(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2018-160919
(P2018-160919A)
(43)公開日　平成30年10月11日(2018.10.11)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
G06F 21/60	(2013.01)	H04L	9/00	601E	
		H04L	9/00	601F	
		G06F	21/60	320	

審査請求 有　請求項の数 20　ＯＬ　（全 31 頁）

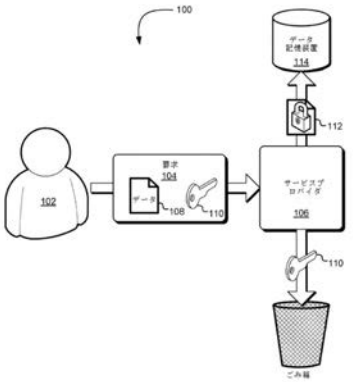
(21)出願番号　特願2018-111507 (P2018-111507)
(22)出願日　平成30年6月12日 (2018.6.12)
(62)分割の表示　特願2016-542891 (P2016-542891)の分割
原出願日　平成26年9月23日 (2014.9.23)
(31)優先権主張番号　14/037,292
(32)優先日　平成25年9月25日 (2013.9.25)
(33)優先権主張国　米国(US)

(71)出願人　506329306
アマゾン　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　９８１０８－１２２６
ワシントン州　シアトル　ピーオー　ボックス　８１２２６
(74)代理人　100106541
弁理士　伊藤　信和
(72)発明者　ロス　グレゴリー　ブランチェック
アメリカ合衆国　９８１０９－５２１０
ワシントン州　シアトル　テリー　アヴェニュー　ノース　４１０

最終頁に続く

(54)【発明の名称】要求によって供給される鍵を用いたデータセキュリティ

(57)【要約】　（修正有）
【課題】要求によって供給される鍵を用いたデータセキュリティ方法を提供する。
【解決手段】要求処理エンティティに要求１０４が提示される。このとき、要求には、当該要求を実施する際に使用すべき暗号鍵１１０が含まれる。要求処理エンティティは、要求を受信すると、その要求から鍵を抽出し、その鍵を使用して１つ以上の暗号化操作を実行することによって要求を実施する。１つ以上の暗号化操作は、暗号化された形式で要求処理エンティティのサブシステムによって記憶され得る／記憶されているデータの暗号化／復号化を含み得る。要求が実施されると、要求処理エンティティは、要求に含まれる鍵へのアクセスをできなくするための１つ以上の操作を実行してもよく、それによって鍵の使用が不可能となる。
【選択図】図１



【特許請求の範囲】
【請求項１】
暗号化された暗号鍵を含み、データを指定しそのデータを含まない要求を、ネットワークを介して受信することと、
少なくとも前記暗号化された暗号鍵を別のエンティティに転送することにより、暗号化された前記暗号鍵を復号化させ、復号化した暗号鍵を生成することと、
前記復号化した暗号鍵を使用し、指定されたデータを暗号化して要求を満たすために、前記指定されたデータに１つ以上の暗号化操作を実行することと、
前記１つ以上の暗号化操作を実行した結果を提供することと、を含む、コンピュータ実装方法。
【請求項２】
前記要求は、前記復号化した暗号鍵を使用して前記要求を認証するために使用可能な情報を含む、請求項１に記載のコンピュータ実装方法。
【請求項３】
前記復号化した暗号鍵は対称暗号鍵である、請求項１または２に記載のコンピュータ実装方法。
【請求項４】
前記要求は、データ記憶システムに前記指定されたデータを暗号化形式で記憶する要求であり、
前記１つ以上の暗号化操作は、前記復号化した暗号鍵を使用して特定のデータを暗号化する操作を含み、
前記１つ以上の暗号化操作を実行した結果を提供することは、前記指定されたデータを暗号化形式で永続記憶用のデータ記憶システムに転送することを含む、請求項１から請求項３のいずれか一項に記載のコンピュータ実装方法。
【請求項５】
前記１つ以上の暗号化操作の実行後、前記復号化した暗号鍵へのアクセスを出来なくさせる１つ以上の操作を実行することをさらに備える、請求項１から請求項４のいずれか一項に記載のコンピュータ実装方法。
【請求項６】
前記別のエンティティから前記復号化した暗号鍵を受けとることにより、前記暗号鍵を受けとる前には出来なかった前記復号化した暗号鍵へのアクセスを可能とする、請求項１から請求項５に記載のコンピュータ実装方法。
【請求項７】
１つ以上のプロセッサとメモリとを備えるシステムであって、
前記１つ以上のプロセッサによって、前記システムに、
ネットワークを介して、要求元から要求を受信することであって、前記要求の実施が、前記要求で供給された復号化した暗号鍵を備える情報を使用し、前記要求で指定されたデータに対して１つ以上の暗号化操作を実行することを含み、前記要求に前記データは含まれない、前記要求を受信することと、
少なくとも前記暗号化した暗号鍵を復号化のために別のエンティティに転送し、前記前記要求で供給された前記暗号鍵を復号化させることを含み、前記復号化した暗号鍵を使用して前記指定されたデータを暗号化する、前記要求で供給された前記暗号化した暗号鍵を使用して前記指定されたデータに１つ以上の暗号化操作を実行することと、
前記１つ以上の暗号化操作の実行結果を提供することと、を実行されるシステム。
【請求項８】
前記指定されたデータに前記１つ以上の暗号化操作を実行することは、前記復号化した暗号鍵を使用し、データ記憶システムから前記指定されたデータを復号化することを含む、請求項７に記載のシステム。
【請求項９】
前記情報は、前記暗号化された前記暗号鍵とは異なる第２の暗号鍵に少なくとも部分的

に基づいて生成された電子署名を含むことによって前記要求を認証するために使用可能である、請求項７または請求項８に記載のシステム。
【請求項１０】
前記要求は、前記指定されたデータを暗号化形式で永続記憶用のデータ記憶システムに記憶する要求を含み、
前記１つ以上の暗号化操作は、前記指定されたデータの暗号化を含み、
前記１つ以上の暗号化操作を実行した結果を提供することは、前記指定されたデータを暗号化形式で永続記憶用のデータ記憶システムに転送することを含む、請求項７から請求項９のいずれか一項に記載のシステム。
【請求項１１】
前記情報は、前記１つ以上の暗号化操作の実行後、前記システムに前記復号化した暗号鍵へのアクセスを出来なくさせる１つ以上の操作を実行させることをさらに含む、請求項７から請求項１０のいずれか一項に記載のシステム。
【請求項１２】
前記システムは、前記要求を受信するまでの時間は前記復号化された暗号鍵にアクセスできない、請求項７から請求項１１のいずれか一項に記載のシステム。
【請求項１３】
前記要求は、ユニフォームリソースロケータに暗号化した暗号鍵を含む、請求項７から請求項１２のいずれか一項に記載のシステム。
【請求項１４】
前記別のエンティティは、前記要求から供給される暗号化された暗号鍵を復号化するために使用可能な複合鍵を含み、外部からは接続できない、複数の暗号鍵を記憶するサブシステムであって、
前記命令は暗号化された前記暗号鍵を前記サブシステムに復号化させることを前記システムにさらに行わせる、請求項７から請求項１３のいずれか一項に記載のシステム。
【請求項１５】
非一時的コンピュータ可読記憶媒体であって、コンピュータシステムの１つ以上のプロセッサによって、前記コンピュータシステムに、少なくとも、
ネットワークを介して要求元から要求を受信させることであって、前記要求の実施が、前記要求で供給された復号化した暗号鍵を備える情報を使用し、前記要求で指定されたデータに対して１つ以上の暗号化操作を実行することを含み、前記要求に前記データは含まれない、前記要求を受信させることと、
少なくとも前記暗号化した暗号鍵を復号化のために別のエンティティに転送し、前記前記要求で供給された前記暗号鍵を復号化させることを含み、前記復号化した暗号鍵を使用して前記指定されたデータを暗号化する、前記要求で供給された前記暗号化した暗号鍵を使用して前記指定されたデータに１つ以上の暗号化操作を実行させることと、
前記１つ以上の暗号化操作の実行結果を提供させることと、を実行される非一時的コンピュータ可読記憶媒体。
【請求項１６】
前記指定されたデータに前記１つ以上の暗号化操作を実行させることは、前記復号化した暗号鍵を使用し、データ記憶システムから前記指定されたデータを復号化させることを含む、請求項１５に記載の非一時的コンピュータ可読記憶媒体。
【請求項１７】
前記情報は、前記復号化された暗号鍵を使用して前記要求を認証することにより、前記要求を認証するために使用可能である、請求項１５または請求項１６に記載の非一時的コンピュータ可読記憶媒体。
【請求項１８】
前記要求は、前記指定されたデータを暗号化形式で永続記憶用のデータ記憶システムに記憶する要求であり、
前記１つ以上の暗号化操作は、前記指定されたデータの暗号化を含み、

前記１つ以上の暗号化操作を実行した結果を提供することは、前記指定されたデータを暗号化形式で永続記憶用のデータ記憶システムに転送することを含む、請求項１５から請求項１７のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。
【請求項１９】
前記復号化した暗号鍵は、対称暗号鍵である、請求項１５から請求項１８のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。
【請求項２０】
ユニフォームリソースロケータから入手した暗号化した暗号鍵が前記要求に含まれる、請求項１５から請求項１９のいずれか一項に記載の非一時的コンピュータ可読記憶媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、２０１３年９月２５に出願された「ＲＥＳＯＵＲＣＥ　ＬＯＣＡＴＯＲＳ　ＷＩＴＨ　ＫＥＹＳ」と題する米国特許出願第１４／０３７，２８２号及び２０１３年９月２５に出願された「ＤＡＴＡ　ＳＥＣＵＲＩＴＹ　ＵＳＩＮＧ　ＲＥＱＵＥＳＴ－ＳＵＰＰＬＩＥＤ　ＫＥＹＳ」と題する米国特許出願第１４／０３７，２９２号の全開示を、本明細書の一部を構成するものとしてあらゆる目的のために援用する。
【背景技術】
【０００２】
コンピューティングリソース及び関連データのセキュリティは、多くの状況において非常に重要である。ある例として、組織は、多くの場合、コンピューティング装置からなるネットワークを利用して、一連の堅牢なサービスを組織のユーザーに提供する。ネットワークは、往々にして多数の地理的境界にまたがっているため、他のネットワークと接続していることが多い。例えば、組織は、コンピューティングリソースからなる内部ネットワークと他者によって管理されているコンピューティングリソースとの両方を用いて、自らの運用を支援する場合がある。組織のコンピュータは、例えば、別の組織のサービスを利用している間に、他の組織のコンピュータと通信してデータにアクセスし、かつ／またはデータを提供する場合がある。多くの事例では、組織は、他の組織によって管理されたハードウェアを用いて遠隔ネットワークを構築・運用しており、それによって基盤コストを低減させると共に他の利点を実現している。こうしたコンピューティングリソースの構成により、特に、かかる構成の規模や複雑さが増大するにつれ、組織が保有するリソース及びデータへのアクセスを確実に保証することが困難となる可能性がある。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】米国特許第２０１３／０１９８５１９号
【発明の概要】
【課題を解決するための手段】
【０００４】
要求処理エンティティに要求が提示される。このとき、要求には、当該要求を実施する際に使用すべき暗号鍵が含まれる。要求処理エンティティは、要求を受信すると、その要求から鍵を抽出し、その鍵を使用して１つ以上の暗号化操作を実行することによって要求を実施する。１つ以上の暗号化操作は、暗号化された形式で要求処理エンティティのサブシステムによって記憶され得る／記憶されているデータの暗号化／復号化を含み得る。要求が実施されると、要求処理エンティティは、要求に含まれる鍵へのアクセスをできなくするための１つ以上の操作を実行してもよく、それによって鍵の使用が不可能となる。
【図面の簡単な説明】
【０００５】

図面を参照しながら、本開示に係る様々な実施形態について説明する。
【０００６】
【図１】様々な実施形態を実装可能な環境の例示的な実施例を示す図である。
【図２】様々な実施形態を実装可能な環境の例示的な実施例を示す図である。
【図３】少なくとも１つの実施形態に係る要求の表現の例示的な実施例を示す図である。
【図４】少なくとも１つの実施形態に係る要求の提示プロセスの例示的な実施例を示す図である。
【図５】少なくとも１つの実施形態に係る要求の処理プロセスの例示的な実施例を示す図である。
【図６】少なくとも１つの実施形態に係る要求の表現の例示的な実施例を示す図である。
【図７】少なくとも１つの実施形態に係るＰＵＴ要求の処理プロセスの例示的な実施例を示す図である。
【図８】少なくとも１つの実施形態に係るＧＥＴ要求の提示プロセスの例示的な実施例を示す図である。
【図９】様々な実施形態に係る要求の表現の実施例を示す図である。
【図１０】少なくとも１つの実施形態に係る要求の提示プロセスの例示的な実施例を示す図である。
【図１１】様々な実施形態を実装可能な環境の例示的な実施例を示す図である。
【図１２】少なくとも１つの実施形態に係る要求の処理プロセスの例示的な実施例を示す図である。
【図１３】様々な実施形態を実装可能な環境の例示的な実施例を示す図である。
【図１４】少なくとも１つの実施形態に係る要求の処理プロセスの例示的な実施例を示す図である。
【図１５】様々な実施形態を実装可能な環境を示す図である。
【発明を実施するための形態】
【０００７】
以下の説明では、様々な実施形態について説明する。説明の都合上、これらの実施形態の理解を完全なものとするため、特定の構成及び詳細について記載する。しかしながら、当業者にとっては、特定の詳細に関係なくこれらの実施形態を実施可能であることも明らかであろう。さらに、実施形態の記載が不明瞭にならないようにするため、周知の特徴については省略または簡略化する場合がある。
【０００８】
本明細書で説明され、提案される技法は、要求に暗号鍵が含まれる場合における要求の提示及び処理に関する。この要求は、コンピューティングリソースのサービスプロバイダなどのサービスプロバイダの顧客によって生成され、その顧客から提示され得る。要求を処理することには、データに対する暗号化、復号化及び電子（デジタル）署名の生成といった１つ以上の暗号化操作を実行するために、当該要求に含まれる鍵を使用することを含んでもよい。いくつかの実施形態では、本明細書において説明及び提案がなされる技法は、サーバー側暗号化（及び／または復号化などの関連技法）を可能にするために使用される。この場合、暗号化／復号化に使用すべき鍵は、クライアント（すなわち、顧客の装置または顧客に代わって動作する装置）によって制御される。
【０００９】
様々な実施形態では、要求で提供された鍵の使用は、その鍵を使用するための限定的な時間を除き、サービスプロバイダがその鍵にアクセスできないように実行される。例えば、サービスプロバイダは、データ記憶サービスを運用し得る。顧客は、データ記憶サービスによって記憶させるため、サービスプロバイダにデータを送信し得る。サービスプロバイダへの要求には、データを暗号化するのに使用すべき鍵が含まれる場合がある。サービスプロバイダは、その要求から鍵を取得し、その鍵を使用してデータを暗号化し得る。それにより、暗号化データは、データ記憶サービスを用いて永続的に記憶され得る。鍵がもはや必要とされなくなったとき（例えば、データの暗号化が完了したとき）には、サービ

スプロバイダは、鍵のメモリ内コピーを破壊し、あるいはその破壊を許可するなどして、その鍵へのアクセスをできなくするための１つ以上の操作を実行してもよい。平文形式のデータがコピーされていた場合には、それらコピーについても同様に破壊され、あるいは破壊が許可される場合がある。鍵及び平文データが一旦破壊されると、プロバイダによるデータの復号化が不可能となることを顧客に保証することができる。従って、プロバイダでのセキュリティ違反または他のイベントにより、顧客の承認を受けていないデータへのアクセスが発生したとしても、違反が起きただけでは平文形式のデータへのアクセスは可能とならない。

【００１０】

鍵は、種々の実施形態に従って様々な方法で要求において提供され得る。例えば、いくつかの実施形態では、平文形式の鍵が要求に含まれる。平文鍵は、対称鍵アルゴリズムに使用される対称鍵であってよい。平文鍵は、非対称鍵アルゴリズム用の公開－私有鍵のペアのうちの公開鍵であってもよい。この場合、サービスプロバイダは、その鍵のペアのうちの私有鍵にはアクセスすることができず、私有鍵は、その私有鍵を用いて復号化することができるエンティティ（例えば、顧客）にとってアクセス可能である。いくつかの実施形態では、要求には、暗号化された（ラップされた）形式で鍵が含まれる。例えば、鍵を暗号化して、サービスプロバイダまたはサービスプロバイダの指示を受ける別のエンティティによって復号化できるようにしてもよい。要求に含まれる鍵の暗号化に使用される鍵は、その鍵の復号化が可能なエンティティ（例えば、サービスプロバイダ）と共有された秘密、または公開－私有鍵のペアのうちの公開鍵であってよい。この場合、私有鍵は、要求を処理するための暗号化された鍵を復号化するためにエンティティによって使用されることになる。［注記：段落間隔を更新する必要がある］

【００１１】

鍵付きの要求を受信すると、サービスプロバイダは、その要求に含まれる鍵にアクセスし得るが、必要であれば、復号化し、あるいは復号化させた後にその要求を処理し得る。要求の電子署名を検証すること、または、任意の適用可能な方針に要求の実施が適合するかどうかを確認することなどによって他の操作を実行してもよい。実行され得る操作の他の詳細については、以下でさらに詳しく述べる。

【００１２】

様々な実施形態を実装可能な環境１００の例示的な実施例を図１に示す。環境１００においては、顧客１０２が、要求１０４をサービスプロバイダ１０６に送信する。顧客１０２は、例えば、サービスプロバイダ１０６のサービスを利用してもよい。サービスプロバイダは、顧客によって利用され得るデータに関する任意の種類のサービスを提供し得る。例示的なサービスとしては、データ記憶サービス、データベースサービス、データなどを処理するサービスが挙げられる。サービスプロバイダ１０６に要求１０４を提示するために、顧客１０２は、パーソナルコンピュータまたはラップトップコンピュータ、携帯機器、タブレットコンピューティング装置、電子ブックリーダー、及び／または図１５に関連して以下でさらに詳しくされる他のものなどの、１つ以上の顧客の装置を活用して要求を送信してもよい。加えて、要求１０４は、顧客１０２の１つ以上の自動化プロセスに従って提示されてもよい。例えば、要求１０４は、顧客１０２の装置上で動作するブラウザまたは他のアプリケーションと対話している顧客１０２の装置の人的操作の結果として送信され得る。要求１０４は、インターネットもしくはその他のネットワーク、または後述するネットワークの組み合わせなどのネットワークを介して送信される電子的要求であってよい。いくつかの実施形態では、例えば、要求１０４は、サービスプロバイダ１０６によって提供されるウェブサービスインターフェースへのウェブサービス要求である。一般に、要求１０４は、要求を電子的に提示できるようにするための様々なプロトコルに従って構成されてもよい。

【００１３】

図１に示すように、要求１０４は、データ１０８及び暗号鍵１１０を含む。このデータは、各種の情報を含む場合があり、様々な実施形態に従って様々な方法でフォーマットさ

れ得る。例えば、いくつかの実施形態では、メディアファイルなどのファイルとしてデータが構成される。データは、他の方法でフォーマットされてもよい。データは、例えば、データベースまたはそれ以外のものに含まれるように構成され得る。暗号鍵１１０は、以下でさらに詳しく述べるように、データ１０８またはそれ以外のものを暗号化して１つ以上の暗号化操作をデータに実行するのに使用される鍵であってよい。なお、以下でさらに詳しく述べるように、様々な方法で要求１０４に暗号鍵１１０を含めてもよいことに留意すべきである。例えば、いくつかの実施形態では、要求１０４は、平文形式の暗号鍵１１０を含む。他の実施形態では、要求１０４は、暗号化された形式の暗号鍵を含む。例えば、以下でさらに詳しく述べるように、暗号鍵１１０を別の鍵によって暗号化することにより、この別の鍵に関連したサービスプロバイダ１０６または別のシステムが暗号鍵１１０を復号化できるようにしてもよい。このように、顧客１０２からサービスプロバイダ１０６に要求１０４が提示されると、サービスプロバイダ１０６は、暗号鍵１１０を使用して、要求１０４で受信したデータ１０８を暗号化し、それによって暗号化データ１１２を生成し得る。

【００１４】

次いで、暗号化データ１１２をデータ記憶システム１１４に記憶させてもよい。データ記憶システム１１４は、サービスプロバイダ１０６とは別々であるように示されているが、サービスプロバイダ１０６のサブシステムであってもよい。例えば、サービスプロバイダ１０６のウェブサーバーに要求１０４を提示してもよい。この場合、ウェブサーバーは、データ記憶システム１１４へのアクセスが可能であるように構成されている。一般に、顧客へのサービスとしてデータ記憶システム１１４を運用してもよく、それにより、顧客は、データを記憶させる目的でサービスプロバイダ１０６のリソースを利用できるようになっている。他の実施形態においても、データ記憶システム１１４とサービスプロバイダ１０６とが別々になっている場合がある。データ記憶システム１１４は、例えば、サービスプロバイダ１０６と顧客１０２との第三者であるエンティティによって運用されてもよく、またはいくつかの実施形態では、データ記憶システム１１４は、顧客１０２のサブシステム、すなわち、顧客１０２のシステムのサブシステムであってもよい。なお、「顧客」及び「サービス」プロバイダなどの用語は多くの意味を持つことが可能であり、こうした意味は文脈から明らかになることに留意すべきである。例えば、用語「顧客」は、顧客エンティティの運用を支援するエンティティ（例えば、組織もしくは個人などの法的実体）、またはシステム（例えば、コンピューティング装置もしくはコンピューティング装置からなるネットワーク）を指す場合がある。同様に、用語「サービスプロバイダ」は、サービスプロバイダエンティティの運用を支援する法的実体またはシステムを指す場合がある。

【００１５】

図１に示したように、データ１０８を暗号化して暗号化データ１１２を生成する際、サービスプロバイダ１０６は、１つ以上の動作を実行して、サービスプロバイダ１０６による暗号鍵１１０へのアクセスをできなくするようにしてもよい。これは、図１では、ごみ箱とラベル付けされたアイコンに対してサービスプロバイダ１０６が暗号鍵１１０を渡すこととして表されている。なお、説明の都合上、ごみ箱に暗号鍵１１０を渡すことを図面に示したが、様々な実施形態では、暗号鍵１１０にアクセスできなくするための動作を実行する際に必ずしも暗号鍵１１０の転送を伴わなくてもよいことに留意すべきである。例えば、いくつかの実施形態では、要求１０４の受信と暗号鍵１１０の使用とに応じて、サービスプロバイダ１０６は、１つ以上の操作を実行して暗号鍵１１０を破壊してもよい。様々な実施形態に従って様々な方法で暗号鍵１１０の破壊を実行してもよい。例えば、いくつかの実施形態では、暗号鍵１１０及び要求１０４は、サービスプロバイダ１０６によって永続的には記憶されないが、サービスプロバイダ１０６の装置に搭載された揮発性メモリに保持されている。

【００１６】

暗号鍵１１０の破壊は、暗号鍵１１０が記憶されている１つ以上のメモリ位置を、後続

の要求の一部として受信したデータなどの他のデータを用いて上書きすることを可能にすることによって実行されてもよい。他の操作を実行してもよい。例えば、暗号鍵１１０が揮発性メモリまたは不揮発性メモリに記憶されている場合、暗号鍵１１０の記憶に使用されている１つ以上のメモリ位置を、（例えば、暗号鍵の破壊を意図した１つ以上の書き込み操作を介して）ランダムデータまたは一連のゼロデータなどの非ランダムデータといった他のデータを用いて上書きすることによって暗号鍵１１０を破壊してもよい。一般に、サービスプロバイダ１０６による暗号鍵１１０へのアクセスを失効せる任意の操作を利用してもよい。このように、顧客１０２は、サービスプロバイダ１０６に対して暗号鍵付きの要求を提示することが可能であるが、この暗号鍵は、データ１０８の暗号化に使用されることを顧客１０２が望んでいるものである。さらに、サービスプロバイダ１０６は、様々な実施形態では、暗号鍵１１０を使用した後に暗号鍵１１０へのアクセスをできなくするように構成されており、サービスプロバイダが、要求１０４を処理すると、復号化データ１１２の復号化によってデータ１０８にアクセスできなくなることを顧客１０２に保証することができる。換言すれば、データ１１２のセキュリティは、サービスプロバイダ１０６が時間を限ってデータにアクセスしつつ、最終的には顧客１０２によって制御される。

【００１７】

なお、暗号化データ（及び対応する復号化データ）が得られる様々なプロセスが全体を通して例示のために使用されているが、これらの様々なプロセスは他の実施形態に応じて変わり得ることに留意すべきである。例えば、本明細書で示した例示的な暗号化プロセスは、サービスプロバイダの顧客から供給された鍵を用いた暗号化を示しており、この場合、ある時間が経過した後、使用された鍵へのサービスプロバイダのアクセスをできなくするように暗号化が実行される。しかしながら、より複雑な方式を利用してもよく、その場合、２つ以上の鍵を使用してデータへのアクセスを制御する。例えば、図１を参照すると、いくつかの実施形態では、要求において顧客から供給された鍵と、サービスプロバイダによって保持されている、あるいはサービスプロバイダにとってアクセス可能な鍵との両方を用いてデータを暗号化してもよい。このように、暗号化データを復号化する性能を備えるという目的で、顧客１０２とサービスプロバイダ１０６との間の連携動作がデータ１０８へのアクセスに必要とされる。いくつかの実施形態では、例えば、ある鍵を用いてデータ１０８を暗号化し、次いで別の鍵を用いて再度暗号化してもよい。他の実施例では、暗号鍵１１０と別の鍵とを組み合わせてさらに別の鍵を生成し、これをデータ１０８の暗号化に使用してもよい。このような変形例は、顧客１０２及びサービスプロバイダ１０６に加えて多くの当事者に適用される場合もある。従って、一般に、暗号化されたデータ、すなわち平文形式のデータに適法にアクセスするためには、複数のエンティティによる連携動作が必要とされる。他の変形例も本開示の範囲内にあるものとみなされる。

【００１８】

加えて、本明細書で説明された様々な実施形態では、ある種類のデータを有する要求について説明したが、要求には他の種類のデータを含めてもよい。例えば、要求には、要求の様々なパラメータについてのデータを含めてもよく、このデータは、要求を実施するかどうか及び／または要求の実施方法を決定するために、サービスプロバイダによって使用され得る。一般に、本明細書で述べるような要求は、説明の都合上簡略化されている。要求には、例えば、要求元の識別情報、要求の発生元ネットワークアドレス、要求及び／または他の種類のデータの一部または全てを生成したエンティティの識別情報などの、状況に即した様々なデータを含めてもよい。

【００１９】

さらに、図１には、暗号化対象のデータ１０８を要求１０４が有することを示したが、本開示の範囲内の要求は、必ずしも暗号化対象データを有するものではないことにも留意すべきである。例えば、いくつかの実施形態では、要求は、その要求に必ずしも含める必要のないデータへの参照（例えば、データオブジェクトの識別子であり、これはＵＲＬの形態であってよい）を有してもよい。かかる要求を処理することは、参照を使用してデー

タを取得することを含んでもよい。別の実施例として、ある要求にはデータが欠けていてもよい。なぜなら、要求には、１つ以上の要求された操作としてデータを読み出すことが含まれるためである。データを読み出すことを求める要求には暗号鍵を含めてもよいが、データは、別の場所に記憶されていてもよい。要求を処理することは、暗号化データにアクセスして、これを、要求で提供された暗号鍵を用いて復号化することを含んでもよい。他の変形例も本開示の範囲内にあるものとみなされる。

【００２０】

様々な実施形態に係るサービスプロバイダ２００の環境の例示的な実施例を図２に示す。図２に示すように、サービスプロバイダ２００は顧客インターフェース２０２を含む。顧客インターフェースは、サービスプロバイダ２００のサブシステムであってよい。このインターフェースにより、図１に関連して上述したように、サービスプロバイダ２００によって処理され得る顧客からの要求を提示することが可能となる。従って、顧客インターフェースは、サービスプロバイダ２００に要求を提示する機能を顧客に提供できるように、適切なコンピューティング装置を含んでもよい。この顧客インターフェースは、例えば、インターネットまたは別のネットワークを介して要求を受信するように構成された１つ以上のウェブサーバーを含んでもよい。このように例示されてはいないが、他の基盤を顧客インターフェース２０２に含めてもよい。このような基盤としては、サービスプロバイダ２００の顧客にとって顧客インターフェース２０２が適切に稼働することを可能にするための適切なネットワーク機器などがある。

【００２１】

顧客インターフェース２０２を通じて要求が受信されるときには、適切な認証情報と共に要求が受信され得る。例えば、図２に示すように、要求２０４は、当該要求の署名２０６と共に受信されてもよい。この署名は、様々な実施形態に従って生成され得る。例えば、要求２０４を提示した顧客は、顧客とサービスプロバイダ２００との間で共有された秘密情報を用いて署名２０６を生成してもよい。別の実施例として、顧客は、非対称デジタル署名方式を使用して、私有鍵／公開鍵のペアのうちの私有鍵を用いて要求２０４に署名していた場合がある。一般に、要求２０４の認証に用いられる任意の種類の情報を使用してもよく、いくつかの実施形態では、こうした情報を含めずに要求を提示してもよい。さらに、いくつかの実施形態では、要求に対する電子署名は、当該要求で供給された暗号鍵とは異なる暗号鍵を用いて生成されるが、いくつかの実施形態では、電子署名は、その要求で供給されたものと同じ鍵を用いて生成される。

【００２２】

しかしながら、図２に示すように、顧客インターフェース２０２を通じて要求２０４を受信するときには、要求２０４は、（例えば、サービスプロバイダ２００の内部ネットワークを介して）署名２０６と共にサービスプロバイダ２００の認証システム２０８に提供される。あるいは、要求全体ではなく、電子署名２０６を生成するのに十分な要求の一部を提供してもよい。認証システム２０８は、サービスプロバイダ２００のサブシステムであってよい。このサブシステムは、要求と共に提供された電子署名を検証するなどして要求を認証するように構成されている。要求２０４の署名２０６を検証する際、認証システム２０８は、顧客インターフェース２０２に応答を提供し、それによって署名２０６が有効であるかどうかを示してもよい。顧客インターフェース２０２の装置は、要求２０４の処理方法を決定するために、認証システム２０８によって提供された情報を使用してもよい。例えば、署名２０６が無効であることを認証システム２０８が示した場合、顧客インターフェース２０２はその要求を拒否してもよい。同様に、認証システム２０８からの情報によって要求２０４の署名２０６が有効であることが示された場合、顧客インターフェース２０２によって要求２０４を処理させてもよい。

【００２３】

図面には示されていないが、認証システム２０８、またはサービスプロバイダ２００内で動作する、もしくはサービスプロバイダ２００に代わって動作する別のシステムを稼働して、要求の処理方法を決定することに関連して他の操作を実行してもよい。例えば、認

証システム２０８またはこれと連携して動作する別のシステムを使用して、要求の実施が可能であるかどうかにとって決定的となり得る１つ以上の方針を決定してもよい。方針の決定は、様々な要素に少なくとも部分的に基づいてなされる場合がある。このような要素としては、要求を提示した要求元の識別情報、時刻、データが記憶されている、またはデータが記憶され得る位置の論理識別子、及び状況に即した他の情報などがある。方針は、顧客インターフェース２０２または別のインターフェースを通じ、適切に構成されたアプリケーションプログラミングインターフェース（ａｐｐｌｉｃａｔｉｏｎ　ｐｒｏｇｒａｍｍｉｎｇ　ｉｎｔｅｒｆａｃｅ：ＡＰＩ）の呼び出しを通じて扱われる場合がある。

【００２４】

図２に示した実施形態に戻ると、署名２０６が有効であると認証システム２０８が判定した場合、顧客インターフェース２０２は、その要求を処理することを決定してもよい。要求を処理する際には、顧客インターフェース２０２と要求処理基盤２１２との間で暗号化データ２１０を転送することが必要となる場合がある。要求処理基盤２１２は、サービスプロバイダ２００のサービスを提供するために集合的に動作する１つ以上の装置を備えてもよい。例えば、図２に示すように、要求処理基盤は、サービスプロバイダ２００の顧客に代わってデータを記憶するのに使用される複数のデータ記憶システム２１４を備えてもよい。図示されてはいないが、ネットワーク通信基盤を含む他の基盤が含まれてもよい。例えば、顧客インターフェース２０２と要求処理基盤２１２との間のネットワークを介したデータの移動は、顧客インターフェース２０２を通じて提示され得る各種の要求に応じて、様々な実施形態に従って様々な方法で発生する場合がある。例えば、要求２０４がデータの記憶を求める要求である場合、顧客インターフェースは、要求２０４で提供された鍵を利用して当該データを暗号化し、この暗号化データ２１０を要求処理基盤２１２に送信することにより、データ記憶システム２１４の１つ以上に記憶させてもよい。

【００２５】

同様に、要求２０４がデータの読み出しを求める要求である場合、顧客インターフェース２０２は、要求処理基盤２１２に通信情報を送信し、それにより、データ記憶システム２１４の１つ以上から取り出したデータを顧客インターフェース２０２に提供できるようにしてもよい。次いで、顧客インターフェース２０２は、要求２０４で提供された鍵を使用して、暗号化データ２１０を復号化し、要求２０４を提示した顧客に対してこの復号化データを提供してもよい。なお、図２に示したサービスプロバイダ２００の環境は説明の都合上簡略化されていること、及び顧客によるサービスプロバイダ２００の使用経過を常に把握する会計システムなどの、その他多数の装置及びサブシステムも含まれ得ることに留意すべきである。さらに、サービスプロバイダ２００は、冗長化及び／または可用性のために、種々の地理的位置に配置された施設を含んでもよい。

【００２６】

様々な実施形態に係る要求３００の例示的な実施例を図３に示す。この場合、要求は、図１～２に関連して上述したような要求であってよい。図３に示した実施例に示すように、要求３００には対称鍵が含まれる。この対称鍵は、データの暗号化と復号化の両方に使用される暗号鍵であってよい。ある実施形態では、要求３００の対称鍵３０２は、要求３００において平文形式で提供される。なお、いくつかの実施形態では、要求３００において対称鍵が平文形式で提供されるが、顧客からサービスプロバイダへの、または一般的にはエンティティ間での要求の転送には、要求３００に含まれる任意のデータのセキュリティを確保するために様々なプロトコルが必要となり得ることに留意すべきである。例えば、要求３００を送信する際には、トランスポート層セキュリティ（ｔｒａｎｓｐｏｒｔ　ｌａｙｅｒ　ｓｅｃｕｒｉｔｙ：ＴＬＳ）及び／または別のプロトコルが必要となる場合があるが、それによって対称鍵３０２は、あるエンティティから他のエンティティへの送信中は暗号化されるようになる。さらに、図３には要求３００が対称鍵３０２を有することを示したが、要求３００は、図面に示されていない他のデータを含んでもよい。上記のこのようなデータには、様々な要求パラメータ、認証情報、暗号化対象データ及び／または他の情報を含めてもよい。

【００２７】
加えて、図３には鍵付きの要求を示したが、本明細書で説明及び図示した全ての要求と同様に、他の様々なデータを要求内に格納してもよい。このようなデータとしては、操作対象データ、並びに／または、要求についての状況に即した情報、及び要求の真正性を検証するのに使用可能な認証情報を含む様々なメタデータなどがある。様々な要求パラメータを要求に含めてもよい。例えば、要求パラメータは、要求と共に提供された鍵を用いてデータを暗号化するためにサーバー側暗号化を使用することになっていることを指定してもよい。こうしたパラメータがない場合、かつ／またはこうしたパラメータによってサーバー側暗号化の不使用が示された場合、鍵が要求に含まれているかどうかに関係なく、暗号化を行わずに要求を処理してもよい。さらに、電子署名と共に提示された要求の場合、パラメータは、要求のどの部分を使用して電子署名を生成したかを指定してもよい。こうしたパラメータは、電子署名を照合するのに要求のどの部分を使用すべきかを指示することができる。それにより、要求の実施中に操作対象データを加えるなどして、要求を生成した後にそれらを変更することが可能となる。全体として、本開示では説明の都合上、要求を簡略化している。
【００２８】
様々な実施形態に係る要求に対する応答を送受信するのに使用され得るプロセス４００の例示的な実施例を図４に示す。プロセス４００は、図１５に関連して前述及び後述するような顧客の装置などの任意の適切なシステムによって実行され得る。ある実施形態では、プロセス４００は、暗号鍵を取得すること４０２を含む。この暗号鍵は、４０２において、様々な実施形態に従って様々な方法で取得され得る。例えば、いくつかの実施形態では、暗号鍵は、当該暗号鍵を生成することによって４０２で取得される。暗号鍵は、例えば、乱数発生器、または公開鍵導出関数２（ｐｕｂｌｉｃ　ｋｅｙ　ｄｅｒｉｖａｔｉｏｎ　ｆｕｎｃｔｉｏｎ　２：ＰＰＫＤＦ２）もしくはＢｃｒｙｐｔなどの鍵導出関数を用いて生成され得る。暗号鍵は、他の方法でも取得され得る４０２。例えば、暗号鍵は、データ記憶装置からアクセスされ得る。別の実施例として、暗号鍵は、メモリからアクセスされ、かつ／またはプロセス４００を実行するシステムのユーザーによって入力されるパスワード、パスフレーズ、または他の種類のパスコードであってもよい。一般に、暗号鍵を取得すること４０２については任意の方法を使用してもよい。
【００２９】
暗号鍵を４０２で取得したことにより、プロセス４００は、取得した暗号鍵付きの要求を生成すること（すなわち、取得した暗号鍵を含む要求を生成すること）４０４を含んでもよい。この要求は、当該要求の提示を受けるシステムによって処理可能なフォーマットに従った、転送に適した方法で要求用のデータを並べることによって生成され得る。４０４で一旦生成されると、生成された要求は４０６で提示され得る。生成された要求の提示４０６は、生成された要求を受信するように構成されたウェブサーバーのＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスに送信するなどの任意の適切な方法で実行され得る。他の操作を実行してもよく、例えば、いくつかの実施形態では、ユニフォームリソースロケータ（ｕｎｉｆｏｒｍ　ｒｅｓｏｕｒｃｅ　ｌｏｃａｔｏｒ：ＵＲＬ）から要求が生成される。生成された要求の提示をその後４０６にて受けるシステムのＩＰアドレスを取得するために、ドメインネームサービス（ｄｏｍａｉｎ　ｎａｍｅ　ｓｅｒｖｉｃｅ：ＤＮＳ）との通信が生じ得る。一般に、要求の発行については、任意の方法を実行してもよい。
【００３０】
提示すると、要求は、当該生成された要求の提示４０６を受けたシステムによって処理され得る。従って、プロセス４００は、その要求に対する応答を受信すること４０８を含んでもよく、あるいは、その応答は、要求を提示するのに用いたプロトコルに応じて適切に構成された応答であってもよい。なお、要求に対する応答を受信することが全ての実施形態にとって必要となるわけではないことに留意すべきである。例えば、いくつかのプロトコルを用いると、要求を受信した、かつ／または実施したという確認応答がなくても要

求を提示できる場合がある。例示的な実施例として、この要求は、データを記憶させることを求めるものであってよい。いくつかの実施形態では、提示すると、要求の処理についての確認応答を必要としなくてよい場合には要求が処理された、または要求がすでに処理されてしまった可能性があるとみなされることがある。

【００３１】

要求を処理するプロセス５００の例示的な実施例を図５に示す。ここで、要求は、上記のように受信されてもよく、上記のようなプロセス４００などのプロセスに従って提示されてもよい。プロセス５００は、上記のような顧客インターフェースを提供するために動作する装置（例えば、サーバー）によるなどして、任意の適切なシステムによって実行され得る。ある実施形態では、プロセス５００は、暗号鍵付きの要求を受信すること５０２を含む。この要求は、５０２において、様々な実施形態に従って様々な方法で受信され得る。例えば、上述したように、通信プロトコルに従ってネットワークを介して要求が提示されてもよく、こうしたプロトコルに従って要求が受信されてもよい。一般に、任意の適切な方法を用いて要求を５０２で受信してもよい。

【００３２】

要求の受信時、プロセス５００は、要求を実施するかどうかを決定すること５０４を含んでもよい。要求を実施するかどうかの決定５０４は、様々な実施形態に従って様々な方法でなされてもよい。例えば、上述したように、いくつかの事例では、要求は、当該要求の電子署名と共に受信される場合がある。従って、署名が有効であるかどうかを判定することによって決定をなす場合がある。署名が有効であるかどうかの判定は、様々な方法で実行され得る。例えば、プロセス５００を実行するシステムは、署名自体を検証してもよく、あるいは、署名及び要求（または一般的に、署名を生成するためにサインされたデータ）を、電子署名を検証するように動作可能な別のシステムに送信してもよい。さらに、上述したように、要求を実施するかどうかの決定５０４は、１つ以上の方針によって要求の実施が排除されているかどうかの判定を実行することを含んでもよい。一般に、要求を実施するかどうかを決定する際には任意の方法を実行してもよい。

【００３３】

加えて、本明細書に示した図５及び他のプロセスでは、要求を実施するかどうかの決定を示したが、様々な実施形態では、システムは、有効な電子署名を備え、かつ／または方針に適合する必要がなくとも、適切に構成されたあらゆる要求を実施し得る。図５に示した実施形態に戻ると、署名が無効であり、かつ／または方針によって要求の実施が排除されている場合などのように、要求を実施しないと５０４で決定された場合、プロセス５００は、その要求を拒否すること５０６を含んでもよい。要求を拒否すること５０６は、様々な実施形態に従って様々な方法で実行され得る。例えば、要求に対する応答を提供して、要求が否定されたことを示し、かつ／または要求が拒否された理由に関する情報を提供するようにしてもよい。別の実施例として、要求を拒否することは、何の動作もとらないことによって単に実行されてもよい。すなわち、上記は、要求に対する応答を提供せず、かつ単に要求を実施しないことによってなされる。一般に、要求を実施しなくてもよい方法はいずれも、要求を拒否することとみなされ得る。

【００３４】

しかしながら、要求を実施すると決定された場合、プロセス５００は、その要求から暗号鍵を抽出すること５０８を含んでもよい。次いで、要求された１つ以上の暗号化操作を実行するために、すなわち要求の実施に関わる１つ以上の暗号化操作を実行するために、抽出された暗号鍵を５１０で使用してもよい。１つ以上の暗号化操作は、様々な実施形態に応じて、さらには受信した要求の種類に応じて変わり得る。いくつかの実施形態では、例えば、１つ以上の暗号化操作は、要求に含まれるデータの暗号化及び／または他のデータの暗号化を含む。別の実施例として、１つ以上の暗号化操作は、要求によって参照され、かつ／または要求で提供されたデータの復号化を含んでもよい。一般に、１つ以上の暗号化操作の一部として、鍵の導出並びに／または電子署名の生成及び／もしくは検証などの任意の種類の暗号化操作を実行してもよい。さらに、本明細書で説明された種々の例示

的な実施形態では、暗号化などの単一の暗号化操作を示したが、１つの要求を実施する際に多くの種類の暗号化操作を実行してもよい。ある実施例として、要求で提供された１つ以上の鍵を使用してデータを暗号化し、データの電子署名、及び／または暗号化データを生成してもよい。この場合、電子署名は、データが変更されたことを後で検証するのに使用することができる。他の変形例も本開示の範囲内にあるものとみなされる。

【００３５】

１つ以上の暗号化操作を実行する際、プロセス５００は、要求に対する応答を提供すること５１２を含んでもよい。この応答は、様々な実施形態に応じて、さらには、なされた要求の種類に応じて変わり得る。例えば、要求がデータの読み出しを求めるものであった場合、その応答には、読み出され、復号化されたデータを含めてもよい。要求がデータの記憶を求めるものであった場合、その応答は、データが記憶されたという確認応答であってもよい。チェックサムまたは他の検証情報を応答と共に提供してもよい。要求の実施に関わる１つ以上の暗号化操作を実行した後のある時点で、プロセス５００は、抽出された暗号鍵へのアクセスをできなくすること５１４を含んでもよい。この場合、上記のような様々な方法でアクセスが失われるようにしてもよい。

【００３６】

様々な実施形態に係る要求６００の例示的な実施例を図６に示す。図６に示すように、図３に関連して上述した要求とは異なり、要求６００は顧客公開鍵６０２を含む。この鍵は、公開鍵／私有鍵のペアのうちの公開鍵であってよい。ここで、この私有鍵は、顧客により、または顧客に代わって保持されている。本明細書で説明された他の要求と同様に、要求６００は、上記のような他のデータを含んでもよい。要求６００は、図４に関連して上述したように提示され得る。

【００３７】

プロセス７００の例示的な実施例を図７に示す。このプロセスは、図６に関連して上述したような顧客公開鍵を含む要求を処理するのに使用され得る。プロセス７００は、上記のような顧客インターフェースを提供するシステムなどの任意の適切なシステムによって実行され得る。図７に示すように、プロセス７００は、顧客公開鍵付きのＰＵＴ要求、換言すれば、この要求の一部として、顧客公開鍵を有するＰＵＴ要求（すなわち、データの記憶を求める要求）を受信すること７０２を含む。この要求は、７０２において、上記のように、さらには一般に任意の適切な方法で受信され得る。顧客公開鍵付きのＰＵＴ要求を７０２で受信する際、プロセス７００は、要求を実施するかどうかを決定すること７０４を含んでもよい。この場合、要求を実施するかどうかの決定は上記のようになされ得る。要求を実施すべきでないと７０４で決定された場合、プロセス７００は、上記のように要求を拒否すること７０６を含んでもよい。しかしながら、要求を実施すべきであると７０４で決定された場合、プロセス７００は、使用のために要求から顧客公開鍵を抽出すること７０８を含んでもよい。ある実施形態では、プロセス７００は、暗号鍵を取得すること７１０を含む。この場合、暗号鍵は上記のような対称鍵であってよい。暗号化は、７１０において、上記のような任意の適切な方法で取得され得る。例えば、暗号鍵は、データ記憶装置からアクセスされてもよく、または生成されてもよい。７１０で取得された暗号鍵は、要求で提供されたデータ、あるいは暗号化するように要求によって依頼されたデータを暗号化するために７１２で使用され得る。暗号鍵を暗号化する（ラップする）ために顧客公開鍵を７１４で使用してもよい。このように、暗号化された暗号鍵は、顧客公開鍵に対応する私有鍵を用いて復号可能である。従って、プロセス７００を実行するプロバイダが暗号化された暗号鍵へアクセスできない場合、プロバイダは、暗号化された暗号鍵を復号化することができない。

【００３８】

プロセス７００は、暗号化データを記憶すること７１６を含んでもよい。暗号化データを、例えば、データ記憶システムに送信して、そのデータを永続的に記憶させるようにしてもよい。要求に対する応答は、暗号化された暗号鍵を含ませて供されてもよい７１８。プロセス７００を実行するシステムは、上記のように暗号鍵へのアクセスを７２０で失効

し得る。このように、プロセス７００を実行するシステムが暗号鍵へのアクセスを７２０で一旦できなくなると、システムはもはや暗号化データを復号化することができない。そのため、復号化データを復号化するために最初に暗号鍵を復号化することによって暗号化データを適法に（すなわち、鍵を推測することも、さもなければ不正な方法でデータへのアクセスを得ることもなく）復号化するには、一般に、顧客公開鍵に対応する私有鍵を使用することが必要である。

【００３９】

なお、本明細書で説明されたあらゆるプロセスと同様に、変形例は本開示の範囲内にあるものとみなされることに留意すべきである。ある実施例として、ＰＵＴ要求を処理するプロセスを図７に示す。ここで、要求は顧客公開鍵を含む。こうした要求は、様々な実施形態に従って様々な方法で処理することができる。いくつかの実施形態では、例えば、対称暗号鍵を使用することが一般に計算上より効率的であるものの、公開鍵によってその後ラップされる暗号鍵を使用する代わりに、顧客公開鍵を使用して要求で受信したデータを暗号化してもよい。このように、顧客公開鍵に対応する私有鍵へアクセスすることのできるエンティティによってのみデータの復号化が可能である。このエンティティは、様々な実施形態では、要求を発行した顧客のみであってよい。

【００４０】

本開示の範囲内にあるものとみなされる変形例の別の実施例として、暗号化された暗号鍵は、暗号化データと共に記憶されてもよく、さらには要求に応答して送信されてもよく、送信されなくてもよい。データを復号化するためのこうした実施形態では、暗号鍵は、当該暗号鍵の復号化が可能なエンティティ（例えば、その暗号鍵を復号化するのに使用可能な私有鍵を有する顧客）に提供された記憶装置からアクセスされ得る。次いで、この記憶装置は、データの復号化を可能にするために、復号化された暗号鍵を返信してもよい。例えば、データの読み出しを求める顧客の要求が送られると、プロバイダは、（暗号化された暗号鍵を含む）初期応答を送信し得る。この応答には、当該暗号鍵が復号化に必要となるという通知が含まれる。顧客は、暗号鍵を復号化し、この復号化された暗号鍵をプロバイダに返信することにより、プロバイダが復号化データを復号化し、その復号化データを顧客に提供することができるようにしてもよい。他の変形例としては、暗号文の復号化に使用可能な暗号化された鍵と共にプロバイダから顧客に当該暗号文が提供される変形例が挙げられるが、これらも本開示の範囲内にあるものとみなされる。例えば、ＰＵＴ要求にはサーバー側暗号化を使用するが、クライアント側暗号化を使用して記憶データへのアクセスを取得する実施形態の場合、プロバイダは、復号化を正確に実行することを確保にするために（すなわち、データの復号化に成功するような仕方で復号化を実行することを確保するために）、（例えば、復号化のためにデータを適切に正規化することによって）適切にデータを処理するための命令を提供してもよく、またはクライアントライブラリの形態をとった実行可能命令を提供してもよい。

【００４１】

データを取得するプロセス８００の例示的な実施例を図８に示す。このデータは、上記のようなプロバイダによるなどして、暗号化された形式で別のシステムによって記憶されている。プロセス８００は、上記のようなプロバイダの顧客の装置によるなどして、任意の適切なシステムによって実行され得る。ある実施形態では、プロセス８００は、暗号化された暗号鍵を取得すること８０２を含む。例えば、暗号化された暗号鍵は、上記のプロセス７００またはその変形例の実行によって受信されていてもよい。暗号化された暗号鍵を取得することは、暗号化された暗号鍵を受信すること、または暗号化された暗号鍵に永続的データ記憶装置からアクセスすることを含んでもよい。一般に、暗号化された暗号鍵は、８０２において、任意の適切な方法で取得され得る。

【００４２】

暗号鍵の暗号化に使用される公開鍵に対応する私有鍵を８０４で使用して、暗号化された暗号鍵を復号化してもよい。復号化された暗号鍵を一旦取得すると、プロセス８００は、上記のように、復号化された暗号鍵付きのＧＥＴ要求を生成すること８０６、及び生成

したＧＥＴ要求を提示すること（例えば、送信すること）８０８を含んでもよい。ＧＥＴ要求を受信するシステムは、この要求に含まれる暗号鍵を用いることによって当該要求を処理して、この暗号鍵によって暗号化されたデータを復号化してもよい。次いで、応答を８１０で受信してもよい。ここで、この応答には、ＧＥＴ要求で提供された、復号化された暗号鍵を用いて復号化されたデータなどの、適切な情報を含めてもよい。

【００４３】

本明細書で説明されたあらゆるプロセスと同様に、プロセス８００の変形例は、本開示の範囲内にあるものとみなされる。例えば、暗号化された暗号鍵が、暗号化された暗号鍵の下で暗号化されているデータと共に記憶されているときには、暗号化された暗号鍵は、暗号化された暗号鍵に遠隔記憶装置からアクセスすることによって取得されてもよい。別の実施例として、いくつかの実施形態では、プロセス８００は、暗号化された暗号鍵の下で暗号化されたデータを提供することによって実施されるＧＥＴ要求を提示することを含んでもよい。プロセス８００を実行するシステムは、暗号化データを取得し、復号化された暗号鍵を使用してその暗号化データを復号化してもよい。換言すれば、プロセス８００は、たとえサーバー側でデータが暗号化されていた場合でも、クライアント側でデータを復号化するように変更され得る。

【００４４】

様々な要求の例示的な実施例を図９に示す。これらの要求は、様々な実施形態に従って様々な形式でラップされた（すなわち、暗号化された）暗号鍵を含んでもよい。例えば、プロバイダと共有された秘密９０６の下で暗号化された対称鍵９０４を有する要求９０２の例示的な実施例を図９に示す。ここで、プロバイダと共有された秘密は、顧客とプロバイダとの間で共有された別の対称鍵であってよい。別の実施例として、プロバイダ公開鍵９１２の下で暗号化された対称鍵９１０を含む要求９０８の実施例を図９に示す。このプロバイダ公開鍵は、それに対応する私有鍵へプロバイダがアクセスすることのできる公開私有鍵のペアに対応する公開鍵であってよい。別の要求９１４は、第三者と共有された秘密９１８の下で暗号化された対称鍵９１６を含む。この第三者とは、顧客とプロバイダの双方に対する第三者であるエンティティである。さらに別の実施例として、第三者の公開鍵９２４の下で暗号化された対称鍵９２２を有する要求９２０を図９に示す。ここで、この第三者は、顧客とプロバイダとに対する第三者であってよい。既に述べたように、図９に示したこれらの要求には別の情報を含めてもよい。

【００４５】

様々な実施形態に従って要求を提示するのに使用され得るプロセス１０００の例示的な実施例を図１０に示す。プロセス１０００は、上記のようなプロバイダの顧客のシステムによるなどして、任意の適切なシステムによって実行され得る。ある実施形態では、プロセス１０００は、暗号鍵を取得すること１００２を含む。ここで、この暗号鍵は、上記のように１００２で取得され得る。取得した暗号鍵は、ラップされた暗号鍵を１００４で生成するのに使用され得る。このようにラップされた暗号鍵は上記で取得した暗号鍵であり、これは別の鍵の下で暗号化されている。図９に関連して、ラップされた暗号鍵の実施例については既に説明されている。プロセス１０００は、ラップされた暗号鍵付きの要求を生成すること１００６を含んでもよい。すなわち、ラップされた暗号鍵を含むように要求が生成され得る。次いで、生成された要求を上記のように１００８で提示してもよい。様々な実施形態では、プロセス１０００は、１００８で提示された要求に対する応答を受信すること１０１０を含んでもよい。

【００４６】

上述したように、多くの実施形態は、本開示の範囲内にあるものとみなされる。いくつかの実施形態では、暗号化操作に必要とされる鍵からラップを解くために第三者のシステムを使用せずとも、顧客及びサービスプロバイダが対話することによってデータセキュリティを実現することができる。そのため、様々な実施形態を実装可能な環境１１００の例示的な実施例を図１１に示す。図１と同様であるが、図１１に示すように、環境１１００は、サービスプロバイダ１１０６に要求１１０４を提示する顧客１１０２を含む。本実施

例では、要求１１０４は暗号鍵１１０８を含む。この暗号鍵は、当該暗号鍵を囲む括弧で示すように、別の鍵によってラップされている。サービスプロバイダ１１０６は、暗号鍵からラップを解くのに使用可能な鍵１１１０へアクセスすることができ、それにより、サービスプロバイダ１１０６が暗号鍵１１０８を用いて暗号化操作を実行することが可能となる。

【００４７】

プロセス１２００の例示的な実施例を図１２に示す。このプロセスは、ラップされた暗号鍵を含む要求を処理するのに使用され得る。プロセス１２００は、図１１に関連して上述したサービスプロバイダ１１０６のウェブサーバーによるなどして、任意の適切なシステムによって実行され得る。ある実施形態では、プロセス１２００は、ラップされた暗号鍵を有する要求を受信すること１２０２を含む。要求を実施するかどうかの決定が１２０４でなされ得る。要求を実施しないと１２０４で決定された場合、プロセス１２００は、上記のように要求を拒否すること１２０６を含んでもよい。しかしながら、要求を実施すべきであると１２０４で決定された場合、プロセス１２００は、ラップされた暗号鍵をその要求から抽出すること１２０８を含んでもよい。

【００４８】

暗号鍵からラップを解くのに使用可能な鍵を１２１０で取得してもよい。暗号鍵からラップを解くのに使用可能な鍵を取得することは、様々な実施形態に従って様々な方法で実行され得る。例えば、ラップされた暗号鍵からラップを解くのに使用可能な鍵は、プロセス１２００を実行するシステムによって記憶されてもよい。ラップされた暗号鍵からラップを解くのに使用可能な鍵の識別子を使用して、ラップされた暗号鍵からラップを解くのに使用可能な鍵を、システムによって記憶され得る他の鍵から探してもよい。この識別子は、１２０２で受信した要求で提供されてもよく、あるいは、要求を提示したエンティティとの連携などによって確定されてもよい。ラップされた暗号鍵からラップを解くのに使用可能な鍵が１２１０で一旦取得されると、プロセス１２００は、ラップされた暗号鍵からラップを解くために、取得した鍵を使用すること１２１２を含んでもよい。このようにして、ラップが解かれた暗号鍵を取得する。ラップが解かれた暗号鍵を１２１４で使用して、１２０２で受信した要求の実施に関わる１つ以上の暗号化操作を実行してもよい。要求に対する応答が、上記のように１２１６で提供され、ラップが解かれた暗号鍵へのアクセスが１２１８でできなくしてもよい。

【００４９】

いくつかの実施形態では、既に述べたように、第三者が関与することが、データのセキュリティを維持することの一部となっている。そのため、様々な実施形態を実装可能な環境１３００の例示的な実施例を図１３に示す。図示した環境１３００は、上記のようにサービスプロバイダ１３０６に要求１３０４を提示する顧客１３０２を含む。また、上記のように、要求１３０４は、図９に関連して上述したように別の鍵によってラップされている暗号鍵１３０８を含んでもよい。しかしながら、図１３の実施例では、要求を受信するサービスプロバイダ１３０６のあるサブシステム（または、いくつかの実施形態では、サービスプロバイダの全てのサブシステム）は、暗号鍵１３０８からラップを解くのに使用可能な鍵へアクセスができなくてもよい。従って、環境１３００は、ラップされた暗号鍵１３０８からラップを解くのに使用可能な鍵１３１２へアクセスすることのできる鍵管理システム１３１０を有している。鍵管理システム１３１０は、サービスプロバイダ１３０６の１人以上の顧客に代わって暗号鍵を管理するように動作可能な任意のシステムであってよい。

【００５０】

鍵管理システム１３１０は、様々な実施形態に従って様々な方法で実装され得る。いくつかの実施形態では、鍵管理システムは、サービスプロバイダ１３０６のサブシステムであってよい。このサブシステムは、例えば、サービスプロバイダ１３０６によってホストされているハードウェアセキュリティモジュール（ｈａｒｄｗａｒｅ　ｓｅｃｕｒｉｔｙ　ｍｏｄｕｌｅ：ＨＳＭ）、または暗号鍵を安全に記憶する別の種類のセキュリティモジ

ュールによって実装され得る。いくつかの実施形態では、鍵管理システム１３１０は、サービスプロバイダ１３０６の別のサービスとして実装されている。このサービスは、サービスプロバイダ１３０６によって提供されるいくつかのサービスのうちの１つであってよく、以下に説明されるようにネットワークを介して顧客１３０２にとってアクセス可能であってよい。いくつかの実施形態では、鍵管理システムは、上記のようなシステムであるが、サービスプロバイダ１３０６と顧客１３０２とに対する第三者によって実装されている。このような実施形態では、暗号鍵からラップを解くのに使用可能な鍵１３１２が顧客１３０２またはサービスプロバイダ１３０６のうちの１以上と共有されていない限り、顧客１３０２もサービスプロバイダ１３０６も、暗号鍵１３０８からラップを解くのに使用可能な鍵へのアクセスはできない。他の変形例も本開示の範囲内にあるものとみなされる。例えば、鍵管理システム１３１０は、いくつかの実施形態では、顧客１３０２の一部として実装され得る。一般に、鍵管理システム１３１０は、サービスプロバイダ１３０６が、暗号鍵からラップを解くのに使用可能な鍵１３１２を用いて暗号鍵１３０８からラップを解くために、または一般的にはラップから解かれた状態とさせるために、通信しなければならないシステムである。サービスプロバイダ１３０６と鍵管理システム１３１０との間の通信は、１つ以上のネットワークを介して、さらには１つ以上の適切なネットワークプロトコルに従って発生し得る。このネットワークは、例えば、インターネットまたは以下で説明するような任意の適切なネットワークであってよい。

【００５１】

プロセス１４００の例示的な実施例を図１４に示す。このプロセスは、図１３に関連して上述したように、ラップされた暗号鍵を含む要求を処理するように実行され得る。ある実施形態では、プロセス１４００は、上記のように、ラップされた暗号鍵付きの要求を受信すること１４０２を含む。他のプロセスに関連して上述したように、要求を実施するかどうかの決定が１４０４でなされてもよく、要求を実施すべきではないと１４０４で決定された場合、プロセス１４００は、その要求を拒否すること１４０６を含んでもよい。一方、要求を実施すべきであると１４０４で決定された場合、プロセス１４００は、ラップされた暗号鍵をその要求から抽出することを含んでもよい。ラップされた暗号鍵は、１４１０においてアンラップシステムに送信され得る。このシステムは、図１３に関連して上述したような鍵管理システムであってよく、一般的には、ラップされた暗号鍵からラップを解くのに使用可能な鍵へのアクセスを伴うシステムであってよい。

【００５２】

ラップされた暗号鍵は、要求の形態をとってアンラップシステムに送信され得る。この要求は、アンラップシステムによって実施できるように適切に構成されている。例えば、この要求は、アンラップシステムにとってアクセス可能なフォーマットに従ってフォーマットされてもよく、要求を実施するかどうかを決定するために、アンラップシステムによって使用可能な情報を含んでもよい。こうした情報には、例えば、アンラップシステムへの要求、及び／またはラップされた暗号鍵と共に１４０２で受信した要求を認証するのに使用される認証情報を含めてもよい。例えば、アンラップシステムへの要求の実施が１つ以上の方針に適合するかどうかを決定するために使用され得る他の情報を提供してもよく、またはこの情報は、上記のような、状況に即したデータであってよい。別の情報として、ラップされた暗号鍵からラップを解くのに使用可能な鍵の識別子を含めてもよい。１４１０で送信された要求をアンラップシステムが実施するとすれば、プロセス１４００は、ラップが解かれた暗号鍵をアンラップシステムから受信すること１４１２を含んでもよい。ラップが解かれた暗号鍵を１４１４で使用して、１４０２で受信した要求の実施に関わる１つ以上の暗号化操作を実行してもよい。要求に対する応答は、上記のように１４１６で提供され、ラップが解かれた暗号鍵へのアクセスが１４１８でできなくしてもよい。

【００５３】

本開示の実施形態は、以下の条項に照らして説明することができる。

１．コンピュータ実装方法であって、

サービスプロバイダの１つ以上のコンピュータシステムであって、実行可能命令を用い

て構成された１つ以上のコンピュータシステムの制御下で、
前記サービスプロバイダの顧客に対応する要求元から、要求であって、前記要求の実施が、前記要求と共に提供されたデータに対して１つ以上の暗号化操作を実行すること、及び前記要求で供給された暗号鍵を使用することを含む前記要求を受信することであって、前記サービスプロバイダは、前記要求を受信するまでの時間は前記暗号鍵にアクセスすることができない、こと、
前記指定されたデータに対して前記１つ以上の暗号化操作を実行することの一部として、前記供給された暗号鍵を用いることによって前記要求を実施すること、
前記１つ以上の暗号化操作の実行結果をデータ記憶システムに提供すること、並びに
前記１つ以上の暗号化操作の実行後のある時間に、前記サービスプロバイダによる前記暗号鍵へのアクセスをできなくさせる１つ以上の操作を実行することを含むコンピュータ実装方法。
２．前記要求を実施することは、前記要求を解析して前記要求から前記暗号鍵を平文形式で抽出することを含む、条項１に記載のコンピュータ実装方法。
３．前記暗号鍵は、前記サービスプロバイダがアクセスできない、公開－私有鍵のペアのうちの公開鍵であり、
前記１つ以上の暗号化操作は、前記公開鍵を用いた非対称アルゴリズムの実行を含む、条項１または条項２に記載のコンピュータ実装方法。
４．前記要求で供給された前記暗号鍵が別の鍵によって暗号化されており、
前記コンピュータ実装方法は、前記要求で供給された前記暗号鍵を復号化することをさらに含み、
前記供給された暗号鍵を使用して前記１つ以上の暗号化操作を実行することは、前記復号化された、供給された暗号鍵を使用して前記１つ以上の暗号化操作を実行することを含む、条項１から条項３のいずれか一項に記載のコンピュータ実装方法。
５．前記要求で供給された前記暗号鍵を復号化することは、前記暗号鍵を復号用の別のエンティティに転送することを含む、条項１から条項４のいずれか一項に記載のコンピュータ実装方法。
６．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、前記システムに、
ネットワークを介して要求元から、要求であって、前記要求の実施が、前記要求で供給された暗号鍵を含む、前記要求を認証するのに使用可能な情報を用いて、前記要求で指定されたデータに対して１つ以上の暗号化操作を実行することを含む前記要求を受信すること、
前記要求を受信かつ認証した結果として、前記指定されたデータに対して前記１つ以上の暗号化操作を実行すること、及び
前記１つ以上の暗号化操作の実行結果を提供すること
を行わせる命令を含むメモリと
を備えたシステム。
７．前記要求は、データ記憶システムから暗号化データを読み出すことを求める要求であり、前記情報は、前記要求で供給された前記暗号鍵を用いて前記要求を認証するのに使用可能である、条項６に記載のシステム。
８．前記情報は、前記要求で供給された前記暗号鍵とは異なる第２の暗号鍵に少なくとも部分的に基づいて生成された電子署名を含むことによって前記要求を認証するのに使用可能である、条項６または条項７に記載のシステム。
９．前記１つ以上の暗号化操作は、前記指定されたデータの暗号化を含み、
前記１つ以上の暗号化操作の前記実行結果を提供することは、前記指定されたデータを暗号化形式で永続記憶用のデータ記憶システムに転送することを含む、条項６から条項８に記載のシステム。
１０．前記命令は、前記要求で供給された前記暗号鍵へのアクセスをできなくするため

の１つ以上の操作を、前記１つ以上の暗号化操作の実行後のある時間に前記システムに実行させることをさらに含む、条項６から条項９に記載のシステム。

１１．前記要求で供給された前記暗号鍵は、暗号化された形式をとっており、

前記命令は、前記暗号鍵を復号化された形式で前記システムに取得させることをさらに含み、

前記１つ以上の暗号化操作を実行することは、前記暗号鍵を復号化された形式で利用することである、条項６から条項１０に記載のシステム。

１２．前記要求で供給された前記暗号鍵が公開－私有鍵のペアのうちの公開鍵であり、

前記指定されたデータに対して前記１つ以上の暗号化操作を実行することは、

前記指定されたデータを、対称鍵を用いて暗号化すること、及び

前記公開鍵を使用して前記対称鍵を暗号化すること

を含む、条項６から条項１１に記載のシステム。

１３．前記システムは、前記要求を受信するまでの時間は前記暗号鍵にアクセスできない、条項６から条項１２に記載のシステム。

１４．前記要求で供給された前記暗号鍵は、暗号化された形式で前記要求において供給されており、

前記システムは、サブシステムであって、暗号化された形式で供給された前記暗号鍵を復号化するのに使用可能な特定の暗号鍵を含む複数の暗号鍵を、前記サブシステムの外部からアクセス不可能に、安全に記憶するように構成されたサブシステムをさらに含み、

前記命令は、暗号化された形式で供給された前記暗号鍵を前記サブシステムに復号化させて、前記１つ以上の暗号化操作を実行する際に使用させることを前記システムにさらに行わせる、条項６から条項１３に記載のシステム。

１５．前記情報は、前記要求を認証するための前記暗号鍵を使用して前記要求を認証するのに使用可能である、条項６から条項１４に記載のシステム。

１６．非一時的コンピュータ可読記憶媒体であって、コンピュータシステムの１つ以上のプロセッサによって実行されると、前記コンピュータシステムに、

サービスプロバイダのアプリケーションプログラミングインターフェース用にフォーマットされたアプリケーションプログラミングインターフェース要求であって、暗号鍵を含み、前記含まれた暗号鍵を用いて前記サービスプロバイダによってデータに対して実行され得る１つ以上の暗号化操作を指定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要求を生成すること、及び

前記生成されたアプリケーションプログラミングインターフェース要求を、前記アプリケーションプログラミングインターフェース要求に少なくとも部分的に基づいて生成された認証情報と共に、ネットワークを介してサービスプロバイダに送信することを可能にすることにより、前記暗号鍵を使用して前記１つ以上の暗号化操作を前記データに対して実行することを前記サービスプロバイダに行わせること

を行わせる命令が記憶された非一時的コンピュータ可読記憶媒体。

１７．前記アプリケーションプログラミングインターフェース要求は、前記サービスプロバイダのデータ記憶システムにデータを記憶させることを求めるものであり、前記１つ以上の暗号化操作は、前記データ記憶システムに記憶させる前に前記データを暗号化することを含む、条項１６に記載の非一時的コンピュータ可読記憶媒体。

１８．前記アプリケーションプログラミングインターフェース要求は、データ記憶システム内のデータであって、暗号化された形式で前記データ記憶システムに記憶されているデータを読み出すことを求めるものであり、前記１つ以上の暗号化操作は、前記データ記憶システムから読み出した後に前記データを復号化することを含む、条項１６または条項１７に記載の非一時的コンピュータ可読記憶媒体。

１９．前記暗号鍵を、暗号化された形式で前記アプリケーションプログラミングインターフェース要求に含めることにより、前記サービスプロバイダは、前記１つ以上の暗号化操作を実行する際に使用するために、暗号化された形式の前記暗号鍵を使用して暗号化されていない形式の前記暗号鍵を取得することができるようになっている、条項１６から条

項１８に記載の非一時的コンピュータ可読記憶媒体。
２０．前記暗号鍵は、前記要求を受信するまでは前記サービスプロバイダにとってアクセス不可能である、条項１６から条項１９に記載の非一時的コンピュータ可読記憶媒体。
２１．前記送信されたアプリケーションプログラミングインターフェース要求がデータを欠いている、条項１６から条項２０に記載の非一時的コンピュータ可読記憶媒体。
２２．前記認証情報は、前記アプリケーションプログラミングインターフェース要求に含まれる前記暗号鍵とは異なる別の暗号鍵に少なくとも部分的に基づいて生成される、条項１６から条項２１に記載の非一時的コンピュータ可読記憶媒体。
２３．前記アプリケーションプログラミングインターフェース要求は、前記要求の実施が前記要求に適用可能な１つ以上の方針に適合するかどうかを決定するために前記サービスプロバイダによって要求された情報をさらに含む、条項１６から条項２２に記載の非一時的コンピュータ可読記憶媒体。
【００５４】
上記の開示全体を通じて何度か述べたように、他の多くの変形例は、本開示の範囲内にあるものとみなされる。例えば、上述したように、多くの変形例では、対称暗号原始関数及び／または非対称暗号原始関数が利用される。対称鍵アルゴリズムには、ブロック暗号、ストリーム暗号及びデジタル署名方式を含む、データに暗号化操作を実行するための様々な方式が含まれる場合がある。例示的な対称鍵アルゴリズムとしては、高度暗号化標準（ａｄｖａｎｃｅｄ ｅｎｃｒｙｐｔｉｏｎ ｓｔａｎｄａｒｄ：ＡＥＳ）、データ暗号化標準（ｄａｔａ ｅｎｃｒｙｐｔｉｏｎ ｓｔａｎｄａｒｄ：ＤＥＳ）、トリプルＤＥＳ（ｔｒｉｐｌｅ ＤＥＳ：３ＤＥＳ）、サーペント（Ｓｅｒｐｅｎｔ）、トゥーフィッシュ（Ｔｗｏｆｉｓｈ）、ブローフィッシュ（ｂｌｏｗｆｉｓｈ）、ＣＡＳＴ５、ＲＣ４、及び国際データ暗号化アルゴリズム（ｉｎｔｅｒｎａｔｉｏｎａｌ ｄａｔａ ｅｎｃｒｙｐｔｉｏｎ ａｌｇｏｒｉｔｈｍ：ＩＤＥＡ）が挙げられるが、これらに限定されることはない。対称鍵アルゴリズムには、一方向性関数の出力を生成するのに使用されるものも含まれる場合があり、ハッシュベース・メッセージ認証コード（ｈａｓｈ－ｂａｓｅｄ ｍｅｓｓａｇｅ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｃｏｄｅ：ＨＭＡＣ）、メッセージ認証コード（ｍｅｓｓａｇｅ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｃｏｄｅ：ＭＡＣ）全般、ＰＢＫＤＦ２、及びＢｃｒｙｐｔを利用するアルゴリズムが挙げられるが、これらに限定されることはない。非対称鍵アルゴリズムにも、データに暗号化操作を実行するための様々な方式が含まれる場合がある。例示的なアルゴリズムとしては、ディフィー・ヘルマン鍵交換プロトコル、デジタル署名標準（ｄｉｇｉｔａｌ ｓｉｇｎａｔｕｒｅ ｓｔａｎｄａｒｄ：ＤＳＳ）、デジタル署名アルゴリズム、エルガマル（ＥｌＧａｍａｌ）アルゴリズム、種々の楕円曲線アルゴリズム、パスワード認証鍵交換（ｐａｓｓｗｏｒｄ－ａｕｔｈｅｎｔｉｃａｔｅｄ ｋｅｙ ａｇｒｅｅｍｅｎｔ）技法、ｐａｌｌｉｅｒ暗号システム、ＲＳＡ暗号化アルゴリズム（ＰＫＣＳ＃１）、Ｃｒａｍｅｒ－Ｓｈｏｕｐ暗号システム、ＹＡＫ認証鍵交換プロトコル（ＹＡＫ ａｕｔｈｅｎｔｉｃａｔｅｄ ｋｅｙ ａｇｒｅｅｍｅｎｔ ｐｒｏｔｏｃｏｌ）、ＮＴＲＵ暗号を用いた暗号システム、ＭｃＥｌｉｅｃｅ暗号システムなどを利用するものが挙げられるが、これらに限定されることはない。楕円曲線アルゴリズムとしては、楕円曲線ディフィー・ヘルマン（ｅｌｌｉｐｔｉｃ ｃｕｒｖｅ Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ：ＥＣＤＨ）鍵交換方式、楕円曲線統合暗号化方式（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｉｎｔｅｇｒａｔｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｃｈｅｍｅ：ＥＣＩＥＳ）、楕円曲線デジタル署名アルゴリズム（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅ Ａｌｇｏｒｉｔｈｍ：ＥＣＤＳＡ）、ＥＣＭＱＶ鍵交換方式、及びＥＣＱＶ非明示的証明方式（ｉｍｐｌｉｃｉｔ ｃｅｒｔｉｆｉｃａｔｅ ｓｃｈｅｍｅ）が挙げられる。他のアルゴリズム及びアルゴリズムの組み合わせも本開示の範囲内にあるものとみなされる。
【００５５】
加えて、既に述べたように、本開示の様々な実施形態は、様々な暗号化操作の実行を求める要求に含まれる暗号鍵の使用に関する。このような操作を実行するために使用される

ものとしてこれらの鍵について述べたが、本開示の様々な実施形態には、使用前に何らかの方法を用いて鍵を変換する場合も含まれることに留意すべきである。ある実施例として、要求に含まれる鍵がパスコードである場合、そのパスコードは、別の暗号化操作の実行に使用される前に、（例えば、鍵導出関数を用いて）変換され得る。さらに、上記の開示では特定種類の鍵（例えば、暗号鍵）について述べたが、こうした鍵も、使用前に同じように変換され得る。他の変形例としては、複数の鍵を要求で提供し、要求パラメータ及び／または要求のフォーマット設定において、これら複数の鍵をどのように使用すべきかを指定する変形例が挙げられる。

【００５６】

本開示の範囲内にあるものとみなされる他の変形例には、署名付きＵＲＬ（ｕｎｉｆｏｒｍ　ｒｅｓｏｕｒｃｅ　ｌｏｃａｔｏｒ）を利用する実施形態が含まれる。サービスプロバイダの顧客を含む図１に示したような環境を参照すると、顧客は、ＵＲＬ及び／または暗号鍵などの他の情報の一部に対する電子署名を含むＵＲＬを事前に生成することができる。顧客は、このＵＲＬを別のエンティティに提供してもよく、他のエンティティは、このＵＲＬを利用して要求をサービスプロバイダに提示することにより、その顧客の認証の下で１つ以上の操作を当該サービスプロバイダに実行させることができる。サービスプロバイダは、ＵＲＬ付きで提示された要求を受信し、電子署名を検証し、そのＵＲＬにおいて提供された鍵を用いて１つ以上の操作を実行することができる。このように、鍵による顧客の制御を伴ってサーバー側で暗号化及び復号化すること、並びに、必要がある場合を除きプロバイダの鍵へのアクセスが不可能となることを含む様々な利便性が得られる。署名付きＵＲＬ及びその変形例の利用については、「Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒｓ　Ｗｉｔｈ　Ｋｅｙｓ」と題する、同時出願された米国特許出願第１４／０３７，２８２号において詳しく述べられており、本出願全体が参照によって援用される。

【００５７】

様々な実施形態に従って態様を実装するための例示的な環境１５００の態様を図１５に示す。理解されるであろうが、説明の都合上ウェブベース環境を使用しているものの、種々の実施形態を実装するために、必要に応じて、種々の環境を使用してもよい。この環境は、電子クライアント装置１５０２を含む。この装置は、要求、メッセージまたは情報を適切なネットワーク１５０４を介して送受信し、当該装置のユーザーに情報を送り返すように動作可能な任意の適切な装置で構成することができる。このようなクライアント装置の実施例としては、パーソナルコンピュータ、携帯電話、ハンドヘルドメッセージ通信装置、ラップトップコンピュータ、タブレットコンピュータ、セットトップボックス、パーソナルデータアシスタント、組み込みコンピュータシステム、電子ブックリーダーなどが挙げられる。ネットワークには、イントラネット、インターネット、セルラーネットワーク、ローカルエリアネットワーク、もしくは他のこうしたネットワーク、またはそれらの組み合わせなどの任意の適切なネットワークを含めることができる。こうしたシステムに使用される構成要素は、少なくとも部分的には、選択されたネットワーク及び／または環境の種類によって決めてよい。こうしたネットワークを経由して通信するためのプロトコル及び構成要素は周知であり、本明細書で詳細に述べることはない。ネットワークを介した通信は、有線通信または無線通信及びこれらの組み合わせによって可能にすることができる。本実施例では、ネットワークにインターネットが含まれるが、これは、要求を受信し、これに応答してコンテンツを供給するウェブサーバー１５０６が環境に含まれるためである。しかしながら、当業者にとっては明らかであろうが、他のネットワークの場合には、同様の目的を果たす代替装置を使用することができる。

【００５８】

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ー１５０８及び１つのデータ記憶装置１５１０を含む。なお、複数のアプリケーションサーバー、アプリケーション層もしくは他のアプリケーション要素、アプリケーションプロセス、またはアプリケーションコンポーネントを用意することが可能であり、これらを連結し、あるいは別の方法で構成してもよく、これらが対話して、適切なデータ記憶装置からデータを取得するなどの

タスクの実行が可能であることを理解すべきである。本明細書で用いられるサーバーは、ハードウェア装置または仮想コンピュータシステムなどの様々な方法で実装されてもよい。いくつかの状況では、サーバーは、コンピュータシステム上で実行されているプログラミングモジュールを指す場合がある。本明細書で用いられる用語「データ記憶装置」は、任意の装置、またはデータの記憶、データへのアクセス及びデータの読み出しが可能な装置の組み合わせを指す。この装置は、任意の標準的な環境、分散環境またはクラスター環境において、データサーバー、データベース、データ記憶装置及びデータ記憶媒体を任意の組み合わせ及び個数で含んでもよい。アプリケーションサーバーは、必要に応じてデータ記憶装置と一体化してクライアント装置用の１つ以上のアプリケーションの態様を実行するための任意の適切なハードウェア及びソフトウェアを含むことができ、アプリケーションに対するデータアクセス及びビジネスロジックの一部（大部分でさえも）を処理する。アプリケーションサーバーは、データ記憶装置と連携してアクセス制御サービスを提供してもよく、テキスト、グラフィックス、音声及び／または映像などの、ユーザーに転送され得るコンテンツを生成することができる。これらのコンテンツは、本実施例において、ハイパーテキストマークアップ言語（ＨｙｐｅｒＴｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ：ＨＴＭＬ）、拡張マークアップ言語（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ：ＸＭＬ）または別の適切な構造化言語の形態でウェブサーバーによってユーザーに供給されてもよい。クライアント装置１５０２とアプリケーションサーバー１５０８との間でのコンテンツの受け渡しに加え、全ての要求及び応答の処理は、ウェブサーバーによって行うことができる。なお、ウェブサーバー及びアプリケーションサーバーは必須ではなく、単なる例示的な構成要素であることを理解すべきである。というのも、本明細書で述べた構造化コードは、本明細書の他の箇所で述べたような任意の適切な装置またはホストマシンで実行することができるためである。さらに、１つの装置によって実行されるものとして本明細書で説明した操作は、文脈から別途明らかでない限り、分散システムを形成し得る多数の装置によって集合的に実行されてもよい。

【００５９】

データ記憶装置１５１０は、複数の独立したデータテーブル、データベース、または他のデータ記憶機構及びデータ記憶媒体を含み、それによって本開示の特定の態様に関するデータを記憶することができる。例えば、図示したデータ記憶装置は、制作データ１５１２及びユーザー情報１５１６を記憶するための機構を含んでもよく、この機構を使用して制作側のためのコンテンツを供給することができる。データ記憶装置は、ログデータ１５１４を記憶するための機構を含むようにも図示されており、この機構は、報告、分析または他のこうした目的のために使用することができる。なお、ページ画像情報及びアクセス権情報などの、データ記憶装置への記憶が必要となり得る多くの他の態様が存在する可能性があり、これらは、必要に応じて上記に列挙した機構のいずれにも記憶させることができ、あるいはデータ記憶装置１５１０内の別の機構に記憶させることができることを理解すべきである。データ記憶装置１５１０は、アプリケーションサーバー１５０８から命令を受信し、それに応答してデータの取得、更新または処理を行うように、この装置に関連したロジックを通じて動作させることが可能である。一実施例では、ユーザーは、当該ユーザーによって操作される装置を通じて、ある種類の項目の検索要求を提示する場合がある。この場合、データ記憶装置は、ユーザー情報にアクセスして当該ユーザーの識別情報を検証する場合があり、カタログ詳細情報にアクセスしてその種類の項目に関する情報を取得することができる。次いで、この情報を、ユーザー装置１５０２で動作するブラウザを介してユーザーが見ることのできるウェブページ上の結果リストなどにより、ユーザーに返すことができる。特定の対象項目についての情報は、ブラウザの専用ページまたは専用ウィンドウで見ることができる。しかしながら、本開示の実施形態は、必ずしもウェブページ関連に限定されるとは限らず、要求全般の処理に対してより広く適用可能であってもよく、この場合、これらの要求は、必ずしもコンテンツを求める要求とは限らないことに留意すべきである。

【００６０】

各サーバーは、通常、そのサーバーの一般的な管理及び運用を行うために実行可能なプログラム命令を提供するオペレーティングシステムを含み、通常、コンピュータ可読記憶媒体（例えば、ハードディスク、ランダムアクセスメモリ、リードオンリーメモリなど）を備える。この記憶媒体は、サーバーのプロセッサによって実行されると、意図した機能をサーバーに実行させる命令を記憶するものである。サーバーのオペレーティングシステム及び一般的な機能の好適な実装は、既知であり、あるいは市販されており、特に本明細書の開示に照らして、当業者によって容易に実装される。

【００６１】

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用いて、通信リンク経由で相互接続されている複数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、当業者にとっては、こうしたシステムが、図１５に示したものよりも数の少ない、または多い構成要素を備えたシステムにおいても同様に動作可能であることが理解されるであろう。従って、図１５におけるシステム１５００の描写は、実際には例示であって、本開示の範囲を限定するものではないとみなすべきである。

【００６２】

さらに、多様な動作環境において様々な実施形態を実装することができる。これらの環境は、場合によっては、１つ以上のユーザーコンピュータ、コンピューティング装置、または処理装置を含むことができ、これらを使用して、任意の数のアプリケーションを動作させることができる。ユーザー装置またはクライアント装置としては、標準的なオペレーティングシステムが動作しているデスクトップコンピュータ、ラップトップコンピュータまたはタブレットコンピュータなどの任意の数の汎用パーソナルコンピュータ、並びにモバイルソフトウェアが動作しており、複数のネットワーク通信プロトコル及びメッセージ通信プロトコルに対応可能な携帯機器、無線機器及びハンドヘルド機器を挙げることができる。こうしたシステムは、開発及びデータベース管理などの目的のために、多種多様な市販オペレーティングシステム及び他の既知のアプリケーションが動作している複数のワークステーションも含むことができる。これらの装置としては、ダミー端末、シンクライアント、ゲームシステム、及びネットワークを介して通信可能な他の装置などの他の電子装置も挙げることができる。

【００６３】

本開示の様々な実施形態は、当業者に公知であろう少なくとも１つのネットワークを利用して、商業的に利用可能な多種多様なプロトコルを用いた通信に対応できるようになっている。このようなプロトコルとしては、伝送制御プロトコル／インターネットプロトコル（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ：ＴＣＰ／ＩＰ）、開放型システム間相互接続（Ｏｐｅｎ Ｓｙｓｔｅｍ Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ：ＯＳＩ）モデルの種々の層で動作するプロトコル、ファイル転送プロトコル（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ：ＦＴＰ）、ユニバーサルプラグアンドプレイ（Ｕｎｉｖｅｒｓａｌ Ｐｌｕｇ ａｎｄ Ｐｌａｙ：ＵｐｎＰ）、ネットワークファイルシステム（Ｎｅｔｗｏｒｋ Ｆｉｌｅ Ｓｙｓｔｅｍ：ＮＦＳ）、共通インターネットファイルシステム（Ｃｏｍｍｏｎ Ｉｎｔｅｒｎｅｔ Ｆｉｌｅ Ｓｙｓｔｅｍ：ＣＩＦＳ）及びアップルトーク（ＡｐｐｌｅＴａｌｋ）などがある。ネットワークとしては、例えば、ローカルエリアネットワーク、ワイドエリアネットワーク、バーチャル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、及びこれらの任意の組み合わせを挙げることができる。

【００６４】

ウェブサーバーを利用する実施形態では、ウェブサーバーは、ハイパーテキスト転送プロトコル（Ｈｙｐｅｒｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ：ＨＴＴＰ）サーバー、ＦＴＰサーバー、共通ゲートウェイインターフェース（Ｃｏｍｍｏｎ Ｇａｔｅｗａｙ Ｉｎｔｅｒｆａｃｅ：ＣＧＩ）サーバー、データサーバー、Ｊａｖａ（登録商標）

サーバー及びビジネスアプリケーションサーバーなどの、多種多様なサーバーまたは中間層アプリケーションを実行することができる。１つ以上のサーバーは、任意のプログラミング言語で書かれた１つ以上のスクリプトまたはプログラムとして実装され得る１つ以上のウェブアプリケーションを実行するなどして、ユーザー装置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できるようにしてもよい。このようなプログラミング言語としては、Ｊａｖａ（登録商標）、Ｃ、Ｃ＃もしくは Ｃ＋＋、またはＰｅｒｌ、Ｐｙｔｈｏｎもしくは ＴＣＬなどの任意のスクリプト言語、及びこれらの組み合わせなどがある。１つ以上のサーバーには、データベースサーバーを含めてもよい。データベースサーバーとしては、Ｏｒａｃｌｅ（登録商標）、Ｍｉｃｒｏｓｏｆｔ（登録商標）、Ｓｙｂａｓｅ（登録商標）及びＩＢＭ（登録商標）から市販されているものが挙げられるが、これらに限定されることはない。

【００６５】

環境は、上記のような様々なデータ記憶装置並びに他のメモリ及び記録媒体を含むことができる。これらは、１つ以上のコンピュータに対してローカルな（及び／もしくはそれに存在する）、またはネットワークにわたるコンピュータのいずれかもしくは全てから遠隔にある記憶媒体上などの、様々な位置に存在することができる。特定の一連の実施形態では、情報は、当業者にとって公知のストレージエリアネットワーク（ｓｔｏｒａｇｅ－ａｒｅａ ｎｅｔｗｏｒｋ：ＳＡＮ）に存在してもよい。同様に、コンピュータ、サーバーまたは他のネットワーク装置に起因する機能を実行するための任意の必要なファイルは、必要に応じてローカルに、かつ／または遠隔的に記憶されてもよい。システムがコンピュータ化された装置を含む場合、このような各装置は、バスを介して電子的に接続され得るハードウェア要素を含むことができ、これらの要素には、例えば、少なくとも１つの中央処理装置（ｃｅｎｔｒａｌ ｐｒｏｃｅｓｓｉｎｇ ｕｎｉｔ：ＣＰＵまたはｐｒｏｃｅｓｓｏｒ）、少なくとも１つの入力装置（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つの出力装置（例えば、表示装置、プリンタまたはスピーカ）が含まれる。また、こうしたシステムは、着脱可能媒体装置、メモリカード、フラッシュカードなどと共に、ディスクドライブ、光学式記憶装置、及びランダムアクセスメモリ（ｒａｎｄｏｍ ａｃｃｅｓｓ ｍｅｍｏｒｙ：ＲＡＭ）またはリードオンリーメモリ（ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ：ＲＯＭ）などの固体記憶装置などの１つ以上の記憶装置を含んでもよい。

【００６６】

また、こうした装置は、上記のようなコンピュータ可読記憶媒体リーダー、通信装置（例えば、モデム、（無線式または有線式）ネットワークカード、赤外線通信装置など）、及び作業メモリを含むこともできる。一時的かつ／またはより永続的にコンピュータ可読情報の収容、記憶、送信及び読み出しを行うために、コンピュータ可読記憶媒体リーダーを、遠隔記憶装置、ローカル記憶装置、固定型記憶装置及び／または着脱可能記憶装置、並びに記憶媒体を表すコンピュータ可読記憶媒体と接続することができ、またはそれを受け入れるように構成することができる。また、システム及び種々の装置は、通常、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などのアプリケーションプログラムを含む、少なくとも１つの作業メモリデバイス内に位置する複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、または他の要素も含む。なお、代替的実施形態は、上述したものからの多数の変形例を有してもよいことを理解するべきである。例えば、カスタマイズされたハードウェアを同様に使用してもよく、かつ／または、特定の要素が、ハードウェア、（アプレットなどのポータブルソフトウェアを含む）ソフトウェアもしくは両方で実装されてもよい。さらに、ネットワーク入出力装置などの他のコンピューティング装置への接続を採用してもよい。

【００６７】

コードまたはコードの一部を収容するための記憶媒体及びコンピュータ可読媒体としては、コンピュータ可読命令、データ構造、プログラムモジュールまたは他のデータなどの情報の記憶及び／または送信のための任意の方法または技術を用いて実装された、揮発性

媒体及び不揮発性媒体、着脱可能媒体及び着脱不可能媒体などであるもののこれらに限定されない記憶媒体及び通信媒体を含む、本分野において既知であり、または使用される任意の適切な媒体を挙げることができる。このような媒体としては、ＲＡＭ、ＲＯＭ、電気的消去可能なプログラマブルリードオンリーメモリ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ－Ｏｎｌｙ Ｍｅｍｏｒｙ：ＥＥＰＲＯＭ）、フラッシュメモリもしくは他のメモリ技術、コンパクトディスクリードオンリーメモリ（Ｃｏｍｐａｃｔ Ｄｉｓｃ Ｒｅａｄ－Ｏｎｌｙ Ｍｅｍｏｒｙ：ＣＤ－ＲＯＭ）、デジタル多用途ディスク（ｄｉｇｉｔａｌ ｖｅｒｓａｔｉｌｅ ｄｉｓｋ：ＤＶＤ）もしくは他の光学式記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置もしくは他の磁気記憶装置、または所望の情報を記憶するのに使用することができ、かつシステム装置によってアクセスすることができる任意の他の媒体が挙げられる。本明細書で提供される開示及び教示に基づき、当業者は、種々の実施形態を実装するための適切な他の方式及び／または方法を理解するであろう。

【００６８】

従って、本明細書及び本図面は、限定的な意味ではなく例示とみなされるべきである。しかしながら、特許請求の範囲に記載された本発明の広義の概念及び範囲から逸脱することなく、種々の変形及び変更がそれらになされてもよいことは明白であろう。

【００６９】

他の変形例は、本開示の概念の範囲内にある。従って、開示された技法には様々な変形及び代替構成の余地があるが、それらのある例示された実施形態について、図面に示し、上記で詳細に説明してきた。しかしながら、特定の形態または開示された形態に本発明を限定する意図はなく、むしろ、その意図は、添付された特許請求の範囲において定められるような、本発明の概念及び範囲内に属するあらゆる変形例、代替構成及び均等物に及ぶものであることを理解すべきである。

【００７０】

本明細書において示されるかまたは文脈によって明らかに否定されない限り、開示された実施形態を記載した文脈における（特に、以下の特許請求の範囲の文脈における）用語「ａ」及び「ａｎ」並びに「ｔｈｅ」並びに類似の指示対象の使用は、単数及び複数の両方を含むと解釈されるべきである。別段の記載がない限り、用語「備える（ｃｏｍｐｒｉｓｉｎｇ）」、「有する（ｈａｖｉｎｇ）」、「含む（ｉｎｃｌｕｄｉｎｇ）」及び「含有する（ｃｏｎｔａｉｎｉｎｇ）」は、開放型用語（すなわち、「含むが、これに限定されるものではない」ことを意味する）として解釈されるべきである。用語「接続された（ｃｏｎｎｅｃｔｅｄ）」は、修飾されておらず、かつ物理的接続を指すときには、介在するものがあったとしても、部分的または全体的に、内部に収容され、取り付けられ、または互いに結合されていると解釈されるべきである。本明細書における値の範囲の列挙は、本明細書において別段の指示がない限り、単に、その範囲内に属する各別個の値を個々に言及する簡略な方法として働くことが意図されるに過ぎず、各別個の値は、本明細書にそれが個々に列挙されているかのように本明細書に援用される。用語「集合（ｓｅｔ）」（例えば、項目の集合（ａ ｓｅｔ ｏｆ ｉｔｅｍｓ））または用語「部分集合（ｓｕｂｓｅｔ）」の使用は、別段の記載がないかまたは文脈によって否定されない限り、１つ以上の要素を含む空ではない集まりと解釈されるべきである。さらに、別段の記載がないかまたは文脈によって否定されない限り、対応する集合の用語「部分集合（ｓｕｂｓｅｔ）」は必ずしも対応する集合の適切な部分集合を指すものではなく、部分集合と対応する集合とが等しい場合がある。

【００７１】

「Ａ、Ｂ及びＣの少なくとも１つ（ａｔ ｌｅａｓｔ ｏｎｅ ｏｆ Ａ，Ｂ，ａｎｄ Ｃ）」または「Ａ、Ｂ及びＣの少なくとも１つ（ａｔ ｌｅａｓｔ ｏｎｅ ｏｆ Ａ，Ｂ，ａｎｄ Ｃ）」の形をとった句などの接続語句は、特に明確に記載がないかまたは文脈によって明らかに否定されない限り、通常であれば、項目、用語などがＡまたはＢまたはＣのいずれか、あるいはＡとＢとＣからなる集合の空ではない任意の部分集合となる

場合があることを表すために一般に使用される文脈と共に理解される。例えば、上記の接続語句に使用された３つの要素を有する集合の例示的な実施例では、「Ａ、Ｂ及びＣの少なくとも１つ（ａｔ　ｌｅａｓｔ　ｏｎｅ　ｏｆ　Ａ，Ｂ，ａｎｄ　Ｃ）」及び「Ａ、Ｂ及びＣの少なくとも１つ（ａｔ　ｌｅａｓｔ　ｏｎｅ　ｏｆ　Ａ，Ｂ，ａｎｄ　Ｃ）」は、以下の集合：｛Ａ｝、｛Ｂ｝、｛Ｃ｝、｛Ａ，Ｂ｝、｛Ａ，Ｃ｝、｛Ｂ，Ｃ｝、｛Ａ，Ｂ，Ｃ｝のいずれかを指す。従って、こうした接続語句は、一般には、ある実施形態が、少なくとも１つのＡ、少なくとも１つのＢ、及び少なくとも１つのＣを必須のものとしてそれぞれを含めるようにすることを意味することを意図するものではない。

【００７２】

本明細書で説明されたプロセスの操作は、本明細書に別段の指示がないかまたは文脈によって明らかに否定されない限り、任意の適切な順序で実行することができる。本明細書で説明されたプロセス（もしくは変形例及び／またはそれらの組み合わせ）は、実行可能命令を用いて構成された１つ以上のコンピュータシステムの制御下で実行される場合があり、ハードウェアまたはその組み合わせにより、１つ以上のプロセッサで集合的に実行されるコード（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）として実装される場合がある。このコードは、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態でコンピュータ可読記憶媒体に記憶されてもよい。コンピュータ可読記憶媒体は非一時的であってもよい。

【００７３】

本明細書で与えられた任意の実施例及び全ての実施例、または例示的な語句（例えば、「～など（ｓｕｃｈ　ａｓ）」）の使用は、単に、本発明の実施形態をより適切に説明することを意図しているに過ぎず、別に特許請求されない限り、本発明の範囲に限定を課すものではない。明細書中の語句はいずれも、本発明の実施に不可欠である任意の特許請求されていない要素を示すものとして解釈されるべきではない。

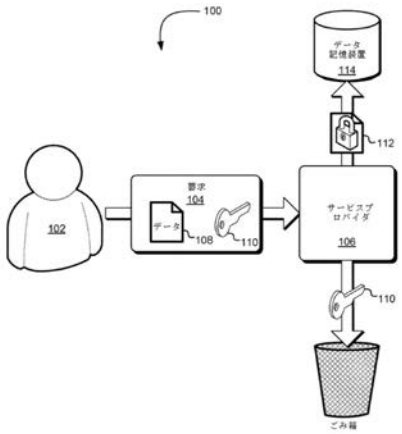
【００７４】

本開示の好ましい実施形態は、本発明者らに知られた、本発明を実施するためのベストモードを含めて、本明細書で説明されている。これらの好ましい実施形態の変形例は、前述の記載を読めば当業者にとって明らかとなり得る。本発明者らは、当業者が必要に応じてこのような変形例を採用することを予期しており、本明細書中に具体的に記載されたものとは異なる方法で本開示の実施形態が実施されることを意図している。従って、本開示の範囲は、適用可能な法律によって許容されるような、本明細書に添付された特許請求の範囲に列挙された主題の全ての変形例及び均等物を含む。さらに、全ての可能なその変形例における上述の要素の任意の組み合わせは、本明細書に別段の指示がないかまたは文脈によって明らかに否定されない限り、本開示の範囲によって包含される。

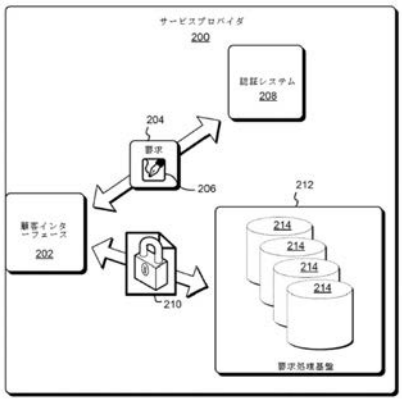
【００７５】

本明細書に列挙された、刊行物、特許出願及び特許を含む全ての引用文献は、各引用文献が、参照によって援用されるように個々にかつ詳細に示され、かつその全体が本明細書に記載されるのと同じ程度まで、参照によってここに援用される。

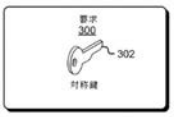
【図１】


100
データ
記憶装置
114
112
102
要求
104
データ
108
110
サービスプ
ロバイダ
106
110
ごみ箱

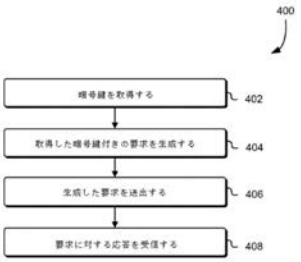
【図２】


サービスプロバイダ
200
認証システム
208
204
要求
206
212
顧客インタ
ーフェース
202
214
214
214
214
210
要求処理基盤

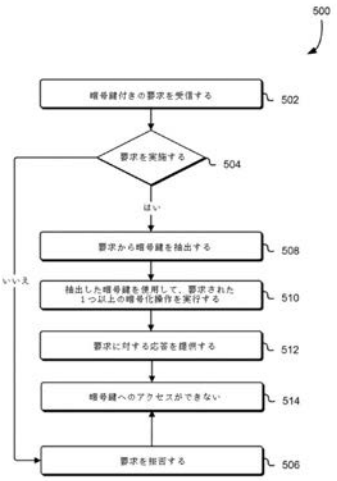
【図３】


要求
300
302
付符鍵

【図４】


400
暗号鍵を取得する
402
取得した暗号鍵付きの要求を生成する
404
生成した要求を送出する
406
要求に対する応答を受信する
408

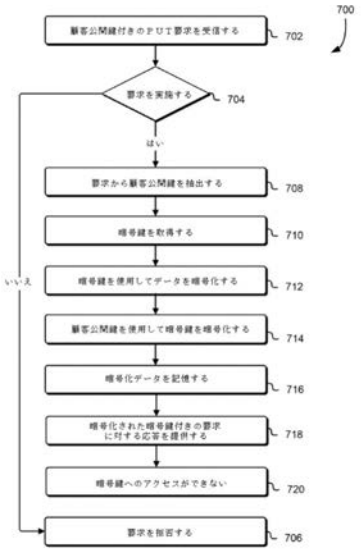
【図５】


500
暗号鍵付きの要求を受信する
502
要求を実施する
504
はい
いいえ
要求から暗号鍵を抽出する
508
抽出した暗号鍵を使用して、要求された
1つ以上の暗号化操作を実行する
510
要求に対する応答を提供する
512
暗号鍵へのアクセスができない
514
要求を拒否する
506

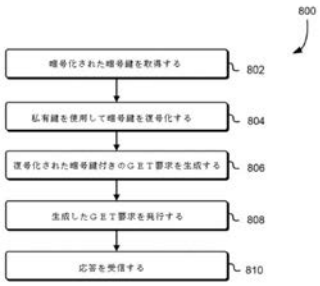
【図６】


要求
600
602
顧客公開鍵

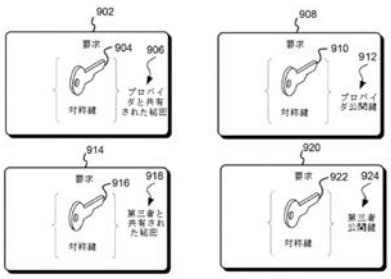
【図７】


700
顧客公開鍵付きのＰＵＴ要求を受信する
702
要求を実施する
704
はい
いいえ
要求から顧客公開鍵を抽出する
708
暗号鍵を取得する
710
暗号鍵を使用してデータを暗号化する
712
顧客公開鍵を使用して暗号鍵を暗号化する
714
暗号化データを記憶する
716
暗号化された暗号鍵付きの要求に対する応答を提供する
718
暗号鍵へのアクセスができない
720
要求を拒否する
706

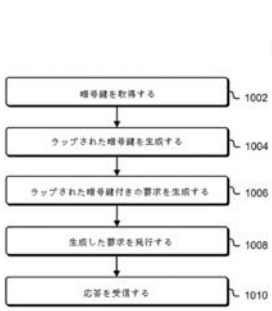
【図８】


800
暗号化された暗号鍵を取得する
802
私有鍵を使用して暗号鍵を復号化する
804
復号化された暗号鍵付きのＧＥＴ要求を生成する
806
生成したＧＥＴ要求を発行する
808
応答を受信する
810

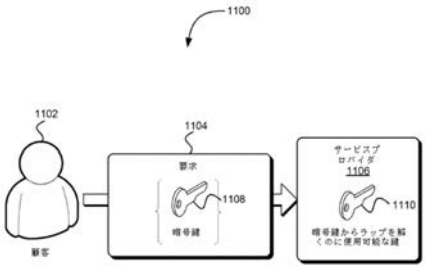
【図９】


902
要求
904
906
対称鍵
プロバイダと共有された秘密
908
要求
910
912
対称鍵
プロバイダ公開鍵
914
要求
916
918
対称鍵
第三者と共有された秘密
920
要求
922
924
対称鍵
第三者公開鍵

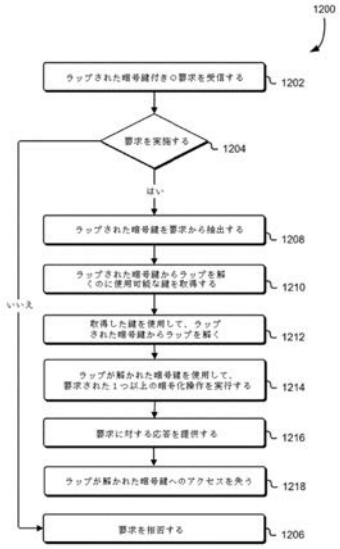
【図１０】



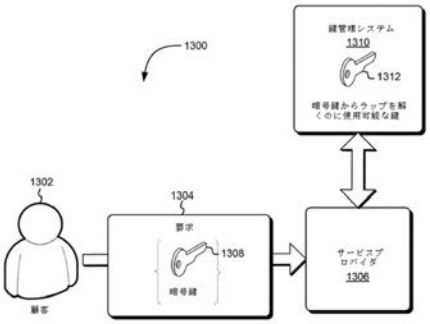
【図１１】



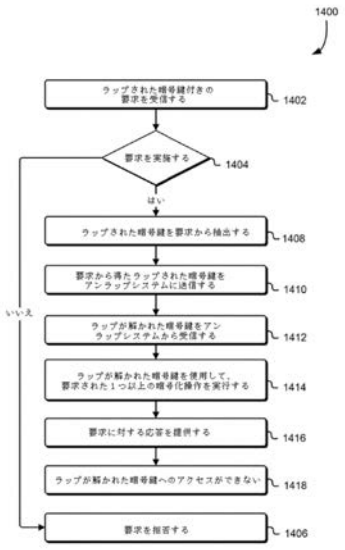
【図１２】



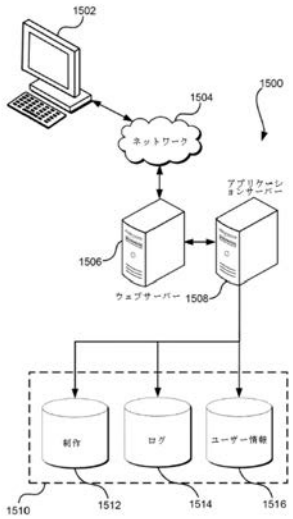
【図１３】



【図１４】



【図１５】


1502
1504
1500
ネットワーク
アプリケーションサーバー
1506
ウェブサーバー
1508
制作
ログ
ユーザー情報
1510
1512
1514
1516

フロントページの続き

(72)発明者　ブランドワイン　エリック　ジェイソン
アメリカ合衆国　９８１０９－５２１０　ワシントン州　シアトル　テリー　アヴェニュー　ノース　４１０

Ｆターム(参考) 5J104 AA16　EA19