(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2020-9500
(P2020-9500A)
(43)公開日　令和2年1月16日(2020.1.16)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/60	(2013.01)	G06F	21/60	320	
G06F 21/62	(2013.01)	G06F	21/62	318	

審査請求 有　請求項の数 20　ＯＬ　（全 45 頁）

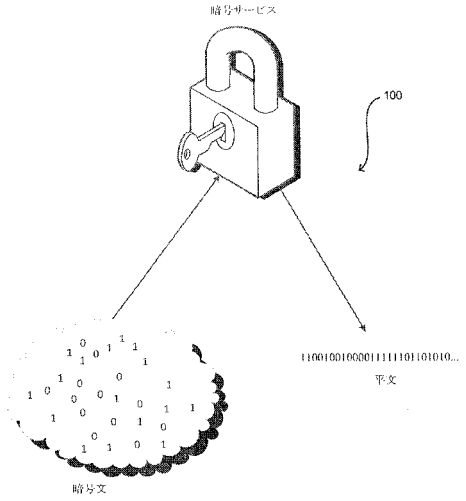
(21)出願番号　特願2019-190480 (P2019-190480)
(22)出願日　令和1年10月17日 (2019.10.17)
(62)分割の表示　特願2017-217362 (P2017-217362)の分割
原出願日　平成26年2月7日 (2014.2.7)
(31)優先権主張番号　13/764,963
(32)優先日　平成25年2月12日 (2013.2.12)
(33)優先権主張国・地域又は機関
米国 (US)

(71)出願人　506329306
アマゾン　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　９８１０８－１２２６
ワシントン州　シアトル　ピーオー　ボックス　８１２２６
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　グレゴリー　ブランチェク　ロス
アメリカ合衆国　９８１０９－５２１０
ワシントン州　シアトル　テリー　アベニュー　ノース　４１０

最終頁に続く

(54)【発明の名称】データセキュリティサービス

(57)【要約】
【課題】分散コンピューティングリソースを含む環境における、強化されたデータセキュリティを可能にする。
【解決手段】分散コンピューティング環境は、暗号サービスを利用する。暗号サービスは、１つ以上のエンティティのために鍵を安全に管理する。暗号サービスは、暗号化及び解読等の暗号動作を実行するための要求を受信し、それに応答するように構成される。要求は、分散コンピューティング環境及び／または分散コンピューティング環境のサブシステムを使用するエンティティから由来し得る。
【選択図】図１



【特許請求の範囲】
【請求項１】
データストレージサービスを提供するコンピュータ実行方法であって、
コンピューティングリソースサービスプロバイダに関連付けられた顧客装置から、暗号サービスに関連付けられたポリシーに関連する情報を取得することであって、前記ポリシーは、前記コンピューティングリソースサービスプロバイダの暗号サービスによって生成された暗号情報の制限を含む、ことと、
前記ポリシーを処理して、前記暗号サービスに、前記暗号情報の前記制限を課すことと、
前記暗号情報が前記暗号サービスにのみアクセス可能となるように、前記暗号サービスに、前記制限に従って、前記暗号情報を使用してデータを暗号化または復号させることであって、前記データを暗号化または復号させることは、前記制限に少なくとも部分的に基づいて、前記暗号サービスが、前記暗号サービスによって格納された複数の暗号情報の中から暗号情報を選択することを可能にすることを含む、ことと、
前記暗号情報の使用の結果を提供することと
を備えるコンピュータ実行方法。
【発明の詳細な説明】
【背景技術】
【０００１】
関連出願の相互参照
本出願は、2013年2月12日出願の米国特許出願番号13/764,963の優先権を主張するものであり、その内容は参照によりその全体が本明細書内に組み込まれる。本出願は、本出願と同時に出願された同時係属中の米国特許第13/764,944号、表題「AUTOMATIC KEY ROTATION」、本出願と同時に出願された同時係属中の米国特許第13/764,995号、表題「POLICY ENFORCEMENT WITH ASSOCIATED DATA」、本出願と同時に出願された同時係属中の米国特許第13/765,020号、表題「DATA SECURITY WITH A SECURITY MODULE」、本出願と同時に出願された同時係属中の米国特許第13/765,209号、表題「FEDERATED KEY MANAGEMENT」、本出願と同時に出願された同時係属中の米国特許第13/765,239号、表題「DELAYED DATA ACCESS」、本出願と同時に出願された同時係属中の米国特許第13/765,265号、表題「DATA SECURITY SERVICE」、及び本出願と同時に出願された同時係属中の米国特許第13/765,283号、表題「SECURE MANAGEMENT OF INFORMATION USING A SECURITY MODULE」の全開示を参照により全ての目的のために組み込む。
【０００２】
コンピューティングリソース及び関連データのセキュリティは、多くの文脈において重要性が高い。例えば、組織は多くの場合、ユーザにサービスの堅固な組を提供するためにコンピューティングデバイスのネットワークを利用する。ネットワークは、多くの場合複数の地理的境界線に広がり、多くの場合他のネットワークと接続する。例えばある組織は、コンピューティングリソースの内部ネットワーク及び他によって管理されるコンピューティングリソースの両方を使用してその動作を支え得る。例えば該組織のコンピュータは、別の組織のサービスを使用しながらデータにアクセスする及び／またはデータを提供するために、他の組織のコンピュータと通信し得る。多くの例において、組織は他の組織によって管理されるハードウェアを使用して遠隔ネットワークを構成して動作させ、それにより設備費を削減して他の利点を達成する。コンピューティングリソースのかかる構成を伴って、リソース及びそれらが保持するデータへのアクセスを保証することは、特にかかる構成の大きさ及び複雑性が増大するにしたがって困難になり得る。
【図面の簡単な説明】
【０００３】
本開示に従う様々な実施形態が、図面を参照して説明され得る。
【図１】様々な実施形態に従う本開示の様々な態様を表す例示的な図を示す。
【図２】本開示の様々な態様が実装され得る環境の例示的な実施例を示す。

【図３】少なくとも１つの実施形態に従う、本開示の様々な態様が実装され得る環境の例示的な実施例と、環境の様々な構成要素の間の情報の流れの実施例と、を示す。
【図４】少なくとも１つの実施形態に従う、暗号文を格納するための例示的なプロセスのステップの実施例を示す。
【図５】少なくとも１つの実施形態に従う、本開示の様々な態様が実装され得る環境の例示的な実施例と、環境の様々な構成要素の間の情報の流れの実施例と、を示す。
【図６】少なくとも１つの実施形態に従う、データを読み出すための要求に応答するための例示的なプロセスのステップの実施例を示す。
【図７】少なくとも１つの実施形態に従う、本開示の様々な態様が実装され得る環境の例示的な実施例と、環境の様々な構成要素の間の情報の流れの実施例と、を示す。
【図８】少なくとも１つの実施形態に従う、データを格納するための要求に応答するための例示的なプロセスのステップの実施例を示す。
【図９】少なくとも１つの実施形態に従う、本開示の様々な態様が実装され得る環境の例示的な実施例と、環境の様々な構成要素の間の情報の流れの実施例と、を示す。
【図１０】少なくとも１つの実施形態に従う、データを読み出すための要求に応答するための例示的なプロセスのステップの実施例を示す。
【図１１】本開示の様々な態様が実装され得る環境の例示的な実施例を示す。
【図１２】少なくとも１つの実施形態に従う、本開示の様々な態様が実装され得る環境の例示的な実施例と、環境の様々な構成要素の間の情報の流れの実施例と、を示す。
【図１３】少なくとも１つの実施形態に従う、データを読み出すための要求に応答するための例示的なプロセスのステップの実施例を示す。
【図１４】少なくとも１つの実施形態に従う、データを解読するための要求に応答するための例示的なプロセスのステップの実施例を示す。
【図１５】少なくとも１つの実施形態に従う、解読されたデータを得るための例示的なプロセスのステップの実施例を示す。
【図１６】少なくとも１つの実施形態に従う、暗号サービスの実施例の図表示を示す。
【図１７】少なくとも１つの実施形態に従う、ポリシーを構成するための例示的なプロセスのステップの実施例を示す。
【図１８】少なくとも１つの実施形態に従う、ポリシーを実施しながら暗号動作を実行するための、例示的なプロセスのステップの実施例を示す。
【図１９】様々な実施形態が実装され得る環境の例示的な実施例を示す。
【発明を実施するための形態】
【０００４】
以下の説明において、様々な実施形態が説明される。説明の目的で、実施形態の徹底的な理解を提供するために具体的な構成及び詳細が述べられる。しかしながら、当業者には、実施形態がその具体的な詳細を伴わずに実践され得るということもまた明らかになるであろう。さらに、公知の特徴は、説明される実施形態を不明瞭にしないために、省略または簡素化され得る。
【０００５】
本明細書に記載及び提案される技術は、分散コンピューティングリソースを含む環境における、強化されたデータセキュリティを可能にする。一実施例では、分散コンピューティング環境は、適切なコンピューティングリソースによって実装され得る１つ以上のデータサービスを含む。データサービスは、様々な動作がデータに関連して実行されることを可能にし得る。１つの例示的な実施例としては、分散コンピューティング環境は１つ以上のデータ格納サービスを含む。電子要求がデータ格納サービスに伝送され、データ格納動作を実行し得る。動作の例は、データ格納サービスを使用してデータを格納すること、及びデータ格納サービスを使用してデータ格納サービスによって格納されたデータを読み出すことである。データ格納サービスを含むデータサービスは、データを操作する動作もまた実行し得る。例えば、いくつかの実施形態では、データ格納サービスはデータを暗号化することができる。

【０００６】
本開示の様々な実施形態は、適切なコンピューティングリソースを使用して実装される暗号サービスを含む、分散コンピューティング環境を含む。暗号サービスは、平文の暗号化及び暗号文の解読等の、暗号動作を実行するための電子要求を受信してそれに応答する、分散システムによって実装され得る。いくつかの実施形態では暗号サービスは鍵を管理する。暗号動作を実行するための要求に応答して、暗号サービスは管理される鍵を使用する暗号動作を実行し得る。例えば、暗号サービスは、受信された要求に応答して、暗号動作を実行するための適切な鍵を選択して、暗号動作を実行して、暗号動作の１つ以上の結果を提供することができる。代替の構成では、暗号サービスはエンベロープ鍵（例えば具体的なデータアイテムを暗号化するために使用されるセッション鍵）を生成して、そのエンベロープ鍵をシステムに戻し、サービスの暗号動作を発動することができる。システムは、その後エンベロープ鍵を使用して暗号動作を実行することができる。
【０００７】
いくつかの実施形態では、暗号サービスはコンピューティングリソースサービスプロバイダの複数のテナントの鍵を管理する。コンピューティングリソースのテナントは、コンピューティングリソースプロバイダの顧客として動作するエンティティ（例えば組織または個人）であり得る。顧客は、コンピューティングリソースプロバイダによって物理的にホストされるリソースを、遠隔的にかつプログラムで構成して動作させ得る。顧客が暗号サービスに、暗号動作を実行するための要求を提出するとき（またはエンティティが暗号サービスに要求を提出するとき）、暗号サービスは、顧客のために、暗号サービスによって管理される鍵を選択して、暗号動作を実行する。暗号サービスによって管理される鍵は、他のユーザ及び／またはデータサービスは、他人が鍵へのアクセスを有さないように、安全に管理され得る。あるエンティティ（例えば、ユーザ、顧客、サービス）による別のエンティティの鍵へのアクセスの欠如は、そのエンティティが他人の鍵を得る許可された方法を有さないということ、及び／または、そのエンティティが、そのエンティティの方向で鍵を使用する他人の鍵を管理するシステムを行わせる許可された方法を有さないということ、を意味し得る。例えば、暗号サービスは、顧客、他の顧客の両方が、顧客の鍵（複数可）へのアクセスを有さず、かつ、暗号サービスに、顧客の鍵（複数可）を使用して暗号動作を実行させることができないように、鍵を管理し得る。別の実施例として、暗号サービスは、データ格納サービス等の他のサービスが、暗号サービスがいくつかまたは全ての鍵を使用して、暗号動作を実行させることができないように、鍵を管理し得る。鍵への許可なしのアクセスは、例えば許可なしのアクセスが困難または不可能になるように、適切なセキュリティ手段によって防止され得る。困難は、コンピュータ使用上非実用的である及び／またはアクセスが得られるために非許可（例えば、違法、不法、及び／または許可証明の危殆化等の別様で許可されないもの）が生じる必要性によるものであり得る。様々な実施形態に従うシステムは、鍵へのアクセスを得るための、コンピュータ非実用性の客観的尺度を保証するように構成され得る。かかる尺度は、例えば時間量に関して測定され、平均では、鍵への許可されたアクセスのために必要とされる、暗号化された情報をクラッキングするために、コンピュータ能力の定義されたユニット（例えば時間の単位当たりの特定の動作）を有するコンピュータを取り得る。
【０００８】
述べられたように、暗号サービスは、コンピューティングリソースプロバイダの顧客等の様々なエンティティから要求を受信し得る。暗号サービスは、コンピューティングリソースプロバイダの内部のエンティティからもまた要求を受信し得る。例えば、いくつかの実施形態では、コンピューティングリソースプロバイダによって実装されるデータサービスは、暗号サービスに暗号動作を実行させるために、暗号サービスに要求を伝送し得る。一実施例としては、顧客は、データ対象を格納するために、データ格納サービスに要求を伝送し得る。要求は、データ対象が格納されるときに暗号化されなければならないということを示し得る。データ格納サービスは、暗号動作を実行するために、暗号サービスに要求を通信し得る。暗号動作は、例えば、データ格納サービスによって使用される鍵を暗号

化してデータ対象を暗号化することであり得る。暗号動作は、データ対象自体の暗号化であり得る。暗号動作は、データ対象を暗号化するためにデータ格納サービスが使用することができる、エンベロープ鍵を生成することであり得る。

【０００９】

様々な実施形態に従うシステムは、様々なセキュリティ手段を実装して強化されたデータセキュリティを提供する。例えば、様々な実施形態では、暗号サービスが管理する鍵を利用できる様式は限定される。例えば、いくつかの実施形態では、暗号サービスは、適切な許可時に顧客に対応する鍵を使用するようにのみ構成される。顧客の鍵を使用するための要求が、顧客から（すなわち顧客のために動作しているコンピューティングデバイスから）由来するとされる場合、暗号サービスは、その要求が、顧客によって所有される適切な証明書を使用して、電子的に（デジタルで）署名されることを要求するように構成され得る。顧客の鍵を使用するための要求が、別のデータサービスから由来した場合、暗号サービスは、そのデータサービスが、データサービスへの署名された要求が顧客によって作られたものであるという証明を提供することを要求するように構成され得る。いくつかの実施形態では、例えば、データサービスは、認証された顧客要求の証明としての役割を果たすトークンを得て、提供するように構成される。他のセキュリティ手段もまた暗号サービスを含む電子環境の構成に組み込まれ得る。例えば、いくつかの実施形態では、暗号サービスは、文脈に応じて鍵の使用を限定するように構成される。１つの例示的な実施例として、暗号サービスは、顧客からまたは顧客のために作用しているデータサービスからの、要求の暗号化のための鍵を使用するように構成され得る。しかしながら、暗号サービスは、顧客からの（別のデータサービスからではなく）要求の解読のためにのみ鍵を使用するように構成され得る。このようにして、データサービスが危殆化される場合、データサービスは暗号サービスにデータを解読させることができなくなり得る。

【００１０】

様々なセキュリティ手段が、暗号サービス及び／またはその電子環境に組み込まれ得る。いくつかのセキュリティ手段は、ポリシーに従って管理され得、これはいくつかの実施形態では構成可能である。一実施例として、暗号サービスは、ユーザが鍵に関するポリシーを構成することができるようにする、アプリケーションプログラミングインターフェース（ＡＰＩ）を利用し得る。鍵に関するポリシーは、暗号サービスによって処理されるときに、鍵が特定の状況で使用され得るかどうかの決定因である情報であり得る。ポリシーは、例えば、鍵の使用を指揮する、鍵が使用され得る回数を限定する、暗号動作を実行するために鍵が使用され得るデータを限定する、及び他の限定を提供することができる、ユーザ及び／またはシステムの識別を限定し得る。ポリシーは、明示的な限定（例えば誰が鍵を使用することができないか）を提供し得、及び／または、明示的な許可（例えば誰が鍵を使用することができるか）を提供し得る。さらに、ポリシーは、鍵がいつ使用できる及びできないかの条件を概して提供するように、複雑に構造され得る。鍵を使用して暗号動作を実行するための要求が受信される場合、ポリシーに従って要求が遂行され得るかを判断するために、鍵に関する任意のポリシーがアクセス及び処理され得る。

【００１１】

図１は、本開示の様々な実施形態を実証する例示的な図１００である。一実施形態では、暗号サービスは、１つ以上の暗号アルゴリズムに従う１つ以上の計算の適用を含み得る暗号動作を実行する。図１に例示されるように、暗号サービスは、ユーザまたはサービスが暗号文から平文を生成することができるようにする。構成の実施例では、暗号サービスは、鍵を暗号化／解読するために使用され得、かつこれらの鍵は、データ格納サービス内に格納されるデータ等のデータを暗号化／解読するために使用され得る。例えば、暗号サービスは、鍵下で暗号化された暗号文から平文を生成するための要求を受信する。暗号サービスは、要求者が許可されたエンティティであることを判定し、マスター鍵を使用して鍵を解読し、解読された鍵をサービスに戻し、これは、解読された鍵を使用して暗号文から平文を生成することができる。別の構成では、暗号サービスは暗号文を受信して、受信された暗号文を、暗号サービスによりサービスとして提供される平文へと処理する。この

実施例では、暗号文は、暗号サービスを動作させるコンピューティングリソースプロバイダの顧客であり得る、及び／または、コンピューティングリソースプロバイダの別のサービスであり得る、許可されたエンティティから、暗号サービスへの電子要求の一部として、暗号サービスに提供され得る。図１に例示される暗号サービスは、１つ以上の暗号的に強いアルゴリズムを利用してデータを暗号化し得る。かかる暗号的に強いアルゴリズムは、例えば、高度暗号化標準（ＡＥＳ）、Ｂｌｏｗｆｉｓｈ、データ暗号化標準（ＤＥＳ）、トリプルＤＥＳ、Ｓｅｒｐｅｎｔ、またはＴｗｏｆｉｓｈを含み得、かつ、選択される具体的な実装に依存して、非対称性または対称性鍵システムのいずれかであり得る。概して、暗号サービスは、任意の暗号及び／もしくは解読アルゴリズム（暗号）、または暗号サービスによって管理されるデータを利用するアルゴリズムの組み合わせを利用し得る。

【００１２】

下記により詳細に記載されるように、暗号サービスは様々な方法で実装され得る。一実施形態では、暗号サービスは、下記の説明に従って構成されるコンピュータシステムによって実装される。コンピュータシステムは、それ自体が１つ以上のコンピュータシステムを備え得る。例えば、暗号サービスは、様々な実施形態に従い暗号動作を実行するように集合的に構成される、コンピュータシステムのネットワークとして実装され得る。または、換言すると、コンピュータシステムは分散システムであり得る。一実施形態では、暗号文は、暗号アルゴリズムを使用して暗号化された情報である。図１の実施例では、暗号文は暗号化形式の平文である。平文は任意の情報であり得、その名前は語を含まないテキストを含むが、平文及び暗号文は、任意の好適な形式でコードされた情報であり得、必ずしも文字情報を含まないが、文字情報を含んでよい。例えば、図１に例示されるように、計画文及び暗号文は、ビットの配列を含む。平文及び暗号文は、他の方法でならびに暗号化及び解読がコンピュータシステムによって実行され得る任意の様式でもまた表され得る。

【００１３】

図２は、図１に例示されるような暗号サービスが実装され得る、環境２００の例示的な実施例を示す。環境２００では、安全なデータ関連サービスを提供するために、様々な構成要素が一緒に動作する。この具体的な実施例では、環境２００は、暗号サービス、認証サービス、データサービスフロントエンド、及びデータサービスバックエンド格納システムを含む。一実施形態では、暗号サービスは、サービスがエンベロープ鍵を使用して暗号動作を実行することができるように、環境２００において、データサービスフロントエンドから平文を受信して引き換えに暗号文を提供すること、またはエンベロープ鍵をサービスに提供すること等によって、暗号動作を実行するように構成される。暗号サービスは、下記に記載のような、暗号動作の実行のための鍵の安全な格納、平文を暗号文に変換すること及び暗号文を平文に解読すること等の、追加の機能を実行し得る。暗号サービスは、例えばそこに格納される鍵に関連付けられるポリシーを実施することによって、ポリシー実施に関与する動作もまた実行し得る。暗号サービスによって実施され得るポリシーの実施例が下記に提供される。一実施形態におけるデータサービスフロントエンドは、様々なユーザからネットワークを介して伝送される要求を受信してそれらに応答するように構成されるシステムである。要求は、データサービスバックエンド格納システム内に格納されたまたは格納されるべきデータに関連する動作を実行するための要求であり得る。環境２００では、認証サービス、暗号サービス、データサービスフロントエンド、及びデータサービスバックエンド格納システムは、システムを利用して図２に例示されるユーザによって表される顧客にサービスを提供する、コンピューティングリソースプロバイダのシステムであり得る。図２に例示されるネットワークは、下記に記載されるものを含む、任意の好適なネットワークまたはネットワークの組み合わせであり得る。

【００１４】

一実施形態における認証サービスは、ユーザの認証に関与する動作を実行するように構成されるコンピュータシステムである。例えば、データサービスフロントエンドは、ユーザからの情報を認証サービスに提供して、引き換えにユーザ要求が真正であるかどうかを示す情報を受信し得る。ユーザ要求が真正であるかどうかの判断は、任意の好適な様式で

実行され得、認証が実行される様式は、様々な実施形態の間で変動し得る。例えば、いくつかの実施形態では、ユーザはデータサービスフロントエンドに伝送されるメッセージに電子署名する。電子署名は、認証するエンティティ（例えばユーザ）及び認証サービスの両方に使用可能である、秘密情報（例えばユーザに関連付けられる１対の鍵の秘密鍵）を使用して生成され得る。要求及び要求のための署名は、認証サービスに提供され得、これは、秘密情報を使用して、受信された署名との比較のために、参照署名を算定して、要求が真正であるかどうかを判断し得る。要求が真正である場合、認証サービスは、データサービスフロントエンドが、暗号サービス等の他のサービスに証明するために使用することができる、要求が真正であるという情報を提供し得、それによって、他のサービスがそれに応じて動作することを可能にする。例えば、認証サービスは、別のサービスが要求の真正を検証するために分析することができる、トークンを提供し得る。電子署名及び／またはトークンは、様々な方法で限定される有効性を有し得る。例えば、電子署名及び／またはトークンは、特定の時間量の間有効であり得る。一実施例では、電子署名及び／またはトークンは、検証のための電子署名及び／またはトークンと共に含まれる、タイムスタンプを入力として取る関数（例えばハッシュベースメッセージ認証コード）に少なくとも部分的に基づいて生成される。提出された電子署名及び／またはトークンを検証するエンティティは、受信されたタイムスタンプが十分に最新のものである（例えば現在時刻から所定の時間量内である）ことを点検して、受信されたタイムスタンプのために使用している参照署名／トークンを生成し得る。提出された電子署名／トークンを生成するために使用されたタイムスタンプが、十分に最新のものでない、かつ／または、提出された署名／トークンと参照署名／トークンが一致しない場合、認証は失敗し得る。このようにして、電子署名が危殆化される場合、それは短い時間量の間のみ有効となり得、それによって危険に曝すことによって引き起こされる潜在的な被害を限定する。真正を検証する他の方法もまた、本開示の範囲内であるとみなされるということに留意すべきである。

【００１５】

一実施形態におけるデータサービスバックエンド格納システムは、データサービスフロントエンドを通して受信される要求に従ってデータを格納するコンピュータシステムである。下記により詳細に記載されるように、データサービスバックエンド格納システムは、暗号化形式でデータを格納し得る。データサービスバックエンド格納システム内のデータは、非暗号化形式でもまた格納され得る。いくつかの実施形態では、データサービスフロントエンドによって実装されるＡＰＩは、要求が、データサービスバックエンド格納システム内に格納されるべきデータが、暗号化されるべきかどうかを特定することを可能にする。暗号化されてデータサービスバックエンド格納システム内に格納されるデータは、様々な実施形態に従い、様々な方法で暗号化され得る。例えば、様々な実施形態では、データは、暗号サービスにアクセス可能であるが、環境２００の他のシステムのいくつかまたは全てにはアクセス不能な鍵を使用して、暗号化される。データは、データサービスバックエンド格納システム内の格納のために、暗号サービスによってコードされ得、及び／または、いくつかの実施形態では、データは、暗号サービスによって解読された鍵を使用して、ユーザシステムまたはデータサービスフロントエンドのシステム等の、別のシステムによって暗号化され得る。それによって環境２００がデータを暗号化するために動作し得る様々な方法の実施例は、下記に提供される。

【００１６】

環境２００（及び本明細書に記載される他の環境）の多数の変形は本開示の範囲内であるとみなされる。例えば、環境２００は、暗号サービス及び／または認証サービスと通信し得る、追加のサービスを含み得る。例えば、環境２００は、異なる方法でデータを格納し得る、追加のデータ格納サービス（それぞれがフロントエンドシステム及びバックエンドシステムを備え得る）を含み得る。例えば、あるデータ格納サービスは、データ格納サービスが同期様式でデータ格納サービスを実行するデータへの、アクティブアクセスを提供し得る（例えばデータを読み出すための要求が読み出されたデータと共に同期の応答を受信し得る）。別のデータ格納サービスは、保存用データ格納サービスを提供し得る。か

かる保存用データ格納サービスは、非同期の要求処理を利用し得る。例えば、データを読み出すための要求は、読み出されたデータを含む同期応答を受信しないことがある。むしろ、保存用データ格納サービスは、保存用データ格納サービスが読み出されたデータを提供する準備ができると、読み出されたデータを得るために、第２の要求が提出されることを要求し得る。別の実施例として、環境２００は、暗号サービス（及び／または他のサービス）から情報を受信して、その情報を使用してアカウント記録を生成する計量サービスを含み得る。アカウント記録は、暗号サービス（及び／または他のサービス）の使用について顧客に課金するために使用され得る。さらに、暗号サービスからの情報は、料金がどのように課せられるべきかについての指示を提供し得る。例えば、いくつかの例では、顧客は暗号サービスの使用について、請求書が提供され得る。他の例では、暗号サービスの使用についての料金は、その動作の一部として暗号サービスを利用するデータサービス等の、他のサービスの使用料金に合わされ得る。使用は、動作当たり、時間当たり、及び／または他の方法等の、様々な方法で計量されて課金され得る。他のデータサービスもまた環境２００（または本明細書に記載される他の環境）内に含まれ得る。

【００１７】

さらに、図２は、データサービスフロントエンドと対話するユーザを描写する。ユーザは、図面には例示されていないユーザデバイス（例えばコンピュータ）を通してデータサービスフロントエンドと対話し得るということが理解されるべきである。さらに、図２（及び図面の他の箇所）に描写されるユーザは、非人間エンティティもまた表し得る。例えば、コンピュータシステム上で実行する自動化プロセスは、本明細書に記載されるデータサービスフロントエンドと対話し得る。例示的な一実施例として、図２のユーザによって表されるエンティティは、その動作の一部として、データサービスフロントエンドを使用して、データサービスバックエンド格納システムにデータを格納する及び／またはそこからデータを読み出す、サーバであり得る。さらに別の実施例として、図２のユーザによって表されるエンティティは、図２のサービスのうちの１つ以上を動作させるコンピューティングリソースプロバイダのサービスとして提供されるエンティティであり得る。例えば、図２のユーザは、コンピューティングリソースプロバイダによって提供される、プログラム実行サービスの仮想または他のコンピュータシステムを表し得る。下記に記載の他の環境の変形を含む他の変形もまた、本開示の範囲内であるとみなされる。

【００１８】

例えば、図３は、本開示の様々な実施形態が実装され得る、環境３００の例示的な実施例を示す。図２と同様に、図３の環境は、認証サービス、データサービスフロントエンドシステム（データサービスフロントエンド）、暗号サービス、及びデータサービスバックエンド格納システムを含む。認証サービス、データサービスフロントエンド、暗号サービス、及びデータサービスバックエンド格納システムは、図２に関連して上記に説明するように構成され得る。例えば、ユーザは、好適な通信ネットワークを介してデータサービスフロントエンドにアクセスし得るが、かかるネットワークは図面に例示されない。図３に例示される環境の実施例３００において、情報の流れを表す矢印が提供される。本実施例では、ユーザはＰＵＴ要求をデータサービスフロントエンドに伝送する。ＰＵＴ要求は、特定のデータをデータサービスバックエンド格納システム内に格納するための要求であり得る。ＰＵＴ要求に応答して、データサービスフロントエンドはＰＵＴ要求が真正であるかどうかを判断し得るが、これは、ユーザが、要求される動作が、システムによって実施される認証ポリシーに従って実行され得る様式で、その要求を提出したかである。

【００１９】

図３では、かかる認証決定がどのように行われ得るかの例示的な実施例が、例示される。この具体的な実施例では、データサービスフロントエンドは、認証要求を認証サービスに提出する。認証サービスは、認証要求を使用して、ユーザからのＰＵＴ要求が真正であるかどうかを判断し得る。要求が真正である場合、認証サービスは、認証証明をデータサービスフロントエンドに提供し得る。認証証明は、真正要求が受信されたことを独立して判断するために、暗号サービス等の別のサービスによって使用可能である、電子トークン

または他の情報であり得る。１つの例示的な実施例では、ＰＵＴ要求はＰＵＴ要求のための署名と共に伝送される。ＰＵＴ要求及びその署名は、認証サービスを通して提供され、これは真正である場合署名がどうあるべきかを独立的に算定する。認証サービスによって生成される署名がユーザによって提供される署名と一致する場合、認証サービスは、ＰＵＴ要求が真正であると判断し得、応答して認証証明を提供し得る。ＰＵＴ要求が真正であるかどうかを判断することは、ポリシーの実施に関連する１つ以上の動作もまた含み得る。例えば、署名が有効であるがポリシーが別様でＰＵＴ要求が完了されるべきでないと示す（例えば要求がポリシーによって許可されない時間に提出された）場合、認証サービスは、要求が真正でないということを示す情報を提供し得る。（しかしながら、かかるポリシーの実施は、環境３００の他の構成要素によって実行され得るということに留意すべきである。）認証サービスは、認証サービス及びユーザによって共有される鍵を使用すること等によって、署名を生成し得る。述べられたように、認証証明は、暗号サービス等の別のサービスが、それから要求が真正であることを独立して検証することができる、情報であり得る。例えば、図３に例示される暗号サービスの実施例を使用して、認証証明は、他のサービスにはアクセス不能である鍵等の、認証サービス及び暗号サービスの両方によって共有される鍵に、少なくとも部分的に基づいて生成され得る。

【００２０】

図３に例示されるように、データサービスフロントエンドは、認証サービスからの認証証明の受信の際に、平文及び認証証明を暗号サービスに提供する。平文及び認証証明は、暗号サービスへのＡＰＩ呼び出しまたは他の電子要求（例えば暗号ＡＰＩ呼び出し）に応じて提供され得る。暗号サービスは、認証証明を分析して、平文を暗号化するかどうかを判断し得る。

【００２１】

暗号サービスに追加の情報が提供され得るということに留意すべきである。例えば、平文を暗号化するために使用される鍵の識別子は、入力パラメータとして、データサービスフロントエンドからのＡＰＩ呼び出し（順に、ユーザから識別子を受信した可能性がある）に提供され得る。しかしながら、識別子は暗号サービスに伝送されないことがあるということに留意すべきである。例えば、様々な実施形態では、平文を暗号化するためにどの鍵を使用するかは、別様で判断可能であり得る。例えば、データサービスフロントエンドから暗号サービスに伝送される情報は、ユーザがそのためにＰＵＴ要求を提出した顧客の識別子等の、ユーザ及び／またはユーザに関連付けられる組織の識別子等の、ユーザに関連付けられる情報を含み得る。かかる情報は、暗号サービスによって使用されて、使用される初期設定の鍵を判断し得る。換言すると、鍵は、鍵を判断することに有用である情報によって、暗黙的に特定され得る。概して、使用される鍵の判断は、任意の好適な様式で実行され得る。さらに、いくつかの実施形態では、暗号サービスは、鍵を生成または選択して、後で使用される生成または選択された鍵の識別子を提供し得る。ＡＰＩパラメータの別の実施例は、そのために暗号動作が実行されている顧客アカウントのためのマスター鍵の識別子であり得る。

【００２２】

図３に例示されるように、認証証明が、平文を暗号化するために、暗号サービスに十分である場合、暗号サービスは１つ以上の暗号動作を実行し得る。一実施形態では、１つ以上の暗号動作は、平文を暗号化するために使用されるエンベロープ鍵を生成するための動作を含み得る。エンベロープ鍵は、無作為に生成された対称性鍵または一対の鍵のうちの秘密鍵であり得る。エンベロープ鍵が生成された後で、暗号サービスは、エンベロープ鍵を、ＡＰＩ呼び出しにおいて特定されるマスター鍵を用いて暗号化し得、暗号化された鍵が永続的に格納（例えば、暗号化された鍵を格納サービスもしくはいくつかの他の耐久性格納装置内に格納することによって）または廃棄されることを引き起こし得る。さらに、暗号サービスは、エンベロープ鍵の平文版も、暗号化されたエンベロープ鍵と同様に、データサービスフロントエンドに送信し得る。データサービスは、その後エンベロープ鍵の平文版を使用して平文（すなわち、暗号化要求に関連付けられるデータ）を暗号化し得、

エンベロープ鍵が、エンベロープ鍵を暗号化するために使用されたマスター鍵の識別子に関連して、永続的格納装置内に格納されることを引き起こし得る。さらに、データサービスは、エンベロープ鍵の平文版を廃棄し得る。したがって、一実施形態では、データサービスがエンベロープ鍵の平文版を廃棄した後、それはもう暗号文を解読することができなくなる。

【００２３】

代替の実施形態では、暗号動作は平文を暗号化することを含み得る。例えば、暗号サービスは、平文を暗号化して、データサービスフロントエンド格納システムに暗号文を提供する。データサービスフロントエンドは、その後、その動作に従う永続的な格納のために、データサービスバックエンド格納システムに暗号文を提供し得る。他の情報もまた、データサービスフロントエンドからデータサービスバックエンド格納システムに伝送され得る。例えば、平文を暗号化して暗号文を生成するために使用される鍵の識別子には、データサービスバックエンド格納システムによる格納のために、暗号文が提供され得る。ユーザ及び／またはユーザの組織を識別するメタデータ等の、他の情報もまた提供され得る。

【００２４】

本明細書に記載される全ての環境と同様に、多数の変形が本開示の範囲内であるとみなされる。例えば、環境３００の様々な構成要素の間の情報の流れは、示されるものから変動し得る。例えば、中間構成要素を通して、ある構成要素から別の構成要素に流れる情報（例えば認証サービスから暗号サービスへのデータ及び／または暗号サービスからデータサービスバックエンド格納システムへのデータ）は、その目的地に直接及び／または環境３００の他の中間構成要素（必ずしも図面に含まれない）を通して提供され得る。別の実施例として、ＰＵＴ要求（及び以下のＧＥＴ要求）は、例示の目的のために提供される。しかしながら、記載される動作を実行するための任意の好適な要求が使用され得る。

【００２５】

図４は、一実施形態に従ってデータ格納サービス内にデータを格納するために使用され得る、プロセス４００の例示的な実施例を示す。プロセス４００は、例えば図３に例示されるデータサービスフロントエンドによって実行され得る。プロセス４００（あるいは本明細書に記載される任意の他のプロセス、またはその変形及び／もしくは組み合わせ）のうちのいくらかまたは全ては、実行可能命令で構成される１つ以上のコンピュータシステム下で実行され得、かつ、１つ以上のプロセッサ上で集合的に、ハードウェアによって、またはそれらの組み合わせで実行する、コード（例えば実行可能命令、１つ以上のコンピュータプログラム、または１つ以上のアプリケーション）として実装され得る。コードは、例えば、１つ以上のプロセッサによって実行可能な複数の命令を含むコンピュータプログラムの形式で、コンピュータ可読格納媒体上に格納され得る。コンピュータ可読格納媒体は、非一過性であり得る。

【００２６】

図４に例示されるように、プロセス４００はＰＵＴ要求を受信すること４０２を含む。ＰＵＴ要求は、ネットワークを介して電子的に受信され得、ＰＵＴ要求の電子署名のような、認証のために要求される情報等の、要求に関連付けられる情報を含み得る。ＰＵＴ要求を受信したことに応答して、プロセス４００は、認証要求を提出４０４することを含み得る。例えば、プロセス４００において実行されるシステムは、図３に関連して上記のように、別個の認証サービスに認証要求を提出し得る（例えば適切に構成されたＡＰＩ呼び出しを介して）。同様に、それ自体の認証を実行するデータサービスフロントエンドは、認証要求を、データサービスフロントエンドによって実装される認証モジュールに提出し得る。概して、認証要求は、様々な実施形態に従う任意の好適な様式で提出され得る。

【００２７】

認証要求の提出の際に、認証要求が提出４０４されたエンティティによって、認証応答が受信４０６される。例えば、図３を参照すると、認証サービスは、他のサービスによる使用のための認証の証明を含む応答を、データサービスフロントエンドに提供し得る。認証が成功であったかどうかの表示等の他の情報もまた伝送され得る。要求が真正であるか

どうかが判断４０８され得る。要求の真正性は、認証サービス等のエンティティまたはかかる点検を集合的に実行するエンティティの組み合わせによって点検される、１つ以上の因子に従属し得る。例えば真正性は、要求が、必要とされる有効な証明（例えば、点検するエンティティによって共有される秘密鍵によって生成される電子署名）を提供すること、及び／またはポリシーが、要求が遂行されることを可能にすることを要求し得る。認証要求を提出４０４して認証応答を受信するシステムの視点からは、真正性は、受信される認証応答に従属し得る。結果的に、一実施形態では、要求が真正であるかどうかの判断４０８は、受信される認証応答に少なくとも部分的に基づいて実行され得る。例えば、認証が真正でなかった場合、認証応答はそのように示し、それに応じて判断４０８され得る。同様に、応答は、例えば要求が真正であった場合に含まれ得る情報を含まないことによって、認証要求が真正であることを暗黙的に示し得る。ＰＵＴ要求が真正でないと判断４０８された場合、ＰＵＴ要求は拒否４１０され得る。ＰＵＴ要求を拒否することは、任意の好適な様式で実行され得、かつ、プロセス４００が実行されている様々な実施形態に依存し得る。例えば、拒否４１０することで、ＰＵＴ要求は、ＰＵＴ要求を提出したユーザにメッセージを伝送することを含み得る。メッセージは、要求が拒否されたことを示し得る。要求を拒否することは、ＰＵＴ要求が真正でないまたは許可されていないことをもたらした、任意の問題を解決する方法を判断するために使用され得る、電子署名が正確でないまたは他の理由等の、なぜ要求が拒否されたかについての情報を提供することもまた含み得る。

【００２８】

ＰＵＴ要求が真正かつ許可されると判断４０８される場合、一実施形態では、プロセス４００は、平文が暗号化されることをもたらす１つ以上の暗号動作を実行４１２することを含む。例えば、暗号サービスに、１つ以上の暗号動作を実行するために使用される鍵を提供するための要求（例えば適切に構成されたＡＰＩ呼び出し）が提出され得る。暗号サービスが暗号動作（例えば、平文を暗号化して暗号文を提供する、または平文を暗号化するために使用され得るエンベロープ鍵を生成すること）を実行するかどうかを独立して判断することができるように、暗号サービスに提供される要求には、ＰＵＴ要求が真正であることの証明が提供され得る。しかしながら、様々な実施形態では、認証証明が暗号サービスに提供されないことがあり、例えば、暗号サービスはそれが受信する要求に従って動作し得る。例えば、暗号サービスがデータサービスフロントエンドから要求を受信する場合、暗号サービスは、データサービスフロントエンドが既に要求の認証を独立して検証したという事実に依存し得る。かかる実施形態及び他の実施形態では、データサービスフロントエンドは、暗号サービスを用いて自体を認証して、セキュリティの追加の層を提供し得る。暗号サービスは、鍵を生成するまたは別様で得て、得られた鍵を暗号化するかまたは別様で暗号化された鍵を得て（例えばメモリから）、要求に応答して、得られた鍵及び暗号化された鍵を提供し得る。得られた鍵は、暗号サービスへの要求において識別される鍵を使用して、暗号化され得る。得られた鍵は、平文を暗号化するために使用され得、平文を暗号化した後で、得られた鍵は廃棄（例えばメモリから取消不可に除去）され得る。代替の実施形態では、プロセス４００を実行するシステムは、１つ以上の暗号動作を実行するために使用される鍵を、生成するまたは別様で得て、暗号化するために得られた鍵を暗号サービスに提供し得る。

【００２９】

いくつかの実施形態では、１つ以上の暗号動作を実行することは、暗号文が生成されることをもたらし得る。１つ以上の暗号動作の結果として生成された暗号文は、後の起こり得る読み出しのために、格納４１４され得る。上記のように、暗号文の格納は、後の暗号文の解読を可能にし得る追加の情報の格納を含み得る。例えば、その識別子を有する鍵が後で暗号文を解読して平文を得るために使用され得るように、暗号文は、平文を暗号文に暗号化するために使用された鍵の識別子と共に格納され得る。暗号文の格納は、任意の好適な様式でもまた実行され得る。例えば、暗号文の格納は、上記のように、データサービスバックエンド格納システムによって実行され得る。

【００３０】
したがって、図５は、環境５００及び平文がどのように得られ得るかを例示する情報の流れの、例示的な実施例を示す。本実施例の環境５００は、認証サービス、暗号サービス、データサービスフロントエンド、及びデータサービスバックエンド格納システムを含む。認証サービス、暗号サービス、データサービスフロントエンド、及びデータサービスバックエンド格納システムは、上記のようなシステムであり得る。図５に例示されるように、データサービスフロントエンドは、ユーザからＧＥＴ要求を受信し、応答して平文を提供するように構成される。これを行うために、データサービスフロントエンドは、適切な場合に、認証証明をデータサービスフロントエンドに提供するように、それ自体が構成され得る、認証サービスに、認証要求を提出するようにもまた構成され得る。データサービスフロントエンドは、データを解読することに関連する１つ以上の暗号動作を実行させるために、暗号サービスに要求を送信するようにもまた構成され得る。エンベロープ鍵が使用される一実施形態では、データサービスは、暗号化されたエンベロープ鍵（または暗号化されたエンベロープ鍵の識別子）の認証証明を含むまたは特定する要求（例えばＡＰＩ呼び出し）を、暗号サービスに提出し、かつ、エンベロープ鍵を暗号化するために使用されたマスター鍵の識別子を暗号サービスに提出することができる。暗号サービスは、認証証明が、動作を可能にするのに十分であるかどうかを判断することができ、かつ、認証証明が十分である場合エンベロープ鍵を解読することができる。解読されたエンベロープ鍵は、暗号化された平文を解読するために鍵を使用し得るデータサービスに、送信して戻され得る。データサービスはその後解読された平文鍵を廃棄し得る。

【００３１】
代替の実施形態では、データサービスフロントエンドは、暗号サービスに、受信された認証証明を、暗号サービスが解読する暗号文とともに、提供するように構成され得る。結果的に、暗号サービスは、認証証明が、暗号文の解読を可能にするのに十分であるかどうかを判断して、認証証明が十分である場合、適切な鍵（データサービスフロントエンドによって、暗号サービスに識別され得る）を使用して暗号文を解読して、データサービスフロントエンドに解読された暗号文（平文）を提供するように構成され得る。暗号サービスに暗号文を提供するために、データサービスフロントエンドは、データサービスバックエンド格納システムから暗号文を得る（例えば、適切に構成されたＡＰＩ呼び出しを介して）ように構成され得る。

【００３２】
図６は、様々な実施形態に従う、平文を得るために使用され得る、プロセス６００の例示的な実施例を示す。プロセス６００は、例えば、図５に関連して上記に例示される、データサービスフロントエンドシステム（データサービスフロントエンド）によって実行され得るが、プロセス６００及びその変形は任意の好適なシステムによって実行されてよい。一実施形態では、プロセス６００は、ユーザからＧＥＴ要求（または他の適切な要求）を受信６０２することを含む。ＧＥＴ要求を受信することは、他の種類の要求に関連して上記のように実行され得る。ＧＥＴ要求の受信６０２の際に、認証要求が、認証サービスに、または上記のような任意の様式で、提出６０４され得る。それに応じて、認証応答が受信され得る。受信された認証応答に少なくとも部分的に基づいて、ＧＥＴ要求が真正であるかどうかが判断６０８され得る。ＧＥＴ要求が真正でないと判断６０８される場合、プロセス６００は、上記のように、様々な実施形態に従う様々な様式で実行され得る要求を拒否６１０することを含み得る。

【００３３】
ＧＥＴ要求が真正であると判断６０８される場合、プロセス６００は格納装置から暗号文を読み出すことを含み得る。格納装置から暗号文を回復６１２することは、任意の好適な様式で実行され得る。例えば、図５に関連して上記の環境５００を参照すると、データサービスフロントエンドは、暗号文のための要求をデータサービスバックエンド格納システムに提出し得、応答として暗号文を受信し得る。概して、暗号文は、任意の好適な様式で格納装置から得られ得る。暗号文の受信の際に、プロセス６００は、暗号文を解読する

ことに関連する１つ以上の動作を実行６１４することを含み得る。例えば、一実施形態では、データ格納サービスは、暗号文を解読することに関連する１つ以上の暗号動作を実行６１４するために、暗号サービスに要求を送信し得る。構成の一実施例では、データサービスは、暗号サービスに、暗号化されたエンベロープ鍵（または暗号化されたエンベロープ鍵の識別子）認証証明を含むＡＰＩ呼び出しを送信し得、かつ、エンベロープ鍵を暗号化するために使用されるマスター鍵の識別子を暗号サービスに送信し得る。暗号サービスは、認証証明が、動作を可能にするのに十分であるかどうかを判断することができ、かつ、認証証明が十分である場合エンベロープ鍵を解読することができる。解読されたエンベロープ鍵は、暗号化された平文を解読するために鍵を使用し得るデータサービスに、送信して戻され得る。

【００３４】

別の構成では、暗号文は、図５に関連して上記の暗号サービスのような、暗号サービスに提供され得る。暗号文を解読するかどうかを判断するために暗号サービスによって使用され得る認証の証明等の、他の情報もまた、暗号サービスに提供され得る。さらに、いくつかの実施形態では、暗号文を解読するために暗号サービスによって使用される鍵の識別子が、暗号サービスに提供され得る。しかしながら、他の実施形態では、鍵は暗号サービスに暗黙的に示され得る。例えば、暗号サービスは、暗号サービスに示される顧客に関連付けられる初期設定の鍵を使用し得る。概して、暗号サービスが、暗号文を解読するためにどの鍵を使用するかを判断することができる、任意の様式が使用され得る。

【００３５】

図６に例示されるように、暗号文が解読された後で、プロセス６００はＧＥＴ要求に応答を提供６１６することを含み得る。ＧＥＴ要求に応答を提供することは、様々な実施形態に従う様々な方法で実行され得る。例えば、ＧＥＴ要求に応答を提供することは、平文を提供することを含み得る。他の実施形態では、平文は、その後ＧＥＴ要求に応答して提供される、他の暗号化された情報を解読するために使用される鍵であり得る。概して、本開示の特定の実施形態における平文の役割に依存して、ＧＥＴ要求に応答を提供することは、様々な方法で実行され得る。

【００３６】

述べられたように、本開示の様々な実施形態は、データがデータ格納サービスによって様々な方法で格納されることを可能にする。図７は、かかる実施形態に従う、情報の流れを示す矢印を伴う環境７００の例示的な実施例を示す。図７に例示されるように、環境７００は、上記のような、認証サービス、暗号サービス、データサービスフロントエンド、及びデータサービスバックエンド格納システムを含む。この特定の実施例では、データサービスフロントエンドは、様々なユーザからＰＵＴ要求を受信するように構成されるコンピュータシステムである。ＰＵＴ要求は、データサービスバックエンド格納システムによって格納されるべきデータ対象を含むかまたは特定し得る。ＰＵＴ要求は、データ対象を暗号化するために使用される鍵の鍵識別子もまた特定し得る。データサービスフロントエンドは、鍵及び鍵識別子を受信して、それに応答して鍵識別子によって識別される鍵によって暗号化される鍵を提供するように動作可能である暗号サービスに認証証明を提供するために、上記のように、認証サービスと対話するようにもまた構成され得る。データサービスフロントエンドは、その後データサービスバックエンド格納システム内で格納を引き起こし得る。格納され得るデータは、鍵によって暗号化されたデータ対象を含み得る。格納され得るデータは、鍵識別子によって識別される鍵によって暗号化される鍵もまた含み得る。本明細書の他の箇所で記載されるように、暗号化されたデータ対象及び暗号化された鍵は、異なるサービス内に格納され得る。

【００３７】

図７に例示されるように、データサービスフロントエンドは、暗号化された情報を、格納のためにデータサービスバックエンド格納システムに提供するように構成される。この実施例では、データサービスフロントエンドは、鍵下で暗号化されたデータ対象と、鍵ＩＤを有する別の鍵下で暗号化された鍵と、を提供するように構成される。例示の目的のた

めに、暗号化を示すために中括弧表記が使用されるということに留意すべきである。特に、中括弧の中の情報は、添字で特定される鍵下で暗号化される情報である。例えば、｛データ対象｝鍵は、「データ対象」というデータが、「鍵」という鍵下で暗号化されるということを示す。この中括弧表記を使用して、鍵識別子も添字で出現し得るということに留意すべきである。添字に鍵識別子が出現する場合、中括弧の中の情報は、その鍵識別子によって識別される鍵下で暗号化される。例えば、｛データ対象｝鍵ＩＤは、「データ対象」というデータ対象が、「鍵ＩＤ」という鍵識別子によって識別される鍵下で暗号化されるということを示す。同様に、｛鍵｝鍵ＩＤは、「鍵」という鍵が、「鍵ＩＤ」という鍵識別子によって識別される鍵下で暗号化されるということを示す。換言すると、本開示は、添字において鍵及び鍵識別子の両方を利用し、添字の意味は文脈から明白であるはずである。暗号文は、関連する解読鍵のＩＤを判断するために使用可能な、追加のメタデータを含み得る。

【００３８】

図８は、図７に関連して上記されるデータサービスバックエンド格納システム等の、データ格納システム内にデータ対象を格納するために実行され得るプロセス８００の例示的な実施例を示す。プロセス８００は、例えば図７に関連して上記されるデータサービスフロントエンドシステム等の、任意の好適なシステムによって実行され得る。一実施形態では、プロセス８００は、データ対象のためのＰＵＴ要求を受信８０２することを含む。データ対象のためのＰＵＴ要求を受信することは、例えば上記のような、任意の好適な様式で実行され得る。データ対象は要求に関連して受信され得、または別のサービスから受信され得るということに留意すべきである。例えば、要求は、識別子を使用して別のサービスから得られ得る、データ対象の識別子を含み得る。上記の他のプロセスと同様に、一実施形態におけるプロセス８００は、認証要求を提出８０４すること及び認証応答を受信８０６することを含む。受信８０６された認証応答は、ＰＵＴ要求が真正要求であるかどうかを判断８０８するために使用され得る。ＰＵＴ要求が真正でないと判断８０８される場合、プロセス８００は、上記のように要求を拒否８１０することを含み得る。ＰＵＴ要求が真正であると判断８０８される場合、プロセス８００は、エンベロープ鍵を暗号化するために使用されるマスター鍵の鍵ＩＤ等の、鍵識別子（鍵ＩＤ）を得る８１２ことを含み得る。鍵ＩＤを得る８１２ことは、任意の好適な様式で実行され得、鍵ＩＤが得られる様式は様々な実施形態に従って変動し得る。例えば、図７に例示されるように、ＰＵＴ要求は鍵ＩＤを特定し得る。別の実施例として、ユーザのＩＤまたは別様でユーザに関付けられるＩＤは、識別子または初期設定の鍵を得るために使用され得る。別の例として、暗号文は関連する鍵ＩＤの表示を提供し得る。さらに別の実施例として、どの鍵識別子を得るかを判断するために、１つ以上のポリシー判断が使用され得る。

【００３９】

一実施形態では、プロセス８００は、エンベロープ鍵等の鍵を生成８１４することもまた含む。鍵を生成することは、例えば、暗号サービスまたは暗号サービスから暗号動作を要求するサービス（例えば、データ格納サービス）によって、任意の好適な様式で実行され得る。例えば、鍵は、鍵導出関数への適切な入力を使用し、鍵導出関数を使用して生成され得る。鍵導出機能の実施例には、ＩＥＥＥ規格１３６３　２０００において定義されるＫＤＦ１、ＡＮＳＩ　Ｘ９．４２において定義される鍵導出機能、及びＲＦＣ５８６９において特定されるＨＭＡＣ－Ｂａｓｅｄ　Ｅｘｔｒａｃｔ－ａｎｄ－Ｅｘｐａｎｄ　Ｋｅｙ　Ｄｅｒｉｖａｔｉｏｎ　Ｆｕｎｃｔｉｏｎ（ＨＫＤＦ）等のＨＭＡＣベースの鍵導出機能が挙げられる。別の例として、鍵は、米国国立標準技術研究所特別刊行物（ＮＩＳＴ　ＳＰ）８００－９０Ａによって特定されるもの等の、無作為もしくは偽性無作為数生成器、ハードウェアエントロピーソース、または決定的無作為ビット生成手段によって生成され得る。図８が鍵を生成８１４することを含むプロセス８００を示す一方で、鍵は格納装置からの回復等によって他の方法で得られ得るということに留意すべきである。換言すると、鍵は予め生成されていることがある。

【００４０】

図８に例示されるプロセス８００を続けると、一実施形態では、プロセス８００はデータ対象を暗号化するために生成された鍵を使用８１６することを含む。例えば、暗号サービスが鍵を生成する実施形態では、暗号サービスは、鍵、鍵ＩＤ、及び鍵の暗号化されたコピーを、データサービスに提供し得る。例えば、図７を参照すると、データサービスフロントエンドは、エンベロープ鍵及びエンベロープ鍵を暗号化するために使用されるマスター鍵の鍵ＩＤを、認証証明等の任意の他の関連する情報と共に、暗号サービスから受信し得る。暗号鍵の平文コピーはその後データ対象を暗号化するために使用され得る。暗号鍵の平文コピーは廃棄され得、暗号化されたデータ対象ならびに暗号化された鍵は、その後格納８１８され得る。例えば、図７を参照すると、データサービスフロントエンドは、暗号化されたデータ対象及び暗号化された鍵を、格納のためにデータサービスバックエンド格納システムに伝送し得る。サービスが鍵を生成する構成では、サービスは鍵及び鍵ＩＤを暗号サービスに提供し得る。例えば、データサービスフロントエンドは、エンベロープ鍵及びエンベロープ鍵を暗号化するために使用されるマスター鍵の鍵ＩＤを、認証承認等の、任意の他の関連する情報と共に暗号サービスに送信し得る。暗号鍵の平文コピーはその後データ対象を暗号化するために使用され得る。サービスは、暗号鍵の平文コピー及び暗号化されたデータ対象を廃棄し得、ならびに、暗号化された鍵はその後格納され得る。例えば、図７を参照すると、データサービスフロントエンドは、暗号化されたデータ対象及び暗号化された鍵を、格納のためにデータサービスバックエンド格納システムに伝送し得る。

【００４１】

暗号化されたデータ対象及び暗号化されたエンベロープ鍵は、鍵の平文版を伴わずに格納され得る、つまり、平文鍵は、データサービスバックエンド格納システム及び１つ以上の他のシステムに対してアクセス不能であり得る。その下でデータ対象が暗号化される鍵（例えばマスター鍵）は、任意の好適な様式でアクセス不能にされ得る。いくつかの実施形態では、これは、暗号サービスにのみアクセス可能であるメモリ内にそれを格納することによって達成される。いくつかの他の実施形態では、これは、マスター鍵をハードウェアまたは他のセキュリティモジュール内に、または別様でハードウェアもしくは他のセキュリティモジュールの保護下に格納することによって、達成され得る。いくつかの実施形態では、平文エンベロープ鍵を格納するメモリ位置（例えばデータサービスのメモリ）は、上書きすることが可能であり得るか、または、鍵を格納するメモリ位置は、データサービスフロントエンドへの鍵をアクセス不能にするために、意図的に上書きされ得る。別の実施例として、平文エンベロープ鍵は、最終的に鍵を格納しなくなる揮発性メモリ内に維持され得る。このようにして、エンベロープ鍵は、それが、鍵ＩＤによって識別された、または、コンピュータ的に非実用的であり得るが、鍵ＩＤによって識別される鍵を用いずに鍵をクラッキングする等によって別様で、非許可様式で得られた、鍵を使用して解読される場合にのみ、アクセス可能である。換言すると、鍵ＩＤによって識別される鍵は、その下でデータ対象が暗号化される鍵への、許可されたアクセスを要求される。したがって、図７のデータサービスバックエンド格納システムが危殆化される場合、かかる危殆化は、暗号化されていないデータ対象へのアクセスを提供し得ず、これは、データ対象を解読することが、鍵ＩＤによって識別される鍵を使用した解読を通して、または、コンピュータ的に実現可能ではない他の方法を通してのみ得ることができる、鍵へのアクセスを必要とし得るためである。

【００４２】

述べられたように、本開示の様々な実施形態は、ユーザがデータ対象を格納すること及び安全な様式でそれらを読み出すことを可能にする。したがって、図９は格納装置からデータ対象を得るために使用され得る環境９００の例示的な実施例を示す。図９に例示されるように、環境９００は、認証サービス、暗号サービス、データサービスフロントエンドシステム、及びデータサービスバックエンド格納システムを含む。認証サービス、暗号サービス、データサービスフロントエンド、及びデータサービスバックエンド格納システムは、上記のようなコンピュータシステムであり得る。図９に例示されるように、データサ

ービスフロントエンドシステムは、データ対象要求を受信し、それに応答してデータ対象を提供するように構成される。応答してデータ対象を提供するために、本実施形態におけるデータ格納フロントエンドシステムは、図９に例示されるように、認証サービス、暗号サービス、及びデータサービスバックエンド格納システムと、対話するように構成される。例えば、様々な実施形態では、データサービスフロントエンドシステムは、認証要求を認証サービスに提出し、要求に応答して認証証明を受信するように構成される。別の実施例として、データサービスフロントエンドは、鍵ＩＤによって識別される鍵によって暗号化された鍵及び認証証明を、鍵を提供するかどうかを認証証明に少なくとも部分的に基づいて判断するように動作可能である暗号サービスに提供して、鍵を提供するように判断された場合、鍵をデータサービスフロントエンドに提供するように構成される。データサービスフロントエンドは、鍵ＩＤ等の他の情報を暗号サービスに提供するようにもまた構成され得る。しかし、いくつかの実施形態では、鍵ＩＤは、例えば暗号サービスに提供される他の情報との関連を通して、暗号サービスに暗黙的に示され得る。いくつかの実施形態では、ユーザは、要求をデータサービスフロントエンドに提出することに関連して、鍵ＩＤをデータサービスフロントエンドに提供するということにもまた留意すべきである。さらに、図９に例示されるように、一実施形態では、データサービスフロントエンドは、データサービスバックエンド格納システムからデータ対象を要求して、それに応答して、鍵によって暗号化されたデータ対象及び鍵ＩＤによって識別された鍵によって暗号化された鍵を受信するように、構成される。いくつかの実施形態では、暗号サービスは、特定される鍵ＩＤに関連付けられる鍵を使用して生成されなかった暗号文の解読を実行することを、拒否するように動作可能であり得る。

【００４３】

一実施形態では、データサービスフロントエンドは、暗号サービスから受信される鍵を使用してデータ対象を解読し、解読されたデータ対象をユーザに提供するように構成される。したがって、図１０は、様々な実施形態に従う、解読された対象を提供するために使用され得るプロセス１０００の例示的な実施例を示す。プロセス１０００は、図９に関連して記載されるデータサービスフロントエンドシステム等の、任意の好適なシステムによって実行され得る。一実施形態では、プロセス１０００は、データ対象のためのＧＥＴ要求を受信１００２することを含む。データ対象のためのＧＥＴ要求を受信することは、他の種類の要求に関連して上で述べられたような、任意の好適な様式で実行され得る。例えば、データ対象のためのＧＥＴ要求は、要求及び／または他の情報を認証するために使用される情報を含み得る。したがって、一実施形態では、プロセス１０００は、本明細書に記載される他のプロセスと同様に、認証要求を認証システムに提出１００４すること、及び認証応答を受信１００６することを含む。認証要求を提出すること及び認証応答を受信することは、上記のような任意の好適な様式で実行され得る。認証応答は、ＧＥＴ要求が真正であるかどうかを判断１００８するために使用され得る。ＧＥＴ要求が真正でないと判断１００８される場合、一実施形態では、プロセス１０００は要求を拒否１０１０することを含む。しかしながら、ＧＥＴ要求が真正であると判断１００８される場合、一実施形態では、プロセス１０００は、暗号化されたデータ対象及び暗号化された鍵を格納装置から回復１０１２することを含む。例えば、データサービスフロントエンドシステムは、暗号化されたデータ対象及び暗号化された鍵を、図９に関連して上記に例示される、データサービスバックエンド格納システムから得ることができる。

【００４４】

一実施形態では、プロセス１０００は、暗号化されたエンベロープ鍵を暗号サービスに提供１０１４することを含む。暗号化されたエンベロープ鍵を暗号サービスに提供１０１４することは、任意の好適な様式で実行され得、かつ、暗号サービスが暗号化された鍵を解読するかどうかを判断することができるようにする認証証明等の、他の情報と共に提供され得る。さらに、暗号化されたエンベロープ鍵を暗号サービスに提供１０１４することは、暗号サービスが、暗号サービスによって管理される複数の鍵の中から、識別子によって識別される鍵を選択することができるようにするために、暗号化されたエンベロープ鍵

の許可された解読のために要求される鍵の識別子を提供することを含み得る。しかしながら、上で述べられたように、鍵は暗黙的に識別され得る。したがって、暗号サービスは、適切な鍵を選択して暗号化された鍵を解読し得る。したがって、一実施形態では、プロセス１０００は、解読されたエンベロープ鍵を暗号サービスから受信１０１６することを含む。例えば、暗号サービスが、認証証明が有効である、及び／または、暗号化されたものの解読が任意の適用可能なポリシーに従って許容可能であると判断した場合、暗号サービスは、解読された鍵を、データ対象を解読しようとしているシステムに提供し得る。その後、解読されたエンベロープ鍵を使用して、データ対象が解読１０１８され得る。その後、解読されたデータ対象は、ユーザまたはＧＥＴ要求を提出した他のシステム等の要求者に提供１０２０され得る。

【００４５】

多くの例では、ユーザ（すなわち、一般的には暗号サービスを利用するデバイス）が暗号サービスと直接対話することが望ましい。したがって、図１１は、暗号サービスへの直接的なユーザアクセスを可能にする、環境１１００の例示的な実施例を示す。環境１１００では、認証サービス、データサービスフロントエンド、及びデータサービスバックエンド格納システムが含まれる。認証サービス、データサービスフロントエンド、及びデータサービスバックエンド格納システムは、上記の通りであり得る。例えば、データサービスフロントエンドは、好適なネットワークを介して、図１１に例示されるように、ユーザからの要求を受信してそれに応答するように構成され得る。ネットワークを介してユーザからの要求に応答することの一部として、データサービスフロントエンドは、ユーザ要求が真正であるかどうかを判断する及び／または要求に関するポリシーを実施するために、認証サービスと対話するようにもまた構成され得る。データサービスフロントエンドは、ユーザ要求を遂行することの一部として、データサービスバックエンド格納システムと対話するようにもまた構成され得る。ユーザ要求は、例えば、データをバックエンド格納システム内に格納するためのＰＵＴ要求、及びデータサービスバックエンド格納システムからデータを読み出すためのＧＥＴ要求を含み得る。上記のように、例えば、データサービスバックエンド格納システム内に格納されたデータを削除するための要求、データサービスバックエンド格納システム内に格納されたデータを更新するための要求等の、他の要求もまた様々な実施形態に従って使用され得る。

【００４６】

図１１の具体的な実施例では、環境１１００において、暗号サービスは暗号サービスフロントエンド及びデータサービスバックエンドを含む。データサービスフロントエンドと同様に、暗号サービスフロントエンドは、ネットワークを介してユーザからの要求を受信してそれに応答するように構成される。暗号サービスフロントエンドは、ユーザ要求が真正であるかどうかを判断するために、認証サービスと対話するようにもまた構成される。ユーザ要求が真正であるかどうかを判断することは、上記のような簡単な様式で実行され得る。暗号サービスフロントエンド及びデータサービスフロントエンドが、同じ認証サービスと対話するが、暗号サービスフロントエンド及びデータサービスフロントエンドは、異なる認証サービスと対話し得るということに留意すべきである。さらに、暗号サービスフロントエンドは、ユーザ要求に応答するときに、ポリシーを実施するように構成され得る。

【００４７】

一実施形態では、暗号サービスフロントエンドは、暗号サービスバックエンドと対話するように構成される。暗号サービスバックエンドは、暗号サービスフロントエンドから受信された命令に従って、暗号動作を実行するように構成される。暗号動作は、暗号化、解読、及びハッシュ計算等を含む。環境１１００は、例えば、暗号化されたデータがデータサービスバックエンド格納システム内に格納され得るように、暗号サービスによって暗号化された平文を有するために、ユーザによって使用され得る。環境１１００のかかる使用の実施例は下記に提供される。さらに、暗号サービスの実施例の詳細の例もまた下記に提供される。

【００４８】
データは、上記のような任意の好適な様式で、データサービスバックエンド格納システム内に格納され得る。例えば、上記の暗号化されたデータをバックエンド格納システム内に格納するための技術は、環境１１００において使用され得る。例えば、例示されていないが、データサービスフロントエンドは、暗号サービスフロントエンドと通信して、暗号サービスバックエンドがデータを暗号化することを引き起こし得、そのデータは後にデータサービスバックエンド格納システム内に格納され得る。暗号化されたデータは、データ対象及び／またはデータ対象を暗号化するために使用された暗号化された鍵であり得る。環境１１００では、データは、別様でもまたデータサービスバックエンド格納システムに配置され得る。例えば、ユーザは暗号サービスによって暗号化される平文を提供し得、かつ、それに応答して暗号文を受信し得る。ユーザはその後、データサービスフロントエンドに要求を提出して、暗号文がデータサービスバックエンド格納システム内に格納されることを要求し得る。データサービスフロントエンドは、本実施例では、任意の様式で暗号文を格納し得る。例えば、データサービスフロントエンド及びバックエンド格納システムは、データが暗号されるかどうかに無関係であるように構成され得る。
【００４９】
さらに、本明細書に例示される全ての環境と同様に、システム間の行動を協調させるために、追加のフロントエンドシステムが、ユーザと、データサービスフロントエンドと、暗号サービスフロントエンドと、おそらく他のフロントエンドシステムとの間に、論理的に位置付けられ得る。例えば、いくつかの実施形態では、ユーザの視点からの動作がより簡単になるように、ユーザは、それ自体が暗号サービスフロントエンド及びデータサービスフロントエンドと対話する、フロントエンドシステムと対話し得る。例えば、ユーザはデータ対象が暗号化されて格納されること、ならびに、フロントエンドシステムが暗号サービスフロントエンド及びデータサービスフロントエンドとの適切な対話によって要求に応答することを要求し得る。しかしながら、ユーザの視点からは、かかることは単一の要求によって実行され得る。他の変形もまた本開示の範囲内である。
【００５０】
図１２は、本開示の様々な実施形態を実装するために使用され得る、環境１２００の例示的な実施例を示す。図１２では、環境１２００は、ユーザがデータサービスバックエンド格納システム内に暗号文を格納することができるようにするように構成される。したがって、図１２に例示されるように、環境１２００は、データサービスフロントエンド、データサービスバックエンド格納システム、認証サービス、暗号サービスフロントエンド、及び暗号サービスバックエンドを含む。データサービスバックエンド格納システム、データサービスフロントエンド、認証サービス、暗号サービスフロントエンド、及び暗号サービスバックエンドは、図１１に関連して上記のようなシステムであり得る。例えば、図１２に例示されるように、データサービスフロントエンドは、ユーザ要求を受信してそれに応答するように構成され、かつユーザ要求に関するポリシーを実施するようにもまた構成され得る。データサービスフロントエンドは、要求に応答することの一部として、認証要求を認証サービスに提出して、それに応答して応答して認証証明を受信するように構成され得る。認証が成功すると、データサービスフロントエンドは、データサービスバックエンド格納システムと対話して、暗号化されたデータ対象及びおそらく暗号化されていないデータ対象をデータサービスバックエンド格納システムから得るようにさらに構成され得、これは後でユーザに提供され得る。
【００５１】
図１２に例示されるように、暗号サービスフロントエンドは、認証要求を認証サービスに提出して、それに応答して認証証明を受信するようにもまた構成される。認証証明は、暗号サービスバックエンドからサービスを得るために使用され得る。例えば、暗号サービスフロントエンドは、暗号文を認証証明と共に暗号サービスバックエンドに提供するように構成され得、暗号サービスバックエンドは、暗号文を解読して引き換えに暗号文を提供するように構成され得る。図１２に例示されるように、暗号文は暗号化された鍵であり得

、暗号サービスバックエンドは暗号化された鍵を解読して、解読された鍵、つまり平文鍵を暗号サービスフロントエンドに提供し得、これは平文鍵をユーザに提供するようにさらに構成される。ユーザは、その後鍵を使用して、データサービスフロントエンドから受信される暗号化されたデータ対象を解読し得、またはユーザのドメイン内（例えば、ユーザが動作または制御するデータセンターまたはコンピュータシステム内）に格納される暗号化されたデータ対象を解読し得る。本実施例では、ユーザは暗号化された鍵をデータサービスフロントエンドから得た可能性がある。例えば、ユーザは、データ対象及び／またはデータ対象を暗号化するために使用された鍵のために、要求をデータサービスフロントエンドに提出した可能性がある。図１１では単一の要求として例示される一方で、データ対象及び鍵の両方のために別個の要求がなされ得る。図１１に例示されるように、データサービスフロントエンドは、暗号化されたデータ対象及び暗号化された鍵をデータサービスバックエンド格納システムから得て、暗号化されたデータ対象及び暗号化された鍵をユーザに提供し得る。

【００５２】

本明細書に例示される全ての環境と同様に、変形は本開示の範囲内であるとみなされるということに留意すべきである。例えば、図１２は、鍵下で暗号化されたデータ対象、及び鍵識別子によって識別される別の鍵によって暗号化された鍵が、ユーザに提供されているところを示す。さらなるレベルの暗号化もまた使用され得る。例えば、データ対象は、ユーザにのみアクセス可能である（かつ／または環境１２００の他の構成要素によってアクセス可能でない）鍵下で暗号化され得る。データ対象を暗号化するために使用される鍵もまた、ユーザにのみアクセス可能である鍵下で暗号化され得る。本実施例では、ユーザの鍵へのアクセスが許可された解読のためになお要求されるため、環境１２００（ユーザ不在）の構成要素への許可のないアクセスは、データ対象の暗号化されていないコンテンツへのアクセスを提供しない。

【００５３】

別の実施例として、図１２に例示される環境１２００では、データサービスフロントエンド及びデータサービスバックエンド格納システムは、データサービスバックエンド格納システムによって格納される平文データへのアクセスを有さず、これは、データサービスフロントエンド及びデータサービスバックエンド格納システムは、暗号化されたデータを解読するために必要とされる鍵へのアクセスを有さないためである。しかしながら、いくつかの実施形態では、データサービスフロントエンド及び／またはデータサービスバックエンド格納システムへのアクセスが認められ得る。例えば、一実施形態では、鍵への一時的なアクセスがデータサービスフロントエンドに提供され、データサービスフロントエンドが、暗号化されたデータを得ること、暗号化されたデータを解読すること、特定の目的（例えばインデックス作成）のために解読されたデータを使用すること、及びその後解読されたデータへのアクセスを削除するか別様で失くすことが、できるようにし得る。かかる行動は、データサービスフロントエンド及び／または暗号サービスによって実施されるポリシーによって統治され得、ユーザからの許可を要求し得る。

【００５４】

図１３は、プロセス１３００の例示的な実施例を示し、これは暗号化されたデータ対象及び暗号化された鍵を、上記のようなデータサービスバックエンド格納システム等から得るために使用され得る。例えば、プロセス１３００は、図１２に関連して上記されるデータサービスフロントエンドシステムによって実行され得る。一実施形態では、プロセス１３００は、暗号化されたデータ対象のためのＧＥＴ要求を受信１３０２することを含む。ＧＥＴ要求を受信することは、データサービスフロントエンドシステムへのＡＰＩ呼び出しを介して要求を受信すること等によって、任意の好適な様式で実行され得る。ＧＥＴ要求の受信の結果として、プロセス１３００は、認証要求を提出１３０４すること及び認証応答を受信１３０６することを含み得る。認証要求を提出１３０４すること及び認証応答を受信１３０６することは、上記のような任意の好適な様式で実行され得る。認証応答は、ＧＥＴ要求が真正であるかどうかを判断１３０８するために使用され得る。ＧＥＴ要求

が真正でないと判断１３０８される場合、プロセス１３００はＧＥＴ要求を拒否１３１０することを含み得る。ＧＥＴ要求を拒否１３１０することは、上記のような任意の好適な様式で実行され得る。しかしながら、ＧＥＴ要求が真正であると判断１３０８される場合、プロセス１３００は暗号化されたデータ対象に、解読されると暗号化されたデータ対象を解読するために使用可能である暗号化された鍵を、提供１３１２することを含み得る。本明細書に記載される全てのプロセスと同様に、多数の変形が本開示の範囲内であるとみなされるということに留意すべきである。例えば、プロセス１３００は、ＧＥＴ要求が真正である場合、暗号化されたデータ対象を提供するが暗号化された鍵は提供しないことによって、ＧＥＴ要求に応答するように構成され得る。要求者、つまりＧＥＴ要求を提出したユーザまたはシステムは、他の方法で、暗号化された鍵を得ることができる。例えば、いくつかの実施形態では、ユーザはユーザの制御下で、暗号化された鍵を自体でデータ格納システム内に格納し得る。別の例として、ある格納サービスが暗号化されたデータ対象を格納し得、別のサービスが暗号化された鍵を格納し得、ユーザは暗号化されたデータ対象及び暗号化された鍵をそれぞれのサービスから得ることができる。別の例として、別のサービスまたは第三者が、暗号化された鍵を格納するために使用され得、ユーザは要求の際に暗号化された鍵を得ることができる。概して、暗号化された鍵が提供され得る任意の方法が使用され得る。

【００５５】

図１３に例示されるように、プロセス１３００は、データ対象及びデータ対象を解読するために使用可能である暗号化された鍵が提供されたエンティティをもたらし得る。様々な実施形態では、データ対象を解読するために、暗号化された鍵は解読されなければならない。したがって図１４は、解読された鍵を、暗号化されたデータ対象の解読のために解読された鍵を使用するために、かかる解読された鍵を必要とするエンティティに提供するために使用され得る、プロセス１４００の例示的な実施例を示す。プロセス１４００は、図１２に関連して上記される暗号サービスフロントエンドシステム等によって、任意の好適なシステムによって実行され得る。一実施形態では、プロセス１４００は、特定された鍵ＩＤを有する別の鍵を使用して鍵を解読するために、解読を受信１４０２することを含む。プロセス１４００は鍵の解読に関連して記載されるが、プロセス１４００は概してデータの解読のために適合し得るということに留意すべきである。解読要求は、上記のような任意の好適な様式で（例えば適切に構成されたＡＰＩ呼び出しを介して）受信１４０２され得る。さらに、解読要求は、プロセス１４００が実行されている文脈に適切である、任意のエンティティによって受信され得る。例えば、解読要求は、ユーザまたは上記のデータサービスフロントエンド等の別のシステムから由来し得る。解読要求は、解読されるデータ（例えば鍵）またはそれへの参照もまた含み得る。鍵ＩＤは、任意の好適な様式でもまた特定され得る。例えば、いくつかの実施形態では、解読要求は、鍵ＩＤまたは鍵ＩＤへの参照、つまり鍵ＩＤを判断するために使用することができる情報を含む。上記のように、鍵ＩＤは暗黙的にもまた特定され得る。例えば、鍵ＩＤは、解読要求を提出した要求者のＩＤ等の使用可能なデータとの関連を通して得られ得る。例えば、鍵ＩＤに対応する鍵は、要求者、またはそのために要求が提出されたエンティティのための、初期設定の鍵であり得る。

【００５６】

一実施形態では、プロセス１４００は、認証要求を提出１４０４すること及び認証応答を受信１４０６することを含む。認証要求を提出１４０４すること及び認証応答を受信１４０６することは、上記のような任意の好適な様式で実行され得る。さらに、上記のように、受信された認証応答は、ＧＥＴ要求が真正であるかどうかを判断１４０８するために使用され得る。ＧＥＴ要求が真正でないと判断１４０８される場合、プロセス１４００はＧＥＴ要求を拒否１４１０することを含み得る。ＧＥＴ要求を拒否１４１０することは、上記のように、任意の好適な様式で実行され得る。しかしながら、ＧＥＴ要求が真正であると判断１４０８される場合、プロセス１４００は、特定される鍵ＩＤについての及び／または要求者についての、ポリシー情報にアクセスすることを含み得る。ポリシー情報は

、鍵ＩＤ及び／または要求者の１つ以上のポリシーを含み得る。

【００５７】

一実施形態では、アクセスされたポリシー情報は、任意の適用可能なポリシーが特定の鍵ＩＤを有する鍵の解読を可能にするかどうかを判断１４１４するために使用される。ポリシーが鍵ＩＤによって特定される鍵の解読を可能にしないと判断１４１４される場合、プロセス１４００は、上記のようにＧＥＴ要求を拒否１４１０することを含み得る。しかしながら、ポリシーが特定される鍵ＩＤを有する鍵の解読を可能にすると判断１４１４される場合、プロセス１４００は、鍵ＩＤによって識別される鍵を使用して鍵を解読１４１６することを含み得る。鍵ＩＤを有する鍵を使用して鍵が解読されると、解読された鍵はその後、ネットワークを介する伝送等によって、解読要求を提出した要求者（またはいくつかの実施形態では別の許可された行先）に提供１４１８され得る。

【００５８】

上記の環境１２００において例示されるように、ユーザは、暗号化されたデータ対象及びデータ対象を解読するための鍵を、様々な方法で得ることができる。図１５は、様々な実施形態に従い平文を得るために使用され得る、プロセス１５００の例示的な実施例を示す。プロセス１５００は、図１２に関連して記載されるように、ユーザによって動作及び／またはホストされているシステムによって等、任意の好適なシステムによって実行され得る。他の好適なシステムは、ユーザのために動作するシステムを含み、提供されるリアルタイムユーザに必ずしも従わず、おそらく予めプログラムされたプロセスに従う。

【００５９】

一実施形態では、プロセス１５００は、データ格納サービスから暗号文を受信１５０２することを含む。データ格納サービスから暗号文を要求１５０２することは、上記のような任意の好適な様式で実行され得る。例えば、プロセス１５００を実行するシステムは、図１２に関連して上記に例示される環境１２００の適切に構成されたＡＰＩ呼び出しを使用して、及び／または図１３に関連して上で述べられたプロセス１３００によって、暗号文を要求１５０２し得る。

【００６０】

プロセス１５００は、暗号文及び暗号化された鍵を受信することもまた含み得る。暗号文及び暗号化された鍵を受信することは、任意の好適な様式で実行され得る。例えば、暗号文及び暗号化された鍵は、データ格納サービスからの暗号文の要求に応答して、受信され得る。しかしながら、概して、暗号文及び暗号化された鍵は、他の好適な方法で受信１５０４され得る。例えば、データ格納サービスから暗号文を受信するための要求は非同期要求であり得、暗号文は後で提出される別の要求に従って受信１５０４され得る。さらに、暗号文及び暗号化された鍵は、単一の応答で提供され得るか、または異なる応答（同じまたは異なるシステムからであり得る）等によって別個に得られ得る。別の例として、プロセス１５００を実行するシステムは、暗号化された鍵をローカルにまたは別様で格納し得、暗号化された鍵はローカルメモリから受信され得る。

【００６１】

一実施形態では、プロセス１５００は、特定された鍵ＩＤを有する鍵を使用した、暗号化された鍵の解読を要求することを含む。鍵ＩＤは、上記のような任意の好適な様式で特定され得る。さらに、プロセス１５００を実行しているシステムは、任意の好適な様式で鍵ＩＤを特定することができ得るということに留意すべきである。例えば、暗号化された鍵及び／またはそこに提供された情報は鍵ＩＤを特定し得る。別の例として、プロセス１５００を実行しているシステムは、鍵ＩＤを判断することを可能にする情報へのローカルまたは遠隔アクセスを有し得る。例えば、ローカルまたは遠隔データベースは、データ対象識別子を、データ対象を暗号化するために使用された鍵の鍵識別子に関連付け得る。概して、システムが鍵ＩＤを特定することができるようにし得る任意の様式が使用され得る。さらに、いくつかの実施形態では、暗号サービスに提供される情報が鍵ＩＤを判断するのに十分である場合等では、鍵ＩＤは特定される必要がない。暗号化された鍵の解読の要求１５０６は、図１２に関連して上記される環境に関連して、及び／または図１４に関連

して上記されるプロセス１４００の実行等によって、任意の好適な様式で実行され得る。
【００６２】
プロセス１５００は、一実施形態では、解読された鍵を受信１５０８することを含む。解読された鍵を受信１５０８することは、任意の好適な様式で実行され得る。例えば、解読された鍵は、暗号化された鍵の解読の要求に応答して受信され得る。別の例として、暗号化された鍵の解読の要求は非同期要求であり得、解読された鍵を受信するために別の要求が提出された可能性がある。概して、解読された鍵は、任意の好適な様式で受信され得る。さらに、あるデバイスから別のデバイスに流れる全ての情報と同様に、情報の通過は安全なチャネルを使用して実行され得る。例えば、解読された鍵は、解読された鍵を受信するエンティティによる解読のために、再度暗号化され得る。概して、安全な通信の任意の様式が、あるエンティティから別のエンティティに情報を通過させるために使用され得る。
【００６３】
解読された鍵が受信１５０８されると、プロセス１５００は解読された鍵を使用１５１０して暗号文を解読１５１０し、よって平文を得ることを含み得る。本明細書に記載される全てのプロセスと同様に、変形が本開示の範囲内であるとみなされるということに留意すべきである。例えば、プロセス１５００は、暗号文の要求及び暗号化された鍵の解読の要求が、連続的に実行されているところを示す。しかしながら、様々なプロセスに関連して本明細書に記載される多くの動作と同様に、様々な実施形態では動作は連続的に実行される必要がない。例えば、プロセス１５００を実行するシステムが、暗号文を要求する前に、暗号化された鍵へのアクセスを有する、または別様でそうすることができる場合、システムは暗号文を要求し得、かつ、平行してまたは例示されるものとは異なる順序で、暗号化された鍵の解読を要求し得る。他の変形もまた本開示の範囲内であるとみなされる。
【００６４】
上記のように、本開示の様々な実施形態は暗号サービスを提供することを対象とする。暗号サービスは、上記のような暗号サービスシステムによって提供され得る。したがって図１６は、様々な実施形態に従う暗号サービス１６００の例示的な実施例を示す。図１６に例示されかつ上で述べられたように、暗号サービス１６００は、フロントエンドシステム及びバックエンドシステムから論理的に構成される。フロントエンドシステム及びバックエンドシステムの両方は、本明細書に記載される動作を実行するように構成される１つ以上のコンピュータシステムによって実装され得る。例えば、図１６に例示されるように、暗号サービス１６００のフロントエンドシステムは、要求ＡＰＩ及びポリシー構成ＡＰＩを実装する。一実施形態では、要求ＡＰＩは、暗号化及び他の動作が暗号サービスによって実行されることを要求するために構成されるＡＰＩである。よって、かかる暗号動作が暗号サービスによって実行されるように、要求ＡＰＩを介してフロントエンドシステムに要求がなされ得る。
【００６５】
要求ＡＰＩは、以下の、高レベルの使用可能な要求の実施例で構成され得る。
鍵作成（鍵ＩＤ）
暗号化（鍵ＩＤ、データ、［ＡＡＤ］）
解読（鍵ＩＤ、暗号文、［ＡＡＤ］）
細断（鍵ＩＤ）
鍵再作成（暗号文、旧鍵ＩＤ、新鍵ＩＤ）。
【００６６】
鍵作成（鍵ＩＤ）要求は、一実施形態では、暗号サービスに、要求において識別される鍵ＩＤによって識別される鍵を作成させる。要求の受信の際に、暗号サービスは鍵を生成してその鍵を鍵ＩＤに関連付け得る。鍵ＩＤのものは、固有の識別子であり得るが必ずしもそうではないということを理解すべきである。例えば、鍵ＩＤは鍵のファミリーを識別し得る。例えば、いくつかの実施形態では、鍵回転が実行される。鍵回転は、使用される暗号の実用的なクラッキングを可能にするのに十分な解読されたデータの収集を防止する

ために、鍵を他の鍵と交換することを含み得る。暗号サービスとは異なるエンティティの方向で実行される場合、鍵作成（鍵ＩＤ）要求の使用は、暗号サービスに、鍵ＩＤによって識別される旧鍵と交換するための新鍵を作成させ得る。旧鍵は、鍵ＩＤによって識別されるままであり得るが、例えば、（旧鍵を使用して既に暗号化されたデータの）解読に使用されるのみで将来の暗号化には使用されないことがある。別の実施例として、いくつかの実施形態では、暗号サービスのユーザは彼ら自身の鍵識別子を提供し、かつ、２人の異なる顧客が同じ識別子を提供し得る可能性がある。かかる例では、識別子は鍵を一意に識別し得ず、またはさらには鍵のファミリーも一意に識別し得ない。これに対処するために、様々な方法が整えられ得る。例えば、識別または暗号サービスのユーザに関連付けられる他の情報が、適切な鍵または鍵のファミリーを識別するために使用され得る。さらに他の実施形態では、暗号サービスは、無作為に、連続的に、または任意の他の方法を使用して、鍵ＩＤを割り当て得る。

【００６７】

鍵ＩＤが鍵を一意に識別しない場合、適切な機能を可能にするために様々なシステムが整えられ得るということに留意すべきである。例えば、様々な実施形態では、ある鍵ＩＤによって識別される鍵のファミリーは有限である。鍵ＩＤによって識別される鍵を使用した解読動作が要求される場合、追加のデータ（例えば、暗号化が実行されたときのタイムスタンプ）が使用すべき適切な鍵の判断を可能にし得る。いくつかの実施形態では、暗号文は鍵版を示す情報を含み得る。いくつかの実施形態では、データの異なる解読を提供するために全ての可能な鍵が使用される。有限数の鍵があるため、適切な解読は提供されるものから選択され得る。いくつかの実施形態では、鍵を用いた解読は、認証された暗号化を使用すること等によって、暗号サービスがその暗号文が少なくとも部分的にその鍵に基づいて生成されなかったことを検出することができるようにする様式で、実行される。他の変形もまた本開示の範囲内であるとみなされる。

【００６８】

暗号化（鍵ＩＤ、データ、［ＡＡＤ］）要求は、暗号サービスに、鍵ＩＤによって識別される鍵を使用して特定されるデータを暗号化させるために使用され得る。追加の認証されたデータ（ＡＡＤ）が、様々な目的のために使用され得、かつ、必ずしも暗号化されていないが、例えば、電子署名、メッセージ認証コード、または概してＡＡＤと共に含まれる鍵付ハッシュ値によって、認証されたデータであり得る。いくつかの実施形態では、暗号文はＡＡＤの少なくとも一部を含んで生成される。いくつかの他の実施形態では、ＡＡＤは解読の間に別個に提供される。いくつかの他の実施形態では、解読が、メタデータがパスする際にのみ成功するように、ＡＡＤは、要求及び他のメタデータに少なくとも部分的に基づいて、解読時間に生成される。いくつかの実施形態では、ポリシーは、暗号動作が特定のＡＡＤに関して実行され得るかどうかを制約し得る。暗号化（鍵ＩＤ、データ、［ＡＡＤ］）要求の処理は、論理及び／または暗号サービスによって実施されるポリシーをプログラムすることによって、ＡＡＤが特定の値を含むこと及びＡＡＤが真正である（例えば元来の伝送から修正されていない）ことの両方を要求し得る。同様に、解読（鍵ＩＤ、暗号文、［ＡＡＤ］）要求は、暗号サービスに、鍵ＩＤによって識別される鍵を使用して特定される暗号文を解読させるために、使用され得る。解読（鍵ＩＤ、暗号文、［ＡＡＤ］）要求におけるＡＡＤは、上記のように使用され得る。例えば、解読（鍵ＩＤ、暗号文、［ＡＡＤ］）の処理は、論理及び／または暗号サービスによって実施されるポリシーを実施することによって、ＡＡＤが特定の値を含むこと及びＡＡＤが真正である（例えば元来の伝送から修正されていない）ことの両方を要求し得る。

【００６９】

一実施形態では、細断（鍵ＩＤ）は、暗号サービスに、特定される鍵ＩＤによって識別される鍵または鍵のファミリーを電子的に細断させるために、使用され得る。電子的細断は鍵をもうアクセス可能でなくすることを含み得る。例えば、細断（鍵ＩＤ）要求の使用は、暗号システムに、１つ以上のハードウェアデバイスに、特定される鍵ＩＤによって識別される１つ以上の鍵上で安全消去動作を実行するように命令させ得る。概して、鍵ＩＤ

によって識別される鍵（複数可）は、他のデータ（例えば一連の０または１または無作為な文字列）を用いて鍵をコードするデータを上書きすること等によって、任意の好適な様式で電子的に細断され得る。鍵（複数可）がある鍵下で暗号化されて格納される場合、鍵を暗号化するために使用された鍵は、電子的に細断され得、よってその鍵（複数可）へのアクセスの損失を引き起こす。いくつかの実施形態では、細断動作は、細断された鍵ＩＤが将来の何らかの確固たる時点で失敗することを示す、解読動作を行わせ得る。鍵（複数可）への任意の可能なアクセスを安全にかつ永続的に破壊する他の様式が使用され得る。

【００７０】

一実施形態では、鍵再作成（暗号文、旧鍵ＩＤ、新鍵ＩＤ）要求は、暗号サービスに、異なる鍵下で、暗号文を暗号化させるために使用され得る。暗号サービスが鍵再作成（暗号文、旧鍵ＩＤ、新鍵ＩＤ）要求を受信するとき、それは、特定される暗号文を解読するために旧鍵ＩＤによって識別される鍵を使用して、その後、解読された暗号文を暗号化するために新鍵ＩＤによって識別される鍵を使用し得る。新鍵ＩＤによって識別される鍵がまだ存在しない場合、上記される作成（鍵ＩＤ）要求との関連で上で述べられたように、暗号サービスは、使用する鍵を生成して生成された鍵を特定される新鍵ＩＤに関連付け得る。いくつかの実施形態では、鍵再作成動作は、データを暗号サービスの孤立したインスタンス間で移送可能にするように動作可能であり得る。いくつかの実施形態では、ポリシーは、鍵再作成動作が暗号文上で実行されることを許可し得るが、同じ要求者が暗号文を直接解読することを許可しないことがある。いくつかの実施形態では、鍵再作成は、第１のアカウント内の第１の鍵ＩＤによって識別される鍵から、第２のアカウント内の鍵ＩＤによって識別される鍵へ、暗号文を鍵再作成することを支持し得る。

【００７１】

同様に、フロントエンドシステムは、ポリシー構成ＡＰＩを実装し得、これは、一実施形態では、ユーザが、暗号動作の実行についての及び他のポリシー関連動作についてのポリシーを構成するための要求を、提出することができるようにする。様々な実施形態では、ポリシーは、鍵、鍵のグループ、アカウント、ユーザ、または他の論理的なエンティティに関連付けられ得る。ポリシー構成ＡＰＩを介して構成され得るポリシーの実施例は、下に提供される。一実施形態では、暗号サービスポリシー構成ＡＰＩは次の要求を含む：

鍵設定ポリシー（鍵ＩＤ、ポリシー）
保留（鍵ＩＤ、公開鍵）
復元（鍵ＩＤ、秘密鍵）

【００７２】

一実施形態では、鍵設定ポリシー（鍵ＩＤ、ポリシー）要求は、暗号サービスに、鍵ＩＤによって識別される鍵（または鍵のファミリー）に関するポリシーを格納させるために使用され得る。ポリシーは、要求された暗号動作が特定の文脈において実行され得るかどうかの決定因である情報であり得る。ポリシーは、ｅＸｔｅｎｓｉｎｂｌｅ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（ＸＡＣＭＬ）、Ｅｎｔｅｒｐｒｉｓｅ Ｐｒｉｖａｃｙ Ａｕｔｈｏｒｉｚａｔｉｏｎ Ｌａｎｇｕａｇｅ（ＥＰＡＬ）、Ａｍａｚｏｎ Ｗｅｂ Ｓｅｒｖｉｃｅｓ Ａｃｃｅｓｓ Ｐｏｌｉｃｙ Ｌａｎｇｕａｇｅ、Ｍｉｃｒｏｓｏｆｔ ＳｅｃＰｏｌ、または実行される暗号動作についても満たさなければならない１つ以上の条件をコードする任意の好適な方法等の、宣言アクセス制御ポリシー言語内にコードされ得る。ポリシーは、何の動作が実行され得るか、動作がいつ実行され得るか、どのエンティティが、動作が実行されるための許可要求をすることができるか、特定の要求が許可されるためにどの情報が要求されるか等を、定義し得る。さらに、ポリシーは、アクセス制御リスト、ユーザに関連付けられる特権、及び／または動作ビットマスクを、上記に与えられた例に追加してまたはその代わりに使用して、定義及び／または実施され得る。ポリシーの実施例を下に示す。

【００７３】

いくつかの実施形態では、暗号サービスは、例えば保留（鍵ＩＤ、公開鍵）ＡＰＩ呼び出しを使用して、保留動作を支持し得る。保留動作は、暗号サービスの顧客が、暗号サー

ビスの動作者の、鍵の使用または鍵へのアクセスを拒否することを可能にする。これは、秘密の合法命令または暗号サービスの動作者が鍵を使用して何らかの動作を実行することを強要され得る他の状況を懸念する顧客に有用であり得る。これは、特定のデータをロックしてオンラインでアクセス不能にすることを望む顧客にも有用であり得る。いくつかの実施形態では、例えば、鍵ＩＤを特定しかつ秘密鍵も含む、復元（鍵ＩＤ、秘密鍵）ＡＰＩ呼び出しを使用して、公開鍵に関連付けられる秘密鍵が提供されない限り、プロバイダが保留された鍵にアクセスすることができないように、保留動作は、顧客から公開鍵を受信すること、及び、受信された公開鍵を用いて所与の鍵ＩＤによって特定される鍵を暗号化すること、及び鍵ＩＤによって特定される鍵を細断することを含み得る。いくつかの他の実施形態では、保留動作は、即時保留動作の目的のために作成されるものを含むがこれに限定されない、暗号サービスによって管理される別の鍵を使用して、特定される鍵ＩＤに関連付けられる鍵を暗号化することを含み得る。この動作によって生成される暗号文は、顧客に提供され得、暗号サービス内に保持され得ない。鍵ＩＤによって識別される元来の鍵はその後細断され得る。暗号サービスは、提供された暗号文を受信して保留された鍵を再インポートするように動作可能であり得る。いくつかの実施形態では、暗号文は、暗号サービスが解読版を顧客に返すことを防止し得る様式で、生成され得る。

【００７４】

図１６に例示されるように、いくつかの実施形態では、暗号サービス１６００は、それ自体が様々な構成要素を備えるバックエンドシステムを含む。例えば、本実施例におけるバックエンドシステムは、要求ＡＰＩまたはポリシー構成ＡＰＩのいずれかを通して受信される要求に従って動作を実行するように構成される暗号サービス１６００のサブシステムであり得る、要求処理システムを含む。例えば、要求処理構成要素は、要求ＡＰＩを介して受信される要求を受信し得、ポリシー構成ＡＰＩは、かかる要求が真正であるかどうか及びよって遂行可能であるかどうかを判断して、要求を遂行し得る。要求を遂行することは、例えば、暗号動作を実行すること及び／または実行したことを含む。要求処理ユニットは、要求処理ユニットが、要求が真正であるかどうかを判断することを可能にする、認証インターフェースと対話するように構成され得る。認証インターフェースは、上記のような認証システムと対話するように構成され得る。例えば、要求が要求処理ユニットによって受信されるとき、要求処理ユニットは、認証インターフェースを利用して、適用可能であれば、暗号動作の実行を行わせるために使用され得る認証証明を提供し得る、認証サービスと対話し得る。

【００７５】

暗号サービス１６００のバックエンドシステムは、本例示的実施例では、複数のセキュリティモジュール（暗号モジュール）及びポリシー実施モジュールを含む。様々な実施形態では、セキュリティモジュールは、本明細書に記載される能力を有するように構成される任意の好適なコンピュータデバイスであり得るが、セキュリティモジュールのうちの１つ以上は、ハードウェアセキュリティモジュールであり得る。一実施形態におけるそれぞれのセキュリティモジュールは、鍵ＩＤに関連付けられる複数の鍵を格納する。それぞれのセキュリティモジュールは、暗号サービス１６００の他の構成要素及び／または他のシステムの他の構成要素によってアクセス可能とならないように、鍵を安全に格納するように構成され得る。一実施形態では、セキュリティモジュールのうちのいくつかまたは全てが、少なくとも１つのセキュリティ標準に準拠する。例えば、いくつかの実施形態では、セキュリティモジュールは、ＦＩＰＳ刊行物１４０－２において概説される１つ以上のセキュリティレベル等の、ＦＩＰＳ刊行物１４０－１及び／または１４０－２において概説される連邦情報処理標準（ＦＩＰＳ）に準拠するとそれぞれ立証される。さらに、いくつかの実施形態では、それぞれのセキュリティモジュールは、暗号モジュール立証プログラム（ＣＭＶＰ）下で認定される。セキュリティモジュールは、ハードウェアセキュリティモジュール（ＨＳＭ）またはＨＳＭのいくらかまたは全ての能力を有する別のセキュリティモジュールとして実装され得る。いくつかの実施形態では、立証されたモジュールは動作をブートストラップするために使用される。いくつかの実施形態では、顧客は、立証さ

れたモジュール内に格納されそれによってのみ動作するいくつかの鍵、及びソフトウェアによって動作する他の鍵を構成し得る。いくつかの実施形態では、これらの様々な選択肢に関連付けられる実行または経費は異なり得る。

【００７６】

セキュリティモジュールは、要求処理ユニットによって提供される命令に従って暗号動作を実行するように構成され得る。例えば、要求処理ユニットは、暗号文及び鍵ＩＤを、その鍵ＩＤに関連付けられる鍵を使用して暗号文を解読し、応答して平文を提供するための、セキュリティモジュールへの命令を有する、適切なセキュリティモジュールに提供し得る。一実施形態では、暗号サービス１６００のバックエンドシステムは、鍵空間を形成する複数の鍵を安全に格納する。セキュリティモジュールのそれぞれは、鍵空間内の全ての鍵を格納し得るが、しかしながら、変形は、本開示の範囲内であるとみなされる。例えば、セキュリティモジュールのそれぞれは、鍵空間のサブ空間を格納し得る。鍵がセキュリティモジュールを通して重複して格納されるように、セキュリティモジュールによって格納される鍵空間のサブ空間は、重複し得る。いくつかの実施形態では、特定の鍵は、特定される地理的領域内にのみ格納され得る。いくつかの実施形態では、特定の鍵は、特定の認定またはクリアランスレベルを有する動作にのみアクセス可能であり得る。いくつかの実施形態では、特定の鍵は、データ格納サービスのプロバイダとの契約下で、特定の第三者によって動作するモジュール内にのみ格納され得、かつそれと共にのみ使用され得る。いくつかの実施形態では、セキュリティモジュールの建設的制御は、顧客によって許可される以外の鍵の使用を強要しようとする合法命令が、強要されている追加のエンティティ、または行動を強要する追加の管轄のいずれかを含むことを要求し得る。いくつかの実施形態では、顧客は、それらの暗号文が格納されかつそれらの鍵が格納される管轄のための、独立した選択肢を提供され得る。いくつかの実施形態では、鍵を格納するセキュリティモジュールは、鍵の所有者に監査情報を提供するように構成され得、かつ、セキュリティモジュールは、監査情報の生成及び提供が顧客によって抑圧可能でなくなるように構成され得る。いくつかの実施形態では、プロバイダ（例えば、セキュリティモジュールをホストする）が、セキュリティモジュールによって格納される鍵下で動作を実行することができないように、セキュリティモジュールは、独立して、顧客によって生成された署名を立証するように構成され得る。さらに、いくつかのセキュリティモデルは、鍵空間の全てを格納し得、いくつかのセキュリティモジュールは鍵空間のサブ空間を格納し得る。他の変形もまた、本開示の範囲であるとみなされる。異なるセキュリティモジュールが鍵空間の異なるサブ空間を格納する例では、要求処理ユニットは、例えば関係表または他の機構を用いて、様々な要求に従って暗号動作を実行するよう命令すべきセキュリティモジュールを判断するように構成され得る。

【００７７】

一実施形態では、ポリシー実施モジュールは、要求処理ユニットから情報を得て、その情報に少なくとも部分的に基づいて、ＡＰＩを通して受信された要求が実行され得るかどうかを判断するように、構成される。例えば、暗号動作を実行するための要求が、要求ＡＰＩを通して受信される場合、要求処理ユニットは、ポリシー実施モジュールと対話して、要求において特定される鍵ＩＤに適用可能なポリシー等の任意の適用可能なポリシー及び／または要求者に関連付けられるポリシー等の他のポリシー等に従って、要求の遂行が許可されるかどうかを判断し得る。ポリシー実施モジュールが要求の遂行を可能にする場合、要求処理ユニットは、それに応じて、適切なセキュリティモジュールに、要求の遂行に従って暗号動作を実行するように命令し得る。

【００７８】

本明細書に記載される全ての図面と同様に、多くの変形が本開示の範囲内であるとみなされる。例えば、図１６は、セキュリティモジュールとは別個のポリシー実施モジュールを示す。しかしながら、それぞれのセキュリティモジュールは、別個に例示されるポリシー実施モジュールに加えて、またはその代わりに、ポリシー実施モジュールを含み得る。よって、それぞれのセキュリティモジュールは、独立して、ポリシーを実施するように構

成され得る。さらに、別の実施例として、それぞれのセキュリティモジュールは、別個のポリシー実施モジュールによって実施されるポリシーとは異なるポリシーを実施する、ポリシー実施モジュールを含み得る。多くの他の変形は、本開示の範囲内であるとみなされる。

【００７９】

上記のように、要求が鍵ＩＤに対応する鍵に関連して実行されている暗号動作を特定する場合、ポリシーが実施され得るように、様々なポリシーは、鍵ＩＤに関連するユーザによって構成され得る。図１７は、様々な実施形態に従う、ポリシーを更新するためのプロセス１７００の例示的な実施例を提供する。プロセス１７００は、図１６に関連して上で述べられたような、暗号サービスシステム等によって、任意の好適なシステムによって実行され得る。一実施形態では、プロセス１７００は、鍵ＩＤについてのポリシーを更新するための要求を受信１７０２することを含む。要求は、任意の好適な様式で受信１７０２され得る。例えば、例として図１６を参照すると、要求は、上記の暗号サービス１６００のフロントエンドシステムのポリシー構成ＡＰＩを通して受信され得る。要求は、任意の好適な様式で受信され得る。

【００８０】

一実施形態では、プロセス１７００は、認証要求を提出１７０４すること及び認証応答を受信１７０６することを含む。認証要求を提出１７０４すること及び認証応答を受信１７０６することは、上記のような任意の好適な様式で実行され得る。さらに、上記のように、受信された認証応答は、鍵ＩＤについてのポリシーを更新するための要求が真正であるかどうかを判断１７０８するために使用され得る。鍵ＩＤについてのポリシーを更新するための受信された要求が真正でないと判断１７０８される場合、要求は拒否１７１０され得る。要求を拒否１７１０することは、上記のような任意の好適な様式で実行され得る。しかしながら、鍵ＩＤについてのポリシーを更新するための受信された要求が真正であると判断１７０８される場合、プロセス１７００は、要求者に適用可能なポリシー情報にアクセス１７１２することを含み得る。ポリシー情報は、それから要求者に適用可能な任意のポリシーが実施され得る、情報であり得る。例えば、プロセス１７００によって実行される暗号サービスを利用する組織内では、組織の特定のユーザのみが、鍵ＩＤについてのポリシーを更新することができるようにされ得る。ポリシー情報は、どのユーザが暗号サービスに鍵ＩＤについてのポリシーを更新させることができるか、及び／またはさらには、ポリシーが既存のポリシーに従って更新可能であるかどうかを示し得る。例えば、いくつかの実施形態では、暗号サービスは、新ポリシーを実施するための要求を受信し得る。暗号サービスは、任意の既存のポリシーが、新ポリシーを所定の位置に置くことを可能にするかどうかを点検し得る。暗号サービスが、既存のポリシーが新ポリシーの実施を可能にしないと判断する場合、要求は拒否され得る。概して、ポリシー情報は、要求者に適用可能なポリシーの実施のために使用可能な任意の情報であり得る。

【００８１】

図１７に例示されるように、プロセス１７００は、アクセスポリシー情報を使用して、ポリシーが要求された更新を実行することを可能にするかどうかを判断１７０４することを含む。ポリシーが、要求された更新を実行することを可能にしないと判断１７１４される場合、プロセス１７００は、上記のように要求を拒否１７１０することを含み得る。しかしながら、ポリシーが要求された更新を実行することを可能にすると判断１７１４される場合、プロセス１７００は、鍵ＩＤについてのポリシーを更新１７１６することを含み得る。鍵ＩＤについてのポリシーを更新することは、鍵ＩＤに従ってまたはそれに関連して、ポリシー情報を更新すること及び更新されたポリシーを格納することを含み得る。更新されたポリシー情報は、例えば、図１６に関連して上記のような暗号サービスのポリシー実施モジュールによって格納され得る。

【００８２】

ポリシーは、暗号サービスに関連して動作する電子環境の他の構成要素によってもまた実施され得る。例えば、上記の図２を参照すると、暗号サービスは、データサービスフロ

ントエンドが実施するように、ポリシーの電子表示を、データサービスフロントエンドに提供し得る。このようなことは、データサービスがポリシーを実施するためにより良好に適する状況において、有用であり得る。例えば、行動がポリシーによって可能にされるかどうかは、暗号サービスではなく、データサービスフロントエンドにアクセス可能な情報に、少なくとも部分的に基づき得る。一実施例として、ポリシーは、そのポリシーに関連付けられる顧客のために、データサービスバックエンド格納システムによって格納されるデータに依存し得る。

【００８３】

上記のように、暗号サービスは、鍵ＩＤを有する鍵に関するポリシーに従うポリシーの実施を可能にする、様々なシステムを含み得る。したがって、図１８は、ポリシーを実施するために使用され得るプロセス１８００の例示された実施例を示す。プロセス１８００は、図１６に関連して上で述べられたような、暗号サービスシステム等によって、任意の好適なシステムによって実行され得る。一実施形態では、プロセス１８００は、鍵ＩＤを有する鍵を使用して１つ以上の暗号動作を実行するための要求を受信１８０２することを含む。図１８は、プロセス１８００が、１つ以上の暗号動作を実行するための要求に関連して実行されているところを例示するが、プロセス１８００は、必ずしも暗号化に関連しているとは限らない動作を実行するための任意の要求との使用に、適合し得るということに留意すべきである。動作の実施例は上で述べられている。

【００８４】

受信された要求が真正であるかどうかが判断１８０４され得る。受信された要求が真正であるかどうかを判断することは、上記のような任意の好適な様式で実行され得る。例えば、要求が真正であるかどうかを判断１８０４することは、上記のように、認証要求を提出すること及び認証応答を受信することを含み得る。要求が真正であると判断１８０４される場合、プロセス１８００は、要求を拒否１８０６することを含み得る。要求を拒否１８０６することは、上記のような任意の好適な様式で実行され得る。しかしながら、要求が真正であると判断１８０４される場合、プロセス１８００は、鍵ＩＤ及び／または要求者についてのポリシー情報にアクセス１８０８することを含み得る。鍵ＩＤ及び／または要求についてのポリシー情報にアクセスすることは、任意の好適な様式で実行され得る。例えば、鍵ＩＤ及び／または要求者についてのポリシー情報にアクセスすることは、かかるポリシー情報を格納する１つ以上の格納システムからの格納ポリシー情報にアクセスすることによって、実行され得る。アクセスポリシー情報は、ポリシーが１つ以上の動作を実行することを可能にするかどうかを判断１８１０するために使用され得る。

【００８５】

ポリシーが、１つ以上の動作を実行することを可能にしないと判断１８１０される場合、プロセス１８００は、要求を拒否１８０６することを含み得る。しかしながら、ポリシーが１つ以上の動作を実行することを可能にすると判断される場合、プロセス１８００は、要求された１つ以上の暗号動作を実行１８１２することを含み得る。１つ以上の暗号動作の実行の１つ以上の結果は、提供１８１４され得、例えば、１つ以上の暗号動作を実行するための受信１８０２された要求を提出した要求者に、提供される。いくつかの実施形態では、可能にされた要求及びまたは拒否された要求から少なくとも部分的に由来する情報は、監査サブシステムを通して提供され得る。

【００８６】

上記のように、本開示の実施形態は、柔軟なポリシー構成及び実施を可能にする。いくつかの実施形態では、ポリシーは、どのサービスがどの動作をどの文脈で実行することができるかを述べ得る。例えば、鍵に関するポリシーは、データ格納サービスが、暗号サービスに解読動作ではなく暗号動作を実行させることを、可能にし得る。鍵に関するポリシーは、暗号文及び／または解読された平文上に１つ以上の条件もまた含み得る。例えば、ポリシーは、暗号文及び／または平文が、動作の結果が要求に応答して提供される前に、特定のハッシュ値（鍵付ハッシュ値であり得る）を生成することを要求し得る。ポリシーは、そこから要求が由来するインターネットプロトコル（ＩＰ）、暗号化／解読されるコ

ンテンツの種類、ＡＡＤ、及び／または他の情報に、少なくとも部分的に基づく、１つ以上の制限及び／または許可を特定し得る。

【００８７】

多くの変形が、本開示の範囲内であるとみなされる。例えば、上記の様々な実施形態は、別個の認証サービスとの対話について記載する。しかしながら、上記の環境の構成要素は、それら自体の許可構成要素を有し得、要求が真正であるかどうかを判断することは、別のエンティティとの通信を含んでも含まなくてもよい。さらに、上記の環境のそれぞれは、環境によって可能にされる特定の動作及び能力に関連して例示される。異なる環境に関連して上記の技術は、組み合され得、かつ、概して、本開示に従う環境は、様々な技術の柔軟な使用を可能にし得る。ほんの一実施例として、暗号サービスは、要求の際に、鍵及び非鍵データ対象等の他のコンテンツの両方を暗号化するために使用され得る。別の例として、暗号サービスは、ユーザ（例えば、コンピューティングリソースプロバイダの顧客）及び他のサービス（例えば、データ格納サービス）の両方からの要求を受信してそれに応答するように構成され得る。いくつかの実施形態では、暗号サービス及び／または関連する認証サービスは、格納されたデータの暗号化を実行するための携帯デバイスとの使用のために構成され得る。いくつかの実施形態では、少なくとも１つのロック解除ピンが、暗号サービスによって立証され得る。なおも他の実施形態では、暗号サービスは、動作の一部として、ハードウェア構成証明によって生成される情報を受信し得る。いくつかの実施形態では、暗号サービスは、コンテンツに関して、デジタル権利管理サービスを提供するように動作可能であり得る。

【００８８】

本開示の実施形態は、以下の付記を考慮して説明することができる。

１．データ格納サービスを提供するためのコンピュータ実装方法であって、

コンピューティングリソースサービスプロバイダの、実行可能命令で構成される１つ以上のコンピュータシステムの制御下で、

該コンピューティングリソースサービスプロバイダの顧客から、該コンピューティングリソースサービスプロバイダのデータ格納サービスを利用するための要求を受信することと、

該データ格納サービスを利用するための要求を受信した結果として、該コンピューティングリソースサービスプロバイダの暗号サービスに、該データ格納サービスにアクセス不能な鍵を使用して該暗号サービスによって暗号化された情報を提供させることであって、該情報が、非暗号化形式の該データ対象と、該コンピューティングリソースサービスプロバイダの複数の顧客のために該暗号サービスによって管理される複数の鍵からの該鍵と、を得るために使用可能である、提供させることと、

該暗号化された情報を格納するために該データ格納サービスを使用することと、を含む、該コンピュータ実装方法。

２．該暗号サービスに該暗号化された情報を提供させることが、該暗号サービスが該受信された要求の申請を検証することができるようにする証明情報を、該暗号サービスに提供することを含み、

該証明情報が、該暗号サービスが該暗号化された情報を提供するために必須である、付記１に記載の該コンピュータ実装方法。

３．該データ格納サービスを利用するための該要求が、該データ格納サービスを使用してデータを暗号化形式で格納するための要求を含み、

該情報が該データ対象を暗号化するために使用される第２の鍵を含み、

該暗号化された情報を格納するために該データ格納サービスを使用することが、該データ対象を暗号化形式で格納するために該データ格納サービスを使用することを含む、付記１または２に記載の該コンピュータ実装方法。

４．該データ格納サービスから該データ対象を読み出すための要求を受信することと、

該データ格納サービスから該暗号化された情報を得ることと、

該暗号サービスに該暗号化された情報を解読させることと、

該データ対象を読み出すための該受信された要求に応答して、該データ対象を提供するために該情報を使用することと、をさらに含む、付記１～３のいずれか一項に記載の該コンピュータ実装方法。
５．該データ対象を読み出すための該受信された要求に応答して該データ対象を提供するために該情報を使用することが、該暗号化されたデータ対象を解読するために該鍵を使用することを含む、付記４に記載の該コンピュータ実装方法。
６．解読のために該暗号化された情報を該暗号サービスに提供することと、
該暗号サービスに、該鍵に関するポリシーが、該鍵が該暗号化された情報を解読するために使用されることを可能にするかどうかを点検させ、該ポリシーによって可能にされる場合、該暗号化された情報を解読させることと、をさらに含む、付記１～５のいずれか一項に記載の該コンピュータ実装方法。
７．該顧客から、該鍵に関するポリシーを表す情報を受信することをさらに含み、
該暗号サービスに、該表されるポリシーに従って動作させる、付記１～６のいずれか一項に記載の該コンピュータ実装方法。
８．該暗号サービスから該鍵に関するポリシーを受信することと、
該受信されたポリシーが該要求の遂行を可能にするかどうかを点検することと、をさらに含み、
該暗号サービスに該暗号化された情報を提供させることが、該要求の遂行を可能にする該ポリシーに依存し、
該暗号サービスに、該表されるポリシーに従って動作させる、付記１に記載の該コンピュータ実装方法。をさらに含む、付記１～７のいずれか一項に記載の該コンピュータ実装方法。
９．暗号サービスを提供するためのコンピュータ実装方法であって、
実行可能命令で構成される１つ以上のコンピュータシステムの制御下で、
サービスが該サービスを利用するための第１の要求を受信することの結果として、該第１の要求を遂行するために必要な１つ以上の暗号動作を実行するための第２の要求を受信することと、
該要求された１つ以上の暗号動作を実行することと、
該要求された１つ以上の暗号動作の実行の１つ以上の結果を該サービスに提供することであって、該１つ以上の結果が、該サービスを利用するための該受信された要求の遂行の少なくとも１つの様式に必要である、提供することと、を含む、該コンピュータ実装方法。
１０．該１つ以上の暗号動作が、該データサービスを利用するための該受信された要求を遂行するために必要とされる鍵の解読を含む、付記９に記載の該コンピュータ実装方法。
１１．該データサービスを利用するための該受信された要求が真正であることを検証する情報を受信することをさらに含み、
該１つ以上の暗号動作を実行することが、該サービスを利用するための該受信された要求が真正であることを検証する該情報の受信を必要とする、付記９または１０に記載の該コンピュータ実装方法。
１２．該サービスを利用するための該受信された要求が、該サービスによって格納されるデータを得るための要求である、付記９～１１のいずれか一項に記載の該コンピュータ実装方法。
１３．該サービスを利用するための該受信された要求が、該サービスを使用してデータを格納するための要求である、付記９～１２のいずれか一項に記載の該コンピュータ実装方法。
１４．異なるエンティティのために該暗号サービスによってそれぞれ管理される少なくとも２つの鍵を含む複数の鍵から、該１つ以上の暗号動作を実行するための少なくとも１つの鍵を選択することをさらに含む、付記９～１３のいずれか一項に記載の該コンピュータ実装方法。
１５．該１つ以上の暗号動作が鍵の使用を必要とし、

該方法が、該鍵のために該鍵についてのポリシーを受信することをさらに含み、
該１つ以上の暗号動作を実行することが、該１つ以上の暗号動作の実行が該受信されたポリシーを順守することを必要とする、付記９～１４のいずれか一項に記載の該コンピュータ実装方法。
１６．該１つ以上の暗号動作を実行するために使用可能な鍵についてのポリシーを受信することと、
既存のポリシーが該ポリシーの実装を可能にするかどうかを点検することと、
該既存のポリシーが該ポリシーの実装を許可しないことの結果として、該受信されたポリシーを拒否することと、をさらに含む、をさらに含む、付記９～１５のいずれか一項に記載の該コンピュータ実装方法。
１７．コンピュータシステムであって、
１つ以上のプロセッサと、
メモリであって、該コンピュータシステムに、少なくとも、
暗号サービスであって、少なくとも、
複数の鍵が該暗号サービスとは異なるサービスにアクセス不能になるように、該複数の鍵を格納することと、
該サービスにおいて保留中の要求の検出時に、該複数の鍵から１つの鍵を選択し、該選択された鍵を使用して該保留中の要求を遂行するために必要とされる１つ以上の暗号動作を実行することと、を行うように構成される暗号サービスを、実装させるための、該１つ以上のプロセッサによって実行可能な命令を格納する、メモリと、を備える該コンピュータシステム。
１８．該サービスにおいて保留中の該要求を検出することが、該サービスから該サービスにおいて保留中の該要求の通知及び証明を受信することを含む、付記１７に記載の該コンピュータシステム。
１９．該コンピュータシステムがコンピューティングリソースサービスプロバイダによって動作し、
該要求が、該コンピューティングリソースプロバイダの複数の顧客のうちの１人の顧客によって生成され、
該複数の鍵のそれぞれの鍵が、該コンピューティングリソースプロバイダの対応する顧客を有する、付記１７または１８に記載の該コンピュータシステム。
２０．該暗号サービスが、該保留中の要求が許可されることを検証するようにさらに構成される、付記１７～１９のいずれか一項に記載の該コンピュータシステム。
２１．該暗号サービスの出力を受信し、かつ該受信された出力に少なくとも部分的に基づいてアカウント記録を生成するように構成される、計量サービスをさらに備える、付記１７～２０のいずれか一項に記載の該コンピュータシステム。
２２．該暗号サービスが、
該複数の鍵の少なくとも１つのサブセットのそれぞれについての１つ以上のポリシーを定義するポリシー情報を格納することと、
該定義された１つ以上のポリシーを実施することと、を行うようにさらに構成される、付記１７～２１のいずれか一項に記載の該コンピュータシステム。
２３．該コンピュータシステムがコンピューティングリソースサービスプロバイダによって動作し、
該複数の鍵のそれぞれの鍵が、該コンピューティングリソースプロバイダの顧客に対応し、
該暗号サービスが、
該コンピューティングリソースプロバイダの顧客からポリシー更新を受信することと、
該受信されたポリシー更新に従って該格納されたポリシー情報を更新することと、を行うように構成される、付記２２に記載の該コンピュータシステム。
２４．コンピュータ可読格納媒体であって、コンピュータシステムの１つ以上のプロセッ

サによって実行されると、該コンピュータシステムに、少なくとも、
サービスを利用するための要求を受信することと、
該サービスを利用するための該要求を受信したことの結果として、
該要求に少なくとも部分的に基づいて、暗号サービスに、該要求が受信されたという証明を提供して、それにより、１つ以上の暗号動作が実行された後、該サービスを利用するための該要求を遂行するために使用可能になる情報に関する、該１つ以上の暗号動作を実行させるために鍵を使用させることと、
それに関して該１つ以上の暗号動作が実行された該情報を使用して、該サービスを利用するための該要求を遂行することと、を行わせる、そこに格納される命令を有する、該コンピュータ可読格納媒体。
２５．該証明が、該暗号サービスが、該サービスを利用するための該要求が真正であることを検証することができるようにする、認証情報を含む、付記２４に記載の該コンピュータ可読格納媒体。
２６．該サービスを利用するための該要求が、データ対象に関連する動作を実行するための要求を含み、
該情報が、該データ対象を暗号化するために使用される鍵である、付記２４または２５に記載の該コンピュータ可読格納媒体。
２７．該命令が、該１つ以上のプロセッサによって実行されると、該暗号サービスに、該鍵に関する１つ以上のポリシーを実施させ、該１つ以上のポリシーが、該１つ以上の暗号動作が該鍵を使用して実行可能であるかどうかの決定因である、付記２４～２６のいずれか一項に記載の該コンピュータ可読格納媒体。
２８．該サービスを利用するための該要求が、データ対象に関連する格納動作を実行するための要求である、付記２４～２７のいずれか一項に記載の該コンピュータ可読格納媒体。
２９．該暗号サービスに、１つ以上の暗号動作を実行するために該鍵を使用させることが、該暗号サービスが該暗号サービスによって格納される複数の鍵から該鍵を選択することを可能にするために、該鍵の識別子を提供することを含む、付記２４～２８のいずれか一項に記載の該コンピュータ可読格納媒体。

【００８９】

図１９は、様々な実施形態に従う態様を実装するための、環境１９００の実施例の態様を例示する。理解され得るように、ウェブベースの環境が説明の目的のために使用されるが、様々な実施形態を実装するために異なる環境が適切なように使用され得る。環境は、電子クライアントデバイス１９０２を含み、これは、要求、メッセージ、または情報を、適切なネットワーク１９０４を介して送信及び受信するように、ならびにデバイスのユーザに情報を運んで戻すように動作可能な、任意の適切なデバイスを含み得る。かかるクライアントデバイスの例には、パーソナルコンピュータ、携帯電話、携帯型メッセージングデバイス、ノートパソコン、セットトップボックス、携帯情報端末、電子ブックリーダ等が挙げられる。ネットワークは、イントラネット、インターネット、セルラーネットワーク、ローカルエリアネットワーク、もしくは任意の他のかかるネットワーク、またはそれらの組み合わせを含む、任意の適切なネットワークを含み得る。かかるシステムのために使用される構成要素は、選択されるネットワーク及び／または環境の種類に、少なくとも部分的に依存し得る。かかるネットワークを介して通信するためのプロトコル及び構成要素は公知であり、本明細書において詳細に説明されない。ネットワークを介する通信は、有線または無線接続及びそれらの組み合わせによって可能にされ得る。本実施例では、環境が、要求の受信及びそれに応答するコンテンツの提供のためのウェブサーバ１９０６を含むため、ネットワークはインターネットを含むが、他のネットワークについては、当業者には明白であり得るように、同様の目的に提供する代替のデバイスが使用され得る。

【００９０】

例示的な環境は、少なくとも１つのアプリケーションサーバ１９０８及びデータストア１９１０を含む。いくつかのアプリケーションサーバ、レイヤー、または、チェーン接続

もしくは別様で構成され得、適切なデータストアからデータを得る等のタスクを実行するために対話し得る、他の要素、プロセス、もしくは構成要素があり得るということが理解されるべきである。本明細書で使用する場合、「データストア」という用語は、データを格納、データにアクセス、及びデータを読み出すことができる、任意のデバイスまたはデバイスの組み合わせを指し、これは、任意の標準、分散、またはクラスタ環境内の、データサーバ、データベース、データ格納デバイス、及びデータ格納媒体を、任意の組み合わせで任意の数含み得る。アプリケーションサーバは、クライアントデバイスのための１つ以上のアプリケーションの態様を実行するために必要とされるため、データストアと統合するための、アプリケーションのための大半のデータアクセス及びビジネス論理を処理する、任意の適切なハードウェア及びソフトウェアを含み得る。アプリケーションサーバは、データストアと協働してアクセス制御サービスを提供し、ユーザに移送される、テキスト、画像、音声、及び／または動画等のコンテンツを生成することができ、これは、本実施例では、ハイパーテキストマークアップ言語（「ＨＴＭＬ」）、拡張マークアップ言語（「ＸＭＬ」）、または別の適切な構造言語の形態で、ウェブサーバによってユーザに提供され得る。全ての要求及び応答の処理、ならびにクライアントデバイス１９０２とアプリケーションサーバ１９０８との間のコンテンツの送達は、ウェブサーバによって処理され得る。本明細書に記載される構造コードは任意の適切なデバイス上で実行され得、または本明細書の他の箇所で記載のように機械をホストし得るので、ウェブ及びアプリケーションサーバは、要求されず、かつ、単に構成要素の例であるということが理解されるべきである。

【００９１】

データストア１９１０は、いくつかの別個のデータ表、データベース、または他のデータ格納機構、及び特定の態様に関連するデータを格納するための媒体を含み得る。例えば、例示されるデータストアは、生産データ１９１２及びユーザ情報１９１６を格納するための機構を含み、これは、生産側にコンテンツを提供するために使用され得る。データストアは、ログデータ１９１４を格納するための機構を含むこともまた示され、これは、報告、分析、または他のかかる目的のために使用され得る。適切なように上記の機構のうちのいずれか内に、またはデータストア１９１０内の追加の機構内に、格納され得る、ページ画像情報のため及び正しい情報にアクセスするために、データストア内に格納される必要があり得る、多くの他の態様があり得るということが理解されるべきである。データストア１９１０は、そこに関連付けられる論理を通して、アプリケーションサーバ１９０８から命令を受信して、それに応答してデータを得る、更新する、または別様で処理するように動作可能である。一実施例では、ユーザは、特定の種類のアイテムについての検索要求を提出し得る。この場合、データストアは、ユーザ情報にアクセスしてユーザの識別を検証し得、かつ、カタログ詳細情報にアクセスしてその種類のアイテムについての情報を得ることができる。その後情報は、ユーザがユーザデバイス１９０２のブラウザを介して見ることができるウェブページ上に記載される結果において、ユーザに戻され得る。対象の特定のアイテムについての情報は、ブラウザの専用ページまたはウィンドウで見ることができる。

【００９２】

それぞれのサーバは、典型的に、そのサーバの一般管理及び動作についての実行可能プログラム命令を提供するオペレーティングシステムを含み得、かつ、典型的に、サーバのプロセッサによって実行されると、サーバがその意図される機能を実行することができるようにする命令を格納する、コンピュータ可読格納媒体（例えば、ハードディスク、ランダムアクセスメモリ、読み取り専用メモリ等）を含み得る。サーバのオペレーティングシステム及び一般機能性についての好適な実装は、既知または商用的に入手可能であり、かつ、特に本明細書の開示を踏まえると当業者によって容易に実装される。いくつかの実施形態では、オペレーティングシステムは、評価保証レベル（ＥＡＬ）のレベル４等の、１つ以上の立証体制に従って構成され得、またはその下で立証され得る。

【００９３】

一実施形態における環境は、１つ以上のコンピュータネットワークまたは直接接続を使用して、通信リンクを介して相互接続される、いくつかのコンピュータシステム及び構成要素を利用する、分散コンピューティング環境である。しかしながら、このようなシステムは、図１９に図示されるものよりも少ないかまたは多い数の構成要素を有するシステムにおいても、同様に良好に動作し得ることが、当業者には理解されるであろう。したがって、図１９のシステム１９００の説明は、本質的に例示的であり、本開示の範囲を限定するものではないと捉えられるべきである。

【００９４】

様々な実施形態は、さらに、幅広い様々な動作環境において実装され得、これは、いくつかの場合では、多数のアプリケーションのうちのいずれかを動作させるために使用することができる、１つ以上のユーザコンピュータ、コンピューティングデバイス、または処理デバイスを含み得る。ユーザまたはクライアントデバイスは、標準オペレーティングシステムを稼働させるデスクトップもしくはラップトップコンピュータ、ならびに、携帯ソフトウェアを稼働させかつ多数のネットワーキング及びメッセージプロトコルを支持することができる、セルラー、無線、及び携帯型デバイス等の、多数の汎用パーソナルコンピュータのうちのいずれかを含み得る。かかるシステムは、様々な商用的に入手可能なオペレーティングシステムならびに開発及びデータベース管理等の目的のための他の既知のアプリケーションを稼働させる、いくつかのワークステーションもまた含み得る。これらのデバイスは、ダミー端子、シンクライアント、ゲーム機、及びネットワークを介して通信することができる他のデバイス等の、他の電子デバイスもまた含み得る。

【００９５】

ほとんどの実施形態は、伝送制御プロトコル／インターネットプロトコル（「ＴＣＰ／ＩＰ」）、開放型システム間相互接続（「ＯＳＩ」）、ファイル転送プロトコル（「ＦＴＰ」）、ユニバーサルプラグアンドプレイ（「ＵｐｎＰ」）、ネットワークファイルシステム（「ＮＦＳ」）、共通インターネットファイルシステム（「ＣＩＦＳ」）、及びＡｐｐｌｅ　Ｔａｌｋ等の、様々な商用的に入手可能なモデル及びプロトコルのいずれかを使用する通信を支持するために、当業者になじみのあり得る少なくとも１つのネットワークを利用する。ネットワークは、例えば、ローカルエリアネットワーク、広域ネットワーク、仮想プライベートネットワーク、インターネット、イントラネット、エクストラネット、公衆交換電話網、赤外線ネットワーク、無線ネットワーク、及びそれらの任意の組み合わせであり得る。

【００９６】

ウェブサーバを利用する実施形態では、ウェブサーバは、ハイパーテキスト転送プロトコル（「ＨＴＴＰ」）、サーバ、ＦＴＰサーバ、共通ゲートウェイインターフェース（「ＧＣＩ」）サーバ、データサーバ、Ｊａｖａサーバ、及びビジネスアプリケーションサーバを含む、様々なサーバもしくは中間階層アプリケーションのいずれかを稼働させ得る。サーバ（複数可）は、Ｊａｖａ（登録商標）、Ｃ、Ｃ＃、またはＣ＋＋等の任意のプログラム言語、または、Ｐｅｒｌ、Ｐｙｔｈｏｎ、もしくはＴＣＬ等のスクリプト言語、ならびにそれらの組み合わせで書き込まれる、１つ以上のスクリプトまたはプログラムとして実装され得る、１つ以上のウェブアプリケーションを実行することによって、ユーザデバイスからの要求に応答して、プログラムまたはスクリプトを実行することもまたでき得る。サーバ（複数可）は、Ｏｒａｃｌｅ（登録商標）、Ｍｉｃｒｏｓｏｆｔ（登録商標）、Ｓｙｂａｓｅ（登録商標）、及びＩＢＭ（登録商標）から商用的に入手可能なものを含むがこれらに限定されない、データベースサーバもまた含み得る。

【００９７】

環境は、上記のように様々なデータストアならびに他のメモリ及び格納媒体を含み得る。これらは、コンピュータのうちの１つ以上にローカルな（かつ／もしくはそこに常駐する）、または、ネットワークを渡るコンピュータのいずれかまたは全てから遠隔の、格納媒体上等の、様々な位置に常駐し得る。実施形態の特定の組では、情報は、当業者になじみのあるストレージエリアネットワーク（「ＳＡＮ」）内に存在し得る。同様に、コンピ

ュータ、サーバ、または他のネットワークデバイスに属する機能を実行するための任意の必要なファイルは、適宜、ローカルに及び／または遠隔に格納され得る。システムがコンピュータ化されたデバイスを含む場合、それぞれのかかるデバイスは、バスを介して電気的に連結され得るハードウェア要素を含み得、要素は、例えば、少なくとも１つの中央処理ユニット（「ＣＰＵ」）、少なくとも１つの入力デバイス（例えば、マウス、キーボード、コントローラ、タッチスクリーン、またはキーパッド）、及び少なくとも１つの出力デバイス（例えば、ディスプレイデバイス、プリンタ、またはスピーカ）を含む。かかるシステムは、ディスクドライブ、光格納デバイス、及びランダムアクセスメモリ（「ＲＡＭ」）または読み取り専用メモリ（「ＲＯＭ」）等の固体格納デバイス、ならびに取り外し可能媒体デバイス、メモリカード、フラッシュカード等の、１つ以上の格納デバイスもまた含み得る。本開示の様々な実施形態は、カスタム暗号プロセッサ、スマートカード、及び／またはハードウェアセキュリティモジュールを含むがこれらに限定されない、カスタムハードウェアを使用してもまた実装され得る。

【００９８】

かかるデバイスは、上記のように、コンピュータ可読格納媒体リーダ、通信デバイス（例えば、モデム、ネットワークカード（無線もしくは有線）、赤外線通信デバイス等）及びワーキングメモリもまた含み得る。コンピュータ可読格納媒体リーダは、コンピュータ可読情報を、一時的及び／またはより永続的に、含有、格納、伝送、及び読み出すための、遠隔、ローカル、固定、及び／または取り外し可能格納デバイス、ならびに格納媒体を表す、コンピュータ可読格納媒体と、接続されるかまたはそれを受信するように、構成され得る。システム及び様々なデバイスは、典型的に、オペレーティングシステム、及びクライアントアプリケーションまたはウェブブラウザ等のアプリケーションプログラムを含む、少なくとも１つのワーキングメモリデバイス内に位置する、多数のソフトウェアアプリケーション、モジュール、サービス、または他の要素を含み得る。代替の実施形態は、上記のものからの多数の変形を有し得ることが理解されるべきである。例えば、特製のハードウェアもまた使用され得、かつ／または、特定の要素がハードウェア、ソフトウェア（アプレット等のポータブルソフトウェアを含む）、もしくはその両方において実装され得る。さらに、ネットワーク入力／出力デバイス等の、他のコンピューティングデバイスへの接続が用いられ得る。

【００９９】

コードまたはコードの一部を含有するための、格納媒体及びコンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、電気的消去可能プログラム可能読み取り専用メモリ（「ＥＥＰＲＯＭ」）、フラッシュメモリもしくは他のメモリ技術、コンパクトディスク読み取り専用メモリ（「ＣＤ－ＲＯＭ」）、デジタル多用途ディスク（ＤＶＤ）、または他の光格納装置、磁気カセット、磁気テープ、磁気ディスク格納装置、もしくは他の磁気格納デバイス、または所望の情報を格納するために使用することができかつシステムデバイスによってアクセスすることができる、任意の他の媒体を含む、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータ等の情報の、格納及び／または伝送の任意の方法または技術において実装される、揮発性及び非揮発性、取り外し可能及び取り外し不能媒体等の、しかしこれらに限定されない格納媒体を含む、当業者に既知のまたは使用される任意の適切な媒体を含み得る。本明細書に提供される開示及び教示に基づいて、当業者は、様々な実施形態を実装するための、他の方法及び手法を理解するであろう。

【０１００】

したがって、明細書及び図面は、制限的というよりも例示的な意味で見なされるべきである。しかしながら、特許請求の範囲で述べられる本発明のより広い精神及び範囲から逸脱することなく、それに様々な修正及び変更がなされ得るということが明らかである。

【０１０１】

他の変形は、本開示の精神の範囲内である。よって、開示される技術は、様々な修正及び代替の構造を取り得るが、それらの特定の例示される実施形態が、図面に示され、詳細に上記で説明された。しかしながら、本発明を特定の形式または開示される形式に限定す

る意図はなく、しかし、逆に、意図は、添付の特許請求の範囲において定義される本発明の精神及び範囲内に収まる、全ての修正、代替構造、及び等価物を網羅することであるということが理解されるべきである。

【０１０２】

開示される実施形態を説明する文脈における（特に、以下の特許請求の範囲の文脈における）、「ａ」、「ａｎ」、及び「ｔｈｅ」という用語、ならびに同様の指示対象は、本明細書に別様が示されない限りまたは文脈によって明らかに矛盾しない限り、単数及び複数の両方を網羅すると解釈されるべきである。「備える」、「有する」、「含む」、及び「含有する」という用語は、別様が述べられない限り、開放型用語（すなわち、「含むがそれに限定されない」ことを意味する）であると解釈されるべきである。「接続される」という用語は、介在する何かがある場合であっても、部分的にまたは全体的に、内部に含有される、取り付けられる、一緒に接合されると解釈されるべきである。本明細書の値の範囲の列挙は、本明細書で別様が示されない限り、単に、範囲内に収まるそれぞれの別個の値を個々に指す速記方法としての役割を果たすことが意図され、それぞれの別個の値は、本明細書に個々に列挙されるかのように、本明細書に組み込まれる。本明細書に記載される全ての方法は、本明細書に別様が示されない限り、または文脈によって別様が明らかに矛盾しない限り、任意の好適な順序で実行され得る。本明細書で提供される、任意の及び全ての実施例、または例を示す表現（例えば、「等」）の使用は、単に、本発明の実施形態をより良好に解明することを意図し、別様が主張されない限り、本発明の範囲に限定を課すものではない。いかなる本明細書の表現も、非請求要素を本発明の実践に必須であるとして示すと解釈されるべきではない。

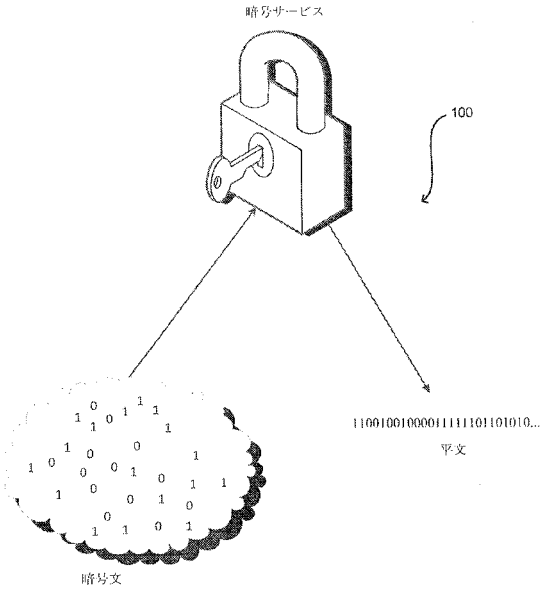
【０１０３】

本発明を実行するために発明者に既知の最善のモードを含む、本開示の好ましい実施形態が本明細書に記載される。これらの好ましい実施形態の変形は、前述の説明を読む際に、当業者に明らかになり得る。発明者は、当業者がかかる変形を適切なように用いることを予期し、発明者は、発明が本明細書に具体的に記載されるのとは別様で実践されることを意図する。したがって、本発明は、適用法によって許可されるように、本明細書に添付される特許請求の範囲で列挙される主題の全ての修正及び等価物を含む。さらに、それらの全ての可能な変形における、上記の要素の任意の組み合わせは、本明細書に別様が示されない限り、または文脈によって別様が明らかに矛盾しない限り、本発明によって包括される。

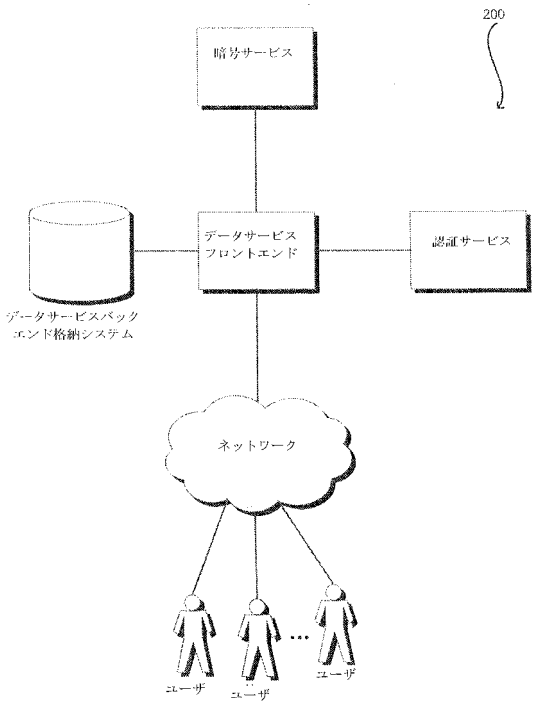
【０１０４】

本明細書に引用される、出版物、特許出願、及び特許を含む、全ての参照文献は、それぞれの参照文献が、あたかも個々にかつ具体的に参照により組み込まれることが示され、かつ本明細書にその全体が述べられるのと同じ程度で、参照によりここに組み込まれる。

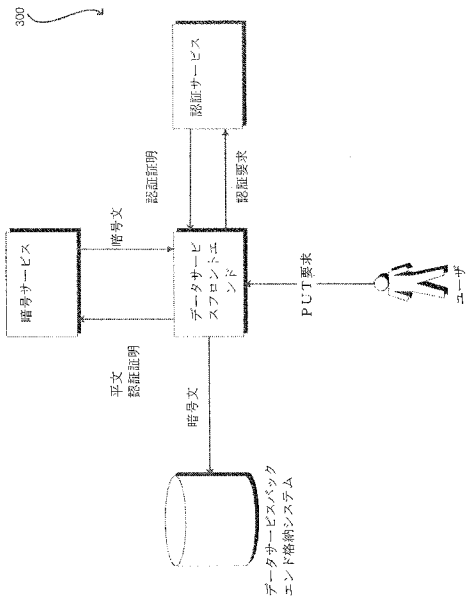
【図１】


暗号サービス
100
1100100100001111101101010...
平文
暗号文

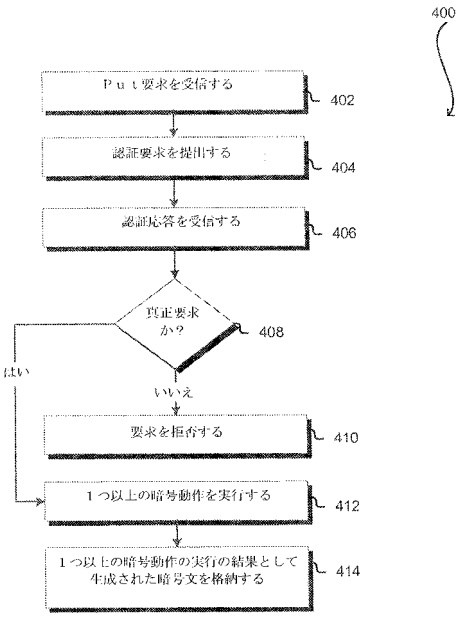
【図２】


200
暗号サービス
データサービス
フロントエンド
認証サービス
データサービスバック
エンド格納システム
ネットワーク
ユーザ
ユーザ
ユーザ

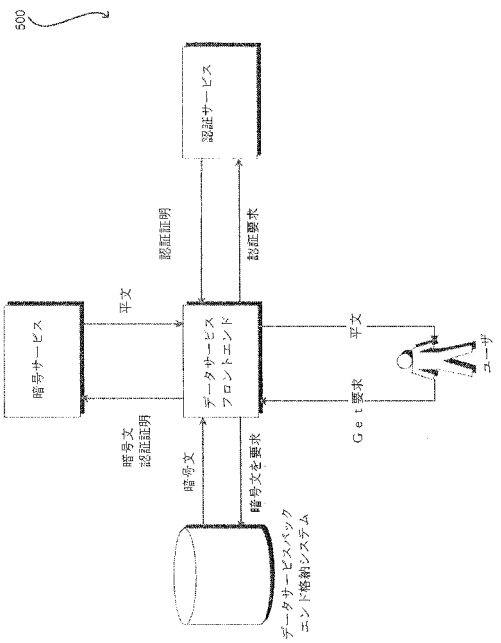
【図３】


300
認証サービス
認証証明
認証要求
暗号文
暗号サービス
データサービス
フロントエンド
PUT要求
ユーザ
平文
認証証明
暗号文
データサービスバック
エンド格納システム

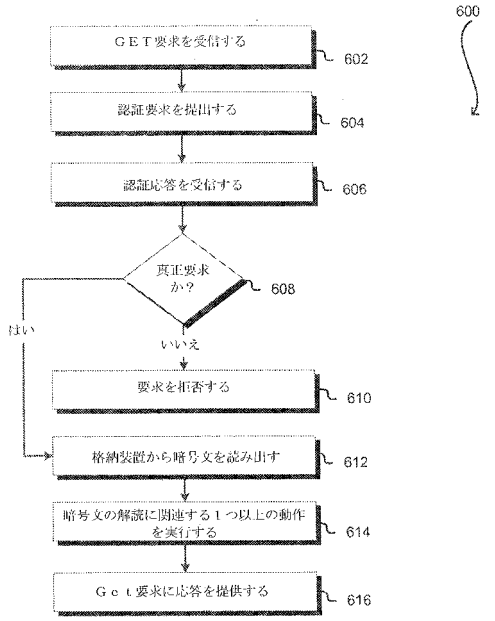
【図４】


400
Put要求を受信する
402
認証要求を提出する
404
認証応答を受信する
406
署名要求か？
408
はい
いいえ
要求を拒否する
410
1つ以上の暗号動作を実行する
412
1つ以上の暗号動作の実行の結果として生成された暗号文を格納する
414

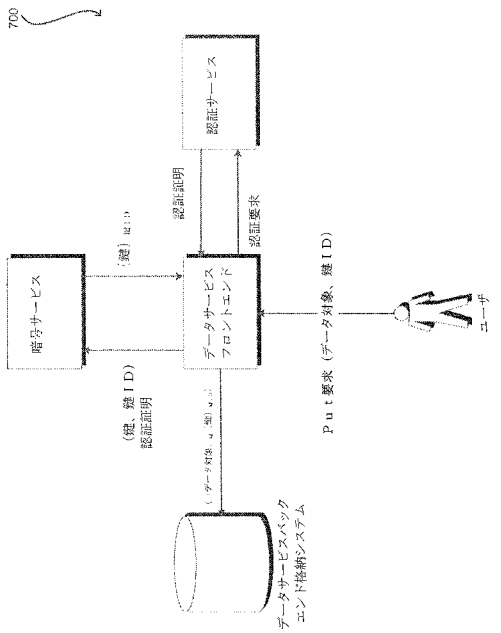
【図５】


500
認証サービス
認証証明
認証要求
暗号サービス
平文
データサービス
フロントエンド
平文
ユーザ
Ｇｅｔ要求
暗号文
認証証明
暗号文
暗号文を要求
データサービスバック
エンド格納システム

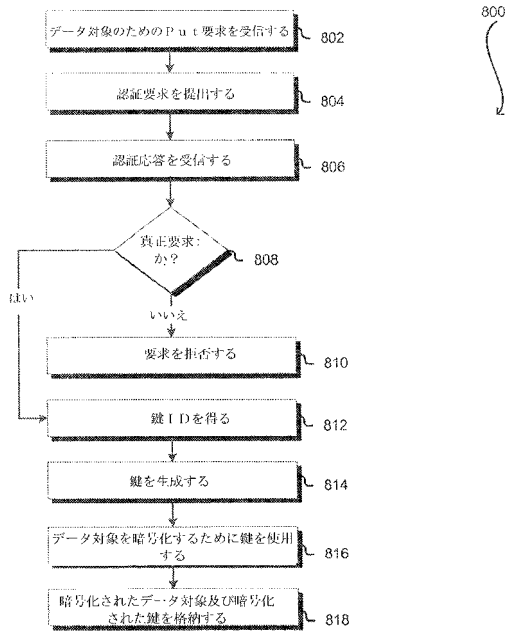
【図６】


600
ＧＥＴ要求を受信する
602
認証要求を提出する
604
認証応答を受信する
606
真正要求か？
608
はい
いいえ
要求を拒否する
610
格納装置から暗号文を読み出す
612
暗号文の解読に関連する１つ以上の動作を実行する
614
Ｇｅｔ要求に応答を提供する
616

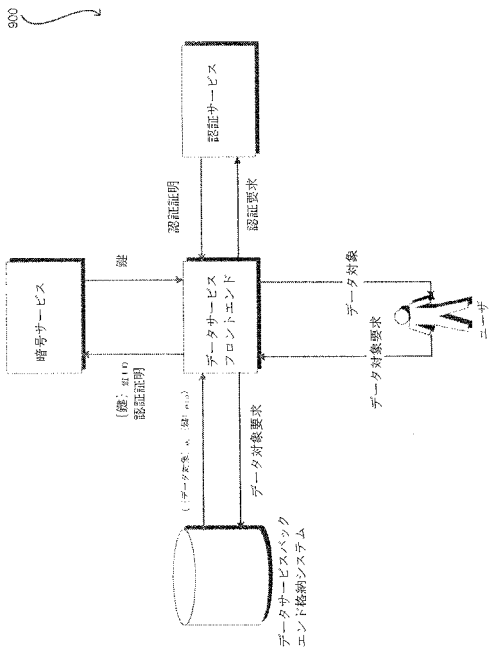
【図７】


700
認証サービス
認証証明
認証要求
暗号サービス
データサービス
フロントエンド
ユーザ
Ｐｕｔ要求（データ対象、鍵ＩＤ）
（鍵、鍵ＩＤ）
認証証明
データサービスバック
エンド格納システム

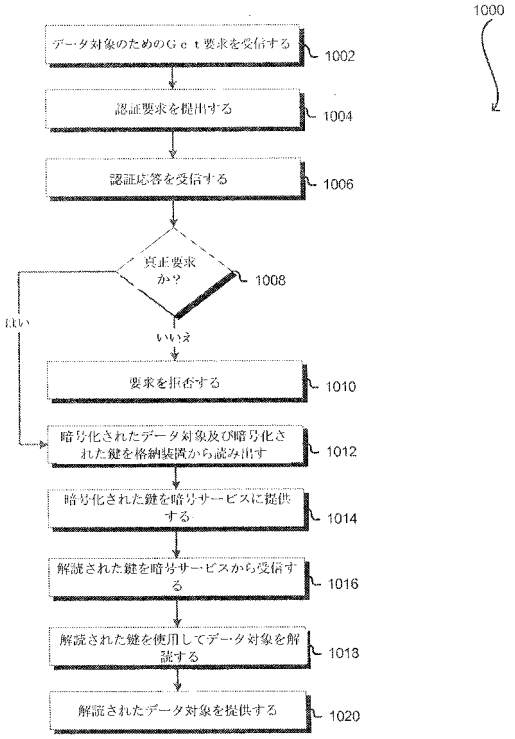
【図８】


800
データ対象のためのＰｕｔ要求を受信する
802
認証要求を提出する
804
認証応答を受信する
806
真正要求か？
808
はい
いいえ
要求を拒否する
810
鍵ＩＤを得る
812
鍵を生成する
814
データ対象を暗号化するために鍵を使用する
816
暗号化されたデータ対象及び暗号化された鍵を格納する
818

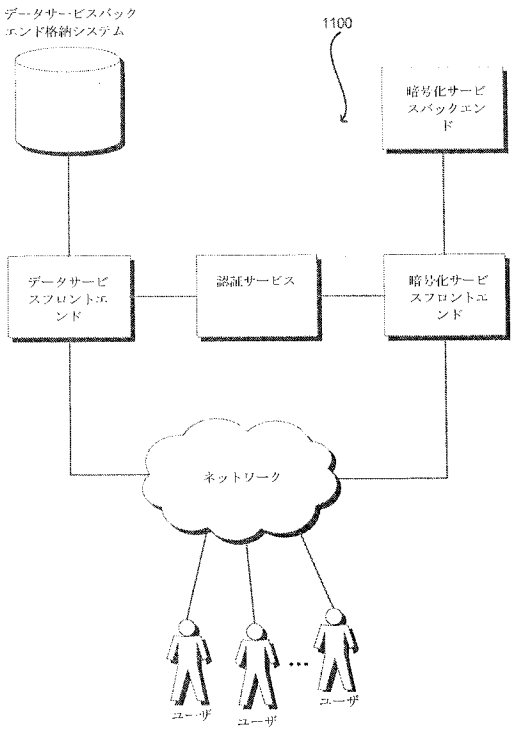
【図９】



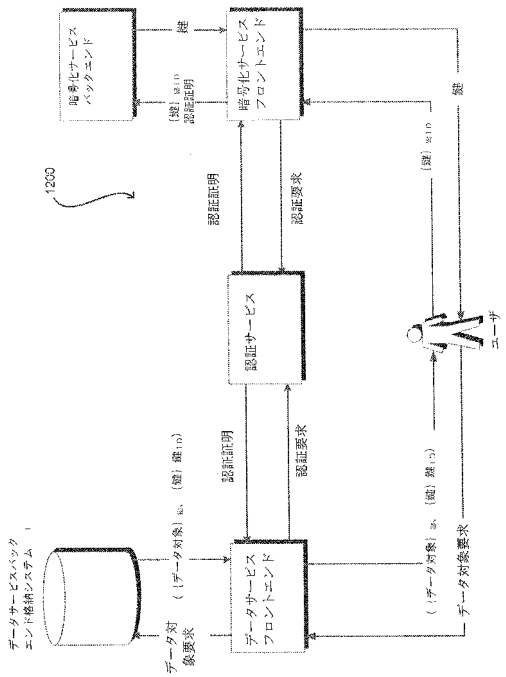
【図１０】



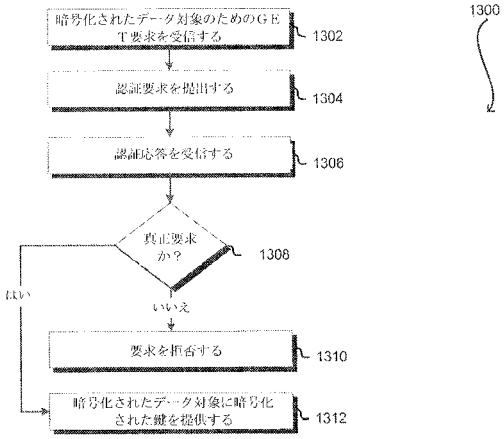
【図１１】



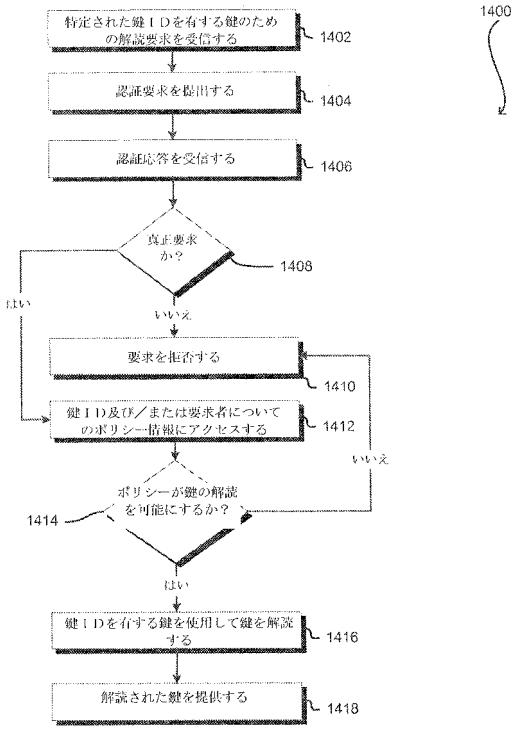
【図１２】



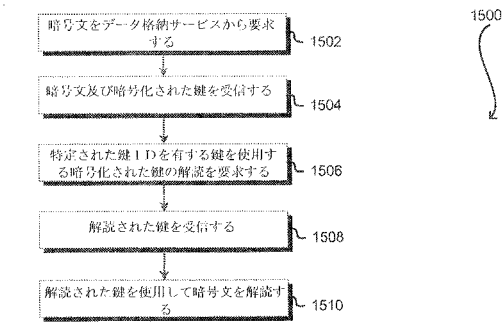
【図１３】



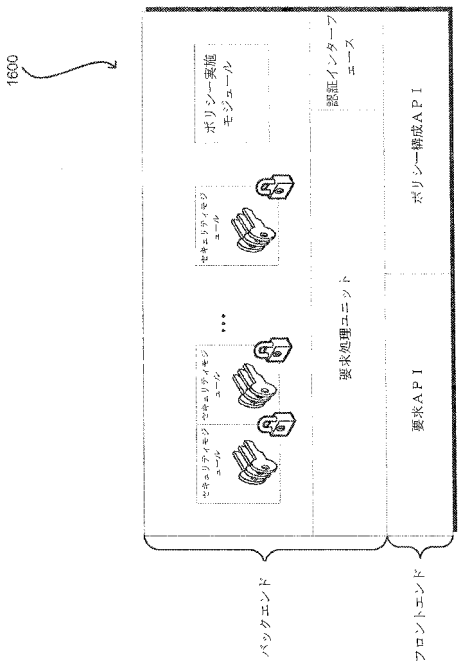
【図１４】



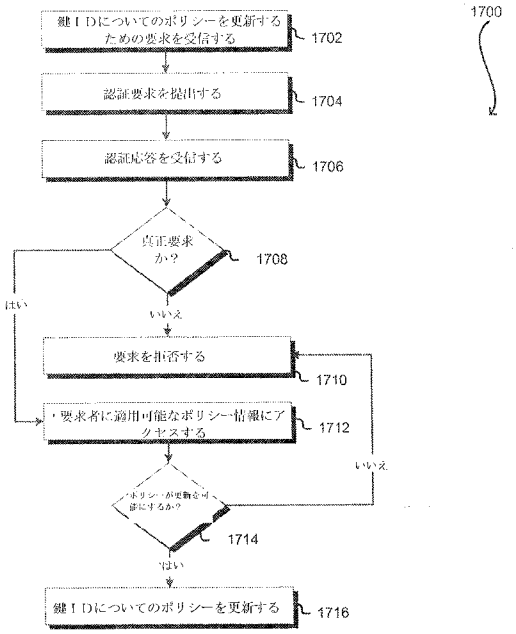
【図１５】



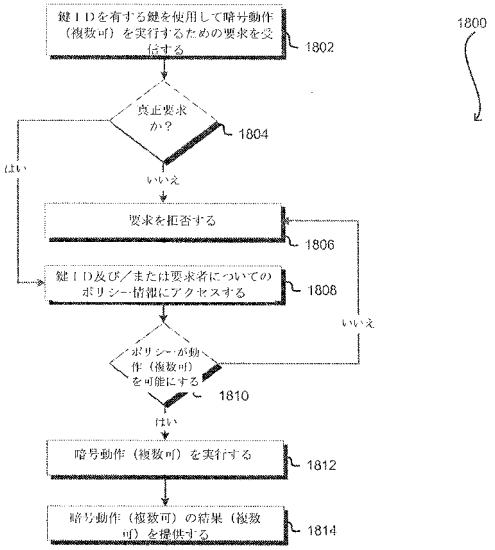
【図１６】



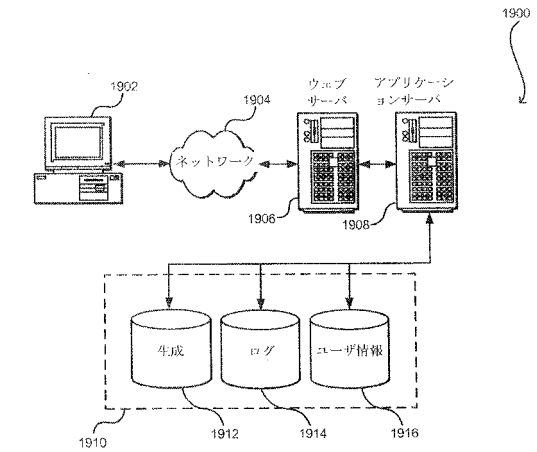
【図１７】


1700
鍵ＩＤについてのポリシーを更新するための要求を受信する
1702
認証要求を提出する
1704
認証応答を受信する
1706
真正要求か？
1708
はい
いいえ
要求を拒否する
1710
要求者に適用可能なポリシー情報にアクセスする
1712
ポリシーが更新を可能にするか？
1714
はい
いいえ
鍵ＩＤについてのポリシーを更新する
1716

【図１８】


1800
鍵ＩＤを有する鍵を使用して暗号動作（複数可）を実行するための要求を受信する
1802
真正要求か？
1804
はい
いいえ
要求を拒否する
1806
鍵ＩＤ及び／または要求者についてのポリシー情報にアクセスする
1808
ポリシーが動作（複数可）を可能にする
1810
いいえ
はい
暗号動作（複数可）を実行する
1812
暗号動作（複数可）の結果（複数可）を提供する
1814

【図１９】


1900
1902
1904
ネットワーク
ウェブサーバ
アプリケーションサーバ
1906
1908
生成
ログ
ユーザ情報
1910
1912
1914
1916

【手続補正書】
【提出日】令和1年11月18日(2019.11.18)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
データストレージサービスを提供するコンピュータ実行方法であって、
鍵の使用を制限する一組のパーミッションを定義するポリシーを格納することであって、前記鍵は、ハードウェアセキュリティモジュールを使用して暗号サービスによって保護された複数の鍵のうちの１つである、ことと、
前記鍵を識別する鍵識別子（ＩＤ）の第１のパラメータを含む第１のアプリケーションプログラミングインターフェースを介して提示される第１の要求を取得したことに応答して、前記暗号サービスに、前記ポリシーに従って、前記鍵を使用させ、データ暗号化鍵を高度暗号化標準（ＡＥＳ）暗号で暗号化して暗号化されたデータ暗号化鍵を作り出すことと、
前記鍵ＩＤの第２のパラメータと、前記暗号化されたデータ暗号化鍵に対応する暗号文を識別する第３のパラメータとを含む第２のアプリケーションプログラミングインターフェースを介して提示される第２の要求を取得したことに応答して、前記暗号サービスに、前記ポリシーに従って、前記鍵を使用させ、前記鍵が前記暗号サービスのみによって使用可能であるように前記暗号化されたデータ暗号化鍵をＡＥＳ復号で復号することと、
前記データストレージサービスによって格納された暗号化データを復号するために使用される前記データ暗号化鍵を提供することと
を備えるコンピュータ実行方法。
【請求項２】
前記暗号化データを復号することは、前記暗号サービスが前記暗号化データを暗号化または復号するための取得した要求の真正性を検証できるようにする有効な証明情報にさらに従う、請求項１のコンピュータ実行方法。
【請求項３】
前記ポリシーは、前記暗号サービスに前記鍵を使用して暗号化操作を実行させることが可能な許可されたリクエスタに対する制限を含む、請求項１のコンピュータ実行方法。
【請求項４】
前記鍵は、前記暗号サービスの信頼境界内で生成される、請求項１のコンピュータ実行方法。
【請求項５】
前記ポリシーは、要求の発信元のインターネットプロトコル（ＩＰ）または暗号化若しくは復号されるコンテンツの種類に少なくとも部分的に基づく１つまたは複数のパーミッションを規定する、請求項１のコンピュータ実行方法。
【請求項６】
コンピュータシステムであって、
１つまたは複数のプロセッサと、
前記１つまたは複数のプロセッサによって実行される結果として、前記コンピュータシステムに、少なくとも、
鍵の使用を制限する一組のパーミッションを定義するポリシーを格納し、前記鍵は、ハードウェアセキュリティモジュールを使用して暗号サービスによって保護された複数の鍵のうちの１つであり、前記複数の鍵は、前記暗号サービスとは異なるデータストレージサービスにアクセスできず、
前記鍵を識別する鍵ＩＤの第１のパラメータを含む第１のアプリケーションプログラ

ミングインターフェースを介して提示される第１の要求を取得したことに応答して、ＡＥＳ暗号を使用して、前記鍵でデータ暗号化鍵を暗号化して暗号化されたデータ暗号化鍵を作り出し、

前記鍵ＩＤの第２のパラメータと、前記暗号化されたデータ暗号化鍵に対応する暗号文を識別する第３のパラメータとを含む第２のアプリケーションプログラミングインターフェースを介して提示される第２の要求を取得したことに応答して、ＡＥＳ復号を使用して、前記鍵で前記暗号化されたデータ暗号化鍵を復号して、前記データストレージサービスによって前記データ暗号化鍵の使用を可能にする

暗号サービスを実行させる命令を格納するメモリと

を備えたコンピュータシステム。

【請求項７】

前記命令は、前記暗号サービスに、前記データストレージサービスから、要求の通知および証明を取得させる、請求項６のコンピュータシステム。

【請求項８】

前記コンピュータシステムは、コンピューティングリソースサービスプロバイダによって操作され、

前記複数の鍵のそれぞれの鍵は、前記コンピューティングリソースサービスプロバイダの異なる顧客に関連付けられる、請求項６のコンピュータシステム。

【請求項９】

前記暗号サービスは、前記データストレージサービスによって提示された保留中の要求が承認されることを前記ポリシーに対して検証するようにさらに構成される、請求項６のコンピュータシステム。

【請求項１０】

前記暗号サービスはさらに、

前記データ暗号化鍵を暗号化する要求の一部として追加データを取得し、

前記暗号化されたデータ暗号化鍵を復号する要求を前記追加データに提供する

請求項６のコンピュータシステム。

【請求項１１】

前記暗号サービスは、前記複数の鍵の少なくともサブセットのそれぞれに対して少なくとも１つまたは複数のポリシーを実施するようにさらに構成される、請求項６のコンピュータシステム。

【請求項１２】

前記コンピュータシステムは、コンピューティングリソースサービスプロバイダによって操作され、

前記複数の鍵のそれぞれの鍵は、前記コンピューティングリソースサービスプロバイダの顧客に対応し、

前記暗号サービスは、

前記コンピューティングリソースサービスプロバイダの顧客からポリシー更新を取得し、

前記取得したポリシー更新に従って前記ポリシーを更新する、

請求項１１のコンピュータシステム。

【請求項１３】

命令を格納するコンピュータ読み取り可能な記憶媒体であって、

前記命令は、コンピュータシステムの１つまたは複数のプロセッサによって実行されると、前記コンピュータシステムに、少なくとも、

鍵の使用を制限する一組のパーミッションを定義するポリシーを格納することであって、前記鍵は、ハードウェアセキュリティモジュールを使用して暗号サービスによって保護された複数の鍵のうちの１つであり、前記複数の鍵は、前記暗号サービスとは異なるデータストレージサービスにアクセスできない、ことと、

前記鍵を識別する鍵ＩＤの第１のパラメータを含む第１のアプリケーションプログラ

ミングインターフェースを介して提示される第１の要求を取得したことに応答して、ＡＥＳ暗号化を使用して、前記鍵でデータ暗号化鍵を暗号化して暗号化されたデータ暗号化鍵を作り出すことと、

前記鍵ＩＤの第２のパラメータと、前記暗号化されたデータ暗号化鍵に対応する暗号文を識別する第３のパラメータとを含む第２のアプリケーションプログラミングインターフェースを介して提示される第２の要求を取得したことに応答して、前記暗号サービスに、前記鍵を使用させ、ＡＥＳ復号を使用し、前記ポリシーに従って、前記暗号化されたデータ暗号化鍵を復号して前記データ暗号化鍵を回復することであって、前記データ暗号化鍵は、前記データストレージサービスによって格納された暗号化データを復号し、前記データ暗号化鍵は、暗号化形式で前記暗号化データとともに格納される、ことと、

前記データストレージサービスに格納された暗号化データを復号する要求を取得したことに応答して、前記データ暗号化鍵を使用して前記データストレージサービスによって格納された前記暗号化データを復号することと

を実行させる、コンピュータ読み取り可能な記憶媒体。

【請求項１４】

前記要求は、前記暗号サービスが、前記ポリシーに対して、前記暗号サービスを利用する前記要求が本物であることを検証できるようにする証明情報を含む、請求項１３のコンピュータ読み取り可能な記憶媒体。

【請求項１５】

前記データストレージサービスは、エンベロープ暗号で暗号化されたデータを格納し、

前記データストレージサービスは、前記データ暗号化鍵で暗号化されたデータを格納し、

前記データ暗号化鍵は、前記鍵で暗号化され、

前記データストレージサービスは、暗号化形式で前記データ暗号化鍵を格納する

請求項１３のコンピュータ読み取り可能な記憶媒体。

【請求項１６】

前記暗号化されたデータ暗号化鍵は、前記データストレージサービスによって前記暗号化データとともに格納される、請求項１５のコンピュータ読み取り可能な記憶媒体。

【請求項１７】

前記命令は、前記１つまたは複数のプロセッサによって実行されると、前記コンピュータシステムに、前記ポリシーを含む複数のポリシーをさらに実施させる、請求項１３のコンピュータ読み取り可能な記憶媒体。

【請求項１８】

前記命令は、前記１つまたは複数のプロセッサによって実行されると、前記コンピュータシステムに、前記コンピュータシステムに関連付けられた顧客装置から、前記ポリシーを更新する要求を取得させる、請求項１３のコンピュータ読み取り可能な記憶媒体。

【請求項１９】

前記ポリシーを更新する前記要求は、前記コンピュータシステムによって提供されるアプリケーションプログラミングインターフェースを介して取得される、請求項１８のコンピュータ読み取り可能な記憶媒体。

【請求項２０】

前記第１の要求は、第１の追加データを識別するパラメータを含み、

前記第２の要求は、第２の追加データを識別するパラメータを含み、

前記暗号化されたデータ暗号化鍵を復号することは、前記暗号サービスが前記第１の追加データが前記第２の追加データと一致することを検証することを条件とする、請求項１３のコンピュータ読み取り可能な記憶媒体。

フロントページの続き

(72)発明者　マシュー　ジェイムズ　レン
アメリカ合衆国　９８１０９－５２１０　ワシントン州　シアトル　テリー　アベニュー　ノース　４１０
(72)発明者　エリック　ジェイソン　ブランドワイン
アメリカ合衆国　９８１０９－５２１０　ワシントン州　シアトル　テリー　アベニュー　ノース　４１０
(72)発明者　ブライアン　アール　プラット
アメリカ合衆国　９８１０９－５２１０　ワシントン州　シアトル　テリー　アベニュー　ノース　４１０