なシナリオ全体に対して可能にして、「非常に」信頼できるエンティティも単一点情報漏洩も存在しないようにする。

【００８９】

検索可能な暗号化に関するある補足的な文脈について、ユーザは一般的にはキーワード(単数または複数）に対する「機能」または「トラップドア」を持ち、または取得して、およびその後、キーワード(単数または複数）を提示する「機能」を使用して要求をサーバに送信する。サーバは、機能とインデックスを「組み合せ」て、関連のある文書またはデータを見つける。ユーザに、検索の結果得られる文書のみへのアクセスを与える（ユーザは、それらの文書より多くのものへのアクセスを有している場合があるが）。

【００９０】

上述したように、１つのアルゴリズムが、本明細書に記載されるような検索可能に暗号化されたデータストアの提供に対する制限として解釈されるべきではないが、以下は例示の非制限的アルゴリズムの背景にある理論の一部を一般的に概説するものであり、および検索可能対称暗号（ＳＳＥ）のパターンの教材を提供する。

【００９１】

- Message: m
- Keywords: w_1, ...,w_n
- PRF: H
- Generating escrow key
- Choose random S for H
- Encrypting
- Choose random key K
- Choose random fixed-length r
- For 1 <= i <= n

Compute $a_i = H_s(w_i)$
Compute $b_i = H_{ai}(r)$
Compute $c_i = b_i \oplus flag$
Output $(E_K(m), r, c_1, \ldots, C_n)$
- Generating trapdoor or capability for w
- $d = H_{Sj}(w)$
- Testing for w
- Compute $p = H_d(r)$
- Compute $z = p \oplus C_i$
- Output "true" if z = flag
- Decrypt $E_K(m)$ to obtain m

【００９２】

再度、本明細書に記載される任意の実施形態に制限を与えるものとは見なされないが、以下は検索可能公開鍵暗号化（ＰＥＫＳ）のパターンに関する教材である。

Public-key encryption
a. PKE = (Gen,Enc,Dec)

Identity-based Encryption
b. IBE = (Gen,Enc,Extract,Dec)
c. Generating master keys
i. (msk,mpk) = IBE.Gen()
d. Encrypting m for ID
i. c = IBE.Enc(mpk,ID,m)
e. Generating secret key for ID
i. sk = IBE.Extract(msk,ID)
f. Decrypting
i. m = IBE.Dec(sk,c)
g. Message: m
h. Keywords: w_1, ...,w_n
i. Generating escrow keys
i. (msk,mpk) = IBE.Gen()
ii. (pk,sk) = PKE.GenO
j. Encrypting
k. For 1 < i < n
i. C1 = IBE.Enc(mpk,W1,flag)
l. Return (PKE.Enc(pk,m),Ci,...,Cn)
m. Generating capability or trapdoor for w
i. d = IBE.Extract(msk,w)
n. Testing for w
o. For 1 <= i <= n

i. z = IBE.DeC(d,c_i)
ii. Output "true" if z = flag
Decrypt EK (m) to obtain m

【００９３】

例示のネットワーク化分散環境

当業者は十分に理解できるであろうが、本明細書に記載される信頼済みクラウドサービスのフレームワークのための方法およびデバイスの種々の実施形態、ならびに関連する実施形態を、コンピュータネットワークの一部として、または分散コンピュータ環境において展開可能、ならびに任意の種類のデータストアに接続可能である、任意のコンピュータ、または他のクライアントデバイス、またはサーバデバイスとの関連で、実装することができる。この点において、本明細書に記載される種々の実施形態を、任意の数のメモリまたは記憶装置、ならびに任意の数の記憶装置にわたって起動する任意の数のアプリケーションおよび処理を有する、任意のコンピュータシステムまたはコンピュータ環境において実装することができる。これには、リモートストレージまたはローカルストレージを有する、ネットワーク環境、または分散コンピュータ環境において展開される、サーバコンピュータ、およびクライアントコンピュータを有する環境が含まれるが、これらに限定されない。

【００９４】

図３２は、例示のネットワーク化されたまたは分散されたコンピュータ環境の非制限的な概略図を提供する。分散コンピュータ環境は、コンピュータオブジェクト３２１０、３２１２等、およびコンピュータオブジェクトまたはコンピュータデバイス３２２０，３２２２、３２２４、３２２６、３２２８等を含み、これらはアプリケーション３２３０、３２３２、３２３４、３２３６、３２３８で表されるようなプログラム、メソッド、データストア、プログラマブルロジック等を含むことができる。オブジェクト３２１０、３２１２等、およびコンピュータオブジェクトまたはコンピュータデバイス３２２０、３２２２、３２２４、３２２６、３２２８等が、ＰＤＡ、音声／映像デバイス、携帯電話、ＭＰ３プレーヤ、ラップトップ等の異なるデバイスを含むことができることは、十分に理解できるであろう。

【００９５】

各オブジェクト３２１０、３２１２等、およびコンピュータオブジェクト、またはコンピュータデバイス３２２０、３２２２、３２２４、３２２６、３２２８等は、１つまたは複数の他のオブジェクト３２１０、３２１２等、およびコンピュータオブジェクト、またはコンピュータデバイス３２２０、３２２２、３２２４、３２２６、３２２８等と、通信ネットワーク３２４０を介して、直接または間接的に通信することができる。図３２においては単一の要素として例示されるが、ネットワーク３２４０は、図３２のシステムにサービスを提供する他のコンピュータオブジェクトおよびコンピュータデバイスを含むことができ、および／または、図示されない複数の相互に接続されたネットワークを表すことができる。各オブジェクト３２１０、３２１２等、または３２２０、３２２２、３２２４、３２２６、３２２８等はまた、ＡＰＩを使用するアプリケーション３２３０、３２３２、３２３４、３２３６、３２３８等のアプリケーション、または信頼済みクラウドコンピューティングサービス、もしくは種々の実施形態に従って提供されるようなアプリケーションとの通信またはその実装に適切な、他のオブジェクト、ソフトウェア、ファームウェアおよび／もしくはハードウェアを含むことができる。

【００９６】

分散コンピュータ環境を支援する様々なシステム、コンポーネント、およびネットワーク構造が存在する。例えば、コンピュータシステムを、有線または無線のシステム、ローカルネットワーク、または広範囲な分散ネットワークにより、まとめて接続することができる。現在、多くのネットワークがインターネットに連結され、これにより、広範囲に分散されたコンピューティングのインフラストラクチャを提供して、および多くの異なるネットワークを包含するが、任意のネットワークインフラストラクチャを、種々の実施形態

において記載されるような技術に付随する例示の通信に使用することができる。
【００９７】
従って、クライアント／サーバ、ピアツーピア、またはハイブリッドなアーキテクチャ等の、ネットワークトポロジ、およびネットワークインフラストラクチャの提供を利用することができる。クライアント／サーバアーキテクチャ、特にネットワーク化システムにおいて、クライアントは、通常、別のコンピュータ、例えばサーバにより提供される共有ネットワークリソースにアクセスするコンピュータである。図３２の説明図においては、非制限的な例として、コンピュータ３２２０、３２２２、３２２４、３２２６、３２２８等をクライアントと考えることができ、およびコンピュータ３２１０、３２１２等をサーバと考えることができ、この場合、サーバ３２１０、３２１２等は、クライアントコンピュータ３２２０、３２２２、３２２４、３２２６、３２２８等からのデータの受信、データの記憶、データの処理、クライアントコンピュータ３２２０、３２２２、３２２４、３２２６、３２２８等へのデータの伝送などのデータサービスを提供するが、任意のコンピュータを、状況に応じてクライアント、サーバ、または両方と見なすことができる。これらのコンピュータデバイスのいずれかが、データを処理しているか、または改良されたユーザのプロファイリング、および１つまたは複数の実施形態に対して本明細書に記載されるような関連する技術に関係し得るサービス、もしくはタスクを要求していることになる。
【００９８】
サーバは、一般的にインターネット、または無線ネットワークインフラストラクチャ等のリモートまたはローカルなネットワークを介してアクセス可能なリモートコンピュータシステムである。クライアントの処理は、第１のコンピュータシステムにおいてアクティブであり、およびサーバの処理は、第２のコンピュータシステムにおいてアクティブであり得、通信媒体を介してお互いに通信し、従って分散機能を提供し、および複数のクライアントがサーバの情報収集能力をうまく利用することができる。ユーザのプロファイリングに従って利用される任意のソフトウェアオブジェクトを、単独で提供して、および複数のコンピュータデバイスまたはオブジェクトにわたって分散することができる。
【００９９】
通信ネットワーク／バス３２４０がインターネットであるネットワーク環境において、例えば、サーバ３２１０、３２１２等は、クライアント３２２０、３２２２、３２２４、３２２６、３２２８等が、ＨＴＴＰ（ハイパーテキストプロトコル）等の任意の複数の既知のプロトコルを介して通信を行う、ウェブサーバとすることができる。サーバ３２１０、３２１２等はまた、分散コンピュータ環境の特徴であるように、クライアント３２２０、３２２２、３２２４、３２２６、３２２８等として機能することができる。
【０１００】
例示のコンピュータデバイス
上述したように、本明細書に記載される種々の実施形態は、任意のデバイスに適用され、それにおいて、１つまたは複数の信頼済みクラウドサービスのフレームワークを実装することが望ましい。従って、全ての種類のハンドヘルド、携帯機器、ならびに他のコンピュータデバイスおよびコンピュータオブジェクトは、本明細書に記載される種々の実施形態との関連で使用するため、すなわちデバイスが、信頼済みクラウドサービスのフレームワークに関連して何らかの機能性を提供し得る場合は全て、予想されると考えられることは理解されるはずである。従って、図３３において記載される以下の汎用のリモートコンピュータは、ほんの一例にすぎず、および本開示の実施形態を、ネットワーク／バスの相互運用性および相互作用性を有する任意のクライアントと共に実装することができる。
【０１０１】
必要ではないが、実施形態のいずれかを、オペレーティングシステムを介して部分的に実装して、デバイスまたはオブジェクトのサービスの開発者が使用できるようにすることができ、および／または操作可能なコンポーネント(単数または複数）に関連して操作するアプリケーションソフトウェア内に含めることができる。ソフトウェアを、クライアン

トワークステーション、サーバ、または他のデバイス等の１つまたは複数のコンピュータにより実行される、プログラムモジュール等のコンピュータ実行可能命令の一般的な文脈で記載することができる。当業者は理解するであろうが、ネットワークインタラクションを、様々なコンピュータシステム構造およびプロトコルと共に実装することができる。

【０１０２】

従って、図３３は、１つまたは複数の実施形態を実装することができる適切なコンピュータシステム環境３３００の一例を示すが、上記で明らかにされたように、コンピュータシステム環境３３００は、適切なコンピュータ環境の単なる一実施例であり、および実施形態のうちのいずれかの使用または機能の範囲について任意の制限を示唆することは意図されない。また、コンピュータ環境３３００を、例示の動作環境３３００に示されるコンポーネントの任意の１つまたは組み合わせに関して任意の依存性または要件を有するものとして解釈しない。

【０１０３】

図３３を参照すると、本明細書における１つまたは複数の実施形態を実装する例示のリモートデバイスは、ハンドヘルドコンピュータ３３１０の形式の汎用コンピュータデバイスを含むことができる。ハンドヘルドコンピュータ３３１０のコンポーネントは、プロセスユニット３３２０、システムメモリ３３３０、およびシステムメモリを含む種々のシステムコンポーネントをプロセスユニット３３２０に結合するシステムバス３３２１を含むことができるが、これに限定されない。

【０１０４】

コンピュータ３３１０は典型的は、様々なコンピュータ可読媒体を含み、およびコンピュータ３３１０によりアクセス可能な任意の利用可能な媒体とすることができる。システムメモリ３３３０は、ＲＯＭ(read only memory)および／またはＲＡＭ(random access memory)等の揮発性および／または不揮発性メモリの形式のコンピュータ記憶媒体を含むことができる。制限ではなく実施例として、メモリ３３３０はまた、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、およびプログラムデータを含むことができる。

【０１０５】

ユーザは、入力装置３３４０を介してコンピュータ３３１０にコマンドおよび情報を入力することができる。モニタまたは他のタイプの表示デバイスも、出力インターフェース３３５０等のインターフェースを介してシステムバス３３２１に接続する。モニタに加えて、コンピュータはまた、出力インターフェース３３５０を介して接続可能な、スピーカ、およびプリンタ等の他の周辺出力装置を含むことができる。

【０１０６】

コンピュータ３３１０は、リモートコンピュータ３３７０等の１つまたは複数の他のリモートコンピュータへの論理接続を使用して、ネットワーク化または分散された環境において操作することができる。リモートコンピュータ３３７０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、ピアツーピアデバイスもしくは他の共通のネットワークノード、または任意の他のリモート媒体の消費もしくは伝送デバイスとすることができ、およびコンピュータ３３１０に関して上述した要素のいずれかまたは全てを含むことができる。図３３に示される論理接続は、ＬＡＮ（ローカルエリアネットワーク）、またはＷＡＮ（ワイドエリアネットワーク）等のネットワーク３３７１を含むが、他のネットワーク／バスも含むことができる。そのようなネットワーク環境は、家庭、事務所、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において一般的なものである。

【０１０７】

上述したように、例示の実施形態を、種々のコンピュータデバイス、ネットワーク、および広告のアーキテクチャに関連して記載してきたが、基礎となる概念を、クラウドサービスとの対話に関連して信頼を提供することが望ましい、任意のネットワークシステム、および任意のコンピュータデバイスまたはシステムに対して適用することができる。

【０１０８】
本明細書に記載される１つまたは複数の実施形態を実装する方法は複数存在し、例えば適切なＡＰＩ、ツールキット、ドライバコード、オペレーティングシステム、制御、単独のまたはダウンロード可能なソフトウェアオブジェクト等があり、これにより、アプリケーションおよびサービスが信頼済みクラウドサービスのフレームワークを使用することが可能になる。実施形態を、ＡＰＩ（または他のソフトウェアオブジェクト）の観点から、同様に、１つまたは複数の記載される実施形態に従って、サービスを提供するソフトウェアオブジェクトまたはハードウェアオブジェクトの観点から、考えることができる。本明細書に記載される種々の実装および実施形態は、全体としてハードウェア、部分的にハードウェア、および部分的にソフトウェア、また同様にソフトウェアにおける態様を有することができる。

【０１０９】
「例示の」という単語を、本明細書において使用して、例、事例または実例の意味となる。誤解を避けるために、本明細書に開示される主題は、そのような例に限定されない。加えて、本明細書に「例示の」ものとして記載される任意の態様または設計を、必ずしも他の態様または設計よりも好ましいまたは有利であると解釈するわけではなく、また当業者には既知の等価の例示の構造および技術を排除することも意味されない。さらに、発明を実施するための形態または特許請求の範囲で、用語「含む」「有する」「含有する」および他の同様の言葉を使用する範囲において、誤解を避けるために、そのような用語は、任意の追加のまたは他の要素を排除することなく、開放遷移語(open transition word)としての用語「備える」と同様に包括的であることを意図する。

【０１１０】
上述したように、本明細書に記載される種々の技術は、ハードウェアもしくはソフトウェア、または適切な場合には両者の組み合わせとの関連で実装することができる。本明細書で使用される時、用語「コンポーネント」「システム」などは、同様に、コンピュータ関連エンティティ、すなわちハードウェア、ハードウェアとソフトウェアの組み合わせ、ソフトウェア、または実行中のソフトウェアを参照することを意図する。例えば、コンポーネントは、プロセッサ上で稼働中の処理、プロセッサ、オブジェクト、実行ファイル、実行のスレッド、プログラム、および／またはコンピュータとすることができるが、これらに限定されない。例として、コンピュータ上で実行中のアプリケーション、およびコンピュータの両方を、コンポーネントとすることができる。１つまたは複数のコンポーネントは、処理および／または実行のスレッド内に存在し、ならびにコンポーネントを、１つのコンピュータ上でローカライズして、および／または２つ以上のコンピュータ間で分散する。

【０１１１】
上述したシステムを、いくつかのコンポーネント間の相互作用に関して記載した。そのようなシステムおよびコンポーネントが、それらのコンポーネントまたは特定のサブコンポーネント、特定のコンポーネントまたはサブコンポーネントの内のいくつか、および／または追加のコンポーネント、ならびに前述のものの種々の置き換えおよび組み合わせによるものを含むことができることは十分に理解できるであろう。サブコンポーネントはまた、（階層的に）親のコンポーネント内に含まれるよりもむしろ、他のコンポーネントに通信可能に連結されるコンポーネントとして実装可能である。加えて、１つまたは複数のコンポーネントを、統合的な機能性を提供する単一のコンポーネントに組み合わせても、またはいくつかの別個のサブコンポーネントに分割してもよく、および管理層等の任意の１つまたは複数の中間層を提供して、そのようなサブコンポーネントに通信可能に連結させ、統合された機能性を提供することができる。本明細書に記載される任意のコンポーネントはまた、本明細書に特には記載されないが、当業者には一般に知られる１つまたは複数の他のコンポーネントと相互作用することもできる。

【０１１２】
上記に記載される例示のシステムを考えると、開示される主題に従って実装できる方法

論を、種々の図面のフローチャートを参照してより十分に理解できるであろう。説明を簡単にする目的で、方法論を一連のブロックとして示し、および記載するが、特許請求の範囲に記載される主題をブロックの順番により制限せず、いくつかのブロックを本明細書に示して、および記載するものとは異なる順番および／または他のブロックと同時に起こり得ることは理解および認識すべきである。連続しない、すなわち分岐するフローをフローチャートを介して示す場合、同一または同様の結果を達成する種々の他の分岐、フロー経路、およびブロックの順番を実装できることは理解できるであろう。さらに、例示される全てのブロックを、以下に記載される方法論の実装に必要とするわけではない。

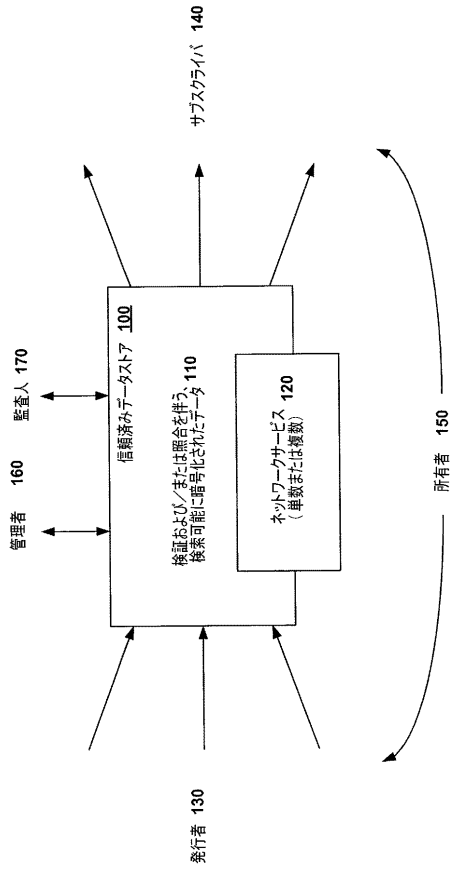
【０１１３】

ある実施形態において、クライアント側の見地を示すが、誤解を避けるために、対応するサーバ側の見地が存在し、その逆も同様であることは理解すべきである。同様に、方法を実装する場合、１つまたは複数のコンポーネントを介してその方法を実装するために構成されるストレージおよび少なくとも１つのプロセッサを有する対応するデバイスを提供することができる。

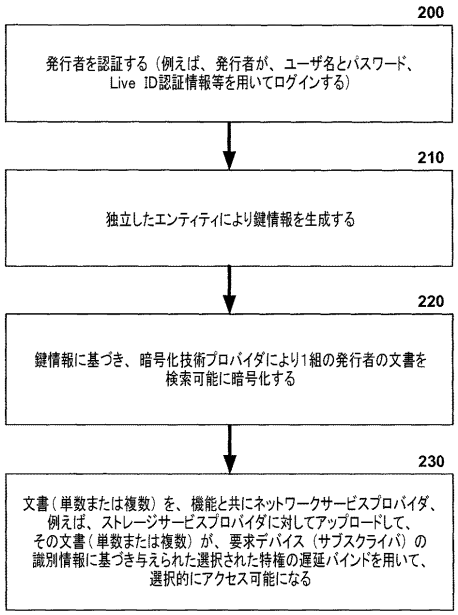
【０１１４】

種々の実施形態を、種々の図面の好ましい実施形態と関連して記載してきたが、他の同様の実施形態を使用することができ、または記載される実施形態に変形および追加を行って、そこから逸脱することなく同一の機能を実行することができることは理解すべきである。さらに、上記に記載される実施形態の内の１つまたは複数の態様は、複数の処理チップまたは処理デバイスにおいてまたはそれら全体にわたって実装することができ、および複数のデバイスにわたって同様にストレージを達成することができる。従って、本発明を、任意の単一の実施形態に限定すべきではなく、むしろ添付の特許請求の犯意に従う幅および範囲で解釈すべきである。

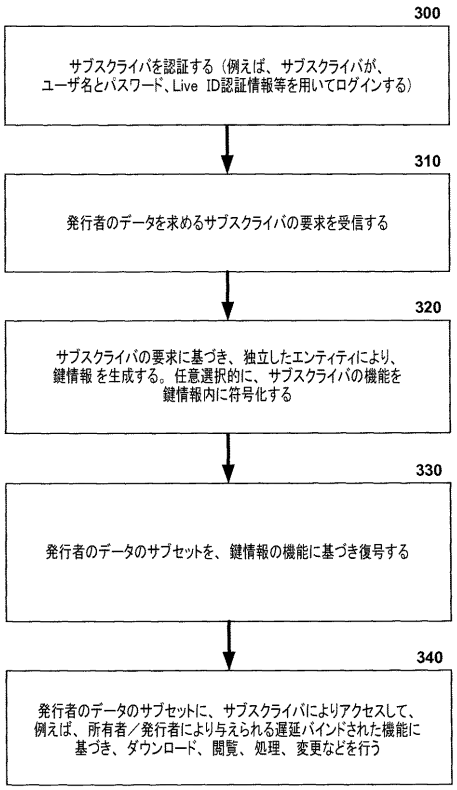
【図１】



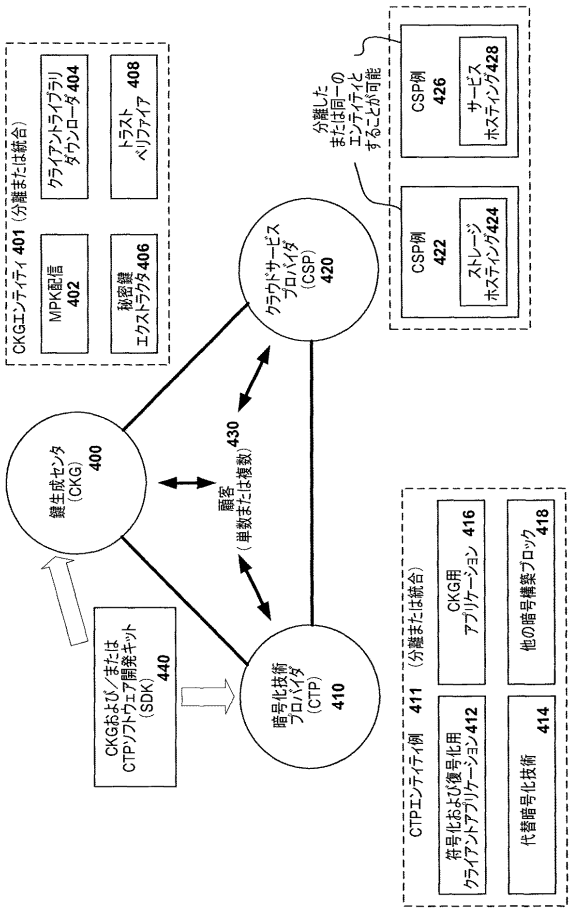
【図２】



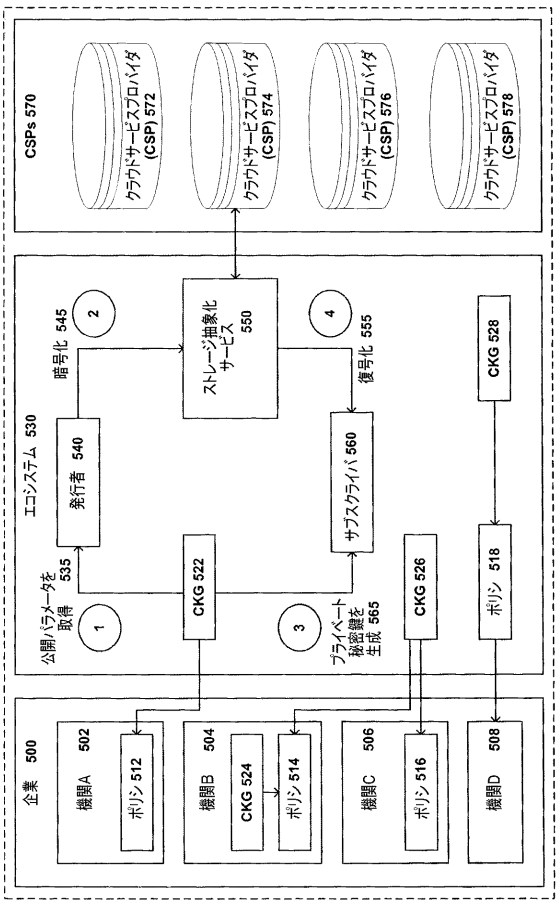
【図３】


300
サブスクライバを認証する（例えば、サブスクライバが、ユーザ名とパスワード、Live ID認証情報等を用いてログインする）
310
発行者のデータを求めるサブスクライバの要求を受信する
320
サブスクライバの要求に基づき、独立したエンティティにより、鍵情報を生成する。任意選択的に、サブスクライバの機能を鍵情報内に符号化する
330
発行者のデータのサブセットを、鍵情報の機能に基づき復号する
340
発行者のデータのサブセットに、サブスクライバによりアクセスして、例えば、所有者／発行者により与えられる遅延バインドされた機能に基づき、ダウンロード、閲覧、処理、変更などを行う

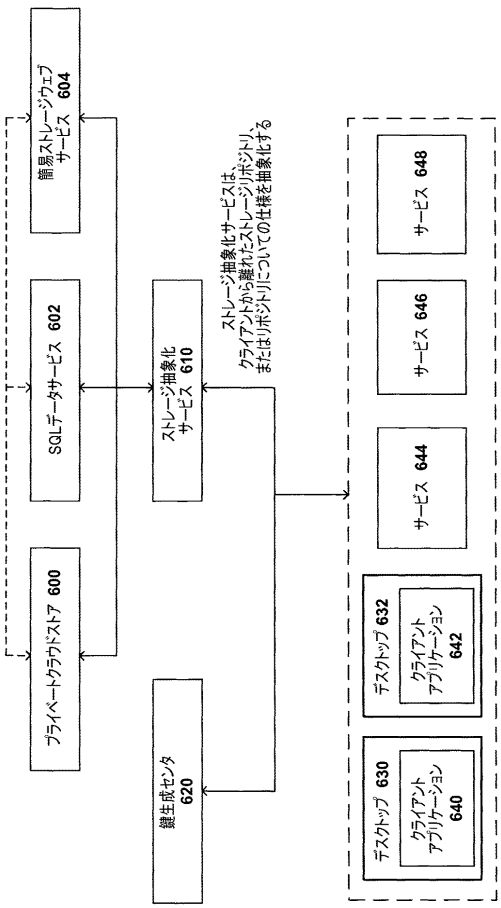
【図４】


CKGエンティティ 401（分離または統合）
クライアントライブラリダウンローダ 404
トラストベリファイア 408
MPK配信 402
秘密鍵エクストラクタ 406
鍵生成センタ（CKG）400
CKGおよび／またはCTPソフトウェア開発キット（SDK）440
暗号化技術プロバイダ（CTP）410
クラウドサービスプロバイダ（CSP）420
顧客（単数または複数）430
分離したまたは同一のエンティティとすることが可能
CSP例 426
サービスホスティング 428
CSP例 422
ストレージホスティング 424
CTPエンティティ例 411（分離または統合）
符号化および復号化用クライアントアプリケーション 412
CKG用アプリケーション 416
代替暗号化技術 414
他の暗号構築ブロック 418

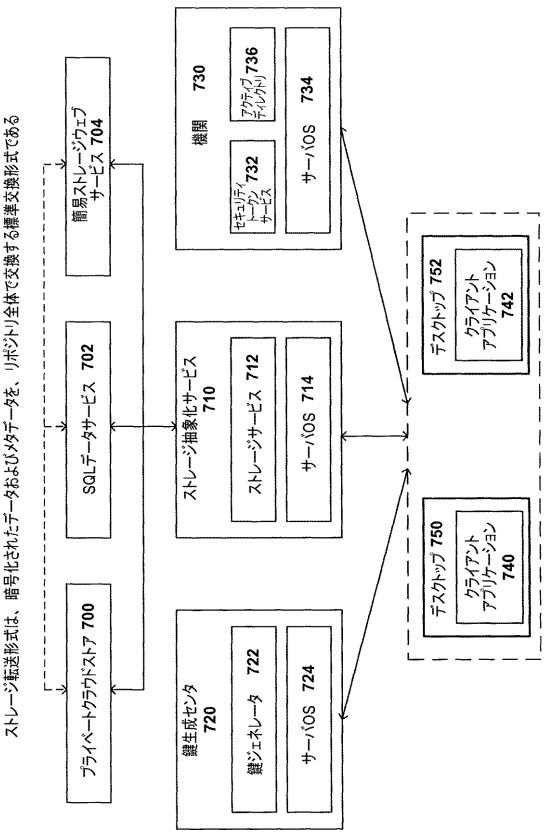
【図５】


CSPs 570
クラウドサービスプロバイダ（CSP）572
クラウドサービスプロバイダ（CSP）574
クラウドサービスプロバイダ（CSP）576
クラウドサービスプロバイダ（CSP）578
エコシステム 530
ストレージ抽象化サービス 550
暗号化 545
発行者 540
公開パラメータを取得 535
CKG 522
サブスクライバ 560
復号化 555
プライベート秘密鍵を生成 565
CKG 528
CKG 526
ポリシ 518
企業 500
機関A 502
ポリシ 512
機関B 504
CKG 524
ポリシ 514
機関C 506
ポリシ 516
機関D 508

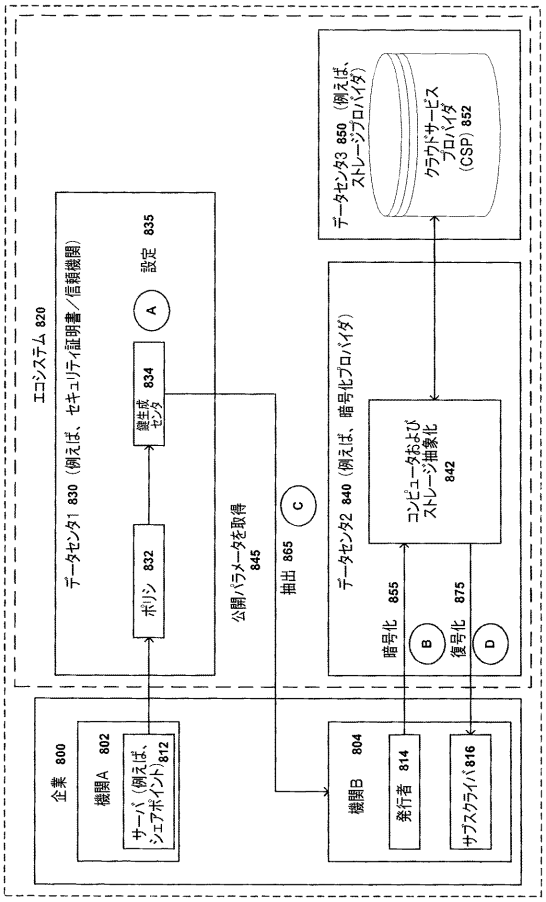
【図６】


簡易ストレージウェブサービス 604
SQLデータサービス 602
プライベートクラウドストア 600
ストレージ抽象化サービス 610
ストレージ抽象化サービスは、クライアントから隠れたストレージリポジトリ、またはリポジトリについての仕様を抽象化する
鍵生成センタ 620
サービス 644
サービス 646
サービス 648
デスクトップ 632
クライアントアプリケーション 642
デスクトップ 630
クライアントアプリケーション 640

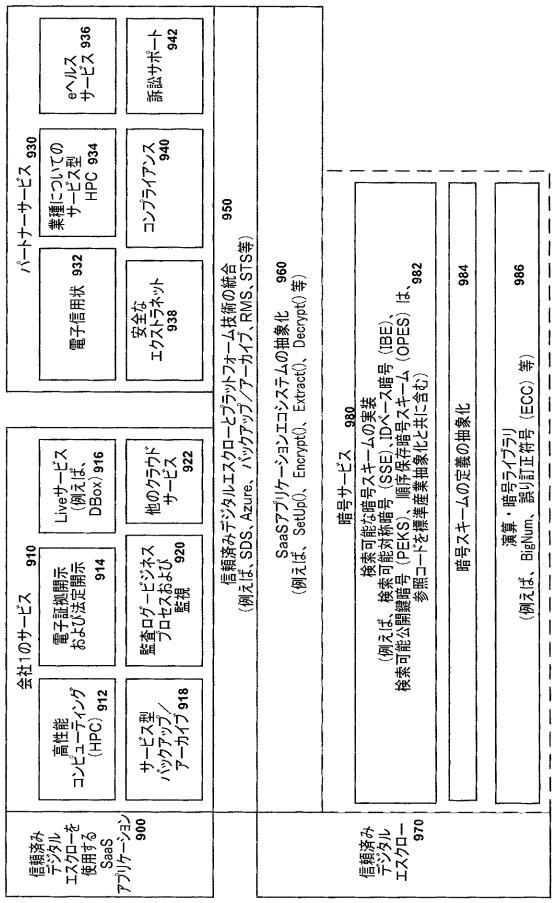
【図７】


ストレージ転送形式は、暗号化されたデータおよびメタデータを、リポジトリ全体で交換する標準交換形式である
プライベートクラウドストア 700
SQLデータサービス 702
簡易ストレージウェブサービス 704
鍵生成センタ 720
鍵ジェネレータ 722
サーバOS 724
ストレージ抽象化サービス 710
ストレージサービス 712
サーバOS 714
機関 730
セキュリティトークンサービス 732
アクティブディレクトリ 736
サーバOS 734
デスクトップ 750
クライアントアプリケーション 740
デスクトップ 752
クライアントアプリケーション 742

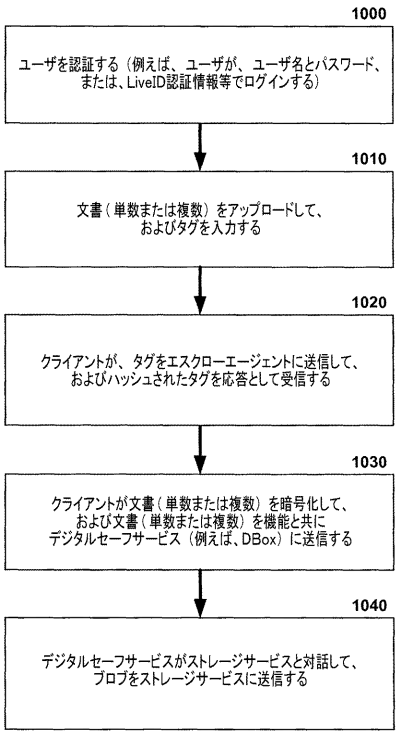
【図８】


エンタープライズ 820
データセンタ1 830（例えば、セキュリティ証明書／信頼機関）
ポリシ 832
鍵生成センタ 834
A
設定 835
公開パラメータを取得 845
抽出 865
C
データセンタ2 840（例えば、暗号化プロバイダ）
暗号化 855
B
復号化 875
D
コンピューティングおよびストレージ抽象化 842
データセンタ3 850（例えば、ストレージプロバイダ）
クラウドサービスプロバイダ（CSP）852
企業 800
機関A 802
サーバ（例えば、シェアポイント）812
機関B 804
発行者 814
サブスクライバ 816

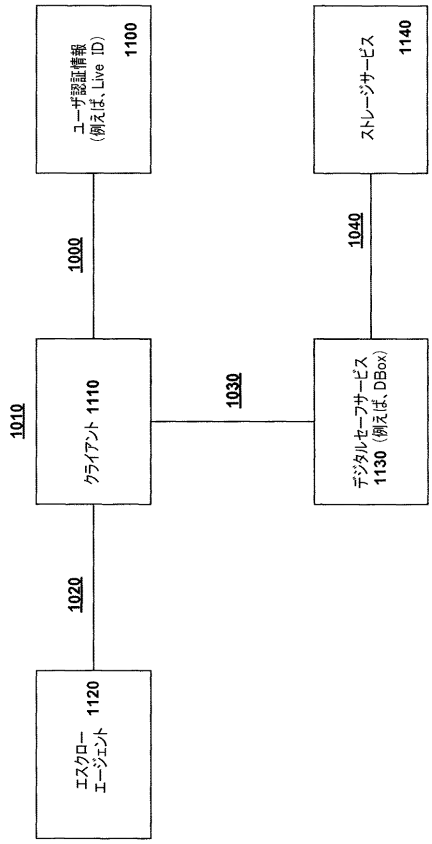
【図９】


信頼済みデジタルエスクローを使用するSaaSアプリケーション 900
会社1のサービス 910
高性能コンピューティング（HPC）912
電子証拠開示および法定開示 914
監査ログ ビジネスプロセスおよび監視 920
サービス型バックアップ／アーカイブ 918
Liveサービス（例えば、DBox）916
他のクラウドサービス 922
パートナーサービス 930
電子信用状 932
業種についてのサービス型HPC 934
安全なエクストラネット 938
コンプライアンス 940
eヘルスサービス 936
訴訟サポート 942
信頼済みデジタルエスクローとプラットフォーム技術の統合（例えば、SDS、Azure、バックアップ／アーカイブ、RMS、STS等）950
SaaSアプリケーションエコシステムの抽象化 960（例えば、SetUp()、Encrypt()、Extract()、Decrypt()等）
暗号サービス 980
検索可能な暗号スキームの実装（例えば、検索可能対称暗号（SSE）、IDベース暗号（IBE）、検索可能公開鍵暗号（PEKS）、順序保存暗号スキーム（OPES）は、参照コードを標準産業抽象化と共に含む）982
暗号スキームの定義の抽象化 984
演算・暗号ライブラリ（例えば、BigNum、誤り訂正符号（ECC）等）986
信頼済みデジタルエスクロー 970

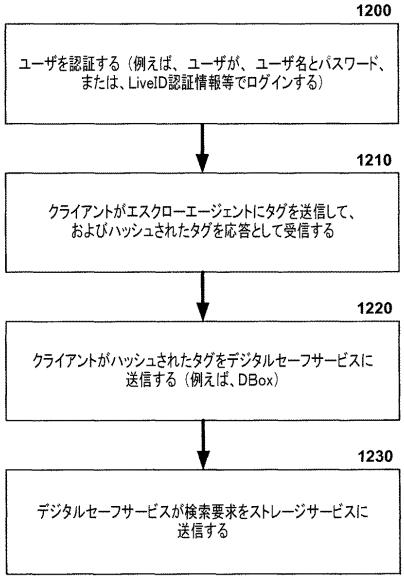
【図１０】


1000
ユーザを認証する（例えば、ユーザが、ユーザ名とパスワード、または、LiveID認証情報等でログインする）
1010
文書（単数または複数）をアップロードして、およびタグを入力する
1020
クライアントが、タグをエスクローエージェントに送信して、およびハッシュされたタグを応答として受信する
1030
クライアントが文書（単数または複数）を暗号化して、および文書（単数または複数）を機能と共にデジタルセーフサービス（例えば、DBox）に送信する
1040
デジタルセーフサービスがストレージサービスと対話して、プロブをストレージサービスに送信する

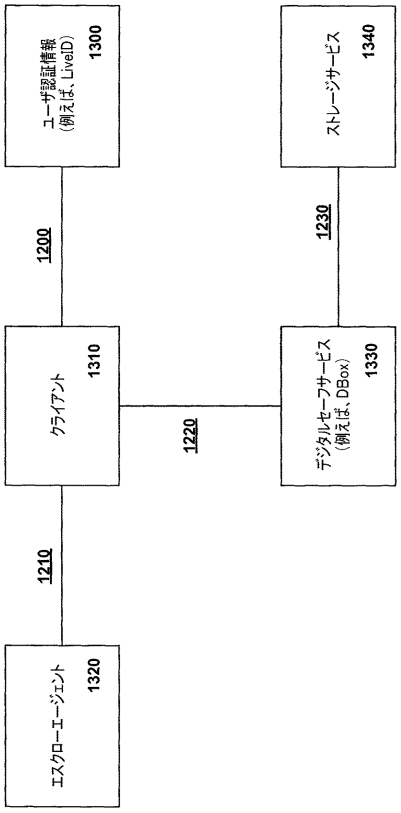
【図１１】



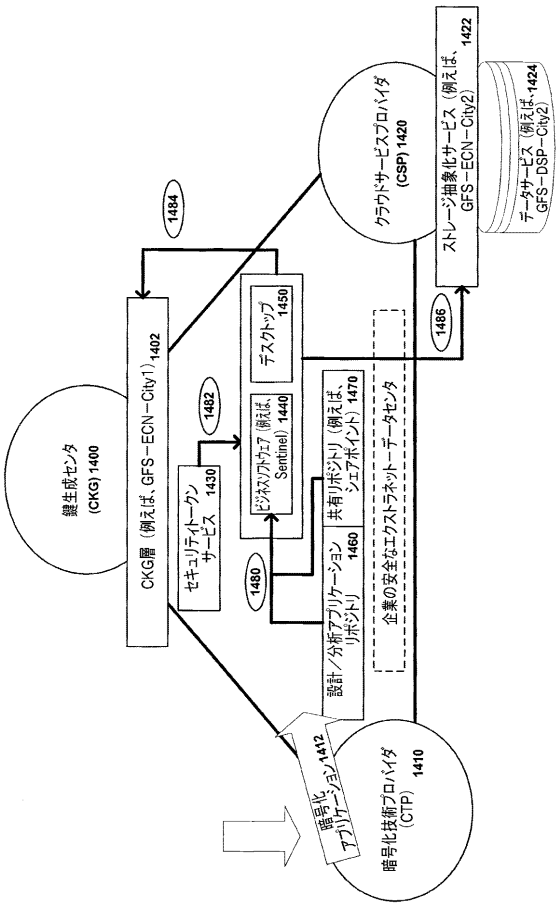
【図１２】



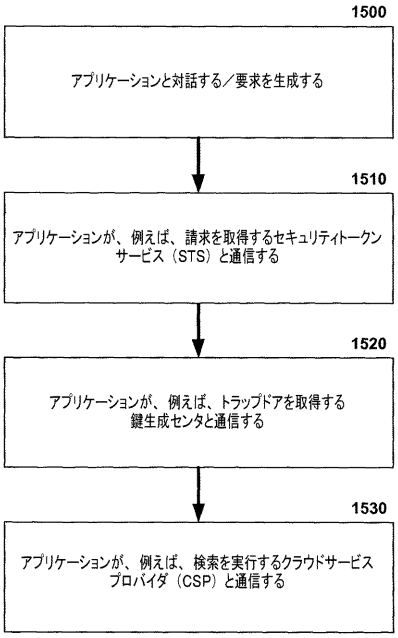
【図１３】



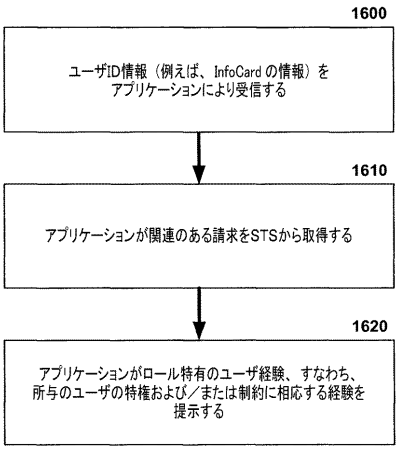
【図１４】



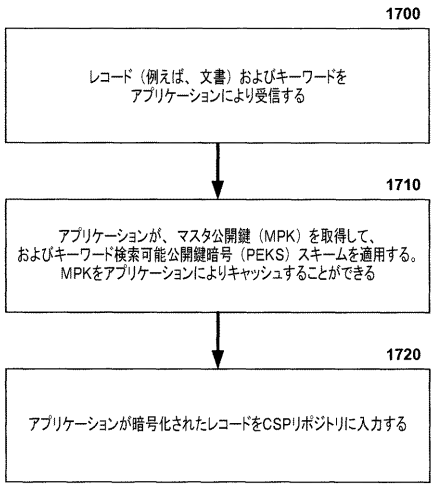
【図１５】



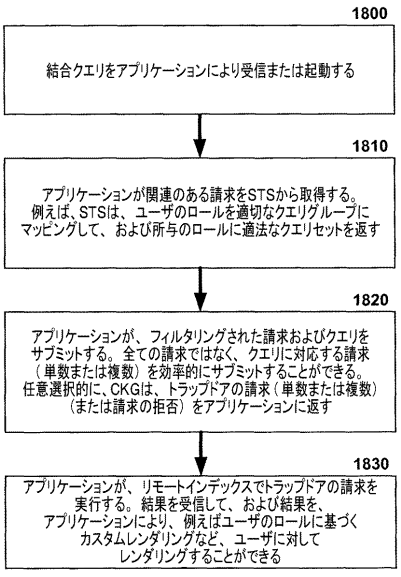
【図１６】



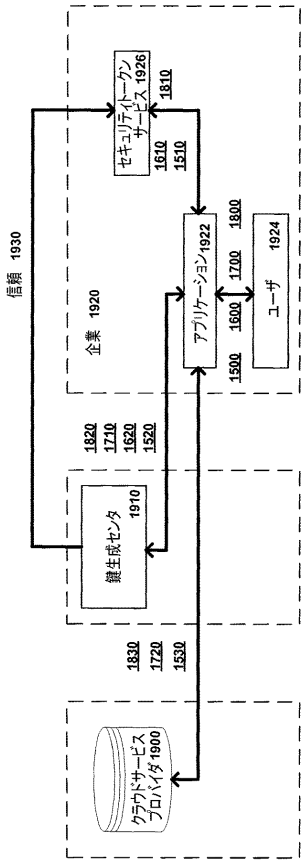
【図１７】



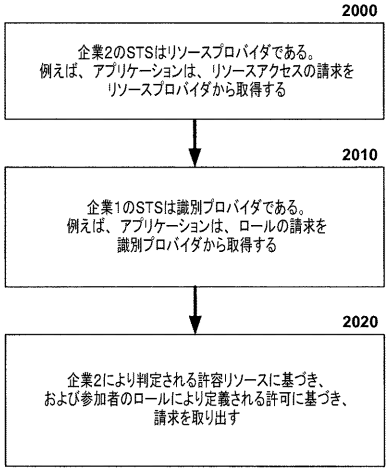
【図１８】



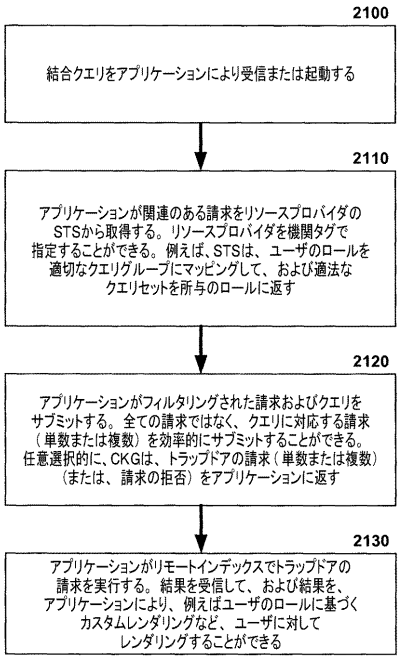
【図１９】



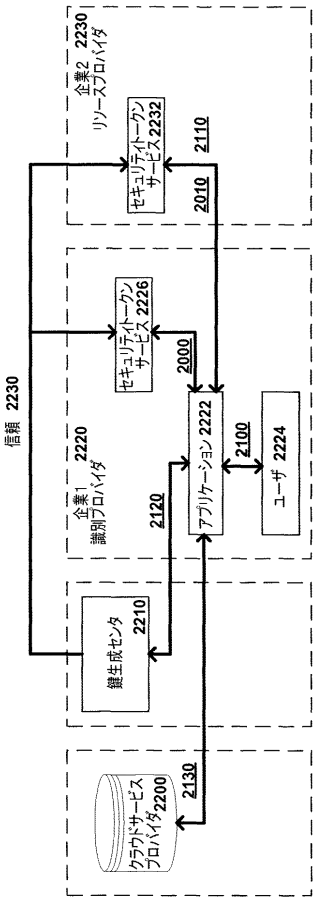
【図２０】



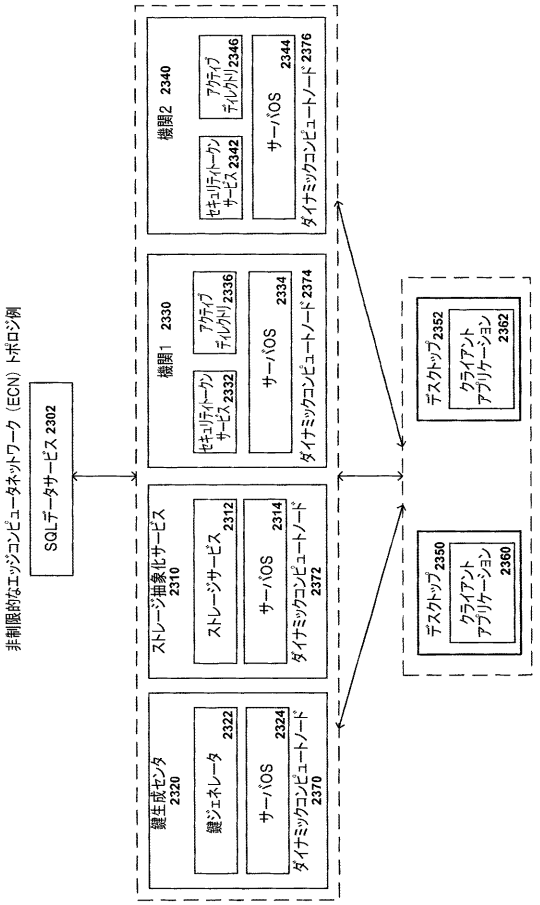
【図２１】



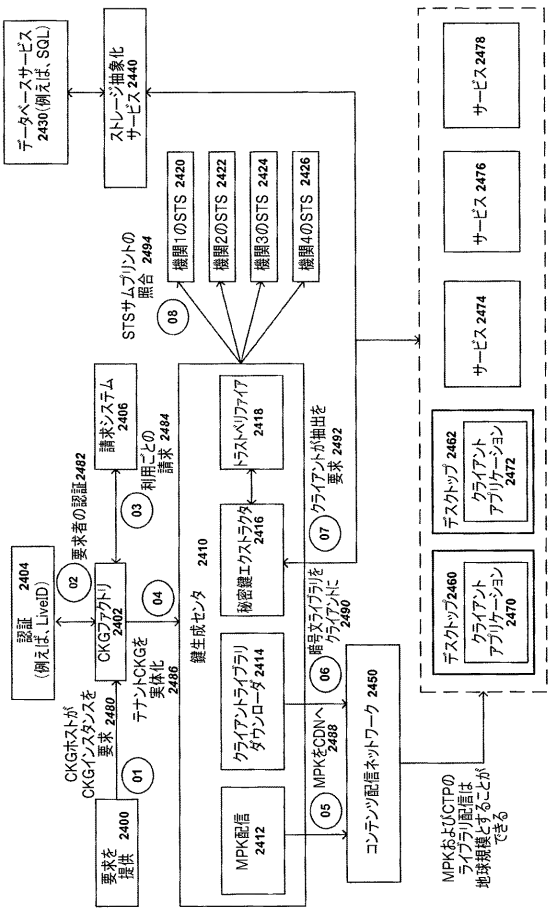
【図２２】



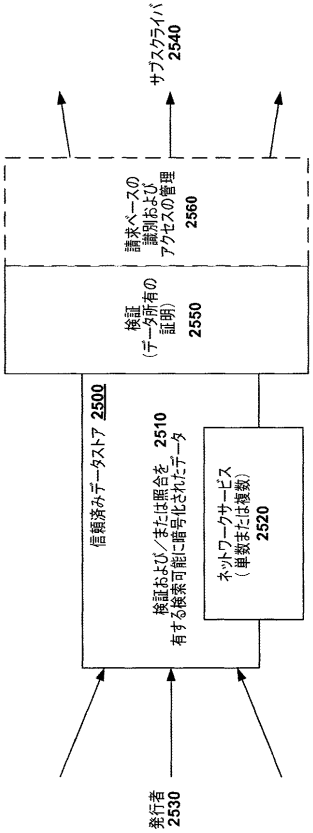
【図２３】



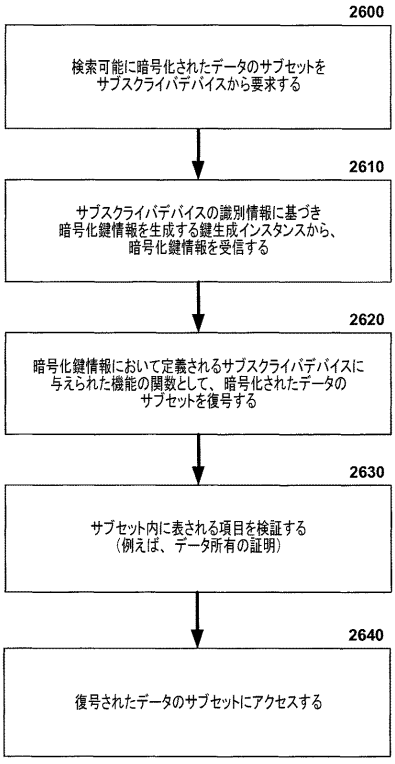
【図２４】



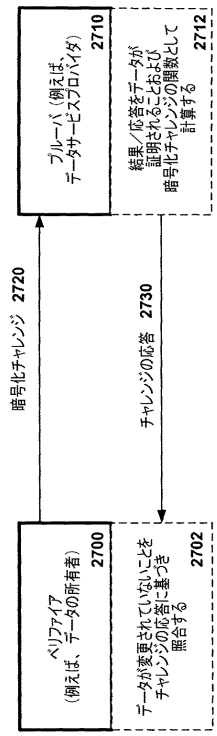
【図２５】



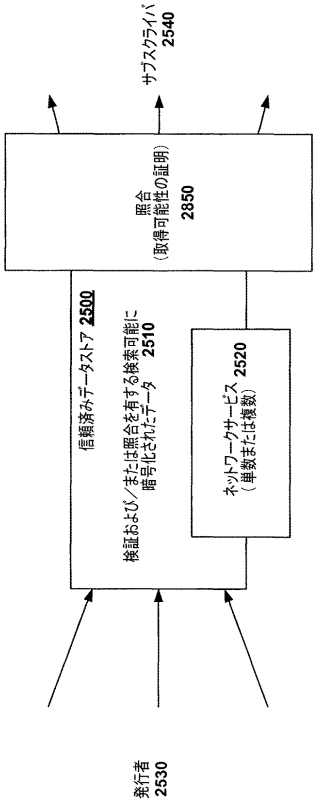
【図２６】



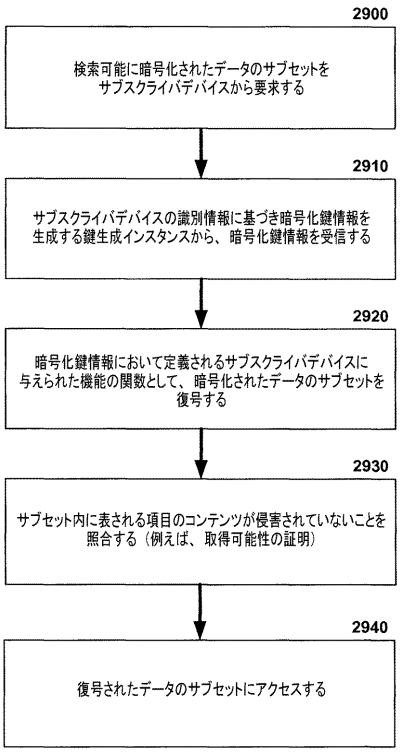
【図２７】



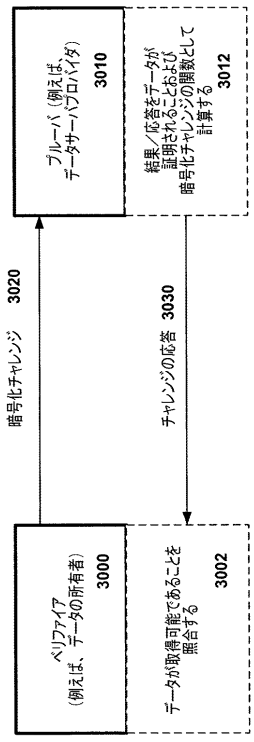
【図２８】



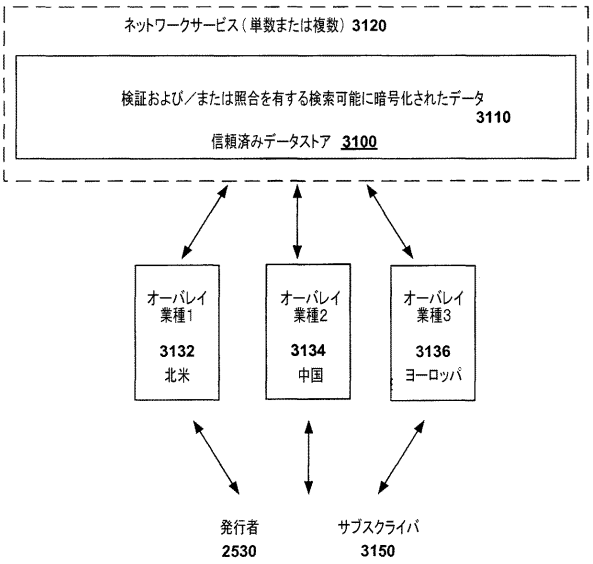
【図２９】



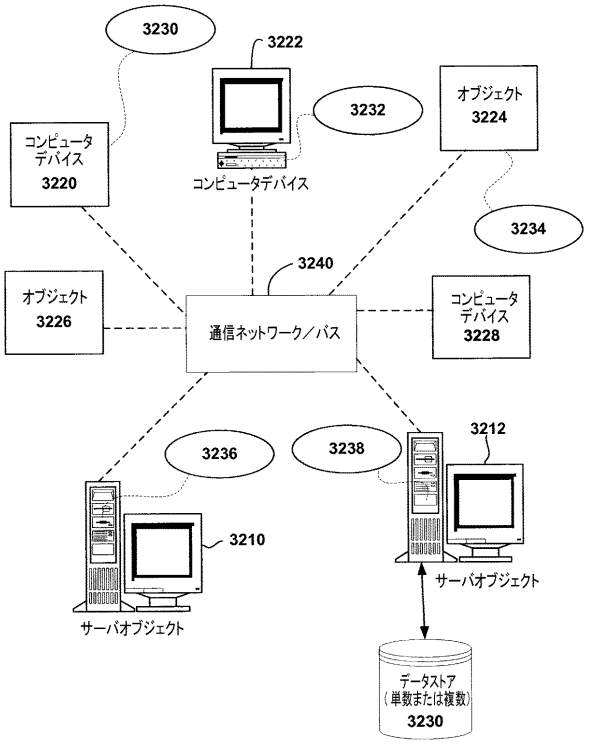
【図３０】



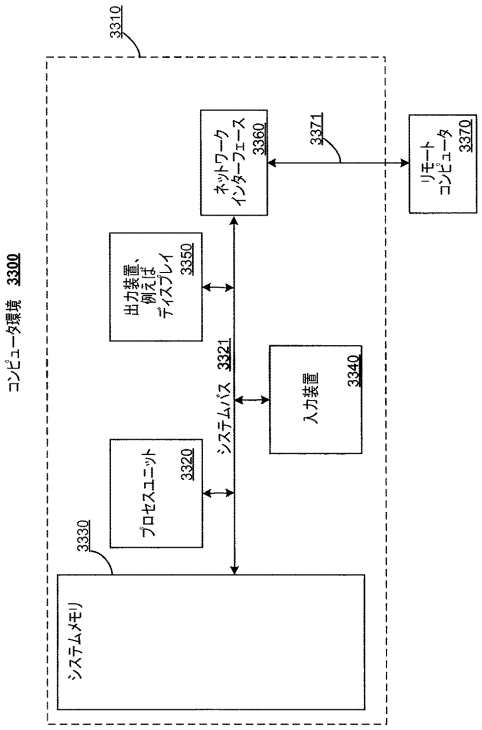
【図３１】


ネットワークサービス（単数または複数）3120
検証および／または照合を有する検索可能に暗号化されたデータ
3110
信頼済みデータストア 3100
オーバレイ業種1
3132
北米
オーバレイ業種2
3134
中国
オーバレイ業種3
3136
ヨーロッパ
発行者
2530
サブスクライバ
3150

【図３２】


3230
3222
3232
オブジェクト
3224
コンピュータデバイス
3220
コンピュータデバイス
3234
3240
オブジェクト
3226
通信ネットワーク／バス
コンピュータデバイス
3228
3212
3236
3238
3210
サーバオブジェクト
サーバオブジェクト
データストア
（単数または複数）
3230

【図３３】


3310
コンピュータ環境 3300
ネットワークインターフェース 3360
3371
リモートコンピュータ 3370
出力装置、例えば、ディスプレイ 3350
システムバス 3321
入力装置 3340
プロセスユニット 3320
3330
システムメモリ

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2010/023239

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i, G06F 21/00(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)

H04L 9/32; H04L 9/10; H04L 9/30; H04L 9/00

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
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: could, grid, SaaS, software as a service, iaas, naas, ipmass, cryptogra*, encrypt*, decrypt*, identity, capability, privileg*, authenticat*

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008-0091613 A1 (William H. Gates et al.) 17 April 2008 See abstract; figures 1-3; page 2, paragraph 26 - page 3, paragraph 34	1-15
X	US 2008-0066185 A1 (James Lester et al.) 13 March 2008 See abstract; figures 1-3; page 1, paragraph 14 - page 4, paragraph 39	1-15
A	US 2008-0080718 A1 (Henricus Johannes Maria Meijer et al.) 03 April 2008 See abstract; figures 1 and 4; page 2, paragraph 25 - page 4, paragraph 53	1-15
A	US 2008-0083025 A1 (Henricus Johannes Maria Meijer et al.) 03 April 2008 See abstract; figures 1-4; page 3, paragraph 33 - page 4, paragraph 47	1-15

☐ 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
09 SEPTEMBER 2010 (09.09.2010)	**09 SEPTEMBER 2010 (09.09.2010)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Lee Hyoung Il Telephone No. 82-42-481-8199

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2010/023239

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0091613 A1	17.04.2008	CA 2659408 A1	04.09.2008
		CN 101523365 A	02.09.2009
		EP 2076840 A2	08.07.2009
		JP 2010-505206 A	18.02.2010
		US 2008-0082448 A1	03.04.2008
		WO 2008-105937 A2	04.09.2008
		WO 2008-105937 A3	08.01.2009
US 2008-0066185 A1	13.03.2008	CN 101512479 A	19.08.2009
		WO 2008-033445 A2	20.03.2008
		WO 2008-033445 A3	16.10.2008
US 2008-0080718 A1	03.04.2008	US 2008-0083036 A1	03.04.2008
US 2008-0083025 A1	03.04.2008	US 2008-0083040 A1	03.04.2008

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,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,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,PE,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 ロイ ピーター デスーザ
アメリカ合衆国 ９８０５２－６３９９ 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－インターナショナル パテンツ内

Ｆターム(参考) 5J104 AA07 AA12 AA16 AA32 EA01 EA04 EA08 EA18 JA03 JA21
KA01 NA02 NA36 NA37 PA07