(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2020-184800
(P2020-184800A)
(43)公開日　令和2年11月12日(2020.11.12)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 9/32	(2006.01)	H04L 9/00	675B	

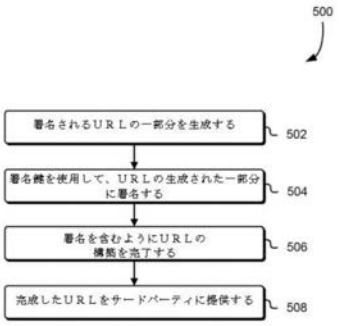
審査請求 有　請求項の数 14　ＯＬ　（全 28 頁）

(21)出願番号　特願2020-126140 (P2020-126140)
(22)出願日　令和2年7月27日 (2020.7.27)
(62)分割の表示　特願2018-78782 (P2018-78782)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　14/037,282
(32)優先日　平成25年9月25日 (2013.9.25)
(33)優先権主張国・地域又は機関
米国 (US)

(71)出願人　506329306
アマゾン　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　９８１０８－１２２６
ワシントン州　シアトル　ピーオー　ボックス　８１２２６
(74)代理人　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
(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

(54)【発明の名称】鍵を有するリソースロケーター

(57)【要約】　（修正有）
【課題】読み出し又は上書きのために時間制限付きでリソースへのアクセスを与えるＵＲＬを生成する方法を提供する。
【解決手段】方法は、データの記憶または取り出しを含む動作を可能とする情報と、ＵＲＬの期限が満了しリソースへのアクセスに使用できない旨を示す有効期限の情報と、リソースへの経路の情報とを含む情報を、ＵＲＬの一部分として構築し、暗号化鍵によってＵＲＬの一部分に署名するための署名を生成し、ＵＲＬの一部分を署名でＵＲＬの署名済部分として構築し、ＵＲＬの他部分をＵＲＬの未署名済部分として構築する。構築されたＵＲＬは、顧客によって供給される暗号化鍵を持つユーザに供給される。
【選択図】図５



【特許請求の範囲】
【請求項１】
読み出し又は上書きのために時間制限付きでリソースへのアクセスを与える、ＵＲＬを生成するコンピュータ実施方法であって、
データの記憶または取り出しを含む動作を可能とする情報と、前記ＵＲＬの期限が満了しリソースへのアクセスに使用できない旨を示す有効期限の情報と、リソースへの経路の情報とを含む情報を、ＵＲＬの一部分として構築することと、
暗号化鍵によって前記ＵＲＬの一部分に署名するための署名を生成することと、
前記ＵＲＬの一部分を前記署名で前記ＵＲＬの署名済部分として構築することと、
前記ＵＲＬの他部分を前記ＵＲＬの未署名済部分として構築することと、
顧客によって供給される暗号化鍵を持つユーザに前記署名済部分及び前記未署名部分を含む前記ＵＲＬを供給することと、を備える、コンピュータ実施方法。

【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、完全な開示である、２０１３年９月２５日に出願された米国特許第１４，０３７，２８２号、名称「ＲＥＳＯＵＲＣＥ　ＬＯＣＡＴＯＲＳ　ＷＩＴＨ　ＫＥＹＳ」、及び２０１３年９月２５日に出願された米国特許出願第１４／０３７，２９２号、名称「ＤＡＴＡ　ＳＥＣＵＲＩＴＹ　ＵＳＩＮＧ　ＲＥＱＵＥＳＴ－ＳＵＰＰＬＩＥＤ　ＫＥＹＳ」を、全ての目的に対して参照により組み込む。
【背景技術】
【０００２】
コンピューティングリソース及び関連付けられるデータのセキュリティは、多くの状況において重要性が高い。一例として、組織は、しばしば、強固な１組のサービスを該組織のユーザに提供するために、コンピューティングデバイスのネットワークを利用する。ネットワークは、しばしば、複数の地理的境界にまたがり、また、しばしば、他のネットワークと接続する。ある組織は、例えば、コンピューティングリソースの内部ネットワーク及び他のものによって管理されるコンピューティングリソースの双方を使用して、その運用をサポートし得る。この組織のコンピュータは、例えば、他の組織のコンピュータと通信して、別の組織のサービスを使用しながらデータにアクセスし得、及び／またはデータを提供し得る。多くの場合において、組織は、他の組織によって管理されるハードウェアを使用して、リモートネットワークを構成及び運用し、それによって、インフラストラクチャコストを削減し、他の利点を達成する。コンピューティングリソースのそのような構成では、特にそのような構成の規模及び複雑さが増大するにつれて、リソース及びリソースが保持するデータへの安全なアクセスを確実にすることが困難になる可能性がある。
【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】
要求を満たす際に使用される暗号化鍵を含むために、要求が予め生成される。要求は、ユニフォームリソースロケータの中に符号化され得、また、要求が提出されるサービスプロバイダが、要求が認可されたかどうかを判定することを可能にするために、認証情報を含み得る。要求は、種々のエンティティに渡され得、次いで、エンティティは、該要求をサービスプロバイダに提出することができる。サービスプロバイダは、要求を受け取ると、認証情報を検証し、要求の中に符号化された暗号化鍵を使用して要求を満たすことがで

きる。
【図面の簡単な説明】
【０００５】
以下、本開示に従う種々の実施形態を、図面を参照して説明する。
【０００６】
【図１】種々の実施形態を実現することができる環境の実例となる実施例を示す図である。
【図２】種々の実施形態を実現することができる環境の実例となる実施例を示す図である。
【図３】少なくとも１つの実施形態に従う、ユニフォームリソースロケーテッド（ＵＲＬ）の実例となる実施例を示す図である。
【図４】少なくとも１つの実施形態に従う、ＵＲＬの別の実施例を示す図である。
【図５】少なくとも１つの実施形態に従う、データへのアクセスを提供するためのプロセスの実例となる実施例を示す図である。
【図６】少なくとも１つの実施形態に従う、ウェブページの実例となる実施例を示す図である。
【図７】少なくとも１つの実施形態に従う、データへのアクセスを取得するためのプロセスの実例となる実施例を示す図である。
【図８】少なくとも１つの実施形態に従う、要求を処理のためのプロセスの実例となる実施例を示す図である。
【図９】少なくとも１つの実施形態に従う、データへのアクセスを要求し、提供するためのプロセスの実例となる実施例を示す図である。
【図１０】種々の実施形態を実現することができる環境を例示する図である。
【発明を実施するための形態】
【０００７】
以下の説明では、種々の実施形態が説明される。説明の目的で、実施形態の完全な理解を提供するために、特定の構成及び詳細が記載される。しかしながら、当業者には、実施形態が具体的な詳細を伴わずに実践され得ることも明らかになるであろう。さらに、よく知られている特徴は、説明されている実施形態を不明瞭にしないために、省略または簡略化され得る。
【０００８】
本明細書で説明され、提案される技法は、サービスプロバイダのサービスにアクセスすることを可能にするための、ユニフォームリソースロケータ（ＵＲＬ）の使用、及びコンピューティングリソース（全般的に「リソースロケーター」）への他の参照を含む。ＵＲＬは、例示の目的で本開示の全体を通して使用されるが、本明細書で説明される技法は、全般的に、他のリソースロケーター（すなわち、システム内のコンピューティングリソースの場所を特定するために、システムによって使用できる情報のインスタンス）に適用することができることを理解されたい。さらに、本明細書で説明される技法は、全般的に、電子的な要求に適用することができる。
【０００９】
一実施形態において、サービスプロバイダ（例えば、コンピューティングリソースサービスプロバイダ）の顧客は、サービスプロバイダの１つまたは複数のサービスを利用する。一例として、顧客は、設備投資の削減、より簡単なデータ管理、より高い可用性、分散させたデータ処理設備によるより少ない待ち時間、及び同類のもの等の、種々の利点を達成するために、サービスプロバイダのデータ記憶サービスを利用し得る。他の人（例えば、顧客の顧客、または全般的に、顧客によって認可されたユーザ）が、プロバイダによって管理される顧客のリソースにアクセスすることを可能にするために、顧客は、予め署名したＵＲＬを利用し得る。予め署名したＵＲＬを生成するために、顧客は、ＵＲＬ（または全般的に、要求）及び該ＵＲＬの一部分の電子（デジタル）署名を生成し得る。電子署名を生成するために使用されるＵＲＬの一部分は、要求を処理する際に使用される暗号化

鍵を含み得る。暗号化鍵は、種々の形態で提供され得る。例えば、暗号化鍵は、サービスプロバイダが要求を満たすためにその鍵を使用して１つまたは複数の暗号化動作を行って解読することができる、または解読した方法で解読される、プレーンテキスト対称鍵、公開鍵－秘密鍵対のうちのプレーンテキスト公開鍵、または対称鍵であり得る。

【００１０】

全般的に、ＵＲＬは、要求、暗号化鍵、及び要求を検証するために使用できる認証情報（例えば、電子署名）を含み得る認可情報を符号化するように構成され得る。ＵＲＬは、顧客から別のエンティティに提供され得、このエンティティは、必ずしもサードパーティではなく、本開示ではサードパーティと称されるが、サービスプロバイダに要求を満たさせるために顧客によって認可される任意のエンティティとすることができる。ＵＲＬは、種々の方法でサードパーティに提供され得る。例えば、いくつかの実施形態において、ＵＲＬは、サードパーティへのネットワークを通じて伝送されるコンテンツのウェブページまたは他の組織に提供される。ＵＲＬを提供することは、サードパーティからの有効なログイン信用証明書の受け取り、サードパーティからの支払いの受け取りもしくは支払いの約束、及び／または他の条件等の、１つまたは複数の条件が課され得る。

【００１１】

サードパーティは、サービスプロバイダに要求を満たさせるために、要求をサービスプロバイダに提出し得る。要求を提出する前に、サードパーティは、操作されるデータ、及び／または要求をどのように処理するのかをサービスプロバイダに示す１つまたは複数のパラメータの１つまたは複数の値等の、追加的な情報を要求に加え得る。例えば、パラメータは、サービスプロバイダが使用する能力とともに構成される複数の暗号化スキーム／モードから、使用する暗号化スキーム及び／または暗号化スキームのモードの選択を指定し得る。

【００１２】

要求を受け取ると、サービスプロバイダは、要求を満たすかどうかを判定するために、電子署名の有効性を確認し得る。他の動作は、要求を満たすことが、任煮の適用可能なポリシーを遵守するかどうか、及び／または要求に符号化される（例えば、認可情報の一部として符号化される）１つまたは複数のパラメータ（例えば、有効期限）を遵守するかどうかを判定する等の、要求を満たすかどうかを判定する際に行われ得る。サービスプロバイダが満たすことができるとみなされる要求の場合、サービスプロバイダは、該要求から暗号化鍵を抽出し、（該当する場合は）抽出した暗号化鍵を解読し、そして、要求を満たす際に関与する１つまたは複数の動作を行い得る。要求が満たされたという肯定応答、及び／または１つまたは複数の動作を行った結果（例えば、要求の中に提供された鍵を使用して解読したデータ）等の、顧客に対する応答が提供され得る。

【００１３】

図１は、種々の実施形態を実現することができる環境１００の実例となる実施例を示す。図１で例示されるように、環境１００は、顧客１０２を含み、また、サービスプロバイダ１０４である。サービスプロバイダ１０４の顧客１０２は、サービスプロバイダ１０４によって提供される種々のコンピューティングリソースを利用するために、サービスプロバイダの種々のサービスを利用し得る。例えば、顧客１０２は、自分でコンピューティングリソースを実現することの出費及び／または複雑な問題を回避するために、顧客自身のサービスを動作させ、サービスプロバイダ１０４のコンピューティングリソースを利用し得る。一例として、顧客１０２は、他の顧客に対するサービスとして、ビデオファイル及び／またはオーディオファイル等のメディアファイルへのアクセスを提供し得る。しかしながら、十分に強固な記憶システムを維持することの出費及びトラブルを回避するために、顧客１０２は、サービスプロバイダ１０４のデータ記憶システムを利用し得、該サービスプロバイダは、データ記憶システムへのアクセスを、顧客１０２等の多数の顧客に提供し得る。

【００１４】

上で述べられるように、顧客１０２は、顧客自身の１人または複数の顧客を有し得、故

に、本開示の種々の技法は、サービスプロバイダ１０４によって記憶されたデータのプロキシとしての役割を果たすことを必要とせずに、顧客１０２が、サービスプロバイダ１０４のサービスを利用するその顧客にサービスを提供することを可能にすることに関する。これを行うための１つの方法は、図１で例示されるように、ＵＲＬ１０６をサードパーティ１０８に提供する顧客１０２を含み、該サードパーティは、顧客１０２の顧客であり得るか、または全般的に、顧客１０２のサービスのユーザである。下でさらに詳細に述べられるように、ＵＲＬ１０６は、顧客１０２からサードパーティ１０８に種々の方法で提供され得る。

【００１５】

下でさらに詳細に論じられるように、ＵＲＬ１０６をサードパーティ１０８に提供する１つの方法は、サードパーティ１０８の人間のオペレータによって選択できるようにＵＲＬを符号化するウェブページまたは他のインターフェースの使用によるものであり得る。実例となる実施例として、顧客１０２を伴うアカウントを有する人間のオペレータは、顧客１０２のウェブサイトにログインし得、そして、ログインした結果として、ＵＲＬ１０６へのアクセスを有し得る。ＵＲＬ１０６は、顧客１０２からサードパーティ１０８に他の方法でも同様に提供され得る。例えば、ＵＲＬ１０６は、顧客１０２からサードパーティ１０８への電子メールメッセージまたは他のメッセージに符合化され得る。別の実施例として、ＵＲＬ１０６は、顧客１０２からサードパーティ１０８に任意の好適な方法で提供される文書に符合化され得る。全般的に、サードパーティ１０８がＵＲＬ１０６へのアクセスを有する任意の方法は、アクセスを提供することがＵＲＬ１０６のネットワークを通じたサードパーティ１０８への伝送を含むかどうかにかかわらず、本開示の範囲内にあるとみなされる。

【００１６】

図１は、顧客１０２と、組織及び／または個人等のエンティティであり得るサードパーティ１０８との間での情報の流れを例示していることに留意されたい。データがエンティティ間で流れているように示されているが、別途文脈から明らかでない限り、データは、それぞれのエンティティの適切なコンピューティングデバイスによって転送されることを理解するべきであり、その実施例は、図１０と関連して下で説明される。一実施例として、ＵＲＬ１０６は、顧客１０２から、顧客１０２のウェブまたは他のサーバから提供され得る。同様に、サードパーティ１０８の人間のオペレータは、パーソナルコンピュータ、モバイルデバイス、タブレットコンピューティングデバイス、電子ブックリーダー、または全般的に、ネットワークもしくは他のデータ受信インターフェースを通して情報を受け取るように構成される任意のデバイス等の、適切なデバイスによってＵＲＬ１０６を受け取り得る。

【００１７】

また、図１は、ＵＲＬ１０６が顧客１０２からサードパーティ１０８に直接提供されているように示されているが、ＵＲＬ１０６は、種々の実施形態に従って、種々の方法で提供され得ることにも留意されたい。上で述べられるように、例えば、顧客１０２のサーバは、顧客１０８に提供されるウェブページに符号化する等で、ＵＲＬ１０６をサードパーティ１０８に提供し得る。しかしながら、そのようなサーバは、コンピューティングリソース、例えばサービスプロバイダ１０４によってホストされる仮想コンピュータシステム及び／または１つまたは複数の記憶デバイスを使用して実現され得る。換言すれば、顧客１０２は、ＵＲＬ１０６をサードパーティ１０８に提供することを制御し得るが、ＵＲＬ１０６がサードパーティ１０８に提供されるリソースは、顧客１０２によって直接ホストされない場合がある。加えて、ＵＲＬ１０６は、図１で例示されない１つまたは複数の中間物を通過し得る。他の変形例も本開示の範囲内にあるとみなされる。

【００１８】

述べられるように、サードパーティ１０８は、ＵＲＬ１０６を受け取ると、ＵＲＬ１０６を使用して、サービスプロバイダ１０４のサービスにアクセスすることができる。本開示の全体を通して使用される一実施例として、サードパーティ１０８は、ＵＲＬ１０６を

使用して、顧客１０２に代わってサービスプロバイダ１０４によって記憶されたデータにアクセスすることができる。換言すれば、サービスプロバイダ１０４の顧客１０２は、ＵＲＬ１０６を使用して、サードパーティ１０８が、サービスプロバイダ１０４によってポストされたメディアファイル等の、１つまたは複数のコンピューティングリソースへのアクセスを取得することを可能にすることができる。本開示の全体を通して、実例となる実施例として、データへのアクセス（例えば、データの取り出し）が使用されているが、本明細書で説明される技法は、サービスへのアクセスを多数の方法で提供するために使用できることに留意されたい。例えば、ＵＲＬ１０６は、サードパーティ１０８がサービスプロバイダ１０４のリソースを使用してデータを記憶することを可能にするために使用され得る。そのような使用は、例えば、顧客１０２が提供するサービスの一部として、データを記憶する能力をサードパーティに提供する場合に有用であり得る。全般的に、ＵＲＬ１０６は、サービスプロバイダ１０４によって満たすことができる要求に従う任意の方法でアクセスを提供するために使用され得る。

【００１９】

例示される実施形態に戻ると、サービスプロバイダ１０４によってホストされるリソースへのアクセスを獲得するために、サードパーティ１０８は、ＵＲＬをサービスプロバイダ１０４に提供し得る。サービスプロバイダ１０４が、ＵＲＬ１０６を使用してサードパーティ１０８によってサービスプロバイダ１０４に提出された要求をどのように満たすか、及び／または要求を満たすかどうかを判定することを可能にするために、種々の情報がＵＲＬに含まれ得る。例えば、図１で例示されるように、ＵＲＬ１０６は、電子署名１１０を含み、該電子署名は、顧客１０２に対応する署名検証鍵１１２へのアクセスを有することによって、サービスプロバイダ１０４によって検証することができる。署名検証鍵１１２は、例えば、顧客１０２もアクセスを有する対称暗号化鍵であり得る。そのような実施形態において、サービスプロバイダ１０４は、サードパーティ１０８がＵＲＬ１０６を使用して要求を提出することを顧客１０２によって認可されたと判定するために、１つまたは複数の対称暗号化署名検証アルゴリズムを使用して、電子署名１１０を検証することができる。別の実施例として、署名検証鍵１１２は、公開鍵－秘密鍵対のうちの公開鍵とすることができ、ここで、顧客１０２は、公開鍵－秘密鍵対のうちの秘密鍵へのアクセスを有する。顧客１０２は、秘密鍵を使用して電子署名１１０を生成し得、該秘密鍵は、次いで、サードパーティ１０８から署名１１０を受け取った時点で、サービスプロバイダ１０４によって検証され得る。全般的に、ＵＲＬ１０６に含まれる任意のタイプの情報が使用され得、該情報は、サービスプロバイダ１０４が、ＵＲＬ１０６を使用して提出された顧客１０８からの要求が顧客１０２によって認可されたと判定することを可能にする。

【００２０】

図１で例示されるように、ＵＲＬ１０６はまた、暗号化鍵１１４も含み得る。暗号化鍵１１４は、顧客１０２がアクセスを有する暗号化鍵であり得る。ＵＲＬ１０６に含まれる暗号化鍵のタイプは、種々の実施形態に従って変化し得る。いくつかの実施形態において、例えば、暗号化鍵１１４は、サービスプロバイダ１０４によって暗号化または暗号解読に使用される対称鍵である。別の実施例として、暗号化鍵１１４は、公開鍵－秘密鍵対のうちの公開鍵であり得、秘密鍵は、顧客１０２によって保持されるが、サービスプロバイダ１０４によるアクセスは存在しない。さらに別の実施例として、暗号化鍵１１４は、ＵＲＬに含まれ得、別の鍵の下で暗号化される形態で対称鍵がＵＲＬ１０６に含まれ得、ここで、他の鍵は、種々の実施形態に従って変化し得るが、全般的に、サードパーティ１０８からＵＲＬ１０６を受け取った時点で、サービスプロバイダ１０４がそれ自体で、または別のサービス、例えば別のサードパーティのサービスを使用して、暗号化鍵１１４を使用するために解読することができるような鍵である。全般的に、サードパーティ１０８がＵＲＬ１０６をサービスプロバイダ１０４に提供することを可能にして、サービスプロバイダ１０４が１つまたは複数の動作のために暗号化鍵１１４を使用することを可能にするために、暗号化鍵１１４がＵＲＬ１０６でサードパーティ１０８に提供され得る、任意の方法が使用され得る。このように、サードパーティ１０８は、顧客１０２によって提供さ

れる暗号化鍵１１４を使用して、サービスプロバイダ１０４のサービスを利用することができる。

【００２１】

これが有用である１つの方法の実例となる実施例として、顧客１０２は、サービスプロバイダ１０４のデータ記憶サービスを利用してデータを記憶し得、ここで、データは、サービスプロバイダ１０４がアクセスできない鍵を使用した暗号化された形態で記憶される。暗号化鍵１１４をサードパーティ１０８へのＵＲＬ１０６に含めることによって、サードパーティ１０８は、サービスプロバイダ１０４が、暗号化鍵１１４を使用して、顧客１０２によってデータ記憶サービスに記憶したデータを解読することを可能にするために、ＵＲＬ１０６を使用して要求をサービスプロバイダ１０４に提出することができる。したがって、サービスプロバイダ１０４がＵＲＬ１０６を提供するまで、サービスプロバイダ１０４は、プレーンテキストの形態の顧客１０２のデータにアクセスする能力を有しない。サードパーティ１０８は、種々の方法でＵＲＬ１０６を使用して要求をサービスプロバイダ１０４に提出し得ることに留意されたい。例えば、サードパーティ１０８のアプリケーションは、グラフィカルユーザインターフェース上の選択可能なユーザインターフェース要素の一部として、ＵＲＬを提供し得る。選択可能な要素を選択すると、要求を提出するべきインターネットプロトコル（ＩＰ）アドレスを決定するために、サードパーティのブラウザ等のアプリケーションが、ドメインネームサービス（ＤＮＳ）に接触し得る。次いで、要求がＩＰアドレスに提出され得、ここで、この要求は、ＵＲＬ１０６を含み得る。次いで、ＵＲＬ１０６の中の情報が、サービスプロバイダ１０４がそれに応じて要求を処理することを可能にし得る。

【００２２】

図２は、種々の実施形態に従う、サービスプロバイダ２００の環境の実例となる実施例を示す。図２で例示されるように、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り得、該サブシステムは、図１と関連して上で説明されるように、顧客からの要求の提出をサービスプロバイダ２００によって処理することを可能にする。故に、顧客インターフェースは、顧客が要求をサービスプロバイダ２００に提出する能力を提供するための、適切なコンピューティングデバイスを含み得る。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通じて要求を受け取るように構成される、１つまたは複数のウェブサーバを含み得る。そのように例示されていないが、顧客インターフェース２０２がサービスプロバイダ２００の顧客に対して適切に動作することを可能にする適切なネットワーキング装置等の、他のインフラストラクチャも顧客インターフェース２０２に含まれ得る。

【００２３】

顧客インターフェース２０２を通して要求を受け取るときに、該要求は、適切な認証情報とともに受け取られ得る。例えば、図２で例示されるように、要求は、ＵＲＬの一部分の署名２０６を含むＵＲＬ２０４とともに受け取られ得る。署名は、種々の実施形態に従って生成され得る。例えば、ＵＲＬ２０４を生成した顧客は、顧客とサービスプロバイダ２００との間で共有される秘密情報を使用して署名２０６を生成し得る。別の実施例として、顧客は、秘密鍵－公開鍵対のうちの秘密鍵を使用してＵＲＬ２０４に署名するために、非対称のデジタル署名スキームを使用している場合がある。全般的に、ＵＲＬ２０４を認証するために使用される任意のタイプの情報が使用され得、いくつかの実施形態では、要求は、そのような情報を伴わずに提出され得る。

【００２４】

しかしながら、図２で例示されるように、顧客インターフェース２０２を通して要求を受け取るときには、要求のＵＲＬ２０４が、（例えば、サービスプロバイダ２００の内部ネットワークを通じて）署名２０６ととも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。代替的に、ＵＲＬの全部の代わりに、電子署名２０６を生成するのに十分なＵＲＬの一部分が提供され得る。認証システム２０８は、要求とともに含まれるＵ

ＲＬとともに提供される電子署名を検証することなどによって要求を認証するように構成される、サービスプロバイダ２００のサブシステムであり得る。ＵＲＬ２０４の署名２０６を検証すると、認証システム２０８は、署名２０６が有効であるかどうかを示す応答を顧客インターフェース２０２に提供し得る。顧客インターフェース２０２のデバイス（例えば、ウェブサーバ）は、ＵＲＬ２０４をどのように処理するのかを決定するために、認証システム２０８によって提供される情報を使用し得る。例えば、認証システム２０８が、署名２０６が無効であることを示した場合、顧客インターフェース２０２は、要求を拒否し得る。同様に、認証システム２０８からの情報が、ＵＲＬ２０４の署名２０６が有効であることを示した場合、顧客インターフェース２０２は、要求を処理させ得る。

【００２５】

図で例示されていないが、サービスプロバイダ２００内で、もしくはそれに代わって動作する認証システム２０８または別のシステムは、要求をどのように処理するのかを決定することと関連して他の動作を行うように動作し得る。例えば、要求を満たすことができるかどうかを判定し得る１つまたは複数のポリシーを確認するために、認証システム２０８またはそれと協働して動作する別のシステムが使用され得る。ポリシーの判定は、要求を提出した要求側の識別情報、時刻、データが記憶されるまたは記憶されるべき場所の論理的識別子、及び他のコンテキスト情報等の、種々の要因に少なくとも部分的に基づいて行われ得る。ポリシーは、顧客インターフェース２０２を通して、または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フェース（ＡＰＩ）コールによる別のインターフェースを通して管理され得る。

【００２６】

図２で例示される実施形態に戻ると、認証システム２０８が、署名２０６が有効であると判定した場合、顧客インターフェース２０２は、要求を処理すると判定し得る。要求を処理することは、顧客インターフェース２０２と要求処理インフラストラクチャ２１２との間で、暗号化されたデータ２１０を転送することを含み得る。要求処理インフラストラクチャ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つまたは複数のデバイスを備え得る。例えば、図２で例示されるように、要求処理インフラストラクチャは、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ために使用される、複数のデータ記憶システム２１４を備え得る。また、例示されていないが、ネットワークインフラストラクチャを含む他のインフラストラクチャも含まれ得る。例えば顧客インターフェース２０２と要求処理インフラストラクチャ２１２との間のネットワークを通じた、データの移動は、顧客インターフェース２０２を通して提出され得る種々のタイプの要求に従って、種々の実施形態に従う種々の方法で起こり得る。例えば、データを記憶する要求にＵＲＬ２０４が含まれる場合、顧客インターフェースは、ＵＲＬ２０４に提供される鍵２１６を利用して、データ記憶システム２１４のうちの１つまたは複数に記憶するために、データを暗号化し、暗号化したデータ２１０を要求処理インフラストラクチャ２１２に伝送し得る。

【００２７】

同様に、要求が、データを取り出す要求である場合、顧客インターフェース２０２は、データ記憶システム２１４のうちの１つまたは複数からのデータを顧客インターフェース２０２に提供することを可能にする通信を、要求処理インフラストラクチャ２１２に伝送し得る。次いで、顧客インターフェース２０２は、ＵＲＬ２０４に提供される鍵２１６を使用して、暗号化されたデータ２１０を解読し、解読したデータを、要求を提出した顧客に提供し得る。図２で例示されるサービスプロバイダ２００の環境は、例示の目的で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の使用を記録するアカウンティングシステム等の、多数の他のデバイス及びサブシステムも含まれ得ることに留意されたい。さらに、サービスプロバイダ２００は、重複性及び／または可用性の目的で、異なる地理的な場所に位置する設備を含み得る。

【００２８】

図３は、種々の実施形態に従う、ＵＲＬ３００の実例となる実施例を示す。一実施形態

において、上で述べられるように、ＵＲＬ３００は、ＵＲＬ３００の一部分の電子署名３０２と、暗号化鍵３０４とを含み得る。ＵＲＬ３００はまた、経路３０６等の他の情報も含み得る。経路３０６は、上で説明されるようなサービスプロバイダが、ＵＲＬ３００を介して提出される要求と関連付けられる１つまたは複数のリソースの場所を特定することを可能にする情報を含み得る。ＵＲＬ３００の他の情報としては、要求を満たすことによって行われる１つまたは複数の動作３０８を示す情報が挙げられ得る。指定され得る例示的な動作としては、データの記憶、データの取り出し、データのデジタル署名の生成、及び他の動作が挙げられるが、それらに限定されない。いくつかの実施形態において、ＵＲＬは、複数の動作、及び動作が行われるべき順序を指定し得る。

【００２９】

例示されるように、ＵＲＬ３００は、有効期限３１０を含む。有効期限は、満たすことができる要求をサービスプロバイダに提出するためにＵＲＬ３００を使用することができなくなるまでの時間にわたって、値を符号化し得る。換言すれば、有効期限は、そうでなければＵＲＬを使用して提出された満たすことができる要求が、時間に到達したために満たすことができなくなるまでの時間を示す。一実施例として、図１を参照すると、ある特定のデータへの一時的なアクセスの提供を望む顧客１０２は、ＵＲＬ１０６がサードパート１０８に対して使用することができる時間の量を制限するために、ＵＲＬ１０６の有効期限３１０を利用し得る。有効期限３１０が顧客によって発行されてから修正されていないときにだけ署名３０２が有効であることを確実にするために、有効期限３１０は、電子署名３０２を生成するために使用されるＵＲＬ３００のデータに含まれ得る。このようにして、有効期限を過ぎた後のＵＲＬへのアクセスは、単に有効期限を修正することによってデータにアクセスする能力を提供しない。要求を満たすかどうかを判定するときにＵＲＬ３００を受け取るサービスプロバイダは、有効期限及び／または他の情報を利用して、要求を満たすかどうかを判定し得る。例えば、有効期限３１０の前にＵＲＬが要求を提供した場合、サービスプロバイダは、要求を満たし得る（要求を満たすための全ての他の要件が、該当する場合は、満たされていると仮定する）。同様に、有効期限３１０を過ぎた後にＵＲＬ３００が要求とともにサービスプロバイダに提供された場合、サービスプロバイダは、要求を満たすための任意の他の要件が満たされているとしても拒否し得る。有効期限は、プロバイダが要求を満たすかどうかを潜在的に判定するパラメータとして、本開示の全体を通して使用されるが、要求を満たす基準は、より複雑になり得ることに留意されたい。例えば、要求を満たす基準は、終了時間を過ぎたとしても要求を満たすことができるように構成され得る。他のコンテキスト情報（例えば、要求側の識別情報）は、例えば、有効期限に優先し得る。

【００３０】

例示されるように、ＵＲＬ３００はまた、他のパラメータ３１２も含み得る。他のパラメータは、サービスプロバイダが要求を満たすかどうか、及び／またはどのように満たすのかを判定することを可能にするパラメータであり得る。例えば、上で述べられるように、ＵＲＬ３００は、有効期限３１０を含み得る。他のパラメータ３１２に含まれる別のパラメータは、ＵＲＬ３００が要求をサービスプロバイダに提出するために使用できるようになる時間を示す、開始時間であり得る。開始時間と終了時間との組み合わせは、ＵＲＬを使用して提出された要求を満たすことができる時間ウィンドウを提供し得る。開始時間は、例えば、ある特定の時間（例えば、メディアファイルの発行）まで、データへのアクセスを阻止する場合に有用である。したがって、サービスプロバイダの顧客は、データへのアクセスを提供する、または別様には満たすことができる要求をサービスプロバイダに後で提出するために使用できる、１つまたは複数のＵＲＬを予め生成することができる。将来にデータへのアクセスを可能にするＵＲＬを予め生成するそのような能力は、そのようなアクセスを与えることが所望されるまである特定のデータへのアクセスを提供することなく、コンテンツ配信ネットワーク（ＣＤＮ）を予め用意する、及び／またはＵＲＬを伴うコンテンツを予め構成する等の、技術的利点を提供する。

【００３１】

図１を参照すると、図３で例示されるＵＲＬの他のパラメータは、暗号化鍵３０４（または図１を参照するときには１１４）を使用して１つまたは複数の暗号化動作が行われるデータ、要求を満たすことをどのように行うかに関するパラメータ、が挙げられるが、それらに限定されない、サードパーティによって加えられる他の情報を含み得る。

【００３２】

図４は、上で論じられるＵＲＬ３００または全般的に本明細書で説明される任意のＵＲＬであり得る、ＵＲＬ４００の実例となる実施例を示す。例示されるように、ＵＲＬ４００は、署名済部分４０２と未署名部分４０４とを含む。署名済部分は、その修正がＵＲＬ４００を無効にさせることができる情報を含み得る。一実施例として上で論じられるように、署名済部分４０２は、有効期限４０６を含み得る。加えて、署名済部分は、暗号化鍵４０８を含み得る。全般的に、署名済部分は、ＵＲＬ４００を提供する顧客が任意の情報の偽造を阻止することを意図する、そのような情報を含み得る。情報としては、例えば、ＵＲＬ４００の提出を認可された識別情報、ＵＲＬ４００をいつ使用できるのかに関するタイミング情報（例えば、１つまたは複数の開始時間及び／または終了時間）、及びＵＲＬ４００を使用して提出された要求を処理するべきかどうか、及び／またはどのように処理するべきかを判定する他のコンテキスト情報を挙げることができる。ＵＲＬ４００の未署名部分は、上で説明されるような電子署名４１０、暗号化鍵４０８を使用して１つまたは複数の暗号化動作が行われるサードパーティによって加えられたデータであり得る追加的な要求データ４１２、及び／または全般的に、サードパーティが電子署名４１０の無効性を生じさせることなく変更することができる情報等の、種々の情報を含み得る。

【００３３】

ＵＲＬ４００は、本開示の種々の態様を例示するために、特定の方法で例示される。多数の変形例が本開示の範囲内にあるとみなされる。例えば、図４で例示されるように、ＵＲＬ４００は、ＵＲＬ４００の署名済部分の中の暗号化鍵を示す。ＵＲＬ４００の署名済部分の中の暗号化鍵に加えて、またはそれに代わるものとして、ＵＲＬの未署名部分は、暗号化鍵を備え得る。例えば、いくつかの実施形態において、サービスプロバイダの顧客は、署名済部分を有するＵＲＬをサードパーティに提供し得る。サードパーティは、暗号化鍵をＵＲＬに加え得、追加的な暗号化鍵を有するＵＲＬを使用して、要求をサービスプロバイダに提出し得、ここで、要求を満たすことは、ＵＲＬの署名済部分に少なくとも部分的に基づいて生成される署名を介して、顧客によって認可される。このようにして、サードパーティは、暗号化鍵へのアクセスをサービスプロバイダ（要求を満たすことの一部として１つまたは複数の暗号化動作を行うときを除く）、または顧客のいずれにも提供することなく、サービスプロバイダの１つまたは複数のサービスを利用し得る。したがって、顧客またはサービスプロバイダのいずれかでのセキュリティ違反または他のイベントは、暗号化鍵へのアクセスを提供せず、その結果、プレーンテキストの形態のデータへのアクセスを可能にしない。さらに、暗号化動作は、ＵＲＬの署名済部分の中の鍵（顧客によって供給される）、及びＵＲＬの未署名部分の中の鍵（サードパーティによって供給される）の双方を使用して行われ得る。このようにして、プレーンテキストの形態のデータへのアクセスには、サードパーティ及び顧客の双方の間の協働が必要とされる。また、サービスプロバイダの鍵が代替として、または加えて使用される変形例を含む、他の変形例も本開示の範囲内にあるとみなされる。

【００３４】

図５は、種々の実施形態に従う、データへのアクセスを提供するためのプロセス５００の実例となる実施例を示す。プロセス５００は、図１と関連して上で説明されるような、顧客によって操作されるシステム等の、任意の適切なシステムによって行われ得る。一実施形態において、プロセス５００は、５０２で、署名されるＵＲＬの一部分を生成することを含む。ＵＲＬの一部分は、プロセス５００を行うエンティティが偽造の阻止を所望する情報を含み得る。種々の実施形態において、署名されるＵＲＬの一部分に含まれる情報の量は、変動し得る。例えば、署名されるＵＲＬの一部分は、顧客のリソースへの経路、暗号化鍵、サービスプロバイダによって要求を満たすことを可能にするためにＵＲＬをい

つ及び／またはどのように使用することができるのかを定義する１つまたは複数のコンテキストパラメータ、及び／または他の情報を含み得る。

【００３５】

５０２で、署名されるＵＲＬの一部分が生成されると、プロセス５００は、５０４で、生成されたＵＲＬの一部分に署名するために、署名鍵を使用することを含み得る。署名鍵は、任意の暗号化鍵であり得、該暗号化鍵は、電子署名を生成するために使用されたときに、ＵＲＬを提出することができるサービスプロバイダによって検証できる電子証明を提供する。例えば、いくつかの実施形態において、署名鍵は、プロセス５００を行うエンティティとサービスプロバイダとの間で共有される秘密情報であり得る。他の実施形態において、署名鍵は、公開鍵－秘密鍵対のうちの秘密鍵であり得、ここで、サービスプロバイダは、公開鍵－秘密鍵対のうちの公開鍵（及び、場合により、認可機関）を利用して、電子署名を検証することができる。図５は、暗号化鍵を含む署名されるＵＲＬの一部分を示しているが、いくつかの実施形態は、署名されるＵＲＬの一部分以外に含まれる署名鍵を有し得ることに留意されたい。暗号化鍵のそのような包含は、例えば、鍵の偽造が問題にならない場合に使用され得る。例えば、データ記憶装置からのデータにアクセスするためにＵＲＬを使用できる場合、修正された暗号鍵は、全般的に、データを解読するために使用できず、その結果、鍵の修正に対して保護することが必要になり得ない。

【００３６】

ＵＲＬの生成された一部分の電子署名を生成するために署名鍵を使用すると、プロセス５００は、５０６で、電子署名を含むようにＵＲＬの構築を完成することを含み得る。論じられるように、５０６ではまた、ＵＲＬの構築を完成するために、ＵＲＬの追加的なパラメータ等の他の情報も使用され得る。５０６で完成すると、プロセス５００は、５０８で、完成したＵＲＬをサードパーティに提供することを含み得る。サードパーティは、例えば、上で説明されるようなプロセス５００を行うエンティティの顧客であり得る。５０８で、完成したＵＲＬをサードパーティに提供することは、種々の実施形態に従う、種々の方法で行われ得る。例えば、下でさらに詳細に論じられるように、ＵＲＬは、ウェブページにおいてサードパーティに提供され得、ここで、ウェブページが提供される前に、ウェブページにアクセスするための１つまたは複数の要件が必要とされ得る。実例となる実施例のように、サードパーティは、完成したＵＲＬを有するウェブページにアクセスするために、ログイン／サインインプロシージャを行うことが必要とされ得る。全般的に、ＵＲＬは、電子メッセージ等の任意の方法で、または一方のシステムからもう一方にデータが渡され得る任意の方法で提供され得る。さらに、サードパーティは、例示の目的で使用されているが、ＵＲＬが提供されるエンティティは、必ずしもプロバイダまたは顧客に対するサードパーティではないことに留意されたい。例えば、プロセス５００が組織のシステムによって行われる一実施形態において、本明細書で説明される技法は、データへのアクセスを組織の職員に提供するために使用され得る。したがって、サードパーティの代わりに、ＵＲＬは、プロセス５００が行われる組織内のユーザに提供され得る。他の変形例も本開示の範囲内にあるとみなされる。

【００３７】

図６は、種々の実施形態に従う、ＵＲＬを提供するために使用され得るウェブページ６００の実例となる実施例である。図６で例示されるように、ウェブページ６００は、種々のコンテンツを含む。ウェブページ６００で例示されるコンテンツは、本質的に実例であり、コンテンツのタイプ及び外観、ならびにその量は、種々の実施形態に従って変動し得る。ウェブページ６００は、種々の実施形態に従って種々の方法で提供され得る。例えば、ウェブページは、図１と関連して上で説明されるサードパーティ等のクライアントのブラウザアプリケーション等のアプリケーションに、ネットワークを通じて提供され得る。しかしながら、ウェブページ６００は、全般的に、ウェブページを受け取り、処理することができる任意の適切なデバイスによって提供され得る。ウェブページ６００は、例示の目的で使用されているが、本明細書で説明される種々の実施形態に従って構成されるＵＲＬまたは他のリソースロケーターは、種々の実施形態に従って種々の方法でコンテンツに

提供され得る。例えば、コンテンツは、必ずしもブラウザアプリケーションに分類されない、モバイルアプリケーションまたは他のアプリケーションに提供され得る。全般的に、ＵＲＬまたは他のリソースロケーターが提供され得るあらゆる方法が、本開示の範囲内にあるとみなされる。

【００３８】

図６で例示されるように、ウェブページ６００は、ウェブページ６００が一部であるウェブサイトの全体を通してのナビゲーションを可能にする、種々のグラフィックユーザインターフェース要素を含む。本実施例において、ウェブページ６００は、ストリーミングビデオコンテンツを１人または複数の顧客に提供すること等によってアクセスをビデオコンテンツに提供する、電子商取引ウェブサイトの一部である。例えば、ウェブページ６００の左側には、種々のビデオジャンルへの種々のリンク６０２が提供される。本実施例において、リンクは、テキストワードとして現れ、該テキストワードは、キーボード、マウス、タッチスクリーン、または他の入力デバイス等の適切な入力デバイスを使用してリンクを選択することを可能にする。リンクの選択は、ウェブページ６００を表示させるアプリケーションに、ウェブページ６００のプログラミングによってリンクと関連付けられるＵＲＬに従って、ｈｔｔｐ要求を、ウェブページ６００を提供したサーバまたは別のサーバに提出させ得る。本実施例において、ウェブページ６００はまた、再生ボタン６０４として構成されるグラフィカルユーザ要素も含む。再生ボタン６０４は、ウェブページ６００のグラフィカルユーザインターフェース要素であり得、ここで、ウェブページ６００の下層のコードは、ボタン６０４の入力デバイスによる選択が、要求を適切なサーバに提出させるように構成される。

【００３９】

本実施例において、ウェブページ６００のコードは、本明細書で説明される種々の技法に従って構成され得るＵＲＬ６０６を含む。この実例となる実施例において、ＵＲＬ６０６は、この場合ではビデオファイルであるリソースへの経路６０８を含む。ＵＲＬ６０６はまた、暗号化鍵６１０、有効期限６１２、及び電子署名６１４も含み得る。電子署名は、経路６０８、暗号化鍵６１０、及び有効期限６１２、及び／または他の情報に対して少なくとも部分的に生成され得る。全般的に、ＵＲＬ６０６は、図に例示されない追加的な情報を含み得る。故に、ユーザがボタン６０４を選択すると、適切に構成された要求、本実施例ではｈｔｔｐ要求が、ＵＲＬ６０６を使用してサーバに提出される。図で例示されていないが、そのような要求は、ドメインネームサービス（ＤＮＳ）からサーバのＩＰアドレスを取得するためにＵＲＬ６０６の経路６０８を使用し、そして、ＵＲＬ６０６を有する要求をインターネットまたは他のネットワークを通じてＩＰアドレスに提出することによって提出され得る。

【００４０】

ウェブページ６００を処理するデバイスは、応答を受け取り得、該応答は、要求の提出時にＵＲＬ６０６が有効である場合に、経路６０８が指すリソースを含み得る。本明細書のどこかで述べられるように、例えばＵＲＬ６０６が有効期限６１２を過ぎて提出されたため、またはＵＲＬ６０６が修正されたため該ＵＲＬが無効であった場合、そのような要求は拒否され得る。

【００４１】

図７は、種々の実施形態に従う、データにアクセスするためのプロセス７００の実例となる実施例を示す。プロセス７００は、図１と関連して上で説明されるサードパーティのシステム等の、任意の適切なシステムによって行われ得るが、述べられるように、プロセス７００を行うシステムは、必ずしもプロセス７００によって行うことに関与する他のエンティティ対するサードパーティとは限らない。一実施形態において、プロセス７００は、７０２で、プロバイダの顧客からＵＲＬを取得することを含む。７０２で、上で説明されるようにウェブページを通す、または別の方法等で、種々の実施形態に従って種々の方法でＵＲＬが取得され得る。７０２で取得すると、７０４で、取得したＵＲＬを使用して、要求をプロバイダに提出し得る。いくつかの実施形態において、ＵＲＬは、ＨＴＴＰに

従う等の、プロバイダが許容できる様式でフォーマットされる要求として、プロバイダに提供される。しかしながら、いくつかの実施形態において、７０４で、取得したＵＲＬを使用して、要求をプロバイダに提出することは、要求を提出する前にＵＲＬを修正することを含み得る。例えば、いくつかの実施形態において、ＵＲＬは、プロセス７００を行うシステムによってＵＲＬに加えられるデータに対して、ＵＲＬによって供給される暗号化鍵を使用して１つまたは複数の動作を行う要求を提出するために使用され得る。別の実施例として、プロセス７００を行うシステムは、どのように要求を処理するのかを、及び／または要求を満たすために、取得したＵＲＬの有効な署名に加えて、プロバイダによって必要とされ得る情報を供給することをプロバイダに指示するため等の、種々の目的で、１つまたは複数のパラメータをＵＲＬに加え得る。プロセス７００を行うシステム及び／またはプロバイダに有用な他の情報も含まれ得る。

【００４２】

取得したＵＲＬに加えることは、取得したＵＲＬとともに含まれた電子署名を生成するために使用される一部分以外のＵＲＬの一部分に情報を加えることを含み得る。このようにして、電子署名を無効にすることなく、情報をＵＲＬに加えることができる。７０４で、取得したＵＲＬを使用して、要求をプロバイダに提出すると、プロセス７００は、要求が適切に提出された、別様には、満たすことができると仮定すると、７０６で、プロバイダから要求を処理した結果を取得する。例えば、要求によって指定される１つまたは複数の動作に応じて、プロバイダからの応答に結果が含まれ得る。一実施例として、要求が、要求とともに提供されるデータを、または別様には要求によって指定されるデータを、暗号化または解読することであった場合、必要に応じて、７０６で取得した結果は、暗号化または解読したデータを含み得る。全般的に、要求において提供される暗号化鍵を使用して行われる暗号化動作に応じて、７０６で取得した結果は、変動し得る。

【００４３】

図８は、データへのアクセスを提供するためのプロセス８００の実例となる実施例を示す。プロセス８００は、上で説明されるようなサービスプロバイダのウェブサーバ等の適切なシステムによって行われ得る。一実施形態において、プロセス８００は、８０２で、ＵＲＬを有する要求を受け取ることを含む。ＵＲＬは、上で説明されるような暗号化鍵及び電子署名及び／または他の情報を含み得る。８０４で、電子署名がＵＲＬから抽出され得、そして８０６で、要求が有効かどうかを判定するために使用され得る。８０６で、要求が有効であるかどうかを判定することは、電子署名を検証するために対称署名検証アルゴリズムまたは非対称署名検証アルゴリズムを使用する等によって、種々の実施形態に従う種々の方法で行われ得、これは、公開鍵－秘密鍵対のうちの公開鍵を使用して、電子署名の有効性を判定するために、認可機関と通信することを含み得る。

【００４４】

８０６で、署名が無効であると判定された場合、プロセス８００は、８０８で、要求を拒否することを含み得る。要求は、要求が拒否されたことを示す通信及び／またはその拒否の１つまたは複数の理由を伝送すること等によって、８０８で、種々の実施形態に従う種々の方法で拒否され得る。また、必ずしも要求に応答する通信を伝送することを必要とすることなく、単に要求を満たさないこと等によって要求が拒否され得る他の方法も使用され得る。全般的に、要求が拒否され得る任意の方法が使用され得る。しかしながら、８０６で、署名が有効であると判定された場合、プロセス８００は、８１０で、８０２で受け取ったＵＲＬから暗号化鍵を抽出することを含み得る。抽出した暗号化鍵は、８１２で、要求を処理する（すなわち、満たす）ために使用され得る。要求を処理することは、暗号化鍵を使用して、要求とともに含まれるデータ、または別様には要求によって指定されるデータに対して１つまたは複数の暗号化動作を行うことを含み得る。８１４で、要求に対する応答が提供され得る。８１４で、応答を提供することは、暗号化鍵を使用して１つまたは複数の暗号化動作を行った結果（例えば、暗号化したデータ、解読したデータ、及び／または電子署名）、及び／またはそのような動作を行った肯定応答を提供することを含み得る。

【００４５】
プロセス８００は、例示の目的で、ある特定の方法で説明されているが、変形例は、本開示の範囲内にあるとみなされる。例えば、図８は、署名が有効であるという条件で処理されている要求を示す。しかしながら、要求を処理するべきかどうかを判定するために、１つまたは複数の他の動作が行われ得る。一実施例として、要求が有効であるかどうかを判定することは、要求がポリシーを遵守するかどうかを確認することを含み得る。故に、要求を満たすことがポリシーを遵守するかどうかを判定するために、サービスプロバイダの顧客によって構成されるポリシーが確認され得る。さらに、上で述べられるように、ＵＲＬは、要求を行うべきであるかどうか、及び／またはどのように行うべきであるかに関する種々のコンテキスト情報を含み得る。故に、８０６で、プロセス８００を行っている間に要求が有効であるかどうかを判定することは、そのような条件が満たされるかどうかを確認すること、及び／またはＵＲＬに含まれるそのような情報に従って要求を処理することを含み得る。全般的に、要求を満たすことは、１つまたは複数の条件を満たすことを必要とし得、要求が満たされる様式は、要求において指定されるパラメータに少なくとも部分的に依存し得る。
【００４６】
さらに、いくつかの実施形態において、暗号化鍵を使用すると、プロセスは、１つまたは複数の動作を行うことを含み得、該動作は、システムによる、及び全般的にプロセス８００が行われるエンティティによる暗号化鍵へのアクセスを失わせる。暗号化鍵へのアクセスを失わせる動作は、例えば、暗号化鍵が記憶される１つまたは複数のメモリロケーションに上書きすること、及び／または以降の要求を処理する等のためにそのようなメモリロケーションに上書きすることを可能にする１つまたは複数のアクションを行うことを含み得る。全般的に、即座にまたは最終的に暗号化鍵へのアクセスを失わせる任意の動作が行われ得る。このようにして、ＵＲＬにおいて鍵を供給した顧客は、サービスプロバイダが、暗号化鍵が要求を満たす必要があるときに対応する限られた継続時間にわたって、暗号化鍵へのアクセスを有することを確実にすることができる。他の変形例も本開示の範囲内にあるとみなされる。
【００４７】
図９は、一実施形態に従う、アクセスをデータに提供するためのプロセスの実例となる実施例を示す。図９で例示されるように、プロセスは、適切なシステムによって、及びこの特定の実施例では、場合により、プロセス９００の動作を互いに分離する破線によって示される複数のシステムによって行われ得る。一実施形態において、プロセス９００は、９０２で、顧客が、プロバイダによってラップ解除できる（利用できる）ように暗号化秘密をラップすることを含む。暗号化秘密をラップすることは、例えば、プロバイダによって鍵をラップ解除できる（解読できる）ように適切な暗号化鍵を使用して、暗号化秘密を暗号化することによって行われ得る。例えば、暗号化秘密は、プロバイダの顧客とプロバイダとの間で共有される秘密情報を使用してラップされ得る。別の実施例として、暗号化秘密は、公開鍵－秘密鍵対のうちの公開鍵を使用してラップされ得、ここで、プロバイダは、公開鍵－秘密鍵対からの秘密鍵を使用して暗号化秘密をラップ解除することができる。図９は、ラップした暗号化秘密がプロバイダによってラップ解除できるように例示されているが、全般的に、本開示の変形例は、プロバイダが暗号化秘密自体をラップ解除するのではなく、プロバイダの代わりに暗号化秘密をラップ解除する別のシステム（例えば、サードパーティのシステム）を有することができることに留意されたい。
【００４８】
図９の実例となる実施例に戻ると、９０４で、顧客は、ラップした秘密を有するＵＲＬを構築し得る。ＵＲＬは、９０４で、上で説明されるように構築され得る。次いで、９０６で、顧客は、適切な署名鍵を使用して、構築したＵＲＬの電子署名を生成することによって、ＵＲＬに署名し得る。次いで、９０８で、電子署名を含むようにＵＲＬが完成され得る。次いで、９１０で、完成したＵＲＬが上で説明されるようなサードパーティに提供され得る。９１０で、完成したＵＲＬを提供すると、９１２で、サードパーティは、完成

したＵＲＬを使用して、要求をプロバイダに提出し得る。一実施例として、ＵＲＬは、サードパーティのアプリケーションに、完成したＵＲＬを使用して要求をプロバイダに提出させるために、サードパーティのユーザによって選択できるように、ウェブページまたは他のコンテンツに符号化され得る。

【００４９】

要求がプロバイダに提出されると、９１４で、プロバイダが要求を正規化し、検証し得る。正規化は、一方のエンティティからもう一方に要求を伝送する間に、要求が変更され得る種々の方法を逆転させるために行われ得ることに留意されたい。正規化は、例えば、電子署名の検証が正しく行われることを確実にするために行われ得る。例えば、要求が有効である場合に、電子署名も同様に有効であることを確実にするために、要求に挿入される、または要求から削除される追加的な特性が、必要に応じて除去され得、及び／または加えられ得る。９１０で、プロバイダは、要求を検証すると、暗号化鍵を解読するために適切な暗号化アルゴリズムを行うことによって（または別様には、行わせることによって）、暗号化秘密をラップ解除し得る。次いで、９１２で、暗号化鍵を使用して要求を処理し得、９１４で、プロバイダは、プロバイダが行った１つまたは複数の暗号化動作を行った結果、及び／または該暗号化動作を行ったことの肯定応答を提供する等で、サードパーティの要求に応答し得る。上で述べられるように、次いで、９１６で、プロバイダは、上で説明されるように、暗号化秘密へのアクセスを失い得る。

【００５０】

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。

【００５１】

付記１

コンピュータで実現される方法であって、

実行可能命令とともに構成される１つまたは複数のコンピュータシステムの制御下で、

要求を受け取る前に前記１つまたは複数のコンピュータシステムによるアクセスが存在しない暗号化鍵を使用して、要求側から、１つまたは複数の動作を行う該要求を受け取ることであって、該要求は、ユニフォームリソースロケータを含み、該ユニフォームリソースロケータは、

前記１つまたは複数の動作を示し、

前記ユニフォームリソースロケータの一部分及び前記要求側がアクセスできない秘密情報に少なくとも部分的に基づいて、第１のエンティティによって生成される電子署名を含み、また、前記暗号化鍵を含む、受け取ることと、

電子署名が有効であるかどうか判定を行うことと、

この判定が、前記電子署名が有効であることを示すということを条件として、前記示された１つまたは複数の動作をデータに対して行って、前記１つまたは複数の動作の結果を生成するために、前記要求からの前記暗号化鍵を使用することと、

前記要求に従って前記１つまたは複数の動作の前記結果を提供することと、

前記示された１つまたは複数の動作を前記データに対して行うために、前記要求からの前記暗号化鍵を使用した後に、前記暗号化鍵へのアクセスを失わせるための１つまたは複数の動作を行うことと、を含む、コンピュータで実現される方法。

【００５２】

付記２

前記ユニフォームリソースロケータはさらに、前記データを識別する経路を符合化し、

前記示された１つまたは複数の動作を行うために前記暗号化鍵を使用することは、前記データにアクセスする前記符合化された経路を使用することを含む、付記１に記載のコンピュータで実現される方法。

【００５３】

付記３

前記データの少なくともいくつかは、前記要求において前記要求側によって供給される、付記１～２に記載のコンピュータで実現される方法。

【００５４】
付記４
前記ユニフォームリソースロケータの前記一部分は、有効期限を示し、
前記示された１つまたは複数の動作を行うために前記暗号化鍵を使用することは、前記有効期限の前に前記要求を受け取ることをさらなる条件として行われる、付記１～３のいずれか１つに記載のコンピュータで実現される方法。
【００５５】
付記５
前記要求を受け取ることは、サービスプロバイダによって行われ、
前記第１のエンティティは、前記サービスプロバイダの顧客であり、
前記要求側は、前記サービスプロバイダの顧客でない、付記１～４のいずれか１つに記載のコンピュータで実現される方法。
【００５６】
付記６
前記示された１つまたは複数の動作を行うために前記暗号化鍵を使用することは、前記第１のエンティティによって構成される１つまたは複数のポリシーを前記要求が遵守することをさらなる条件として行われる、付記１～５のいずれか１つに記載のコンピュータで実現される方法。
【００５７】
付記７
前記要求は、前記要求を生成するために前記第１のエンティティによって生成される最初のユニフォームリソースロケータに加えられる情報を含み、
前記示された１つまたは複数の動作を行うために前記暗号化鍵を前記使用することは、前記最初のユニフォームリソースロケータに加えられる前記情報に少なくとも部分的に基づく、付記１～６のいずれか１つに記載のコンピュータで実現される方法。
【００５８】
付記８
前記ユニフォームリソースロケータは、暗号化された形態の前記暗号化鍵を含み、
前記方法はさらに、前記示された１つまたは複数の動作を行うために前記暗号化鍵を使用する前に、暗号化された形態の前記暗号化鍵を解読することを含む、付記１～７のいずれか１つに記載のコンピュータで実現される方法。
【００５９】
付記９
システムであって、
１つまたは複数のプロセッサと、
命令を含むメモリと、を備え、該命令は、前記１つまたは複数のプロセッサによって実行されたときに、前記システムに、
要求側からの要求を受け取らせることであって、該要求は、第１のエンティティによって生成された認可情報及び暗号化鍵を含む予め生成された一部分を含む、受け取らせることと、
前記認可情報が、前記要求を満たすために前記第１のエンティティによって認可を示すと判定されることを条件として、前記暗号化鍵を使用して１つまたは複数の動作を行わせることと、
前記行った１つまたは複数の動作の結果を提供させることと、を行わせる、システム。
【００６０】
付記１０
前記予め生成された一部分は、ユニフォームリソースロケータとしてフォーマットされる、付記９に記載のシステム。
【００６１】
付記１１

前記１つまたは複数の動作は、暗号化された形態で前記第１のエンティティによって記憶されるデータにアクセスし、前記暗号化鍵を使用して前記データを解読することを含み、
前記結果を提供することは、前記要求側に前記解読したデータを伝送することを含む、付記９～１０に記載のシステム。
【００６２】
付記１２
前記要求はさらに、前記予め生成された一部分に加えられたデータを含み、
前記暗号化鍵を使用して前記１つまたは複数の動作を行うことは、前記予め生成された一部分に加えられた前記データに対して１つまたは複数の暗号化動作を行うことを含む、付記９～１１に記載のシステム。
【００６３】
付記１３
前記認可情報は、前記要求側がアクセスできない秘密情報を使用して生成される電子署名を含む、付記９～１２に記載のシステム。
【００６４】
付記１４
前記認可情報は、前記要求を提出するためのコンテキストに対して１つまたは複数の条件を指定し、
前記暗号化鍵を使用して１つまたは複数の動作を行うことはさらに、前記１つまたは複数の条件を遵守して前記要求を受け取ることを条件として行われる、付記９～１３に記載のシステム。
【００６５】
付記１５
前記１つまたは複数の条件は、前記要求を満たすことができる継続時間を定義する、付記９～１４に記載のシステム。
【００６６】
付記１６
前記認可情報は、前記暗号化鍵に少なくとも部分的に基づいて生成される電子署名を含み、
前記第１のエンティティによる認可を示す前記認可情報は、前記電子署名が有効であることを必要とする、付記９～１５に記載のシステム。
【００６７】
付記１７
前記システムはさらに、前記要求側と、前記要求側と異なる顧客システムとを備え、
前記顧客システムは、前記要求を提出する際に使用するための前記要求の表現を提供し、それによって、前記要求を前記要求側から受け取ることを可能にする、付記９～１６に記載のシステム。
【００６８】
付記１８
そこに記憶される命令を有する非一時的なコンピュータ読み出し可能な記憶媒体であって、該命令は、コンピュータシステムの１つまたは複数のプロセッサによって実行されたときに、該コンピュータシステムに、
要求及び暗号化鍵を符号化する情報を生成することと、
前記要求を満たすことができるサービスプロバイダによって検証できる情報の電子署名を生成することと、
前記情報及び電子署名を前記サービスプロバイダに提供することを可能にして、前記サービスプロバイダに前記暗号化鍵を使用させて前記要求を満たすために、前記情報及び前記電子署名を利用できるようにすることと、を行わせる、非一時的なコンピュータ読み出し可能な記憶媒体。
【００６９】

付記１９
前記情報及び前記電子署名を利用できるようにすることは、前記情報及び前記電子署名を含むユニフォームリソースロケータを生成することを含む、付記１８に記載の非一時的なコンピュータ読み出し可能な記憶媒体。
【００７０】
付記２０
前記情報及び前記電子署名を利用できるようにすることは、選択可能な要素とともに構成されるウェブページを提供することを含み、該要素は、選択されたときに、前記情報及び電子署名を含む前記要求を前記サービスプロバイダに伝送させる、付記１８～１９に記載の非一時的なコンピュータ読み出し可能な記憶媒体。
【００７１】
付記２１
前記ウェブページを提供することは、前記ウェブページを、前記サービスプロバイダと異なるサードパーティに提供することを含む、付記１９～２０に記載の非一時的なコンピュータ読み出し可能な記憶媒体。
【００７２】
付記２２
前記情報はさらに、前記サービスプロバイダによってホストされるリソースの識別子を符合化し、
前記要求は、前記リソースと関連して行われる１つまたは複数の動作を指定する、付記１８～２１に記載の非一時的なコンピュータ読み出し可能な記憶媒体。
【００７３】
付記２３
前記情報は、プレーンテキストの形態で前記暗号化鍵を符合化する、付記１８～２２に記載の非一時的なコンピュータ読み出し可能な記憶媒体。
【００７４】
付記２４
前記情報は、前記要求を前記サービスプロバイダによって満たすことができるようにするための、前記要求の提出に対する１つまたは複数の条件を符号化する、付記１８～２３に記載の非一時的なコンピュータ読み出し可能な記憶媒体。
【００７５】
他の変形例は、本開示の範囲内にあるとみなされる。例えば、鍵がＵＲＬに提供されるタイプ及び方法、または全般的にプロバイダに対する要求は、種々の実施形態に従って変動し得る。本開示の技法と組み合わせられ得るいくつかの技法は、２０１３年９月２５日に出願された米国特許出願第１４，０３７，２８２号、名称「ＲＥＳＯＵＲＣＥ　ＬＯＣＡＴＯＲＳ　ＷＩＴＨ　ＫＥＹＳ」、及び２０１３年９月２５日に出願された米国特許出願第１４／０３７，２９２号、名称「ＤＡＴＡ　ＳＥＣＵＲＩＴＹ　ＵＳＩＮＧ　ＲＥＱＵＥＳＴ－ＳＵＰＰＬＩＥＤ　ＫＥＹＳ」で説明されており、これらは全ての目的に対して参照により本明細書に組み込まれる。
【００７６】
図１０は、種々の実施形態に従う、態様を実現するための例示的な環境１０００の態様を例示する。認識されるように、説明の目的でウェブに基づく環境が使用されるが、種々の実施形態を実現するために、必要に応じて、異なる環境が使用され得る。環境は、電子クライアントデバイス１００２を含み、該デバイスとしては、適切なネットワーク１００４を通じて要求、メッセージ、または情報を送信及び受信し、情報をデバイスのユーザに搬送するように動作可能な、任意の適切なデバイスが挙げられる。そのようなクライアントデバイスの例としては、パーソナルコンピュータ、携帯電話、ハンドヘルドメッセージングデバイス、ラップトップコンピュータ、タブレットコンピュータ、セットトップボックス、携帯情報端末、組み込み型コンピュータシステム、電子ブックリーダー等が挙げられる。ネットワークとしては、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そのようなネットワーク、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が挙げられる。そのようなシステムに使用される構成要素は、選択されたネットワーク及び／または選択環境のタイプに少なくとも部分的に依存し得る。そのようなネットワークを介して通信するためのプロトコル及び構成要素はよく知られており、本明細書では詳細に論じない。ネットワークを通じた通信は、有線接続または無線接続、及びそれらの組み合わせによって可能にすることができる。本実施例では、当業者には明らかなように、要求を受け取り、それに応じてコンテンツを提供するためのウェブサーバ１００６を環境が含むので、このネットワークは、インターネットを含むが、他のネットワークの場合、類似の目的を提供する代替のデバイスを使用することができる。

【００７７】

実例となる環境は、少なくとも１つのアプリケーションサーバ１００８と、データストア１０１０とを含む。連鎖され得るまたは別様には構成され得る、適切なデータストアからデータを取得する等の作業を行うように相互作用することができる、いくつかのアプリケーションサーバ、層もしくは他の要素、過程、または構成要素があり得ることを理解されたい。サーバは、本明細書で使用されるとき、ハードウェアデバイスまたは仮想コンピュータシステム等の種々の方法で実現され得る。いくつかの文脈において、サーバは、コンピュータシステム上で実行されているプログラムモジュールを指し得る。本明細書で使用される「データストア」という用語は、データを記憶し、それにアクセスし、それを取り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、任意の数のデータサーバ、データベース、データ記憶デバイス、データ記憶媒体、及びそれらの任意の組み合わせを、任意の標準型、分散型、またはクラスタ型の環境において含み得る。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つまたは複数のアプリケーションの態様を実行するために、必要に応じて、データストアと統合するための、また、アプリケーションのためのデータアクセス及びビジネスロジックの一部（さらには大部分）を取り扱うための、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る。アプリケーションサーバは、データストアと連携してアクセス制御サービスを提供し得、また、この実施例において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化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、ユーザに転送されるテキスト、グラフィックス、オーディオ、及び／またはビデオ等のコンテンツを生成することができる。全ての要求及び応答、ならびにクライアントデバイス１００２とアプリケーションサーバ１００８との間のコンテンツの送達は、ウェブサーバによって取り扱うことができる。本明細書で論じられる構造化コードは、本明細書で他の場所で論じられるように、任意の適切なデバイスまたはホストマシン上で実行することができるので、ウェブサーバ及びアプリケーションサーバは必要とされず、これらは単に例示的な構成要素に過ぎないことを理解されたい。さらに、単一のデバイスによって行われるように本明細書で説明される動作は、別途文脈から明らかでない限り、分散型システムを形成し得る複数のデバイスによって集合的に行われ得る。

【００７８】

データストア１０１０は、いくつかの別個のデータテーブル、データベース、または他のデータ記憶機構、及び本開示の特定の態様に関連するデータを記憶するための媒体を含むことができる。例えば、例示されるデータストアは、製品側のコンテンツを提供するために使用することができる、製品データ１０１２及びユーザ情報１０１６を記憶するための機構を含み得る。データストアはまた、ログデータ１０１４を記憶するための機構も含むように示され、該機構は、レポーティング、分析、または他のそのような目的のために使用することができる。ページ画像情報及びアクセス権利情報等の、データストアに記憶する必要があり得る、数多くの他の態様があり得、それらは、必要に応じて上で列記した機構のいずれかに、またはデータストア１０１０の追加的な機構に記憶することができることを理解されたい。データストア１０１０は、アプリケーションサーバ１００８から命令を受け取って、それに応じてデータを取得する、更新する、または別様には処理するた

めに、それと関連する論理を通して操作可能である。一実施例において、ユーザは、ユーザによって操作されるデバイスを通して、ある特定の種類の品目の検索要求を提出し得る。この事例において、データストアは、ユーザの識別情報を検証するためにユーザ情報にアクセスし得、また、そのタイプの品目に関する情報を取得するために、カタログの詳細情報にアクセスすることができる。次いで、ユーザがユーザデバイス１００２上のブラウザを介して視聴することができるウェブページ上の結果リスト等で、情報をユーザに返すことができる。関心の特定の品目の情報は、ブラウザの専用ページまたはウィンドウで視聴することができる。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のコンテンツに限定されるわけではなく、より全般的には、処理要求全般に適用可能であり得、ここで、要求は、必ずしもコンテンツに対する要求ではないことに留意されたい。

【００７９】

各サーバは、一般的に、そのサーバの一般的な管理及び操作のため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、また、一般的に、サーバのプロセッサによって実行されたときに、サーバがその意図する機能を行うことを可能にする命令を記憶する、コンピュータ読み出し可能な記憶媒体（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等）を含む。オペレーティングシステム及びサーバの一般的な機能の適切な実現形態は、既知であるか、または市販されており、また、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現される。

【００８０】

一実施形態における環境は、１つまたは複数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、そのようなシステムは、図１０で例示されるよりも少ない数または多い数の構成要素を有するシステムで十分同等に動作できることが、当業者に認識されるであろう。したがって、図１０のシステム１０００の描写は、本質的に実例となるものであり、本開示の範囲を限定するものとみなすべきではない。

【００８１】

種々の実施形態はさらに、多種多様な動作環境で実現することができ、いくつかの事例において、数多く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つまたは複数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むことができる。ユーザまたはクライアントデバイスとしては、標準的なオペレーティングシステムを実行す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等の、数多くの汎用パーソナルコンピュータ、ならびに、モバイルソフトウェアを実行する、及び数多くのネットワーキング及びメッセージングプロトコルをサポートすることができる、セルラーデバイス、無線デバイス、及びハンドヘルドデバイスのうちのいずれかが挙げられる。そのようなシステムとしてはまた、開発及びデータベース管理等の目的で、種々の市販のオペレーティングシステム及び他の既知のアプリケーションのいずれかを動作させる、数多くのワークステーションも挙げられる。これらのデバイスとしてはまた、ネットワークを介して通信することができる、ダミー端末、シンクライアント、ゲーミングシステム、及び他のデバイス等の、他の電子デバイスも挙げられる。

【００８２】

本開示の種々の実施形態は、伝送制御プロトコル／インターネットプロトコル（「ＴＣＰ／ＩＰ」）、オープンシステムインターコネクション（「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（「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ＡｐｐｌｅＴａｌｋ等の、様々な市販のプロトコルのいずれかを使用して通信をサポートするための、当業者によく知られている、少なくとも１つのネットワークを利用する。ネットワークは、例えば、ローカルエリアネットワーク、ワイドエリアネットワーク、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、公衆交換電話ネットワーク、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とすることができる。

【００８３】

ウェブサーバを利用する実施形態において、ウェブサーバは、ハイパーテキストトランスファープロトコル（「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（登録商標）サーバ、及びビジネスアプリケーションサーバを含む、様々な任意のサーバまたは中間層アプリケーションのうちのいずれかを実行することができる。サーバ（複数可）はまた、ユーザデバイスからの要求に応答して、Ｊａｖａ（登録商標）、Ｃ、Ｃ＃、もしくはＣ＋＋等の任意のプログラミング言語、またはＰｅｒｌ、Ｐｙｔｈｏｎ、もしくはＴＣＬ等の任意のスクリプト言語、ならびにそれらの組み合わせで書かれた１つまたは複数のスクリプトまたはプログラムとして実現され得る１つまたは複数のウェブアプリケーションを実行すること等によって、プログラムまたはスクリプトを実行することも可能であり得る。サーバ（複数可）としてはまた、Ｏｒａｃｌｅ（登録商標）、Ｍｉｃｒｏｓｏｆｔ（登録商標）、Ｓｙｂａｓｅ（登録商標）、及びＩＢＭ（登録商標）から市販されているものが挙げられるがそれらに限定されない、データベースサーバも挙げられ得る。

【００８４】

環境は、上で論じられるように、種々のデータストア、ならびに他のメモリ及び記憶媒体を含むことができる。これらは、コンピュータの１つまたは複数に対してローカルな（及び／またはその中に存在する）記憶媒体上、またはネットワーク全体にわたるコンピュータのいずれかまたは全てからリモートな記憶媒体上等の、種々の場所に存在することができる。特定の１組の実施形態において、情報は、当業者によく知られているストレージエリアネットワーク（「ＳＡＮ」）の中に存在し得る。同様に、必要に応じて、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起因する機能を行うための任意の必要なファイルが、ローカル及び／またはリモートに記憶され得る。システムがコンピュータ制御のデバイスを含む場合、そのような各デバイスは、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むことができ、該要素は、例えば、少なくとも１つの中央処理ユニット（「ＣＰＵ」または「プロセッサ」）と、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）と、少なくとも１つの出力デバイス（例えば、表示デバイス、プリンタ、またはスピーカー）とを含む。そのようなシステムはまた、ディスクドライブ、光記憶デバイス、及びランダムアクセスメモリ（「ＲＡＭ」）またはリードオンリーメモリ（「ＲＯＭ」）等の固体記憶デバイス、ならびにリムーバブル媒体デバイス、メモリカード、フラッシュカード等の、１つまたは複数の記憶デバイスも含み得る。

【００８５】

そのようなデバイスはまた、上で説明されるように、コンピュータ読み出し可能な記憶媒体リーダー、通信デバイス（例えば、モデム、ネットワークカード（無線または有線）、赤外線通信デバイス等）、及びワーキングメモリも含み得る。コンピュータ読み出し可能な記憶媒体リーダーは、リモート、ローカル、固定の、及び／またはリムーバブル記憶デバイスを表すコンピュータ読み出し可能な記憶媒体、ならびにコンピュータ読み出し可能な情報を一時的に及び／または永続的に含む、記憶する、伝送する、及び取り出すための記憶媒体と接続することができるか、または該記憶媒体を受容するように構成することができる。システム及び種々のデバイスはまた、一般的に、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数多く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。代替の実施形態は、上で説明されるものからの多数の変形例を有し得ることを理解されたい。例えば、カスタマイズされたハードウェアも使用され得、及び／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）、または双方で実現され得る。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。

【００８６】

コードまたはコードの一部分を含むための記憶媒体及びコンピュータ読み出し可能な媒体としては、ＲＡＭ、ＲＯＭ、電気的消去可能プログラマブルリードオンリーメモリ（「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リードオンリーメモリ（「ＣＤ－ＲＯＭ」）、デジタル多用途ディスク（ＤＶＤ）、もしくは他の光記憶装置、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デバイス、または所望の情報を記憶するために使用することができ、かつシステムデバイスによってアクセスすることができる任意の他の媒体を含む、コンピュータ読み出し可能な命令、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を記憶及び／または伝送するための任意の方法または技術で実現される揮発性及び不揮発性のリムーバブルな及び非リムーバブルな媒体等が挙げられるが、それらに限定されない、記憶媒体及び通信媒体を含む、当技術分野で知られているまたは使用されている、任意の適切な媒体が挙げられる。本明細書で提供される開示及び教示に基づいて、当業者は、種々の実施形態を実現するための他の手段及び／または方法を認識するであろう。

【００８７】

故に、本明細書及び図面は、限定的な意味ではなく、実例的な意味である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る本発明のより広範な趣旨及び範囲から逸脱することなく、種々の修正及び変更が行われ得ることが明らかになるであろう。

【００８８】

他の変形例は、本開示の趣旨の範囲内である。したがって、開示される手法は、種々の修正及び代替の構造が可能であるが、その特定の例示される実施形態を図面に示し、上で詳細に説明した。しかしながら、本発明を、開示される特定の形態に限定するいかなる意図もなく、逆に、本発明は、添付の特許請求の範囲で定義されるように、本発明の趣旨及び範囲内に入る全ての修正物、均等物、及び代替物を包含することを意図するものであることを理解されたい。

【００８９】

開示される実施形態を説明する文脈での（特に、特許請求の範囲の文脈での）「ａ」及び「ａｎ」及び「ｔｈｅ」という用語、ならびに類似の指示対象の使用は、本明細書で別途指示されていない限り、または明らかに文脈と矛盾していない限り、単数及び複数の双方を包含するものと解釈されたい。「備える」、「有する」、「含む」、及び「含有する」という用語は、別途注記のない限り、オープンエンドの用語（すなわち、「含むが、それに限定されない」ことを意味する）として解釈されたい。「接続される」という用語は、未修正であるとき、及び物理的接続を指すときに、途中に中断がある場合であっても、部分的または全体的にその中に含まれる、取り付けられる、または互いに接合されるものとして解釈されたい。本明細書での値の範囲の列挙は、本明細書で別途指示されない限り、単に、その範囲内に入るそれぞれの値を個々に参照する簡単な方法としての役割を果たすように意図されたものであり、それぞれの値は、本明細書で個々に列挙されているかのように、本明細書に組み込まれる。「組」（例えば、「１組の品目」）あるいは「サブセット」という用語の使用は、別途注記のない限り、または文脈と矛盾しない限り、１つまたは複数の部材を備える、空でない集合であるものとして解釈されたい。さらに、別途注記のない限り、または文脈と矛盾しない限り、対応する組の「サブセット」という用語は、必ずしも対応する組の適切なサブセットを意味するものではなく、サブセット及び対応する組は、同等であり得る。

【００９０】

「Ａ、Ｂ、及びＣのうちの少なくとも１つ」または「Ａ、Ｂ及びＣのうちの少なくとも１つ」という形態の慣用句等の接続語は、別途具体的に提示されない限り、または別様には明らかに文脈と矛盾しない限り、そうでなければ、その文脈は、一般に、品目、用語等がＡまたはＢまたはＣ、またはＡ及びＢ及びＣの組の任意の空でないサブセットであり得

ることを提示するために使用されるものと理解されたい。例えば、上の接続語句で使用される３つの項を有する組の実例となる例において、「Ａ、Ｂ、及びＣのうちの少なくとも１つ」及び「Ａ、Ｂ及びＣのうちの少なくとも１つ」は、｛Ａ｝、｛Ｂ｝、｛Ｃ｝、｛Ａ、Ｂ｝、｛Ａ、Ｃ｝、｛Ｂ、Ｃ｝、｛Ａ、Ｂ、Ｃ｝という組のうちのいずれかを指す。したがって、そのような接続語は、全般的に、ある特定の実施形態が、少なくとも１つのＡ、少なくとも１つのＢ、少なくとも１つのＣがそれぞれ存在することを必要とすることを意味することを意図しない。

【００９１】

本明細書で説明されるプロセスの動作は、本明細書で別途指示されない限り、または文脈によって明らかに矛盾しない限り、任意の好適な順序で行うことができる。本明細書で説明されるプロセス（またはその変形及び／または組み合わせ）は、実行可能命令とともに構成される１つまたは複数のコンピュータシステムの制御下で行われ得、また、ハードウェアまたはその組み合わせによって、１つまたは複数のプロセッサ上で集合的に実行するコード（例えば、実行可能命令、１つまたは複数のコンピュータプログラム、または１つまたは複数のアプリケーション）として実現され得る。このコードは、例えば１つまたは複数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、コンピュータ読み出し可能な記憶媒体に記憶され得る。コンピュータ読み出し可能な記憶媒体は、非一時的であり得る。

【００９２】

本明細書で提供される任意の及び全ての例、または例示的な言葉（例えば「等」の使用は、単に、本発明の実施形態をより明確にすることを意図しているに過ぎず、別途特許請求されていない限り、本発明の範囲を限定するものではない。明細書の中のいかなる言葉も、特許請求されていない何らかの要素が本発明の実践に必須であることを示すものではないと解釈されたい。

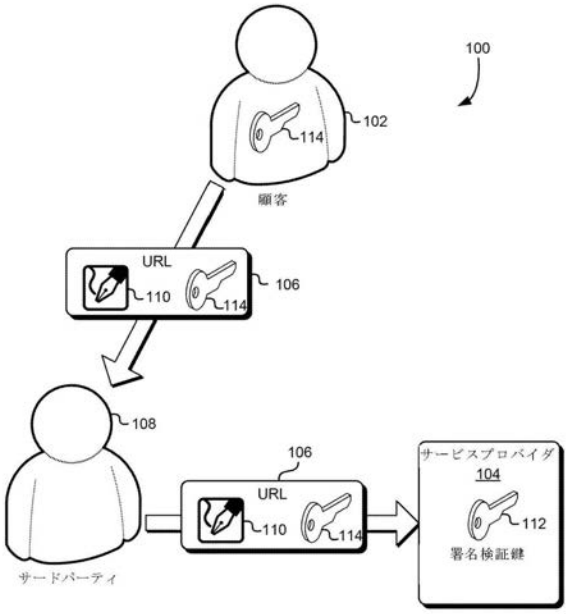
【００９３】

本発明を行うための、発明者等に知られている最良の方法を含む、本開示の好ましい実施形態が本明細書で説明される。当業者には、上の説明を読むことにより、こうした好ましい実施形態の変形が明らかになるであろう。本発明者らは、そのような変形を必要に応じて採用することを予期し、本発明者らは、本明細書で具体的に説明されるもの以外で本開示の実施形態が実践されることを意図する。故に、本開示の範囲は、適用法によって許容される本明細書に添付される特許請求の範囲に記載される主題の全ての修正物及び等価物を含む。さらに、上で説明される要素の全ての可能な変形におけるその要素の任意の組み合わせは、本明細書で別途指示されない限り、または明らかに文脈と矛盾しない限り、本開示の範囲によって包含される。

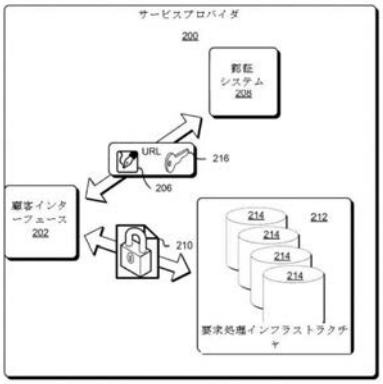
【００９４】

本明細書で引用される刊行物、特許出願、及び特許を含む、全ての参考文献は、あたかも各文献が個々にかつ具体的に参照により組み込まれるように示され、かつ本明細書で全体として説明されているかのように、同じ範囲で参照により本明細書に組み込まれる。

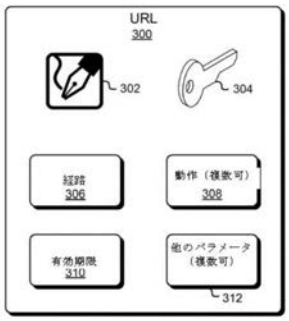
【図１】


100
102
114
顧客
URL
110
114
106
108
106
URL
110
114
サードパーティ
サービスプロバイダ
104
112
署名検証鍵

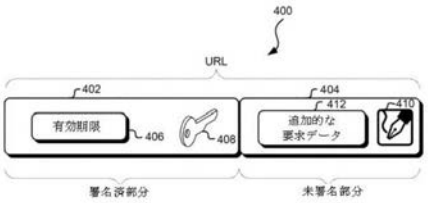
【図２】


サービスプロバイダ
200
顧客インターフェース
202
URL
216
206
210
212
214
214
214
214
要求処理インフラストラクチャ

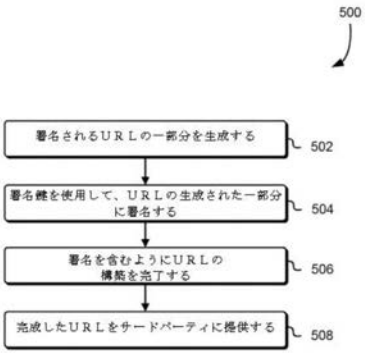
【図３】


URL
300
302
304
経路
306
動作（複数可）
308
有効期限
310
他のパラメータ
（複数可）
312

【図４】


400
URL
402
404
412
410
有効期限
406
408
追加的な
要求データ
署名済部分
未署名部分

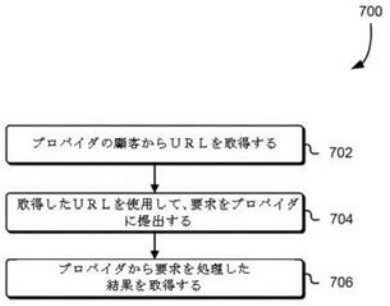
【図５】


500
署名されるＵＲＬの一部分を生成する
502
署名鍵を使用して、ＵＲＬの生成された一部分に署名する
504
署名を含むようにＵＲＬの構築を完了する
506
完成したＵＲＬをサードパーティに提供する
508

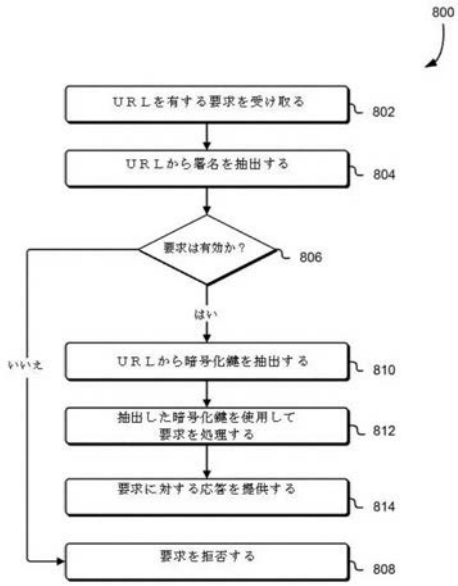
【図６】


EVideoStore
Alyosha.com
Ilya.com
Stasya.com
Katyaさん ようこそ！ (サインアウト)
2015年3月14日
注文履歴
マイリスト
セール！
現在レンタル中です：
ビデオ
アクション
アドベンチャ
コメディ
外国
ホラー
ロマンス
スリラー
TV
(他のジャンル)
広告
THE TEAM
600
602
チームが売上税のない状態から栄光を手にするまでを描いたストーリー。
すぐに見る
604
Provider.com/.../TheTeam.mp4
614
610
608
606
有効期限：2015年3月15日
612

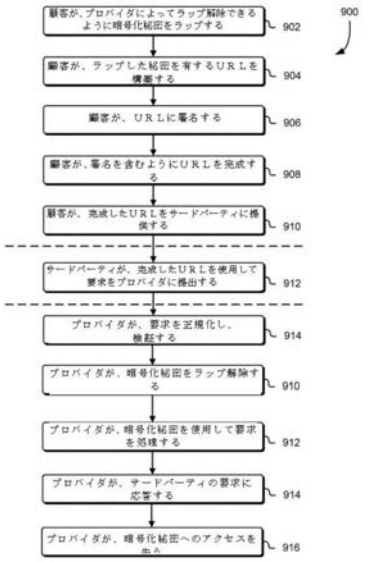
【図７】


700
プロバイダの顧客からＵＲＬを取得する
702
取得したＵＲＬを使用して、要求をプロバイダに提出する
704
プロバイダから要求を処理した結果を取得する
706

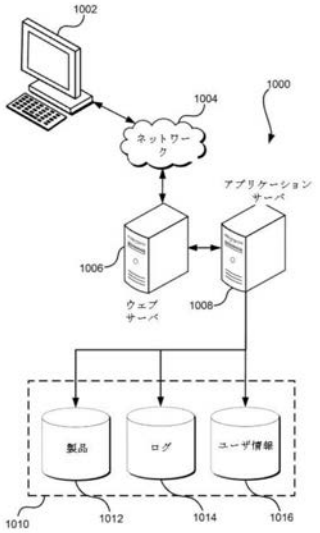
【図８】


800
ＵＲＬを有する要求を受け取る
802
ＵＲＬから署名を抽出する
804
要求は有効か？
806
はい
いいえ
ＵＲＬから暗号化鍵を抽出する
810
抽出した暗号化鍵を使用して要求を処理する
812
要求に対する応答を提供する
814
要求を拒否する
808

【図９】



【図１０】



【手続補正書】
【提出日】令和2年8月3日(2020.8.3)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
コンピュータシステムの１以上のプロセッサによって実行される命令を記憶した非一時的なコンピュータ読み取り可能な記憶媒体であって、
前記命令が実行されると前記コンピュータシステムに、
第１暗号鍵、該第１暗号鍵と関連する署名済部分および未署名部分を含むユニフォームリソースロケータ（ＵＲＬ）の要求を取得させることと、
前記要求を伝送させることと、
前記第１暗号鍵と前記未署名部分の情報とに基づいて生成される前記要求の応答を受信させることと、を備え、
前記未署名部分の情報は、前記署名済部分の有効性に影響を与えない、コンピュータ読み取り可能な記憶媒体。
【請求項２】
前記命令が実行されると前記コンピュータシステムに、
前記要求とともに第２暗号鍵で生成された暗号署名を取得させることと、
前記要求とともに前記暗号署名を伝送させることと、
を備える、請求項１に記載のコンピュータ読み取り可能な記憶媒体。
【請求項３】

前記第２暗号鍵は、前記コンピュータシステムには利用できない、
請求項２に記載のコンピュータ読み取り可能な記憶媒体。
【請求項４】
前記第２暗号鍵は、公開鍵－秘密鍵対の秘密鍵であり、
前記暗号署名は、公開鍵を使用して暗号的に検証可能である、
請求項２に記載のコンピュータ読み取り可能な記憶媒体。
【請求項５】
前記要求はウェブサービスのためＵＲＬの形態であり、
前記要求は前記ウェブサービスに伝送される、
請求項１に記載のコンピュータ読み取り可能な記憶媒体。
【請求項６】
前記命令が実行されると前記コンピュータシステムに、
前記要求とともに前記第１暗号鍵で暗号化されたデータを伝送させることと、
前記暗号化されたデータのプレーンテキスト形態を受信させることと、
を備える、請求項１に記載のコンピュータ読み取り可能な記憶媒体。
【請求項７】
前記命令が実行されると前記コンピュータシステムに、
前記要求とともにデータを伝送させることと、
前記第１暗号鍵で暗号化されたデータの暗号形態を受信させることと、
を備える、請求項１に記載のコンピュータ読み取り可能な記憶媒体。
【請求項８】
１以上のプロセッサと、
命令を含むメモリと、を有するシステムであって、
前記プロセッサによって命令が実行された結果、前記システムに、
第１暗号鍵、該第１暗号鍵と関連する署名済部分および未署名部分を含むユニフォームリソースロケータ（ＵＲＬ）の情報の要求をユーザから受け取らせることと、
前記第１暗号鍵とサードパーティに修正された前記未署名部分の情報に基づいて、前記ユーザに要求された情報を提供させることと、を備え、
前記サードパーティにより修正は、前記署名済部分の有効性に影響を与えない、システム。
【請求項９】
前記要求は、前記ＵＲＬの暗号署名と前記第１暗号鍵とを有し、
前記命令は、前記プロセッサによって実行されると、前記暗号署名が第２暗号鍵を使用して有効か否かを決定する、
請求項８に記載のシステム。
【請求項１０】
前記プロセッサによって命令が実行された結果、前記システムに、
前記暗号署名が有効と決定した結果として前記情報へのアクセスを提供させる、
請求項９に記載のシステム。
【請求項１１】
前記要求は、認可されたエンティティによって前記ユーザに適用され、
前記第２暗号鍵は、前記認可されたエンティティに関連している、
請求項９に記載のシステム。
【請求項１２】
前記プロセッサによって命令が実行された結果、前記システムに、
前記第１暗号鍵を使って暗号化動作を行うことによって情報を取得させる、
請求項８に記載のシステム。
【請求項１３】
前記暗号化動作は、前記第１暗号鍵を使って前記情報の暗号化された形態の解読を含む、

請求項１２に記載のシステム。
【請求項１４】
前記第２暗号鍵は、前記認可されたエンティティに関連する公開鍵－秘密鍵対の公開鍵であり、
前記公開鍵－秘密鍵対の秘密鍵は、前記システムにアクセスできない、
請求項１１に記載のシステム。