(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2018-77893
(P2018-77893A)
(43)公開日　平成30年5月17日(2018.5.17)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/60	(2013.01)	G06F	21/60	320	5J104
H04L 9/32	(2006.01)	H04L	9/00	675A	

審査請求 未請求　請求項の数 1　OL　（全 58 頁）

(21)出願番号　特願2018-821 (P2018-821)
(22)出願日　平成30年1月5日 (2018.1.5)
(62)分割の表示　特願2015-558044 (P2015-558044)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　13/764,995
(32)優先日　平成25年2月12日 (2013.2.12)
(33)優先権主張国　米国(US)

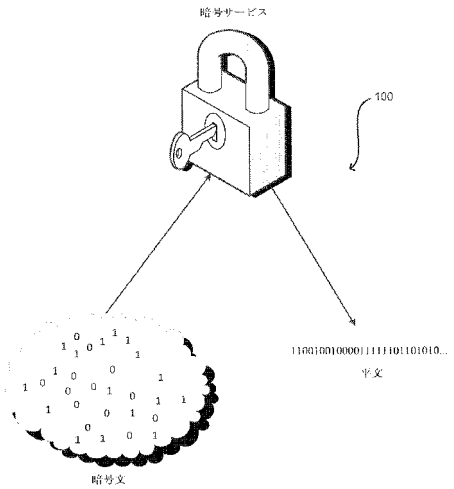
（特許庁注：以下のものは登録商標）
1．ＪＡＶＡＳＣＲＩＰＴ

(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】関連データを有するポリシー施行

(57)【要約】
【課題】分散コンピューティングリソースを伴う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】コンピュータシステムに提出される要求は、データセキュリティを確実にするためにポリシーの遵守を評価される。平文及び関連データは、暗号文を生成するために暗号への入力として使用される。暗号文を復号した結果を要求に応じて提供することができるかどうかは、それ自体が少なくとも部分的に関連データに基づくポリシーの評価に少なくとも部分的に基づいて決定される。他のポリシーは、キーを決定することを目的とする暗号攻撃を可能にするのに十分な操作でキーが使用されることを防ぐためのキーの自動ローテーションを含む。
【選択図】図１



【特許請求の範囲】
【請求項１】
ポリシーを施行するためのコンピュータ実装方法であって、
実行可能な命令で構成される１つ以上のコンピュータシステムの制御下で、
暗号文を復号するための要求を受信することであって、前記暗号文が少なくとも部分的に平文及びキーに基づいて生成されている、受信することと、
前記暗号文及び前記キーで検証可能なデータに少なくとも部分的に基づいて、要求に応じて、ポリシーが前記平文を提供することを許可するかどうかを決定することと、
前記ポリシーが前記平文を提供することを許可することを決定した結果、前記要求に応じて、少なくとも前記平文を提供することと、を含む前記方法。
【発明の詳細な説明】
【技術分野】
【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第１３／７６４，９９５号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に組み込まれる。本出願は、全ての目的上、本明細書と同時出願された表題「ＡＵＴＯＭＡＴＩＣ　ＫＥＹ　ＲＯＴＡＴＩＯＮ」の同時係属中の米国特許出願第１３／７６４，９４４号、本明細書と同時出願された表題「ＤＡＴＡ　ＳＥＣＵＲＩＴＹ　ＳＥＲＶＩＣＥ」の同時係属中の米国特許出願第１３／７６４，９６３号、本明細書と同時出願された表題「ＤＡＴＡ　ＳＥＣＵＲＩＴＹ　ＷＩＴＨ　Ａ　ＳＥＣＵＲＩＴＹ　ＭＯＤＵＬＥ」の同時係属中の米国特許出願第１３／７６５，０２０号、本明細書と同時出願された表題「ＦＥＤＥＲＡＴＥＤ　ＫＥＹ　ＭＡＮＡＧＥＭＥＮＴ」の同時係属中の米国特許出願第１３／７６５，２０９号、本明細書と同時出願された表題「ＤＥＬＡＹＥＤ　ＤＡＴＡ　ＡＣＣＥＳＳ」の同時係属中の米国特許出願第１３／７６５，２３９号、本明細書と同時出願された表題「ＤＡＴＡ　ＳＥＣＵＲＩＴＹ　ＳＥＲＶＩＣＥ」の同時係属中の米国特許出願第１３／７６５，２６５号、本明細書と同時出願された表題「ＳＥＣＵＲＥ　ＭＡＮＡＧＥＭＥＮＴ　ＯＦ　ＩＮＦＯＲＭＡＴＩＯＮ　ＵＳＩＮＧ　Ａ　ＳＥＣＵＲＩＴＹ　ＭＯＤＵＬＥ」の同時係属中の米国特許出願第１３／７６５，２８３号の全開示を、参照により組み込む。
【背景技術】
【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、多くの状況において重要性が高い。例として、組織は多くの場合、コンピューティングデバイスのネットワークを利用してユーザにサービスの頑強なセットを提供する。ネットワークは多くの場合、複数の地理的境界線にまたがり、多くの場合他のネットワークと繋がっている。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と他者によって管理されるコンピューティングリソースとの双方を使用してその業務を支援し得る。そのような組織のコンピュータは、例えば、別の組織のサービスを使用しながら、他の組織のコンピュータと通信してデータにアクセス及び／またはデータを提供し得る。多くの場合、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リモートネットワークを構成及び操作し、それによって、インフラストラクチャ費用を削減し、他の優位性を達成する。コンピューティングリソースのそのような構成では、自分たちが保有するリソース及びデータへのアクセスが安全であることを確実にすることは、特にそのような構成のサイズ及び複雑性が大きくなると困難になり得る。
【図面の簡単な説明】
【０００３】
本開示に従う様々な実施形態を、図面を参照して説明する。
【０００４】
【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例を示す。

【図３】本開示の様々な態様が実装され得る環境の例示的な例、及び少なくとも１つの実施形態に従う環境の様々な構成要素間の情報の流れの例を示す。
【図４】少なくとも１つの実施形態に従う、暗号文を記憶するための例示的プロセスのステップ例を示す。
【図５】本開示の様々な態様が実装され得る環境の例示的な例、及び少なくとも１つの実施形態に従う環境の様々な構成要素間の情報の流れの例を示す。
【図６】少なくとも１つの実施形態に従う、データを取得するための要求に応答するための例示的プロセスのステップ例を示す。
【図７】本開示の様々な態様が実装され得る環境の例示的な例、及び少なくとも１つの実施形態に従う環境の様々な構成要素間の情報の流れの例を示す。
【図８】少なくとも１つの実施形態に従う、データを記憶するための要求に応答するための例示的プロセスのステップ例を示す。
【図９】本開示の様々な態様が実装され得る環境の例示的な例、及び少なくとも１つの実施形態に従う環境の様々な構成要素間の情報の流れの例を示す。
【図１０】少なくとも１つの実施形態に従う、データを取得するための要求に応答するための例示的プロセスのステップ例を示す。
【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例を示す。
【図１２】本開示の様々な態様が実装され得る環境の例示的な例、及び少なくとも１つの実施形態に従う環境の様々な構成要素間の情報の流れの例を示す。
【図１３】少なくとも１つの実施形態に従う、データを取得するための要求に応答するための例示的プロセスのステップ例を示す。
【図１４】少なくとも１つの実施形態に従う、データを復号するための要求に応答するための例示的プロセスのステップ例を示す。
【図１５】少なくとも１つの実施形態に従う、復号されたデータを獲得するための例示的プロセスのステップ例を示す。
【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プロセスのステップ例を示す。
【図１８】少なくとも１つの実施形態に従う、ポリシーを施行しながら暗号操作を実行するための例示的プロセスのステップ例を示す。
【図１９】少なくとも１つの実施形態に従う、データを暗号化するためのプロセスの例示的な例を示す。
【図２０】少なくとも１つの実施形態に従う、セキュリティモジュールを使用してデータを暗号化するための例示的な例を示す。
【図２１】少なくとも１つの実施形態に従う、セキュリティモジュールを使用してデータの暗号化に使用されるキーを暗号化するための例示的な例を示す。
【図２２】少なくとも１つの実施形態に従う、関連データを使用してポリシーを施行するためのプロセスの例示的な例を示す。
【図２３】少なくとも１つの実施形態に従う、関連データ及びセキュリティモジュールを使用してポリシーを施行するためのプロセスの例示的な例を示す。
【図２４】少なくとも１つの実施形態に従う、ポリシーの状態図の例示的な例を示す。
【図２５】少なくとも１つの実施形態に従う、ポリシーの別の状態図の例示的な例を示す。
【図２６】少なくとも１つの実施形態に従う、自動ローテートキーのプロセスの例示的な例を示す。
【図２７】少なくとも１つの実施形態に従う、自動ローテートキーのプロセスの例示的な例を示す。
【図２８】少なくとも１つの実施形態に従う、キー使用を追跡するために使用され得るデータベースの表示の例示的な例を示す。
【図２９】様々な実施形態が実装され得る環境を例示する。

【発明を実施するための形態】
【０００５】
以下の説明において、様々な実施形態を説明する。説明の目的で、実施形態の完全な理解を提供するために特定の構成及び詳細を記載する。しかしながら、実施例が特定の詳細なしに実践され得ることも、当業者には明らかであろう。さらには、周知の特徴は、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略化され得る。
【０００６】
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伴う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。一例において、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。そのデータサービスは、様々な操作がデータと関連して実行されることを可能にし得る。１つの例示的な例として、分散コンピューティング環境は、１つ以上のデータ記憶サービスを含む。電子要求は、データ記憶操作を実行するためにデータ記憶サービスに送信され得る。操作例は、データ記憶サービスを使用してデータを記憶するため、及びデータ記憶サービスを使用してデータ記憶サービスによって記憶されたデータを取得するための操作である。データ記憶サービスをはじめとするデータサービスはまた、データを取り扱う操作も実行し得る。例えば、いくつかの実施形態において、データ記憶サービスは、データを暗号化することができる。
【０００７】
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、電子要求を受信し、かつそれに応答して、平文の暗号化及び暗号文の復号などの暗号操作を実行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において、暗号サービスはキーを管理する。暗号操作を実行するための要求に応じて、暗号サービスは、管理されるキーを使用する暗号操作を実行し得る。例えば、暗号サービスは、暗号操作を実行するために適切なキーを選択すること、暗号操作を実行すること、及び受信した要求に応じて暗号操作の１つ以上の結果を提供することができる。代替の構成において、暗号サービスは、エンベロープキー（例えば、特定のデータ項目を暗号化するために使用されるセッションキー）を生成し、該サービスの暗号操作を呼び出すシステムにエンベロープキーを返却することができる。該システムは、次いで、そのエンベロープキーを使用して暗号操作を実行することができる。
【０００８】
いくつかの実施形態において、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キーを管理する。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操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、遠隔で、及びプログラムによって、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構成及び操作し得る。顧客が暗号操作を実行するために暗号サービスに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キーを選択して、暗号操作を実行し得る。暗号サービスによって管理されるキーは、他のユーザ及び／またはデータサービスが、他者のキーへのアクセスを有しないように、安全に管理され得る。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キーへのアクセスの欠如は、エンティティが他者のキーを獲得する承認された方法を有しないこと、及び／またはエンティティが他者のキーを管理するシステムに、エンティティの指示でキーを使用させる承認された方法を有しないことを意味し得る。例えば、暗号サービスは、顧客のために、他の顧客が、その顧客のキー（複数可）へのアクセスを有すること、及び暗号サービスにその顧客のキー（複数可）を使用して暗号操作を実行させることの双方ができないように、キーを管理し得る。別の例として、暗号サービスは、データ記憶サービスなどの他のサービスが、暗号サービスにいくつかまたはすべてのキーを使用して暗号操作を実行させることができないように、キー

を管理し得る。キーへの不正アクセスは、例えば、不正アクセスが困難または不可能であるように、適切なセキュリティ対策によって防止され得る。困難さは、アクセスを獲得するための、計算実行不能に起因し、かつ／または不正（例えば、許可証明書の侵害など、違法、不法、及び／または別の様式で禁止された）が発生する必要性に起因し得る。様々な実施形態に従うシステムは、キーへのアクセスを獲得するための計算実行不能の客観的尺度を確実にするように構成され得る。そのような尺度は、例えば、規定単位の計算能力（例えば、単位時間当たりの特定の操作）を有するコンピュータが、キーへの承認されたアクセスに必要な暗号化された情報を解読するために平均して要するであろう時間量の観点から測定され得る。

【０００９】

述べたように、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など、様々なエンティティから要求を受信し得る。暗号サービスはまた、コンピューティングリソースプロバイダ内部のエンティティからも要求を受信し得る。例えば、いくつかの実施形態において、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操作を実行させるために、要求を暗号サービスに送信し得る。一例として、顧客は、データオブジェクトを記憶するために、要求をデータ記憶サービスに送信し得る。その要求は、データオブジェクトが記憶されるときに暗号化されるべきであることを示し得る。データ記憶サービスは、暗号操作を実行するために、要求を暗号サービスに通信する。暗号操作は、例えば、データオブジェクトを暗号化するためにデータ記憶サービスによって使用されるキーの暗号化であり得る。暗号操作は、データオブジェクト自体の暗号化であり得る。暗号操作は、データ記憶サービスがデータオブジェクトを暗号化するために使用できるエンベロープキーを生成することであり得る。

【００１０】

様々な実施形態に従うシステムは、強化されたデータセキュリティを提供するために様々なセキュリティ対策を実装する。例えば、様々な実施形態において、暗号サービスが、それが管理するキーを利用できる様態には限りがある。例えば、いくつかの実施形態において、暗号サービスは、適切な承認時に顧客に対応するキーのみを使用するために構成される。顧客のキーを使用するための要求が、顧客から（すなわち、顧客に代わって操作するコンピューティングデバイスから）生じると称される場合、暗号サービスは、該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（デジタル）署名されることを必要とするように構成され得る。顧客のキーを使用するための要求が別のデータサービスから生じた場合、暗号サービスは、該データサービスが、該データサービスへの署名済み要求が顧客によって為されたという証明を提供することを必要とするように構成される。いくつかの実施形態において、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機能するトークンを獲得及び提供するように構成される。他のセキュリティ対策もまた、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において、暗号サービスは、コンテクストに従ってキー使用を制限するように構成される。１つの例示的な例として、暗号サービスは、顧客から、または顧客の代理を果たすデータサービスからの要求に対して、暗号化のためのキー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（しかし別のデータサービスからではない）要求に対して、復号のためのキーのみを使用するように構成され得る。この様態において、データサービスが侵害された場合、データサービスは、暗号サービスにデータを復号させることができない。

【００１１】

様々なセキュリティ対策が、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対策は、いくつかの実施形態において、構成可能なポリシーに従って管理され得る。一例として、暗号サービスは、ユーザがキー上のポリシーを構成することを可能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。キー上のポリシーは、暗号サービスによって処理されるとき、キーが特定の状況で使用され得るかどうかについて決定力のある情報であり得る。ポリシーは、例えば、キ

ーの使用を指示できるユーザ及び／またはシステムのアイデンティティを制限し得、キーを使用することができる時間を制限し得、どのキーを使用して暗号操作を実行するかに関するデータを制限し得、かつ他の制限を提供し得る。ポリシーは、明示的制限（例えば、誰がキーを使用することができないのか）を提供し得、かつ／または明示的承認（例えば、誰がキー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、キーを使用できるとき、及び使用できないときの条件を一般的に提供するように複雑に構成され得る。キーを使用して暗号操作を実行するための要求が受信されるとき、ポリシーに従って要求が遂行されることができるかどうか決定するために、キー上のいかなるポリシーもアクセス及び処理され得る。

【００１２】

本開示の様々な実施形態は、キーと関連付けられるポリシーの施行に関し、該キーは暗号サービスによって管理され得る。暗号サービスをホストするコンピューティングリソースプロバイダの顧客など、暗号サービスのユーザは、暗号サービスによって施行されるキー上のポリシーを指定し得る。ポリシーは、キーを使用するために誰が暗号サービスを指示することができるか、キーを使用してどのような操作が実行され得るか、どのような状況でキーが使用され得るか、及び／または他のキー使用に関連した制約及び／または特権を符号化し得る。

【００１３】

ある実施形態において、暗号文と関連付けられるデータは、ポリシーの施行に使用される。暗号文と関連付けられるデータは、先進暗号化標準（ＡＥＳ）モードなど、暗号の使用によって獲得されるデータであり得る。例えば、暗号アルゴリズムへの入力は、暗号化される平文及び関連データを含み得る。暗号アルゴリズムは、平文を暗号化するためのキーを使用し得、かつ関連データが変更されているかどうかの決定を可能にするメッセージ認証コード（ＭＡＣ）などの、認証出力を提供し得る。認証出力は、少なくとも部分的に関連データ及び平文に基づいて決定され得る。

【００１４】

ポリシー施行は、少なくとも部分的に関連データに基づき得る。例えば、いくつかのポリシーは、復号された暗号文（すなわち、平文）が提供される前に、関連データが特定の値を有することを必要とし得る。認証出力（例えば、ＭＡＣ）は、関連データが変更されておらず、それ故にポリシーの施行が正しく実行されることを確実にするために使用され得る。関連データは、任意の好適なデータであり得、そのデータ自体は、ポリシーによって明示的または暗黙的に指定され得る。例えば、ポリシーは、暗号文を復号するための要求が、暗号文を暗号化するために使用される関連データ内に符号化されるユーザ識別子を有するユーザによって提出された場合のみ、復号された暗号文（平文）を提供することができるということを指定し得る。この様態において、別のユーザが暗号文の復号を要求した場合は（ユーザ識別子を有するユーザになりすますことなく）、ポリシーと相反するため、要求は遂行されない。別の例として、ポリシーは、暗号文が指定された情報にタグ付けされている場合のみ、復号された暗号文を提供することができると明言し得る。さらに別の例として、ポリシーは、平文のハッシュ、暗号文のハッシュ、または他の指定された値に等しい関連データにタグ付けされている場合のみ、復号された暗号文を提供することができると明言し得る。一般的に、本開示の実施形態は、暗号アルゴリズムの出力が明らかにされる前に、暗号アルゴリズムの入力または出力を中心とした豊富なポリシー施行を可能にする。いくつかの実施形態において、関連データはそれ自体がポリシーを表すことができる。

【００１５】

本開示の様々な実施形態はまた、キー使用を中心としたポリシーも可能にする。例えば、いくつかの実施形態において、キーを明らかにすることができる暗号攻撃の成功を可能にするのに十分な時間キーが使用されることを防止するために、キーは自動ローテートされる。起こり得るセキュリティ違反をもたらすのに十分な時間キーが使用されることを防止するため、暗号サービスまたはキーを利用する他のシステムは、キーを用いて実行され

る操作を追跡し得る。キー識別子（ＫｅｙＩＤ）によって識別されるキーが操作の閾値数において使用されるとき、そのキーはリタイアされ（例えば、将来の暗号化操作に使用不可能であるが、将来の復号操作には使用可能）、ＫｅｙＩＤによって識別される新しいキーと交換され得る。この様態において、新しいキーは適時に生成される。さらに、本開示の様々な実施形態は、特定のエンティティに対して透過的な様態でそのようなキーローテーションを実行する。一例として、コンピューティングリソースプロバイダの顧客または他のエンティティは、ＫｅｙＩＤによって識別されるキーを使用して操作を実行するために、暗号サービスに要求を提出し得る。暗号サービスは、キーローテーションを実行するためのエンティティからのいかなる要求からも独立して、キーローテーションを実行し得る。顧客または他のエンティティの観点から、要求は、リタイアされて新しいキーと交換されたキーに起因して必要な任意の再プログラミングまたは他の再構成なしに、ＫｅｙＩＤを使用して依然として提供され得る。

【００１６】

いくつかの実施形態において、暗号または他のサービスを支援する複数のシステムが、同時に、キーへのアクセスを有し、暗号操作を実行するための要求を遂行するために使用される。例えば、暗号サービスは、セキュリティモジュールのクラスタを利用し得、その少なくともいくつかは１つ以上のキーを冗長して記憶する。該サービスは、操作をセキュリティモジュールに割り当て、それ自身のカウンタを維持し得る。セキュリティモジュールがその割り当てを使用する（例えば、キーを使用して割り当てられた数の操作を実行する）とき、該サービスは、キーが依然として使用可能かどうか、またはキーをリタイアさせるべきかどうかをチェックし得る。セキュリティモジュール（または他のコンピュータシステム）は、暗号化、復号、電子署名生成等の、キーを使用した複数の種類の操作を実行するように構成され得ることに留意されたい。いくつかの実施形態において、すべての種類の操作が、セキュリティモジュールに操作の割り当ての一部を使用させるわけではない。例えば、復号操作は、割り当てられた操作が使用される結果をもたらさない場合がある一方、暗号化操作は、割り当てられた操作が使用される結果をもたらし得る。一般的に、様々な実施形態において、新たな情報（例えば、暗号文及び／または電子署名）の生成をもたらす暗号操作は、割り当てられた操作が使用される結果をもたらし得る一方、新たな情報の生成をもたらさない暗号操作は、割り当てられた操作が使用される結果をもたらさない場合がある。さらに、異なる種類の操作は、異なる数の暗号操作が実行される結果をもたらし得る。一例として、平文の暗号化は、少なくとも部分的に平文のサイズに基づいて、必要とされる暗号操作の量が変化し得る。例えば、ブロック暗号の使用によって、割り当てられた暗号操作は、生成される暗号文の各ブロックに使用され得る。

【００１７】

１つのキーに利用できる操作の合計数が依然として使用可能である場合、該サービスは、追加の操作をセキュリティモジュールに割り当て得る。キーをリタイアすべき場合（例えば、カウンタがそのように示しているため）、該サービスは、キーを冗長して記憶するセキュリティモジュールに、キーをリタイアさせ、かつそのキーを新しいキーと交換させ、ここでその新しいキーは生成され得るか、または１つのセキュリティモジュールによって別の様式で獲得されて残りのセキュリティモジュールへと安全に渡され得る。いくつかの実施形態において、他のセキュリティモジュールは、代わりに、古いキーの下、それらの割り当てられた操作を使い尽す。セキュリティモジュールが正常に機能しない場合、動作不能になった場合、意図的にオフラインとなった場合（例えば、保守のため）、かつ／あるいはそれが１つ以上のキーを使用して実行した操作の数に関する情報を提供せず、暗号操作の実行が別の様式で利用不可能になった場合、該サービスは、その非有用性をその割り当ての使用として処理し得る。例えば、セキュリティモジュールがキーのセット内の各キーに対して１００万の操作を割り当てられ、セキュリティモジュールが動作不能となる場合、該サービスは、セキュリティモジュールがキーのセット内の各キーに対して１００万の操作を実行したかのように、動作し得る。例えば、該サービスは、追加の操作をセキュリティモジュールまたは別のセキュリティモジュールに割り当て、それに従ってカウ

ンタを調整し得、かつ／または対応するカウンタが、交換が必要であることを示す場合、キーのうちの１つ以上をリタイア及び交換させ得る。

【００１８】

図１は、本開示の様々な実施形態を説明する例示的な図１００である。ある実施形態において、暗号サービスは、１つ以上の暗号アルゴリズムに従う１つ以上の計算のアプリケーションを含み得る暗号操作を実行する。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を可能にする。ある構成例において、暗号サービスを使用して、キーを暗号化する／復号することができ、これらのキーを使用して、データ記憶サービス内に記憶されるデータなどのデータを暗号化する／復号することができる。例えば、暗号サービスは、キーの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し得る。暗号サービスは、要求者が承認されたエンティティであると決定し、マスターキーを使用してキーを復号し、そこで復号されたキーをサービスに返し、それによって復号されたキーを使用して暗号文から平文を生成することができる。別の構成において、暗号サービスは、暗号文を受信して、受信した暗号文を処理して、暗号サービスによってサービスとして提供される平文にする。この例において、暗号文は、暗号サービスを操作す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承認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、データを暗号化するために、１つ以上の暗号法上強力なアルゴリズムを利用し得る。そのような暗号法上強力なアルゴリズムとしては、例えば、高度暗号化標準（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）（ＡＥＳ）、ブローフィッシュ（Ｂｌｏｗｆｉｓｈ）、データ暗号化標準（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）（ＤＥＳ）、トリプルＤＥＳ、Ｓｅｒｐｅｎｔ、またはトゥーフィッシュ（Ｔｗｏｆｉｓｈ）が挙げられ、選択される特定の実装によっては、非対称、または対称いずれかのキーシステムであり得る。一般的に、暗号サービスは、任意の暗号化及び／もしくは復号アルゴリズム（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したアルゴリズムの組み合わせを利用し得る。

【００１９】

以下により詳細に記載するように、暗号サービスを、様々な方法で実装することができる。ある実施形態において、暗号サービスは、以下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う暗号操作を実行するようにまとめて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。または別の言い方をすると、コンピュータシステムは分散システムであり得る。ある実施形態において、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の例において、暗号文は、暗号化された形態の平文である。平文は、任意の情報であり得、その名称は文字テキストを含まないが、平文及び暗号文は任意の好適な形態で符号化される情報であり得、必ずしもテキスト情報を含まないが、テキスト情報を含んでもよい。例えば、図１に例示されるように、平文及び暗号文は、ビットのシーケンスを含む。平文及び暗号文はまた、他の方法、及び一般的には、暗号化及び復号をコンピュータシステムによって実行することができる任意の様態でも表され得る。

【００２０】

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の例示的な例を示す。２００の環境において、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。この特定の例において、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記憶システムを含む。ある実施形態において、暗号サービスは、データサービスフロントエンドから平文を受信し、代わりに暗号文を提供すること、または該サービスがエンベロープキーを使用して暗号化操作を実行することができるように該サービスにエンベロープキーを提供することによってなど、暗号操作を実行するように環境２００内に構成される。暗号サービ

スは、平文を暗号文に変換すること及び暗号文を平文に復号することなどの暗号操作の実行のためのキーの安全な記憶など、以下に記載されるような追加の関数を実行し得る。暗号サービスはまた、そこに格納されるキーと関連のあるポリシーを施行することによるなど、ポリシー施行に関連付けられる操作を実行する。暗号サービスによって施行され得るポリシー例は、以下に提供される。ある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送信される要求を受信し、それ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記憶システム内に記憶された、または記憶されることとなるデータと関連して操作を実行するための要求であり得る。環境２００において、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記憶システムは、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ためにシステムを利用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、以下に記載されるものをはじめとする、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。

【００２１】

ある実施形態における認証サービスは、ユーザの認証に関与した操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得、代わりに、ユーザ要求が真正であるかどうかを示す情報を受信する。ユーザ要求が真正であるかどうかの決定は、任意の好適な様態で実行され得、及び認証が実行される様態は、様々な実施形態間において変化し得る。例えば、いくつかの実施形態において、ユーザはデータサービスフロントエンドに送信されるメッセージに電子署名をする。電子署名は、認証エンティティ（例えば、ユーザ）及び認証サービスの双方が利用可能な秘密情報（例えば、ユーザに関連付けられるキーペアのプライベートキー）を使用して生成され得る。要求及び要求のための署名は、秘密情報を使用して、受信した署名との比較のために参照署名を計算して、要求が真正かどうかを決定し得る認証サービスに提供され得る。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などの他のサービスに対して、要求が真正であるということを証明するために使用できる情報を提供し得、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ができるようにする。例えば、認証サービスは、別のサービスが要求の真正性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、様々な方法で制限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、特定の時間量において有効である。一例において、電子署名及び／またはトークンは、検証のために電子署名及び／またはトークンとともに含まれる、入力をタイムスタンプと見なす関数（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。提出される電子署名及び／またはトークンを検証するエンティティは、受信したタイムスタンプが十分に最新（例えば、現在時刻から規定の時間量以内）であることをチェックし、受信したタイムスタンプのために使用する参照署名／トークンを生成し得る。提出される電子署名／トークンを生成するために使用されるタイムスタンプが十分に最新ではない場合、及び／または提出される署名／トークンと参照署名／トークンとが一致しない場合、認証は失敗となり得る。この様態において、電子署名が侵害される場合、電子署名が短い時間量のみ有効であることから、侵害によって引き起こされる潜在的被害を制限する。真正性を検証する他の方法もまた、本開示の範囲内であると見なされることに留意されたい。

【００２２】

ある実施形態におけるデータサービスバックエンド記憶システムは、データサービスフロントエンドを介して受信される要求に従ってデータを記憶するコンピュータシステムである。以下でより詳細に議論されるように、データサービスバックエンド記憶システムは、暗号化形態でデータを記憶し得る。データサービスバックエンド記憶システム内のデータはまた、暗号化されていない形態でも記憶され得る。いくつかの実施形態において、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

クエンド記憶システム内に記憶されるデータが暗号化されるべきかどうかを指定することを可能にする。暗号化され、データサービスバックエンド記憶システム内に記憶されるデータは、様々な実施形態に従う様々な方法で暗号化され得る。例えば、様々な実施形態において、データは、暗号サービスにアクセス可能だが、環境２００のいくつかまたはすべてのシステムにはアクセス不可能なキー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記憶システム内での記憶のために暗号サービスによって符号化され得、及び／または、いくつかの実施形態において、データは、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などの別のシステムによって、暗号サービスによって復号されたキーを使用して暗号化され得る。環境２００がデータを暗号化するために操作し得る様々な方法の例は以下に提供される。

【００２３】

環境２００の多数の変形（及び本明細書に記載される他の環境）は、本開示の範囲内であると見なされる。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記憶し得る追加のデータ記憶サービス（各々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、１つのデータ記憶サービスは、データ記憶サービスが同期様態でデータ記憶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、データを取得するための要求は、取得されるデータとともに同期応答を受信し得る）。別のデータ記憶サービスは、アーカイブデータ記憶サービスを提供し得る。そのようなアーカイブデータ記憶サービスは、非同期要求処理を利用し得る。例えば、データを取得するための要求は、取得されるデータを含む同期応答を受信しない場合がある。むしろ、アーカイブデータ記憶サービスは、取得されるデータを提供する準備が整うと、取得されるデータを獲得するために提出される第２の要求を必要とし得る。別の例として、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、その情報を使用して課金記録を作成する計量サービスを含み得る。課金記録は、暗号サービス（及び／または他のサービス）の使用に対して顧客に支払いを請求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、どれくらいの料金が課されるべきかの指針を提供し得る。例えば、いくつかの例において、顧客は、暗号サービスの使用に対する請求書を提供され得る。他の例において、暗号サービスの使用に対する料金は、その操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など、他のサービスの使用料金に合わせられ得る。使用は、操作ごと、一定期間ごと、及び／または他の方法など、様々な方法で、計量及び請求され得る。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）に含まれ得る。

【００２４】

加えて、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く。ユーザは、図中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）を介してデータサービスフロントエンドと対話し得ることを理解されたい。さらに、図２（及び図中の他の部分）に描かれるユーザはまた、人間以外のエンティティも表し得る。例えば、コンピュータシステム上で実行する自動処理は、本明細書に記載されるようにデータサービスフロントエンドと対話し得る。１つの例示的な例として、図２中でユーザによって表されるエンティティは、その操作の一部として、データサービスフロントエンドを使用して、データをデータサービスバックエンド記憶システムに記憶する、及び／またはデータサービスバックエンド記憶システムから取得するサーバであり得る。さらに別の例として、図２中でユーザによって表されるエンティティは、図２中のサービスのうちの１つ以上を操作す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中のユーザは、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。以下に記載される他の環境の変形を含め、他の変形もまた、本開示の範囲内であると見なされる。

【００２５】

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記憶システムを含む。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記憶システムは、図２と関連して上記のように構成され得る。例えば、ユーザは、好適なコミュニケーション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、そのようなネットワークは図中には例示されていない。図３に例示される環境３００の例では、情報の流れを表す矢印が提供される。この例において、ユーザはＰＵＴ要求をデータサービスフロントエンドに送信する。ＰＵＴ要求は、指定されたデータをデータサービスバックエンド記憶システム内に記憶するための要求であり得る。ＰＵＴ要求に応じて、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、つまりユーザが要求された操作をシステムによって実装される認証ポリシーに従って実行することができる様態で要求を提出したかどうか、を決定し得る。

【００２６】

図３において、そのような認証決定がどのように行われ得るかの例示的な例が例示される。この特定の例において、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決定し得る。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、電子トークン、または暗号サービスなどの別のサービスが真正な要求が受信されたことを独立して決定するために使用可能な他の情報であり得る。１つの例示的な例において、ＰＵＴ要求は、ＰＵＴ要求のための署名とともに送信される。ＰＵＴ要求及びその署名は、真正である場合の署名はどうあるべきかを独立して計算する認証サービスを介して提供される。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その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決定し得、かつそれに応じて認証証明を提供し得る。ＰＵＴ要求が真正であるかどうかの決定はまた、ポリシーの施行に関連する１つ以上の操作も含む。例えば、署名は有効であるが別途ポリシーがＰＵＴ要求を完了すべきではないと示す（例えば、要求がポリシーによって禁止される時間中に提出された）場合、認証サービスは、要求が真正ではないことを示す情報を提供し得る。（しかしながら、そのようなポリシー施行は、環境３００の他の構成要素によって実行され得ることに留意されたい。）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キーを使用することなどによって、署名を生成し得る。認証証明は、述べたように、暗号サービスなどの別のサービスが、要求が真正であることを独立して検証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例を使用すると、認証証明は、他のサービスにアクセス不可能なキーなど、認証サービス及び暗号サービスの双方によって共有されるキーに少なくとも部分的に基づいて生成され得る。

【００２７】

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、認証サービスから認証証明を受信すると、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、ＡＰＩコールまたは他の電子要求に従って暗号サービスに提供される（例えば、Ｅｎｃｒｙｐｔ　ＡＰＩコール）。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決定し得る。

【００２８】

追加情報が暗号サービスに提供され得ることに留意されたい。例えば、平文を暗号化するために使用されるキーの識別子は、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コールへ提供され得る（代わりに、ユーザから識別子を受信している場合がある）。しかしながら、識別子は暗号サービスに送信されない場合があることに留意されたい。例えば、様々な実施形態において、平文を暗号化するためにどのキーを使用するか別途決定可能であり得る。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へ送信される情報は、代理としてユーザがＰＵＴ要求を提出した顧客の識別子などの、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など、ユーザに関連付けられる情報を含み得る。そのような情報は、使用されるデフォルトキーを決定するために暗号サービスによって使用され得る。言い換えると、そのキーは、キーを決定するために使用可能な情報によって暗黙的に指定され得る。一般的に、使用されるキーの決定は、任意の好適な様態で実行され得る。さらに、いくつかの実施形態において、暗号サービスはキーを生成または選択し得、かつ後に使用される生成または選択されたキーの識別子を提供し得る。ＡＰＩパラメータの別の例は、暗号化操作が実行される顧客アカウント用マスターキーのための識別子であり得る。

【００２９】

図３に例示されるように、認証証明が、平文が暗号化されるのに暗号サービスにとって十分である場合、暗号サービスは１つ以上の暗号操作を実行することができる。ある実施形態において、１つ以上の暗号操作は、平文を暗号化するために使用されるエンベロープキーを生成するための操作を含むことができる。エンベロープキーは、ランダムに生成される対称キー、またはキーペアのプライベートキーであり得る。エンベロープキーが生成された後、暗号サービスは、ＡＰＩコール内で指定されるマスターキーを用いてエンベロープキーを暗号化することができ、その暗号化されたエンベロープキーを永続的に記憶する（例えば、記憶サービスまたはいくつかの他の持続性ストレージ内に暗号化されたキーを記憶することによって）、または破棄することができる。加えて、暗号サービスは、エンベロープキーの平文バージョンならびに暗号化されたエンベロープキーをデータサービスフロントエンドに送ることができる。データサービスは次いで、エンベロープキーの平文バージョンを使用して平文（すなわち、暗号化要求と関連付けられるデータ）を暗号化することができ、エンベロープキーを、エンベロープキーを暗号化するために使用されるマスターキーのための識別子と関連して永続ストレージ内に記憶させることができる。加えて、データサービスはエンベロープキーの平文バージョンを破棄することができる。そのため、ある実施形態において、データサービスは、エンベロープキーの平文バージョンを破棄した後は、もはや暗号文を復号することができなくなる。

【００３０】

代替の実施形態において、暗号操作は平文を暗号化することに関与できる。例えば、暗号サービスは平文を暗号化し、暗号文をデータサービスフロントエンド記憶システムに提供する。データサービスフロントエンドは次いで、その操作に従ってその暗号文を永続記憶のためにデータサービスバックエンド記憶システムに提供し得る。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記憶システムへ送信され得る。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キーの識別子が、記憶のため暗号文とともにデータサービスバックエンド記憶システムによって提供され得る。ユーザ及び／またはユーザの組織を識別するメタデータなど、他の情報もまた提供され得る。

【００３１】

本明細書に記載されるすべての環境と同様に、多くの変形が本開示の範囲内であると見なされる。例えば、環境３００の様々な構成要素間の情報の流れは、示されるものと異なる場合がある。例えば、中間構成要素を介した１つの構成要素から別の構成要素への情報の流れ（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記憶システムへのデータ）は、その送信先に直接的に、及び／または環境３００の他の中間構成要素（図中に含まれるとは限らない）を介して提供され得る。別の例として、ＰＵＴ要求（及び、以下、ＧＥＴ要求）が、例示の目的のために提供される。しかしながら、記載される操作を実行するための任意の好適な要求が使用され得る。

【００３２】

図４は、ある実施形態に従ってデータ記憶サービス内にデータを記憶するために使用され得るプロセス４００の例示的な例を示す。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の一部またはす

べて（あるいは、本明細書に記載される任意の他のプロセス、またはそれらの変形及び／もしくは組み合わせ）は、実行可能な命令で構成される１つ以上のコンピュータシステムの制御下で実行され得、及び１つ以上のプロセッサ上で、ハードウェアによって、またはその組み合わせによって、まとめて実行するコード（例えば、実行可能な命令、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、コンピュータ可読記憶媒体上に、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態で記憶され得る。コンピュータ可読記憶媒体は、非一時的であり得る。

【００３３】

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、かつＰＵＴ要求の電子署名などの、認証に必要とされる情報など、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じて、プロセス４００は、認証要求を提出すること４０４を含み得る。例えば、プロセス４００内で実行されるシステムは、（例えば、適切に構成されたＡＰＩコールを介して）認証要求を、図３と関連して上に記載されるような別個の認証サービスに提出し得る。同様に、独自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。一般的に、認証要求は、様々な実施形態に従う任意の好適な様態で提出され得る。

【００３４】

認証要求が提出されると、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される４０６。例えば、図３を参照すると、認証サービスは、応答を他のサービスによる使用のための認証の証明を含むデータサービスフロントエンドに提供し得る。認証が成功したかどうかを示すものなど、他の情報もまた送信され得る。要求が真正であるかどうかの決定がなされ得る４０８。要求の真正性は、認証サービスなどのエンティティ、またはそのようなチェックをまとめて実行するエンティティの組み合わせなどによってチェックされる１つ以上の要因に従属し得る。真正性は、例えば、要求が必須の有効な証明書（例えば、チェックするエンティティによって共有される秘密キー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許可することを必要とし得る。認証要求を提出し４０４、認証応答を受信するシステムの観点から、真正性は受信した認証応答に従属し得る。したがって、ある実施形態において、要求が真正であるかどうかの決定４０８は、受信した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、それに従って決定４０８がなされ得る。同様に、応答は、要求が真正でなかった場合に含まれる情報を含まないことなどによって、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決定される４０８場合、ＰＵＴ要求は拒否４１０され得る。ＰＵＴ要求の拒否は、任意の好適な様態で実行され得、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、ＰＵＴ要求を拒否すること４１０は、ＰＵＴ要求を提出したユーザにメッセージを送信することを含み得る。そのメッセージは、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また、電子署名が正しくない、またはＰＵＴ要求が真正でない、もしくは承認されていないという結果となった任意の問題の解決方法を決定するために使用され得る他の理由など、要求が拒否された理由についての情報を提供することも含み得る。

【００３５】

ＰＵＴ要求が真正であり、かつ承認されていると決定される場合４０８、ある実施形態において、プロセス４００は、平文の暗号化という結果をもたらす１つ以上の暗号操作を実行すること４１２を含む。例えば、要求（例えば、適切に構成されたＡＰＩコール）が、暗号サービスに提出され、１つ以上の暗号操作を実行するために使用されるキーが提供される。暗号サービスに提供される要求は、ＰＵＴ要求が真正であるという証明とともに提供され得るため、暗号サービスは、暗号操作（例えば、平文を暗号化して暗号文を提供すること、または平文を暗号化するために使用することができるエンベロープキーを生成

すること）を実行するかどうか独立して決定することができる。しかしながら、様々な実施形態において、認証証明が暗号サービスに提供されない場合があり、例えば、暗号サービスは、それが受信する要求に従って操作してもよい。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すでに独立してその要求の認証を検証したという事実に頼り得る。そのような実施形態及び他の実施形態において、データサービスフロントエンドは、セキュリティの追加の層を提供するために、暗号サービスを用いて自身を認証し得る。暗号サービスは、キーを生成し、または別の様式で獲得し、獲得したキーを暗号化し、または別途暗号化されたキーを獲得し（例えば、メモリから）、要求に応じて、獲得したキー及び暗号化された獲得したキーを提供し得る。獲得したキーは、暗号サービスへの要求において識別されるキーを使用して暗号化され得る。獲得したキーを使用して平文を暗号化し得、平文を暗号化した後、獲得したキーは破棄され得る（例えば、取消不能の形でメモリから削除される）。代替の実施形態において、プロセス４００を実行するシステムは、１つ以上の暗号操作を実行するために使用されるキーを生成あるいは別の様式で獲得し得、獲得したキーを暗号化のために暗号サービスに提供し得る。

【００３６】

いくつかの実施形態において、１つ以上の暗号操作を実行することは、暗号文が生成されるという結果をもたらし得る。１つ以上の暗号操作の結果として生成される暗号文は、その後に起こり得る取得のために記憶され得る４１４。上に述べたように、暗号文の記憶は、その後の暗号文の復号を可能にする追加情報の記憶を含み得る。例えば、暗号文は、平文を暗号文に暗号化するために使用されるキーの識別子とともに記憶され得るため、識別子を有するキーは、暗号文を復号して平文を獲得するために後に使用され得る。暗号文の記憶もまた、任意の好適の様態で実行され得る。例えば、暗号文の記憶は、上記のように、データサービスバックエンド記憶システムによって実行され得る。

【００３７】

図５は、したがって、環境５００の例示的な例、及び平文がどのように獲得され得るかを例示する情報の流れを示す。この例における環境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記憶システムを含む。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記憶システムは、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要求を受信して、代わりに平文を提供するように構成される。これをするためには、データサービスフロントエンドはまた、認証要求を認証サービスに提出するようにも構成され得、認証サービス自体が、適切な場合、データサービスフロントエンドに認証証明を提供するように構成され得る。データサービスフロントエンドはまた、暗号サービスに要求を送り、暗号サービスにデータの復号に関する１つ以上の暗号操作の実行をさせるようにも構成され得る。エンベロープキーが使用される実施形態において、データサービスは、要求（例えば、ＡＰＩコール）を、暗号化されたエンベロープキー（または暗号化されたエンベロープキーのための識別子）認証証明、及び暗号サービスに対するエンベロープキーを暗号化するために使用されるマスターキーの識別子を含むまたは指定する暗号サービスに提出することができる。暗号サービスは、認証証明が操作を許可するのに十分であるかどうかを決定することができ、認証証明が十分であれば、エンベロープキーを復号する。復号されたエンベロープキーをデータサービスに送り返すことができ、データサービスはそのキーを使用して暗号化された平文を復号することができる。データサービスは次いで、復号された平文キーを破棄することができる。

【００３８】

代替の実施形態において、データサービスフロントエンドは、受信した認証証明を暗号サービスが復号する暗号文とともに暗号サービスに提供するように構成され得る。暗号サービスは、それに応じて、認証証明が暗号文の復号を許可するのに十分であるかどうかを決定し、認証証明が十分であれば、適切なキー（データサービスフロントエンドによって

暗号サービスに対して識別され得る）を使用して暗号文を復号し、復号された暗号文（平文）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得る。暗号サービスに暗号文を提供するため、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記憶システムから暗号文を獲得する（例えば、適切に構成されたＡＰＩコールを介して）ように構成され得る。

【００３９】

図６は、様々な実施形態に従って平文を獲得するために使用され得るプロセス６００の例示的な例を示す。プロセス６００は、例えば、図５と関連して上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得る。ある実施形態において、プロセス６００は、ＧＥＴ要求（または他の適切な要求）をユーザから受信すること６０２を含む。ＧＥＴ要求の受信は、他の種類の要求と関連して上に記載されるように実行され得る。ＧＥＴ要求の受信６０２の際、認証要求が認証サービスに、または上記のように任意の様態で提出され得る６０４。認証応答が、それに応じて受信され得る。受信し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の決定がなされ得る６０８。ＧＥＴ要求が真正でないと決定される場合６０８、プロセス６００は、上記のように、様々な実施形態に従って様々な様態で実行され得る要求を拒否すること６１０を含み得る。

【００４０】

ＧＥＴ要求が真正であると決定６０８される場合、プロセス６００は記憶から暗号文を取得することを含み得る。記憶から暗号文を取得すること６１２は、任意の好適な様態で実行され得る。例えば、図５と関連して上に記載される環境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記憶システムに提出し得、それに応じて暗号文を受信し得る。一般的に、暗号文は、任意の好適な様態で記憶から獲得され得る。暗号文の受信の際、プロセス６００は、暗号文の復号に関連した１つ以上の操作を実行すること６１４を含み得る。例えば、ある実施形態において、データ記憶サービスは、暗号文の復号に関連した１つ以上の暗号操作を実行する６１４ために要求を暗号サービスに送り得る。１つの構成例において、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キー（または、暗号化されたエンベロープキーの識別子）認証証明、及び暗号サービスに対するエンベロープキーを暗号化するために使用されるマスターキーの識別子を含むＡＰＩコールを送ることができる。暗号サービスは、認証証明が操作を許可するのに十分であるかどうかを決定することができ、認証証明が十分であれば、エンベロープキーを復号する。復号されたエンベロープキーをデータサービスに送り返すことができ、データサービスはそのキーを使用して暗号化された平文を復号することができる。

【００４１】

別の構成において、暗号文は、図５と関連して上に記載される暗号サービスなどの暗号サービスに提供され得る。暗号文を復号するかどうかを決定するために暗号サービスが使用することができる認証の証明など、他の情報もまた、暗号サービスに提供され得る。加えて、いくつかの実施形態において、暗号文を復号するために暗号サービスによって使用されるキーの識別子が、暗号サービスに提供され得る。しかしながら、他の実施形態において、そのキー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、暗号サービスに対して示される顧客と関連付けられるデフォルトキーを使用し得る。一般的に、暗号サービスが暗号文を復号するためにどのキーを使用するか決定することができる任意の様態が使用され得る。

【００４２】

図６に例示されるように、暗号文が復号された後、プロセス６００は、ＧＥＴ要求に応答を提供すること６１６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って様々な様態で実行され得る。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。他の実施形態において、平文は、後にＧＥＴ要求に応じて

提供される他の暗号化された情報を復号するために使用されるキーであり得る。一般的に、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。

【００４３】

述べたように、本開示の様々な実施形態は、データが様々な方法でデータ記憶サービスによって記憶されることを可能にする。図７は、そのような実施形態に従う情報の流れを示す矢印とともに環境７００の例示的な例を示す。図７に例示されるように、環境７００は、上記のように、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記憶システムを含む。この特定の例において、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記憶システムによって記憶されるデータオブジェクトを含み得る、または指定し得る。ＰＵＴ要求はまた、データオブジェクトを暗号化するために使用されるキーのためのキー識別子を指定し得る。データサービスフロントエンドはまた、上記のように、認証証明をキー及びキー識別子を受信するために操作可能な暗号サービスに提供し、それに応じてキー識別子によって識別されるキーによって暗号化されるキーを提供するために、認証サービスと対話するようにも構成され得る。データサービスフロントエンドは次いで、データサービスバックエンド記憶システム内の記憶をもたらし得る。記憶され得るデータは、キーによって暗号化されるデータオブジェクトを含み得る。記憶され得るデータはまた、キー識別子によって識別されるキーによって暗号化されるキーも含み得る。本明細書内の他の部分で議論したように、暗号化されたデータオブジェクト及び暗号化されたキーは、異なるサービス内に記憶され得る。

【００４４】

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記憶のためにデータサービスバックエンド記憶システムに提供するように構成される。この例において、データサービスフロントエンドは、キーの下で暗号化されるデータオブジェクト、及びＫｅｙＩＤを有する別のキーの下で暗号化されるキーを提供するように構成される。例示の目的のため、暗号化を表すために中括弧表記が使用されることに留意されたい。具体的には、中括弧内の情報は、下付き文字で指定されるキーの下で暗号化される情報である。例えば、｛Ｄａｔａ　Ｏｂｊｅｃｔ｝$_{Key}$は、データ「Ｄａｔａ　Ｏｂｊｅｃｔ」が「Ｋｅｙ」というキーの下で暗号化されることを表す。キー識別子もまた、この中括弧表記を使用して下付き文字で現れ得る。キー識別子が下付き文字で現れるとき、中括弧内の情報は、そのキー識別子によって識別されるキーの下で暗号化される。例えば、｛Ｄａｔａ　Ｏｂｊｅｃｔ｝$_{KeyID}$は、データオブジェクト「Ｄａｔａ　Ｏｂｊｅｃｔ」が、キー識別子「ＫｅｙＩＤ」によって識別されるキーの下で暗号化されることを表す。同様に、｛Ｋｅｙ｝$_{KeyID}$は、キー「Ｋｅｙ」が識別子「ＫｅｙＩＤ」によって識別されるキーの下で暗号化されることを表す。言い換えると、本開示は、キー及びキー識別子の双方を下付き文字で使用し、下付き文字の意味は文脈から明白であるべきである。暗号文は、関連した復号キーのアイデンティティを決定するために使用可能な追加のメタデータを含み得る。

【００４５】

図８は、図７と関連して上に記載されるデータサービスバックエンド記憶システムなどのデータ記憶システム内にデータオブジェクトを記憶するために実行され得るプロセス８００の例示的な例を示す。プロセス８００は、図７と関連して上に記載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など、任意の好適なシステムによって実行され得る。ある実施形態において、プロセス８００は、データオブジェクトのＰＵＴ要求を受信すること８０２を含む。データオブジェクトのＰＵＴ要求を受信することは、上記のように、任意の好適な様態で実行され得る。データオブジェクトを要求と関連して受信することができること、または別のサービスから受信し得ることに留意されたい。例えば、要求は、識別子を使用して別のサービスから獲得され得るデータオブジェクトのための識別子を

含み得る。上記の他のプロセスと同様、ある実施形態におけるプロセス８００は、認証要求を提出すること８０４、及び認証応答を受信すること８０６を含む。受信された認証応答８０６は、ＰＵＴ要求が真正な要求であるかどうかを決定する８０８ために使用され得る。ＰＵＴ要求が真正でないと決定される場合８０８、プロセス８００は、上記のように要求を拒否すること８１０を含み得る。ＰＵＴ要求が真正であると決定される場合８０８、プロセス８００は、エンベロープキーを暗号化するために使用されるマスターキーのためのｋｅｙＩＤなどのキー識別子（ＫｅｙＩＤ）を獲得すること８１２を含み得る。ＫｅｙＩＤを獲得すること８１２は、任意の好適な様態で実行され得、ＫｅｙＩＤが獲得される様態は、様々な実施形態に従って異なり得る。例えば、図７に例示されるように、ＰＵＴ要求は、ＫｅｙＩＤを指定し得る。別の例として、ユーザのアイデンティティ、または別の様式でユーザと関連付けられるアイデンティティが、識別子またはデフォルトキーを獲得するために使用され得る。別の例として、暗号文は関連したキーＩＤを示すものを提供し得る。さらに別の例として、１つ以上のポリシー決定は、どのキー識別子を獲得するか決定するために使用され得る。

【００４６】

ある実施形態において、プロセス８００はまた、エンベロープキーなどのキーを生成すること８１４も含む。キーの生成は、任意の好適な様態で、例えば、暗号サービスまたは暗号サービスから暗号化操作を要求するサービス（例えば、データ記憶サービス）によって実行され得る。例えば、キーは、キー導出関数への適切な入力を使用したキー導出関数を使用して生成され得る。キー導出関数の例は、ＩＥＥＥ Ｓｔｄ １３６３ ２０００で定義されるＫＤＦ１、ＡＮＳＩ Ｘ９．４２で定義されるキー導出関数、及びＲＦＣ ５８６９で指定されるＨＭＡＣ－Ｂａｓｅｄ Ｅｘｔｒａｃｔ－ａｎｄ－Ｅｘｐａｎｄ Ｋｅｙ Ｄｅｒｉｖａｔｉｏｎ Ｆｕｎｃｔｉｏｎ（ＨＫＤＦ）などのＨＭＡＣベースのキー導出関数を含む。別の例として、キーは、乱数もしくは擬似乱数発生器、ハードウェアエントロピーソース、またはＮａｔｉｏｎａｌ Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｓｔａｎｄａｒｄｓ ａｎｄ Ｔｅｃｈｎｏｌｏｇｙ Ｓｐｅｃｉａｌ Ｐｕｂｌｉｃａｔｉｏｎ（ＮＩＳＴ ＳＰ） ８００－９０Ａによって指定されるような確定論的ランダムビット生成器によって生成され得る。図８は、キーを生成すること８１４を含むプロセス８００を示す一方、キーは、記憶からの取得によるなど他の方法で獲得され得ることに留意されたい。言い換えると、キーは予め生成されていてもよい。

【００４７】

図８に例示されるプロセス８００を続けると、ある実施形態において、プロセス８００は、データオブジェクトを暗号化するために生成されたキーを使用すること８１６を含む。例えば、暗号サービスがキーを生成する実施形態において、暗号サービスは、キー、ＫｅｙＩＤ、及びキーの暗号化されたコピーをデータサービスに提供することができる。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、エンベロープキー、及び暗号サービスからのエンベロープキーを暗号化するために使用されるマスターキーのためのＫｅｙＩＤを、認証証明などの任意の他の関連情報とともに受信し得る。暗号化キーの平文コピーは次いで、データオブジェクトを暗号化するために使用され得る。暗号化キーの平文コピーを破棄することができ、暗号化されたデータオブジェクトならびに暗号化されたキーは次いで、記憶され得る８１８。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オブジェクト及び暗号化されたキーを、記憶のためにデータサービスバックエンド記憶システムに送信し得る。該サービスがキーを生成する構成において、該サービスは、キー及びＫｅｙＩＤを暗号サービスに提供することができる。例えば、データサービスフロントエンドは、エンベロープキー及びエンベロープキーを暗号化するために使用されるマスターキーのためのＫｅｙＩＤを、認証証明などの任意の関連情報とともに暗号サービスに送り得る。暗号化キーの平文コピーは次いで、データオブジェクトを暗号化するために使用され得る。サービスは、暗号化キーの平文コピーを破棄することができ、暗号化されたデータオブジェクトならびに暗号化されたキーは次いで、記憶され得る。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

されたデータオブジェクト及び暗号化されたキーを、記憶のためにデータサービスバックエンド記憶システムに送信し得る。

【００４８】

暗号化されたデータオブジェクト及び暗号化されたエンベロープキーは、キーの平文バージョンなしで記憶され得、すなわち、平文キーは、データサービスバックエンド記憶システム及び１つ以上の他のシステムへのアクセスが不可能な場合がある。その下でデータオブジェクトが暗号化されるキー（例えば、マスターキー）は、任意の好適な様態でアクセス不可能にされ得る。いくつかの実施形態において、これは、暗号サービスのみがアクセス可能なメモリにそれを記憶することによって達成される。いくつかの他の実施形態において、これは、ハードウェアまたは他のセキュリティモジュール内に、または別の様式でハードウェアまたは他のセキュリティモジュールの保護下で、マスターキーを記憶することによって達成することができる。いくつかの実施形態において、平文エンベロープキーを記憶するメモリ位置（例えば、データサービスのメモリ）は、上書きされることを許可され得るか、キーを記憶するメモリ位置は、データサービスフロントエンドにはキーへのアクセスを不可能にするために意図的に上書きされ得る。別の例として、平文エンベロープキーは、最終的にはキーを記憶することをやめる揮発性メモリ内に維持され得る。この様態において、エンベロープキーは、ＫｅｙＩＤによって識別されるキーを使用して復号される場合、または別の様式で、ＫｅｙＩＤによって識別されるキーなしでキーを解読することによってなど、計算的に実行不可能であり得る、不正な様態で獲得される場合にのみアクセス可能である。言い換えると、データオブジェクトが暗号化されるキーへの承認されたアクセスのためには、ＫｅｙＩＤによって識別されるキーが必要とされる。このように、データオブジェクトを復号することは、キーへのアクセスを必要とし、そのキーはＫｅｙＩＤによって識別されるキーを使用した復号によって、または計算的に実現可能ではない他の方法によってのみ獲得可能であるため、図７のデータサービスバックエンド記憶システムが侵害される場合、そのような侵害は、暗号化されていないデータオブジェクトへのアクセスを提供しない。

【００４９】

述べられたように、本開示の様々な実施形態は、ユーザが、データオブジェクトを記憶すること、及びそれらを安全な様態で取得することの双方を可能にする。図９は、したがって、記憶からデータオブジェクトを獲得するために使用され得る環境９００の例示的な例を示す。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記憶システムを含む。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記憶システムは、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、データオブジェクト要求を受信し、それに応じてデータオブジェクトを提供するように構成される。呼応してデータオブジェクトを提供するために、この実施形態におけるデータ記憶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記憶システムと対話するように構成される。例えば、様々な実施形態において、データサービスフロントエンドシステムは、認証サービスに認証要求を提出し、その要求に応じて認証証明を受信するように構成される。別の例として、データサービスフロントエンドは、ＫｅｙＩＤによって識別されるキーによって暗号化されるキー及び認証証明を暗号サービスに提供するように構成され、暗号サービスは、少なくとも部分的に認証証明に基づいてキーを提供するかどうか決定するために操作可能であり、キーを提供することが決定されると、データサービスフロントエンドにキーを提供する。データサービスフロントエンドはまた、ＫｅｙＩＤなどの他の情報を暗号サービスに提供するようにも構成され得る。しかし、いくつかの実施形態において、ＫｅｙＩＤは、暗号サービスに提供される他の情報との関連によってなど、暗黙的に暗号サービスに示され得る。いくつかの実施形態において、ユーザは、データサービスフロントエンドへ要求を提出することに関連して、ＫｅｙＩＤをデータサービスフロントエンドに提供することにも留意されたい。また

、図９に例示されるように、ある実施形態における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記憶システムからのデータオブジェクトを要求し、それに応じて、キーによって暗号化されるデータオブジェクト、及びＫｅｙＩＤによって識別されるキーによって暗号化されるキーを受信するように構成される。いくつかの実施形態において、暗号サービスは、指定されたＫｅｙＩＤと関連付けられるキーを使用して生成されていない暗号文の復号を実行することを拒否するように操作可能であり得る。

【００５０】

データサービスフロントエンドは、ある実施形態において、暗号サービスから受信されるキーを使用してデータオブジェクトを復号し、その復号されたデータオブジェクトをユーザに提供するように構成される。図１０は、したがって、様々な実施形態に従って復号されたオブジェクトを提供するために使用され得るプロセス１０００の例示的な例を示す。プロセス１０００は、図９と関連して記載されるようなデータサービスフロントエンドシステムなど、任意の好適なシステムによって実行され得る。ある実施形態において、プロセス１０００は、データオブジェクトのＧＥＴ要求を受信すること１００２を含む。データオブジェクトのＧＥＴ要求を受信することは、他の種類の要求と関連して上に記載されるように任意の好適な様態で実行され得る。例えば、データオブジェクトのＧＥＴ要求は、要求を認証するために使用される情報、及び／または他の情報を含み得る。プロセス１０００は、したがって、ある実施形態において、本明細書に記載される他のプロセスと同様、認証要求を認証システムに提出すること１００４、及び認証応答を受信すること１００６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、上記のように、任意の好適な様態で実行され得る。認証応答は、ＧＥＴ要求が真正であるかどうかを決定すること１００８に使用され得る。ＧＥＴ要求が真正でないと決定される１００８場合、ある実施形態におけるプロセス１０００は、要求を拒否すること１０１０を含む。しかしながら、ＧＥＴ要求が真正であると決定される１００８場合、ある実施形態におけるプロセス１０００は、暗号化されたデータオブジェクト及び暗号化されたキーを記憶から取得すること１０１２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オブジェクト及び暗号化されたキーを、図９に関連して上に例示されるデータサービスバックエンド記憶システムから獲得し得る。

【００５１】

ある実施形態において、プロセス１０００は、暗号化されたエンベロープキーを暗号サービスに提供すること１０１４を含む。暗号化されたエンベロープキーを暗号サービスに提供すること１０１４は、任意の好適な様態で実行され得、かつ暗号サービスが暗号化されたキーを復号するかどうかを決定することを可能にする認証証明など、他の情報とともに提供され得る。加えて、暗号化されたエンベロープキーを暗号サービスに提供すること１０１４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キーの中から識別子によって識別されるキーを選択することを可能にするため、暗号化されたエンベロープキーの承認された復号に必要とされるキーの識別子を提供することを含み得る。上に述べたように、しかしながら、キーは暗黙的に識別され得る。暗号サービスは、したがって、適切なキーを選択して、暗号化されたキーを復号し得る。したがって、ある実施形態において、プロセス１０００は、復号されたエンベロープキーを暗号サービスから受信すること１０１６を含む。例えば、暗号サービスが、認証証明は有効である、及び／または暗号化の復号は任意の適用可能なポリシーに従って許容可能であると決定する場合、暗号サービスは、復号されたキーを、データオブジェクトを復号しようとするシステムに提供し得る。データオブジェクトは次いで、復号されたエンベロープキーを使用して復号され得る１０１８。復号されたデータオブジェクトは次いで、ユーザまたはＧＥＴ要求を提出した他のシステムなど、要求者に提供され得る１０２０。

【００５２】

多くの場合、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。図１１は、したがって、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記憶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記憶システムは、上に記載されるようであり得る。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、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また、ユーザ要求が真正であるかどうかを決定し、及び／またはその要求に対してポリシーを施行するために、認証サービスと対話するようにも構成され得る。データサービスフロントエンドはまた、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記憶システムと対話するようにも構成され得る。ユーザ要求は、例えば、バックエンド記憶システム内にデータを記憶するためのＰＵＴ要求、及びデータサービスバックエンド記憶システムからデータを取得するためのＧＥＴ要求を含み得る。上のように、データサービスバックエンド記憶システム内に記憶される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記憶システム内に記憶される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。

【００５３】

図１１の特定の例では、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、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また、認証サービスと対話してユーザ要求が真正であるかどうかを決定するように構成される。ユーザ要求が真正であるかどうか決定することは、上記のような簡便な様態で実行され得る。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は、同じ認証サービスと対話する一方、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ことに留意されたい。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施行するように構成され得る。

【００５４】

暗号サービスフロントエンドは、ある実施形態において、暗号サービスバックエンドと対話するように構成され得る。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る命令に従って、暗号操作を実行するように構成される。暗号操作は、暗号化、復号、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をデータサービスバックエンド記憶システム内に記憶することができるように、平文を暗号サービスによって暗号化させるためにユーザによって使用され得る。環境１１００のそのような使用の例は以下に提供される。加えて、暗号サービス例の詳細例もまた以下に提供される。

【００５５】

データは、上に記載されるような任意の好適な様態でデータサービスバックエンド記憶システム内に記憶され得る。例えば、暗号化されたデータを上に記載されるバックエンド記憶システム内に記憶するための技術が、環境１１００で使用され得る。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、暗号サービスバックエンドにデータを暗号化させ、次いでそれをデータサービスバックエンド記憶システム内に記憶させるために、暗号サービスフロントエンドと通信し得る。暗号化されたデータは、データオブジェクト、及び／またはデータオブジェクトを暗号化するために使用された暗号化されたキーであり得る。環境１１００において、データは、データサービスバックエンド記憶システム内に他の方法でも格納され得る。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、かつそれに応じて暗号文を受信し得る。ユーザは次いで、データサービスバックエンド記憶システム内に暗号文を記憶するように要求するために、対話し得るか、データサービスフロントエンドに要求を提出し得る。データサービスフロントエンドは、この例において、任意の様態で暗号文を記憶し得る。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記憶システムは、データが暗号化されるかどうかに無関係であ

るように構成され得る。

【００５６】

加えて、本明細書に例示されるすべての環境と同様に、追加のフロントエンドシステムが、システム間のアクションを協調させるために、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は他のフロントエンドシステムとの間に論理的に配置され得る。例えば、いくつかの実施形態において、ユーザは、ユーザの観点からの操作がより簡便であるように、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、データオブジェクトを暗号化し、かつ記憶するように要求し得、フロントエンドシステムは、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、その要求に応答する。しかしながら、ユーザの観点からは、そのようなことは、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。

【００５７】

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の例示的な例を示す。図１２において、環境１２００は、ユーザが暗号文をデータサービスバックエンド記憶システム内に記憶することを可能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記憶システム、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記憶システム、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と関連して上に記載される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、かつそれに応答するように構成され、また、ユーザ要求にポリシーを施行するようにも構成され得る。データサービスフロントエンドは、要求への返答の一部として、認証要求を認証サービスに提出し、それに応じてそれに応じ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、後にユーザに提供され得る、暗号化されたデータオブジェクト、及びおそらくは暗号化されていないデータオブジェクトをデータサービスバックエンド記憶システムから獲得するために、データサービスバックエンド記憶システムと対話するようにさらに構成され得る。

【００５８】

図１２に例示されるように、暗号サービスフロントエンドもまた、認証要求を認証サービスに提供し、それに応じて認証証明を受信するように構成される。認証証明は、暗号サービスバックエンドからサービスを獲得す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とも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、暗号文を復号し、代わり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キーであり得、暗号サービスバックエンドは、その暗号化されたキーを復号し、平文キーであるその復号されたキーを、平文キーをユーザに提供するようにさらに構成される暗号サービスフロントエンドに提供し得る。ユーザは次いで、そのキー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オブジェクトを復号し得るか、ユーザのドメイン内（例えば、ユーザによって操作または制御されるデータセンターもしくはコンピュータシステム内）に記憶される暗号化されたデータオブジェクトを復号し得る。この例において、ユーザは、暗号化されたキーをデータサービスフロントエンドから獲得している場合がある。例えば、ユーザは、データオブジェクト及び／またはデータオブジェクトを暗号化するために使用されるキー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ている場合がある。図１１では単一の要求として例示されているが、データオブジェクト及びキーの双方のために別個の要求が出されてもよい。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オブジェクト及び暗号化されたキーをデータサービスバックエンド記憶システムから獲得し、その暗号化されたデータオブジェクト及び暗号化されたキーをユーザに提供し得る。

【００５９】
本明細書に例示されるすべての環境と同様に、変形は、本開示の範囲内であると見なされる。例えば、図１２は、キーの元で暗号化されるデータオブジェクト、及びユーザに提供されているキー識別子によって識別される別のキーによって暗号化されるキーを示す。暗号化のさらなるレベルもまた使用され得る。例えば、データオブジェクトは、ユーザのみがアクセス可能な（及び／または、環境１２００の他の構成要素によってアクセスが不可能な）キーの下で暗号化され得る。データオブジェクトを暗号化するために使用されるキーもまた、ユーザのみがアクセス可能なキーの下で暗号化され得る。この例において、環境１２００の構成要素への不正アクセス（ユーザ不在）は、ユーザのキーへのアクセスが依然として承認された復号を必要とするため、データオブジェクトの暗号化されていないコンテンツへのアクセスを依然として提供しない。
【００６０】
別の例として、図１２に例示される環境１２００において、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記憶システムは、暗号化されたデータを復号するために必要とされるキーへのアクセスを有しないため、データサービスバックエンド記憶システムによって記憶される平文データへのアクセスを有しない。しかしながら、いくつかの実施形態において、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記憶システムにアクセスが付与される場合がある。例えば、ある実施形態において、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獲得し、その暗号化されたデータを復号し、その復号されたデータを特定の目的（例えば、インデックス作成）に使用し、次いで復号されたデータへのアクセスを削除または別の様式で損失することを可能にするため、キー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得る。そのようなアクションは、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施行されるポリシーによって統制され得、かつユーザからの承認を必要とし得る。
【００６１】
図１３は、上に記載されるようなデータサービスバックエンド記憶システム等から暗号化されたデータオブジェクト及び暗号化されたキーを獲得するために使用され得るプロセス１３００の例示的な例を示す。プロセス１３００は、例えば、図１２と関連して上に記載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。ある実施形態において、プロセス１３００は、暗号化されたデータオブジェクトのＧＥＴ要求を受信すること１３０２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コールを介して要求を受信することによってなど、任意の好適な様態で実行され得る。ＧＥＴ要求を受信した結果、プロセス１３００は、認証要求を提出すること１３０４及び認証応答を受信すること１３０６を含み得る。認証要求を提出すること１３０４及び認証応答を受信すること１３０６は、上に記載されるような任意の好適な様態で実行され得る。認証応答は、ＧＥＴ要求が真正であるかどうかを決定する１３０８ために使用され得る。ＧＥＴ要求が真正でないと決定される場合１３０８、プロセス１３００はＧＥＴ要求を拒否すること１３１０を含み得る。ＧＥＴ要求を拒否すること１３１０は、上に記載されるような任意の好適な様態で実行され得る。しかしながら、ＧＥＴ要求が真正であると決定される場合１３０８、プロセス１３００は、暗号化されたデータオブジェクトを、復号されたときに暗号化されたデータオブジェクトを復号するために使用可能な暗号化されたキーとともに提供すること１３１２を含み得る。本明細書に記載されるすべてのプロセスと同様に、多くの変形が本開示の範囲内であると見なされることに留意されたい。例えば、プロセス１３００は、暗号化されたキーを提供することなく暗号化されたデータオブジェクトを提供することによって、真正であるときにＧＥＴ要求に応答するように構成され得る。ＧＥＴ要求を提出したユーザまたはシステムである要求者は、他の方法で暗号化されたキーを獲得し得る。例えば、いくつかの実施形態において、ユーザは、暗号化されたキー自体をユーザの制御下にあるデータ記憶システムに記憶し得る。別の例として、１つの記憶サービスが、暗号化されたデータオブジェクトを記憶し得、別のサービスが、暗号化されたキーを記憶し得、ユーザは、暗号化されたデータオブジェクト及び暗

号化されたキーをそれぞれのサービスから獲得し得る。別の例として、別のサービスまたはユーザにとっての第三者を使用して、暗号化されたキーを記憶し得、ユーザは暗号化されたキーを要求時に獲得し得る。一般的に、暗号化されたキーが提供され得る任意の方法が使用され得る。

【００６２】

図１３に例示されるように、プロセス１３００は、データオブジェクト、及びそのデータオブジェクトを復号するために使用可能な暗号化されたキーを提供されたエンティティをもたらし得る。様々な実施形態において、暗号化されたキーは、データオブジェクトを復号するために、復号されなければならない。図１４は、したがって、復号されたキーを使用して暗号化されたデータオブジェクトを復号するためにそのような復号されたキーを必要とするエンティティに、復号されたキーを提供するために使用され得るプロセス１４００の例示的な例を示す。プロセス１４００は、図１２と関連して上に記載される暗号サービスフロントエンドシステムによってなど、任意の好適なシステムによって実行され得る。ある実施形態において、プロセス１４００は、指定されたＫｅｙＩＤを有する別のキーを使用してキーを復号するための復号を受信すること１４０２を含む。プロセス１４００は、キーの復号と関連して記載されるが、プロセス１４００は一般にデータの復号に適し得ることに留意されたい。復号要求は、上に記載されるような任意の好適な様態で受信され得る１４０２（例えば、適切に構成されたＡＰＩコールを介して）。さらに、復号要求は、プロセス１４００が実行されているコンテクストに適切な任意のエンティティによって受信され得る。例えば、復号要求は、ユーザから、または上に議論されるデータサービスフロントエンドなど別のシステムから生じ得る。復号要求はまた、復号されるデータ（例えば、キー）またはそれへの参照も含み得る。ＫｅｙＩＤは、任意の好適な様態でも指定され得る。例えば、いくつかの実施形態において、復号要求は、ＫｅｙＩＤ、またはＫｅｙＩＤへの参照、つまりＫｅｙＩＤを決定するために使用することができる情報を含む。上に記載されるように、ＫｅｙＩＤはまた、暗黙的にも指定され得る。例えば、ＫｅｙＩＤは、復号要求を提出した要求者のアイデンティティなど、利用可能なデータとの関連によって獲得され得る。例えば、ＫｅｙＩＤに対応するキーは、要求者または要求が提出された代理のエンティティ用のデフォルトキーであり得る。

【００６３】

プロセス１４００は、ある実施形態において、認証要求を提出すること１４０４、及び認証応答を受信すること１４０６を含む。認証要求を提出すること１４０４及び認証応答を受信すること１４０６は、上に記載されるような任意の好適な様態で実行され得る。さらに、上に記載されるように、受信された認証応答は、ＧＥＴ要求が真正であるかどうかを決定する１４０８ために使用され得る。ＧＥＴ要求が真正でないと決定される場合１４０８、プロセス１４００は、ＧＥＴ要求を拒否すること１４１０を含み得る。ＧＥＴ要求を拒否すること１４１０は、上に記載されるような任意の好適な様態で実行され得る。しかしながら、ＧＥＴ要求が真正であると決定される場合１４０８、プロセス１４００は、指定されたＫｅｙＩＤ及び／または要求者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、ＫｅｙＩＤ及び／または要求者に関する１つ以上のポリシーを含む情報を含み得る。

【００６４】

ある実施形態において、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指定されたＫｅｙＩＤを有するキーの復号を許可するかどうかを決定する１４１４ために使用される。ポリシーがＫｅｙＩＤによって指定されるキーの復号を許可しないと決定される場合１４１４、プロセス１４００は、上に記載されるようなＧＥＴ要求を拒否すること１４１０を含み得る。しかしながら、ポリシーが指定されたＫｅｙＩＤを有するキーの復号を許可すると決定される１４１４場合、プロセス１４００は、ＫｅｙＩＤによって識別されるキーを使用してキーを復号すること１４１６を含み得る。ＫｅｙＩＤを有するキーを使用してキーが復号されると、次いでその復号されたキーは、ネットワークを介した送信によってなど、復号要求を提出した要求者（または、いくつかの実施形態において、

別の承認された送信先）に提供１４１８され得る。

【００６５】

上に議論される環境１２００に例示されるように、ユーザは、暗号化されたデータオブジェクト及びデータオブジェクトを復号するためのキーを様々な方法で獲得し得る。図１５は、様々な実施形態に従って平文を獲得するために使用され得るプロセス１５００の例示的な例を示す。プロセス１５００は、図１２と関連して記載されるようなユーザによって操作及び／またはホストされているシステムによってなど、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、提供されるリアルタイムのユーザ入力に従うとは限らないがおそらくは事前にプログラムされたプロセスに従う、ユーザの代理で操作しているシステムを含む。

【００６６】

ある実施形態において、プロセス１５００は、データ記憶サービスから暗号文を受信すること１５０２を含む。データ記憶サービスからの暗号文を要求すること１５０２は、上に記載されるような任意の好適な様態で実行され得る。例えば、プロセス１５００を実行するシステムは、図１２と関連して上に例示される環境１２００内の適切に構成されたＡＰＩコールを使用して、及び／または図１３と関連して上に記載されるプロセス１３００によって、暗号文を要求し得る１５０２。

【００６７】

プロセス１５００はまた、暗号文及び暗号化されたキーを受信することも含み得る。暗号文及び暗号化されたキーを受信することは、任意の好適な様態で実行され得る。例えば、暗号文及び暗号化されたキーは、データ記憶サービスからの暗号文の要求に応じて受信され得る。しかしながら、一般的に、暗号文及び暗号化されたキーは、他の好適な方法で受信され得る１５０４。例えば、データ記憶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、続いて提出される別の要求に準じて受信され得る１５０４。さらに、暗号文及び暗号化されたキーは、単一の応答で提供され得るか、異なる応答（同じまたは異なるシステムからであり得る）によってなど、別々に獲得され得る。別の例として、プロセス１５００を実行するシステムは、暗号化されたキーをローカルまたは別の様式で記憶し得、暗号化されたキーはローカルメモリから取得され得る。

【００６８】

ある実施形態において、プロセス１５００は、指定されたＫｅｙＩＤを有するキーを使用して、暗号化されたキーの復号を要求することを含む。ＫｅｙＩＤは、上に記載されるような任意の好適な様態で指定され得る。さらに、プロセス１５００を実行するシステムは、任意の好適な様態でＫｅｙＩＤを指定することができ得ることに留意されたい。例えば、暗号化されたキー及び／またはそれとともに提供される情報が、ＫｅｙＩＤを指定し得る。別の例として、プロセス１５００を実行するシステムは、ＫｅｙＩＤの決定を可能にする情報へのローカルまたはリモートアクセスを有し得る。ローカルまたはリモートデータベースは、例えば、データオブジェクト識別子を、データオブジェクトを暗号化するために使用されるキーのキー識別子と関連付け得る。一般的に、システムがＫｅｙＩＤを指定することが可能であり得る任意の様態が使用され得る。さらに、いくつかの実施形態において、ＫｅｙＩＤは、暗号サービスに提供される情報がＫｅｙＩＤを決定するのに十分であるときなど、指定される必要がない。暗号化されたキーの復号の要求１５０６は、図１２と関連して上に記載される環境と関連して、及び／または図１４と関連して上に記載されるプロセス１４００の実行によってなど、任意の好適な様態で実行され得る。

【００６９】

プロセス１５００は、ある実施形態において、復号されたキーを受信すること１５０８を含む。復号されたキーを受信すること１５０８は、任意の好適な様態で実行され得る。例えば、復号されたキーは、暗号化されたキーの復号の要求に応じて受信され得る。別の例として、暗号化されたキーの復号の要求は、非同期要求であり得、別の要求が復号されたキーを受信するために提出されている。一般的に、復号されたキーは、任意の好適な様態で受信され得る。さらに、１つのデバイスから別のデバイスへのすべての情報の流れと

同様に、情報の受け渡しは安全なチャネルを使用して実行され得る。例えば、復号されたキーは、復号されたキーを受信するエンティティによる復号のために再び暗号化され得る。一般的に、安全な通信の任意の様態は、１つのエンティティから別のエンティティへ情報を渡すために使用され得る。

【００７０】

復号されたキーが受信される１５０８と、プロセス１５００は、復号されたキーを使用して１５１０暗号文を復号する１５１０ことを含み、それによって平文を獲得し得る。本明細書に記載されるすべてのプロセスと同様に、変形が本開示の範囲内であると見なされることに留意されたい。例えば、プロセス１５００は、暗号文の要求、及び順次実行される暗号化されたキーの複合の要求を示す。しかしながら、様々なプロセスと関連して本明細書に記載される多くの操作と同様に、操作は、様々な実施形態において順次実行される必要はない。例えば、プロセス１５００を実行するシステムが、暗号文の要求の前に暗号化されたキーへのアクセスを有するか、または別の様式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、かつ暗号化されたキーの復号を、並行で、または例示されるものとは異なる順番で要求し得る。他の変形もまた、本開示の範囲内である。

【００７１】

上に記載されるように、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目的とする。暗号サービスは、上に記載される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の例示的な例を示す。図１６に例示されるように、及び上に記載されるように、暗号サービス１６００は、論理的に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なる。フロントエンドシステム及びバックエンドシステムの双方は、本明細書に記載される操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。要求ＡＰＩは、ある実施形態において、暗号の要求、及び暗号サービスによって実行される他の操作のために構成されるＡＰＩである。そのため、要求は、そのような暗号操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対して出され得る。

【００７２】

要求ＡＰＩは、以下の利用可能な高レベルの要求例で構成され得る：

ＣｒｅａｔｅＫｅｙ（ＫｅｙＩＤ）
Ｅｎｃｒｙｐｔ（ＫｅｙＩＤ、Ｄａｔａ、［ＡＡＤ］）
Ｄｅｃｒｙｐｔ（ＫｅｙＩＤ、Ｃｉｐｈｅｒｔｅｘｔ、［ＡＡＤ］）
Ｓｈｒｅｄ（ＫｅｙＩＤ）
ＲｅＫｅｙ（Ｃｉｐｈｅｒｔｅｘｔ、ＯｌｄＫｅｙＩＤ、ＮｅｗＫｅｙＩＤ）。

【００７３】

ＣｒｅａｔｅＫｅｙ（ＫｅｙＩＤ）要求は、ある実施形態において、暗号サービスに、要求内で識別されるＫｅｙＩＤによって識別されるキーを作成させる。要求を受信すると、暗号サービスはキーを生成し、そのキーをＫｅｙＩＤと関連付け得る。ＫｅｙＩＤの識別子は、固有の識別子であり得るが、必ずしもそうであるとは限らないことを知っておくべきである。例えば、ＫｅｙＩＤは、キーのファミリーを識別し得る。例えば、いくつかの実施形態において、キーローテーションが実行される。キーローテーションは、使用される暗号の実質上のクラッキングを可能にするほど十分な復号されたデータの収集を防止するためにキーを別のキーと交換することに関与し得る。暗号サービスと異なるエンティティの指示で実行される場合、ＣｒｅａｔｅＫｅｙ（ＫｅｙＩＤ）要求の使用は、暗号サービスに、ＫｅｙＩＤによって識別される古いキーと交換するために新しいキーを作成させ得る。古いキーは、そのままＫｅｙＩＤによって識別され得るが、例えば、復号（古いキーを使用してすでに暗号化されたデータの）にのみ使用され得、将来の暗号化には使用され得ない。別の例として、いくつかの実施形態において、暗号サービスのユーザは、独自のキー識別子を提供するが、２つの異なる顧客が、同じ識別子を提供し得る可能性があ

る。そのような場合には、識別子はキーを一意的に識別し得ないか、またはキーのファミリーさえ一意的に識別し得ない。これに対処するために様々な対策が設けられ得る。例えば、アイデンティティまたは暗号サービスのユーザと関連付けられる他の情報が、適切なキーまたはキーのファミリーを識別するために使用され得る。依然として他の実施形態において、暗号サービスは、ＫｅｙＩＤを、ランダムに、順次に、または任意の他の方法を使用して、割り当て得る。

【００７４】

ＫｅｙＩＤが一意的にキーを識別しないとき、適切な機能性を可能にするために様々なシステムが設けられ得ることに留意されたい。例えば、様々な実施形態において、ＫｅｙＩＤによって識別されるキーのファミリーは有限である。ＫｅｙＩＤによって識別されるキーを使用した復号操作が要求される場合、追加データ（例えば、暗号化が実行されたときのタイムスタンプ）が、使用に適切なキーを決定することを可能にし得る。いくつかの実施形態において、暗号文は、キーバージョンを示す情報を含み得る。いくつかの実施形態において、可能なあらゆるキーを使用してデータの異なる復号を提供する。キーの有限数が存在するため、適切な復号は提供されたものから選択され得る。いくつかの実施形態において、キーを用いた復号は、暗号サービスが、認証付き暗号化を使用することによってなど、暗号文が少なくとも部分的にキーに基づいて生成されなかったことを検出することを可能にする様態で実行される。他の変形もまた、本開示の範囲内である。

【００７５】

Ｅｎｃｒｙｐｔ（ＫｅｙＩＤ、Ｄａｔａ、［ＡＡＤ］）要求は、暗号サービスに、ＫｅｙＩＤによって識別されるキーを使用して特定のデータを暗号化させるために使用され得る。Ａｄｄｉｔｉｏｎａｌ Ａｕｔｈｅｎｔｉｃａｔｅｄ Ｄａｔａ（ＡＡＤ）は、様々な目的で使用され得、必ずしも暗号化されないが、例えば、ＡＡＤとともに含まれる、電子署名、メッセージ認証コード、または一般的に、キー付ハッシュ値によって、認証されているデータであり得る。いくつかの実施形態において、暗号文は、ＡＡＤの少なくとも一部を含んで生成される。いくつかの実施形態において、ＡＡＤは復号中に別々に提供される。いくつかの他の実施形態において、ＡＡＤは、メタデータが渡るときにのみ復号が成功するように、少なくとも部分的に要求及びまたは他のメタデータに基づいて、復号時に生成される。いくつかの実施形態において、ポリシーは、暗号操作を特定のＡＡＤに対して実行することができるかどうかを制約し得る。プログラミング論理及び／または暗号サービスによって施行されるポリシーによるＥｎｃｒｙｐｔ（ＫｅｙＩＤ、Ｄａｔａ、［ＡＡＤ］）要求の処理は、ＡＡＤが特定の値を含むこと、及びＡＡＤが真正であること（例えば、最初の送信から改変されていない）の双方を必要とし得る。同様に、Ｄｅｃｒｙｐｔ（ＫｅｙＩＤ、Ｃｉｐｈｅｒｔｅｘｔ、［ＡＡＤ］）要求は、暗号サービスに、ＫｅｙＩＤによって識別されるキーを使用して、指定された暗号文を復号させるために使用され得る。Ｄｅｃｒｙｐｔ（ＫｅｙＩＤ、Ｃｉｐｈｅｒｔｅｘｔ、［ＡＡＤ］）要求内のＡＡＤは、上に記載されるように使用され得る。例えば、プログラミング論理及び／または暗号サービスによって施行されるポリシーによるＤｅｃｒｙｐｔ（ＫｅｙＩＤ、Ｃｉｐｈｅｒｔｅｘｔ、［ＡＡＤ］）の処理は、ＡＡＤが特定の値を含むこと、及びＡＡＤが真正であること（例えば、最初の送信から改変されていない）の双方を必要とし得る。

【００７６】

Ｓｈｒｅｄ（ＫｅｙＩＤ）は、ある実施形態において、暗号サービスに、キーまたは、指定されたＫｅｙＩＤによって識別されるキーのファミリーを電子的に破砕させるために使用され得る。電子的破砕は、キーをもはやアクセス不可能にすることを含み得る。例えば、Ｓｈｒｅｄ（ＫｅｙＩＤ）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が指定されたＫｅｙＩＤによって識別される１つ以上のキー上でＳｅｃｕｒｅＥｒａｓｅ操作を実行するように命令させ得る。一般的に、ＫｅｙＩＤによって識別されるキー（複数可）は、キーを符号化しているデータ上に他のデータ（例えば、一連のゼロもしくは１、またはランダムな文字列）を上書きすることによってなど、任意の好適な様態で電子的に破砕され得る。キー（複数可）が、キーの下で暗号化されて記憶される場合、

キーを暗号化するために使用されるキーは、電子的に破砕され得、それによってキー（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において、破砕操作は、破砕されるＫｅｙＩＤを示す復号操作を、将来のある決められた時点で機能させなくし得る。安全かつ永久にキー（複数可）への可能性のあるあらゆるアクセスを破壊することの他の様態が使用され得る。

【００７７】

ＲｅＫｅｙ（Ｃｉｐｈｅｒｔｅｘｔ、ＯｌｄＫｅｙＩＤ、ＮｅｗＫｅｙＩＤ）要求は、ある実施形態において、暗号サービスに異なるキーの下で暗号文を暗号化させるために使用され得る。暗号サービスは、ＲｅＫｅｙ（Ｃｉｐｈｅｒｔｅｘｔ、ＯｌｄＫｅｙＩＤ、ＮｅｗＫｅｙＩＤ）要求を受信すると、ＯｌｄＫｅｙＩＤによって識別されるキーを使用して指定された暗号文を復号し得、次いでＮｅｗＫｅｙＩＤによって識別されるキーを使用して復号された暗号文を暗号化し得る。ＮｅｗＫｅｙＩＤによって識別されるキーがまだ存在しない場合、暗号サービスは、使用するキーを生成し、上に記載されるＣｒｅａｔｅ（ＫｅｙＩＤ）要求と関連して記載されるように、その生成されたキーを指定されたＮｅｗＫｅｙＩＤと関連付け得る。いくつかの実施形態において、ＲｅＫｅｙ操作は、データを暗号サービスの孤立したインスタンス間で送信可能にさせるように操作可能であり得る。いくつかの実施形態において、ポリシーは、キー再設定操作が暗号文上で実行されることを許可する場合もあるが、同じ要求者が暗号文を直接復号することを許可しない場合もある。いくつかの実施形態において、ＲｅＫｅｙは、第１のアカウント内の第１のＫｅｙＩＤによって識別されるキーから第２のアカウント内のＫｅｙＩＤによって識別されるキーへ、暗号文のキー再設定することを支援する場合がある。

【００７８】

同様に、フロントエンドシステムは、ある実施形態において、ユーザが、暗号操作の実行のためのポリシー、及び他のポリシー関連の操作を構成するための要求を提出することを可能にする、ポリシー構成ＡＰＩを実装し得る。ポリシーは、様々な実施形態において、キー、キーのグループ、アカウント、ユーザ、及び他の論理的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例は、以下に提供される。ある実施形態において、暗号サービスポリシー構成ＡＰＩは、以下の要求を含む。

ＳｅｔＫｅｙＰｏｌｉｃｙ（ＫｅｙＩＤ、Ｐｏｌｉｃｙ）

Ｓｕｓｐｅｎｄ（ＫｅｙＩＤ、Ｐｕｂｌｉｃ　Ｋｅｙ）

Ｒｅｉｎｓｔａｔｅ（ＫｅｙＩＤ、Ｐｒｉｖａｔｅ　Ｋｅｙ）

【００７９】

ある実施形態において、ＳｅｔＫｅｙＰｏｌｉｃｙ（ＫｅｙＩＤ、Ｐｏｌｉｃｙ）要求は、暗号サービスに、ＫｅｙＩＤによって識別されるキー（またはキーのファミリー）上にポリシーを記憶させるために使用され得る。ポリシーは、要求された暗号操作を特定のコンテクスト内で実行できるかどうかについて決定力の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操作のために満たされなければならない１つ以上の条件を符号化する任意の好適な方法など、宣言的アクセス制御ポリシー言語で符号化され得る。ポリシーは、どのような操作を実行することができるか、いつ操作を実行することができるか、操作が実行されるための承認された要求をどのエンティティが作ることができるか、特定の要求が承認されるためにはどの情報が必要とされるか等を定義し得る。加えて、ポリシーは、アクセス制御リスト、ユーザと関連付けられた特権、及び／または上に挙げられる例に加えてもしくは代わりに操作ビットマスク、を使用して定義及び／または施行され得る。ポリシー例を以下に示す。

【００８０】

いくつかの実施形態において、暗号サービスは、一時停止操作を、例えば、Ｓｕｓｐｅ

ｎｄ（ＫｅｙＩＤ、Ｐｕｂｌｉｃ　Ｋｅｙ）ＡＰＩコールを使用して支援し得る。一時停止操作は、暗号サービスの顧客が、暗号サービスの操作者によるキーの使用またはキーへのアクセスを拒否することを可能にする。これは、隠れた合法的命令、または暗号サービスの操作者がキーを使用していくつかの操作を実行させられる可能性のある他の状況について懸念している顧客にとって有用であり得る。それはまた、特定のデータをロックし、オンラインでのアクセスを不可能にすることを望む顧客にとっても有用である。いくつかの実施形態において、一時停止操作は、顧客からパブリックキーを受信すること、及び所与のＫｅｙＩＤによって指定されるキーを受信したパブリックキーを用いて暗号化すること、及びパブリックキーと関連付けられたプライベートキーが、例えば、ＫｅｙＩＤを指定しかつプライベートキーを含むＲｅｉｎｓｔａｔｅ（ＫｅｙＩＤ、Ｐｒｉｖａｔｅ　Ｋｅｙ）ＡＰＩコールを使用して、提供されない限りは、プロバイダが一時停止されたキーにアクセスできないようにするために、ＫｅｙＩＤによって指定されるキーを破砕することを含む場合がある。いくつかの実施形態において、一時停止操作は、指定されたＫｅｙＩＤと関連付けられたキーを、暗号サービスによって管理される別のキー（即時の一時停止操作の目的で作成されるものを含むがこれに限定されるものではない）を使用して暗号化することを伴う場合がある。この操作によって生み出される暗号文は、顧客に提供することができ、暗号サービス内に保管しない。ＫｅｙＩＤによって識別されるオリジナルのキーを、次いで破砕することができる。暗号サービスは、提供された暗号文を受信し、一時停止キーを再インポートするように操作可能であり得る。いくつかの実施形態において、暗号文は、暗号サービスが復号されたバージョンを顧客に返すことを防止する様態で生成され得る。

【００８１】

図１６に例示されるように、暗号サービス１６００は、いくつかの実施形態において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、この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のいずれかを介して受信される要求に従う操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、そのような要求が真正であり、それ故に遂行することが可能であるかどうかを決定し、その要求を遂行し得る。要求を遂行することは、例えば、暗号操作を実行すること、及び／または実行したことを含み得る。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決定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、上に記載される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、適切な場合に暗号操作の実行をもたらすために使用され得る認証証明を提供する認証サービスと対話し得る。

【００８２】

暗号サービス１６００のバックエンドシステムはまた、この例示的な例において、複数のセキュリティモジュール（暗号モジュール）及びポリシー施行モジュールも含む。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が、様々な実施形態において、セキュリティモジュールは、本明細書に記載される機能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。ある実施形態における各セキュリティモジュールは、ＫｅｙＩＤに関連付けられた複数のキーを記憶する。各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がアクセスできないように、キーを安全に記憶するように構成され得る。ある実施形態において、セキュリティモジュールのいくつかまたはすべては、少なくとも１つのセキュリティ基準に準拠している。例えば、いくつかの実施形態において、セキュリティモジュールはそれぞれ、ＦＩＰＳ　Ｐｕｂｌｉｃａｔｉｏｎ　１４０－２で概説される１つ以上のセキュリティレベルなど、ＦＩＰＳ　Ｐｕｂｌｉｃａｔｉｏｎ　１４０－１及び／または１４０－２で概説されるＦｅｄｅｒａｌ　Ｉｎｆｏｒｍａｔｉ

ｏｎ Ｐｒｏｃｅｓｓｉｎｇ Ｓｔａｎｄａｒｄ（ＦＩＰＳ）に準拠して検証される。加えて、いくつかの実施形態において、各セキュリティモジュールは、Ｃｒｙｐｔｏｇｒａｐｈｉｃ Ｍｏｄｕｌｅ Ｖａｌｉｄａｔｉｏｎ Ｐｒｏｇｒａｍ（ＣＭＶＰ）の下で認定される。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のいくつかまたはすべての機能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において、検証されたモジュールを使用して操作をブートストラップする。いくつかの実施形態において、顧客は、検証されたモジュール内に記憶され、かつ検証されたモジュールによってのみ操作されるいくつかのキー、及びソフトウェアによって操作される他のキーを構成することができる。いくつかの実施形態において、これらの様々なオプションと関係した性能または費用は異なり得る。

【００８３】

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操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ＫｅｙＩＤを、ＫｅｙＩＤに関連付けられたキーを使用して暗号文を復号し、それに応じて平文を提供せよというセキュリティモジュールに対する命令とともに、適切なセキュリティモジュールに提供し得る。ある実施形態において、暗号サービス１６００のバックエンドシステムは、キー空間を形成する複数のキーを記憶する。セキュリティモジュールの各々は、キー空間内のすべてのキーを記憶し得るが、変形は、本開示の範囲内であると見なされる。例えば、セキュリティモジュールの各々は、キー空間の部分空間を記憶し得る。セキュリティモジュールによって記憶されるキー空間の部分空間は、キーがセキュリティモジュール全体にわたって冗長して記憶されるため、重複し得る。いくつかの実施形態において、特定のキーは、指定された地理的領域内にのみ記憶され得る。いくつかの実施形態において、特定のキーは、特定の証明書またはクリアランスレベルを有する操作者のみがアクセス可能であり得る。いくつかの実施形態において、特定のキーは、データ記憶サービスのプロバイダとの契約の下で特定の第三者プロバイダによって操作されるモジュール内に記憶され得、かつそのモジュールのみとともに使用され得る。いくつかの実施形態において、セキュリティモジュールの構成的制御は、強制される追加のエンティティまたはアクションを強制する追加の管轄権のいずれかに関与することを顧客によって承認される以外に、キーの使用を強制することを求める合法的命令を必要とし得る。いくつかの実施形態において、顧客は、彼らの暗号文が記憶され、かつ彼らのキーが記憶される管轄権のための独立したオプションを提供され得る。いくつかの実施形態において、キーを記憶するセキュリティモジュールは、キーの所有者に監査情報を提供するように構成され得、該セキュリティモジュールは、監査情報の生成及び提供を顧客が抑制できないように構成され得る。いくつかの実施形態において、セキュリティモジュールは、プロバイダ（例えば、セキュリティモジュールをホストしている）がセキュリティモジュールによって記憶されるキーの下で操作を実行することができないように、顧客によって生成される署名を独立して検証するように構成され得る。加えて、いくつかのセキュリティモデルは、キー空間のすべてを記憶し得、いくつかのセキュリティモジュールは、キー空間の部分空間を記憶し得る。他の変形もまた、本開示の範囲内である。異なるセキュリティモジュールがキー空間の異なる部分空間を記憶する場合において、要求処理ユニットは、どのセキュリティモジュールが様々な要求に従って暗号操作を実行するように命令するかを決定するための関係表または他の機序などを用いて構成され得る。

【００８４】

ある実施形態において、ポリシー施行モジュールは、要求処理ユニットから情報を獲得し、少なくとも部分的にその情報に基づいて、ＡＰＩから受信される要求が実行され得るかどうかを決定するように構成される。例えば、暗号操作を実行するための要求が、要求ＡＰＩを介して受信されるとき、要求処理ユニットは、ポリシー施行モジュールと対話して、要求の遂行が任意の適切なポリシー、例えば、要求内の指定されたＫｅｙＩＤに適用可能なポリシー、及び／または要求者と関連付けられたポリシーなどの他のポリシーによって承認されるかどうかを決定し得る。ポリシー施行モジュールが、要求の遂行を許可す

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操作を実行するように命令し得る。

【００８５】

本明細書に記載されるすべての図と同様に、多くの変形が本開示の範囲内であると見なされる。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施行モジュールを示す。しかしながら、各セキュリティモジュールは、別個に例示されるポリシー施行モジュールに加えて、またはその代わりに、ポリシー施行モジュールを含み得る。そのため、各セキュリティモジュールは、ポリシーを施行するように独立して構成され得る。加えて、別の例として、各セキュリティモジュールは、別個のポリシー施行モジュールによって施行されるポリシーとは異なるポリシーを施行するポリシー施行モジュールを含み得る。多くの他の変形が、本開示の範囲内であると見なされる。

【００８６】

上に記載されるように、様々なポリシーは、要求がＫｅｙＩＤに対応するキーと関連して実行される暗号操作を指定するとき、ポリシーが施行され得るように、ＫｅｙＩＤ内の、またはそれと関連した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の例示的な例を提供する。プロセス１７００は、図１６に関連して上に記載されるような暗号サービスシステムによってなど、任意の好適なシステムによって実行され得る。ある実施形態において、プロセス１３００は、ＫｅｙＩＤのポリシーを更新するための要求を受信すること１３０２を含む。要求は、任意の好適な様態で受信され得る１３０２。例えば、例として図１６を参照すると、要求は、上に記載される暗号サービス１６００のフロントエンドシステムのポリシー構成ＡＰＩを介して受信され得る。要求は、任意の好適な様態で受信され得る。

【００８７】

プロセス１７００は、ある実施形態において、認証要求を提出すること１７０４及び認証応答を受信すること１７０６を含む。認証要求を提出すること１７０４及び認証応答を受信すること１７０６は、上に記載されるような任意の好適な様態で実行され得る。さらに上に記載されるように、受信された認証応答は、ＫｅｙＩＤ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決定する１７０８ために使用され得る。ＫｅｙＩＤ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決定される場合１７０８、その要求は拒否され得る１７１０。要求を拒否すること１７１０は、上に記載されるような任意の好適な様態で実行され得る。しかしながら、ＫｅｙＩＤ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決定される場合１７０８、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すること１７１２を含み得る。ポリシー情報は、要求者に適用可能な任意のポリシーが施行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、その組織の特定のユーザのみがＫｅｙＩＤためのポリシーを更新することが許可され得る。ポリシー情報は、どのユーザが暗号サービスにＫｅｙＩＤのポリシーを更新させることができるか、及び／また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さえも示し得る。例えば、暗号サービスは、いくつかの実施形態において、新しいポリシーを施行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しいポリシーが導入されることを許可するかどうかをチェックし得る。暗号サービスが、既存のポリシーが新しいポリシーの施行を許可しないことを決定する場合、その要求は拒否され得る。一般的に、ポリシー情報は、要求者に適用可能なポリシーの施行に使用可能な任意の情報であり得る。

【００８８】

図１７に例示されるように、プロセス１７００は、ポリシー情報を使用して、要求された更新が実行されることをポリシーが許可するかどうかを決定すること１７０４を含む。ポリシーが要求された更新が実行されることを許可しないと決定される場合１７１４、プロセス１７００は、上に記載されるように要求を拒否すること１７１０を含み得る。しかしながら、ポリシーが要求された更新が実行されることを許可すると決定される場合１７１４、プロセス１７００は、ＫｅｙＩＤのポリシーを更新すること１７１６を含み得る。

ＫｅｙＩＤのポリシーを更新することは、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ＫｅｙＩＤに従ってまたはそれに関連して記憶させることを含み得る。更新されたポリシー情報は、例えば、図１６と関連して上に記載されるような暗号サービスのポリシー施行モジュールによって、記憶され得る。

【００８９】

ポリシーはまた、暗号サービスと関連して動作する電子環境の他の構成要素によっても施行され得る。例えば、上に議論される図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施行するために、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。そのようなものは、データサービスがポリシーを施行するのにより適している状況において有用であり得る。例えば、アクションがポリシーによって許可されるかどうかは、データサービスフロントエンドはアクセス可能だが、暗号サービスにはアクセス不可能な情報に少なくとも部分的に基づき得る。一例として、ポリシーは、ポリシーに関連付けられた顧客に代わってデータサービスバックエンド記憶システムによって記憶されるデータに基づき得る。

【００９０】

上に記載されるように、暗号サービスは、ＫｅｙＩＤを有するキー上のポリシーに従ったポリシーの施行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、ポリシーを施行するために使用され得るプロセス１８００の例示された例を示す。プロセス１８００は、図１６に関連して上に記載されるような暗号サービスシステムによってなど、任意の好適なシステムによって実行され得る。ある実施形態において、プロセス１８００は、ＫｅｙＩＤを有するキーを使用して１つ以上の暗号操作を実行するための要求を受信すること１８０２を含む。図１８は、１つ以上の暗号操作を実行するための要求に関連して実行されるものとしてのプロセス１８００を例示するが、プロセス１８００は、必ずしも暗号であるとは限らない操作を実行するための任意の要求での使用に適し得ることに留意されたい。操作例は、上に記載される。

【００９１】

受信された要求が真正であるかどうかの決定がなされ得る１８０４。受信された要求が真正であるかどうか決定することは、上に記載されるように、任意の好適な様態で実行され得る。例えば、要求が真正であるかどうか決定すること１８０４は、上に記載されるように、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。要求が真正でないと決定される場合１８０４、プロセス１８００は、要求を拒否すること１８０６を含み得る。要求を拒否すること１８０６は、上に記載されるような任意の好適な様態で実行され得る。しかしながら、要求が真正であると決定される場合１８０４、プロセス１８００は、ＫｅｙＩＤ及び／または要求者のポリシー情報にアクセスすること１８０８を含み得る。ＫｅｙＩＤ及び／または要求のポリシー情報にアクセスすることは、任意の好適な様態で実行され得る。例えば、ＫｅｙＩＤ及び／または要求者のポリシー情報にアクセスすることは、そのようなポリシー情報を記憶する１つ以上の記憶システムから記憶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つ以上の操作が実行されることを許可するかどうか決定する１８１０ために使用され得る。

【００９２】

ポリシーが１つ以上の操作が実行されることを許可しないと決定される場合１８１０、プロセス１８００は、要求を拒否すること１８０６を含み得る。しかしながら、ポリシーが１つ以上の操作が実行されることを許可すると決定される場合、プロセス１８００は、要求された１つ以上の暗号操作を実行すること１８１２を含み得る。１つ以上の暗号操作の実行の１つ以上の結果は、１つ以上の暗号操作を実行するための受信された要求１８０２を提出した要求者に提供されるなど、提供され得る１８１４。いくつかの実施形態において、許可された要求、及びまたは拒否された要求から少なくとも部分的に派生した情報は、監査サブシステムを介して提供され得る。

【００９３】

議論されるように、本開示の実施形態は、柔軟なポリシー構成及び施行を可能にさせる。いくつかの実施形態において、ポリシーは、どのサービスがどの操作をどのコンテクストにおいて実行することができるかを明言し得る。例えば、キー上のポリシーは、データ記憶サービスが、暗号サービスに復号操作ではなく暗号化操作を実行させることを許可し得る。キー上のポリシーはまた、暗号文及び／または復号された平文に対する１つ以上の条件も含み得る。例えば、ポリシーは、要求に応じて操作の結果が提供される前に、暗号文及び／または平文が特定のハッシュ値（キー付のハッシュ値であり得る）を生み出すことを必要とし得る。ポリシーは、時間、要求が発信されるインターネットプロトコル（ＩＰ）暗号化される／復号される内容の種類、ＡＡＤ、及び／または他の情報に少なくとも部分的に基づく１つ以上の制約及び／または許可を指定し得る。

【００９４】

多くの変形が、本開示の範囲内であると見なされる。例えば、上で議論される様々な実施形態は、別個の認証サービスとの対話について議論する。しかしながら、上で議論される環境の構成要素は、それら独自の承認構成要素を有し得、要求が真正であるかどうかの決定は、別のエンティティとの通信に関与する場合としない場合がある。さらに、上で議論される環境の各々は、環境によって可能になる特定の操作及び機能と関連して例示される。異なる環境と関連して上で議論される技術は、組み合わされ得、一般的に、本開示に従う環境は、様々な技術の柔軟な使用を可能にさせ得る。単に一例として、暗号サービスは、要求時に、キー、及びキー無しデータオブジェクトなどの他のコンテンツの双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、データ記憶サービス）の双方からの要求を受信し、かつ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において、暗号サービス及び／または関連した認証サービスは、記憶されるデータの暗号化を実行するためのモバイルデバイスでの使用のために構成され得る。いくつかの実施形態において、少なくとも１つのロック解除ピンは、暗号サービスによって検証され得る。依然として他の実施形態において、暗号サービスは、操作の一部として、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において、暗号サービスは、内容に対するデジタル権利管理サービスを提供するように操作可能であり得る。

【００９５】

上述のように、本開示の様々な実施形態は、豊富なポリシー施行及びコンフィギュアビリティ（ｃｏｎｆｉｇｕｒａｂｉｌｉｔｙ）を可能にさせる。多くの暗号システムは、暗号操作をデータに対する秘密性、保全性、及び真正性保証を同時に提供するために実行することができる操作の認証付き暗号化モードを提供する。秘密性は、平文データの暗号化によって提供され得る。真正性は、平文、及び暗号化されないままであり得る関連データの双方のために提供され得る。そのようなシステムでは、暗号文または関連データのいずれかに対する変更は、暗号文の復号の失敗を引き起こし得る。

【００９６】

ある実施形態において、平文に関連付けられたデータが、ポリシーの施行において使用される。したがって、図１９は、様々な実施形態に従って関連データを使用したポリシー施行を可能にさせる様態でデータを暗号化するためのプロセス１９００の例示的な例を示す。プロセス１９００は、暗号サービス及び／またはセキュリティモジュールなど、任意の好適なシステムによって実行され得る。例示されるように、プロセス１９００は、平文を獲得すること１９０２を含む。平文は、任意の好適な様態で獲得され得る。例えば、上に記載されるようなサービスプロバイダ環境において、ユーザ（例えば、顧客）は、暗号化されるデータを提供し得る。別の例として、獲得すること１９０２は、キー（暗号化される）を生成すること、及び／または暗号化されるキーを獲得することを含み得る。キーは、上に記載されるように使用され得る。

【００９７】

示されるように、プロセス１９００は、関連データを獲得することを含む。関連データ

は、平文と関連付けられた、または平文と関連付けられる予定の任意のデータであり得る。関連データは、１つ以上のポリシーが少なくとも部分的に基づく任意のデータであり得る。例を以下に示す。さらに、関連データは、ｅＸｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（ＸＭＬ）、ＪａｖａＳｃｒｉｐｔ Ｏｂｊｅｃｔ Ｎｏｔａｔｉｏｎ（ＪＳＯＮ）、Ａｂｓｔｒａｃｔ Ｓｙｎｔａｘ Ｎｏｔａｔｉｏｎ Ｏｎｅ（ＡＳＮ１）、ＹＡＭＬ Ａｉｎ’ｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（Ｙｅｔ Ａｎｏｔｈｅｒ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅとも称される）（ＹＡＭＬ）、または別の構造化拡張可能データ形式など、任意の好適な様態で符号化され得る。ある実施形態において、プロセス１９００は、少なくとも部分的に平文及び関連データに基づいて、メッセージ認証コード（ＭＡＣ）及び暗号文を生成すること１９０６を含む。ＡＥＳ－ＧＣＭ暗号の出力など、ＭＡＣ及び暗号文の組み合わせは、認証付き暗号文と称され得る。ＭＡＣ及び暗号文を生成することは、任意の好適な様態で実行され得、ＭＡＣ及び暗号文の生成は、どの暗号システム（複数可）が使用されるかに依存し得る。例えば、ある実施形態において、高度暗号化規格（ＡＥＳ）は、ＣＣＭモードまたはＧＣＭモードのいずれかで操作されるとき、関連した認証済みデータ（ＡＡＤ）を支援し、ここでＣＣＭはＣｏｕｎｔｅｒ ｗｉｔｈ ＣＢＣ－ＭＡＣを表し、ＧＣＭはＧａｌｏｉｓ／Ｃｏｕｎｔｅｒ Ｍｏｄｅを表し、ＣＢＣは暗号ブロック連鎖（ｃｉｐｈｅｒ ｂｌｏｃｋ ｃｈａｉｎｉｎｇ）を表す。ＣＣＭまたはＧＣＭのいずれかのモードでＡＥＳを使用する場合、平文及び関連データは、平文及び関連データ双方の暗号文及びＭＡＣの連結されたペアの出力を獲得するための入力として提供され得る。ＡＥＳ－ＣＣＭ及びＡＥＳ－ＧＣＭは、例示の目的のために提供されるが、他の認証付き暗号化方式もまた使用され得、本明細書内に明示的に記載される技術をそれに応じて改変することができることに留意されたい。例えば、本開示の技術は、一般に、認証付き暗号化モードを支援した対称ブロック暗号に適用可能である。加えて、他の暗号化方式は、本開示の様々な実施形態に従ってＭＡＣ関数と組み合わせることができる。好適な暗号化方式及びＭＡＣ関数の組み合わせは、暗号化方式が選択平文攻撃の下で強秘匿であり、ＭＡＣ関数が選択メッセージ攻撃の下で偽造不可であるものを含むが、これに限定されない。さらに、本開示の様々な実施形態は、暗号文及びＭＡＣの双方を符号化する単一の出力をもたらす暗号を利用するが、ＭＡＣ及び暗号文は、異なる暗号を使用して生成され得る。さらに、ＭＡＣは例示的な例として使用されるが、一般的なハッシュ、チェックサム、署名、及び／またはＭＡＣの代わりに使用することができる他の値など、一般的にＭＡＣと称されない他の値もまた使用され得る。したがって、関連データを支援する自動化された暗号化モードを有する暗号は、ＭＡＣに加えて、またはＭＡＣの代替として他の暗号プリミティブを使用する暗号を含む。

【００９８】

さらに、ＭＡＣ及び暗号文を生成することは、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、ある実施形態において、平文は、上に記載されるように、セキュリティモジュールに提供される。セキュリティモジュールは、ＭＡＣを生成するように構成され得る。他の実施形態において、セキュリティモジュール以外の電子環境の構成要素は、ＭＡＣ及び暗号文を生成する。そのような実施形態において、セキュリティモジュールは、平文形態にあるときにＭＡＣ及び暗号文を生成するために使用されるキーを復号するために使用され得る。生成されると、ＭＡＣ及び暗号文（すなわち、認証付き暗号文）が提供される１９０８。いくつかの実施形態において、関連データも提供される。ＭＡＣ及び暗号文は、プロセス１９００及びその変形を利用した様々な実装において様々な方法で提供され得る。例えば、いくつかの実施形態において、ＭＡＣ及び暗号文は、上に記載されるように、ユーザに提供されるか、データサービスによる処理のために、上に記載されるように、データサービスに提供される。さらに、述べられるように、関連データは提供され得るが、様々な実施形態において、関連データは提供されない、及び／または一般的に平文形態で保持される。一例として、関連データは、独立して獲得可能である場合、提供されない場合がある。例示的な例として、関連データがデバイスの永続的な識別子（例えば、記憶デバイスの識別子）である場合、関連データは、ポリシー施行及び／または他の

目的で必要とされるときに、後で獲得され得る。

【００９９】

上述のように、本開示の様々な実施形態は、強化されたデータセキュリティを提供するためにセキュリティモジュールを利用する。図２０は、様々な実施形態に従って、新規の豊富なポリシー施行を可能にさせる様態でデータを暗号化するために使用され得るプロセス２０００の例示的な例を示す。プロセス２０００は、暗号サービス及び／またはセキュリティモジュールなど、任意の好適なシステムによって実行される。図２０に例示されるように、プロセス２０００は平文及び関連データを獲得することを含む。上のように、平文及び関連データは、単一の通信で、別個の通信で、及び／または別個のエンティティから受信され得る。獲得されると、平文、関連データ、及びＫｅｙＩＤは、セキュリティモジュールに提供される２００４。セキュリティモジュールは上に記載されるようなものであり得る。さらに、セキュリティモジュールは、上に記載されるように、暗号サービスを支援する環境などの電子環境に関与する複数のセキュリティモジュールから選択され得る。ＫｅｙＩＤは上に記載されるようなものであり得、暗号サービスに提出される平文を暗号化するための要求において指定され得るか、または別の様式で指定され得る。さらに、プロセス２０００の代替の実施形態において、ＫｅｙＩＤは指定されない場合がある。例えば、いくつかの実施形態において、セキュリティモジュールは、ＫｅｙＩＤを選択し得、かつ／または後にＫｅｙＩＤを割り当てられるキーを生成し得る。そのような実施形態において、プロセス２０００は、セキュリティモジュールからＫｅｙＩＤを提供するために改変され得る。

【０１００】

例示される実施形態に戻ると、プロセス２０００は、セキュリティモジュールから暗号文及びＭＡＣを受信すること２００６を含み得る。暗号文は、ＫｅｙＩＤによって識別されるキーの下で暗号化され得る。ＭＡＣは、平文及び関連データの双方の組み合わせに対するＭＡＣであり得るため、暗号文または関連データへの変更は、ＭＡＣのチェックに失敗をもたらす。上のように、変形は、ＭＡＣが少なくとも部分的に関連データに基づくが平文から独立して生成されるものを含むことに留意されたい。さらに、上述のように、暗号文及びＭＡＣは、一緒に提供され得るか（ＡＥＳ－ＣＣＭまたはＡＥＳ－ＧＣＭ暗号の使用の出力からなど）、別個に提供され得る。セキュリティモジュールから受信されると、ＭＡＣ及び暗号文は、上に記載されるように、暗号サービスのユーザ、または暗号サービスと関連して動作するデータサービスなど、適切なエンティティに提供される２００８。

【０１０１】

上述のように、セキュリティモジュールは、データの保護を強化するための様々な方法において使用され得る。上述のように、いくつかの実施形態において、セキュリティモジュールは、他のデータを暗号化するために（平文形態で）使用されるキーを暗号化するために使用される。したがって、図２１は、そのような状況において使用することができるプロセス２１００の例示的な例を示す。プロセス２１００は、暗号サービス及び／またはセキュリティモジュールなど、任意の好適なシステムによって実行される。プロセス２１００は、ある実施形態において、上に記載されるように、平文及び関連データを獲得すること２１０２を含む。例示されるように、プロセス２１００は、セキュリティモジュールに、暗号化されたキー、関連データ、及び暗号化されたキーを復号するためにセキュリティモジュールによって使用可能なキーを識別するＫｅｙＩＤを提供すること２１０４を含む。したがって、プロセス２１００は、暗号化されたキーを復号するためにＫｅｙＩＤによって識別されるキーを使用したセキュリティモジュールから、復号されたキーを獲得することを含む。獲得されたキーは、平文を暗号化し、それによって暗号文及びＭＡＣを計算する２１０８ために使用することができる。暗号文は平文の暗号化であり得、ＭＡＣは、上に記載されるように、関連データ、または関連データ及び平文の双方に対する（すなわち、少なくとも部分的に基づいた）ものであり得る。暗号化されると、プロセス２１００は、上に記載されるように、ＭＡＣ及び暗号文を提供すること２１１０を含み得る。さ

らに、プロセスはまた、ＳｅｃｕｒｅＥｒａｓｅ操作、復号されたキーを記憶するメモリの上書き、キーを記憶する揮発性メモリへの電力の除去、及び／またはシステムがプロセス２１００を実行する（例えば、ある暗号システムはセキュリティモジュールを欠く）任意の他の方法によってなど、任意の好適な様態で実行され得る、復号されたキーへのアクセスを失うこと２１１２も含み得る。並行して例示されているが、関連データ、ＭＡＣ、ならびに／もしくは暗号文を提供すること、及びキーへのアクセスを失うことは、様々な実施形態間で異なり得る順序で、順に実行され得る。

【０１０２】

図２２は、様々な実施形態に従って、関連データを使用してポリシーを施行するために使用され得るプロセス２２００の例示的な例を示す。プロセス２２００は、暗号サービス及び／またはセキュリティモジュールなど、任意の好適なシステムによって実行される。ある実施形態において、プロセス２２００は、操作を実行するための要求を受信すること２２０２を含む。要求は、要求を処理するサービスに提出される任意の要求であり得る。ある実施形態において、要求は、暗号サービスに提出される暗号操作を実行するための要求である。要求を受信すること２２０２に応じて、プロセス２２００は、暗号文、ＭＡＣ、及び予測される関連データを獲得すること２２０４を含み得る。暗号文、ＭＡＣ、及び予測される関連データを獲得すること２２０４は、任意の好適な様態で実行され得る。例えば、いくつかの実施形態において、暗号文、ＭＡＣ、及び予測される関連データのうちの１つ以上は、要求内に受信される。暗号文、ＭＡＣ、及び予測される関連データのうちの２つ以上は、別個の要求もしくは他の通信において受信され得、及び／またはローカルデータストアなど、データストアからアクセスされ得る。例えば、ある実施形態において、暗号文及びＭＡＣは、要求の一部として、連結されたペア（おそらくは、ＡＥＳ－ＧＣＭまたはＡＥＳ－ＣＣＭ暗号の出力から生成される）として受信される。予測される関連データもまた、要求の一部であり得るか、または他の方法で識別され得る。例えば、要求者のアイデンティティを直接的または非直接的に使用して、関連データを決定し得る。具体的な例として、要求が記憶デバイスに記憶されるデータに関連した操作を実行することである場合、関連データを獲得すること２２０４は、データ記憶デバイスの識別子を獲得することを含み得る。識別子は、明示的（例えば、要求の一部として）または暗黙的（例えば、データがデータ記憶デバイス内に記憶されていることを決定するために、他の情報を利用することができるため）に識別され得る。関連データは、データ記憶デバイスの識別子であり得るか、あるいは少なくとも部分的にそれに基づき得る。上述のように、関連データは、様々な実施形態間で大きく異なり得る。

【０１０３】

ある実施形態において、プロセス２２００は、予測される関連データの真正性を決定するのに使用可能な参照ＭＡＣを生成すること２２０６を含む。例えば、暗号文、関連データ、及び適切なキー（要求内で識別され得るか、別の様式で決定され得る）を使用して、参照ＭＡＣを生成する２２０６。ＭＡＣを生成することは、暗号文を獲得するために使用された暗号と同じものを使用することによってなど、任意の好適な様態で実行され得る。参照ＭＡＣと獲得されたＭＡＣとが一致するかどうかの決定がなされ得る２２０８。例えば、多くの暗号システムにおいて、ＭＡＣは、それらが等しいときに一致するが、様々な実施形態において、他の種類の整合が使用され得ることが企図される。参照ＭＡＣと獲得されたＭＡＣとが一致すると決定される場合２２０８、ある実施形態において、プロセス２２００は、少なくとも部分的に関連データに基づいたポリシー情報にアクセスすること２２１０を含む。ポリシー情報にアクセスすること２２１０は、参照ＭＡＣを生成するため及び／または別の暗号操作を実行するために使用されるＫｅｙＩＤに関連付けられる１つ以上のポリシーに少なくとも部分的に基づいた、リモートまたはローカルデータストアからの１つ以上のポリシー（すなわち、１つ以上のポリシーの電子表示）にアクセスすることを含み得る。

【０１０４】

次いで、アクセスされたポリシー情報に少なくとも部分的に基づいて、ポリシーが要求

された操作が実行されることを許可するかどうか（例えば、ポリシーが、要求が遂行されることを許可するかどうか）の決定がなされ得る２２１２。ポリシーが要求された操作が実行されることを許可するかどうか決定することは、暗号文がアクセスされたポリシー情報によって指定される関連データにタグ付けされているかどうかを決定することを含み得る。さらに、例示されていないが、関連データに少なくとも部分的に基づかないポリシー情報（例えば、関連データ以外の情報に基づいたポリシー）もまた、ポリシーが、操作が実行されることを許可するかどうか決定するために使用され得る。ポリシーが操作を許可すると決定される場合２２１２、プロセス２２００は、操作を実行すること２２１４を含み得る。しかしながら、ポリシーが操作を許可しないと決定される場合２２１２、及び／または参照ＭＡＣと獲得されたＭＡＣとが一致しないと決定される場合２２０８、プロセス２２００は、上に記載されるように、要求を拒否すること２２１６を含み得る。

【０１０５】

様々なポリシーは、上に記載される技術を使用して施行可能である。例えば、述べられるように、ポリシーが施行されるときにキーを用いて何ができ及び／またはできないのかを決定するように、ポリシーはキーと関連付けられ得る。一例として、ポリシーは、データサービスが、ポリシーによって指定される特定の種類の操作のみにキーを使用することができる（または、あるいは、特定の操作がデータサービスに対して禁止される）と明言し得る。ポリシーはまた、使用、使用時間、ＩＰアドレス、何が暗号化され得るか、何が復号され得るか等についての条件も指定し得る。１つの例示的な例として、１つのポリシーは、復号された結果を提供することは、復号のハッシュが指定された値と一致する場合にのみ許可されると指定し得る。そのため、暗号サービスまたはポリシーを施行する他のサービスは、平文のハッシュがポリシーに一致しない場合、平文を提供しない。別の例として、あるポリシーは、暗号文の復号は、暗号文が、指定された値と等しいまたはそれで始まる関連データにタグ付けされている場合にのみ許可されると指定し得る。さらに別の例として、あるポリシーは、暗号文の復号は、暗号文が、関連データ内で符号化される記憶デバイスの識別子にタグ付けされている場合にのみ許可されると指定し得る。

【０１０６】

一般的に、ポリシーは、暗号文と関連したデータの値（すなわち、認証された関連データ）に少なくとも部分的に基づいた制約及び／特権を指定し得る。いくつかの追加のポリシーは、復号が、復号を要求するコンピュータの識別子にタグ付けされる暗号文、復号を要求するコンピュータに取り付けられた（操作的に接続された）記憶ボリュームの識別子にタグ付けされる暗号文、及び／または他のコンピューティングリソースの識別子にタグ付けされる暗号文にのみ許可されると指定するポリシーを含む。コンピューティングリソースはまた、ポリシーを施行するコンピューティングリソースプロバイダによってホストされるコンピューティングリソースでもあり得る。他のポリシーは、暗号アルゴリズムの出力が、暗号アルゴリズムを実行するエンティティ以外にエンティティに明らかにされる（例えば、ポリシーを施行する暗号サービス以外にユーザ及び／または他のデータサービスに明らかにされる）前に、暗号アルゴリズムの入力及び／または出力に少なくとも部分的に基づくポリシーなど、本開示の範囲内であると見なされる。上に述べられるように、ポリシーはまた、少なくとも部分的に関連データに基づき得る、ポリシーが改変され得るときの条件も指定し得る。

【０１０７】

図２３は、図２２に関連して上に記載されるプロセス２２００の変形であるプロセス２３００の例示的な例を示し、ここで該変形は、様々な実施形態に従う、ポリシーの施行におけるセキュリティモジュールの使用を例示する。ある実施形態において、プロセス２３００は、暗号化されたキーまたは他の暗号化されたデータであり得る暗号文を復号するための要求を受信すること２３０２を含む。プロセス２３００はまた、図２２に関連して記載されるように、暗号文、ＭＡＣ、及び予測される関連データを獲得すること２３０４も含む。図２３に例示されるように、ある実施形態において、プロセス２３００は、暗号文を復号するためにセキュリティモジュールを使用すること２３０６を含む。セキュリティ

モジュールを使用すること２３０６はまた、暗号文を復号するために操作可能な複数のセキュリティモジュールからセキュリティモジュールを選択し、それによって平文を生み出すことも含み得る。セキュリティモジュールはまた、平文及び予測される関連データに少なくとも部分的に基づいて参照ＭＡＣを生成するためにも使用され得る２３０８。図２３では２つの別個のステップとして示されるが、セキュリティモジュールを使用して暗号文を復号し参照ＭＡＣを生成することは、単一の操作（例えば、セキュリティモジュールに対する単一の要求）で実行され得ることに留意されたい。セキュリティモジュールから獲得されると、プロセス２３００は、図２２に関連して上に記載されるように、参照ＭＡＣと獲得されたＭＡＣが一致するかどうか決定すること２３１０を含む。しかしながら、いくつかの実施形態において、プロセス２３００は、セキュリティモジュールが参照ＭＡＣを提供され、参照ＭＡＣと獲得されたＭＡＣとが一致するかどうかを決定するように改変され得ることに留意されたい。この変形において、セキュリティモジュールは、一致があるかどうかを示す応答を提供し得る。

【０１０８】

図２３に例示される実施形態に戻ると、参照ＭＡＣと獲得されたＭＡＣとが一致すると決定される場合２３１０、プロセス２３００は、図２２に関連して上に記載されるように、少なくとも部分的に関連データに基づいたポリシー情報にアクセスすること２３１２を含む。また、上のように、そのようなものとして例示されていないが、少なくとも部分的に関連データに基づかないポリシーに関する追加のポリシー情報もまたアクセスされ得る。ポリシーが操作を許可するかどうかの決定がなされ得る２３１４。ポリシーが操作を許可すると決定される場合２３１４、平文が提供され得る２３１６。図２２に関連して上のように、ポリシーが操作を許可しないと決定される場合２３１４、及び／または参照ＭＡＣが獲得されたＭＡＣと一致しないと決定される場合、プロセスは、上に記載されるように、要求を拒否すること２３１８を含み得る。

【０１０９】

本開示の様々な実施形態は、暗号の認証モードの関連データを使用して例示されるが、他の実施形態もまた、本開示の範囲内であると見なされる。例えば、本開示の実施形態は、一般的に、ポリシーを施行するための暗号文で検証可能なデータの使用に適用する。例示的な例として、ポリシーの表示は、第１の平文と組み合わせて新しい平文を生成することができる（例えば、平文及びポリシーを含む新しい平文）。新しい平文は、ＡＥＳなどの好適な暗号を使用して暗号化されて、暗号文を生み出すことができる。暗号文を復号するための要求が受信されるとき、要求を受信するシステムは暗号文を復号し、新しい平文からポリシーを抽出し、ポリシーが第１の平文が提供されることを許可するかどうかチェックし得る。ポリシーが第１の平文が提供されることを許可しない場合、要求は拒否され得る。そのような実施形態は、暗号の認証モードの関連データに関連して上に記載される実施形態の代わりに、またはそれに加えて、使用され得る。

【０１１０】

本開示の様々な実施形態はまた、キー上のポリシーが、どのように監査が行われるかの条件を指定することも可能にする。例えば、キー上のポリシーはキーの監査レベルを指定し得、ここで監査レベルとは、暗号サービスがどのようにキーの使用を監査するかについて決定力のある暗号サービスのパラメータである。監査は、任意の好適なシステムによって実行され得る。例えば、図１６を参照すると、要求処理ユニットは、暗号サービスの一部またはそれとは別個であり得る監査システム（図示せず）と通信し得る。暗号操作の実行に関連してイベントが発生するとき、関連情報は、情報を記録する監視システムに提供され得る。イベントは、暗号操作を実行するための要求、及び／または要求された操作が実行されたかどうかを示す情報であり得る。例えば、ユーザが暗号サービスに復号操作を実行するための要求をすることに成功した場合、暗号サービスは、監査システムに、要求を可能にするための情報、及び操作が実行されたという情報を提供し得る。管理アクセスイベント及び、一般的に、暗号サービスの任意の対話または操作は、イベントに関与したエンティティを識別し得る関連情報、イベントを説明する情報、イベントのタイムスタン

プ、及び／または他の情報とともに記録され得る。

【０１１１】

ある実施形態において、監査レベルは、高耐久性レベル及び低耐久性レベルを含む。低耐久性レベルでは、キーの監査操作は、暗号サービスによってベストエフォート型で実行され得る。低耐久性レベルに従う監査では、正常な操作中は、すべての操作が監査されるが、暗号サービスの構成要素の失敗のイベントにおいては、いくつかの監査データは失われ得る。高耐久性レベルに従う監査では、暗号操作の結果を明らかにする前に、操作が発生したという監査記録が耐久的にメモリに引き渡されているという保証が得られる。確認が必要とされるため、高耐久性監査モードにおける操作は、低耐久性監査モードにおける操作よりも遅い。監査記録が耐久的にメモリに引き渡されているという保証は、監査記録を記憶するために使用される１つ以上の他のシステムからの確認を含み得る。そのため、前の段落を参照すると、暗号サービスは、平文をユーザに提供することを、平分をもたらす復号の記録が耐久的にメモリに引き渡されているという監査システムからの確認に至るまで遅らせ得る。耐久的にメモリに引き渡されるとは、データが耐久性のための１つ以上の条件に従って記憶されていることを意味し得る。例えば、データは、データが非揮発性メモリに書き込まれるとき、及び／またはデータが複数のデータ記憶デバイス間に冗長して記憶されている（例えば、イレージャーコーディング（ｅｒａｓｕｒｅ　ｃｏｄｉｎｇ）または他の冗長符号化方式を使用して）とき、耐久的にメモリに引き渡され得る。

【０１１２】

ある実施形態において、暗号サービスは、低耐久性及び高耐久性監査レベルのサブレベルを使用する。例えば、ある実施形態において、各レベルは、２つの別個の状態、不変状態及び可変状態に相当する。状態が不変または不変であるかどうかは、状態間の遷移がどのように起こるのか、及び起こるのかどうかを決定し得る。例えば、監査耐久性の例示的な例を使用すると、キー上のポリシーは、低耐久性可変と高耐久性可変との間で、低耐久性可変から低耐久性不変へ、及び高耐久性可変から高耐久性不変へ変更することができ得る。しかしながら、暗号サービスは、キーのポリシーが低耐久性不変または高耐久性不変のいずれかに一旦置かれると、遷移は禁止されるように構成され得る。そのため、キーのポリシーが不変状態に一旦置かれると、ポリシーを変更することはできない。

【０１１３】

図２４は、オン（施行される）及びオフ（施行されない）であることができるポリシーに一般化される、そのようなシステムの状態図の例示的な例を示す。図２４に例示されるように、キーのためのポリシーは、オンまたはオフであることができる。オン及び不変のとき、ポリシーは、オン及び不変（変化不可能）、またはオフ及び可変（変化可能）へ変更されることができる。同様に、ポリシーがオフであるが可変であるとき、ポリシーを、オンであるが可変、またはオフであるが不変へ変更することができる。オフであるが可変であるポリシーからオン及び不変への直接遷移など、他の遷移もまた利用可能であることに留意されたい。さらに、示されるすべての遷移が利用可能でない場合がある。例えば、キーは、いくつかの場合においては、オフ及び不変状態を有し得ない。

【０１１４】

図２５は、どのようにシステムがキーに適用可能な様々なポリシー間の遷移を許可し得るかを示す一般化された状態図を示す。この例において、３つのポリシー、ポリシーＡとポリシーＢとポリシーＣとが示される。これらのポリシーの各々が、可変及び不変状態を有し、状態及びポリシー間で許容可能な遷移が示される。例えば、不変状態からの遷移は許可されない。しかしながら、可変状態にあるポリシーは、可変状態にある別のポリシーに変更されることができる。例えば、キー上のポリシーは、ポリシーＡ（可変）からポリシーＢ（可変）に変更され得る。ポリシーＢで例示されるように、複数のポリシーに利用可能な遷移があり得る。例えば、ポリシーＢからは、ポリシーはポリシーＣまたはポリシーＡのいずれかに変更されることができる。図２４と同様に、他の遷移及びポリシーが含まれ得、すべてのポリシーがすべての状態を有し得るわけではない。さらに、様々な例が不変及び可変状態を有するポリシーを示す一方、ポリシーは２つを超える状態を有し得、

ここで各状態は、実行することができる、または実行することができないアクションのセットに相当する。例えば、半可変状態は、可変状態下で利用可能な遷移のすべてではないがいくつかを許可し得る。

【０１１５】

述べられるように、ポリシーは、監査に加えて様々な操作のために使用されることができる。例えば、ポリシー遷移における上の制約は、キー破砕性に適用され得る。例えば、あるポリシーは、キーが破砕され得る（取り消し不能の形で失われる）かどうかを示し得る。該ポリシーは、破砕可能－可変、破砕可能－不変、破砕不可能－可変、破砕不可能－不変という４つの状態を有し得る。上のように、不変状態にあるとき、該ポリシーは変更され得ない。別の例として、キーをセキュリティモジュールからエクスポートすることができるかどうかに関するポリシーもまた、そのような４つの状態のポリシーを有し得る。

【０１１６】

ポリシーはまた、セキュリティ攻撃に対する脆弱性を可能にするキー使用を防止するために、キーと関連付けられ得る。例えば、ある実施形態において、１つ以上のキーは、一定使用数の後にキーをリタイアさせる（例えば、もはや暗号化のために使用できないようにマークされる）自動ローテーションポリシーと関連付けられる。そのようなポリシーは、ユーザ（例えば、顧客）がパラメータをアクティブにする及び／または提供する、ユーザ構成可能（例えば、顧客構成可能）ポリシーであり得る。該ポリシーはまた、キーのより大きなセット（顧客に代わって暗号サービスによって管理される少なくともすべてのキーを含むセットなど）に適用可能なグローバルポリシーでもあり得る。この様態において、キーは、十分な平文及び対応する暗号文の知識がキーを決定する能力を提供する暗号攻撃を可能にするのに十分な時間使用される前に、リタイアされ得る。

【０１１７】

図２６は、様々な実施形態に従って、適切な間隔でキーをローテートさせるために使用されるプロセス２６００の例示的な例を示す。プロセス２６００は、上に記載されるセキュリティモジュールなど、任意の好適なデバイスによって実行され得る。ある実施形態において、プロセス２６００は、ＫｅｙＩＤによって識別されるキーを使用して暗号操作を実行するための要求を受信すること２６０２を含む。要求は、上に記載されるような、暗号サービス要求プロセッサから受信される要求であり得る。要求は、電子署名、別のキー、またはキーに少なくとも部分的に基づいた他の情報の生成など、データを暗号化もしくは復号するための、または一般的には、ＫｅｙＩＤによって識別されるキーを使用して任意の暗号操作を実行するための要求であり得る。要求を受信すると２６０２、プロセス２６００は、要求された操作を実行すること２６０４を含む。要求された操作を実行することは、操作を実行するためにキーの適切なバージョンを選択することなど、追加の操作を含み得る。例えば、操作が暗号化である場合、アクティブとしてマークされるキーが暗号化のために使用され得る。操作が復号である場合、操作を実行することは、ＫｅｙＩＤによって識別されるキーの適切なバージョンを選択して復号することを含み得、様々な実施形態において、そのキーは、データを暗号化するために最初に使用されたキーである。キーは様々な方法によって選択され得る。例えば、いくつかの実施形態において、暗号文は、バージョン、シリアルナンバー、日付、またはキーの選択を可能にする他の情報を識別するメタデータを含み得る。いくつかの実施形態において、可能性のあるキーはそれぞれ、データが正しく復号されるまで試され得、正しい復号は、暗号文に関連付けられる平文出力のハッシュによって、または関連データの正当性によって決定され得る。

【０１１８】

一度暗号操作が実行されると２６０４、プロセス２６００は、ＫｅｙＩＤによって識別されるアクティブキー用のキー使用カウンタを更新すること２６０６を含む。例えば、暗号操作が１回のキー使用をもたらす場合、カウンタは１ずつ増加され得る。同様に、暗号操作が、Ｎ（Ｎは正整数）回のキー使用をもたらす場合、カウンタはＮずつ増加され得る。カウンタが閾値を越えるかどうかの決定がなされる２６０８。閾値は、ＫｅｙＩＤによって識別されるキーのバージョンに割り当てられる使用数であり得る。閾値は、キーの操

作の割り当てを管理する暗号サービスの構成要素によって提供され得る。閾値はまた、デフォルトの操作数でもあり得る。カウンタが閾値を越えると決定される場合２６０８、ある実施形態において、プロセス２６００は新しいキーを獲得すること２６１０を含む。新しいキーを獲得することは、任意の好適な様態で実行され得る。例えば、プロセス２６００がセキュリティモジュールによって実行される場合、新しいキーを獲得することは、新しいキーを生成すること、または新しいキーを暗号サービスの操作者によって編成され得る別のセキュリティモジュールから獲得することを含み得る。１つのセキュリティモジュールから他のセキュリティモジュールに鍵を渡すことは、提供側及び受信側のセキュリティモジュールがアクセスを有するキーを用いてキーを暗号化することによって実行され得る。プロセス２６００を実行するセキュリティモジュールは、暗号化されたキーを取得し、かつ復号し得る。公開キーのキー交換技術もまた使用され得る。

【０１１９】

新しいキーが獲得されると、ある実施形態において、プロセス２６００は、現在のアクティブキーをリタイアとしてマークすること２６１２を含み得る。現在のアクティブキーをリタイアとしてマークすることは、セキュリティモジュールによって維持されるデータベース内の適切な値を変更することによってなど、任意の好適な様態で実行され得る。さらに、プロセス２６００は、セキュリティモジュールによって維持されるデータベースを更新することなどによって、新しいキーをＫｅｙＩＤと関連付けること２６１４、及び新しいキーをアクティブとしてマークすることを含む。例示されていないが、プロセス２６００はまた、別のセキュリティモジュールによる使用のための新しいキーを提供することをも含み得る。破線により示されるように、新しいキーが、プロセス２６００を実行するセキュリティモジュール（または他のシステム）による使用のための準備が整った後のある時点で、プロセスは、別の暗号操作を実行するための要求を受信すること２６０２を含み得、プロセス２６００は上述のように処理し得る。さらに、カウンタが閾値を越えないと決定される場合２６０８、プロセス２６００は、終了し得、かつ／または別のリクエストが受信される２６０２と繰り返し得る。

【０１２０】

図２７は、様々な実施形態に従って、暗号サービスまたは他の環境でキーの自動ローテーションを実行するために使用され得るプロセス２７００の例示的な例を示す。プロセス２７００は、キー使用を追跡し、様々な実施形態に従ってキーローテーションを編成する暗号サービスの構成要素など、任意の好適なシステムによって実行され得る。図２７に例示されるように、プロセス２７００は、キーのための多くのキー操作（例えば、複数のキーのそれぞれのための多くの操作）を１つ以上のセキュリティモジュールに割り当てること２７０２を含む。具体的な例として、キーのセットを冗長して記憶／使用するために５つのセキュリティモジュールを利用する環境において、各セキュリティモジュールは、それが管理するそれぞれのキーに１００万個の操作を割り当てられ得る。操作が割り当てられるセキュリティモジュール（または他のコンピュータシステム）は、複数のデータセンター中の同じデータセンターにおいてホストされ得る。例えば、いくつかの実施形態において、コンピューティングリソースプロバイダは、複数の地理的領域にある複数のデータセンター内のセキュリティモジュールを利用して、地理的に分散された暗号または他のサービスを実装する。

【０１２１】

しかしながら、その割り当てはすべてのキーではなくいくつかのキーに対してなされ得ること、及び各キーの割り当ては等しくない場合があることに留意されたい。キー操作を割り当てることは、どのキー操作が割り当てられたか、各セキュリティモジュールに割り当ての通知を提供することを含み得る。その通知は、各キーに割り当てられた数を指定し得、または、いくつかの実施形態において、セキュリティモジュールへの通知は、セキュリティモジュールに対して、セキュリティモジュール内に予めプログラムされたカウンタを再初期化すること、または予めプログラムされた数をカウンタに追加することを示し得る。キー操作をセキュリティモジュールに割り当てる２７０２と、操作が割り当てられた

各キー用のキー使用カウンタが更新され得る。上の具体事例を続けると、５つのセキュリティモジュールの各々が特定のＫｅｙＩＤによって識別されるキーに１００万個の操作を割り当てられた場合、ＫｅｙＩＤ用のカウンタは、５００万ずつ増やされ得る（カウントが上方または下方に実行されるかによって、上方または下方に）。

【０１２２】

キー操作が割り当てられた際に、セキュリティモジュールは上に記載されるような暗号操作を実行し得る。セキュリティモジュールは、なされた割り当てに少なくとも部分的に基づいたそれら独自のカウンタを維持し得る。上の例では、セキュリティモジュールが特定のＫｅｙＩＤによって識別されるキーに１００万個の操作を割り当てられた場合、セキュリティモジュールは、カウンタを１００万にセットし得る（または、既存のカウンタが残りの操作を有する場合は１００万を超える）。キーを使用した暗号操作を実行する際、セキュリティモジュールは、その独自のカウンタをそれに応じて増やし得る。

【０１２３】

ある時点で、１つ以上のＫｅｙＩＤのための割り当て枯渇イベントが検出され得る２７０６。枯渇イベントは、１つ以上のセキュリティモジュールがその割り当てを失うまたはそれに枯渇する、任意のイベントであり得る。一例として、セキュリティモジュールは、特定のＫｅｙＩＤによって識別されるキーに対する操作のその割り当てを使用し得、かつ枯渇イベントの検出は、セキュリティモジュールから、セキュリティモジュールが、対応する数の操作を実行することによってＫｅｙＩＤに対するその割り当てに枯渇している（あるいは、その割り当てに枯渇していることを示すいくらかの規定の閾値の範囲内にある、またはその割り当てにすぐに枯渇することが別の様式で予測される）という通知を受信することを含み得る。別の例として、いくつかの実施形態において、セキュリティモジュールは、故障、侵入もしくは他の改ざんの検出などの特定のイベント時に、または操作者が保守のためにセキュリティモジュールへのアクセスを必要とするとき、そこに記憶されるキー（及び、カウンタなどのキーと関連付けられたデータ）へのアクセスを失うように構成される。したがって、枯渇イベントは、故障、または改ざん／侵入の検出、及び内部アクション（保守のためにセキュリティモジュールを一時的に使用不能にすることなど）に起因するセキュリティモジュールの損失（おそらくは一時的）を含み得る。この例において、セキュリティモジュールは、それが割り当てられた数の操作を必ずしも実行したとは限らないにもかかわらず、その割り当てを使用したかのように処理され得る。しかしながら、すべてのそのようなイベントは、カウンタが永続的に記憶され、それ故に対応するキーへのアクセスの損失時にさえ復元可能であるときなど、特定の実施形態においては枯渇イベントを含まない場合があることに留意されたい。枯渇イベントは１つを超えるセキュリティモジュールに影響を与え得ることにも留意されたい。例えば、データセンター内の複数のセキュリティモジュールに影響を与える電源異常は、複数のセキュリティモジュールに影響を与える枯渇イベントをもたらし得る。

【０１２４】

枯渇イベントの検出時、カウンタが枯渇イベントに関連付けられたキーのうちのいずれかの閾値を越えるかどうか決定がなされ得る２７１０。閾値は、暗号操作を実行するために使用される暗号の数学的性質に少なくとも部分的に基づいた操作の規定の数であり得る。例えば、ＣＢＣモードを用いた暗号では、操作の数は、（１）ブロック内に表される暗号文の長さと、（２）暗号文の数との平方の積で割ったキー空間の大きさであり得るか、少なくとも部分的にそれに基づき得る。ＣＴＲモードを用いた暗号（ＡＥＳ－ＧＣＭなど）では、操作の数は、（１）ブロック内の暗号文の長さの平方と、（２）暗号文の数との積で割ったキー空間の大きさであり得るか、少なくとも部分的にそれに基づき得る。カウンタが枯渇イベントにより影響を受けたキーのうちのいずれかの閾値を越えると決定される場合２７１０、プロセス２７００は、１つ以上のセキュリティモジュール（すなわち、枯渇イベントに関連付けられた１つ以上のセキュリティモジュール）に、操作の割り当てが枯渇している１つ以上の新しいキーを獲得し、影響を受けたキー（複数可）を新しいキー（複数可）と交換するように命令すること２７１２を含み得る。例えば、セキュリティ

モジュールが一時的にオフラインになり（それによって枯渇イベントを引き起こす）、結果として、ＫｅｙＩＤ用のカウンタ（しかしすべてのＫｅｙＩＤとは限らない）が閾値を越えることになる場合、セキュリティモジュールは、上に記載されるように（例えば、新しいキーを作成すること、データ記憶から予め生成されたキーにアクセスすること、または別のセキュリティモジュールから新しいキーを獲得することによって）、新しいキーを獲得するように命令され得る。しかしながら、枯渇イベントによって影響を受けたセキュリティモジュールとは異なるセキュリティモジュールは、１つのセキュリティモジュールがオフラインにされ、新しいセキュリティモジュールがオンラインにされるときなどに、新しいキーを獲得するように命令され得ることに留意されたい。影響を受けたキー（ＫｅｙＩＤによって識別される）を新しいキーと交換することは、影響を受けたキーをリタイアとしてマークすること、新しいキーをＫｅｙＩＤと関連付けること（例えば、データベース内）、及び新しいキーをアクティブとしてマークすることを含み得る。影響を受けたキーを新しいキーと交換することはまた、新しいキー用のカウンタ（影響を受けたキーを新しいキーと交換するセキュリティモジュールによって維持される）を初期化することも含み得、それは、予めプログラムされた値であり得るか、プロセス２７００を実行するシステムから獲得される値であり得る。プロセス２７００はまた、影響を受けたキー（複数可）をリタイアとして、新しいキー（複数可）をアクティブとして、データベースをそれに応じて更新することなどによってマークすること２７１４も含み得る。プロセス２７００を実行するシステムは、影響を受けたキー及び／または新しいキー（複数可）へのアクセスを有しない場合があり、その結果、影響を受けたキー（複数可）をリタイアとして、及び新しいキー（複数可）をアクティブとしてマークすることは、リタイアまたは新規のどちらか適切な方を示す値とキーの識別子を関連付けることを含み得ることに留意されたい。

【０１２５】

ある実施形態において、マークする２７１４際、影響を受けたキーのいずれもが閾値を超えるカウンタを有しないと決定される場合は２７１０、プロセス２７００は、依然としてアクティブな影響を受けたキー（複数可）、及び／またはプロセス２７００の操作を実行した結果として獲得された任意の新しいキー（複数可）に追加のキー操作を割り当てること２７１６を含み得る。追加のキー操作の割り当ての際、適切なキー使用カウンタ（複数可）は、上に記載されるように、更新され得る２７０４。

【０１２６】

本明細書に記載されるすべてのプロセスと同様に、変形は本開示の範囲内であると見なされる。例えば、いくつかの実施形態において、セキュリティモジュールは、キーのそれらの使用を追跡しないが、暗号または他のサービスの別の構成要素は、キーを使用して１つ以上の操作を実行するために任意のセキュリティモジュールに提出される各要求のためのキー用のカウンタを更新する。そのような実施形態において、複数のキーの各キーのため、セキュリティモジュールの構成要素は、キーを使用して操作を実行するための要求を追跡し（または、例えば、要求の遂行に成功したという確認または他の指標によって、実行される操作を追跡し）、それに応じてキー用のカウンタを更新し得る。カウンタが閾値に達すると、カウンタを維持するシステムは、すべての適切なセキュリティモジュールに、キーのリタイアをさせて新しいキーと交換（または、キーを有するセキュリティモジュールに、キーのリタイアをさせること、１つ以上の他のセキュリティモジュールに新しいキーの使用を開始させることなど、キーのリタイアを引き起こすいくつかの他の操作を実行）させ得る。本開示の範囲内である変形の別の例として、いくつかの実施形態において、セキュリティモジュールがキー操作のその割り当てを使用し、カウンタに閾値を超えさせるとき、セキュリティモジュールは、上に記載されるように、新しいキーを獲得することを命令され得る。他のセキュリティモジュールは、それらの割り当てを使用するまでキーを使用し続け得る。セキュリティモジュールがその割り当てを使用するとき、それは、カウンタに閾値を超えさせたセキュリティモジュール内のキーと交換した新しいキーを獲得することができる。言い換えると、セキュリティモジュールは、新しいキーの獲得が必

要になる前にキー操作のそれらの割り当てを使い尽くすことが許可され得る。

【０１２７】

図２８は、キー使用の追跡を維持するために使用されるデータベースの例示的な代表例を示す。データベースは、プロセス２７００を実行するシステムなどの、適切なシステムによって維持され得る。例示されるデータベースにおいて、カラムは、ＫｅｙＩＤ、キーバージョン、ユーザビリティ、及びカウンタに相当する。ＫｅｙＩＤ及びキーバージョンは、上に記載されるようなものであり得る。ユーザビリティカラム内の値は、キーがリタイアもしくはアクティブであるかどうか（または、キーが別の状態を有するかどうか（そのような他の状態が本開示の様々な実施形態によって支援される場合））を示し得る。図２８に例示されるように、データベースは、すべてのリタイアバージョン及びアクティブバージョンを含む、ＫｅｙＩＤによって識別されるキーの各バージョンの列を有する。しかしながら、データベースはキーのすべてのバージョンを欠き得ることに留意されたい。例えば、キーは、様々なセキュリティ上の理由により記憶から永久に削除され得る。削除は、例えば、顧客要求またはポリシーの施行に準じ得る。

【０１２８】

図２８に例示されるように、例示されるデータベースはまた、各アクティブキー用のカウンタも含む。また、この特定の例において、データベースは、非アクティブキー用のカウンタ（例えば、閾値を超える各キーの値を示し、それによって新しいキーが獲得されることになる）を含む。しかしながら、非アクティブキーのカウンタ値は、いくつかの実施形態において、保持されない場合がある。カウンタは、キー操作がセキュリティモジュールに割り当てられるときに、データベースを維持するシステムによって更新され得る。カウンタ列の値が閾値の値を超えると、カウンタが閾値を越えたキーと交換するための新しいキーを収容するために、新しい列がデータベースに追加され得る。

【０１２９】

セキュリティモジュールは、それら独自の目的のために同様のデータベースを維持し得る。例えば、あるセキュリティモジュールは、キーのその独自の使用を追跡し得、かつセキュリティモジュールによるキーの使用がセキュリティモジュールに割り当てられた数を使い果たすとき、セキュリティモジュールは、例えば、追加の操作をセキュリティモジュールに再割り当てするか、キーが利用可能な多数のキー操作が使い果たされている場合は、セキュリティモジュールに新しいキーを獲得させるかのいずれかのために上に記載されるプロセス２７００のようなプロセスを実行し得る暗号サービス（または、セキュリティモジュールを使用する別のサービス）のキーローテーション管理構成要素に通知し得る。

【０１３０】

キー使用を追跡するために使用されるデータベースは、図２８に例示されるもの及び上に記載されるものと相違し得る。例えば、生成の時間、リタイアの時間、キーを使用するユーザに関する情報、及び／または様々な実施形態において有用であり得る他の情報など、キーに関連付けられるメタデータなどの追加の情報がデータベース内に含まれ得る。さらに、例示の目的のために関係表が提供されるが、様々な実施形態を支援してデータを記憶する他の方法が使用され得る。

【０１３１】

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．ポリシーを施行するためのコンピュータ実装方法であって、

実行可能な命令で構成される１つ以上のコンピュータシステムの制御下で、

少なくとも部分的にキー、平文、及び関連データに基づいて、認証付き暗号文を生成するために認証付き暗号化モードを使用することと、

ポリシーをキーと関連付けることであって、該ポリシーが、少なくとも部分的に関連データに基づいて、平文を提供するための条件を指定する、関連付けることと、

キーを使用して認証付き暗号文を復号するための要求に関連して、関連データと称されているものを受信することと、

関連データと称されているもの及び認証付き暗号文に少なくとも部分的に基づいて、

関連データと称されているものが関連データと一致することを検証すること、
　関連データと称されているものが関連データと一致することを検証した結果、関連データと称されているものに少なくとも部分的に基づいて、ポリシーが平文を提供することを許可するかどうかを決定することと、
　ポリシーが平文を提供することを許可することを決定した結果、平文を提供することと、を含む方法。
２．関連データと称されているものが要求の一部である、付記１に記載のコンピュータ実装方法。
３．関連データと称されているものが少なくとも部分的に平文に基づく、付記１または２に記載のコンピュータ実装方法。
４．ポリシーが平文を提供することを許可するかどうか決定することもまた、認証付き暗号文に少なくとも部分的に基づく、付記１～３のいずれか一項に記載のコンピュータ実装方法。
５．ポリシーを施行するためのコンピュータ実装方法であって、
実行可能な命令で構成される１つ以上のコンピュータシステムの制御下で、
　暗号文を復号するための要求を受信することであって、該暗号文が少なくとも部分的に平文及びキーに基づいて生成されている、受信することと、
　暗号文及びキーで検証可能なデータに少なくとも部分的に基づいて、要求に応じて、ポリシーが平文を提供することを許可するかどうかを決定することと、
　ポリシーが平文を提供することを許可することを決定した結果、要求に応じて、少なくとも平文を提供することと、を含む方法。
６．ポリシーが、キーの使用に関する１つ以上の制約を指定するポリシーである、付記５に記載のコンピュータ実装方法。
７．該方法が、関連データと称されているもの及びキーに少なくとも部分的に基づいて、関連データと称されているものが真正であるかどうかを決定することをさらに含み、
　要求に応じて、ポリシーが平文を提供することを許可するかどうかを決定することが、暗号文で検証可能なデータの値がポリシーによって指定される値と一致するかどうかを決定することを含む、付記５または６に記載のコンピュータ実装方法。
８．暗号文が認証付き暗号化モードの出力であり、該出力が、暗号文と関連付けられるデータに少なくとも部分的に基づくメッセージ認証コードも含み、
　該方法が、少なくとも部分的にメッセージ認証コードに基づいて、暗号文と関連付けられていると称するデータが真正であるかどうかを決定することをさらに含む、付記５～７のいずれか一項に記載のコンピュータ実装方法。
９．暗号文がさらに、暗号文及びキーで検証可能なデータに少なくとも部分的に基づく、付記５～８のいずれか一項に記載のコンピュータ実装方法。
１０．ポリシーが、平文を提供することが許容可能であるためには、要求の特性が暗号文と関連付けられるデータと一致することを必要とする、付記５～９のいずれか一項に記載のコンピュータ実装方法。
１１．暗号文で検証可能なデータがポリシーを符号化し、ポリシーが平文を提供することを許可するかどうかを決定することが、暗号文で検証可能なデータからポリシーを獲得することを含む、付記５～１０のいずれか一項に記載のコンピュータ実装方法。
１２．暗号文がポリシーを符号化し、ポリシーが平文を提供することを許可するかどうか決定することが、暗号文からポリシーを獲得することを含む、付記５～１１のいずれか一項に記載のコンピュータ実装方法。
１３．暗号文で検証可能なデータが１つ以上の属性を符号化し、ポリシーが平文を提供することを許可するかどうか決定することが、１つ以上の属性がポリシーの属性と一致するかどうかをチェックすることを含む、付記５～１２のいずれか一項に記載のコンピュータ実装方法。
１４．暗号文が１つ以上の属性を符号化し、ポリシーが平文を提供することを許可するかどうかを決定することが、１つ以上の属性がポリシーの属性と一致するかどうかをチェッ

クすることを含む、付記１～１３のいずれか一項に記載のコンピュータ実装方法。
１５．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、１つ以上のプロセッサによって実行されるとき、コンピュータシステムに、
要求と関連付けられる情報が暗号文と合致していることを検証させ、
要求に関連付けられる情報に少なくとも部分的に基づいて、暗号文及び認証情報を分析して、ポリシーが要求に対する特定の応答を許可するかどうかを決定させ、
ポリシーが特定の応答を許可することを決定した結果、要求に対する特定の応答を有効にさせる、命令を含む、メモリと、を備える、コンピュータシステム。
１６．
暗号文が、認証情報を含む認証付き暗号文であり、
認証情報が、メッセージ認証コードを含み、
要求と関連付けられる情報が暗号文と合致することを検証することが、メッセージ認証コードを使用して要求と関連付けられる情報の真正性をチェックすることを含む、付記１５に記載のシステム。
１７．認証情報が暗号文の構成要素である、付記１５または１６に記載のシステム。
１８．要求と関連付けられる情報が、構造化拡張可能データ形式で符号化される、付記１５～１７のいずれか一項に記載のシステム。
１９．要求が、暗号文を復号するための要求である、付記１５～１８のいずれか一項に記載のシステム。
２０．要求と関連付けられる情報が、暗号文を生成するために暗号によって使用される関連データである、付記１５～１９のいずれか一項に記載のシステム。
２１．認証情報が、平文と、要求に関連付けられる情報で一致しない場合には、ポリシーに特定の応答を却下させる特定の情報とに少なくとも部分的に基づいて生成されるメッセージ認証コードである、付記１５～２０のいずれか一項に記載のシステム。
２２．要求と関連付けられる情報が、少なくとも部分的に特定の情報に基づいて生成され、
認証情報が、特定の情報が要求と関連付けられる情報と一致するかどうかを示す、付記１５～２１のいずれか一項に記載のシステム。
２３．暗号が、認証付き暗号化モード暗号である、付記１５～２２のいずれか一項に記載のシステム。
２４．コンピュータ可読記憶媒体であって、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き、コンピュータシステムに、
平文及び他の入力に少なくとも部分的に基づいて生成されている暗号文から平文を獲得させ、
少なくとも部分的に他の入力に基づいて、ポリシーを評価して、要求に応じて平文を提供するかどうかを決定させ、かつ
平文を提供することを決定した結果、要求に応じて平文を提供させる、命令をそこに記憶している、コンピュータ可読記憶媒体。
２５．他のデータが、暗号文を生成するために暗号に入力される関連データである、付記２４に記載のコンピュータ可読記憶媒体。
２６．コンピュータシステムがサービスプロバイダによってホストされ、
要求されたものが、サービスプロバイダの顧客に代わって提出される、付記２４または２５に記載のコンピュータ可読記憶媒体。
２７．命令がさらに、コンピュータシステムに、顧客からのポリシーを符号化する情報を受信させ、
ポリシーを評価することが、ポリシーを符号化する情報を受信した結果として実施される、付記２６に記載のコンピュータ可読記憶媒体。
２８．平文を獲得することが、暗号文をセキュリティモジュールに提供すること、及びセ

キュリティモジュールから平文を獲得することを含む、付記２４～２７のいずれか一項に記載のコンピュータ可読記憶媒体。
２９．ポリシーを評価することがさらに、要求に関連して獲得される情報に少なくとも部分的に基づく、付記２４～２８のいずれか一項に記載のコンピュータ可読記憶媒体。
３０．ポリシーが、平文から暗号文を生成するために使用されるキーと関連付けられる、付記２４～２９のいずれか一項に記載のコンピュータ可読記憶媒体。
３１．他の入力が、標準化データ形式で符号化される属性のセットを含む、付記２４～３０のいずれか一項に記載のコンピュータ可読記憶媒体。
３２．他の入力がポリシーを符号化する、付記２４～３１のいずれか一項に記載のコンピュータ可読記憶媒体。

【０１３２】
図２９は、様々な実施形態に従う態様を実装するための環境２９００例の態様を例示する。理解されるように、ウェブベースの環境が説明の目的で使用されるが、異なる環境もまた、必要に応じて、様々な実施形態を実装するために使用され得る。該環境は、適切なネットワーク２９０４を介して要求、メッセージ、または情報を送受信し、情報をデバイスのユーザに返送するために操作可能な任意の適切なデバイスを含むことができる、電子クライアントデバイス２９０２を含む。そのようなクライアントデバイスの例としては、パーソナルコンピュータ、携帯電話、ハンドヘルドメッセージングデバイス、ラップトップコンピュータ、セットトップボックス、携帯情報端末、電子書籍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、もしくは他のそのようなネットワーク、またはその組み合わせを含む、任意の適切なネットワークを含むことができる。そのようなシステム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。そのようなネットワークを介した通信のためのプロトコル及び構成要素は、周知であり、本明細書内では詳細に議論されない。ネットワークを介した通信は、有線または無線接続、及びその組み合わせによって可能にされ得る。この例において、該環境は、要求を受信し、それに応じてコンテンツを供給するためのウェブサーバ２９０６を含むため、ネットワークはインターネットを含むが、他のネットワークでは、同様の目的を果たす代替のデバイスを使用することができることは、当業者には明らかであろう。

【０１３３】
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２９０８及びデータストア２９１０を含む。連結されるか、または別の様式で構成され得、適切なデータストアからデータを得ることなどのタスクを実行するために対話することができる、いくつかのアプリケーションサーバ、レイヤ、もしくは他の要素、プロセス、または構成要素が存在し得ることを理解されたい。本明細書内で使用される場合、「データストア」という用語は、データの記憶、アクセス、取得が可能な任意のデバイスまたはデバイスの組み合わせを指し、任意の標準、分散、またはクラスタ環境にある、任意の組み合わせ及び数のデータサーバ、データベース、データ記憶デバイス、及びデータ記憶媒体を含み得る。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に応じてデータストアと統合するための任意の適切なハードウェア及びソフトウェアを含むことができ、アプリケーションのデータアクセス及びビジネスロジックの大部分を処理する。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、ユーザに送信されるテキスト、グラフィック、オーディオ、及び／またはビデオなどのコンテンツを生成することができ、それらは、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」）、またはこの例における別の適切な構造化言語の形態で、ウェブサーバによってユーザに供給され得る。すべ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２９０２とアプリケーションサーバ２９０８との間のコンテンツの配信は、ウェブサーバによって処理され得る。本明細書において論じられる構造化符号は、本明細書の他の部分で論じられるような任意の適切なデバイスまたはホストマシン上で実行され得るため、ウェブ及びアプリケーションサ

ーバは必要とされず、単に例示の構成要素であることを理解されたい。

【０１３４】

データストア２９１０は、特定の態様に関してデータを記憶するために、いくつかの別個のデータテーブル、データベース、または他のデータ記憶機序及び媒体を含むことができる。例えば、例示されるデータストアは、プロダクション側のコンテンツを供給するために使用することができる、プロダクションデータ２９１２、ユーザ情報２９１６を記憶するための機序を含む。データストアはまた、報告、分析、またはそのような目的に使用することができる、ログデータ２９１４を記憶するための機序を含むことも示される。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などにデータストア内に記憶される必要があり得る多くの他の態様があり得、それらの情報を、必要に応じて上に列挙された機序内、またはデータストア２９１０内の追加の機序内に記憶することができることを理解されたい。データストア２９１０は、それと関連付けられたロジックを介して、アプリケーションサーバ２９０８から命令を受信し、それに応じて、データを獲得、更新、または別の様式で処理するように操作可能である。一例として、ユーザはある特定の種類のアイテムの検索要求を提出してもよい。この場合、データストアは、ユーザ情報にアクセスして、ユーザのアイデンティティを検証してもよく、及び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関する情報を獲得することができる。情報は次いで、ユーザがユーザデバイス２９０２上のブラウザを介して閲覧することができるウェブページ上に列挙する結果内などで、ユーザに戻され得る。対象の特定のアイテムの情報を、ブラウザの専用ページまたはウィンドウ内で閲覧することができる。

【０１３５】

各サーバは、典型的には、一般管理及びそのサーバの操作のための実行可能な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、典型的には、サーバのプロセッサによって実行されるとき、サーバがその意図される機能を実行することを許可する命令を記憶するコンピュータ可読記憶媒体（例えば、ハードディスク、ランダムアクセスメモリ、読出し専用メモリ等）を含む。オペレーティングシステム及びサーバの一般的な機能性の好適な実装は、既知であるか、市販されており、特に本明細書における開示に照らして、当業者によって容易に実装される。いくつかの実施形態において、オペレーティングシステムは、評価保証レベル（ＥＡＬ）レベル４などの１つ以上の検証体制に従って、またはその下で構成され得る。

【０１３６】

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、いくつかのコンピュータシステム及び通信リンクを介して相互接続される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、当業者には、そのようなシステムは、図２９に例示されるよりも少数または多数の構成要素を有するシステム内で等しく良好に動作し得ることが理解されよう。そのため、図２９におけるシステム２９００の描写は、本質的に例示的であると見なされるべきであり、本開示の範囲に限定するものではない。

【０１３７】

様々な実施形態はさらに、多種多様な動作環境で実装することができ、場合によっては、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、または多数のアプリケーションのうちのいずれかを操作するために使用することができる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運用するデスクトップまたはラップトップコンピュータ、ならびにモバイルソフトウェアを運用し、多数のネットワーキング及びメッセージングプロトコルを支援することができる携帯、ワイヤレス、及びハンドヘルドデバイスなど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むことができる。そのようなシステムはまた、開発やデータベース管理などの目的のための、多数の市販のオペレーティングシステム及び他の既知のアプリケーションのうちのいずれかを運用する多数のワークステーションも含むことができる。これらのデバイスは、ダミー端子、シンクライアント、ゲーミングシステム、及びネットワークを

介して通信できる他のデバイスなど、他の電子デバイスも含むことができる。

【０１３８】

大半の実施形態は、トランスミッションコントロールプロトコル／インターネットプロトコル（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）（「ＴＣＰ／ＩＰ」）、開放型システム間相互接続（Ｏｐｅｎ Ｓｙｓｔｅｍ Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ）（「ＯＳＩ」）、ファイルトランスファープロトコル（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）（「ＦＴＰ」）、ユニバーサルプラグアンドプレイ（Ｕｎｉｖｅｒｓａｌ Ｐｌｕｇ ａｎｄ Ｐｌａｙ）（「ＵｐｎＰ」）、ネットワークファイルシステム（Ｎｅｔｗｏｒｋ Ｆｉｌｅ Ｓｙｓｔｅｍ）（「ＮＦＳ」）、コモンインターネットファイルシステム（Ｃｏｍｍｏｎ Ｉｎｔｅｒｎｅｔ Ｆｉｌｅ Ｓｙｓｔｅｍ）（「ＣＩＦＳ」）、及びアップルトーク（ＡｐｐｌｅＴａｌｋ）など、多様な市販のモデル及びプロトコルのうちのいずれかを使用して支援するための、当業者によく知られている少なくとも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、ワイヤレスネットワーク、及びそれらの任意の組み合わせであり得る。

【０１３９】

ウェブサーバを利用する実施形態において、ウェブサーバは、ハイパーテキストトランスファープロトコル（Ｈｙｐｅｒｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）（「ＨＴＴＰ」）サーバ、ＦＴＰサーバ、コモンゲートウェイインタフェース（Ｃｏｍｍｏｎ Ｇａｔｅｗａｙ Ｉｎｔｅｒｆａｃｅ）（「ＣＧＩ」）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、多様なサーバまたは中間層アプリケーションのうちのいずれかを運用することができる。サーバ（複数可）はまた、Ｊａｖａ（登録商標）、Ｃ、Ｃ＃、もしくはＣ＋＋などの任意のプログラミング言語、またはＰｅｒｌ、Ｐｙｔｈｏｎ、もしくはＴＣＬなどの任意のスクリプト言語、ならびにそれらの組み合わせで書かれた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など、ユーザデバイスからの要求に応じてプログラムまたはスクリプトを実行することもでき得る。サーバ（複数可）はまた、Ｏｒａｃｌｅ（登録商標）、Ｍｉｃｒｏｓｏｆｔ（登録商標）、Ｓｙｂａｓｅ（登録商標）、及びＩＢＭ（登録商標）から市販される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含み得る。

【０１４０】

該環境は、上述のように、多様なデータストア及び他のメモリ記憶媒体を含むことができる。これらは、コンピュータのうちの１つ以上に対してローカルである（及び／またはその中に存在する）か、またはネットワーク全体のコンピュータのいずれかもしくはすべてから遠隔にある記憶媒体上など、多様な場所に存在することができる。実施形態の特定の一式において、情報は、当業者によく知られてい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した関数を実行するための任意の必須ファイルは、必要に応じて、ローカルに及び／または遠隔に記憶され得る。システムがコンピュータ化デバイスを含む場合、そのようなデバイスはそれぞれ、バスを介して電子的に連結され得るハードウェア要素を含むことができ、該要素は、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。そのようなシステムはまた、ディスクドライブ、光学記憶デバイス、ランダムアクセスメモリ（「ＲＡＭ」）または読出し専用メモリ（「ＲＯＭ」）などの固体記憶デバイス、ならびに可換型媒体デバイス、メモリカード、フラッシュカード等の、１つ以上の記憶デバイスも含み得る。本開示の様々な実施形態はまた、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に限定されないカスタムハードウェアを使用して実装され得る。

【０１４１】

そのようなデバイスはまた、コンピュータ可読記憶媒体リーダ、通信デバイス（例えば、モデム、ネットワークカード（無線または有線）、赤外線通信デバイス等）、及び上に記載されるようなワーキングメモリを含むこともできる。コンピュータ可読記憶媒体リーダは、遠隔、ローカル、固定、及び／または可換型記憶デバイスを意味するコンピュータ可読記憶媒体、ならびに一時的に及び／またはより永久的にコンピュータ可読情報を含有、記憶、送信、及び取得するための記憶媒体と接続され得るか、またはそれら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また、典型的には、クライアントアプリケーションまたはウェブブラウザなどのオペレーティングシステム及びアプリケーションプログラムを含む、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他の要素も含む。代替の実施形態は、上述されるのものからの多数の変形を有し得ることを理解されたい。例えば、カスタマイズされたハードウェアが使用されてもよく、及び／または特定の要素をハードウェア、ソフトウェア（アプレットなどのポータブルソフトウェアを含む）、もしくはその両方に実装してもよい。さらに、ネットワーク入力／出力デバイスなど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。

【０１４２】

符号または符号の一部を含むための記憶媒体及びコンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、電子的消去可能プログラマブル読出し専用メモリ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ－Ｏｎｌｙ Ｍｅｍｏｒｙ）（「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出し専用メモリ（Ｃｏｍｐａｃｔ Ｄｉｓｃ Ｒｅａｄ－Ｏｎｌｙ Ｍｅｍｏｒｙ）（「ＣＤ－ＲＯＭ」）、デジタルバーサタイルディスク（ＤＶＤ）、もしくは他の光学ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージ、もしくは他の磁気ストレージデバイス、または所望の情報を記憶するために使用することができ、かつシステムデバイスによってアクセスされ得る任意の他の媒体をはじめとする、限定するものではないが、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、または他のデータなどの情報の記憶及び／または送信のために任意の方法及び技術で実装される揮発性及び非揮発性、可換型及び非可換型媒体などの記憶媒体及び通信媒体を含む当該術分野において既知の、または使用される任意の適切な媒体を含むことができる。本明細書で提供される開示及び教示に基づいて、当業者であれば、様々な実施形態を実装するための他の手段及び／または方法を理解するであろう。

【０１４３】

本明細書及び図面は、したがって、制限的な意味ではなく、例示的と見なされるものである。しかしながら、様々な修正及び変更が、特許請求の範囲に記載される本発明のより広義の趣旨及び範囲から逸脱することなく、そこになされ得ることは明らかであろう。

【０１４４】

他の変形は本開示の趣旨内にある。そのため、開示される技術は、様々な修正及び代替構成の影響を受けやすいが、その特定の例示される実施形態が図面に示され、上に詳細に記載されている。しかしながら、本発明を開示される特定の形態（複数可）に限定する意図はなく、反対に、添付の特許請求の範囲に定義されるような、本発明の趣旨及び範囲内に含まれるすべての修正、代替構成、及び等価物を網羅することを理解されたい。

【０１４５】

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」という用語及び同様の指示語の使用は、本明細書において別段の指示がない限り、または文脈に明らかに矛盾するものでない限り、単数及び複数の双方を網羅すると解釈される。「備える（ｃｏｍｐｒｉｓｉｎｇ）」、「有する（ｈａｖｉｎｇ）」、「含む（ｉｎｃｌｕｄｉｎｇ）」、及び「含有する（ｃｏｎｔａｉ

ｎｉｎｇ）」という用語は、別段の記載がない限り、制限のない用語（すなわち、「含むが、それに限定されない」を意味する）として解釈される。「接続される（ｃｏｎｎｅｃｔｅｄ）」という用語は、介在するものがある場合でも、部分的または全体的に、その中に含有される、そこに取り付けられる、一緒に接合されるものと解釈される。本明細書における値の範囲の列挙は、本明細書において別段の指示がない限り、単にその範囲内に含まれるそれぞれ別個の値を個別に参照する簡略的な方法として機能することが意図され、それぞれ別個の値は、本明細書において個別に列挙されるかのように、本明細書に組み込まれる。本明細書内に記載されるすべての方法は、本明細書において別段の指示がない限り、または文脈と明らかに矛盾しない限り、任意の適切な順序で実行され得る。本明細書内に提供される任意及びすべての実施例、または例示的言語（例えば、「など」）の使用は、単に本発明の実施形態をより良く明らかにすることが意図され、別段の請求がない限り、本発明の範囲に対して制限を課すものではない。本明細書内のいかなる言い回しも、任意の請求されていない要素を本発明の実施に必須であると示すものとして解釈されるべきではない。

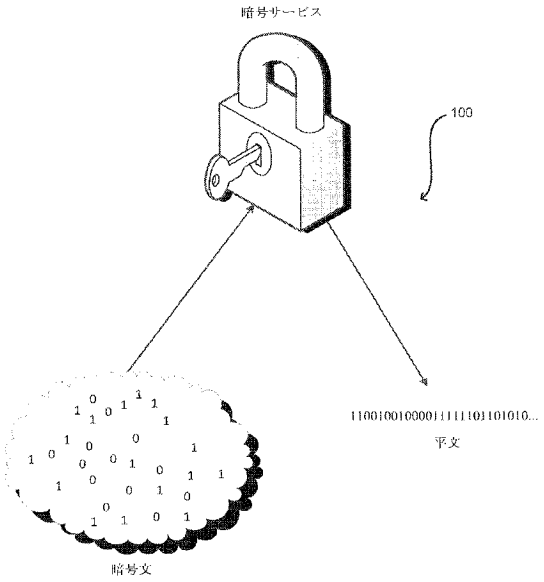
【０１４６】

本開示の好ましい実施形態は、本発明を実効するために発明者らに既知の最良の形態を含んで説明される。それらの好ましい実施形態の変形は、前述の説明を読むことで当業者に明らかとなり得る。発明者らは、当業者がそのような変形を必要に応じて用いることを予期し、及び発明者らは、本発明が本明細書内に具体的に記載されるものとは別の様式で実施されることを意図する。したがって、本発明は、適用可能な法律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に列挙される主題のすべての修正及び等価物を含む。さらには、上述の要素の、その全ての可能な変形にある、任意の組み合わせは、本明細書において別段の指示がない限り、またはさもなければ文脈と明らかに矛盾しない限り、本発明によって包含される。

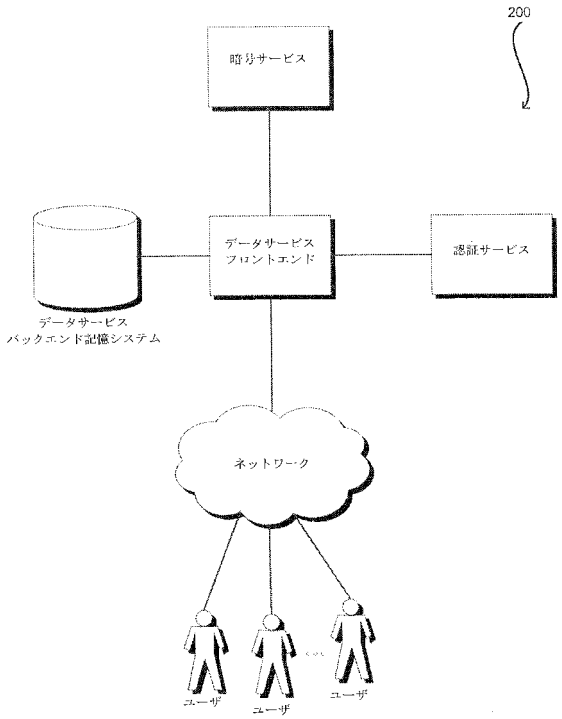
【０１４７】

本明細書において引用される出版物、特許出願、及び特許を含むすべての参照文献は、各参照文献が参照により組み込まれるように個別かつ特定的に示され、その全体が本明細書内に記載されるのと同じ程度に、参照により本明細書内に組み込まれる。

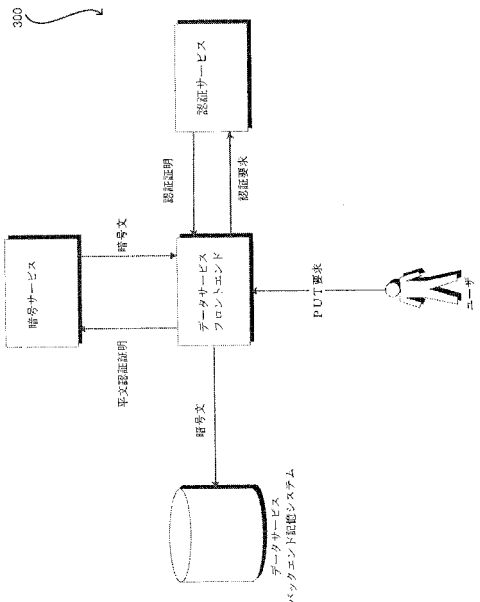
【図１】


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

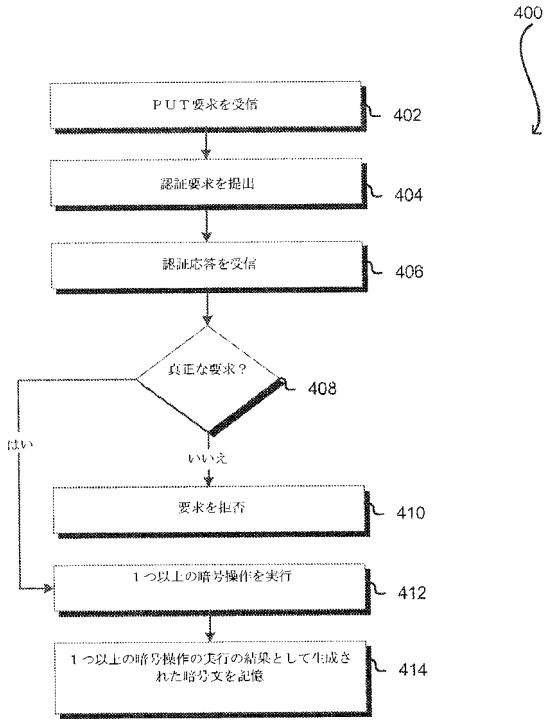
【図２】


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
バックエンド記憶システム
ネットワーク
ユーザ
ユーザ
ユーザ

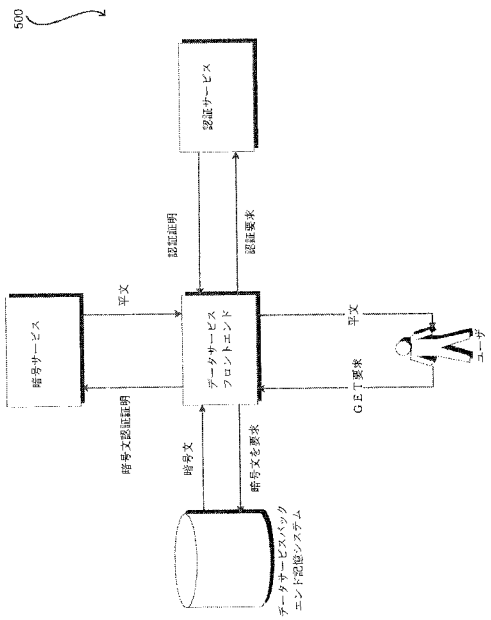
【図３】


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
バックエンド記憶システム

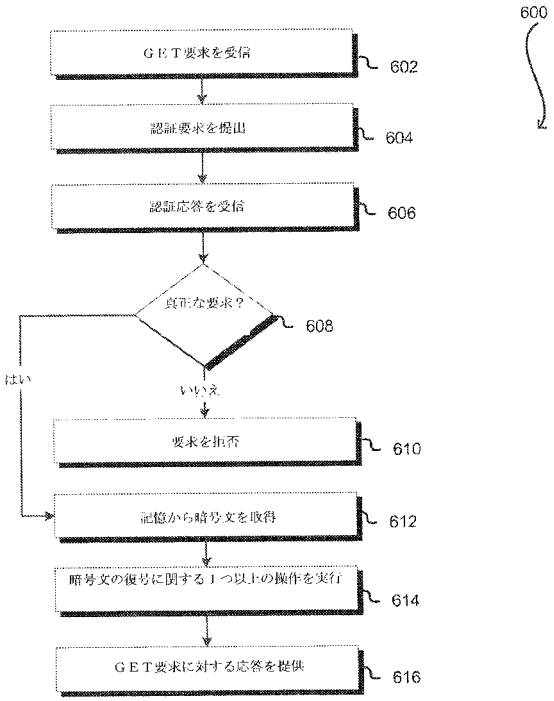
【図４】


400
PUT要求を受信
402
認証要求を提出
404
認証応答を受信
406
真正な要求？
408
はい
いいえ
要求を拒否
410
１つ以上の暗号操作を実行
412
１つ以上の暗号操作の実行の結果として生成された暗号文を記憶
414

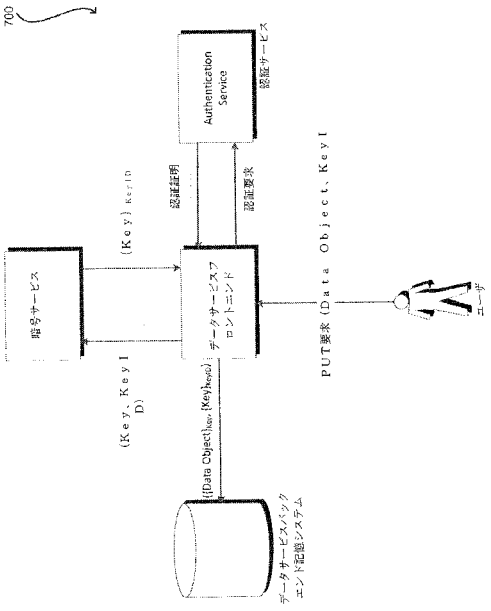
【図５】


500
認証サービス
認証証明
認証要求
平文
暗号サービス
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 エンド記憶システム

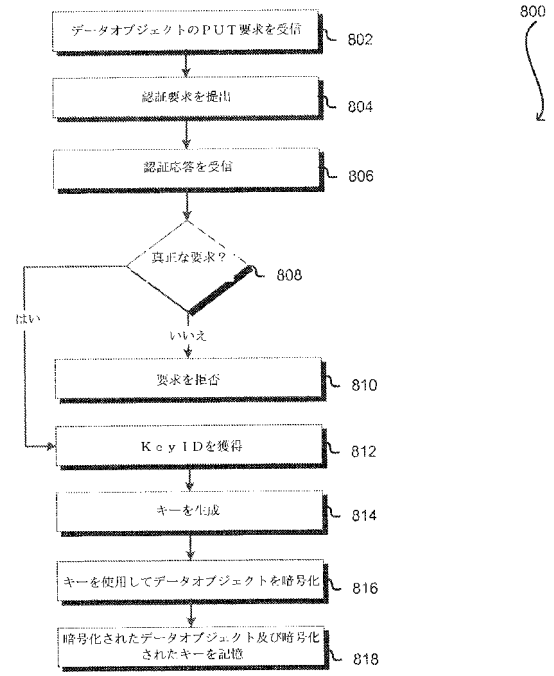
【図６】


600
GET要求を受信
602
認証要求を提出
604
認証応答を受信
606
真正な要求？
608
はい
いいえ
要求を拒否
610
記憶から暗号文を取得
612
暗号文の復号に関する１つ以上の操作を実行
614
GET要求に対する応答を提供
616

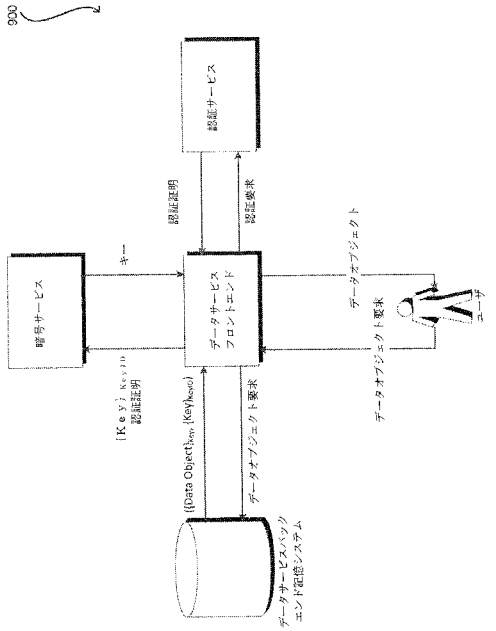
【図７】


700
Authentication Service
認証サービス
認証証明
認証要求
(Key) KeyID
暗号サービス
データサービス フロントエンド
PUT要求 (Data Object, KeyI
ユーザ
(Key, KeyID)
(IData Object)Key (Keyhash)
データサービスバック エンド記憶システム

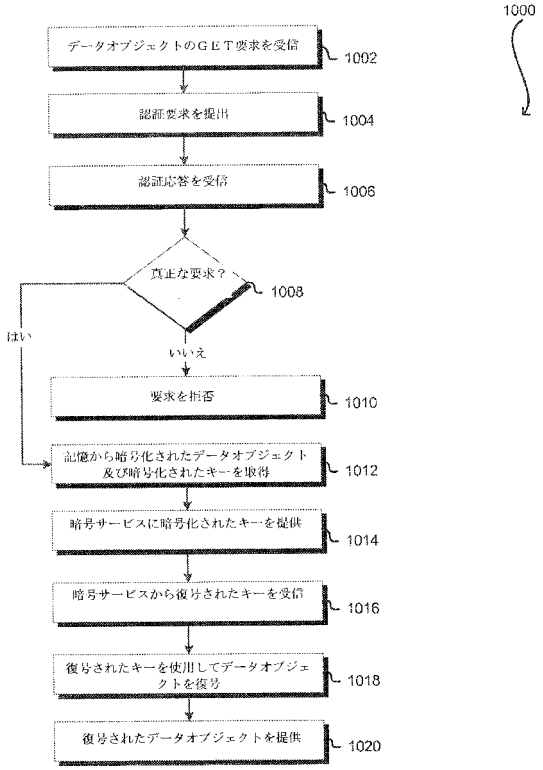
【図８】


800
データオブジェクトのPUT要求を受信
802
認証要求を提出
804
認証応答を受信
806
真正な要求？
808
はい
いいえ
要求を拒否
810
KeyIDを獲得
812
キーを生成
814
キーを使用してデータオブジェクトを暗号化
816
暗号化されたデータオブジェクト及び暗号化されたキーを記憶
818

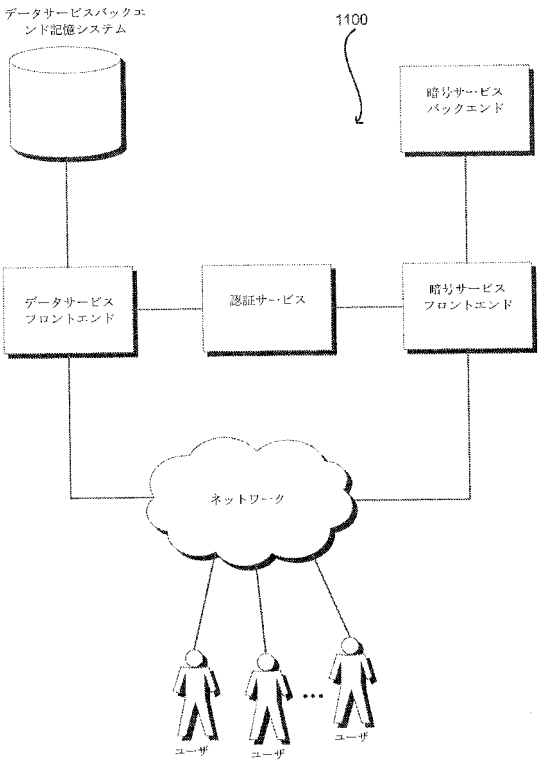
【図９】



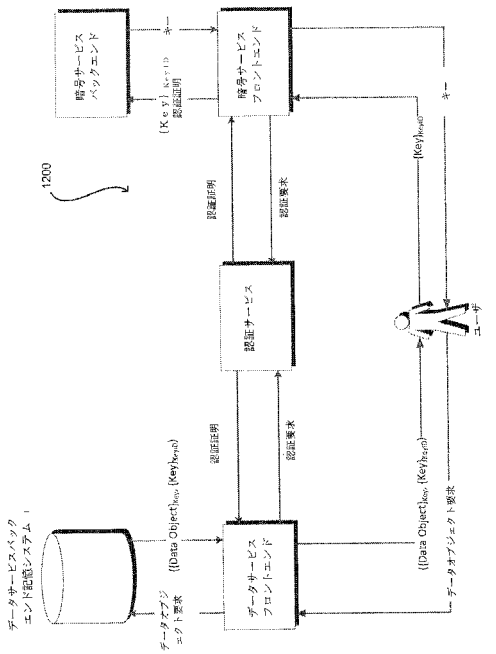
【図１０】



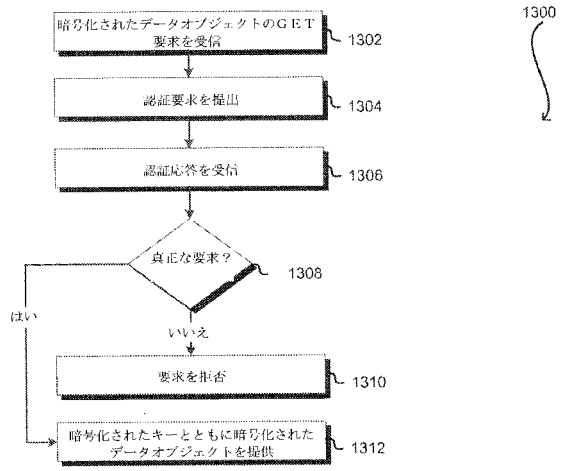
【図１１】



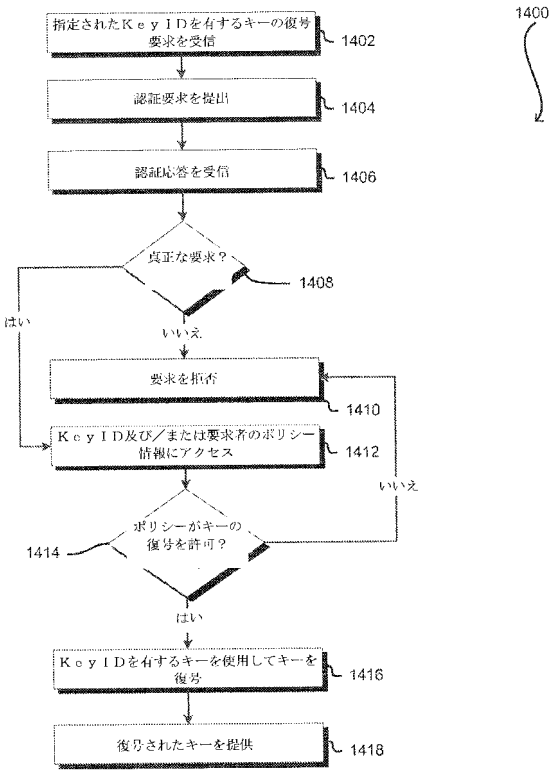
【図１２】



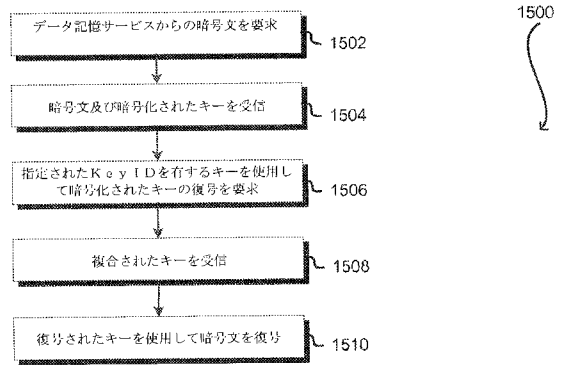
【図１３】



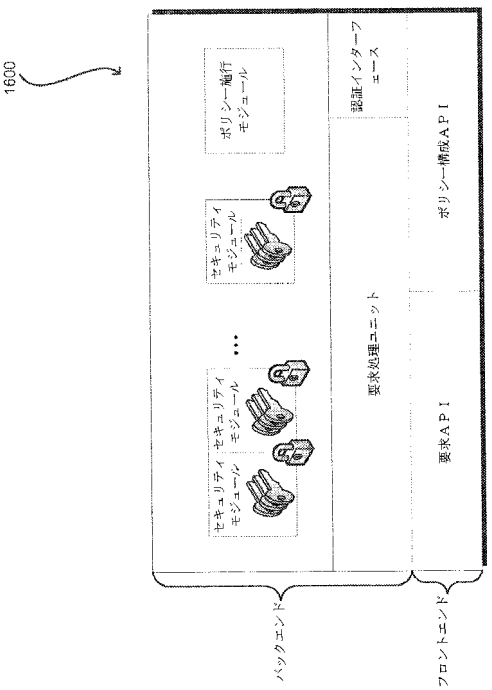
【図１４】



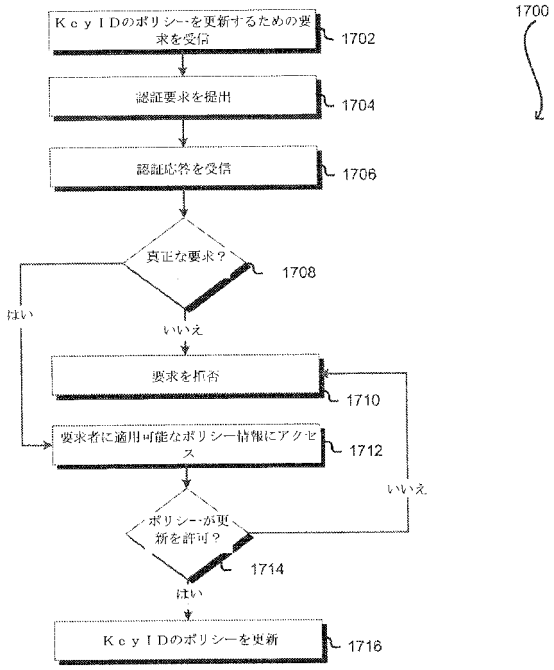
【図１５】



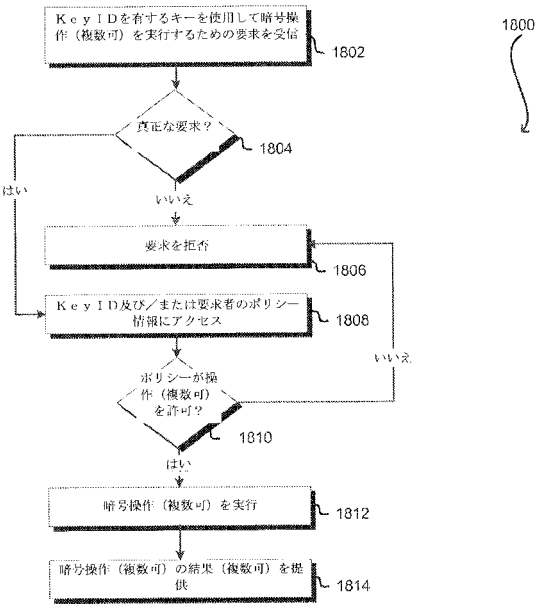
【図１６】



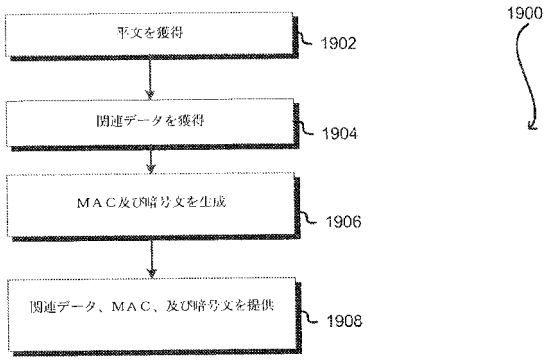
【図１７】



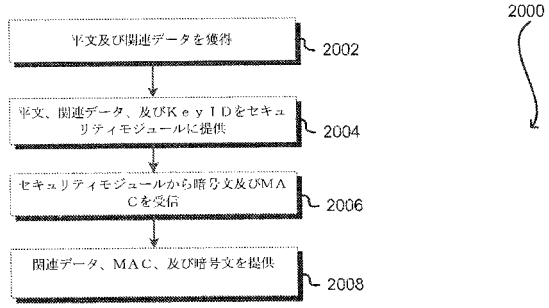
【図１８】



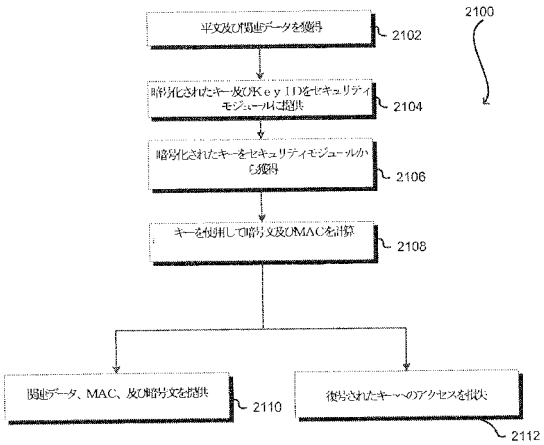
【図１９】



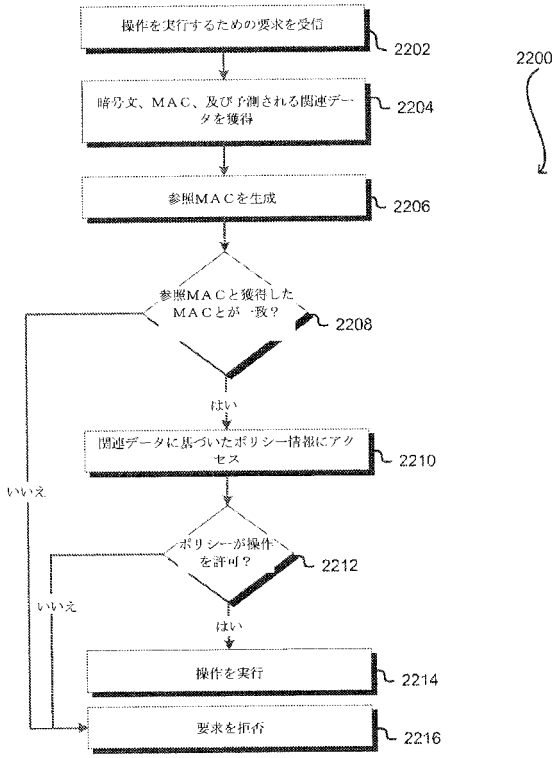
【図２０】



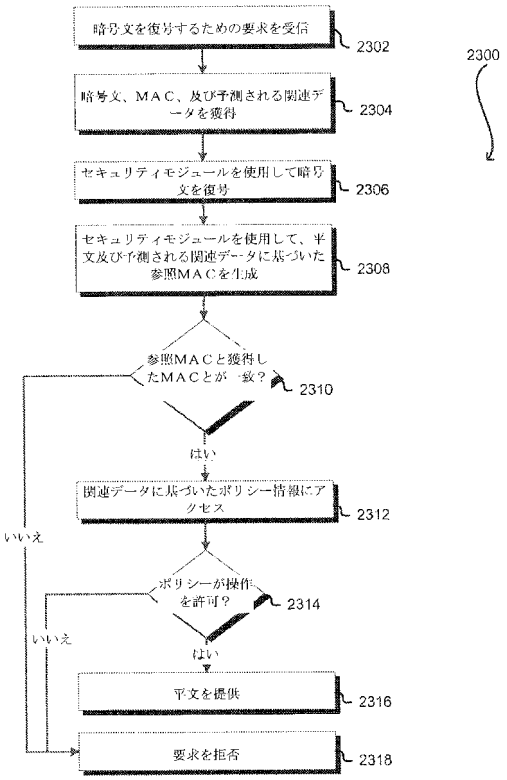
【図２１】



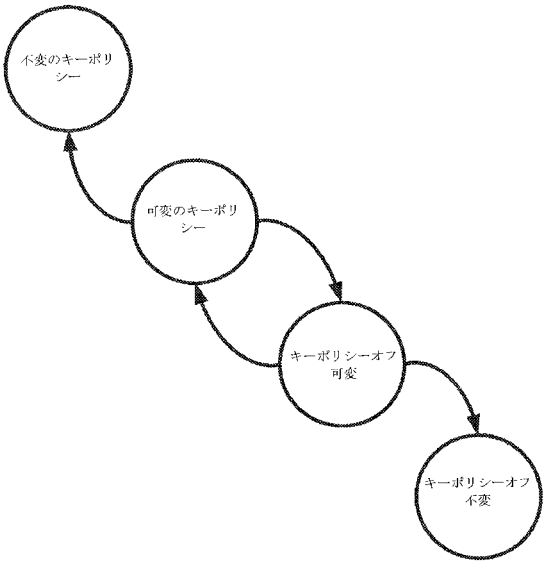
【図２２】



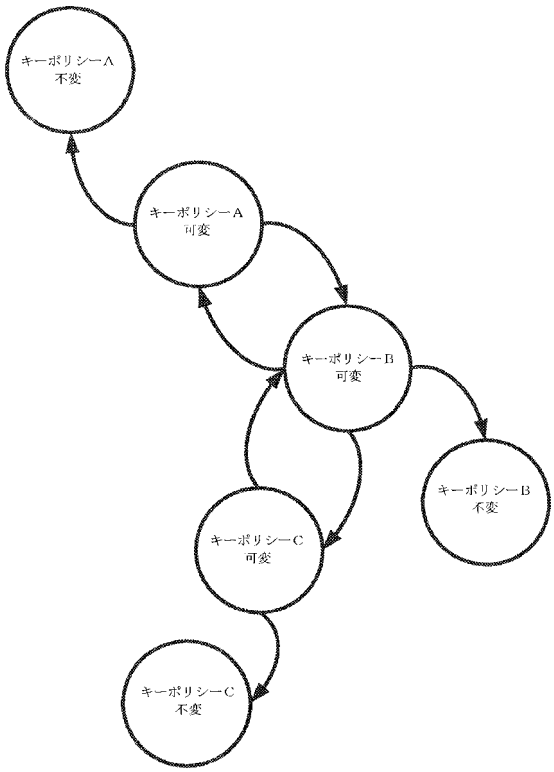
【図２３】



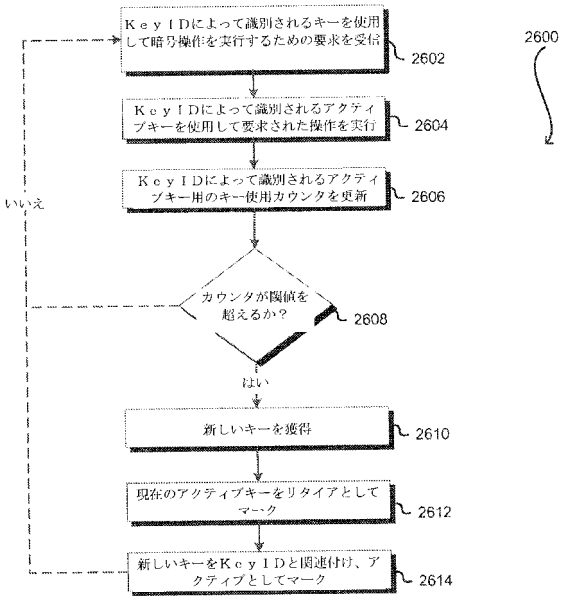
【図２４】



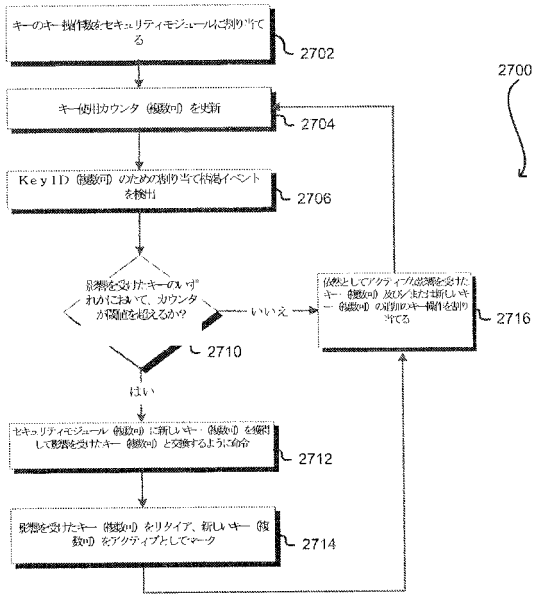
【図２５】



【図２６】



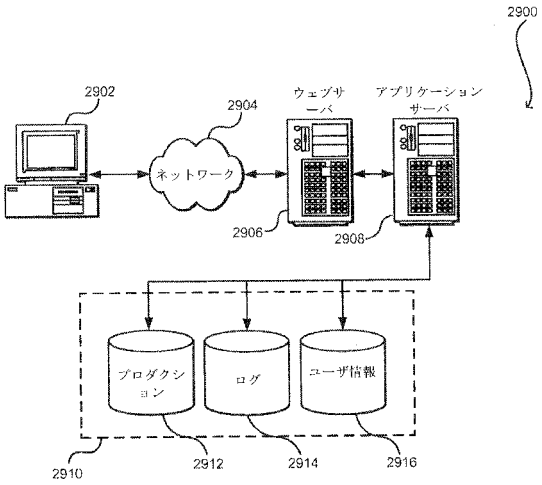
【図２７】



【図２８】

KeyID	キーバージョン	ユーザビリティ	カウンタ
⋮	⋮	⋮	⋮
31415926	1	リタイア	4294967296
31415926	2	リタイア	4294967296
31415926	3	リタイア	4294967296
31415926	4	アクティブ	1048576
31415927	1	アクティブ	2097152
⋮	⋮	⋮	⋮

【図２９】



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

Ｆターム(参考) 5J104 AA08　AA33　LA02　PA07