(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6430968号
(P6430968)

(45)発行日　平成30年11月28日(2018.11.28)　(24)登録日　平成30年11月9日(2018.11.9)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　　H04L 9/00 601B
H04L 9/32 (2006.01)　　H04L 9/00 675A
H04L 9/00 675B

請求項の数 14　(全 65 頁)

(21)出願番号　特願2015-558056(P2015-558056)
(86)(22)出願日　平成26年2月7日(2014.2.7)
(65)公表番号　特表2016-511995(P2016-511995A)
(43)公表日　平成28年4月21日(2016.4.21)
(86)国際出願番号　PCT/US2014/015414
(87)国際公開番号　WO2014/126816
(87)国際公開日　平成26年8月21日(2014.8.21)
審査請求日　平成27年10月6日(2015.10.6)
(31)優先権主張番号　13/765,239
(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)

前置審査

(73)特許権者　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】遅延データアクセス

(57)【特許請求の範囲】
【請求項１】
コンピュータ実装方法であって、
平文にアクセスするためのアクセス要求を第１のユーザから受信することであって、その遂行が１つ以上の暗号動作を要求する、前記受信することと、
前記アクセス要求の遂行に対応する、前記アクセス要求への応答が提供される前に、所定の遅延が要求されるように、前記アクセス要求を処理することと、
前記所定の遅延後に前記アクセス要求への応答を提供することと、
を含み、
前記アクセス要求は、所定の時間が経過する前に、中止要求に応答して中止可能である
前記コンピュータ実装方法。
【請求項２】
前記１つ以上の暗号動作が暗号文の解読を含む、請求項１に記載の前記コンピュータ実装方法。
【請求項３】
前記１つ以上の暗号動作が電子署名を生成することを含む、請求項１または２に記載の前記コンピュータ実装方法。
【請求項４】
暗号文を解読するための鍵に対応するポリシーの結果として、前記所定の遅延が要求される、請求項１～３のいずれか一項に記載の前記コンピュータ実装方法。

【請求項５】
前記アクセス要求を中止する権限を有する１つ以上のエンティティに、前記アクセス要求の１つ以上の通知を送信することをさらに含む、請求項１～４のいずれか一項に記載の前記コンピュータ実装方法。
【請求項６】
前記所定の遅延の間に前記アクセス要求を中止する能力を可能にすることをさらに含む、請求項５に記載の前記コンピュータ実装方法。
【請求項７】
認証された前記アクセス要求が、前記アクセス要求が中止されない限り、前記応答を提供させるのに十分である、請求項１～６のいずれか一項に記載の前記コンピュータ実装方法。
【請求項８】
前記アクセス要求の結果として、増加した監査を引き起こすことをさらに含む、請求項１～７のいずれか一項に記載の前記コンピュータ実装方法。
【請求項９】
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、
前記１つ以上のプロセッサによって実行されると、前記コンピュータシステムに、
平文にアクセスするためのアクセス要求を第１のユーザから受信することであって、その遂行が１つ以上の暗号動作を要求する、前記受信することと、
前記アクセス要求の遂行に対応する、前記アクセス要求への応答が提供される前に、所定の遅延が要求されるように、前記アクセス要求を処理することと、
前記所定の遅延後に前記アクセス要求への応答を提供することと、
を行わせる命令を含む、メモリと、
を備え、
前記アクセス要求は、所定の時間が経過する前に、中止要求に応答して中止可能である
前記コンピュータシステム。
【請求項１０】
前記コンピュータシステムがメッセージングサブシステムをさらに備え、
前記命令が、前記コンピュータシステムに、前記メッセージングサブシステムに前記アクセス要求の通知を伝送させることを、さらに行わせる、請求項９に記載の前記コンピュータシステム。
【請求項１１】
前記所定の遅延が前記１つ以上の暗号動作のために要求される鍵に関するポリシーの結果として要求される、請求項９または１０に記載の前記コンピュータシステム。
【請求項１２】
前記コンピュータシステムが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、
前記アクセス要求が、前記コンピューティングリソースプロバイダの顧客から前記コンピューティングリソースプロバイダによって受信される、請求項９～１１のいずれか一項に記載の前記コンピュータシステム。
【請求項１３】
前記命令がさらに、前記コンピュータシステムに前記１つ以上の暗号動作を実行させる、請求項９～１２のいずれか一項に記載の前記コンピュータシステム。
【請求項１４】
前記１つ以上の暗号動作が鍵を使用し、
前記所定の遅延が、前記アクセス要求が前記所定の時間の間中止可能であることを要求する、前記鍵についてのポリシーの結果として要求される、請求項９～１３のいずれか一項に記載の前記コンピュータシステム。
【発明の詳細な説明】

【背景技術】
【０００１】
（関連出願の相互参照）
本出願は、２０１３年2月１２日出願の米国特許出願番号１３／７６５，２３９の優先権を主張するものであり、その内容は、参照によりその全体が本明細書内に組み込まれる。本出願は、本出願と同時に出願された同時係属中の米国特許第１３／７６４，９４４号、表題「ＡＵＴＯＭＡＴＩＣ　ＫＥＹ　ＲＯＴＡＴＩＯＮ」、本出願と同時に出願された同時係属中の米国特許第１３／７６４，９６３号、表題「ＤＡＴＡ　ＳＥＣＵＲＩＴＹ　ＳＥＲＶＩＣＥ」、本出願と同時に出願された同時係属中の米国特許第１３／７６５，０２０号、表題「ＤＡＴＡ　ＳＥＣＵＲＩＴＹ　ＷＩＴＨ　Ａ　ＳＥＣＵＲＩＴＹ　ＭＯＤＵＬＥ」、本出願と同時に出願された同時係属中の米国特許第１３／７６４，９９５号、表題「ＰＯＬＩＣＹ　ＥＮＦＯＲＣＥＭＥＮＴ　ＷＩＴＨ　ＡＳＳＯＣＩＡＴＥＤ　ＤＡＴＡ」、本出願と同時に出願された同時係属中の米国特許第１３／７６５，２０９号、表題「ＦＥＤＥＲＡＴＥＤ　ＫＥＹ　ＭＡＮＡＧＥＭＥＮＴ」、本出願と同時に出願された同時係属中の米国特許第１３／７６４，９６３号、表題「ＤＡＴＡ　ＳＥＣＵＲＩＴＹ　ＳＥＲＶＩＣＥ」、及び本出願と同時に出願された同時係属中の米国特許第１３／７６５，２８３号、表題「ＳＥＣＵＲＥ　ＭＡＮＡＧＥＭＥＮＴ　ＯＦ　ＩＮＦＯＲＭＡＴＩＯＮ　ＵＳＩＮＧ　Ａ　ＳＥＣＵＲＩＴＹ　ＭＯＤＵＬＥ」の全開示を、参照により全ての目的のために組み込む。
【０００２】
本開示に従う様々な実施形態が、図面を参照して説明され得る。
【図面の簡単な説明】
【０００３】
【図１】様々な実施形態に従う本開示の様々な態様を表す例示的な図を示す。
【図２】本開示の様々な態様が実装され得る環境の例示的な実施例を示す。
【図３】少なくとも１つの実施形態に従う、本開示の様々な態様が実装され得る環境の例示的な実施例と、環境の様々な構成要素の間の情報の流れの実施例と、を示す。
【図４】少なくとも１つの実施形態に従う、暗号文を格納するための例示的なプロセスのステップの実施例を示す。
【図５】少なくとも１つの実施形態に従う、本開示の様々な態様が実装され得る環境の例示的な実施例と、環境の様々な構成要素の間の情報の流れの実施例と、を示す。
【図６】少なくとも１つの実施形態に従う、データを読み出すための要求に応答するための例示的なプロセスのステップの実施例を示す。
【図７】少なくとも１つの実施形態に従う、本開示の様々な態様が実装され得る環境の例示的な実施例と、環境の様々な構成要素の間の情報の流れの実施例と、を示す。
【図８】少なくとも１つの実施形態に従う、データを格納するための要求に応答するための例示的なプロセスのステップの実施例を示す。
【図９】少なくとも１つの実施形態に従う、本開示の様々な態様が実装され得る環境の例示的な実施例と、環境の様々な構成要素の間の情報の流れの実施例と、を示す。
【図１０】少なくとも１つの実施形態に従う、データを読み出すための要求に応答するための例示的なプロセスのステップの実施例を示す。
【図１１】本開示の様々な態様が実装され得る環境の例示的な実施例を示す。
【図１２】少なくとも１つの実施形態に従う、本開示の様々な態様が実装され得る環境の例示的な実施例と、環境の様々な構成要素の間の情報の流れの実施例と、を示す。
【図１３】少なくとも１つの実施形態に従う、データを読み出すための要求に応答するための例示的なプロセスのステップの実施例を示す。
【図１４】少なくとも１つの実施形態に従う、データを解読するための要求に応答するための例示的なプロセスのステップの実施例を示す。
【図１５】少なくとも１つの実施形態に従う、解読されたデータを得るための例示的なプロセスのステップの実施例を示す。

【図１６】少なくとも１つの実施形態に従う、暗号サービスの実施例の図表示を示す。
【図１７】少なくとも１つの実施形態に従う、ポリシーを構成するための例示的なプロセスのステップの実施例を示す。
【図１８】少なくとも１つの実施形態に従う、ポリシーを実施しながら暗号動作を実行するための、例示的なプロセスのステップの実施例を示す。
【図１９】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実施例を示す。
【図２０】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にセキュリティモジュールを使用する例示的な実施例を示す。
【図２１】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に使用される鍵を暗号化するためにセキュリティモジュールを使用する例示的な実施例を示す。
【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実施するためのプロセスの例示的な実施例を示す。
【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実施するためのプロセスの例示的な実施例を示す。
【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実施例を示す。
【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実施例を示す。
【図２６】少なくとも１つの実施形態に従う、鍵を自動的に回転させるためのプロセスの例示的な実施例を示す。
【図２７】少なくとも１つの実施形態に従う、鍵を自動的に回転させるためのプロセスの例示的な実施例を示す。
【図２８】少なくとも１つの実施形態に従う、鍵の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実施例を示す。
【図２９】様々な実施形態が実装され得る環境の例示的な実施例を示す。
【図３０】少なくとも１つの実施形態に従う、鍵に関連付けられ得る情報の図表示を示す。
【図３１】少なくとも１つの実施形態に従う、要求に関連して含まれ得る鍵アクセス注釈の図表示を示す。
【図３２】少なくとも１つの実施形態に従う、要求を処理するためのプロセスの例示的な実施例を示す。
【図３３】少なくとも１つの実施形態に従う、要求を処理するためのプロセスの例示的な実施例を示す。
【図３４】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】
【０００４】
以下の説明において、様々な実施形態が説明される。説明の目的で、実施形態の徹底的な理解を提供するために具体的な構成及び詳細が述べられる。しかしながら、当業者には、実施形態がその具体的な詳細を伴わずに実践され得るということもまた明らかになるであろう。さらに、公知の特徴は、説明される実施形態を不明瞭にしないために、省略または簡素化され得る。
【０００５】
本明細書に記載及び提案される技術は、分散コンピューティングリソースを含む環境における、強化されたデータセキュリティを可能にする。一実施例では、分散コンピューティング環境は、適切なコンピューティングリソースによって実装され得る１つ以上のデータサービスを含む。データサービスは、様々な動作がデータに関連して実行されることを可能にし得る。１つの例示的な実施例としては、分散コンピューティング環境は１つ以上のデータ格納サービスを含む。電子要求がデータ格納サービスに伝送され、データ格納動作を実行し得る。動作の例は、データ格納サービスを使用してデータを格納すること、及

びデータ格納サービスを使用してデータ格納サービスによって格納されたデータを読み出すことである。データ格納サービスを含むデータサービスは、データを操作する動作もまた実行し得る。例えば、いくつかの実施形態では、データ格納サービスはデータを暗号化することができる。

【０００６】

本開示の様々な実施形態は、適切なコンピューティングリソースを使用して実装される暗号サービスを含む、分散コンピューティング環境を含む。暗号サービスは、平文の暗号化及び暗号文の解読等の、暗号動作を実行するための電子要求を受信してそれに応答する、分散システムによって実装され得る。いくつかの実施形態では暗号サービスは鍵を管理する。暗号動作を実行するための要求に応答して、暗号サービスは管理される鍵を使用する暗号動作を実行し得る。例えば、暗号サービスは、受信された要求に応答して、暗号動作を実行するための適切な鍵を選択して、暗号動作を実行して、暗号動作の１つ以上の結果を提供することができる。代替の構成では、暗号サービスはエンベロープ鍵（例えば具体的なデータアイテムを暗号化するために使用されるセッション鍵）を生成して、そのエンベロープ鍵をシステムに戻し、サービスの暗号動作を発動することができる。システムは、その後エンベロープ鍵を使用して暗号動作を実行することができる。

【０００７】

いくつかの実施形態では、暗号サービスはコンピューティングリソースサービスプロバイダの複数のテナントの鍵を管理する。コンピューティングリソースのテナントは、コンピューティングリソースプロバイダの顧客として動作するエンティティ（例えば組織または個人）であり得る。顧客は、コンピューティングリソースプロバイダによって物理的にホストされるリソースを、遠隔的にかつプログラムで構成して動作させ得る。顧客が暗号サービスに、暗号動作を実行するための要求を提出するとき（またはエンティティが暗号サービスに要求を提出するとき）、暗号サービスは、顧客のために、暗号サービスによって管理される鍵を選択して、暗号動作を実行する。暗号サービスによって管理される鍵は、他のユーザ及び／またはデータサービスは、他人が鍵へのアクセスを有さないように、安全に管理され得る。あるエンティティ（例えば、ユーザ、顧客、サービス）による別のエンティティの鍵へのアクセスの欠如は、そのエンティティが他人の鍵を得る許可された方法を有さないということ、及び／または、そのエンティティが、そのエンティティの方向で鍵を使用する他人の鍵を管理するシステムを行わせる許可された方法を有さないということ、を意味し得る。例えば、暗号サービスは、顧客、他の顧客の両方が、顧客の鍵（複数可）へのアクセスを有さず、かつ、暗号サービスに、顧客の鍵（複数可）を使用して暗号動作を実行させることができないように、鍵を管理し得る。別の実施例として、暗号サービスは、データ格納サービス等の他のサービスが、暗号サービスがいくつかまたは全ての鍵を使用して、暗号動作を実行させることができないように、鍵を管理し得る。鍵への許可なしのアクセスは、例えば許可なしのアクセスが困難または不可能になるように、適切なセキュリティ手段によって防止され得る。困難は、コンピュータ使用上非実用的である及び／またはアクセスが得られるために非許可（例えば、違法、不法、及び／または許可証明の危殆化等の別様で許可されないもの）が生じる必要性によるものであり得る。様々な実施形態に従うシステムは、鍵へのアクセスを得るための、コンピュータ非実用性の客観的尺度を保証するように構成され得る。かかる尺度は、例えば時間量に関して測定され、平均では、鍵への許可されたアクセスのために必要とされる、暗号化された情報をクラッキングするために、コンピュータ能力の画定されたユニット（例えば時間の単位当たりの特定の動作）を有するコンピュータを取り得る。

【０００８】

述べられたように、暗号サービスは、コンピューティングリソースプロバイダの顧客等の様々なエンティティから要求を受信し得る。暗号サービスは、コンピューティングリソースプロバイダの内部のエンティティからもまた要求を受信し得る。例えば、いくつかの実施形態では、コンピューティングリソースプロバイダによって実装されるデータサービスは、暗号サービスに暗号動作を実行させるために、暗号サービスに要求を伝送し得る。

一実施例としては、顧客は、データ対象を格納するために、データ格納サービスに要求を伝送し得る。要求は、データ対象が格納されるときに暗号化されなければならないということを示し得る。データ格納サービスは、暗号動作を実行するために、暗号サービスに要求を通信し得る。暗号動作は、例えば、データ格納サービスによって使用される鍵を暗号化してデータ対象を暗号化することであり得る。暗号動作は、データ対象自体の暗号化であり得る。暗号動作は、データ対象を暗号化するためにデータ格納サービスが使用することができる、エンベロープ鍵を生成することであり得る。

【０００９】

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

【００１０】

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

【００１１】

本開示の様々な実施形態は、鍵に関連付けられるポリシーの実施に関し、ここにおいて鍵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等の、暗号サービスのユーザは、暗号サービスによって実施されるべき鍵のポリシーを特定し得る。ポリシーは、だれが鍵を使用するために暗号サービスを指揮することができるか、それを実行するために鍵が使用され得る動作、その鍵が使用され得る状況、及び／または他の鍵の使用に関連する制限及び／または特権をコードし得る。

【００１２】
一実施形態では、暗号文に関連付けられるデータがポリシーの実施において使用される。暗号文に関連付けられるデータは、高度暗号化標準（ＡＥＳ）のモード等の暗号の使用を通して得ら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するデータを含み得る。暗号アルゴリズムは、鍵を使用して平文を暗号し、関連データが変更されたかどうかの判断を可能にするメッセージ認証コード（ＭＡＣ）等の認証出力を提供し得る。認証出力は、関連データ及び平文に少なくとも部分的に基づいて判断され得る。
【００１３】
ポリシー実施は、関連データに少なくとも部分的に基づき得る。例えば、いくつかのポリシーは、解読された暗号文（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要求し得る。認証出力（例えばＭＡＣ）は、関連データが変更されていないこと、及びよってポリシーの実施が正確に実行されるということを保証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、データ自体はポリシーによって明示的にまたは暗黙的に特定され得る。例えば、ポリシーは、解読された暗号文（平文）が、暗号文を解読するための要求が、暗号文を暗号化するために使用される関連データにおいてコードされるユーザ識別子を有するユーザによって提出される場合にのみ、提供され得るということを特定し得る。このようにして、別のユーザが暗号文の解読を要求する場合（ユーザ識別子を有するユーザに扮することなく）、要求は、ポリシーとの衝突により遂行され得ない。別の実施例として、ポリシーは、解読された暗号文が、暗号文が特定の情報でタグ付けされる場合にのみ、提供され得るということを述べ得る。さらに別の実施例として、ポリシーは、解読された暗号文が、平文のハッシュ、暗号文のハッシュ、または他の特定の値と同一のの関連データでタグ付けされる場合に、提供され得るということを述べ得る。概して、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に関する豊かなポリシー実施を可能にする。いくつかの実施形態では、関連データはそれ自体でポリシーを表すことができる。
【００１４】
本開示の様々な実施形態は、鍵の使用に関するポリシーもまた可能にする。例えば、いくつかの実施形態では、鍵は自動的に回転し、鍵を明らかにし得る暗号化攻撃の成功を可能にするために十分な時間使用されることを防止する。鍵が可能性のあるセキュリティ違反をもたらすことに十分な時間使用されることを防止するために、暗号サービスまたは鍵を利用する他のシステムは、鍵を用いて実行される動作を追跡し得る。鍵識別子（鍵ＩＤ）によって識別される鍵が、動作の閾値回数使用される場合、その鍵は退役して（例えば将来の暗号動作には使用不可能であるが、将来の解読動作には使用可能である）、その鍵ＩＤによって識別される新鍵と交換され得る。この様式で、新鍵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は透過的な様式で、かかる鍵回転を実行する。一実施例として、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、鍵ＩＤによって識別される鍵を使用して動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、鍵回転を実行するためのエンティティからの任意の要求から独立して、鍵回転を実行し得る。顧客または他のエンティティの視点から見ると、要求は、鍵が退役して新鍵と交換されたことにより必要な、再プログラミングまたは他の再構成を伴わずに、特定される鍵ＩＤを使用してなお提出され得る。
【００１５】
いくつかの実施形態では、暗号化または他のサービスを同時に支持する複数のシステムが、鍵へのアクセスを有し、暗号動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、そのうちの少なくともいくつかは１つ以上の鍵を重複して格納する。サービスは動作をセキュリティモジュールに割り当て、それ自体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、割り当てられた数の動作を、鍵を使用して実行する）とき、サービスは、鍵がまだ使用可能であるかどうかまたは鍵が退役すべきかどうかを点検

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、鍵を使用して、暗号化、解読、電子署名生成等の、複数の種類の動作を実行するように構成され得るということに留意すべきである。いくつかの実施形態では、全ての種類の動作が、セキュリティモジュールに動作の割り当ての一部を使用させるわけではない。例えば、解読動作は、割り当てられた動作が使用されることをもたらさないことがあり、一方で、暗号動作は、割り当てられた動作が使用されることをもたらすことがある。概して、様々な実施形態では、新しい情報（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動作は、割り当てられた動作が使用されることをもたらすことがあり、一方で、新しい情報の生成をもたらさない暗号動作は、割り当てられた動作が使用されることをもたらさないことがある。さらに、異なる種類の動作は、実行される暗号動作の異なる数をもたらし得る。一実施例として、平文の暗号化は、平文の大きさに少なくとも部分的に基づいて、要求される暗号動作の量において変動し得る。例えば、ブロック暗号の使用は、割り当てられた暗号動作が、生成された暗号文のそれぞれのブロックのために使用されることを引き起こし得る。

【００１６】

鍵に使用可能な動作の合計数がなお使用可能である場合、サービスはセキュリティモジュールに追加の動作を割り当て得る。鍵が退役すべき場合（例えばカウンタがそのように示すため）は、サービスは、鍵を重複して格納するセキュリティモジュールに、鍵を退役させて新鍵と交換させ得、ここにおいて、新鍵は、あるセキュリティモジュールによって生成されるまたは他の方法で得られ得、残りのセキュリティモジュールに安全に渡され得る。いくつかの実施形態では、代わりに、他のセキュリティモジュールがより古い鍵下でそれらの割り当てられた動作を全て使用する。セキュリティモジュールが、誤動作する、動作不能になる、意図的にオフラインにされる（例えばメンテナンスのために）、及び／または他の方法で、１つ以上の鍵を使用していくつの動作を実行したかに関する情報を提供せずに、暗号動作を実行するために使用不能になる場合、サービスは、使用不能性をその割り当ての使用として扱い得る。例えば、セキュリティモジュールが１組の鍵のうちのそれぞれの鍵の１００万の動作に割り当てられ、かつセキュリティモジュールが動作不能になる場合、サービスは、セキュリティモジュールが鍵の組のそれぞれの１００万の動作を実行したかのように動作し得る。例えば、サービスは、それに応じてカウンタを調節して、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追加の動作を割り当て得、及び／または、対応するカウンタが、交換が必要であると示す場合、鍵の１つ以上が退役して交換されることを引き起こし得る。

【００１７】

本開示の実施形態は、注釈及び／または連合鍵管理技術によって、強化されたデータセキュリティを可能にもする。いくつかの実施形態では、サービスに提出される要求（暗号サービスまたは他のデータサービス等）は、ポリシーの実施を可能にする情報を含む注釈（鍵アクセス注釈とも称される）を、含み得るかまたは別様でそれに関連付けられ得る。一実施形態では、鍵アクセス注釈は、対応する要求が遂行され得る前に、１つ以上の条件を満たさなければならない。いくつかの実施形態では、１つ以上の条件は、注釈が鍵ＩＤに関連付けられる鍵を使用して電子署名されるという条件を含み、ここにおいて、鍵ＩＤは要求を遂行するために使用可能である異なる鍵を識別する。有効な電子署名の存在は、注釈内の情報が修正されていないことを示し、かつ電子署名を生成するために使用される鍵の所有を証明もする。

【００１８】

いくつかの実施形態では、鍵アクセス注釈は、要求を遂行するために使用可能な鍵の保持者の識別子を含み得る。鍵の保持者は、要求を受信するシステムをホストするエンティティであり得、または第三者のシステム等の別のシステムであり得る。要求を受信するシステムは、識別子の存在を検出し得、識別子に応じて適切なように、自体で要求を処理し得、または処理のために要求を識別された鍵保持者に伝送し得る。要求を受信するエンティティ及び／または鍵保持者は、上記及び本明細書の他の箇所で記載するような、ポリシ

ーの実施のための電子署名を検証し得る。例えば、電子署名が有効でない場合、要求の受信者はその要求を注釈において識別される鍵保持者に渡すことができない。同様に、鍵保持者が、電子署名が無効であると判断する場合、鍵保持者は要求を拒否し得る。要求を受信するエンティティ及び鍵保持者は、同じ電子署名を検証し得、または、いくつかの実施形態では、要求は、１つは要求の受信者のもの及び１つは鍵保持者のものの、少なくとも２つの署名を含む。それぞれの署名は、署名を検証することを意図されるエンティティに対応する鍵を使用して生成され得る。

【００１９】

本開示の実施形態は、特定の種類の要求が遂行される前に、強制された遅延を通して、強化されたデータセキュリティを可能にもする。例えば、いくつかの実施形態では、特定のデータの解読は、対応する要求に応答得して平文が提供される前に、遅延を要求する。遅延の間、情報を解読するための保留中の要求の関係者に通知するために、様々な行動が取られ得る。このようにして、関係者（例えば組織の法令順守責任者または平文が提供されることを許可することが許可される他の人）に、平文が提供される前に要求を中止する機会が提供される。様々な実施形態では、要求は容易に中止される。例えば、要求を中止するための要件は、要求が遂行されるための要件よりも緊縮ではないことがある。この様式で、非許可データ漏洩は、容易に検出可能かつ／または防止可能である。

【００２０】

図１は、本開示の様々な実施形態を実証する、例示的な図１００である。一実施形態では、暗号サービスは、１つ以上の暗号アルゴリズムに従う１つ以上の計算の適用を含み得る暗号動作を実行する。図１に例示されるように、暗号サービスは、ユーザまたはサービスが暗号文から平文を生成することができるようにする。構成の実施例では、暗号サービスは、鍵を暗号化／解読するために使用され得、かつこれらの鍵は、データ格納サービス内に格納されるデータ等のデータを暗号化／解読するために使用され得る。例えば、暗号サービスは、鍵下で暗号化された暗号文から平文を生成するための要求を受信する。暗号サービスは、要求者が許可されたエンティティであることを判定し、マスター鍵を使用して鍵を解読し、解読された鍵をサービスに戻し、これは、解読された鍵を使用して暗号文から平文を生成することができる。別の構成では、暗号サービスは暗号文を受信して、受信された暗号文を、暗号サービスによりサービスとして提供される平文へと処理する。この実施例では、暗号文は、暗号サービスを動作させるコンピューティングリソースプロバイダの顧客であり得る、及び／または、コンピューティングリソースプロバイダの別のサービスであり得る、許可されたエンティティから、暗号サービスへの電子要求の一部として、暗号サービスに提供され得る。図１に例示される暗号サービスは、１つ以上の暗号的に強いアルゴリズムを利用してデータを暗号化し得る。かかる暗号的に強いアルゴリズムは、例えば、高度暗号化標準（ＡＥＳ）、Ｂｌｏｗｆｉｓｈ、データ暗号化標準（ＤＥＳ）、トリプルＤＥＳ、Ｓｅｒｐｅｎｔ、またはＴｗｏｆｉｓｈを含み得、かつ、選択される具体的な実装に依存して、非対称性または対称性鍵システムのいずれかであり得る。概して、暗号サービスは、任意の暗号及び／もしくは解読アルゴリズム（暗号）、または暗号サービスによって管理されるデータを利用するアルゴリズムの組み合わせを利用し得る。

【００２１】

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

も文字情報を含まないが、文字情報を含んでよい。例えば、図１に例示されるように、計画文及び暗号文は、ビットの配列を含む。平文及び暗号文は、他の方法でならびに暗号化及び解読がコンピュータシステムによって実行され得る任意の様式でもまた表され得る。

【００２２】

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

【００２３】

一実施形態における認証サービスは、ユーザの認証に関与する動作を実行するように構成されるコンピュータシステムである。例えば、データサービスフロントエンドは、ユーザからの情報を認証サービスに提供して、引き換えにユーザ要求が真正であるかどうかを示す情報を受信し得る。ユーザ要求が真正であるかどうかの判断は、任意の好適な様式で実行され得、認証が実行される様式は、様々な実施形態の間で変動し得る。例えば、いくつかの実施形態では、ユーザはデータサービスフロントエンドに伝送されるメッセージに電子署名する。電子署名は、認証するエンティティ（例えばユーザ）及び認証サービスの両方に使用可能である、秘密情報（例えばユーザに関連付けられる１対の鍵の秘密鍵）を使用して生成され得る。要求及び要求のための署名は、認証サービスに提供され得、これは、秘密情報を使用して、受信された署名との比較のために、参照署名を算定して、要求が真正であるかどうかを判断し得る。要求が真正である場合、認証サービスは、データサービスフロントエンドが、暗号サービス等の他のサービスに証明するために使用することができる、要求が真正であるという情報を提供し得、それによって、他のサービスがそれに応じて動作することを可能にする。例えば、認証サービスは、別のサービスが要求の真正を検証するために分析することができる、トークンを提供し得る。電子署名及び／またはトークンは、様々な方法で限定される有効性を有し得る。例えば、電子署名及び／またはトークンは、特定の時間量の間有効であり得る。一実施例では、電子署名及び／またはトークンは、検証のための電子署名及び／またはトークンと共に含まれる、タイムスタンプを入力として取る関数（例えばハッシュベースメッセージ認証コード）に少なくとも部分的に基づいて生成される。提出された電子署名及び／またはトークンを検証するエンティティは、受信されたタイムスタンプが十分に最新のものである（例えば現在時刻から所定の時間量内である）ことを点検して、受信されたタイムスタンプのために使用している参照署名／トークンを生成し得る。提出された電子署名／トークンを生成するために使用されたタイムスタンプが、十分に最新のものでない、かつ／または、提出された署名／ト

ークンと参照署名／トークンが一致しない場合、認証は失敗し得る。このようにして、電子署名が危殆化される場合、それは短い時間量の間のみ有効となり得、それによって危険に曝すことによって引き起こされる潜在的な被害を限定する。真正を検証する他の方法もまた、本開示の範囲内であるとみなされるということに留意すべきである。

【００２４】

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

【００２５】

環境２００（及び本明細書に記載される他の環境）の多数の変形は本開示の範囲内であるとみなされる。例えば、環境２００は、暗号サービス及び／または認証サービスと通信し得る、追加のサービスを含み得る。例えば、環境２００は、異なる方法でデータを格納し得る、追加のデータ格納サービス（それぞれがフロントエンドシステム及びバックエンドシステムを備え得る）を含み得る。例えば、あるデータ格納サービスは、データ格納サービスが同期様式でデータ格納サービスを実行するデータへの、アクティブアクセスを提供し得る（例えばデータを読み出すための要求が読み出されたデータと共に同期の応答を受信し得る）。別のデータ格納サービスは、保存用データ格納サービスを提供し得る。かかる保存用データ格納サービスは、非同期の要求処理を利用し得る。例えば、データを読み出すための要求は、読み出されたデータを含む同期応答を受信しないことがある。むしろ、保存用データ格納サービスは、保存用データ格納サービスが読み出されたデータを提供する準備ができると、読み出されたデータを得るために、第２の要求が提出されることを要求し得る。別の実施例として、環境２００は、暗号サービス（及び／または他のサービス）から情報を受信して、その情報を使用してアカウント記録を生成する計量サービスを含み得る。アカウント記録は、暗号サービス（及び／または他のサービス）の使用について顧客に課金するために使用され得る。さらに、暗号サービスからの情報は、料金がどのように課せられるべきかについての指示を提供し得る。例えば、いくつかの例では、顧客は暗号サービスの使用について、請求書が提供され得る。他の例では、暗号サービスの使用についての料金は、その動作の一部として暗号サービスを利用するデータサービス等の、他のサービスの使用料金に合わされ得る。使用は、動作当たり、時間当たり、及び／または他の方法等の、様々な方法で計量されて課金され得る。他のデータサービスもまた環境２００（または本明細書に記載される他の環境）内に含まれ得る。

【００２６】

さらに、図２は、データサービスフロントエンドと対話するユーザを描写する。ユーザは、図面には例示されていないユーザデバイス（例えばコンピュータ）を通してデータサービスフロントエンドと対話し得るということが理解されるべきである。さらに、図２（及び図面の他の箇所）に描写されるユーザは、非人間エンティティもまた表し得る。例えば、コンピュータシステム上で実行する自動化プロセスは、本明細書に記載されるデータ

サービスフロントエンドと対話し得る。例示的な一実施例として、図２のユーザによって表されるエンティティは、その動作の一部として、データサービスフロントエンドを使用して、データサービスバックエンド格納システムにデータを格納する及び／またはそこからデータを読み出す、サーバであり得る。さらに別の実施例として、図２のユーザによって表されるエンティティは、図２のサービスのうちの１つ以上を動作させるコンピューティングリソースプロバイダのサービスとして提供されるエンティティであり得る。例えば、図２のユーザは、コンピューティングリソースプロバイダによって提供される、プログラム実行サービスの仮想または他のコンピュータシステムを表し得る。下記に記載の他の環境の変形を含む他の変形もまた、本開示の範囲内であるとみなされる。

【００２７】

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

【００２８】

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

【００２９】

図３に例示されるように、データサービスフロントエンドは、認証サービスからの認証証明の受信の際に、平文及び認証証明を暗号サービスに提供する。平文及び認証証明は、暗号サービスへのＡＰＩ呼び出しまたは他の電子要求（例えば暗号ＡＰＩ呼び出し）に応

じて提供され得る。暗号サービスは、認証証明を分析して、平文を暗号化するかどうかを判断し得る。

【００３０】

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

【００３１】

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

【００３２】

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

【００３３】

本明細書に記載される全ての環境と同様に、多数の変形が本開示の範囲内であるとみなされる。例えば、環境３００の様々な構成要素の間の情報の流れは、示されるものから変動し得る。例えば、中間構成要素を通して、ある構成要素から別の構成要素に流れる情報（例えば認証サービスから暗号サービスへのデータ及び／または暗号サービスからデータサービスバックエンド格納システムへのデータ）は、その目的地に直接及び／または環境

３００の他の中間構成要素（必ずしも図面に含まれない）を通して提供され得る。別の実施例として、ＰＵＴ要求（及び以下のＧＥＴ要求）は、例示の目的のために提供される。しかしながら、記載される動作を実行するための任意の好適な要求が使用され得る。

【００３４】

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

【００３５】

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

【００３６】

認証要求の提出の際に、認証要求が提出４０４されたエンティティによって、認証応答が受信４０６される。例えば、図３を参照すると、認証サービスは、他のサービスによる使用のための認証の証明を含む応答を、データサービスフロントエンドに提供し得る。認証が成功であったかどうかの表示等の他の情報もまた伝送され得る。要求が真正であるかどうかが判断４０８され得る。要求の真正性は、認証サービス等のエンティティまたはかかる点検を集合的に実行するエンティティの組み合わせによって点検される、１つ以上の因子に従属し得る。例えば真正性は、要求が、必要とされる有効な証明（例えば、点検するエンティティによって共有される秘密鍵によって生成される電子署名）を提供すること、及び／またはポリシーが、要求が遂行されることを可能にすることを要求し得る。認証要求を提出４０４して認証応答を受信するシステムの視点からは、真正性は、受信される認証応答に従属し得る。結果的に、一実施形態では、要求が真正であるかどうかの判断４０８は、受信される認証応答に少なくとも部分的に基づいて実行され得る。例えば、認証が真正でなかった場合、認証応答はそのように示し、それに応じて判断４０８され得る。同様に、応答は、例えば要求が真正であった場合に含まれ得る情報を含まないことによって、認証要求が真正であることを暗黙的に示し得る。ＰＵＴ要求が真正でないと判断４０８された場合、ＰＵＴ要求は拒否４１０され得る。ＰＵＴ要求を拒否することは、任意の好適な様式で実行され得、かつ、プロセス４００が実行されている様々な実施形態に依存し得る。例えば、拒否４１０することで、ＰＵＴ要求は、ＰＵＴ要求を提出したユーザにメッセージを伝送することを含み得る。メッセージは、要求が拒否されたことを示し得る。要求を拒否することは、ＰＵＴ要求が真正でないまたは許可されていないことをもたらした、任意の問題を解決する方法を判断するために使用され得る、電子署名が正確でないまたは他の理由等の、なぜ要求が拒否されたかについての情報を提供することもまた含み得る。

【００３７】

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

【００３８】

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

【００３９】

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

【００４０】
代替の実施形態では、データサービスフロントエンドは、暗号サービスに、受信された認証証明を、暗号サービスが解読する暗号文とともに、提供するように構成され得る。結果的に、暗号サービスは、認証証明が、暗号文の解読を可能にするのに十分であるかどうかを判断して、認証証明が十分である場合、適切な鍵（データサービスフロントエンドによって、暗号サービスに識別され得る）を使用して暗号文を解読して、データサービスフロントエンドに解読された暗号文（平文）を提供するように構成され得る。暗号サービスに暗号文を提供するために、データサービスフロントエンドは、データサービスバックエンド格納システムから暗号文を得る（例えば、適切に構成されたＡＰＩ呼び出しを介して）ように構成され得る。

【００４１】
図６は、様々な実施形態に従う、平文を得るために使用され得る、プロセス６００の例示的な実施例を示す。プロセス６００は、例えば、図５に関連して上記に例示される、データサービスフロントエンドシステム（データサービスフロントエンド）によって実行され得るが、プロセス６００及びその変形は任意の好適なシステムによって実行されてよい。一実施形態では、プロセス６００は、ユーザからＧＥＴ要求（または他の適切な要求）を受信６０２することを含む。ＧＥＴ要求を受信することは、他の種類の要求に関連して上記のように実行され得る。ＧＥＴ要求の受信６０２の際に、認証要求が、認証サービスに、または上記のような任意の様式で、提出６０４され得る。それに応じて、認証応答が受信され得る。受信された認証応答に少なくとも部分的に基づいて、ＧＥＴ要求が真正であるかどうかが判断６０８され得る。ＧＥＴ要求が真正でないと判断６０８される場合、プロセス６００は、上記のように、様々な実施形態に従う様々な様式で実行され得る要求を拒否６１０することを含み得る。

【００４２】
ＧＥＴ要求が真正であると判断６０８される場合、プロセス６００は格納装置から暗号文を読み出すことを含み得る。格納装置から暗号文を回復６１２することは、任意の好適な様式で実行され得る。例えば、図５に関連して上記の環境５００を参照すると、データサービスフロントエンドは、暗号文のための要求をデータサービスバックエンド格納システムに提出し得、応答として暗号文を受信し得る。概して、暗号文は、任意の好適な様式で格納装置から得られ得る。暗号文の受信の際に、プロセス６００は、暗号文を解読することに関連する１つ以上の動作を実行６１４することを含み得る。例えば、一実施形態では、データ格納サービスは、暗号文を解読することに関連する１つ以上の暗号動作を実行６１４するために、暗号サービスに要求を送信し得る。構成の一実施例では、データサービスは、暗号サービスに、暗号化されたエンベロープ鍵（または暗号化されたエンベロープ鍵の識別子）認証証明を含むＡＰＩ呼び出しを送信し得、かつ、エンベロープ鍵を暗号化するために使用されるマスター鍵の識別子を暗号サービスに送信し得る。暗号サービスは、認証証明が、動作を可能にするのに十分であるかどうかを判断することができ、かつ、認証証明が十分である場合エンベロープ鍵を解読することができる。解読されたエンベロープ鍵は、暗号化された平文を解読するために鍵を使用し得るデータサービスに、送信して戻され得る。

【００４３】
別の構成では、暗号文は、図５に関連して上記の暗号サービスのような、暗号サービスに提供され得る。暗号文を解読するかどうかを判断するために暗号サービスによって使用され得る認証の証明等の、他の情報もまた、暗号サービスに提供され得る。さらに、いくつかの実施形態では、暗号文を解読するために暗号サービスによって使用される鍵の識別子が、暗号サービスに提供され得る。しかしながら、他の実施形態では、鍵は暗号サービスに暗黙的に示され得る。例えば、暗号サービスは、暗号サービスに示される顧客に関連付けられる初期設定の鍵を使用し得る。概して、暗号サービスが、暗号文を解読するためにどの鍵を使用するかを判断することができる、任意の様式が使用され得る。

【００４４】

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

【００４５】

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

【００４６】

図７に例示されるように、データサービスフロントエンドは、暗号化された情報を、格納のためにデータサービスバックエンド格納システムに提供するように構成される。この実施例では、データサービスフロントエンドは、鍵下で暗号化されたデータ対象と、鍵ＩＤを有する別の鍵下で暗号化された鍵と、を提供するように構成される。例示の目的のために、暗号化を示すために中括弧表記が使用されるということに留意すべきである。特に、中括弧の中の情報は、添字で特定される鍵下で暗号化される情報である。例えば、｛データ対象｝$_{鍵}$は、「データ対象」というデータが、「鍵」という鍵下で暗号化されるということを示す。この中括弧表記を使用して、鍵識別子も添字で出現し得るということに留意すべきである。添字に鍵識別子が出現する場合、中括弧の中の情報は、その鍵識別子によって識別される鍵下で暗号化される。例えば、｛データ対象｝$_{鍵\ ID}$は、「データ対象」というデータ対象が、「鍵ＩＤ」という鍵識別子によって識別される鍵下で暗号化されるということを示す。同様に、｛鍵｝$_{鍵\ ID}$は、「鍵」という鍵が、「鍵ＩＤ」という鍵識別子によって識別される鍵下で暗号化されるということを示す。換言すると、本開示は、添字において鍵及び鍵識別子の両方を利用し、添字の意味は文脈から明白であるはずである。暗号文は、関連する解読鍵のＩＤを判断するために使用可能な、追加のメタデータを含み得る。

【００４７】

図８は、図７に関連して上記されるデータサービスバックエンド格納システム等の、データ格納システム内にデータ対象を格納するために実行され得るプロセス８００の例示的な実施例を示す。プロセス８００は、例えば図７に関連して上記されるデータサービスフロントエンドシステム等の、任意の好適なシステムによって実行され得る。一実施形態では、プロセス８００は、データ対象のためのＰＵＴ要求を受信８０２することを含む。データ対象のためのＰＵＴ要求を受信することは、例えば上記のような、任意の好適な様式で実行され得る。データ対象は要求に関連して受信され得、または別のサービスから受信

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

【００４８】

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

【００４９】

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

【００５０】

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

【００５１】

述べられたように、本開示の様々な実施形態は、ユーザがデータ対象を格納すること及び安全な様式でそれらを読み出すことを可能にする。したがって、図９は格納装置からデータ対象を得るために使用され得る環境９００の例示的な実施例を示す。図９に例示されるように、環境９００は、認証サービス、暗号サービス、データサービスフロントエンドシステム、及びデータサービスバックエンド格納システムを含む。認証サービス、暗号サービス、データサービスフロントエンド、及びデータサービスバックエンド格納システムは、上記のようなコンピュータシステムであり得る。図９に例示されるように、データサービスフロントエンドシステムは、データ対象要求を受信し、それに応答してデータ対象を提供するように構成される。応答してデータ対象を提供するために、本実施形態におけるデータ格納フロントエンドシステムは、図９に例示されるように、認証サービス、暗号サービス、及びデータサービスバックエンド格納システムと、対話するように構成される。例えば、様々な実施形態では、データサービスフロントエンドシステムは、認証要求を認証サービスに提出し、要求に応答して認証証明を受信するように構成される。別の実施例として、データサービスフロントエンドは、鍵ＩＤによって識別される鍵によって暗号化された鍵及び認証証明を、鍵を提供するかどうかを認証証明に少なくとも部分的に基づいて判断するように動作可能である暗号サービスに提供して、鍵を提供するように判断された場合、鍵をデータサービスフロントエンドに提供するように構成される。データサービスフロントエンドは、鍵ＩＤ等の他の情報を暗号サービスに提供するようにもまた構成され得る。しかし、いくつかの実施形態では、鍵ＩＤは、例えば暗号サービスに提供される他の情報との関連を通して、暗号サービスに暗黙的に示され得る。いくつかの実施形態では、ユーザは、要求をデータサービスフロントエンドに提出することに関連して、鍵ＩＤをデータサービスフロントエンドに提供するということにもまた留意すべきである。さらに、図９に例示されるように、一実施形態では、データサービスフロントエンドは、データサービスバックエンド格納システムからデータ対象を要求して、それに応答して、鍵によって暗号化されたデータ対象及び鍵ＩＤによって識別された鍵によって暗号化された鍵を受信するように、構成される。いくつかの実施形態では、暗号サービスは、特定される鍵ＩＤに関連付けられる鍵を使用して生成されなかった暗号文の解読を実行することを

、拒否するように動作可能であり得る。

【００５２】

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

【００５３】

一実施形態では、プロセス１０００は、暗号化されたエンベロープ鍵を暗号サービスに提供１０１４することを含む。暗号化されたエンベロープ鍵を暗号サービスに提供１０１４することは、任意の好適な様式で実行され得、かつ、暗号サービスが暗号化された鍵を解読するかどうかを判断することができるようにする認証証明等の、他の情報と共に提供され得る。さらに、暗号化されたエンベロープ鍵を暗号サービスに提供１０１４することは、暗号サービスが、暗号サービスによって管理される複数の鍵の中から、識別子によって識別される鍵を選択することができるようにするために、暗号化されたエンベロープ鍵の許可された解読のために要求される鍵の識別子を提供することを含み得る。しかしながら、上で述べられたように、鍵は暗黙的に識別され得る。したがって、暗号サービスは、適切な鍵を選択して暗号化された鍵を解読し得る。したがって、一実施形態では、プロセス１０００は、解読されたエンベロープ鍵を暗号サービスから受信１０１６することを含む。例えば、暗号サービスが、認証証明が有効である、及び／または、暗号化されたものの解読が任意の適用可能なポリシーに従って許容可能であると判断した場合、暗号サービスは、解読された鍵を、データ対象を解読しようとしているシステムに提供し得る。その後、解読されたエンベロープ鍵を使用して、データ対象が解読１０１８され得る。その後、解読されたデータ対象は、ユーザまたはＧＥＴ要求を提出した他のシステム等の要求者に提供１０２０され得る。

【００５４】

多くの例では、ユーザ（すなわち、一般的には暗号サービスを利用するデバイス）が暗号サービスと直接対話することが望ましい。したがって、図１１は、暗号サービスへの直接的なユーザアクセスを可能にする、環境１１００の例示的な実施例を示す。環境１１００では、認証サービス、データサービスフロントエンド、及びデータサービスバックエンド格納システムが含まれる。認証サービス、データサービスフロントエンド、及びデータサービスバックエンド格納システムは、上記の通りであり得る。例えば、データサービスフロントエンドは、好適なネットワークを介して、図１１に例示されるように、ユーザからの要求を受信してそれに応答するように構成され得る。ネットワークを介してユーザからの要求に応答することの一部として、データサービスフロントエンドは、ユーザ要求が

真正であるかどうかを判断する及び／または要求に関するポリシーを実施するために、認証サービスと対話するようにもまた構成され得る。データサービスフロントエンドは、ユーザ要求を遂行することの一部として、データサービスバックエンド格納システムと対話するようにもまた構成され得る。ユーザ要求は、例えば、データをバックエンド格納システム内に格納するためのＰＵＴ要求、及びデータサービスバックエンド格納システムからデータを読み出すためのＧＥＴ要求を含み得る。上記のように、例えば、データサービスバックエンド格納システム内に格納されたデータを削除するための要求、データサービスバックエンド格納システム内に格納されたデータを更新するための要求等の、他の要求もまた様々な実施形態に従って使用され得る。

【００５５】

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

【００５６】

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

【００５７】

データは、上記のような任意の好適な様式で、データサービスバックエンド格納システム内に格納され得る。例えば、上記の暗号化されたデータをバックエンド格納システム内に格納するための技術は、環境１１００において使用され得る。例えば、例示されていないが、データサービスフロントエンドは、暗号サービスフロントエンドと通信して、暗号サービスバックエンドがデータを暗号化することを引き起こし得、そのデータは後にデータサービスバックエンド格納システム内に格納され得る。暗号化されたデータは、データ対象及び／またはデータ対象を暗号化するために使用された暗号化された鍵であり得る。環境１１００では、データは、別様でもまたデータサービスバックエンド格納システムに配置され得る。例えば、ユーザは暗号サービスによって暗号化される平文を提供し得、かつ、それに応答して暗号文を受信し得る。ユーザはその後、データサービスフロントエンドに要求を提出して、暗号文がデータサービスバックエンド格納システム内に格納されることを要求し得る。データサービスフロントエンドは、本実施例では、任意の様式で暗号文を格納し得る。例えば、データサービスフロントエンド及びバックエンド格納システムは、データが暗号されるかどうかに無関係であるように構成され得る。

【００５８】

さらに、本明細書に例示される全ての環境と同様に、システム間の行動を協調させるために、追加のフロントエンドシステムが、ユーザと、データサービスフロントエンドと、暗号サービスフロントエンドと、おそらく他のフロントエンドシステムとの間に、論理的に位置付けられ得る。例えば、いくつかの実施形態では、ユーザの視点からの動作がより

簡単になるように、ユーザは、それ自体が暗号サービスフロントエンド及びデータサービスフロントエンドと対話する、フロントエンドシステムと対話し得る。例えば、ユーザはデータ対象が暗号化されて格納されること、ならびに、フロントエンドシステムが暗号サービスフロントエンド及びデータサービスフロントエンドとの適切な対話によって要求に応答することを要求し得る。しかしながら、ユーザの視点からは、かかることは単一の要求によって実行され得る。他の変形もまた本開示の範囲内である。

【００５９】

図１２は、本開示の様々な実施形態を実装するために使用され得る、環境１２００の例示的な実施例を示す。図１２では、環境１２００は、ユーザがデータサービスバックエンド格納システム内に暗号文を格納することができるようにするように構成される。したがって、図１２に例示されるように、環境１２００は、データサービスフロントエンド、データサービスバックエンド格納システム、認証サービス、暗号サービスフロントエンド、及び暗号サービスバックエンドを含む。データサービスバックエンド格納システム、データサービスフロントエンド、認証サービス、暗号サービスフロントエンド、及び暗号サービスバックエンドは、図１１に関連して上記のようなシステムであり得る。例えば、図１２に例示されるように、データサービスフロントエンドは、ユーザ要求を受信してそれに応答するように構成され、かつユーザ要求に関するポリシーを実施するようにもまた構成され得る。データサービスフロントエンドは、要求に応答することの一部として、認証要求を認証サービスに提出して、それに応答して応答して認証証明を受信するように構成され得る。認証が成功すると、データサービスフロントエンドは、データサービスバックエンド格納システムと対話して、暗号化されたデータ対象及びおそらく暗号化されていないデータ対象をデータサービスバックエンド格納システムから得るようにさらに構成され得、これは後でユーザに提供され得る。

【００６０】

図１２に例示されるように、暗号サービスフロントエンドは、認証要求を認証サービスに提出して、それに応答して認証証明を受信するようにもまた構成される。認証証明は、暗号サービスバックエンドからサービスを得るために使用され得る。例えば、暗号サービスフロントエンドは、暗号文を認証証明と共に暗号サービスバックエンドに提供するように構成され得、暗号サービスバックエンドは、暗号文を解読して引き換えに暗号文を提供するように構成され得る。図１２に例示されるように、暗号文は暗号化された鍵であり得、暗号サービスバックエンドは暗号化された鍵を解読して、解読された鍵、つまり平文鍵を暗号サービスフロントエンドに提供し得、これは平文鍵をユーザに提供するようにさらに構成される。ユーザは、その後鍵を使用して、データサービスフロントエンドから受信される暗号化されたデータ対象を解読し得、またはユーザのドメイン内（例えば、ユーザが動作または制御するデータセンターまたはコンピュータシステム内）に格納される暗号化されたデータ対象を解読し得る。本実施例では、ユーザは暗号化された鍵をデータサービスフロントエンドから得た可能性がある。例えば、ユーザは、データ対象及び／またはデータ対象を暗号化するために使用された鍵のために、要求をデータサービスフロントエンドに提出した可能性がある。図１１では単一の要求として例示される一方で、データ対象及び鍵の両方のために別個の要求がなされ得る。図１１に例示されるように、データサービスフロントエンドは、暗号化されたデータ対象及び暗号化された鍵をデータサービスバックエンド格納システムから得て、暗号化されたデータ対象及び暗号化された鍵をユーザに提供し得る。

【００６１】

本明細書に例示される全ての環境と同様に、変形は本開示の範囲内であるとみなされるということに留意すべきである。例えば、図１２は、鍵下で暗号化されたデータ対象、及び鍵識別子によって識別される別の鍵によって暗号化された鍵が、ユーザに提供されているところを示す。さらなるレベルの暗号化もまた使用され得る。例えば、データ対象は、ユーザにのみアクセス可能である（かつ／または環境１２００の他の構成要素によってアクセス可能でない）鍵下で暗号化され得る。データ対象を暗号化するために使用される鍵

もまた、ユーザにのみアクセス可能である鍵下で暗号化され得る。本実施例では、ユーザの鍵へのアクセスが許可された解読のためになお要求されるため、環境１２００（ユーザ不在）の構成要素への許可のないアクセスは、データ対象の暗号化されていないコンテンツへのアクセスを提供しない。

【００６２】

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

【００６３】

図１３は、プロセス１３００の例示的な実施例を示し、これは暗号化されたデータ対象及び暗号化された鍵を、上記のようなデータサービスバックエンド格納システム等から得るために使用され得る。例えば、プロセス１３００は、図１２に関連して上記されるデータサービスフロントエンドシステムによって実行され得る。一実施形態では、プロセス１３００は、暗号化されたデータ対象のためのＧＥＴ要求を受信１３０２することを含む。ＧＥＴ要求を受信することは、データサービスフロントエンドシステムへのＡＰＩ呼び出しを介して要求を受信すること等によって、任意の好適な様式で実行され得る。ＧＥＴ要求の受信の結果として、プロセス１３００は、認証要求を提出１３０４すること及び認証応答を受信１３０６することを含み得る。認証要求を提出１３０４すること及び認証応答を受信１３０６することは、上記のような任意の好適な様式で実行され得る。認証応答は、ＧＥＴ要求が真正であるかどうかを判断１３０８するために使用され得る。ＧＥＴ要求が真正でないと判断１３０８される場合、プロセス１３００はＧＥＴ要求を拒否１３１０することを含み得る。ＧＥＴ要求を拒否１３１０することは、上記のような任意の好適な様式で実行され得る。しかしながら、ＧＥＴ要求が真正であると判断１３０８される場合、プロセス１３００は暗号化されたデータ対象に、解読されると暗号化されたデータ対象を解読するために使用可能である暗号化された鍵を、提供１３１２することを含み得る。本明細書に記載される全てのプロセスと同様に、多数の変形が本開示の範囲内であるとみなされるということに留意すべきである。例えば、プロセス１３００は、ＧＥＴ要求が真正である場合、暗号化されたデータ対象を提供するが暗号化された鍵は提供しないことによって、ＧＥＴ要求に応答するように構成され得る。要求者、つまりＧＥＴ要求を提出したユーザまたはシステムは、他の方法で、暗号化された鍵を得ることができる。例えば、いくつかの実施形態では、ユーザはユーザの制御下で、暗号化された鍵を自体でデータ格納システム内に格納し得る。別の例として、ある格納サービスが暗号化されたデータ対象を格納し得、別のサービスが暗号化された鍵を格納し得、ユーザは暗号化されたデータ対象及び暗号化された鍵をそれぞれのサービスから得ることができる。別の例として、別のサービスまたは第三者が、暗号化された鍵を格納するために使用され得、ユーザは要求の際に暗号化された鍵を得ることができる。概して、暗号化された鍵が提供され得る任意の方法が使用され得る。

【００６４】

図１３に例示されるように、プロセス１３００は、データ対象及びデータ対象を解読するために使用可能である暗号化された鍵が提供されたエンティティをもたらし得る。様々

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

【００６５】

一実施形態では、プロセス１４００は、認証要求を提出１４０４すること及び認証応答を受信１４０６することを含む。認証要求を提出１４０４すること及び認証応答を受信１４０６することは、上記のような任意の好適な様式で実行され得る。さらに、上記のように、受信された認証応答は、ＧＥＴ要求が真正であるかどうかを判断１４０８するために使用され得る。ＧＥＴ要求が真正でないと判断１４０８される場合、プロセス１４００はＧＥＴ要求を拒否１４１０することを含み得る。ＧＥＴ要求を拒否１４１０することは、上記のように、任意の好適な様式で実行され得る。しかしながら、ＧＥＴ要求が真正であると判断１４０８される場合、プロセス１４００は、特定される鍵ＩＤについての及び／または要求者についての、ポリシー情報にアクセスすることを含み得る。ポリシー情報は、鍵ＩＤ及び／または要求者の１つ以上のポリシーを含み得る。

【００６６】

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

【００６７】

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

【００６８】

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

【００６９】

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

【００７０】

一実施形態では、プロセス１５００は、特定された鍵ＩＤを有する鍵を使用した、暗号化された鍵の解読を要求することを含む。鍵ＩＤは、上記のような任意の好適な様式で特定され得る。さらに、プロセス１５００を実行しているシステムは、任意の好適な様式で鍵ＩＤを特定することができ得るということに留意すべきである。例えば、暗号化された鍵及び／またはそこに提供された情報は鍵ＩＤを特定し得る。別の例として、プロセス１５００を実行しているシステムは、鍵ＩＤを判断することを可能にする情報へのローカルまたは遠隔アクセスを有し得る。例えば、ローカルまたは遠隔データベースは、データ対象識別子を、データ対象を暗号化するために使用された鍵の鍵識別子に関連付け得る。概して、システムが鍵ＩＤを特定することができるようにし得る任意の様式が使用され得る。さらに、いくつかの実施形態では、暗号サービスに提供される情報が鍵ＩＤを判断するのに十分である場合等では、鍵ＩＤは特定される必要がない。暗号化された鍵の解読の要求１５０６は、図１２に関連して上記される環境に関連して、及び／または図１４に関連して上記されるプロセス１４００の実行等によって、任意の好適な様式で実行され得る。

【００７１】

プロセス１５００は、一実施形態では、解読された鍵を受信１５０８することを含む。解読された鍵を受信１５０８することは、任意の好適な様式で実行され得る。例えば、解読された鍵は、暗号化された鍵の解読の要求に応答して受信され得る。別の例として、暗号化された鍵の解読の要求は非同期要求であり得、解読された鍵を受信するために別の要求が提出された可能性がある。概して、解読された鍵は、任意の好適な様式で受信され得る。さらに、あるデバイスから別のデバイスに流れる全ての情報と同様に、情報の通過は安全なチャネルを使用して実行され得る。例えば、解読された鍵は、解読された鍵を受信するエンティティによる解読のために、再度暗号化され得る。概して、安全な通信の任意の様式が、あるエンティティから別のエンティティに情報を通過させるために使用され得る。

【００７２】

解読された鍵が受信１５０８されると、プロセス１５００は解読された鍵を使用１５１０して暗号文を解読１５１０し、よって平文を得ることを含み得る。本明細書に記載される全てのプロセスと同様に、変形が本開示の範囲内であるとみなされるということに留意すべきである。例えば、プロセス１５００は、暗号文の要求及び暗号化された鍵の解読の要求が、連続的に実行されているところを示す。しかしながら、様々なプロセスに関連して本明細書に記載される多くの動作と同様に、様々な実施形態では動作は連続的に実行される必要がない。例えば、プロセス１５００を実行するシステムが、暗号文を要求する前

に、暗号化された鍵へのアクセスを有する、または別様でそうすることができる場合、システムは暗号文を要求し得、かつ、平行してまたは例示されるものとは異なる順序で、暗号化された鍵の解読を要求し得る。他の変形もまた本開示の範囲内であるとみなされる。

【００７３】

上記のように、本開示の様々な実施形態は暗号サービスを提供することを対象とする。暗号サービスは、上記のような暗号サービスシステムによって提供され得る。したがって図１６は、様々な実施形態に従う暗号サービス１６００の例示的な実施例を示す。図１６に例示されかつ上で述べられたように、暗号サービス１６００は、フロントエンドシステム及びバックエンドシステムから論理的に構成される。フロントエンドシステム及びバックエンドシステムの両方は、本明細書に記載される動作を実行するように構成される１つ以上のコンピュータシステムによって実装され得る。例えば、図１６に例示されるように、暗号サービス１６００のフロントエンドシステムは、要求ＡＰＩ及びポリシー構成ＡＰＩを実装する。一実施形態では、要求ＡＰＩは、暗号化及び他の動作が暗号サービスによって実行されることを要求するために構成されるＡＰＩである。よって、かかる暗号動作が暗号サービスによって実行されるように、要求ＡＰＩを介してフロントエンドシステムに要求がなされ得る。

【００７４】

要求ＡＰＩは、以下の、高レベルの使用可能な要求の実施例で構成され得る。

鍵作成（鍵ＩＤ）
暗号化（鍵ＩＤ、データ、［ＡＡＤ］）
解読（鍵ＩＤ、暗号文、［ＡＡＤ］）
細断（鍵ＩＤ）
鍵再作成（暗号文、旧鍵ＩＤ、新鍵ＩＤ）。

【００７５】

鍵作成（鍵ＩＤ）要求は、一実施形態では、暗号サービスに、要求において識別される鍵ＩＤによって識別される鍵を作成させる。要求の受信の際に、暗号サービスは鍵を生成してその鍵を鍵ＩＤに関連付け得る。鍵ＩＤのものは、固有の識別子であり得るが必ずしもそうではないということを理解すべきである。例えば、鍵ＩＤは鍵のファミリーを識別し得る。例えば、いくつかの実施形態では、鍵回転が実行される。鍵回転は、使用される暗号の実用的なクラッキングを可能にするのに十分な解読されたデータの収集を防止するために、鍵を他の鍵と交換することを含み得る。暗号サービスとは異なるエンティティの方向で実行される場合、鍵作成（鍵ＩＤ）要求の使用は、暗号サービスに、鍵ＩＤによって識別される旧鍵と交換するための新鍵を作成させ得る。旧鍵は、鍵ＩＤによって識別されるままであり得るが、例えば、（旧鍵を使用して既に暗号化されたデータの）解読に使用されるのみで将来の暗号化には使用されないことがある。別の実施例として、いくつかの実施形態では、暗号サービスのユーザは彼ら自身の鍵識別子を提供し、かつ、２人の異なる顧客が同じ識別子を提供し得る可能性がある。かかる例では、識別子は鍵を一意に識別し得ず、またはさらには鍵のファミリーも一意に識別し得ない。これに対処するために、様々な方法が整えられ得る。例えば、識別または暗号サービスのユーザに関連付けられる他の情報が、適切な鍵または鍵のファミリーを識別するために使用され得る。さらに他の実施形態では、暗号サービスは、無作為に、連続的に、または任意の他の方法を使用して、鍵ＩＤを割り当て得る。

【００７６】

鍵ＩＤが鍵を一意に識別しない場合、適切な機能を可能にするために様々なシステムが整えられ得るということに留意すべきである。例えば、様々な実施形態では、ある鍵ＩＤによって識別される鍵のファミリーは有限である。鍵ＩＤによって識別される鍵を使用した解読動作が要求される場合、追加のデータ（例えば、暗号化が実行されたときのタイムスタンプ）が使用すべき適切な鍵の判断を可能にし得る。いくつかの実施形態では、暗号文は鍵版を示す情報を含み得る。いくつかの実施形態では、データの異なる解読を提供するために全ての可能な鍵が使用される。有限数の鍵があるため、適切な解読は提供される

ものから選択され得る。いくつかの実施形態では、鍵を用いた解読は、認証された暗号化を使用すること等によって、暗号サービスがその暗号文が少なくとも部分的にその鍵に基づいて生成されなかったことを検出することができるようにする様式で、実行される。他の変形もまた本開示の範囲内であるとみなされる。

【００７７】

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

【００７８】

一実施形態では、細断（鍵ＩＤ）は、暗号サービスに、特定される鍵ＩＤによって識別される鍵または鍵のファミリーを電子的に細断させるために、使用され得る。電子的細断は、鍵をもうアクセス可能でなくすることを含み得る。例えば、細断（鍵ＩＤ）要求の使用は、暗号システムに、１つ以上のハードウェアデバイスに、特定される鍵ＩＤによって識別される１つ以上の鍵上で安全消去動作を実行するように命令させ得る。概して、鍵ＩＤによって識別される鍵（複数可）は、他のデータ（例えば一連の０または１または無作為な文字列）を用いて鍵をコードするデータを上書きすること等によって、任意の好適な様式で電子的に細断され得る。鍵（複数可）がある鍵下で暗号化されて格納される場合、鍵を暗号化するために使用された鍵は、電子的に細断され得、よってその鍵（複数可）へのアクセスの損失を引き起こす。いくつかの実施形態では、細断動作は、細断された鍵ＩＤが将来の何らかの確固たる時点で失敗することを示す、解読動作を行わせ得る。鍵（複数可）への任意の可能なアクセスを安全にかつ永続的に破壊する他の様式が使用され得る。

【００７９】

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

のアカウント内の第１の鍵ＩＤによって識別される鍵から、第２のアカウント内の鍵ＩＤによって識別される鍵へ、暗号文を鍵再作成することを支持し得る。

【００８０】

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

鍵設定ポリシー（鍵ＩＤ、ポリシー）

保留（鍵ＩＤ、公開鍵）

復元（鍵ＩＤ、秘密鍵）

【００８１】

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

【００８２】

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

【００８３】

図１６に例示されるように、いくつかの実施形態では、暗号サービス１６００は、それ自体が様々な構成要素を備えるバックエンドシステムを含む。例えば、本実施例における

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

【００８４】

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

【００８５】

セキュリティモジュールは、要求処理ユニットによって提供される命令に従って暗号動作を実行するように構成され得る。例えば、要求処理ユニットは、暗号文及び鍵ＩＤを、その鍵ＩＤに関連付けられる鍵を使用して暗号文を解読し、応答して平文を提供するための、セキュリティモジュールへの命令を有する、適切なセキュリティモジュールに提供し得る。一実施形態では、暗号サービス１６００のバックエンドシステムは、鍵空間を形成する複数の鍵を安全に格納する。セキュリティモジュールのそれぞれは、鍵空間内の全ての鍵を格納し得るが、しかしながら、変形は、本開示の範囲内であるとみなされる。例えば、セキュリティモジュールのそれぞれは、鍵空間のサブ空間を格納し得る。鍵がセキュリティモジュールを通して重複して格納されるように、セキュリティモジュールによって格納される鍵空間のサブ空間は、重複し得る。いくつかの実施形態では、特定の鍵は、特定される地理的領域内にのみ格納され得る。いくつかの実施形態では、特定の鍵は、特定の認定またはクリアランスレベルを有する動作にのみアクセス可能であり得る。いくつかの実施形態では、特定の鍵は、データ格納サービスのプロバイダとの契約下で、特定の第三者によって動作するモジュール内にのみ格納され得、かつそれと共にのみ使用され得る。いくつかの実施形態では、セキュリティモジュールの建設的制御は、顧客によって許可

される以外の鍵の使用を強要しようとする合法命令が、強要されている追加のエンティティ、または行動を強要する追加の管轄のいずれかを含むことを要求し得る。いくつかの実施形態では、顧客は、それらの暗号文が格納されかつそれらの鍵が格納される管轄のための、独立した選択肢を提供され得る。いくつかの実施形態では、鍵を格納するセキュリティモジュールは、鍵の所有者に監査情報を提供するように構成され得、かつ、セキュリティモジュールは、監査情報の生成及び提供が顧客によって抑圧可能でなくなるように構成され得る。いくつかの実施形態では、プロバイダ（例えば、セキュリティモジュールをホストする）が、セキュリティモジュールによって格納される鍵下で動作を実行することができないように、セキュリティモジュールは、独立して、顧客によって生成された署名を立証するように構成され得る。さらに、いくつかのセキュリティモデルは、鍵空間の全てを格納し得、いくつかのセキュリティモジュールは鍵空間のサブ空間を格納し得る。他の変形もまた、本開示の範囲であるとみなされる。異なるセキュリティモジュールが鍵空間の異なるサブ空間を格納する例では、要求処理ユニットは、例えば関係表または他の機構を用いて、様々な要求に従って暗号動作を実行するよう命令すべきセキュリティモジュールを判断するように構成され得る。

【００８６】

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

【００８７】

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

【００８８】

上記のように、要求が鍵ＩＤに対応する鍵に関連して実行されている暗号動作を特定する場合、ポリシーが実施され得るように、様々なポリシーは、鍵ＩＤに関連するユーザによって構成され得る。図１７は、様々な実施形態に従う、ポリシーを更新するためのプロセス１７００の例示的な実施例を提供する。プロセス１７００は、図１６に関連して上で述べられたような、暗号サービスシステム等によって、任意の好適なシステムによって実行され得る。一実施形態では、プロセス１３００は、鍵ＩＤについてのポリシーを更新するための要求を受信１３０２することを含む。要求は、任意の好適な様式で受信１３０２され得る。例えば、例として図１６を参照すると、要求は、上記の暗号サービス１６００のフロントエンドシステムのポリシー構成ＡＰＩを通して受信され得る。要求は、任意の好適な様式で受信され得る。

【００８９】

一実施形態では、プロセス１７００は、認証要求を提出１７０４すること及び認証応答を受信１７０６することを含む。認証要求を提出１７０４すること及び認証応答を受信１７０６することは、上記のような任意の好適な様式で実行され得る。さらに、上記のよう

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

【００９０】

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

【００９１】

ポリシーは、暗号サービスに関連して動作する電子環境の他の構成要素によってもまた実施され得る。例えば、上記の図２を参照すると、暗号サービスは、データサービスフロントエンドが実施するように、ポリシーの電子表示を、データサービスフロントエンドに提供し得る。このようなことは、データサービスがポリシーを実施するためにより良好に適する状況において、有用であり得る。例えば、行動がポリシーによって可能にされるかどうかは、暗号サービスではなく、データサービスフロントエンドにアクセス可能な情報に、少なくとも部分的に基づき得る。一実施例として、ポリシーは、そのポリシーに関連付けられる顧客のために、データサービスバックエンド格納システムによって格納されるデータに依存し得る。

【００９２】

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

【００９３】

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

【００９４】

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

【００９５】

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

【００９６】

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

するように動作可能であり得る。

【００９７】

上記のように、本開示の様々な実施形態は、豊かなポリシー実施及び構成可能性を可能にする。多くの暗号システムは、暗号動作が実行されて、同時に、データの機密性、統一性、及び真正性の保証を提供し得る、暗号動作が実行され得る動作の認証された暗号モードを、提供する。機密性は、平文データの暗号化によって提供され得る。真正性は、平文のため及び暗号化されないままであり得る関連データのための両方に、提供され得る。かかるシステムを用いると、暗号文または関連データのいずれかへの変更は、暗号文の解読を失敗させ得る。

【００９８】

一実施形態では、平文に関連付けられるデータは、ポリシーの実施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う、関連データを使用してポリシー実施を可能にする様式でデータを暗号化するためのプロセス１９００の例示的な実施例を示す。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等の、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、平文を得る１９０２ことを含む。平文は、任意の好適な様式で得られ得る。例えば、上記のようなサービスプロバイダ環境では、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、得る１９０２ことは、鍵（暗号化される）を生成すること及び／または暗号化される鍵を得ることを含み得る。鍵は上記のように使用され得る。

【００９９】

示されるように、プロセス１９００は、関連データを得ることを含む。関連データは、平文に関連付けられたまたはこれから関連付けられる、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それに基づく、任意のデータであり得る。実施例を以下に示す。さらに、関連データは、拡張マークアップ言語（ＸＭＬ）、ＪａｖａＳｃｒｉｐｔ Ｏｂｊｅｃｔ Ｎｏｔａｔｉｏｎ （ＪＳＯＮ）、抽象構文記法１（ＡＳＮ１）、ＹＡＭＬはマークアップ言語ではない（さらに別のマークアップ言語とも称される）（ＹＡＭＬ）、または別の構造化拡張可能データフォーマット等で、任意の好適な様式でコードされ得る。一実施形態では、プロセス１９００は、平文及び関連データに少なくとも部分的に基づいて、メッセージ認証コード（ＭＡＣ）及び暗号文を生成１９０６することを含む。ＭＡＣ及び暗号文、例えばＡＥＳ－ＧＣＭ暗号の出力の組み合わせは、認証された暗号文とも称され得る。ＭＡＣ及び暗号文を生成することは、任意の好適な様式で実行され得、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、一実施形態では、高度暗号化標準（ＡＥＳ）は、ＣＣＭモードまたはＧＣＭモードのいずれかで動作すると、関連する認証されたデータ（ＡＡＤ）を支持し、ここにおいて、ＣＣＭはＣＢＣ－ＭＡＣを有するカウンタを示し、ＧＣＭはガロア／カウンタモードを示し、ＣＢＣは暗号ブロックチェーンを示す。ＣＣＭまたはＧＣＭモードのいずれかにおいてＡＥＳを使用することで、平文及び関連データは、平文及び関連データの両方の、連結された一対の暗号文及びＭＡＣの出力を得るために、入力として提供され得る。ＡＥＳ－ＣＣＭ及びＡＥＳ－ＧＣＭが、例示の目的のために提供されるが、他の認証された暗号化スキームが使用され得、本明細書に明示的に記載される技術はそれに応じて修正され得るということに留意すべきである。例えば、本開示の技術は、概して、認証された暗号モードを支持する、対称性ブロック暗号に適用可能である。さらに、他の暗号化スキームは、本開示の様々な実施形態に従って、ＭＡＣ機能と組み合わせ可能である。好適な暗号化スキーム及びＭＡＣ機能の組み合わせは、そこにおいて、暗号化スキームが選択された平文攻撃下で意味的に安全であり、かつ、ＭＡＣ機能が選択されたメッセージ攻撃下で可鍛性でないものを含むが、これらに限定されない。さらに、本開示の様々な実施形態が、暗号文及びＭＡＣの両方をコードする、単一の出力をもたらす暗号を利用する一方で、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が例示的な実施例として使用される一方で、一般的ハッシュ、チェックサム、署名、及び／またはＭＡＣの代わりに使用され得る他の値等の、概してＭＡＣと称されない他

の値もまた使用され得る。したがって、関連データを支持する自動化暗号モードを有する暗号は、ＭＡＣに加えてまたはその代わりとして、他の暗号プリミティブを使用する暗号を含む。

【０１００】

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、一実施形態では、平文は上記のような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。他の実施形態では、セキュリティモジュール以外の電子環境の構成要素がＭＡＣ及び暗号文を生成する。かかる実施形態では、セキュリティモジュールは、平文形式の時に、ＭＡＣ及び暗号文を生成するために使用される鍵を、解読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、認証された暗号文）は、提供１９０８され得る。いくつかの実施形態では、関連データもまた提供される。ＭＡＣ及び暗号文が、プロセス１９００及びその変形を利用して、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では、ＭＡＣ及び暗号文は、データサービスによる処理のために、上記のようにユーザに提供されるか、上記のようにデータサービスに提供される。さらに、述べられたように、関連データが提供され得るが、様々な実施形態では、関連データは、提供されず、かつ／または、概して平文形式に保持される。一実施例として、関連データは、独立して得られる場合、提供されないことがある。例示的な実施例として、関連データがデバイスの一貫した識別子（例えば、格納デバイスの識別子）である場合、関連データは、ポリシー実施のために及び／または他の目的のために必要とされるときに、後で得られ得る。

【０１０１】

上記のように、本開示の様々な実施形態は、セキュリティモジュールを利用して強化したデータセキュリティを提供する。図２０は、様々な実施形態に従う、新規でかつ豊かなポリシー実施を可能にする様式で、データを暗号化するために使用され得るプロセス２０００の例示的な実施例を提供する。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等の、任意の好適なシステムによって実行され得る。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得ることを含む。上記のように、平文及び関連データは、単一の通信において、別個の通信において、及び／または別個のエンティティから、受信され得る。得られると、平文、関連データ、及び鍵ＩＤは、セキュリティモジュールに提供２００４される。セキュリティモジュールは、上記の通りであり得る。さらに、セキュリティモジュールは、上記のような、暗号サービスを支持する環境等の、電子環境に参加する複数のセキュリティモジュールから選択され得る。鍵ＩＤは、上記の通りであり得、かつ、暗号サービスに提出された平文を暗号化するための要求において特定され得、または別様で特定され得る。さらに、プロセス２０００の代替の実施形態では、鍵ＩＤは特定されないことがある。例えば、いくつかの実施形態では、セキュリティモジュールは、鍵ＩＤを選択し得、及び／または鍵ＩＤを後に割り当てられる鍵を生成し得る。かかる実施形態では、プロセス２０００は、セキュリティモジュールから鍵ＩＤを提供するように修正され得る。

【０１０２】

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２００６することを含み得る。暗号文は、鍵ＩＤによって識別される鍵下で暗号化され得る。ＭＡＣは、平文及び関連データの両方の組み合わせを渡るＭＡＣであり得、よって、暗号文または関連データへの変更が、ＭＡＣの点検を失敗させ得る。上記のように、変形は、ＭＡＣが、関連データに少なくとも部分的に基づいて、しかし平文からは独立して、生成されるものを含むということに留意すべきである。さらに、上記のように、暗号文及びＭＡＣは、一緒に提供され得（例えばＡＥＳ－ＣＣＭまたはＡＥＳ－ＧＣＭ暗号の使用の出力から）、または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、上記のような、暗号サービスまたは暗号サービスに関連して動作するデータサービスのユーザ等の、適切なエンティティに提供２００８

される。
【０１０３】
上記のように、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。上記のように、いくつかの実施形態では、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使用される（それらの平文形式で）鍵を暗号化するために使用される。したがって、図２１は、かかる状況において使用され得るプロセス２１００の例示的な実施例を示す。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等の、任意の好適なシステムによって実行され得る。プロセス２１００は、一実施形態では、上記のように、平文及び関連データを得る２１０２ことを含む。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、暗号化された鍵、関連データ、及び暗号化された鍵を解読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鍵を識別する鍵ＩＤを、提供２１０４することを含む。したがって、プロセス２１００は、解読された鍵を、暗号化された鍵を解読するために鍵ＩＤによって識別される鍵を使用したセキュリティモジュールから、得ることを含む。得られると、鍵は、平文を暗号化して、それによって暗号文及びＭＡＣを計算２１０８するために使用され得る。上記のように、暗号文は平文の暗号化であり得、ＭＡＣは関連データまたは関連データ及び平文の両方を渡る（すなわち、それに少なくとも部分的に基づく）ものであり得る。暗号化されると、プロセス２１００は、上記のように、ＭＡＣ及び暗号文を提供２１１０することを含み得る。さらに、プロセスは、解読された鍵へのアクセスを失くす２１１２こともまた含み得、これは、安全消去動作、解読された鍵を格納するメモリの上書き、鍵を格納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（例えば、そのセキュリティモジュールが不在の暗号システム）を実行する任意の他の方法等によって、任意の好適な様式で実行され得る。平行して例示されるが、関連データ、ＭＡＣ、及び／または暗号文を提供すること、ならびに鍵へのアクセスを失くすことは、連続して実行され得、その順序は、様々な実施形態の間で変動し得る。
【０１０４】
図２２は、様々な実施形態に従う、関連データを使用してポリシーを実施するために使用され得る、プロセス２２００の例示的な実施例を示す。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等の、任意の好適なシステムによって実行され得る。一実施形態では、プロセス２２００は、動作を実行するための要求を受信２２０２することを含む。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。一実施形態では、要求は、暗号サービスに提出される、暗号動作を実行するための要求である。要求の受信２２０２に応答して、プロセス２２００は、暗号文、ＭＡＣ、及び予測される関連データを得る２２０４ことを含み得る。暗号文、ＭＡＣ、及び予期される関連データを得る２２０４ことは、任意の好適な様式で実行され得る。例えば、いくつかの実施形態では、暗号文、ＭＡＣ、及び予期される関連データのうちの１つ以上が、要求において受信される。暗号文、ＭＡＣ、及び予期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、かつ／または、ローカルデータストア等のデータストアからアクセスされ得る。例えば、一実施形態では、暗号文とＭＡＣとは、要求の一部の連結された１対として受信される（ＡＥＳ－ＧＣＭまたはＡＥＳ－ＣＣＭ暗号の出力から生成され得る）。予期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、関連データを判断するために、要求者のＩＤが、直接的にまたは間接的に使用され得る。特定の実施例として、要求が、格納デバイス内に格納されるデータに関連して動作を実行するためのものである場合、関連データを得る２２０４ことは、データ格納デバイスの識別子を得ることを含み得る。識別子は、明示的に（例えば要求の一部として）または暗黙的に（例えば、データがデータ格納デバイス内に格納されると判断するために、他の情報が使用可能であるため）識別され得る。関連データは、データ格納デバイスの識別子であり得、またはそうでなければ、データ格納デバイスの識別子に少なくとも部分的に基づき得る。上記のように、関連データは、様々な実施形態の間で大幅に変動し得る。

【０１０５】
一実施形態では、プロセス２２００は、予期される関連データの真正性を判断するために使用可能な、参照ＭＡＣを生成２２０６することを含む。例えば、暗号文、関連データ、及び適切な鍵（要求において識別され得、または別様で判断され得る）が、参照ＭＡＣを生成２２０６するために使用される。ＭＡＣを生成することは、暗号文を得るために使用された同じ暗号を使用すること等によって、任意の好適な様式で実行され得る。参照ＭＡＣと得られたＭＡＣが一致するかどうかが判断２２０８され得る。例えば、様々な実施形態において他の種類の一致が使用され得ることが企図されるが、多くの暗号システムでは、ＭＡＣはそれらが同等である場合、一致する。参照ＭＡＣと得られたＭＡＣが一致すると判断２２０８される場合、一実施形態では、プロセス２２００は、関連データに少なくとも部分的に基づき、ポリシー情報にアクセス２２１０することを含む。ポリシー情報にアクセス２２１０することは、参照ＭＡＣを生成するため及び／または別の暗号動作を実行するために使用される、鍵ＩＤ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き、遠隔またはローカルデータストアから、１つ以上のポリシー（例えば、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。
【０１０６】
その後、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き、ポリシーが、要求された動作が実行されることを可能にするかどうか（例えば、ポリシーが、要求が遂行されることを可能にするかどうか）が、判断２２１２され得る。ポリシーが、要求された動作が実行されることを可能にするかどうかを判断することは、暗号文が、アクセスされたポリシー情報によって特定される関連データでタグ付けされるかどうかを判断することを含み得る。さらに、例示されないが、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くポリシー）もまた、ポリシーが、動作が実行されることを可能にするかどうかを判断するために、使用され得る。ポリシーが動作を可能にすると判断２２１２される場合、プロセス２２００は、動作を実行２２１４することを含み得る。しかしながら、ポリシーが動作を可能にしないと判断２２１２される場合、及び／または、参照ＭＡＣと得られたＭＡＣが一致しないと判断２２０８される場合、プロセス２２００は、上記のように、要求を拒否２２１６することを含み得る。
【０１０７】
上記の技術を使用して、様々なポリシーが実施可能である。例えば、述べられたように、実施されたときに、ポリシーが、その鍵を用いて何ができる及び／または何ができないかを判断するように、ポリシーは、鍵に関連付けられ得る。一実施例として、ポリシーは、データサービスがポリシーによって特定される特定の種類の動作のためだけに鍵を使用し得るということ（または、代替で、特定の動詞がデータサービスに禁止されるということ）を述べ得る。ポリシーは、使用条件、使用時間、ＩＰアドレス、何が暗号化され得るか、何が解読され得るか等、もまた特定し得る。例示的な実施例として、あるポリシーは、解読結果の提供は、解読のハッシュが特定の値と一致する場合にのみ可能にされると、特定し得る。したがって、暗号またはポリシーを実施する他のサービスは、平文のハッシュがポリシーに従わない場合、平文を提供し得ない。別の実施例として、ポリシーは、暗号文の解読は、暗号文が、特定の値と同等のまたは特定の値で開始する、関連データでタグ付けされる場合にのみ、可能にされるということを特定し得る。さらに別の実施例として、ポリシーは、暗号文の解読が、暗号文が関連データ内にコードされる格納デバイスの識別子でタグ付けされる場合にのみ、可能にされるということを特定し得る。
【０１０８】
概して、ポリシーは、暗号文に関連付けられるデータ（すなわち、認証された関連データ）の値に少なくとも部分的に基づいて、制限及び／または特権を特定し得る。いくつかの追加のポリシーは、解読は、解読を要求するコンピュータの識別子でタグ付けされた暗号文、解読を要求するコンピュータに搭載される（動作可能に接続される）格納ボリュームの識別子でタグ付けされた暗号文、及び／または他のコンピューティングリソースの識別子でタグ付けされた暗号文上でのみ、可能にされるということを特定するポリシーを含

む。コンピューティングリソースは、ポリシーを実施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またあり得る。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の外部のエンティティに明らかにされる（例えば、ユーザ及び／またはポリシーを実施する暗号サービスの外部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等の、他のポリシーは、本開示の範囲内であるとみなされる。上述のように、ポリシーは、ポリシーが修正され得る場合のために、条件もまた特定し得、これは少なくとも部分的に関連データに基づき得る。

【０１０９】

図２３は、図２２に関連して上記されるプロセス２２００の変形である、プロセス２３００の例示的な実施例を示し、ここにおいて、変形は、様々な実施形態に従う、ポリシーの実施におけるセキュリティモジュールの使用を例示する。一実施形態では、プロセス２３００は、暗号文を解読するための要求を受信２３０２することを含み、暗号文は、暗号化された鍵または他の暗号化されたデータであり得る。プロセス２３００は、図２２に関連して上記のように、暗号文、ＭＡＣ、及び予期される関連データを得る２３０４こともまた含む。図２３に例示されるように、一実施形態では、プロセス２３００は、暗号文を解読するためにセキュリティモジュールを使用２３０６することを含む。セキュリティモジュールを使用２３０６することは、暗号文を解読するために動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成することもまた含み得る。セキュリティモジュールは、平文及び予期される関連データに少なくとも部分的に基づき参照ＭＡＣを生成するためにもまた使用２３０８され得る。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、暗号文を解読して参照ＭＡＣを生成することは、単一の動作（例えばセキュリティモジュールへの単一の要求）において実行され得るということに留意すべきである。セキュリティモジュールから得られると、プロセス２３００は、図２２に関連して上記のように、参照ＭＡＣと得られたＭＡＣが一致するかどうかを判断２３１０することを含む。しかしながら、いくつかの実施形態では、プロセス２３００は、セキュリティモジュールに参照ＭＡＣが提供されて、参照ＭＡＣと得られたＭＡＣが一致するかどうかを判断するように、修正され得るということに留意すべきである。この変形では、セキュリティモジュールは、整合があるかどうかを示す応答を提供し得る。

【０１１０】

図２３に例示される実施形態に戻ると、参照ＭＡＣと得られたＭＡＣが一致すると判断２３１０される場合、プロセス２３００は、図２２に関連して上で述べられたように、少なくとも部分的に関連データに基づくポリシー情報にアクセス２３１２することを含む。さらに、上記のように、そのようには例示されないが、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。ポリシーが動作を可能にするかどうかが判断２３１４され得る。ポリシーが動作を可能にすると判断２３１４される場合、平文が提供２３１６され得る。図２２に関連して上記のように、ポリシーが動作を可能にしないと判断２３１４される場合、及び／または、参照ＭＡＣが得られたＭＡＣと一致しないと判断される場合、プロセスは、上記のように、要求を拒否２３１８することを含み得る。

【０１１１】

本開示の様々な実施形態が、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みなされる。例えば、本開示の実施形態は、概して、ポリシーを実施するために、暗号文を用いて検証可能なデータの使用に適用される。例示的な実施例として、ポリシーの表示は、第１の平文と組み合わされて、新平文（例えば、平文及びポリシーを含む新平文）を生成し得る。新平文は、ＡＥＳ等の好適な暗号を使用して暗号化されて、暗号文を生成し得る。暗号文を解読するための要求が受信されると、要求を受信するシステムは、暗号文を解読して、平文からポリシーを抽出して、ポリシーが第１の平文が提供されることを可能にするかどうかを点検し得る。ポリシーが

第１の平文が提供されることを可能にしない場合、要求は拒否され得る。かかる実施形態は、暗号の認証モードの関連データに関連して上記の実施形態の、代わりにまたはそれに加えて、使用され得る。

【０１１２】

本開示の様々な実施形態は、どのように監査が行われるかの条件を特定する鍵のポリシーもまた可能にする。例えば、鍵に関するポリシーは、鍵の監査レベルを特定し得、ここにおいて、監査レベルは、暗号サービスが鍵使用をどのように監査するかの決定因である、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、処理ユニットは、暗号サービスの一部化またはそれとは別個であり得る、監査システム（表示せず）と通信し得る。事象が、暗号動作の実行に関連して生じるとき、関連情報は、情報をログする監査システムに提供され得る。事象は、暗号動作を実行するための要求、及び／または、要求された動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、暗号サービスが解読動作を実行するように、成功裏に要求する場合、暗号サービスは、監査システム情報を提供して要求を可能にし得、その動作は実行された。管理アクセス事象、及び概して暗号サービスの任意の対話または動作は、事象に関与するエンティティ、事象を説明する情報、事象のタイムスタンプ、及び／または他の情報を識別し得る、関連情報でログされ得る。

【０１１３】

一実施形態では、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。低耐久性レベルについては、鍵の監査動作は、ベストエフォート基準の暗号サービスによって実行され得る。低耐久性レベルに従う監査を用いて、通常動作の間、全ての動作が監査されるが、暗号サービスの構成要素の失敗の事象において、いくつかの監査データが失われ得る。高耐久性レベルに従う監査を用いて、暗号動作の結果を明らかにする前に、動作が生じたという監査記録がメモリに耐久的にコミットされたという保証が得られる。必要とされる認知のために、高耐久性監査モードにおける動作は、低耐久性監査モードにおける動作よりも遅い。監査記録がメモリに耐久的にコミットされたという保証は、監査記録を格納するために使用される１つ以上の他のシステムからの認知を含み得る。したがって、前の段落を参照すると、暗号サービスは、監査システムからの、平文をもたらす解読の記録がメモリに耐久的にコミットされたという認知まで、平文をユーザに提供することを遅らせ得る。メモリに耐久的にコミットされるということは、データが耐久性の１つ以上の条件に従って格納されたということを意味し得る。例えば、データが非揮発性メモリに書き込まれた場合、及び／または、データが複数のデータ格納デバイスの間で重複して格納された（例えば、抹消コードまたは他の重複コードスキームを使用して）場合、データは、メモリに耐久的にコミットされ得る。

【０１１４】

一実施形態では、暗号サービスは、低耐久性及び高耐久性監査レベルのためのサブレベルを使用する。例えば、一実施形態では、それぞれのレベルは２つの別個の状態、可変状態及び不変状態に対応する。状態が不変または不変であるかは、状態間の移行がどのように生じるか及びそれが生じるかどうかを判断し得る。例えば、監査耐久性の例示的な実施例を使用すると、鍵に関するポリシーは、低耐久性可変と高耐久性可変との間を、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、変化することができ得る。しかしながら、暗号サービスは、鍵について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なると、移行が禁止されるように構成され得る。よって、鍵についてのポリシーが不変状態になると、ポリシーは変更され得ない。

【０１１５】

図２４は、オン（実施される）及びオフ（実施されない）になり得るポリシーに一般化した、かかるシステムの状態図の、例示的な実施例を示す。図２４に例示されるように、鍵についてのポリシーはオンまたはオフであり得る。オンでかつ不変である場合、ポリシーは、オンでかつ不変（変更不能）またはオフでかつ可変（変更可能）に変更され得る。同様に、ポリシーがオフであるが可変である場合、ポリシーは、オンであるが可変か、ま

たはオフでかつ不変に変更され得る。オフであるが可変であるポリシーからオンでかつ不変への直接移行等の、他の移行もまた使用可能であり得るということに留意すべきである。さらに、示される全ての移行が使用可能なわけではない。例えば、いくつかの場合では、鍵はオフでかつ不変の状態を有さないことがある。

【０１１６】

図２５は、システムが、鍵に適用可能な様々なポリシーの間の移行をどのように可能にし得るかを示す、一般化状態図を示す。本実施例では、３つのポリシー、ポリシーＡ、ポリシーＢ、及びポリシーＣが示される。これらのポリシーのそれぞれは、可変及び不変状態を有し、状態及びポリシー間で可能な移行が示される。例えば、不変状態からの移行は可能ではない。しかしながら、可変状態のポリシーは、可変状態の別のポリシーに変更され得る。例えば、鍵に関するポリシーは、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を用いて例示されるように、複数のポリシーに使用可能な移行があり得る。例えば、ポリシーＢから、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得る。図２４と同様に、他の移行及びポリシーが含まれ得、全てのポリシーが全ての状態を有するわけではない。さらに、様々な実施例が、不変及び可変状態のポリシーを示すが、ポリシーは、２つ以上の状態を有し得、ここにおいて、それぞれの状態は、実行され得るまたはされ得ない、１組の動作に対応する。例えば、半可変状態は、可変状態化で使用可能となり得る移行の、全てではないがいくつかを可能にし得る。

【０１１７】

述べられたように、ポリシーは、監査に加え様々な動作のために使用され得る。例えば、ポリシー移行についての上記の制限は、鍵細断能力に適用され得る。例えば、ポリシーは、鍵が細断され（取消不可に失われ）得るかどうかを示し得る。ポリシーは、４つの状態、細断可能－可変、細断可能－不変、細断不能－可変、及び細断不能－不変、を有し得る。上記のように、不変状態では、ポリシーは変更され得ない。別の実施例として、鍵がセキュリティモジュールからエキスポートされ得るかどうかに関するポリシーもまた、かかる４状態ポリシーを有し得る。

【０１１８】

ポリシーはさらに、鍵の使用がセキュリティ攻撃に対する脆弱性を可能にすることを防止するために、鍵に関連付けられ得る。例えば、一実施形態では、１つ以上の鍵は、特定の使用量後に鍵を退役させる（例えば、暗号化にもはや使用可能でなくなるようにマークする）自動回転ポリシーに関連付けられる。かかるポリシーは、ユーザ（例えば顧客）が起動させる及び／またはそのためにパラメータを提供する、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。ポリシーは、より大きい組の鍵（少なくともその顧客のために暗号サービスによって管理される全ての鍵を含む組）に適用可能なグローバルポリシーでもまたあり得る。この様式で、鍵は、それらが、十分な平文及び対応する暗号文の知識が鍵を判断する能力を提供する暗号攻撃を可能にするのに十分な回数使用される前に、退役させることができる。

【０１１９】

図２６は、様々な実施形態に従う、適切な間隔で鍵を回転させるために使用され得る、プロセス２６００の例示的な実施例を示す。プロセス２６００は、上記のセキュリティモジュール等の、任意の好適なデバイスによって実行され得る。一実施形態では、プロセス２６００は、鍵ＩＤによって識別される鍵を使用して、暗号動作を実行するための要求を受信２６０２することを含む。要求は、上記のように、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、データを暗号化もしくは解読するため、または、概して、鍵ＩＤによって識別される鍵を使用して、電子署名、別の鍵、もしくは鍵に少なくとも部分的に基づく他の情報の生成等の、任意の暗号動作を実行するための要求であり得る。要求の受信２６０２の際に、プロセス２６００は、要求された動作を実行２６０４することを含む。要求された動作を実行することは、動作を実行するために適切な版の鍵を選択すること等の、追加の動作を含み得る。例えば、動作が暗号化である場合、アクティブとマークされる鍵が暗号化するために使用され得る。動作が解読される場合、動作を実

行することは、解読するための、鍵ＩＤによって識別された適切な版の鍵を選択することを含み得、これは、様々な実施形態では、データを暗号化するために元来使用された鍵である。鍵は、様々な方法を通して選択され得る。例えば、いくつかの実施形態では、暗号文は、版、シリアル番号、日付、または鍵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では、データが適切に解読されるまで、それぞれの可能な鍵が試され得、ここにおいて、適切な解読は、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、関連データの正確さによって、判断され得る。

【０１２０】

暗号動作が実行２６０４されると、プロセス２６００は、鍵ＩＤによって識別されるアクティブ鍵のために鍵使用カウンタを更新２６０６することを含む。例えば、暗号動作が鍵の単一使用をもたらす場合、カウンタは１増加し得る。同様に、暗号動作が鍵のＮ（正の整数）回の使用をもたらす場合、カウンタはＮ増加し得る。カウンタが閾値を超えるかどうかが判断２６０８され得る。閾値は、鍵ＩＤによって識別される鍵の版に割り当てられる使用回数であり得る。閾値は、鍵のための動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、動作の初期数でもまたあり得る。カウンタが閾値を超えると判断２６０８される場合、一実施形態では、プロセス２６００は、新鍵を得る２６１０ことを含む。新鍵を得ることは、任意の好適な様式で実行され得る。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、新鍵を得ることは、新鍵を生成することまたは別のセキュリティモジュールから新鍵を得ることを含み得、これは、暗号サービスの動作者によって、編成され得る。あるセキュリティモジュールから別のセキュリティモジュールに鍵を渡すことは、提供する及び受信するセキュリティモジュールがアクセスを有する鍵を用いて、鍵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、暗号化された鍵を受信及び解読し得る。公開鍵の鍵交換技術もまた使用され得る。

【０１２１】

新鍵が得られると、一実施形態では、プロセス２６００は、現在のアクティブ鍵を退役とマーク２６１２することを含み得る。現在のアクティブ鍵を退役とマークすることは、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等によって、任意の好適な様式で実行され得る。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等によって、新鍵を鍵ＩＤに関連付ける２６１４こと、及び新鍵をアクティブとマークすることを含み得る。例示されないが、プロセス２６００は、別のセキュリティモジュールによる使用のために新鍵を提供することもまた含み得る。破線で示されるように、新鍵がプロセス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できた後のどこかの時点で、プロセスは、別の暗号動作を実行するための要求を受信２６０２することを含み得、プロセス２６００は上記のように進行し得る。さらに、カウンタが閾値を超えないと判断２６０８される場合、プロセス２６００は、終了し得、かつ／または別の要求が受信２６０２されると反復し得る。

【０１２２】

図２７は、様々な実施形態に従う、暗号サービスまたは他の環境において、鍵の自動回転を実行するために使用され得る、プロセス２７００の例示的な実施例を示す。プロセス２７００は、様々な実施形態に従う、鍵の使用を追跡し鍵回転を編成する、暗号サービスの構成要素等の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、鍵のための鍵動作の回数（例えば、複数の鍵のそれぞれのための動作の回数）を、１つ以上のセキュリティモジュールに割り当てる２７０２ことを含む。具体的な例として、１組の鍵を重複して格納／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では、それぞれのセキュリティモジュールは、それが管理する鍵のそれぞれのために１００万の動作が割り当てられ得る。動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間の同じデータセンター内にホストされ得る。例えば、いくつかの実施形態では、コンピューティング

リソースプロバイダは、複数の地理的区域における、複数のデータサービス内のセキュリティモジュールを利用して、地理的に分散した暗号または他のサービスを実装する。

【０１２３】

しかしながら、割り当ては、全てではないがいくつかの鍵のためになされ得、それぞれの鍵のための割り当ては同等でないことがあるということに留意すべきである。鍵動作を割り当てることは、鍵動作が割り当てられたそれぞれの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。通知は、それぞれの鍵に割り当てられた数を特定し得、または、いくつかの実施形態では、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が、セキュリティモジュールに、予めプログラムされたカウンタを再初期化するように、もしくは、カウンタに予めプログラムされた数を加えるように、示し得る。鍵動作をセキュリティモジュールに割り当てる２７０２際に、動作が割り当てられた鍵のそれぞれのための鍵使用カウンタが更新され得る。上記の具体例を続けると、５つのセキュリティモジュールのうちのそれぞれが、特定の鍵ＩＤによって識別される鍵のために１００万の動作を割り当てられた場合、鍵ＩＤのためのカウンタは、５００万増加（カウントが上向きまたは下向きのどちらかで実行されるかに依存して、上向きまたは下向きで）し得る。

【０１２４】

鍵動作を割り当てられた際に、セキュリティモジュールは、上記のような暗号動作を実行し得る。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く、それら自体のカウンタを維持し得る。上記の実施例では、セキュリティモジュールが、特定の鍵ＩＤによって識別される鍵のために１００万の動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（または既存のカウンタが残存動作を有した場合１００万を超える）に設定し得る。鍵を使用して暗号動作を実行する際に、セキュリティモジュールは、それに応じてそれ自体のカウンタを増加させ得る。

【０１２５】

ある時点で、１つ以上の鍵ＩＤについての割り当て枯渇事象が検出２７０６され得る。枯渇事象は、そのために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枯渇する、任意の事象であり得る。一実施例として、セキュリティモジュールは、特定の鍵ＩＤによって識別される鍵のための動作のその割り当てを使用し得、枯渇事象の検出は、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、対応する数の動作を実行したことによって、鍵ＩＤのためのその割り当てを枯渇した（または、その割り当ての枯渇の何らかの所定の閾値内である、もしくは、別様でその割り当てを間もなく枯渇させると予測される）という通知を受信することを含み得る。別の実施例として、いくつかの実施形態では、セキュリティモジュールは、誤動作、侵入もしくは他の改ざんの検出等の、特定の事象の際に、または、動作者がメンテナンス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、そこに格納される鍵（及びカウンタ等の鍵に関連付けられるデータ）へのアクセスを失うように構成される。したがって、枯渇事象は、誤動作または意図的行動の改ざん／侵入（メンテナンスのためにセキュリティモジュールを委託から一時的に取り出すこと等）の検出が故の、セキュリティモジュールの損失（一時的である可能性がある）を含み得る。本実施例では、セキュリティモジュールは、必ずしも割り当てられた数の動作を実行していなくても、その割り当てを使用したかのように扱われ得る。しかしながら、カウンタが永続的に格納され、よって対応する鍵へのアクセスの損失の際でさえ回復可能である場合等、特定の実施形態では、全てのかかる事象が枯渇事象を含むわけではないということに留意すべきである。枯渇事象は、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ということにもまた留意すべきである。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停電は、複数のセキュリティモジュールに影響を与える枯渇事象をもたらし得る。

【０１２６】

枯渇事象の検出の際に、カウンタが、枯渇事象に関連付けられる鍵のいずれかの閾値を超えるかどうかが、判断２７１０され得る。閾値は、暗号動作を実行するために使用され

る暗号の数学的特性に少なくとも部分的に基づく、動作の所定の数であり得る。例えば、ＣＢＣモードの暗号については、動作の数は、（１）ブロックにおいて発現する暗号文の長さと（２）暗号文の数との平方の積で割った、鍵空間の大きさであり得るかまたは別様でそれに少なくとも部分的に基づき得る。ＣＴＲモードの暗号（ＡＥＳ－ＧＣＭ）については、動作の数は、（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、鍵空間の大きさであり得るかまたは別様でそれに少なくとも部分的に基づき得る。カウンタが、枯渇事象によって影響を受けた鍵のいずれかについて閾値を超えると判断２７１０される場合、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、枯渇事象に関連付けられる１つ以上のセキュリティモジュール）に、動作の割り当てが枯渇した１つ以上の新鍵を得て、影響を受けた鍵（複数可）を新鍵（複数可）と交換するように命令２７１２することを含み得る。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（よって枯渇事象を引き起こし）、結果として、鍵ＩＤ（しかし必ずしも全ての鍵ＩＤではない）のカウンタに閾値を超えさせた場合、セキュリティモジュールは、上記のように、新鍵を得るように命令され得る（例えば、新鍵を生成すること、データ格納装置から予め生成された鍵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鍵を得ることによって）。しかしながら、あるセキュリティモジュールがオフラインにされて新しいセキュリティモジュールがオンラインにされる場合等、枯渇事象による影響を受けたセキュリティモジュールからの異なるセキュリティモジュールが、新鍵を得るように命令され得るということに留意すべきである。影響を受けた鍵（鍵ＩＤによって識別される）を、新鍵と交換することは、影響を受けた鍵を退役とマークすること、新鍵を鍵ＩＤと関連付ける（例えばデータベース内で）こと、及び新鍵をアクティブとマークすることを含み得る。影響を受けた鍵を新鍵と交換することは、新鍵のカウンタ（影響を受けた鍵を新鍵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また含み得、これは、予めプログラムされた値であり得、または、プロセス２７００を実行するシステムから得られる値であり得る。プロセス２７００は、例えばそれに応じてデータベースを更新すること等により、影響を受けた鍵（複数可）を退役、及び新鍵（複数）をアクティブとマーク２７１４することもまた含み得る。プロセス２７００を実行するシステムは、影響を受けた鍵及び／または新鍵（複数可）へのアクセスを有さないことがあり、結果として、影響を受けた鍵（複数可）を退役、及び新鍵（複数可）をアクティブとマークすることは、鍵の識別子を、退役または新であることを示す値と適切に関連付けることを含み得るということに留意すべきである。

【０１２７】

一実施形態では、マーク２７１４する際に、影響を受けた鍵のいずれもが閾値を超えるカウンタを有さないと判断２７１０される場合、プロセス２７００は、なおもアクティブな影響を受けた鍵（複数可）及び／またはプロセス２７００の動作の実行の結果として得られた任意の新鍵（複数可）のために、追加の鍵動作を割り当てる２７１６ことを含み得る。追加の鍵動作の割り当ての際に、適切な鍵使用カウンタ（複数可）が上記のように更新２７０４され得る。

【０１２８】

本明細書に記載される全てのプロセスと同様に、変形は、本開示の範囲内であるとみなされる。例えば、いくつかの実施形態では、セキュリティモジュールはそれらの鍵使用を追跡しないが、しかし、暗号または他のサービスの別の構成要素は、鍵を使用して１つ以上の動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たそれぞれの要求のために鍵のカウンタを更新する。かかる実施形態では、複数の鍵のうちのそれぞれの鍵について、セキュリティモジュールの構成要素は、鍵を使用して動作を実行するための要求を追跡（または例えば、要求がうまく遂行されたという認知または他の表示を通して、実行された動作を追跡）し、それに応じて鍵のカウンタを更新し得る。カウンタが閾値に到達すると、カウンタを維持するシステムは、全ての適切なセキュリティモジュールに、鍵を退役させ、鍵を新鍵と交換させ得る（または、鍵を有するセキュリティモジュールに鍵を退役させて、１つ以上の他のセキュリティモジュールに新鍵を使用し始めさせること等

の、鍵を退役させる何らかの他の動作を実行する）。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では、セキュリティモジュールが鍵動作のその割り当てを使用して、カウンタに閾値を超えさせる場合、セキュリティモジュールは、上記のように新鍵を得るように命令され得る。他のセキュリティモジュールは、それらがそれらの割り当てを使用するまで、鍵を使用し続け得る。セキュリティモジュールがその割り当てを使用する場合、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で鍵を交換した新鍵を得ることができる。換言すると、セキュリティモジュールは、新鍵を得なければならない前に、鍵動作のそれらの割り当てを使用し切ることが可能であり得る。

【０１２９】

図２８は、鍵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実施例の表示を示す。データベースは、プロセス２７００を実行するシステム等の、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、列は、それぞれ、鍵ＩＤ、鍵版、使用可能性、及びカウンタに対応する。鍵ＩＤ及び鍵版は、上記の通りであり得る。使用可能性の列における値は、鍵が退役またはアクティブのいずれであるか（または、かかる他の状態が本開示の様々な実装によって支持される場合、鍵が別の状態を有するかどうか）を示し得る。図２８で例示されるように、データベースは、全ての退役版及びアクティブ版を含む、鍵ＩＤによって識別される鍵のそれぞれの版のための行を有する。しかしながら、データベースは鍵の全ての版を欠如し得るということに留意すべきである。例えば、鍵は、様々なセキュリティの理由のために、格納装置から永続的に除去され得る。除去は、例えば、顧客の要求またはポリシーの実施に準じ得る。

【０１３０】

図２８に例示されるように、例示されるデータベースはそれぞれのアクティブ鍵のためのカウンタもまた含む。さらに、この特定の実施例では、データベースは、非アクティブ鍵のためのカウンタ（例えば、閾値を超えるそれぞれの鍵の値を示し、それによって新鍵を得させる）を含む。しかしながら、非アクティブ鍵のカウンタ値は、いくつかの実施形態では保持されないことがある。カウンタは、鍵動作がセキュリティモジュールに割り当てられる際に、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。カウンタ行における値が閾値を超えると、カウンタ値が閾値を超えた鍵を交換するための新鍵を収容するために、データベースに新しい行が加えられ得る。

【０１３１】

セキュリティモジュールは、それら自体の目的のために、同様のデータベースを維持し得る。例えば、セキュリティモジュールは、それ自体の鍵使用を追跡し得、セキュリティモジュールによる鍵使用がセキュリティモジュールに割り当てられた数を枯渇させた場合、セキュリティモジュールは、暗号サービスの（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）鍵回転管理構成要素に通知し得、これは、例えば、上記のプロセス２７００等のプロセスを実行して、セキュリティモジュールに追加の動作を再び割り当て得、または、鍵のために使用可能な多数の鍵動作が枯渇した場合、セキュリティモジュールに新鍵を得させ得る。

【０１３２】

鍵使用を追跡するために使用されるデータベースは、図２８に例示される及び上記のものから変化し得る。例えば、生成の時間、退役の時間、鍵が使用される顧客についての情報、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等の、鍵に関連付けられるメタデータ等の、追加の情報がデータベース内に含まれ得る。さらには、関係表が例示の目的のために提供されるが、様々な実施形態を支持してデータを格納する他の方法が使用され得る。

【０１３３】

ポリシーを実施するために使用される情報は、様々な方法で暗号サービスによって得られ得る。図２９は、本開示の様々な実施形態が実践され得る環境２９００の例示的な実施例を示す。環境２９００の構成要素は、上記のもののような構成要素を含み得る。例えば、例示されるように、環境２９００は、ユーザデバイスを通して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）と対話する、ユーザを含むが、ユーザにとって代わって、データサービスフロントエンドと対話するように構成される任意のコンピュータシステムであり得る。さらに、例示されるように、環境は、データサービスバックエンド格納システム及び認証サービスを含み、これらは上記の通りであり得る。さらに、環境は、図２９で、図で外部暗号サービスと標識される別の暗号サービスと区別するために、内部暗号サービスと標識される暗号サービスを含み得る。内部及び外部暗号サービスのいずれかまたは両方は、上記のように、暗号サービスとして動作し得る。本明細書に記載される全ての環境と同様に、変形は、本開示の範囲内であるとみなされる。例えば、図２９は、データサービスフロントエンドと通信するユーザを示すが、ユーザは、上記のようなデータサービスフロントエンドを用いずに暗号サービスと通信し得る。

【０１３４】

環境２９００にさらに含まれるのは、一実施形態では、内部暗号サービスからの要求に応答して、少なくともメッセージを、アカウントによって表され得る１人以上の加入者に、公開するように構成されるコンピュータシステム（例えばコンピュータまたはコンピュータのネットワーク）である、メッセージサービスである。以下により詳細に記載されるように、いくつかの要求は、環境２９００内の構成要素が、メッセージサービスを使用して要求についてのメッセージを伝送するように、動作することを引き起こし得る。例えば、いくつかのデータは、解読要求への応答は特定の時間量で遅延させなければならないという、関連ポリシーを有する鍵下で、暗号化されて格納され得る。データを解読するための要求が提出される場合、ポリシーの実施は、遅延した応答及びメッセージサービスによって送信されるべき通知をもたらし得る。このようにして、ユーザまたはメッセージを監視するコンピュータシステムは、遅延の間に、解読要求を中止するための要求を提出するか、または別様で解読要求を中止させる機会を有し得る。メッセージサービスは、電子メール、ショートメッセージサービス（ＳＭＳ）、電話、ページング、ファクシミリ、及び／またはメッセージサービスから別のエンティティへの情報の伝送に有用な任意の好適な技術を含むがこれらに限定されない、１つ以上の技術を使用して、１人以上の加入者にメッセージを伝送し得る。

【０１３５】

図２９に例示されるように、データサービスフロントエンドに提出される要求は、鍵アクセス注釈を含み得る。例えば、示されるように、ユーザによって提出されるｇｅｔ要求は、鍵アクセス注釈を含む。鍵アクセス注釈は、環境２９００の１つ以上の構成要素によるポリシーの実施に必要な情報を含み得る。鍵アクセス注釈は、鍵を使用して生成される電子証明を含み得るか、または別様でそれを提供され得る。署名を生成するために使用される鍵は、ユーザとポリシーを実施する環境２９００の構成要素との間で共有される鍵であり得、公開鍵デジタル署名スキームを利用するいくつかの実施形態では、鍵はユーザの秘密鍵であり得、それによって、対応する公開鍵を使用して検証可能な署名を与える。ポリシーを実施する環境２９００の構成要素は、電子署名を使用して、鍵アクセス注釈内の情報の真正性を検証し得、かつ、鍵アクセス注釈内の情報を使用して、ポリシーが、要求が遂行されることを可能にするかどうかを判断し得る。

【０１３６】

図２９に例示されるように、環境２９００のいくつかの構成要素のいずれも、鍵アクセス注釈を受信して鍵アクセス注釈をポリシーの実施のために使用し得る。例えば、データサービスフロントエンドは、鍵アクセス注釈を、上記のように使用され得る暗号文及び認証証明と共に、内部暗号サービスに渡し得る。内部暗号サービスは、鍵アクセス注釈を使用して、内部暗号サービスによって管理される鍵のポリシーを検証し得る。いくつかの実施形態では、鍵アクセス注釈は、外部暗号サービス等の別のサービスを識別する情報を含む。内部暗号サービスは、外部暗号サービスを識別する情報を検出する際に、鍵アクセス注釈を外部暗号サービスに提供し得、これは、かかる他のサービスは図２９には例示されないが、複数の暗号サービスまたは鍵アクセス注釈を使用する他のサービスのうちの１つであり得る。

【０１３７】
上記のように、様々な実施形態に従って管理される鍵は、鍵の使用の制限及び／または特権をコードするポリシーに関連付けられ得る。ポリシー実施に関連する他の情報もまた、様々な実施形態に従って、かかる鍵に関連付けられ得る。図３０は、鍵３０００（上記のように暗号サービスによって管理される鍵等）の例示的な実施例及び鍵３０００に関連して維持され得る（例えば暗号サービスによって）情報の実施例を示す。例示されるように、鍵３０００の１つ以上のポリシーをコードするポリシー情報は、上記のように鍵３０００に関連して維持される。一実施形態では、鍵の組もまた鍵３０００に関連して（例えばデータベースまたは他のデータ格納システムによって鍵３０００に関連付けられる）維持される。関連付けは、任意の好適な様式で維持され得る。例えば、関係表または他の機構が鍵３０００を鍵の組の中の鍵と直接的に関連付け得る。別の例として、関係表または他の機構は、鍵３０００を、鍵３０００に関連付けられる組の中の鍵の識別子及び／またはそれへの参照と、関連させ得る。

【０１３８】
例えば、いくつかの実施形態では、使用鍵組の１つ以上の鍵及び管理鍵組の１つ以上の鍵が、鍵３０００に関連して維持される。一実施形態では、暗号サービスは、使用鍵組の中の鍵が、いくつかの実施形態において、少なくともいくつかの要求を遂行するために必要となるように、構成される。特に、いくつかの実施形態では、要求が鍵ＩＤによって識別される鍵を使用して動作を実行するためには、要求の遂行は、おそらく、とりわけ、鍵アクセス注釈が、使用鍵組の中の鍵に対応する鍵（例えば、使用鍵組内の任意の鍵、または鍵アクセス注釈によって特定されるもしくは別様でそれに関連する使用鍵組の中の鍵）によって電子（すなわちデジタル）署名されることを要求し得る。かかる署名が存在しない場合、要求は拒否され得る。使用鍵組の中の鍵に対応する鍵は、使用鍵組の中の鍵またはそれへの参照であり得るか、または、使用鍵組の中の公開鍵に対応する秘密鍵であり得る（ここにおいて公開鍵及び秘密鍵は公開鍵デジタル署名スキームにおいて使用される）。

【０１３９】
一実施形態では、管理鍵組の中の鍵は、鍵３０００に関連付けられる鍵の組を修正する目的のために、使用される。例えば、いくつかの実施形態では、使用鍵組または管理鍵組のいずれか（または両方）を修正するための要求が遂行されるためには、管理鍵組の中の鍵に対応する鍵を使用する電子署名が要求され得る。修正は、鍵を鍵組に加えること、鍵組から鍵を除去すること、鍵組の中の鍵を別の鍵と交換すること、鍵組の中の鍵を別のエンティティと再関連付けすること、及び／または他の修正を含み得る。換言すると、管理鍵へのアクセスの証明が、使用鍵組及び／または管理鍵組を修正するために必要とされる。管理鍵は、鍵３０００に適用可能なポリシーの修正及び／または他の管理行動のため等の、他の目的のために同様な方法で使用され得る。図３０に例示されるように、鍵３０００は、動作ビットマスクともまた関連付けられ得る。情報ビットマスクは、鍵３０００がそのために使用され得る動作の組をコードする情報であり得るが、かかる情報はポリシーによってコードされ得る。

【０１４０】
セキュリティモジュールによって管理される鍵に関連する様々な鍵組の使用は、多数の技術的利点を提供する。例えば、図３０を参照すると、鍵３０００に関連付けられる鍵組の中の鍵が危殆化される場合、鍵組は修正されて、鍵３０００を変更する必要なく、データ危険から保護することができる。別の例として、平文にアクセスするためにエンティティ間の共謀が要求されるように、単一のエンティティが、暗号文及び暗号文を解読するのに必要な鍵の両方へのアクセスを有さないように、第三者の鍵が使用され得る。

【０１４１】
図３１は、一実施形態に従う、鍵アクセス注釈３１００の実施例の例示的な表示を示す。図３０では、鍵アクセス注釈３１００は、鍵アクセス注釈がそのために含まれる要求に関連する、ポリシーの実施に関連する情報を含む。本実施例では、鍵アクセス注釈は、タ

イムスタンプ（タイムスタンプ）、及び動作記述子（動作記述子）、使用鍵組または管理鍵組の鍵の、鍵保持者識別子（鍵保持者ＩＤ）、鍵ＩＤ、及び識別子を含むが、より少ないまたはより多い情報が含まれ得る。

【０１４２】

一実施形態では、鍵アクセス注釈３１００内の情報は、要求が遂行され得るかどうかを判断するために使用される。特に、いくつかの実施形態では、鍵アクセス注釈３１００内の情報は、要求が遂行されるために、（必須の電子署名が存在することに加えて）１つ以上の条件を満たさなければならない。例えば、いくつかの実施形態では、タイムスタンプが、要求がいつ受信されたかの何らかの閾値時間量内の時間を示さなければならない。別の例として、鍵アクセス注釈は、動作カウント窓内になければならないか、特定のデータに関連して特定の動作を許可しなければならないか、または、別様で、鍵アクセスを受信したエンティティによって実施される１つ以上の条件を満たさなければならない。

【０１４３】

鍵保持者ＩＤは、本開示の様々な実施形態に従う、連合鍵管理を可能にし得る。図２９を参照すると、例えば、鍵保持者ＩＤは、鍵ＩＤによって特定される鍵を識別するまたはその識別を別様で可能にする情報であり得る。鍵保持者ＩＤは、例えば、ユニフォームリソースロケータ（ＵＲＬ）、インターネットプロトコル（ＩＰ）アドレス、または鍵アクセス注釈を対応するエンティティに提供する（例えば、注釈を含む要求を転送することによって）ために鍵保持者ＩＤの使用を可能にする他の情報であり得る。いくつかの実施形態では、要求の受信者が鍵保持者ＩＤを抽出することができ、適切であれば、要求を適切な第三者に転送することができるように、鍵保持者ＩＤは、鍵ＩＤにおいてコードされる。環境２９００の内部暗号サービスは、例えば、要求の鍵保持者ＩＤが異なるエンティティを特定するかどうかを検出し、異なるエンティティを特定する鍵保持者ＩＤの検出の際に、要求（または、要求に少なくとも部分的に基づく他の情報）を、上記のような外部暗号サービス（例えば、異なるコンピューティングリソースプロバイダの暗号サービス）であり得る、異なるエンティティに転送するように構成され得る。異なるエンティティは本開示の様々な実施形態を利用して、要求に応答するかどうかを判断し得、適用可能であれば、要求に応答を提供し得、これは、暗号サービスを通して提供され得る。鍵アクセス注釈が鍵保持者ＩＤを欠く（または鍵保持者ＩＤが内部暗号サービスを特定する）場合、内部暗号サービスは、ポリシー及び要求遂行のための他の要件との準拠を想定して、要求を自体で遂行し得る。

【０１４４】

図３２は、上記のような、鍵アクセス注釈に関連して提出される要求との関連で、ポリシーを実施するために使用され得る、プロセス３２００の例示的な実施例を示す。プロセス３２００は、要求処理に関与する暗号サービスのデバイス（例えば、暗号サービスのためのフロントエンドＡＰＩを実装するデバイス）等の、任意の好適なデバイスによって実行され得る。暗号サービスは、上記のような、内部または外部暗号サービスであり得る。

【０１４５】

一実施形態では、プロセス３２００は、要求に関連して鍵アクセス注釈を受信３２０２することを含む。鍵アクセス注釈は、要求と共に含まれる注釈であり得、または他の方法で受信され得る。例えば、鍵アクセス注釈を有する要求は処理され得、処理の一部として、鍵アクセス注釈は、プロセス３２００（またはその変形）を実行するデバイスに提供され得る。鍵アクセス注釈が受信されると、一実施形態では、プロセス３２００は、注釈を使用して上記のような参照署名を生成３２０４することを含む。参照署名が注釈の署名と一致するかどうかが判断３２０６され得る。代替の実施形態では、プロセス３２００は、鍵アクセス注釈を、セキュリティモジュールが、参照署名を生成して、参照署名が鍵アクセス注釈の署名と一致するかどうかを点検することができるようにする情報と共に、セキュリティモジュールに提供することを含むということに留意すべきである。換言すると、鍵アクセス注釈の署名が有効であるかどうかを判断することは、セキュリティモジュールからかかる判断を得ることによって実行され得る。

【０１４６】
参照署名が注釈の署名と一致すると判断３２０６される場合、プロセス３２００は、要求において特定される鍵ＩＤに関連付けられる任意のポリシーにアクセス３２０８することを含み得る。ポリシーが鍵ＩＤのために存在することを想定すると、プロセス３２００は、アクセスされたポリシーが、要求の遂行を可能にするかどうかを判断３２１０することを含む。ポリシーが要求の遂行を可能にすると判断３２１０される場合、プロセス３２００は、鍵保持者ＩＤ（上記のような）が外部エンティティを識別するかどうかを判断３２１２することを含み得る。鍵保持者ＩＤが外部エンティティを識別するかどうかを判断３２１２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、鍵アクセス注釈内の鍵保持者ＩＤの不在は、否定判断を示し得、一方で、鍵アクセス注釈内の鍵保持者ＩＤの存在は、肯定判断を示し得る。別の例として、鍵保持者ＩＤは、内部エンティティ（例えば、内部暗号サービス）または外部エンティティ（例えば、外部暗号サービス）のいずれかを示す、要求される値であり得る。

【０１４７】
鍵保持者ＩＤが外部エンティティを識別しないと判断３２１２される場合、プロセス３２００は、上記のように、要求を遂行３２１４することを含み得る。しかしながら、鍵保持者ＩＤが、外部エンティティを識別すると判断３２１２される場合、プロセス３２００は、要求を識別された外部エンティティに転送３２１６すること、及び応答して、要求遂行を可能にする情報を受信３２１６することを含み得る。情報は、例えば、外部エンティティによって暗号文を解読することによって得られた平文、及び／または、外部エンティティによって実行される暗号動作に少なくとも部分的に基づく情報であり得る。例示されないが、加えてまたは代替として、他の情報もまた受信され得る。例えば、外部エンティティが、独立して、要求の遂行を可能にしない（例えば、外部エンティティによって実施されるポリシーが、要求が遂行されることを可能にしないため）ことを判断する場合、拒否を示す情報が提供され得る。要求遂行を可能にする情報が受信３２１６されると想定すると、プロセスは、上記のように、要求を遂行３２１４することを含み得る。例えば、要求遂行を可能にする受信された情報は、要求者に提供され得る。

【０１４８】
明示的に上で述べたものに加えて、変形もまた、本開示の範囲内であるとみなされる。例えば、図３２は、要求のために、電子署名及びポリシーを検証すること、ならびに後続の、要求（またはそれに少なくとも部分的に基づく情報）を外部エンティティに転送することを例示する。本明細書に例示される全てのプロセスと同様に、動作の順序は変動し得る。例えば、プロセス３２００は、あらゆる署名及び／またはポリシー検証が行われる前に、要求が転送されるように、修正され得る。外部エンティティは、プロセス３２００を実行するシステムに加えてまたはその代わりに、署名及び／またはポリシー検証を実行し得る。例えば、いくつかの実施形態では、プロセス３２００の動作を実行するシステムは、署名及び／またはポリシー検証を実行せず、かかる検証を外部エンティティに残す。他の実施形態では、プロセス３２００の動作を実行するシステムは、署名及び／またはポリシー検証を実行し、外部エンティティは追加の署名及び／またはポリシー検証を実行する。外部エンティティは、例えば、要求が遂行される前に点検される、異なる鍵及び／または異なるポリシーを設定して有し得る。

【０１４９】
本開示の実施形態は、強化されたデータセキュリティを提供する技術もまた利用する。例えば、最善の努力にもかかわらず、様々なシステムに関連してセキュリティ違反がしばしば生じる。かかる違反の効果を軽減するために、本開示の様々な実施形態は、違反を検出してそれに応じて応答するための時間を提供する様式で、要求処理を可能にする。例えば、いくつかの実施形態では、暗号化されたデータの解読及び／または解読されたデータへのアクセスは遅延を要求する。遅延が、例えば、システムの構成によって、またはシステムによって実施されるポリシーによって、要求され得、ここにおいて、ポリシーは、本明細書に記載される様々な実施形態に従って構成される。かかる遅延は、例えば、規制ま

たは他の要件が、特定のデータが到達されることを必要とするが、そのデータが即座に使用可能になることを必ずしも必要としない場合等の、暗号化されたデータへの迅速なアクセスが不必要である状況において、有用であり得る。

【０１５０】

図３３は、様々な実施形態に従う、かかる遅延を提供するための、プロセス３３００の例示的な実施例を示す。プロセス３３００は、上記のような内部または外部暗号サービス等の、暗号サービスによって実行され得る。一実施形態では、プロセス３３００は、鍵ＩＤによって識別される鍵を使用して暗号文を解読するための要求を受信３３０２することを含む。要求は、任意の好適な様式で受信され得る。例えば、要求は、上記のように、ユーザからまたはデータサービスから受信され得る。一実施形態では、鍵ＩＤに関連付けられるポリシーがアクセス３３０４される。しかしながら、ポリシーは、いくつかの実施形態では自動的に実施され得、結果として、ポリシーはいくつかの実装ではアクセスされ得ないということに留意すべきである。図３３に例示される実施形態に関して、プロセス３３００は、ポリシーが要求遂行を可能にするかどうかを判断３３０６することを含む。ポリシーが要求遂行を可能にするかどうかの判断３３０６は、上記のような、任意の好適な様式で実行され得る。

【０１５１】

アクセスされたポリシーが、要求の遂行を可能にすると判断３３０６される場合、プロセス３３００は、アクセスされたポリシーのうちの１つ以上の間の時間遅延ポリシーの検出３３０８を含み得る。しかしながら、上記のように、いくつかの実施形態では、時間遅延は自動的であり得、結果として、かかるポリシーの検出は生じ得ない。プロセス３３００は、タイマーを起動３３１０して警報プロセスを実行することを含み得る。タイマーは、所定の時間量についてのタイマーであり得、これは、いくつかの実施形態では、例えば時間遅延ポリシーの一部として構成され得る、構成可能な量である。タイマーは、プロセス３３００を実行するシステムのシステム構成設定内に予め定められ得る。警報プロセスは、様々な警報行動を実行させるように構成されるワークフローの実行を含み得る。警報行動は、例えば、通知システム（上記のような）に、１つ以上のメッセージを、１つ以上の個人またはシステムに伝送させることを含み得る。例えば、暗号化されたデータに関連する組織の法令順守責任者が通知を受け得る。別の例として、警報行動は、監査システムに、例えば、システムへの様々なアクセスに関連してより多くの情報が収集される、強化された監査を実行させることを含み得る。いくつかの実施形態では、警報行動は、警報の可聴及び／または視覚表示を含み得る、警報信号を送ることもまた含み得る。他の警報行動が、本開示の範囲内であるとみなされる。

【０１５２】

タイマーの起動の際に、プロセス３３００は、タイマーが実際に切れたことが判断３３１２されるまで、タイマーが切れたかどうかの点検３３１２を実行することを含み得る。いくつかの実施形態では、要求はその遂行の前に中止され得る。要求を中止することは、情報を解読するための要求よりも、より緊縮でない要件を要求し得る。例えば、いくつかの実施形態では、要求は、システムへのアクセスを有する誰かによって、些細に中止され得る。別の例として、警報行動は、選択されると、メッセージの受信者による認証を伴わずに、要求に中止されるべき要求を中止させるハイパーリンクを含む、メッセージの伝送を含み得る。要求が中止されることを可能にする他の方法もまた使用され得る。したがって、一実施形態では、タイマーが切れると（または、タイマーが切れる前等の他の時）、要求が中止されたかどうかが判断３３１４され得る。要求が中止されたと判断３３１４される場合、プロセス３３００は、例えば、鍵ＩＤによって識別される鍵を使用し、暗号文を解読して生じる平文を提供することによって、または、セキュリティモジュールに暗号文を解読させて対応する平文を提供させ、その後平文を要求者に移送するかもしくは別様で平文へのアクセスを提供することによって、要求を遂行３３１６することを含み得る。しかしながら、要求が中止されなかったと判断３３１４される場合、及び／または、ポリシーが要求の遂行を可能にしないと判断３３０６される場合、プロセス３３００は、上記

のように、要求を拒否することを含み得る。

【０１５３】

多数の他の変形は本開示の範囲内である。例えば、いくつかの実施形態では、鍵は、有効日付を特定するかまたは無限ではない何らかの所定の有効期間を示すポリシーに関連付けられる。例えば、いくつかの実施形態では、鍵は、鍵が特定の時間量後に、特定の日付に、または別様で１つ以上の条件を満たす際に、破壊されるべきであるということを特定する、ポリシーに関連付けられ得る。一実施例として、組織及び／または政府の規則、法律、ポリシー、または規制は、データが特定の時間量の間保持されなければならないということを特定し得る。かかるデータを暗号化するために使用される鍵（例えば、データを暗号化するために暗号において使用される鍵、または、その下でデータが暗号化される別の鍵を暗号化するために暗号において使用される鍵）のポリシーは、要求される時間量の経過の際に鍵が破壊される（すなわち、取消不可に誰にもアクセス不能にさせる）べきであるということを特定し得る。暗号サービスまたは他のシステムは、要求される時間量の経過を検出し得、それに応じて鍵を破壊し得る。暗号サービスは、多くの方法で、必要とされる時間量の経過を検出し得る。例えば、いくつかの実施形態では、暗号サービスは、その中に鍵破壊の時間を示す情報が格納されている、データベースを維持する。暗号サービスによって実行される周期的プロセスは、データベース内で破壊可能と示される鍵を破壊し得る。

【０１５４】

ポリシー有効日付は、他の方法でもまた使用され得る。例えば、データの解読のために実施される時間遅延は、時間が経過するにつれて変化し得る。例えば、鍵下で暗号化されたデータが古くなると、データを解読するために実施される時間遅延は減少し得る。別の例として、プリンシパルは、特定の期間の時間の間のみ鍵を使用して暗号動作を実行させる特権を有し得、これは、暗号サービスのＡＰＩを通して再生可能であり得る。このようにして、個人が、鍵に関連して暗号動作を実行させる能力は、自動的に切れ得る。

【０１５５】

いくつかの実施形態では、要求は、暗号文を解読するための要求に加えてまたはその代替として、他の目的のためになされ得る。例えば、上記の様々な技術は、様々な種類のポリシー実施に適合され得る。例えば、本開示の様々な実施形態に関連して利用されるポリシーは、ポリシーのための有効時間を利用し得る。ポリシー更新は、ポリシー更新がポリシーを実施するシステムにおいて有効となる将来の時点を示す、有効時間を有し得る。既存のポリシーは、いくつかまたは全てのポリシー変化が、特定の条件下で可能であることを要求し得、このうちの１つは、ポリシー更新が将来への特定される時間量（例えば４８時間）である有効時間を有することである。データの解読を含み得る、データの回復を可能にするために、ポリシーを変更するための要求がなされ得る。要求は、例えば、データが回復され得る前に満たすことが要求される条件を弱化させるための要求であり得る。要求は、ポリシー変更の有効時間を特定し得る。ポリシーが適用されるプリンシパルに関連してポリシーを実施するシステムは、有効時間が既存のポリシーを順守するかどうかに少なくとも部分的に基づいて、要求を承認または拒否し得る。システムがポリシー変更を承認する場合、システムは、タイマー（少なくとも部分的に有効時間に基づき得る）を起動し得、上記のように警報プロセスを実行し得る。さらに、ポリシー変更は、上記のように、要求が遂行されるまで中止可能であり得る。この様式で、当事者は、データへの許可のないアクセスを防止するために、通知及び機会が提供され得る。

【０１５６】

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。

付記１．コンピュータ実装方法であって、

実行可能命令で構成される１つ以上のコンピュータシステムの制御下で、

コンピューティングリソースプロバイダへの、要求によって特定される鍵を使用して暗号文を解読するための該要求を受信することであって、該要求が、該要求が遂行されるのに十分な１つ以上の条件の組を満たす、受信することと、

該要求が保留されている間の時に、該要求の１つ以上の通知を、該鍵に対応する顧客の１つ以上のコンピュータシステムに伝送することと、
該要求の保留の間に該要求を中断することを可能にすることと、
該暗号文を解読して平文を得ることと、
少なくとも所定の時間量が経過し、かつ該要求が中断されなかったことの結果として、該平文を提供することと、を含む、該コンピュータ実装方法。
付記２．該所定の時間が該顧客によって構成可能である、付記１に記載のコンピュータ実装方法。
付記３．該１つ以上の通知を伝送することが、通知を受信するように指定される１人以上の個人に電子メッセージを送信することを含む、付記１または２に記載のコンピュータ実装方法。
付記４．該要求を中断するのに十分な１つ以上の条件を満たすことが、要求を遂行するのに不十分である、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。
付記５．該要求の結果として、該暗号文に関連して追加の監査機能を実行することをさらに含む、付記１～４のいずれか一項に記載のコンピュータ実装方法。
付記６．該平文を提供することが、該平文の提供における遅延を実施することを含み、
該１つ以上の通知を伝送すること及び該遅延を実施することが、該鍵に対応するポリシーの構成の結果として、実行される、付記１～５のいずれか一項に記載のコンピュータ実装方法。
付記７．コンピュータ実装方法であって、
実行可能命令で構成される１つ以上のコンピュータシステムの制御下で、
平文にアクセスするための認証された要求を受信することであって、その遂行が１つ以上の暗号動作を要求する、該受信することと、
該要求の遂行に対応する該要求への応答が提供される前に、プログラムされた遅延が要求されるように、該要求を処理することと、
該遅延後に該要求への応答を提供することと、を含む、該コンピュータ実装方法。
付記８．該１つ以上の暗号動作が暗号文の解読を含む、付記７に記載のコンピュータ実装方法。
付記９．該１つ以上の暗号動作が電子署名を生成することを含む、付記７または８に記載のコンピュータ実装方法。
付記１０．該所定の遅延が、暗号文を解読するための鍵に対応するポリシーの結果として要求される、付記７～９のいずれか一項に記載のコンピュータ実装方法。
付記１１．該要求の１つ以上の通知を、該要求を中断する権利を有する１つ以上のエンティティに送信することをさらに含む、付記７～１０のいずれか一項に記載のコンピュータ実装方法。
付記１２．該遅延の間に該要求を中断する能力を可能にすることをさらに含む、付記１１に記載のコンピュータ実装方法。
付記１３．認証された該要求が、該要求が中断されない限り、該応答を提供させるのに十分である、付記７～１２のいずれか一項に記載のコンピュータ実装方法。
付記１４．該要求の結果として、増加した監査を引き起こすことをさらに含む、付記７～１３のいずれか一項に記載のコンピュータ実装方法。
付記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、
該１つ以上のプロセッサによって実行されると、該コンピュータシステムに、
要求者からの、認証されたデータにアクセスする要求に関連するトリガーを検出することであって、該データにアクセスすることが１つ以上の暗号動作の実行を必要とする、該検出することと、
該トリガーの検出の結果として、該データが該要求者にアクセス可能になる前に、予めプログラムされた時間量を経過させることであって、該要求が該時間量の経過の間に該要求者とは異なるエンティティによって中断可能である、該経過させることと、を行わせ

る命令を含む、メモリと、を備えるコンピュータシステム。
付記１６．該システムがメッセージングサブシステムをさらに備え、
該命令が、該コンピュータシステムに、該メッセージングサブシステムに該要求の通知を伝送させることを、さらに行わせる、付記１５に記載のコンピュータシステム。
付記１７．該トリガーが、該１つ以上の暗号動作のために要求される鍵に関するポリシーである、付記１５または１６に記載のコンピュータシステム。
付記１８．該コンピュータシステムがコンピューティングリソースプロバイダによってホストされ、
該要求が、該コンピューティングリソースプロバイダの顧客から該コンピューティングリソースプロバイダによって受信される、付記１５～１７のいずれか一項に記載のコンピュータシステム。
付記１９．該所定の時間量が該顧客によって設定可能である、付記１８に記載のコンピュータシステム。
付記２０．該命令がさらに、該コンピュータシステムに該１つ以上の暗号動作を実行させる、付記１５～１９のいずれか一項に記載のコンピュータシステム。
付記２１．コンピュータシステムの１つ以上のプロセッサによって実行されると、該コンピュータシステムに、
要求者からの認証されたデータにアクセスする要求に関連するトリガーを検出することであって、該データにアクセスすることが１つ以上の暗号動作の実行を必要とする、該検出することと、
該トリガーの検出の結果として、時間量の間該要求を該要求者とは異なるエンティティによって中断可能にさせることと、を行わせる命令をそこに集合的に格納した、１つ以上のコンピュータ可読媒体。
付記２２．該時間量が所定の時間量である、付記２１に記載のコンピュータ可読格納媒体。
付記２３．該命令がさらに、該コンピュータシステムに、該要求の１つ以上の通知の別のコンピュータシステムへの伝送を行わせることを引き起こす、付記２１または２２に記載のコンピュータ可読格納媒体。
付記２４．該１つ以上の暗号動作が鍵を使用し、
該トリガーが、該時間量の間該要求が中止可能であることを要求する該鍵についてのポリシーである、付記２１～２３に記載の１つ以上のコンピュータ可読格納媒体。
付記２５．該要求の有効性が、１つ以上の条件を満たすことを要求し、かつ、
該１つ以上の条件のうちの少なくとも１つが満たされなくても該要求の中止が可能である、
付記２１～２４のいずれか一項に記載の１つ以上のコンピュータ可読格納媒体。
付記２６．該命令がさらに、該システムに、該データにアクセスするための要求の通知を受信するように特定される１人以上の個人に通知させる、付記２１～２５にいずれか一項に記載の１つ以上のコンピュータ可読格納媒体。
付記２７．該データにアクセスするための該要求が、該要求によって特定される鍵を使用して暗号文を解読するための要求である、付記２１～２６のいずれか一項に記載の１つ以上のコンピュータ可読格納媒体。
付記２８．システムであって、
１つ以上のプロセッサと、
該１つ以上のプロセッサによって実行されると、
該システムに、該要求によって示される時間にポリシーを有効にするための要求を受信することと、
該示された時間に少なくとも部分的に基づいて、該要求の遂行が現在有効なポリシーを順守するかどうかを判断することと、
該要求の受信と該示された時間との間の時に、該要求を中断するための別の要求が受信されることを可能にすることと、を行わせる、命令を含むメモリと、を備える、該シス

テム。
付記２９．該要求が、データへのアクセスのために満たすことが必要とされる１つ以上の条件を変更するためのものである、付記２８に記載のシステム。
付記３０．該ポリシーが、暗号サービスによって管理される鍵に対応し、かつ、暗号サービスが１つ以上の暗号動作を実行するために満たすことが必要とされる、１つ以上の条件を示す、付記２８または２９に記載のシステム。
付記３１．該命令がさらに、該要求の受信の結果として、該システムに、それぞれが該要求を中断する権限を有する１つ以上のエンティティに、１つ以上の通知を伝送させる、付記２８～３０のいずれか一項に記載のシステム。
【０１５７】
他の変形もまた、本開示の範囲内であるとみなされる。例えば、いくつかの実施形態では、データ格納システムは、要求を中止する及び／または別様で潜在的セキュリティ違反から保護するための時間を提供するのに十分である、要求処理のための固有の待機時間を有し得る。例えば、保存用データ格納システムは、要求に応答性のデータが、要求が提出された数時間後に使用可能になり得る、非同期要求処理を利用し得る。さらに、要求に応答性のデータは、異なる時間量後に使用可能になり得、これはシステム等の因子に依存し得る。かかるシステムを用いて、固有の待機時間のために、タイマーは不必要となり得る。
【０１５８】
図３４は、様々な実施形態に従う態様を実装するための、環境３４００の実施例の態様を例示する。理解され得るように、ウェブベースの環境が説明の目的のために使用されるが、様々な実施形態を実装するために異なる環境が適切なように使用され得る。環境は、電子クライアントデバイス３４０２を含み、これは、要求、メッセージ、または情報を、適切なネットワーク３４０４を介して送信及び受信するように、ならびにデバイスのユーザに情報を運んで戻すように動作可能な、任意の適切なデバイスを含み得る。かかるクライアントデバイスの例には、パーソナルコンピュータ、携帯電話、携帯型メッセージングデバイス、ノートパソコン、セットトップボックス、携帯情報端末、電子ブックリーダ等が挙げられる。ネットワークは、イントラネット、インターネット、セルラーネットワーク、ローカルエリアネットワーク、もしくは任意の他のかかるネットワーク、またはそれらの組み合わせを含む、任意の適切なネットワークを含み得る。かかるシステムのために使用される構成要素は、選択されるネットワーク及び／または環境の種類に、少なくとも部分的に依存し得る。かかるネットワークを介して通信するためのプロトコル及び構成要素は公知であり、本明細書において詳細に説明されない。ネットワークを介する通信は、有線または無線接続及びそれらの組み合わせによって可能にされ得る。本実施例では、環境が、要求の受信及びそれに応答するコンテンツの提供のためのウェブサーバ３４０６を含むため、ネットワークはインターネットを含むが、他のネットワークについては、当業者には明白であり得るように、同様の目的に提供する代替のデバイスが使用され得る。
【０１５９】
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３４０８及びデータストア３４１０を含む。いくつかのアプリケーションサーバ、レイヤー、または、チェーン接続もしくは別様で構成され得、適切なデータストアからデータを得る等のタスクを実行するために対話し得る、他の要素、プロセス、もしくは構成要素があり得るということが理解されるべきである。本明細書で使用する場合、「データストア」という用語は、データを格納、データにアクセス、及びデータを読み出すことができる、任意のデバイスまたはデバイスの組み合わせを指し、これは、任意の標準、分散、またはクラスタ環境内の、データサーバ、データベース、データ格納デバイス、及びデータ格納媒体を、任意の組み合わせで任意の数含み得る。アプリケーションサーバは、クライアントデバイスのための１つ以上のアプリケーションの態様を実行するために必要とされるため、データストアと統合するための、アプリケーションのための大半のデータアクセス及びビジネス論理を処理する、任意の適切なハードウェア及びソフトウェアを含み得る。アプリケーションサーバは

、データストアと協働してアクセス制御サービスを提供し、ユーザに移送される、テキスト、画像、音声、及び／または動画等のコンテンツを生成することができ、これは、本実施例では、ハイパーテキストマークアップ言語（「ＨＴＭＬ」）、拡張マークアップ言語（「ＸＭＬ」）、または別の適切な構造言語の形態で、ウェブサーバによってユーザに提供され得る。全ての要求及び応答の処理、ならびにクライアントデバイス３４０２とアプリケーションサーバ３４０８との間のコンテンツの送達は、ウェブサーバによって処理され得る。本明細書に記載される構造コードは任意の適切なデバイス上で実行され得、または本明細書の他の箇所で記載のように機械をホストし得るので、ウェブ及びアプリケーションサーバは、要求されず、かつ、単に構成要素の例であるということが理解されるべきである。

【０１６０】

データストア３４１０は、いくつかの別個のデータ表、データベース、または他のデータ格納機構、及び特定の態様に関連するデータを格納するための媒体を含み得る。例えば、例示されるデータストアは、生産データ３４１２及びユーザ情報３４１６を格納するための機構を含み、これは、生産側にコンテンツを提供するために使用され得る。データストアは、ログデータ３４１４を格納するための機構を含むこともまた示され、これは、報告、分析、または他のかかる目的のために使用され得る。適切なように上記の機構のうちのいずれか内に、またはデータストア３４１０内の追加の機構内に、格納され得る、ページ画像情報のため及び正しい情報にアクセスするために、データストア内に格納される必要があり得る、多くの他の態様があり得るということが理解されるべきである。データストア３４１０は、そこに関連付けられる論理を通して、アプリケーションサーバ３４０８から命令を受信して、それに応答してデータを得る、更新する、または別様で処理するように動作可能である。一実施例では、ユーザは、特定の種類のアイテムについての検索要求を提出し得る。この場合、データストアは、ユーザ情報にアクセスしてユーザの識別を検証し得、かつ、カタログ詳細情報にアクセスしてその種類のアイテムについての情報を得ることができる。その後情報は、ユーザがユーザデバイス３４０２のブラウザを介して見ることができるウェブページ上に記載される結果において、ユーザに戻され得る。対象の特定のアイテムについての情報は、ブラウザの専用ページまたはウィンドウで見ることができる。

【０１６１】

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

【０１６２】

一実施形態における環境は、１つ以上のコンピュータネットワークまたは直接接続を使用して、通信リンクを介して相互接続される、いくつかのコンピュータシステム及び構成要素を利用する、分散コンピューティング環境である。しかしながら、かかるシステムは、図３４に例示されるよりも少ないまたは多い数の構成要素を有するシステムにおいて同等に良好に動作し得るということが、当業者に理解されるであろう。したがって、図３４のシステム３４００の説明は、本質的に例示的であり、本開示の範囲を限定するものではないと捉えられるべきである。

【０１６３】

様々な実施形態は、さらに、幅広い様々な動作環境において実装され得、これは、いくつかの場合では、多数のアプリケーションのうちのいずれかを動作させるために使用する

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

【０１６４】

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

【０１６５】

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

【０１６６】

環境は、上記のように様々なデータストアならびに他のメモリ及び格納媒体を含み得る。これらは、コンピュータのうちの１つ以上にローカルな（かつ／もしくはそこに常駐する）、または、ネットワークを渡るコンピュータのいずれかまたは全てから遠隔の、格納媒体上等の、様々な位置に常駐し得る。実施形態の特定の組では、情報は、当業者になじみのあるストレージエリアネットワーク（「ＳＡＮ」）内に存在し得る。同様に、コンピュータ、サーバ、または他のネットワークデバイスに属する機能を実行するための任意の必要なファイルは、適宜、ローカルに及び／または遠隔に格納され得る。システムがコンピュータ化されたデバイスを含む場合、それぞれのかかるデバイスは、バスを介して電気的に連結され得るハードウェア要素を含み得、要素は、例えば、少なくとも１つの中央処理ユニット（「ＣＰＵ」）、少なくとも１つの入力デバイス（例えば、マウス、キーボード、コントローラ、タッチスクリーン、またはキーパッド）、及び少なくとも１つの出力デバイス（例えば、ディスプレイデバイス、プリンタ、またはスピーカ）を含む。かかるシステムは、ディスクドライブ、光格納デバイス、及びランダムアクセスメモリ（「ＲＡＭ」）または読み取り専用メモリ（「ＲＯＭ」）等の固体格納デバイス、ならびに取り外し可能媒体デバイス、メモリカード、フラッシュカード等の、１つ以上の格納デバイスも

また含み得る。本開示の様々な実施形態は、カスタム暗号プロセッサ、スマートカード、及び／またはハードウェアセキュリティモジュールを含むがこれらに限定されない、カスタムハードウェアを使用してもまた実装され得る。

【０１６７】

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

【０１６８】

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

【０１６９】

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

【０１７０】

他の変形は、本開示の精神の範囲内である。よって、開示される技術は、様々な修正及び代替の構造を取り得るが、それらの特定の例示される実施形態が、図面に示され、詳細に上記で説明された。しかしながら、本発明を特定の形式または開示される形式に限定する意図はなく、しかし、逆に、意図は、添付の特許請求の範囲において定義される本発明の精神及び範囲内に収まる、全ての修正、代替構造、及び等価物を網羅することであるということが理解されるべきである。

【０１７１】

開示される実施形態を説明する文脈における（特に、以下の特許請求の範囲の文脈における）、「ａ」、「ａｎ」、及び「ｔｈｅ」という用語、ならびに同様の指示対象は、本明細書に別様が示されない限りまたは文脈によって明らかに矛盾しない限り、単数及び複数の両方を網羅すると解釈されるべきである。「備える」、「有する」、「含む」、及び「含有する」という用語は、別様が述べられない限り、開放型用語（すなわち、「含むがそれに限定されない」ことを意味する）であると解釈されるべきである。「接続される」

という用語は、介在する何かがある場合であっても、部分的にまたは全体的に、内部に含有される、取り付けられる、一緒に接合されると解釈されるべきである。本明細書の値の範囲の列挙は、本明細書で別様が示されない限り、単に、範囲内に収まるそれぞれの別個の値を個々に指す速記方法としての役割を果たすことが意図され、それぞれの別個の値は、本明細書に個々に列挙されるかのように、本明細書に組み込まれる。本明細書に記載される全ての方法は、本明細書に別様が示されない限り、または文脈によって別様が明らかに矛盾しない限り、任意の好適な順序で実行され得る。本明細書で提供される、任意の及び全ての実施例、または例を示す表現（例えば、「等」）の使用は、単に、本発明の実施形態をより良好に解明することを意図し、別様が主張されない限り、本発明の範囲に限定を課すものではない。いかなる本明細書の表現も、非請求要素を本発明の実践に必須であるとして示すと解釈されるべきではない。

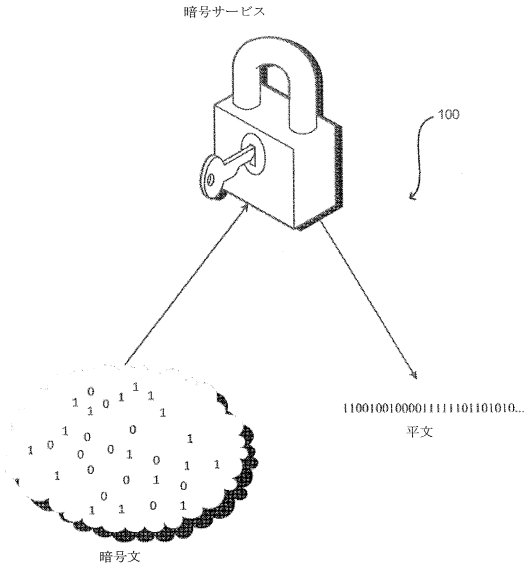
【０１７２】

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

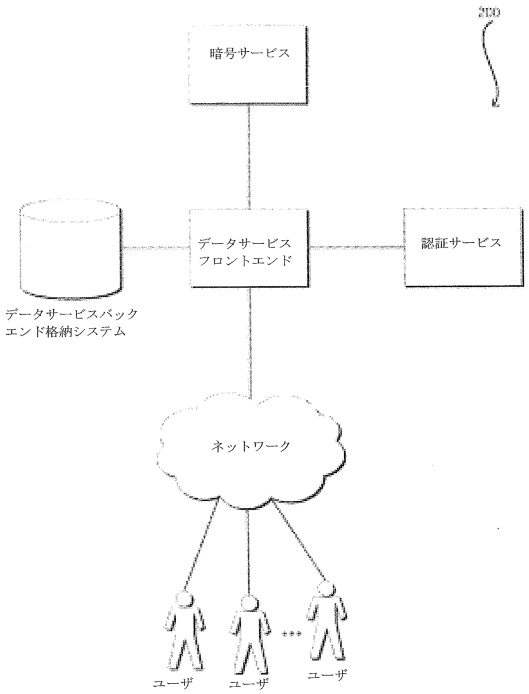
【０１７３】

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

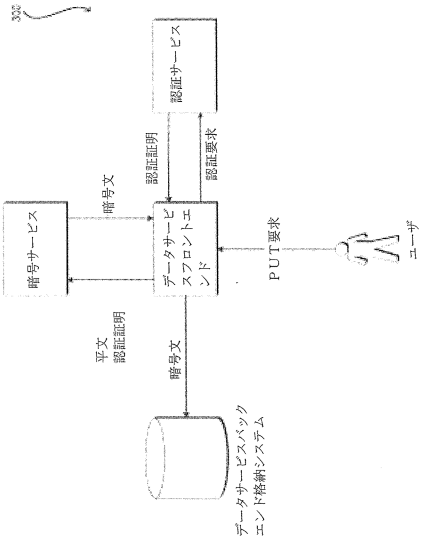
【図１】



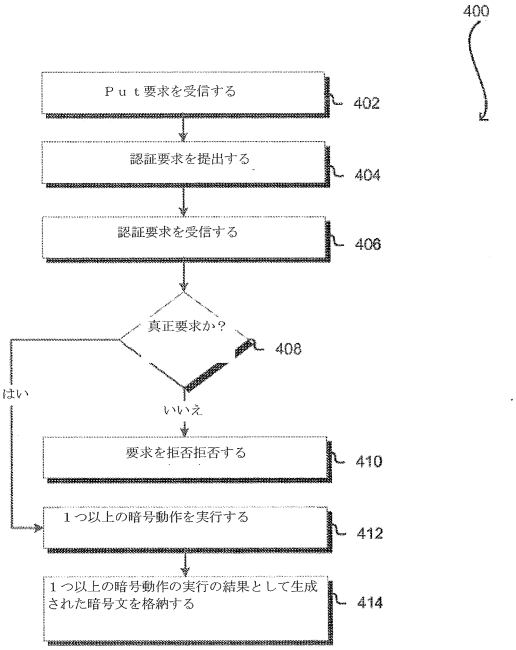
【図２】



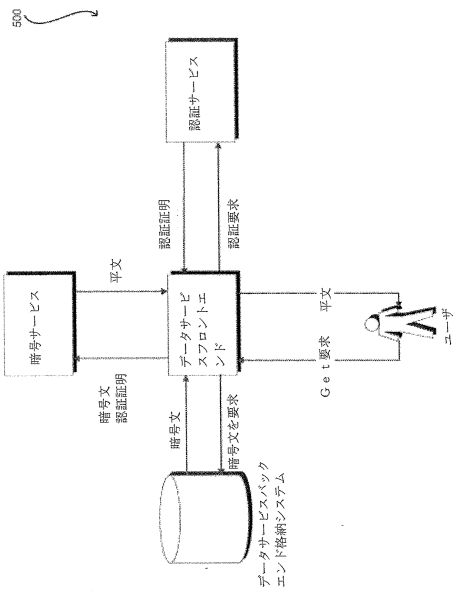
【図３】


502
認証サービス
認証証明
認証要求
暗号文
暗号サービス
データサービスフロントエンド
PUT要求
ユーザ
平文
認証証明
暗号文
データサービスバックエンド格納システム

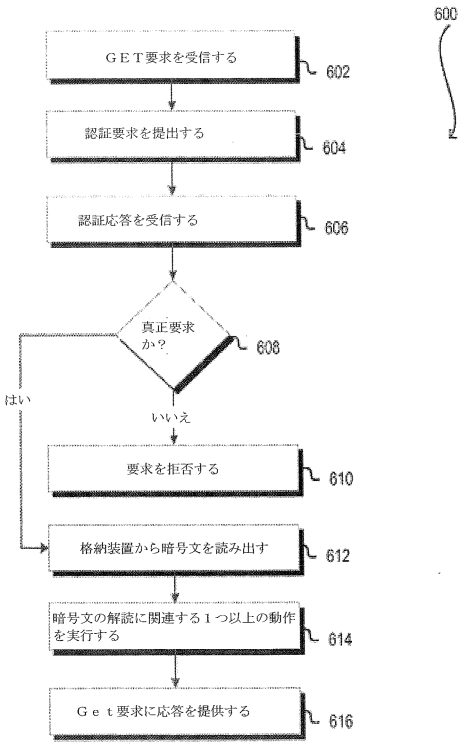
【図４】


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

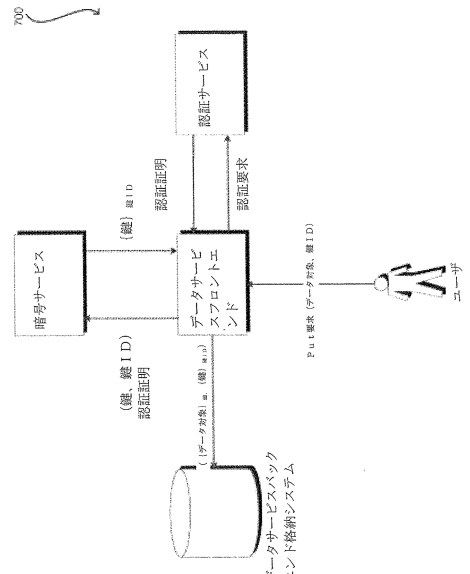
【図５】


500
認証サービス
認証証明
認証要求
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格納システム

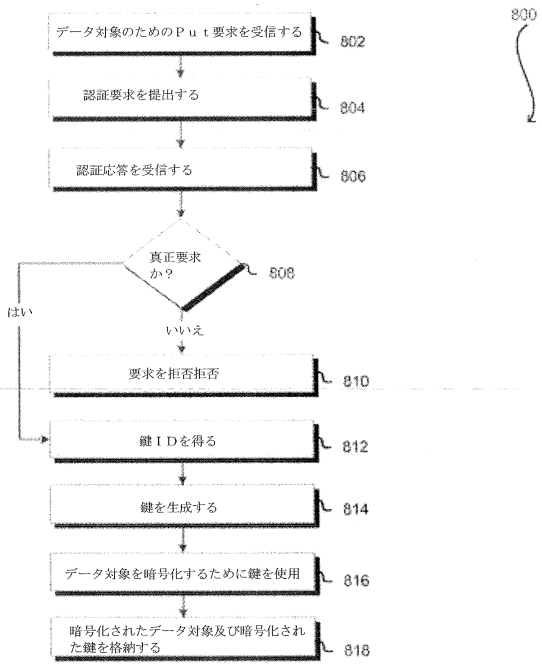
【図６】


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

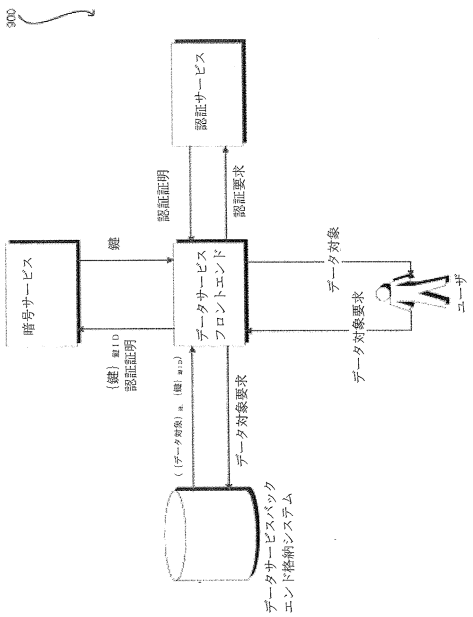
【図７】


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

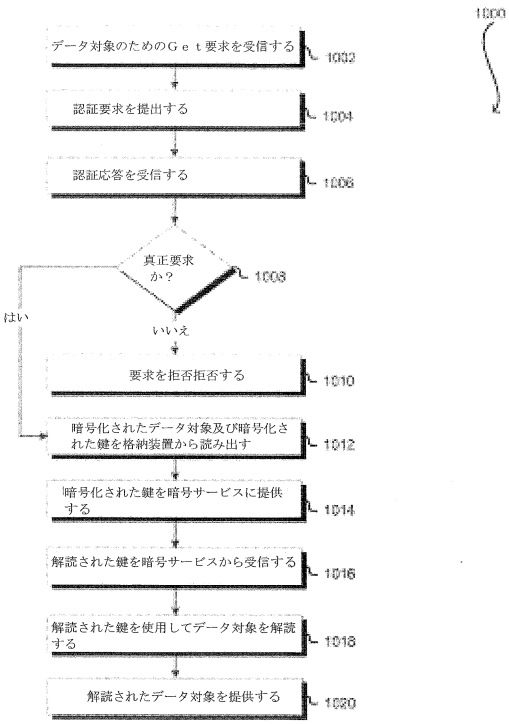
【図８】


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

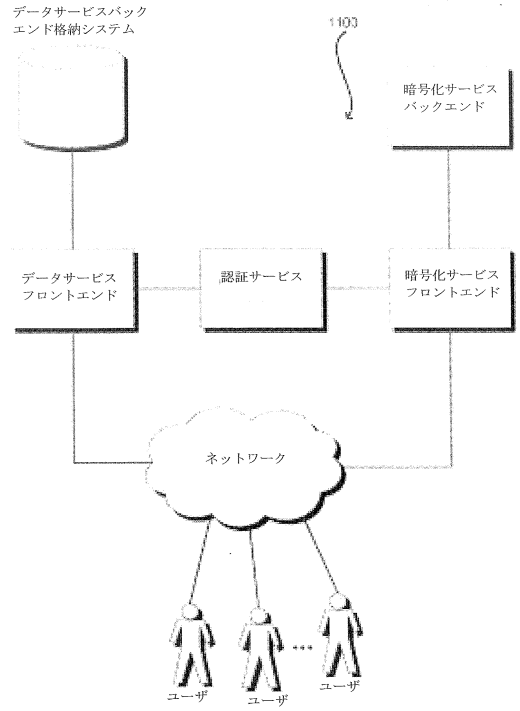
【図９】


900
認証サービス
認証証明
認証要求
鍵
暗号サービス
データサービスフロントエンド
データ対象
ユーザ
データ対象要求
（鍵）鍵ID
認証証明
（データ対象）鍵（鍵）鍵ID
データ対象要求
データサービスバックエンド格納システム

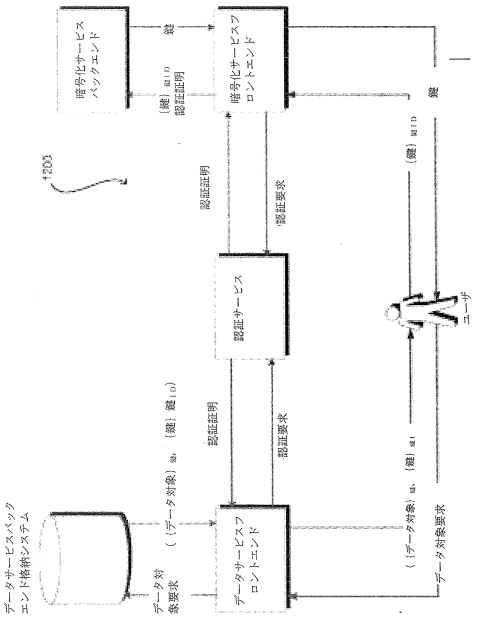
【図１０】


1000
データ対象のためのＧｅｔ要求を受信する
1002
認証要求を提出する
1004
認証応答を受信する
1006
真正要求か？
1008
はい
いいえ
要求を拒否拒否する
1010
暗号化されたデータ対象及び暗号化された鍵を格納装置から読み出す
1012
暗号化された鍵を暗号サービスに提供する
1014
解読された鍵を暗号サービスから受信する
1016
解読された鍵を使用してデータ対象を解読する
1018
解読されたデータ対象を提供する
1020

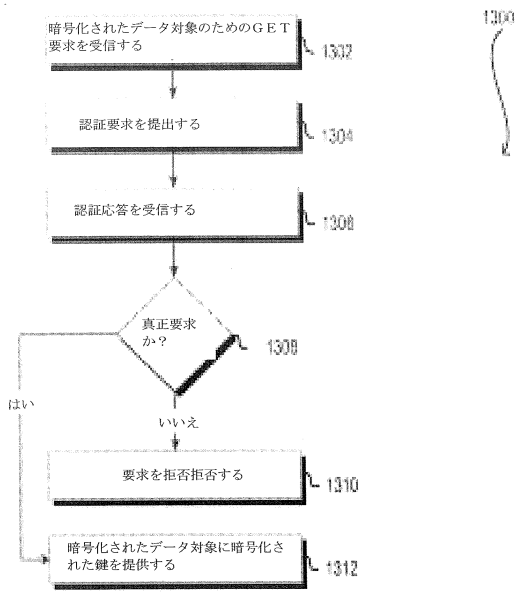
【図１１】



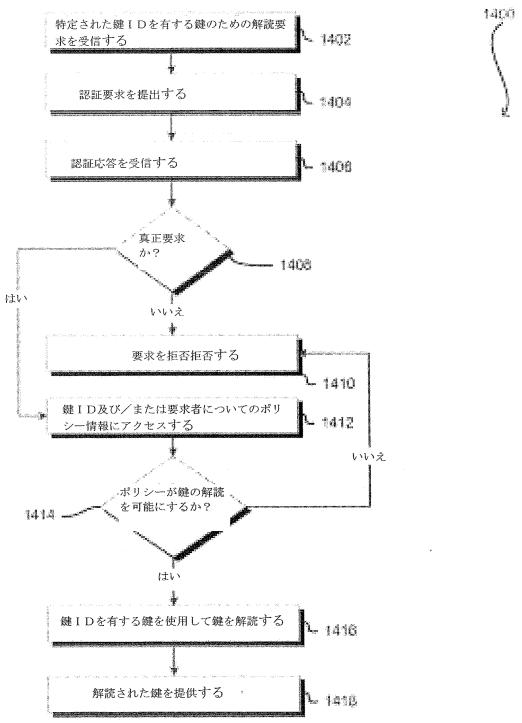
【図１２】



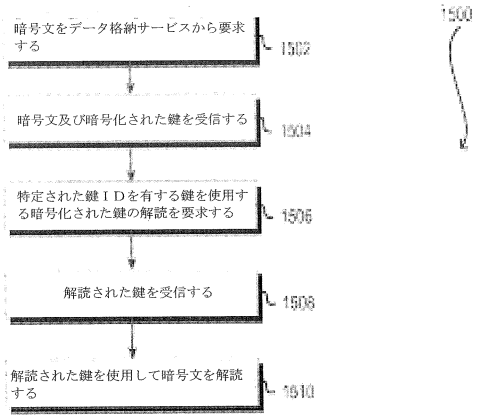
【図１３】



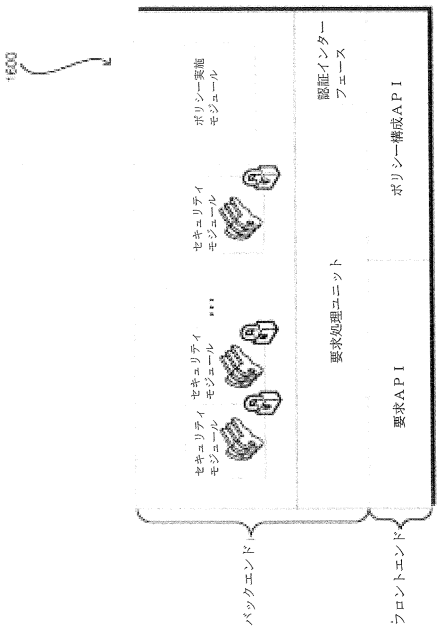
【図１４】



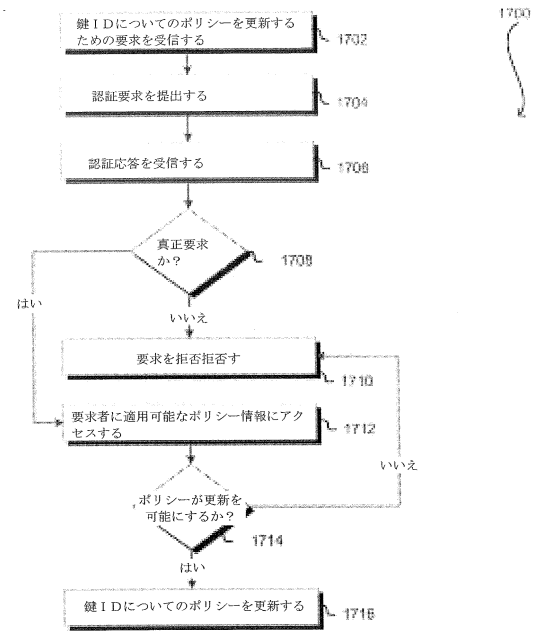
【図１５】



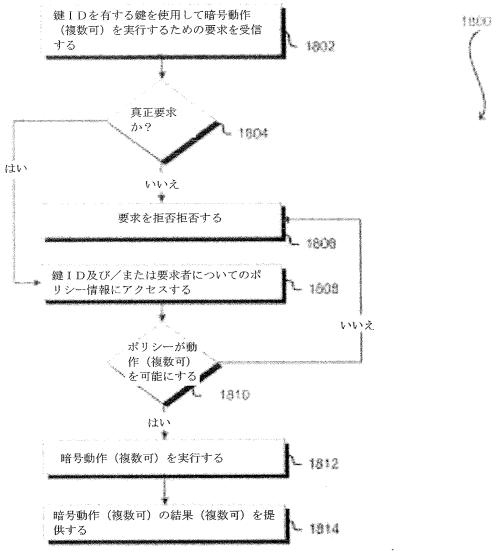
【図１６】



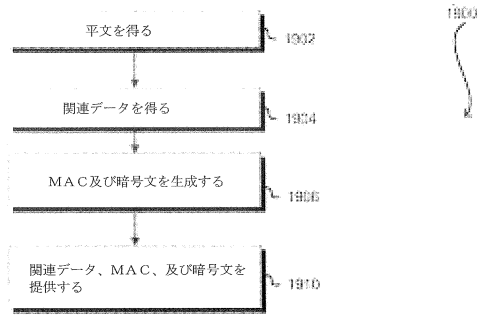
【図１７】



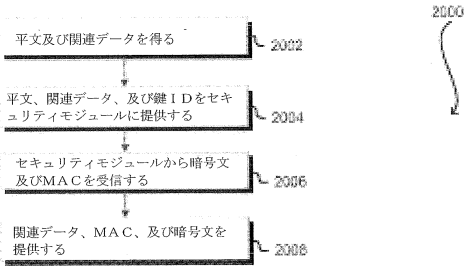
【図１８】



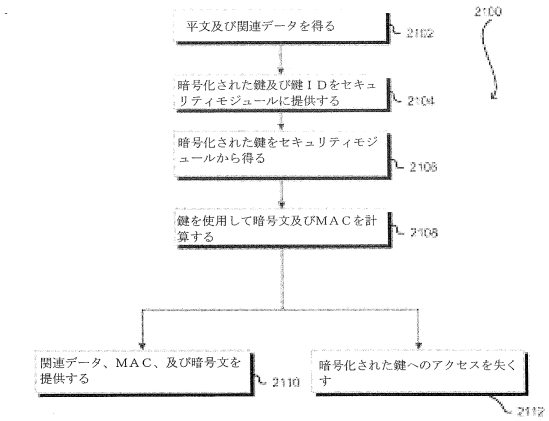
【図１９】



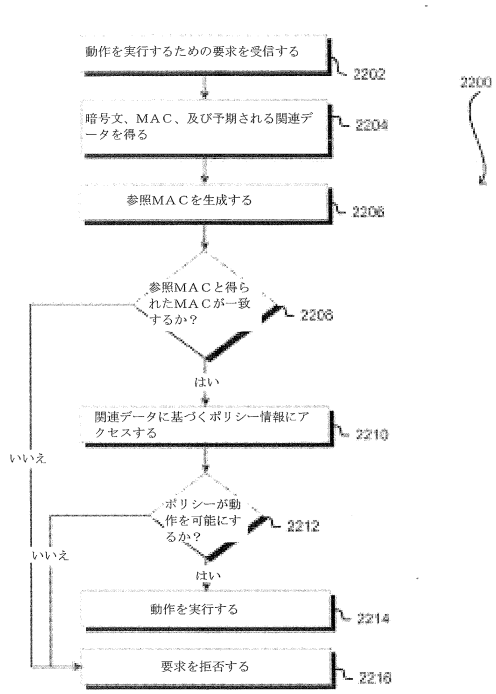
【図２０】



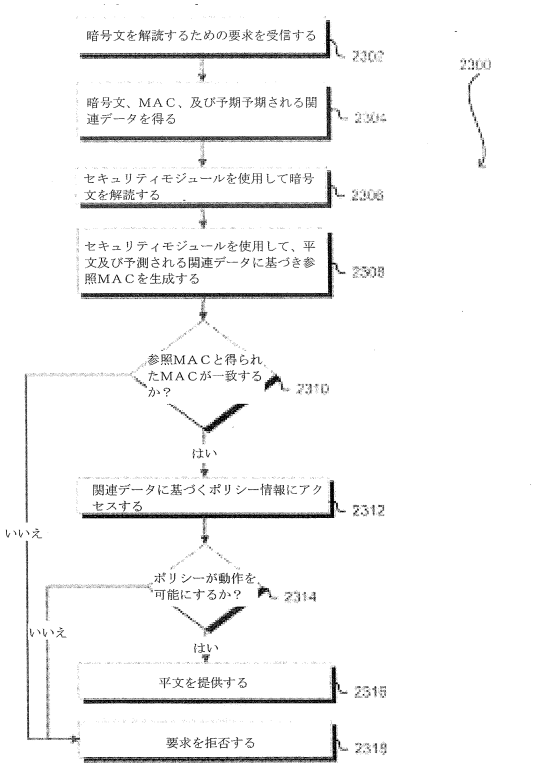
【図２１】



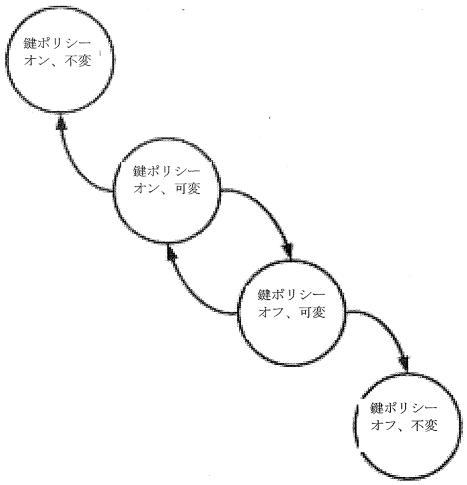
【図２２】



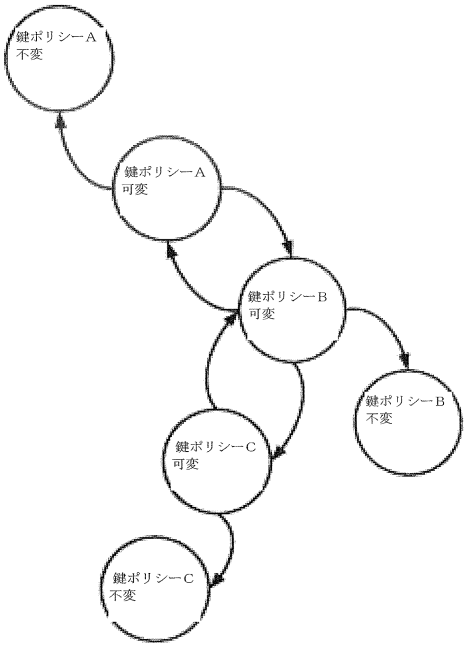
【図２３】



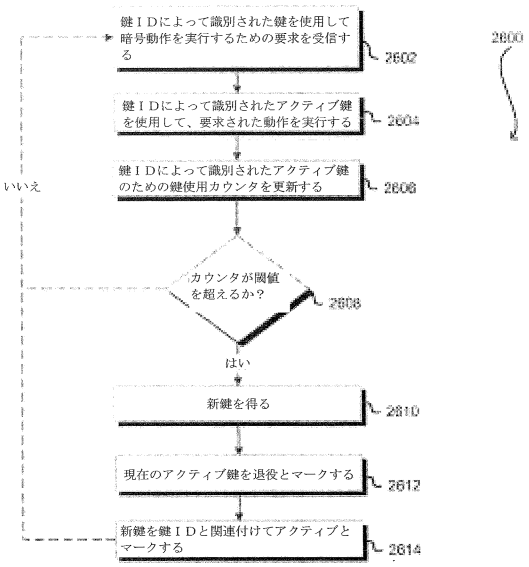
【図２４】



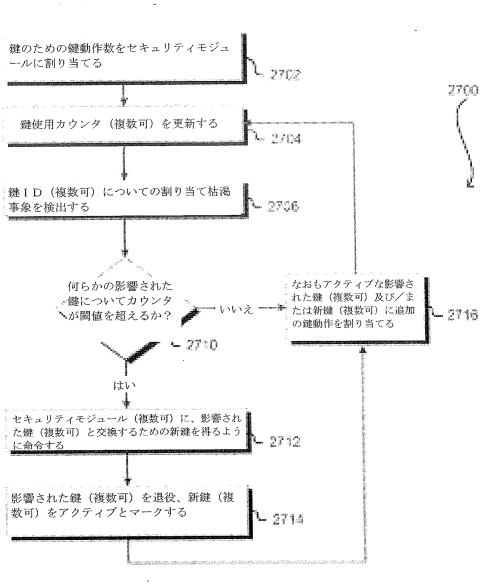
【図２５】



【図２６】



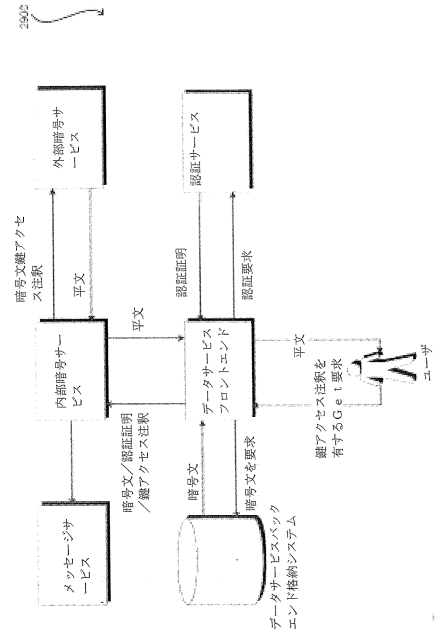
【図２７】



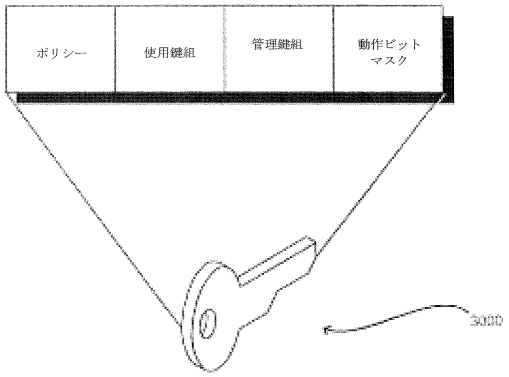
【図２８】

鍵ＩＤ	鍵版	使用可能性	カウンタ
⋮	⋮	⋮	⋮
31415926	1	退役	4294967296
31415926	2	退役	4294967296
31415926	3	退役	4294967296
31415926	4	アクティブ	1048576
31415927	1	アクティブ	2097152
⋮	⋮	⋮	⋮

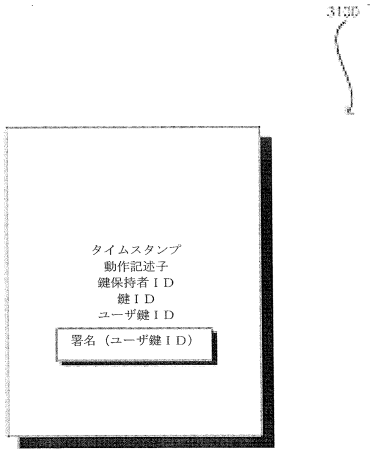
【図２９】



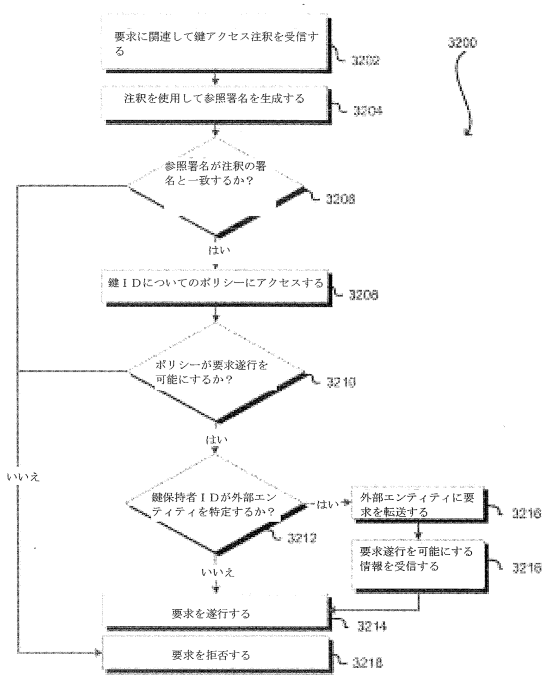
【図３０】



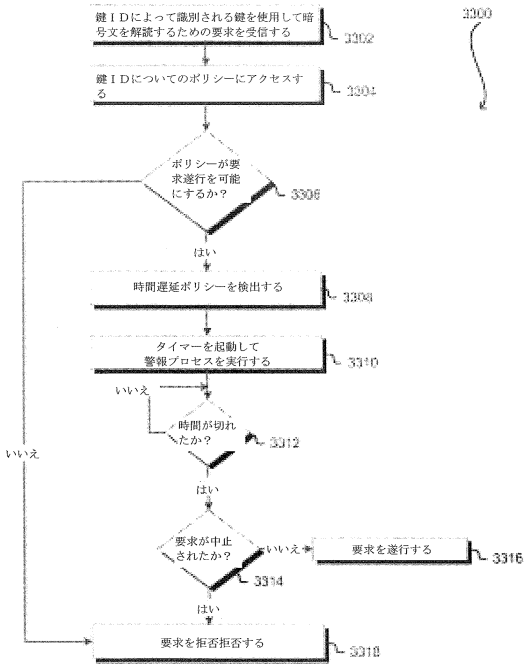
【図３１】



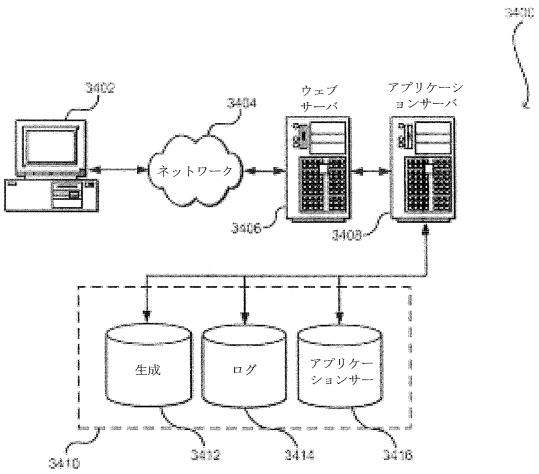
【図３２】



【図３３】


3300
鍵ＩＤによって識別される鍵を使用して暗号文を解読するための要求を受信する
3302
鍵ＩＤについてのポリシーにアクセスする
3304
ポリシーが要求遂行を可能にするか？
3306
はい
時間遅延ポリシーを検出する
3308
タイマーを起動して警報プロセスを実行する
3310
いいえ
時間が切れたか？
3312
いいえ
はい
要求が中止されたか？
3314
いいえ
要求を遂行する
3316
はい
要求を拒否拒否する
3318

【図３４】


3400
3402
3404
ネットワーク
ウェブサーバ
アプリケーションサーバ
3406
3408
生成
ログ
アプリケーション
3410
3412
3414
3416

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

審査官 青木 重徳

(56)参考文献 特開２００７－０８１４８２（ＪＰ，Ａ）
特表２００５－５３３４３８（ＪＰ，Ａ）
特開２０００－２１５２４０（ＪＰ，Ａ）
特開２００５－２５８８０１（ＪＰ，Ａ）
特開２００８－３０６４１８（ＪＰ，Ａ）
米国特許出願公開第２０１１／０２９６４９７（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｈ０４Ｌ ９／３２