(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6851970号
(P6851970)
(45)発行日　令和3年3月31日(2021.3.31)　(24)登録日　令和3年3月12日(2021.3.12)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
H04L 9/14 (2006.01)　H04L 9/00 641
G06F 21/31 (2013.01)　G06F 21/31

請求項の数 14　(全 28 頁)

(21)出願番号　特願2017-529786(P2017-529786)
(86)(22)出願日　平成27年12月14日(2015.12.14)
(65)公表番号　特表2018-504806(P2018-504806A)
(43)公表日　平成30年2月15日(2018.2.15)
(86)国際出願番号　PCT/US2015/065638
(87)国際公開番号　WO2016/126332
(87)国際公開日　平成28年8月11日(2016.8.11)
審査請求日　平成29年7月25日(2017.7.25)
審判番号　不服2020-2347(P2020-2347/J1)
審判請求日　令和2年2月20日(2020.2.20)
(31)優先権主張番号　14/574,337
(32)優先日　平成26年12月17日(2014.12.17)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　506223509
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、ネバダ州　８９５０７、レノ、ピー．オー．ボックス　８１０２
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　ルビン、グレゴリー　アラン
アメリカ合衆国、ワシントン州　９８１０８、シアトル　ピー．オー．ボックス　８１２２６　アマゾン　テクノロジーズ、インコーポレイテッド内

最終頁に続く

(54)【発明の名称】期待値を有するデータセキュリティ処理

(57)【特許請求の範囲】
【請求項１】
コンピュータ実施方法であって、
ウェブサービス要求の履行は前記ウェブサービス要求で定められた暗号化されたデータに対する暗号処理の実施を含む前記ウェブサービス要求を、サービスプロバイダのカスタマと関連するリクエスタから受信することと、
前記ウェブサービス要求の情報の少なくとも一部に基づき、前記サービスプロバイダの複数のカスタマのための、前記サービスプロバイダにより管理される複数の暗号鍵から前記リクエスタに関連付けられた暗号鍵を選択し、セキュリティ期待値セットを決定し、前記セキュリティ期待値セットは、履行の際、選択した前記暗号鍵が前記暗号処理の実施に使用可能であるかどうかにかかわらず、前記暗号鍵の信頼性に対する処理を実施せずに前記暗号処理の結果を信頼することを示す、選択した前記暗号鍵に適用する条件セットを定め、選択した前記暗号鍵に対し前記セキュリティ期待値セットを評価し、前記セキュリティ期待値セットの評価および前記暗号化されたデータの前記暗号処理の結果の少なくとも一部に基づき、前記ウェブサービス要求に対する応答を生成し、生成した前記応答を提供することによって、前記ウェブサービス要求を履行することを含む、前記コンピュータ実施方法。
【請求項２】
前記セキュリティ期待値セットは前記ウェブサービス要求において指定される、請求項１に記載のコンピュータ実施方法。

【請求項３】
前記方法はさらに、
複数の保存ポリシドキュメントから、前記ウェブサービス要求に適用するポリシセットを決定することと、
前記ポリシセットが前記ウェブサービス要求の履行を許可するよう決定することを含み、
前記セキュリティ期待値セットを決定することは、決定した前記ポリシセットから少なくとも１つのセキュリティ期待値を決定することを含む、請求項１に記載のコンピュータ実施方法。
【請求項４】
前記方法はさらに、
前記カスタマによりポリシの修正を許可されたエンティティから、前記カスタマに関連するポリシセットに対し前記セキュリティ期待値セットの実施を求めるウェブサービス要求を受信することと、
前記セキュリティ期待値セットを含むよう前記ポリシセットを修正することで前記ウェブサービス要求を履行することを含む、請求項３に記載のコンピュータ実施方法。
【請求項５】
システムであって、１以上のサービスを実施するよう構成された少なくとも１つのコンピューティングデバイスを備え、前記１以上のサービスは、
クライアントから、要求で定められた暗号化されたデータに対する暗号処理の実施を求める前記要求を受信することと、
前記暗号処理を実施するための前記クライアントに関連付けられた暗号鍵であって、前記システムにより管理される暗号鍵セットからのものである前記暗号鍵を決定し、前記要求に含まれる情報の少なくとも一部に基づき、前記暗号鍵の信頼性に対する処理を実施せずに前記暗号処理の実施結果は前記クライアントにより信頼されるべきとする条件セットを決定し、決定した前記条件セットおよび前記暗号化されたデータの前記暗号処理の結果の少なくとも一部に基づき、前記要求に対する応答を生成し、生成した前記応答を前記クライアントに提供することによって、前記要求を履行することを含む、前記システム。
【請求項６】
前記１以上のサービスはさらに、少なくとも１つの条件が前記要求において指定されることにより、前記条件セットの前記少なくとも１つの条件を決定することを含む、請求項５に記載のシステム。
【請求項７】
前記クライアントのアイデンティティが認証され、
前記１以上のサービスは、少なくとも、前記アイデンティティに適用するポリシセットのサブセットを選択し、前記条件セットの少なくとも１つの条件を、前記少なくとも１つの条件が前記ポリシセットの前記サブセットにおいて指定されることにより決定することによって、前記条件セットを決定することを含む、請求項５または請求項６に記載のシステム。
【請求項８】
前記システムはサービスプロバイダにより動作され、
前記ポリシセットは、前記アイデンティティに関連する前記サービスプロバイダのカスタマによりプログラムでの修正が可能である、請求項７に記載のシステム。
【請求項９】
前記システムは、前記暗号鍵セットのハードウェアベースの保護機能を有するデバイスであり、前記暗号鍵ではプレインテキスト形式に前記デバイスからプログラムでのエクスポートができない、請求項５から請求項８の何れか一項に記載のシステム。
【請求項１０】
前記暗号鍵は、サービスプロバイダの第一カスタマに代わり前記システムにより管理され、

前記暗号鍵セットは、前記サービスプロバイダの第二カスタマに代わり前記システムにより管理される第二暗号鍵を備える、請求項５から請求項９の何れか一項に記載のシステム。

【請求項１１】

前記クライアントは、前記サービスプロバイダの第三カスタマにより動作される、請求項１０に記載のシステム。

【請求項１２】

生成した前記応答は、前記条件セットの評価結果を示す情報を含む、請求項５から請求項１１の何れか一項に記載のシステム。

【請求項１３】

前記条件セットは、前記暗号鍵が、信頼性があると指定された暗号鍵セットからのものであることを求める、請求項５から請求項１２の何れか一項に記載のシステム。

【請求項１４】

システムであって、１以上のサービスを実施するよう構成された少なくとも１つのコンピューティングデバイスを備え、前記１以上のサービスは、

リクエスタからの要求であって、前記要求の履行は前記要求で定められた暗号化されたデータに対する暗号処理を含む、前記要求に含まれる情報の少なくとも一部に基づき、暗号鍵の信頼性に対する処理を実施せずに前記リクエスタが前記暗号処理の結果を信頼すべきかどうかを決定するために、前記リクエスタに関連付けられた前記暗号鍵に適用する条件セットを決定することであって、前記暗号鍵は、前記システムにより管理される前記暗号鍵セットからのものである、決定することと、

前記要求の履行方法を決定するために、決定した前記条件セットを評価することと、

決定した前記条件セットの評価が、前記暗号鍵が信頼できることを示すことを受けて、前記暗号化されたデータに対する前記暗号処理を実施し、前記暗号化されたデータの前記暗号処理の前記結果を前記要求に応答して提供することを含む、前記システム。

【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、２０１４年１２月１７日に「ＤＡＴＡ　ＳＥＣＵＲＩＴＹ　ＯＰＥＲＡＴＩＯＮＳ　ＷＩＴＨ　ＥＸＰＥＣＴＡＴＩＯＮＳ」と題され出願された同時係属中の米国特許出願第１４／５７４，３３７号からの優先権を主張し、その開示内容全体を参照により本明細書に組み込む。

【背景技術】

【０００２】

コンピューティングリソース及び関連データのセキュリティは、多くの場合重要度が高い。実施例として、組織はコンピューティングデバイスのネットワークを使用し、組織のユーザに堅牢なサービスセットを提供する場合が多い。ネットワークは複数の地理領域に広がる場合が多く、他のネットワークと接続することも多い。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者に管理されたコンピューティングリソースの両方を用いて処理をサポートしてもよい。組織のコンピュータは、例えば、他組織のコンピュータと通信し、別組織のサービスを使いながらデータにアクセスし、及び／またはデータを提供してもよい。多くの場合、組織は他組織に管理されているハードウェアを用いてリモートネットワークを構成し操作し、それにより、インフラコストを削減し、その他の効果を実現する。そういったコンピューティングリソース構成であれば、特にそういった構成でのサイズ及び複雑さが増すにつれ、保有するリソース及びデータへのアクセスを確実にセキュアにすることが、求められる。

【０００３】

多くの場合、複数ソースからの暗号鍵は、セキュリティのためにコンピュータネットワークまたはシステムで使用されてもよく、例えば、データへの不正アクセスを防止するた

めに暗号化を使用する。しかしながら、確実に、信頼される鍵を使って暗号化処理を実施し、信頼されないエンティティ（例えば、ハッカ）に暗号鍵の使用が知られないことが求められる。

【０００４】

以下の図面を参照して，本開示による多様な実施形態を説明する。

【図面の簡単な説明】

【０００５】

【図１】多様な実施形態を実施可能な環境を示す。

【図２】多様な実施形態を実施可能な環境を示す。

【図３】一実施形態によるセキュリティポリシを示す。

【図４】一実施形態によるＴＲＵＳＫＥＹアクションを使った例示的なセキュリティ期待値の図である。

【図５】一実施形態による暗号化処理の実施要求を満たすプロセスを示す。

【図６】一実施形態による複数のセキュリティポリシ及び／または複数のセキュリティ期待値間におけるコンフリクトを解消するプロセスを示す。

【図７】多様な実施形態を実施可能な環境を示す。

【発明を実施するための形態】

【０００６】

以下の説明では、多様な実施形態を説明する。実施形態が十分理解されるよう、説明のために特定の構成及び詳細を設定する。しかしながら、当業者であれば、本特定詳細でなくても実施形態を実施できることは明らかであろう。さらに、周知の特徴は、説明する実施形態が不明瞭とならないよう省略または簡略化されてもよい。

【０００７】

本明細書に記載及び提案する技術では、暗号化されたリソースの復号及び妥当性確認など、データの妥当性確認に関する暗号化処理の実行にセキュリティ期待値を使用し、マルチテナント構成可能サービスの暗号化リソースを安全に管理することを含む。一実施形態では、マルチテナントのＡＰＩ構成可能暗号化サービスは、暗号化データの復号化及びデジタル署名検証などの暗号化処理の実施を求める要求（例えば、ＡＰＩ要求であり、ＡＰＩコールとも呼ばれる）をクライアントから受信するよう構成される。用語「デジタル署名」は、ＲＳＡ式デジタル方式（ＲＳＡ－ＰＳＳなど）、デジタル署名アルゴリズム（ＤＳＡ）及び楕円曲線デジタル署名アルゴリズム、ＥｌＧａｍａｌ署名方式、Ｓｃｈｎｏｒ署名方式、Ｐｏｉｎｔｃｈｅｖａｌ－Ｓｔｅｒｎ署名アルゴリズム、Ｒａｂｉｎ署名アルゴリズム、ペアリング式デジタル署名方式（Ｂｏｎｅｈ－Ｌｙｎｎ－Ｓｃｈａｃｈａｍ署名方式など）、否認不可デジタル署名方式などを用いて生成された情報を含むメッセージの真正性を暗号で検証するのに使用可能な情報を含むことに留意する。さらに、メッセージ認証コード（ハッシュベースメッセージ認証コード（ＨＭＡＣ）、鍵付き暗号ハッシュ関数、及び他の情報タイプも、デジタル署名として使用してもよい。

【０００８】

暗号化サービスは、サービス及びサービスを介してアクセス可能なデータのセキュリティ及び完全性を確保するため、多様な機構を採用してもよい。マルチテナント構成可能暗号化サービスで使用可能な機構は、セキュリティポリシを使用したものである。以下に詳述するように、セキュリティポリシ（簡略化して単にポリシという）は、データアクセスに関する権限、及び、コンピュータシステムにＡＰＩ要求の履行などの処理を実施させる権限など、コンピュータシステムにおける権限を定める情報である。いくつかの実施形態では、暗号化サービスにおいて暗号鍵を使用して、安全な通信及び／またはデータ保存の確実な実施など、多様な用途に暗号化処理を実施してもよい。暗号鍵（文脈上明白であれば「鍵」ともいう）をそういった環境で使用し、例えば、データの暗号化及び復号化、デジタル署名の生成、ならびに認証を実施してもよい。

【０００９】

いくつかの実施形態では、ＤＥＣＲＹＰＴ及びＶＥＲＩＦＹ＿ＳＩＧＮＡＴＵＲＥ　Ａ

ＰＩコールを実行するために実施する処理など暗号鍵を使用する処理は、さらに、対応する暗号化処理を実施するためには満たさなければならないセキュリティ期待値を指定してもよい。セキュリティ期待値は、要求（例えば、サービスプロバイダのカスタマから出され、及び／または許可されたＡＰＩコール）履行の一部として評価される条件または条件セットである。つまり、セキュリティ期待値は、どのようにＡＰＩコールを実行するかを示す。セキュリティ期待値は、機密保持の最小ビット数、ホワイトリストキーセット（例えば、信頼性のある暗号鍵セットであり、サービスプロバイダの別のカスタマに管理される暗号鍵のサブセットを含んでもよい）、ブラックリストキーセット（例えば、信頼性のない暗号鍵セットであり、サービスプロバイダの別のカスタマに管理される暗号鍵のサブセットを含んでもよい）、暗号鍵の失効日がそれ以前に設定される有効期限、暗号鍵の信頼性を評価する任意のコード、及び／またはそれらの組み合わせの、少なくとも一部に基づく条件を含んでもよい。セキュリティ期待値の条件は、いくつかの実施形態では、リクエスタが所定状態（例えば、連邦情報処理標準（ＦＩＰＳ）モード）にあることを示す（例えば、リモート証明などで表明し及び／または暗号により証明する）要求情報に照らし評価されてもよい。さらに、セキュリティ期待値は、セキュリティポリシのように、要求の履行を許可または拒否させてもよいが（例えば、復号鍵に信頼性が無くセキュリティ期待値が復号鍵の信頼性を要求する場合、復号化要求に対しプレインテキストの提供を実施しない）、より複雑なエフェクトも有し得る。例えば、セキュリティ期待値のエフェクトにより、妥当性確認に使用する暗号鍵の信頼性に応じて、デジタル署名の妥当性確認要求を変更してもよい。つまり、セキュリティ期待値の実行次第で異なる結果を返すなどして、セキュリティ期待値が同一のＡＰＩ要求を異なって実行させる可能性がある。

【００１０】

セキュリティ期待値を要求の主要目的に付属させてもよい。例えば、暗号化サービスは、デジタル署名の妥当性確認（検証）要求を受信してもよい。いくつかの実施例では、（例えば、セキュリティ期待値による要求が多くない場合）、デジタル署名の検証に使用する暗号鍵の信頼性に対する処理を実施せずにデジタル署名が正しいと検証して、要求を履行してもよい。他の実施例では、セキュリティ期待値は、デジタル署名が正しいこと、さらに、デジタル署名の検証に使用する暗号鍵が信頼性があると指定されたものであることの両方を検証するよう、デジタル署名の妥当性確認要求を求めてもよい（例えば、暗号鍵は信頼性のあるエンティティに関連するものとして暗号により検証可能であるため、及び／または、暗号鍵は期限のないデジタル証明書で指定されているため）。さらに、いくつかの実施形態において、論理演算子を使用して条件及び／または期待値を組み合わせ、論理演算子と併せて集計条件及び／または期待値成分の少なくとも一部に基づく結果をもたらす、集計条件及び／または期待値を形成してもよい。集計条件は、複数の集計段階を順に含み、複雑なマルチレベルの集計条件及び／または期待値を形成してもよい。

【００１１】

いくつかの実施形態では、例えば、暗号鍵を用いた処理の実施要求の一部として提供された追加情報の一部に、クライアントがセキュリティ期待値を提供するか、あるいは指定してもよい。他の実施形態では、要求を出すプリンシパルにセキュリティ期待値を関連づけ、セキュリティ期待値セットが、プリンシパルに使用される暗号鍵全てに適用されるようにしてもよい。さらに他の実施形態では、セキュリティ期待値を、アカウントに関連づけるか、要求コンテキストから決定可能であってもよい。本実施形態は、必ずしも互いに異ならず、及び／または、相互に排他的でないことに留意する。つまり、セキュリティ期待値が要求に明示された実施例もあるが、要求の情報を使用してセキュリティ期待値を適用するかを決定し、適用すると決定した場合にセキュリティ期待値を適用してもよい実施例もある。

【００１２】

セキュリティ期待値は、クライアントにより暗号化サービスに提供されるか、または暗号化サービスにより（例えば、コンピューティングリソースを管理するウェブサービスＡＰＩコールを介して）一元管理されてもよい。いくつかの実施形態では、セキュリティ期

待値は、暗号化サービスによりアクセス可能で一元管理されたリポジトリに保存され、暗号化サービスによりアクセス可能なポリシ管理モジュールに管理される。ポリシ管理モジュールは、暗号化サービスによりアクセス可能なソフトウェア、ハードウェア、または、ハードウェア及びソフトウェアの組み合わせであってもよく、いくつかの実施形態では、コンピューティングリソース（例えば、ＣＰＵ、仮想マシンインスタンス）及びデータ記憶装置の両方を備えるフロントエンドシステムの一部であってもよい。コンピューティングリソースを使って、少なくとも部分的に期待値を評価し、セキュリティ期待値及び／またはポリシデータを検索し、セキュリティ期待値の一部として含まれる実行可能なコードを実行してもよい。

【００１３】

さらに、いくつかの実施形態において、セキュリティ期待値が、暗号化サービスによりアクセス可能なポリシ管理モジュールにより一元管理される場合などでは、セキュリティの危殆化に対してレジリエンスが高く、ユーザ（カスタマ）は恩恵を受ける。一実施例として、特定の暗号鍵が危殆化されたことが判明した場合、ポリシ管理モジュールは、当該鍵をブラックリストに載せてもよい（すなわち、全てのセキュリティ期待値評価に自動的にフェイルする鍵セットに当該危殆化暗号鍵を含める）。これとは対照的に、セキュリティ期待値がクライアントにより要求の一部として暗号化サービスに提供される実施形態では、危殆化暗号鍵を使う可能性のある全クライアントに、当該危殆化暗号鍵をブラックリストに入れるようアップデートを要求してもよい。

【００１４】

いくつかの実施形態では、暗号化サービスにより、使用前に暗号鍵を信頼するという要件をプログラム的に構成できるようにしてもよい。本明細書において、「信頼」とは、暗号鍵を信頼するかどうかに依存したコンピュータシステム処理をいう。例えば、信頼された暗号鍵を使って暗号化サービスから取得可能なデータを暗号化するが、信頼された暗号鍵であると決定されていない暗号鍵を使って暗号化サービスからアクセス可能なデータを暗号化しないよう、コンピュータシステムを構成してもよい。一般的に、コンピュータ実施方法での出力は、信頼性のある暗号鍵であると指定されているかどうかに依存する。

【００１５】

クライアントに使用可能になる前に暗号鍵を信頼することを暗号化サービスが求める実施形態では、様々な利点がある。当該利点には少なくとも、暗号化サービスを使用するコンピューティング環境のデータは、単純に無効状態か有効状態かのいずれかであることを含む。対照的に、より複雑なシステムでは、デジタル署名は正しいが、信頼性のある暗号鍵を使っても検証できない場合など、データが複数の他の状態にある可能性もある。無効状態には少なくとも、暗号化されたデータまたはデジタル署名が（例えば、悪意のある者に、または間違って）変更されて完全でないと検出された状態、または、データは変更されていない（すなわち、完全である）が、信頼性が無いか、危殆化されているか、もしくはそうでなくてもクライアントが相手方を信頼する基準を満たしていないと判明している相手方の暗号鍵を使うという状態がある。信頼されないデジタル署名であることを検証するのに暗号鍵が使用可能であるため、正しく署名されたデータではあるが信頼されない場合など、有効性について中間的な状態での不注意な使用を回避するよう、本開示による暗号化サービスを構成可能である。

【００１６】

いくつかの実施形態において、デフォルトではクライアントは、限られた暗号鍵セットのみ信頼する。例えば、クライアントは、デフォルトでは当初、クライアント内のアカウントのいずれかからの、クライアントの特定アカウントからの、またはクライアントの特定暗号鍵からのデータのみを信頼してもよい。上記の実施形態では、第三者からの暗号鍵（すなわち、他のクライアントから暗号鍵）は信頼されず、クライアントは暗号化処理に使用できない。アプリケーションプログラミングインタフェースコールを使用して暗号化サービスを構成し、クライアントが信頼する暗号鍵に従い暗号化処理を実施してもよい。

【００１７】

図１は、多様な実施形態を実施可能な環境１００を示す。図の環境１００では、暗号化サービス１０６に対し暗号化処理の完了を求める要求１０４を出すクライアント１０２、及び、要求に対する応答１０８を示す。図中、処理１０４はＶＥＲＩＦＹ＿ＳＩＧＮＡＴＵＲＥ処理であり、クライアントがデジタル署名１１０及びセキュリティ期待値１１２を提供する。処理を実施して要求を満たすために、暗号化サービスは、真正性の決定に使用する鍵の真正性及び信頼性の両方について、デジタル署名を検証し得る。応答では、例えば、デジタル署名を正しいと決定したかどうかを明示してもよい。正しいと決定した場合の応答に、他の情報を含めてもよく、例えば、デジタル署名の正確性の検証に使用するデジタル証明書の認証に成功したかどうか、デジタル署名の検証に使用する暗号鍵に信頼性があるかどうか、デジタル証明書が失効していないかどうか、及び／または、デジタル署名が真正であるかどうかの確認に追加して実施される確認の結果得られた他の情報などがある。説明上、ＶＥＲＩＦＹ＿ＳＩＧＮＡＴＵＲＥを使用するが、ＤＥＣＲＹＰＴなど他の暗号化処理を使用してもよいことに留意する。クライアント１０２は、本明細書で説明する多様な処理を（例えば、実行可能なコードを用いて）実施するよう構成されたコンピュータシステムであってもよい。クライアントは、クライアントアプリケーション、オペレーティングシステム、または、本明細書で論じるように動作するよう構成可能な他の適切なソフトウェア、ハードウェア、もしくはそれらの組み合わせに応じて動作してもよい。

【００１８】

一実施形態では、デジタル署名の検証を求める要求１０４は少なくとも、検証するデジタル署名、デジタル署名が生成されたとするメッセージを含み、いくつかの実施形態では、署名を検証するために暗号鍵を備えるかあるいは指定（例えば、識別子により）してもよい。いくつかの実施形態では、要求は暗号鍵を含まず、また指定しないが、暗号化サービスによる暗号鍵の選択に使用可能な情報を含んでもよく、例えば、要求を出すか、暗号化サービスが管理する複数の暗号鍵からの暗号鍵の選択に使用可能な他の情報を出すエンティティの識別子を含み、暗号化サービスが暗号鍵を選択できるようにしてもよい。実施例として、コンピューティングリソースサービスプロバイダのカスタマは、デフォルトで使用する関連暗号鍵を有してもよい。

【００１９】

鍵の識別子は、一意の識別子であってもよいが、必ずしも一意でなくてもよいことに留意する。例えば、鍵の識別子は、暗号鍵の系列を識別してもよい。例えば、いくつかの実施形態では、キーローテーションを実施する。キーローテーションでは鍵を他の鍵に交換して、使用暗号を実質的にクラック可能にするのに十分な復号化データが収集されないようにしてもよい。さらに、鍵の識別子が一意に鍵を識別しない場合、多様な技術を採用して適切な機能を有効にしてもよいことに留意する。例えば、多様な実施形態において、鍵の識別子で識別される鍵の系列は有限である。鍵の識別子で識別される鍵を使用する復号化処理が要求された場合、データ（例えば、暗号化実施の際のタイムスタンプ）を追加して、使用に適した鍵を決定できるようにしてもよい。いくつかの実施形態では、暗号文は、鍵バージョンを示す情報を含んでもよい。いくつかの実施形態では、可能性のある鍵全てを使用して、ハッシュ化された多様な復号化データを提供し、結果得られたハッシュを保存されたハッシュと比較して、使用する鍵を識別してもよい。鍵数は有限であるため、適切な復号を提供された中から選択してもよい。いくつかの実施形態では、認証済の暗号化を用いるなどして、鍵の少なくとも一部に基づいて暗号文が生成されていないことを暗号化サービスが検出できるよう、鍵を使った復号化を実施する。また、他の変形も、本開示の範囲内であると考えられる。

【００２０】

暗号化サービス１０６は、クライアントから要求を受信し、要求に応答して、データの正確性及び信頼性に基づき、また、要求の一部として提供されたメタデータの少なくとも一部に基づき、要求の処理方法を決定してもよい。暗号化サービスは一連の処理１１４を実施し、デジタル署名１１０の正確性及び信頼性、ならびに要求の処理方法を決定しても

よい。デジタル署名（文脈上明白であれば単に署名ともいう）は、デジタルメッセージの真正性を示し、メッセージが特定の既知の送信者により作成されたこと（認証）、送信者がメッセージを送信したことを否定できないこと（否認防止）、及び、メッセージが転送中に変更されていないこと（完全性）を保証するのに使用可能な情報である。現在使用されているデジタル署名には、多様なバージョンの公開キー暗号化標準（ＰＫＣＳ）及びデジタル署名アルゴリズム（ＤＳＡ）がある。一連の処理１１４は、少なくとも、暗号鍵の選択１１６、プリンシパルに適用するセキュリティポリシを満たしているかどうかの決定１１８、暗号鍵に適用されるセキュリティ期待値を満たしているかどうかの決定１２０、及び、要求に対する応答作成１２２のステップを含んでもよい。暗号化サービスは、場合により互いに共有することもある同一アカウントの複数のユーザからのデータを含むか当該データへのアクセスを有してもよく、逆に、データを互いに共有すべきでない複数の独立したカスタマからのデータを含んでもよい。そういった構成では、例えば、コンピューティングリソース及び／または保存リソースの最適化、レイテンシ低減、帯域幅増大などが望ましい場合がある。いくつかの実施形態において、カスタマは、動的にコンピューティングリソースに割り当てられ（例えば、システム全体のコンピューティングリソースの可用性に基づいて）、当該カスタマは、他のコンピューティングリソースに再割り当てされ得る（例えば、システム全体のコンピューティングリソースの可用性の変更に基づいて）。

【００２１】

暗号鍵の選択１１６は、要求１０４のコンテキストの少なくとも一部に基づいてもよい。多様な実施形態において、要求１０４は、鍵の識別子を指定する追加パラメータを含み、及び／または、鍵の識別子は、コール側クライアントまたはコール側クライアントに関連するアカウントに基づいて導出されてもよい。追加してまたは代替的に、暗号鍵は、要求１０４に含まれクライアントにより暗号化サービスに提供されてもよい。

【００２２】

プリンシパルに適用するセキュリティポリシを満たしているかどうかの決定１１８では、１以上の適用セキュリティポリシを識別し取得し（例えば、１以上の適用セキュリティポリシを符号化する１以上の電子文書を取得して）、適用セキュリティポリシを満たしているかどうかを評価してもよい。プリンシパルに適用するセキュリティポリシは、ポリシ管理モジュール１２４から取得されてもよく、かつ、要求を出すクライアント、及び／または、要求の一部として提供される情報の少なくとも一部に基づいてもよい。いくつかの実施形態では、プリンシパルは、デフォルトで、クライアント（例えば、クライアントに関連付けられたマシン、アカウント、またはユーザ）のアイデンティティに関連付けられているが、デフォルトでの関連付けは、要求の一部として提供される追加情報に基づいて上書きされてもよい。

【００２３】

一実施形態では、ポリシ管理モジュール１２４は、セキュリティポリシの保存及び検索を管理し、セキュリティポリシをプリンシパルに関連付けるプログラミングロジックで構成されたコンピュータシステムである。いくつかの実施形態では、セキュリティポリシは、セキュリティポリシに保存されたデータの一部として、ポリシをプリンシパルに関連付ける情報を含んでもよい。他の実施形態では、セキュリティポリシからプリンシパルへのマッピングは、例えば、キー／バリューペアの鍵が一意に１つのプリンシパルとなるような連想配列を使用して、または、関連プリンシパルレコードと一致する外部キーフィールドをセキュリティポリシレコードが含むリレーショナルデータベースを使用して、実施されてもよい。いくつかの実施形態では、さらにグループポリシを設定し、セキュリティポリシを複数のプリンシパルに適用してもよい。一般的に、ポリシ管理モジュール１２４は、要求に関連する情報（例えば、要求内の情報、ならびに／または、要求のコンテキスト情報及び要求外で決定されるコンテキスト情報）を使用するよう構成される。ポリシ管理モジュールから適用セキュリティポリシを取得すると、暗号化サービスは適用セキュリティポリシを満たしているかどうかを評価してもよい。

【００２４】
いくつかの実施形態では、適用セキュリティポリシは、コール側クライアントとは違うプリンシパルに関連付けられてもよい。例えば、いくつかの実施形態では、クライアントは、適用セキュリティポリシを識別する際に異なるアクタの適用セキュリティポリシを使用すべきであると示す追加情報を要求で提供してもよい。例えば、クライアントは、要求の一部に第２クライアントからのデジタル署名トークンを含めてもよく、トークンは、第２クライアントが第２クライアントのセキュリティポリシに基づいた要求発行を第１クライアントに許可することを示す情報を含む。そういった構成では、プリンシパルは、第１（コール側）クライアントではなく、第２クライアントとなる。他の実施形態では、プリンシパルがコール側クライアントでなくてもよい。

【００２５】
暗号鍵に適用するセキュリティ期待値を満たしているかどうかの決定１２０では、１以上の適用セキュリティポリシを識別し取得し、適用セキュリティ期待値を満たしているかどうかを評価してもよい。多様な実施形態では、暗号鍵に適用するセキュリティ期待値は、暗号化サービスにより、ポリシ管理モジュールにより、及び／または、本明細書に記載する技術を実施するよう構成された１以上のサービスを実施するよう構成されたセキュリティチップ（ＴＰＭ）もしくは他のデバイスなど、暗号化材（例えば、ハードウェアトークン）のハードウェアベースのプロテクト機能を有するハードウェアまたは他のセキュリティモジュール（ＨＳＭ）もしくは他のデバイスなどの別個のハードウェアコンポーネントにより、識別され、取得され、及び評価されてもよい。

【００２６】
いくつかの実施形態では、要求に対する応答作成１２２は、適用セキュリティ期待値を満たしているかどうかの少なくとも一部に基づいて行う。セキュリティ期待値を満たしている場合、暗号化サービスはセキュリティ期待値に従い要求を履行してもよい。セキュリティ期待値の評価では、暗号化処理の実施に使用する暗号鍵を信頼すべきかどうか決定してもよく、評価には多様な処理モードがあってもよい。処理モードによって、暗号鍵の信頼性をどのように評価するかが異なる。いくつかの実施形態では、処理モードは要求内に指定されてもよく、または、暗号化サービスにより設定されてもよい。

【００２７】
図２は、多様な実施形態を実施可能な環境２００の実施例を示す。一実施形態では、クライアント２０２（リクエスタともいう）は、ポリシ実施モジュール２１０及び期待値評価エンジン２１２を備えるフロントエンド２０６を備えるコンピュータシステムである暗号化サービス２０４に要求を出してもよい。フロントエンド２０６は、認証ホスト２０８に、及び、ポリシ構成２２０を取得し作成し削除し更新するよう構成されたポリシ管理モジュール２１６にアクセスするよう構成されたコンピュータシステムである。また、暗号化サービスは、１以上のハードウェアセキュリティモジュール（ＨＳＭ）を備えたバックエンド２１４システムを備えるが、分かり易くするため図には１つのＨＳＭ２１８を示す。例示的な暗号化サービスは、参照により本明細書に組み込む「Ｄａｔａ　Ｓｅｃｕｒｉｔｙ　Ｓｅｒｖｉｃｅ」と題され２０１３年２月１２日に出願された米国特許出願第１３／７６４，９６３号に記載されている。

【００２８】
一実施形態では、サービスフロントエンドホスト２０６は、１以上のクライアントから要求を受信し、認証ホスト２０８と通信して要求の処理方法を決定する。認証ホスト２０８は、コンピュータシステム、コンピュータシステムプロセス、プログラムアプリケーション、サービスモジュール、または、これら及び／もしくは他のそういったコンピューティングシステムエンティティの組み合わせであってもよい。認証ホスト２０８を暗号化サービスにより利用し、フロントエンド２０６に出された要求を処理するか及び／または処理方法を決定してもよい。認証ホストは、例えば、暗号化サービスに出された要求のデジタル署名を検証してもよく、あるいは、要求の履行が許可されているかどうかを決定してもよい。さらに、説明では本開示全体でカスタマ／プロバイダの関係を論じているが、本

明細書で説明する技術は、カスタマが暗号化の内部カスタマ２０２（例えば、サービスプロバイダ２０２の別のサービス）である場合など、他のコンテキストに適応可能である。

【００２９】

ポリシ管理モジュール２１６は、適用する場合、ポリシに関する情報及びポリシ自体を提供するよう動作可能な暗号化サービスのサービスまたはサブシステムの実施例である。ポリシ管理モジュールは、ポリシ構成２２０を作成、変更、削除、コピー、または伝播するよう動作可能であってもよい。例示的なポリシ構成（一例にポリシドキュメントがあり、文脈上明白な場合ポリシともいう）を、以下図３に詳述する。図２に戻るが、ポリシ実施モジュール２１０などフロントエンド２０６の構成要素は、アプリケーションプログラミングインターフェイス（ＡＰＩ）を使用して、ポリシ管理モジュール２１６と、さらにはポリシ構成２２０と対話してもよい。いくつかの実施形態では、クライアント要求は、ポリシ管理モジュールに直接送られてもよいが、他の実施形態では、フロントエンドまたは構成要素（例えば、認証ホスト）は、クライアント要求を解析し、ポリシ管理モジュールが受け入れ可能なフォーマットで要求を生成し、ポリシ管理モジュールに当該要求をディスパッチしてもよい。図２では、ポリシ管理モジュールは、フロントエンド及びバックエンドの双方と分離されたサービスとして実施されている。しかしながら、ポリシ管理モジュールは、他の実施形態では、バックエンド２１４の一部として実施されてもよい（すなわち、ポリシ構成へのアクセスを、中間サービスではなくバックエンド２１４に向ける）。そういった実施形態では、バックエンド２１４に向けた要求は、なおポリシ管理モジュールにより実施される。

【００３０】

ポリシ構成２２０は、ユーザ、セキュリティ管理者、システム管理者、または該当する権限を有する他のプリンシパルにより作成、変更、コピー、削除、または継承されてもよい。いくつかの実施形態では、プリンシパルがポリシを作成、変更、コピー、削除、または継承するのに十分な権限を有しているかどうかは、プリンシパルが作成、変更、コピー、削除、または継承を試みるポリシに基づいてもよい。例えば、セキュリティ管理者は、ゲストユーザによるリソースへのアクセスを拒否するようポリシを作成するのに十分な権限を有してもよく、ゲストユーザは、セキュリティ管理者によるリソースへのアクセスを拒否するポリシを作成するのに十分な権限を有していなくてもよい。任意の標準的な、分散された、仮想のまたはクラスタ化された環境において、データサーバ、データベース、データ記憶デバイス、及びデータ記憶媒体を任意に組合せと任意の数とを含む多様なコンピュータベースハードウェア、及び／またはソフトウェアコンポーネントを使用して、ポリシ構成を記憶してもよい。

【００３１】

一実施形態では、サービスフロントエンドホスト２０６がカスタマネットワーク２０２からの要求を受信すると、サービスフロントエンドホスト２０６は、認証ホスト２０８に認証要求を出し、認証ホスト２０８は認証応答及び要求に適したポリシセットを指定する情報を出し、一実施形態では、認証応答は、サービスフロントエンドホスト２０６への要求が真正かどうか（例えば、当該要求のデジタル署名の検証に成功したかどうか）を指定する。ポリシセットを受信すると、サービスフロントエンドホスト２０６は、ポリシ実施モジュールを利用して、要求を履行すべきか否かなど要求の処理方法を決定してもよい。さらに、要求を少なくとも部分的に履行すべきであると決定すると、期待値評価エンジン２１２を使用して、どのように要求を履行するかを決定してもよい。期待値評価エンジンを使って、クライアント及び／または暗号化サービスにより（例えば、適用ポリシ構成により）提供されるセキュリティ期待値に従い要求を評価してもよい。

【００３２】

期待値評価エンジンは、フロントエンドの構成要素として図示されているが、バックエンド２１４の一部として含まれてもよく、または、ＨＳＭ２１６もしくは暗号化材のハードウェアベースプロテクト機能を有する他の適切なデバイスの一部として含まれてもよい。ポリシをポリシ管理モジュール２１６から受信すると、サービスフロントエンドホスト

２０６は、ポリシ実施モジュールに当該ポリシを提供して、要求の処理方法（例えば、ポリシが要求履行を許可するかどうか、及び／または、履行の進め方）を評価してもよい。ポリシ実施モジュール２１６は、デフォルトポリシの実施（例えば、明示的に定められたポリシが無い場合の履行の進め方の決定）、及び複数のポリシ間のコンフリクトが要求処理にどのように影響するかの決定（例えば、複数のポリシを適用する場合の履行の進め方の決定）など、ポリシの認証に関連する多様なタスクを実施してもよい。いくつかの実施形態では、ポリシ管理モジュールは、ポリシセット及び要求コンテキストを受信し、それに応答して、要求の履行方法の決定（例えば、要求を許可するか拒否するか）を提供してもよい。

【００３３】

バックエンド２１４は、暗号鍵を保存し取得するよう動作可能であり、少なくともハードウェアセキュリティモジュール（ＨＳＭ）、または、暗号化材（例えば、ハードウェアトークン）のハードウェアベースの保護機能を有する他のデバイスを備えてもよい。バックエンドは、マルチテナントシステム内の複数のクライアントからの暗号鍵を保存し取得してもよく、１つのクライアントの暗号鍵は、デフォルトでは、システム内の他のクライアントにアクセスできない。

【００３４】

図３は、一実施形態によるポリシドキュメントの実施例（例示的なポリシ構成）を示す。一実施形態では、ポリシドキュメント３００は、ポリシドキュメントにより符号化されたポリシに関連する多様な情報を符号化する。ポリシは、ｅＸｔｅｎｓｉｎｂｌｅ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（ＸＡＣＭＬ）、Ｅｎｔｅｒｐｒｉｓｅ Ｐｒｉｖａｃｙ Ａｕｔｈｏｒｉｚａｔｉｏｎ Ｌａｎｇｕａｇｅ（ＥＰＡＬ）、Ａｍａｚｏｎ Ｗｅｂ Ｓｅｒｖｉｃｅｓ Ａｃｃｅｓｓ Ｐｏｌｉｃｙ Ｌａｎｇｕａｇｅ、Ｍｉｃｒｏｓｏｆｔ ＳｅｃＰｏｌ、または、履行する要求について満たさなければならない１以上の条件の任意の適切な符号化方法など、宣言的アクセス制御ポリシ言語で符号化されてもよい。図３に示すように、ポリシドキュメント３００は、文字列を含むポリシドキュメント３００の名称３０２を含む。名称３０２を使用して、例えば、人による読み取りが可能な用語を使用して有意な識別子を提供してもよい。一実施例として、名称３０２は、例えば「ＭｙＤａｔａＳｔｏｒａｇｅＰｏｌｉｃｙ」という趣旨の文字列であってもよい。また、図３に示すように、ポリシドキュメント３００は、バージョン３０４を含んでもよい。多様な要求が受信され履行されてポリシをアップデートする間、ポリシドキュメント３００が時間とともにどのように変化するかを、バージョン３０４を使って追跡してもよい。ポリシドキュメント３００を更新する度、バージョン３０４は新しい値に更新されてもよい。また、ポリシドキュメント３００は、現行バージョンを備えるポリシドキュメント３００を作成させることとなった要求を出したユーザの識別子である発行者３０６を指定してもよい。図３に示し上記したように、ポリシドキュメント３００は、１以上のステートメント３０８を含んでもよい。ポリシドキュメントのステートメントは、論理和を使用して処理されてもよい。

【００３５】

上記のように、ステートメントは、許可を形式的に記述したもの、または一般的に、１以上のリソースへの１以上のアクセス条件を形式的に記述ものであってもよい。したがって図３は、上述したように、ポリシドキュメントに符号化される場合があるステートメント３０８の実施例を示す。図３に示すように、ステートメント３０８は、１以上のプリンシパル３１０を識別する情報を含んでもよい。プリンシパルは、ステートメント３０８を適用するエンティティ（例えば、ユーザ、ユーザグループ、ユーザクラス、コンピュータシステム、または、システム内のシステムもしくはリソースへのアクセス許可を与える任意のエンティティ）であってもよい。

【００３６】

一実施例として、コンピューティングリソースサービスプロバイダのカスタマは、アカウントを有してもよい。アカウントは複数のサブアカウントに関連付けられ、各サブアカ

ウントは、カスタマの１ユーザに対応してもよい。各ユーザは、ステートメントのプリンシパルとして備えられ得る対応識別子を有してもよい。また、プリンシパルは、他の方法で識別されてもよい。例えば、プリンシパルセットは、当該セットの識別子で識別されてもよい。例示的な実施例として、組織内の１部門は、１つの対応識別子を有してもよい。ステートメント内に部門の識別子を挙げ、１つのステートメントを当該部門に関連する複数ユーザに適用してもよい。プリンシパルセットの識別子は、例えば、従業員が組織及び／または組織の部門に雇用される、及び／または、退職する場合など、プリンシパルセットが動的に変更されている場合に、有用となってもよい。

【００３７】

一般的に、プリンシパルセットは、少なくとも一部のプリンシパル特性に基づいて定められてもよい。また、プリンシパルの識別子は拡張可能であってもよい。例えば、誰にでも、すなわち、コンピューティングリソースサービスプロバイダのアカウントに代わり要求を出すことができる全てのユーザ、または一般的には全てのユーザに、ステートメント３０８を適用することを示す情報が含まれてもよい。いくつかの実施形態では、ステートメントは少なくとも、プリンシパル３１０、リソース３１２、アクション３１６、及びエフェクト３１８を特定しなければならない。セキュリティポリシに記述されたプリンシパルは、例えば、ユーザ、グループ、ドメイン、サービス、コンピュータ、人、プロセス、スレッド、環境、または、暗号化サービスによる認証が可能な他のタイプのエンティティであってもよい。プリンシパルの実施例には、アクタセット（例えば、複数ユーザ、または「管理者」などのユーザグループ）、多様なアクタタイプを含むセット（例えば、ユーザ及びドメインを含むセット）、またはそれらの任意の組み合わせがあってもよい。プリンシパルは、プリンシパルのプロパティに基づいてヒューリスティックに記されてもよく、例えば、ポリシのプリンシパルには、安全なトランスポートレイヤセキュリティ（ＴＬＳ）接続を介して暗号化サービスに接続されたエンティティがあってもよい。

【００３８】

説明するリソースは、ポリシが適用される場合があるコンピュータベースのリソースであってもよい。ポリシに記載されるリソースには、コンピューティングリソース（例えば、プロセッサ、コンピューティングクラスタ）、コンピュータストレージ（例えば、コンピュータファイル、コンピュータディスクドライブまたはパーティション、物理ハードドライブ、磁気テープデータストレージ）、暗号化リソース（例えば、暗号鍵）、コンピュータオペレーション（例えば、ＡＰＩまたはＡＰＩセット）、及びシステムリソース（例えば、同期プリミティブ）など多様なタイプのコンピューティングリソースがあるが、これらに限定されない。プリンシパルと同様に、ポリシに指定されるリソースは、単体リソース（例えば、ファイル）、リソースセット（例えば、任意のファイルリスト）、リソースタイプの組み合わせ（例えば、コンピュータファイル及びプロセッサ）、またはそれらの任意の組合せに適用されてもよい。ポリシのアクションは、ポリシで指定されたリソース上でアクタによる実施が許可されたアクションまたはアクションセットを指定する。アクションは、例えば、１つのＡＰＩコール（例えば、論理コンテナに保存された全てのデータのリストを提供する「ＬｉｓｔＤａｔａ」ＡＰＩ）など特定の単体アクションであってもよく、アクセスレベル（例えば、「ＬｉｓｔＤａｔａ」を含む全ての読み取り処理が含まれた「読み取り」アクセス）、またはその組み合わせを示してもよい。

【００３９】

図３に示すように、ステートメント３０８は、１以上のリソース３１２を識別する。リソースは、上記のようなコンピューティングリソースであってもよい。リソースは、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により提供されるサービスのサブジェクトであってもよい。一実施例として、リソースは、仮想コンピュータシステムであってもよく、複数のデータオブジェクトの関連付けに使用する論理データコンテナであってもよく、ブロックレベルデータ記憶デバイスのボリューム識別子、データベース、データベースに保存されるアイテム、データオブジェクト（例えば、ファイル）、及び、サービスとして提供される場合がある一般的に任意のタイプのリソースであってもよい。いくつ

かの実施形態では、リソースは暗号鍵であり、カスタマもしくは他のエンティティ（例えば、ユーザ、ロール、グループなど）に代わり暗号化サービスにより管理される暗号鍵、及び／または、１以上のデータストレージサービス用のデフォルトキーとして使用する暗号鍵などがある。プリンシパルと同様に、リソースは、リソースの特性の少なくとも一部に基づき定められる場合があるリソースセットの識別子を使用して記述されてもよい。例えば、いくつかの実施形態では、仮想コンピュータシステムは、仮想コンピュータシステムにより実行されたロールを記す場合があるユーザ生成タグに関連付けることができる。一実施例として、仮想コンピュータシステムグループは、「ウェブサーバ」タグに関連付けられてもよい。したがって、リソースは、そういったタグにより識別されてもよい。別の実施例として、リソースは論理データコンテナに対応し、それにより、論理データコンテナ内に保存された、すなわち論理データコンテナに関連する任意のデータオブジェクトにステートメント３０８を適用するようにしてもよい。また、リソース（例えば、データオブジェクト）は、リソースの暗号化に使用する鍵で定められてもよい。上記に加えて、ポリシを適用するオブジェクト（例えば、プリンシパル及びリソース）は、セキュリティアサーションマークアップ言語（ＳＡＭＬ）を使って送信される属性、及び／または、ディレクトリを使用して決定される属性の少なくとも一部に基づいてもよい。

【００４０】

図３に示すように、ステートメント３０８は１以上の条件も含んでもよい。一実施形態では、条件は、ポリシドキュメント内のステートメントを特定のコンテキストに適用するかどうか、すなわち、コンテキスト内で出された要求に適用するかどうか、を決定する。上記条件では、ブール演算子（ｅｑｕａｌ、ｌｅｓｓ　ｔｈａｎなど）を使って、ステートメント内の他の値（プリンシパル、リソースなど）及び認証コンテキスト内の他の値に対し条件を評価できるようにしてもよく、認証コンテキスト内の他の値は、ポリシが評価される要求に提供されても提供されなくてもよい。条件値には、日付、時間、リクエスタのインターネットプロトコル（ＩＰ）アドレス、要求元の識別子、ユーザ名、ユーザ識別子、及び／または、リクエスタのユーザエージェントなどの値を含めることができる。また、値は、条件が適用されるサービスに固有であってもよい。ＡＮＤやＯＲなどの論理コネクタを使用して、評価のために条件を論理的に繋げてもよい。

【００４１】

また、ステートメントは、１以上のアクション３１６を符号化してもよい。一実施形態では、アクションは、サービスプロバイダにより実施可能な処理である。一実施形態では、アクションは、サービスプロバイダによりサポートされたＡＰＩコールに対応する（すなわち、サービスプロバイダに対し出される可能性があり、サービスプロバイダが実行する場合があるＡＰＩコール）。また、指定されたアクションは、ＡＰＩコール（おそらく多種多様あるＡＰＩコール）の実行の一部として実施される処理であってもよく、一部のＡＰＩコールでは他の処理も実施されてもよい。例えば、ＡＰＩコールの実行では、複数の処理を実施し、ポリシに複数処理のうち１以上をアクションとして指定してもよい。

【００４２】

図３に示すように、ステートメント３０８は、１以上のエフェクト３１８も含んでもよい。一実施形態では、エフェクトは、要求に対し期待値される結果を決定し、ポリシのアクタは、ポリシで指定された処理を同一ポリシで指定されたリソース上での実施を試みる。エフェクトは、リソースにアクセスする際の処理を単に「ＡＬＬＯＷ（許可）」または「ＤＥＮＹ（拒否）」してもよい。例えば、ポリシドキュメント３００により符号化されたポリシを復号化要求に適用する場合、ステートメント３０８の条件が成立することで、エフェクト３１８に従って要求の履行を許可または拒否してもよい。２つの異なるステートメントが同時に履行可能なステートメントを含み、当該２つのステートメント間でエフェクトが異なる時、コンフリクト解消ルールをインスタンスに適用してもよい。例えば、明確にポリシで許可しない限り、デフォルトでは拒否としてもよく、明示的拒否は明示的許可より優位、またはその逆となるよう、システムを構成してもよい。コンフリクト解消を含む例示的な方法は、図６を参考に以下で論じる。明示的なエフェクト（例えば、明示

的許可または明示的拒否）とは、ポリシで符号化されたエフェクトである。

【００４３】

図４は、ＴＲＵＳＴＫＥＹアクションを用いて暗号鍵の使用を認可する例示的なセキュリティポリシを示す。分かり易くするため、ポリシドキュメント４００は、プリンシパル、リソース、アクション、及びエフェクトのみで示されているが、ポリシドキュメントは、図３で上述したように追加情報を含んでもよい。ＴＲＵＳＴＫＥＹアクション４０６は、ポリシドキュメントで指定されたエフェクト４０８に基づいて暗号化処理を実施する際に、ポリシドキュメントで識別されたプリンシパル４０２に、リソース４０４の使用を許可または拒否する。いくつかの実施形態では、ポリシドキュメント４００で指定されたリソース４０４は、暗号鍵、及び、暗号化ファイルまたは暗号化メディアストレージなど暗号鍵と併せて使用可能な他のリソースを含んでもよい。ＴＲＵＳＴＫＥＹアクションはＴＲＵＳＴＫＥＹ　ＡＰＩコールに対応する場合がある実施形態もあるが、ＴＲＵＳＴＫＥＹアクションは別のＡＰＩコール（すなわち、追加アクションを有する別のＡＰＩコール）の一部である実施形態もあることに留意する。

【００４４】

いくつかの実施形態では、クライアントは、暗号化サービスにＴＲＵＳＴＫＥＹアクションを介して、信頼性のある暗号鍵セットに暗号鍵を追加して含んでもよい。ＴＲＵＳＴＫＥＹアクションは、少なくとも、データの暗号化及び復号化、ならびに、デジタル署名の生成及び妥当性確認などの暗号化処理を含む、多様な処理を実施するためにクライアントが信頼を望む暗号鍵または暗号鍵セットを少なくとも記述する。信頼性のある暗号鍵のみを使って、暗号化処理を実施してもよい。また、いくつかの実施形態では、ＴＲＵＳＴＫＥＹ処理は、ＴＲＵＳＴＫＥＹ処理が暗号鍵を信頼性があると識別するためには満たさなければならない条件を含んでもよい。いくつかの実施形態では、ＴＲＵＳＴＫＥＹ処理（または、暗号化処理の結果を信頼するかどうかの決定に関連して使用する他の処理）を実行する際に使用する条件では、暗号鍵に固有なプロパティを使用してもよい。暗号鍵に固有なプロパティは、鍵サイズ、及び、鍵自体から決定され得る他の情報を含んでもよい。

【００４５】

図５は、上記の実施形態における要求を処理するプロセス５００の実施例を説明する。プロセス５００は、上記のようなフロントエンドを実施するウェブサーバなど暗号化サービスもしくは暗号化サービスの構成要素など任意の適切なシステムにより、または、アプリケーションサーバ及び／もしくはセキュリティモジュールと連携したウェブサーバにより、実施されてもよい。説明上、プロセスを図２に記載したような暗号化サービスに関連して説明したが、暗号化サービスを実施するためのコンピューティングリソースの他の構成も、本開示の範囲内にあるとみなす。暗号化サービスは、暗号化処理を実施するよう要求を受信してもよい（５０２）。いくつかの実施例では、要求はウェブサービス要求であるが、他のＡＰＩコールを本開示の範囲内であるとみなす。さらに、いくつかの実施形態では、ハードウェアデバイスによりプロセス５００またはその処理のサブセットを実施してもよく、当該ハードウェアデバイスは、例えば、ＨＳＭ、または、暗号鍵のハードウェア保護機能を提供し、いくつかの実施形態では、プレインテキスト形式に暗号鍵のエクスポートができない他のデバイスである。プログラムによってデバイスに情報提供をさせる（例えば、デバイスのインタフェースを通して）正当な方法が無い場合、情報はプログラムによるエクスポートができないと言えよう。例えば、プレインテキスト形式の情報にアクセスして、ハードウェアにプレインテキスト形式の情報を表示させる要求メカニズム（例えば、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）が存在しないよう、情報を保持してもよい。一実施例として、情報を保存するデバイス（例えば、暗号化モジュール）は、複製がプレインテキスト形式の情報を含みメモリの一部または全てを複製するような能力が無いよう構成されてもよい。しかしながら、説明のため本開示全体を通し、プレインテキスト形式の情報を入手するための正当な方法が無い情報を使用するが、多様なセキュリティプロトコルを採用し、プレインテキスト形式の情報への不正ア

クセスの防止を求め、許可使用数を限定して情報取得が可能となるよう保持される情報もあることに留意する。一般的に、プログラムでのエクスポートができない情報とは、プレインテキスト形式の情報を完全に取得可能であれば、プレインテキスト形式の情報を得るために特別な手段を講じる必要がある情報（例えば、１以上の暗号鍵）である。

【００４６】

分かり易くするために、例示的なＤＥＣＲＹＰＴ処理を図５の内容の中で説明する。しかしながら、説明するプロセス５００を用いて、デジタル署名検証などの暗号化処理を実施する他の要求を処理してもよい。要求は、ネットワークを介して受信されてもよく（５０２）、いくつかの実施例では、ウェブサービス要求である。

【００４７】

一実施形態では、要求を処理するために、暗号化サービスは暗号鍵を選択する（５０４）。暗号鍵は、例えば、５０２で受信した要求内の暗号鍵の識別子、及び／または、上記したような要求に含まれる他の情報の少なくとも一部に基づき選択されてもよい。また、要求外の情報から決定されるコンテキスト情報を使用して、暗号鍵を選択（５０４）してもよい。

【００４８】

暗号化サービスまたは暗号化サービスの構成要素は、要求が真正であるかどうかを決定するために確認を行う（５０６）。いくつかの実施形態では、暗号化サービス内または暗証化サービスによりアクセス可能な認証モジュール（図２に示す認証ホストなど）が、当該ステップを実施してもよい。真正要求とは、特定パーティ（例えば、クライアント２０２、または、要求を出す権限をクライアント２０２に委任する第三者）により要求が出されたことを要求の受信側（すなわち、暗号化サービス）に保証できるよう、クライアントのアイデンティティが認証される場合がある要求である。いくつかの実施形態では、認証された暗号、デジタル署名、メッセージ認証コード（ＭＡＣ）を使用するか、暗号化サービスが相手方を認証できるプロパティを有する暗号化プロトコル（例えば、ＴＬＳ接続）を使用して、要求を出す。真正性確認は要求自体に対し、すなわちＤＥＣＲＹＰＴ要求について行われ、真正性確認は少なくとも、要求を出した当事者のアイデンティティの妥当性確認を実施し、いくつかの実施形態では、応答に含まれる暗号文の真正性を検証しないことに留意する。要求が真正であると決定できない（例えば、不正な暗号鍵で、デジタル署名が改ざんされているかデジタル署名が生成された）場合、暗号化サービスは要求を拒否し（５２０）、いくつかの実施形態では、クライアントにエラーを返すか、及び／または他の方法をとってもよい（例えば、１以上の電子メッセージを介してセキュリティ管理者に通知する）。

【００４９】

要求が真正であると決定すると、一実施形態では、暗号化サービスまたは暗号化サービスの構成要素は、要求が適用セキュリティポリシを満たすかどうかを決定する（５０８）。いくつかの実施形態では、暗号化サービス内のまたは暗号化サービスによりアクセス可能なポリシ実施モジュールが、当該ステップを実施してもよい。上記したように、要求の真正性決定の一部として、要求に適用するポリシセット（総称してセキュリティポリシという）を取得してもよいが、他の実施形態ではセキュリティポリシを他の方法で取得してもよい。取得したセキュリティポリシには、プリンシパルに実施が許可されるアクション、及び／または、アクションの実行に使用されるリソースに関する制限が含まれてもよい。例えば、セキュリティポリシの中には、権限の低いプリンシパルの能力を制限し、当該プリンシパルに「読み取り」または「読み取り」型の暗号化処理（例えば、ＤＥＣＲＹＰＴ）の実施のみ許可するが、「書き込み」または「書き込み」関連の暗号化処理（例えば、ＥＮＣＲＹＰＴ）を使って新コンテンツの変更も作成も許可しないものがある。第２の実施例として、セキュリティポリシの中には、プリンシパルに「書き込み」または「書き込み」関連の暗号化処理の実施を許可するが、解読される場合があるリソースセットを制限するものがある。要求がセキュリティポリシ条件を満たさないことを検出すると、暗号化サービスは要求を拒否してもよく（５２０）、いくつかの実施形態では、クライアント

にエラーを返すか、及び／または、他の方法を取ってもよい（例えば、セキュリティ管理者に通知する）。

【００５０】

要求の履行において取得したセキュリティポリシを満たすと決定した結果、一実施形態では、暗号化サービスまたは暗号化サービスの構成要素は、受信した要求の暗号化処理、及び、暗号鍵に関連するセキュリティ期待値の実行に使用する選択暗号鍵を取得する（５１０）。上述したように、セキュリティ期待値セットは、要求から及び／または要求外の情報（例えば、要求に適用するポリシセット）から取得してもよい。論じたように、セキュリティ期待値セットは、実行の際、選択された暗号鍵が暗号化処理の実施に使用可能であるかどうかにかかわらず、暗号化処理の結果を信頼することを示す、選択暗号鍵に適用する条件セットを定めてもよい。

【００５１】

ＤＥＣＲＹＰＴの実施例では、暗号化処理で使用する暗号鍵は、要求から暗号文を復号するよう動作可能な暗号鍵である。いくつかの実施例では、暗号鍵は暗号化形式でデータストレージシステムに保存され、暗号化サービスのセキュリティモジュールによってのみ復号が可能である。そういった実施形態では、暗号化された暗号鍵は、データストレージシステムから取得され、セキュリティモジュールに提供されてもよい。他の実施形態では、セキュリティモジュールは、暗号鍵を記憶しローカルデータストレージから暗号鍵を取得してもよい。一般的に、任意の暗号鍵取得方法を使用してもよく、暗号鍵取得様式は、多様な暗号化サービス構成に従い多様であってもよい。いくつかの実施形態では、暗号化サービスは、ポリシ管理モジュールまたは同様の構成要素を使用して、暗号鍵に関連するセキュリティ期待値を識別し取得してもよい。他の実施形態では、セキュリティ期待値は、要求の少なくとも一部に含まれてもよい。なお、図５は、プロセス５００の一部としての暗号鍵の取得を示すが、いくつかの実施形態では、暗号鍵にアクセスすることなくセキュリティ期待値を評価することができ、そういった評価をすることで暗号鍵を取得する必要が無くなる場合などでは、暗号鍵を取得しなくてもよい。

【００５２】

一実施形態では、暗号化サービスまたは暗号化サービスの構成要素は、セキュリティ期待値に従い要求を評価する（５１２）。当該評価は、図２において上記した期待値評価エンジンなどの構成要素により実施されてもよい。例えば、適用セキュリティ期待値によりそのように評価すると指定されていれば、評価では、暗号化処理の実行に使用する暗号鍵を信頼すべきかどうかを決定してもよい。評価には多様な処理モードがある。処理モードによって、暗号鍵の信頼性をどのように評価するかが決まる。いくつかの実施形態では、処理モードは要求で指定されてもよく、暗号化サービスにより設定されてもよい。

【００５３】

いくつかの実施形態では、処理モードには、無効状態、デフォルト処理モード、またはＴＲＵＳＴＫＥＹ処理モードがあってもよい。処理無効状態とは、当該ステップにおいて妥当性確認がオフになっている処理モードのことである。当該処理状態は、他の処理モードより性能上優位であり、コンピューティングシステムが本質的に安全な（例えば、信頼性の高いコンピューティング環境である）いくつかの実施形態では用いてもよい。デフォルト処理モードは、暗号化処理の実行に使用する暗号鍵を符号化ポリシに基づき検証する処理モードであってもよい。デフォルト処理モードの実施例では全ての要求を評価し、暗号化処理の実行に使用する暗号鍵がプリンシパルアカウントからの鍵でなければならないとしてもよい。ＴＲＵＳＴＫＥＹ処理モードは、ポリシの妥当性確認がコールを出すプリンシパルに付随する処理モードであってもよい。一実施形態では、ポリシ管理モジュールをルックアップに使用して、暗号鍵に対してＴＲＵＳＴＫＥＹアクションを許可するという原則に関するセキュリティポリシが存在するかどうかを決定する。ＤＥＣＲＹＰＴの実施例では、暗号文ファイル／リソースに対してＴＲＵＳＴＫＥＹアクションを考慮する。コール側クライアントに関連するセキュリティポリシが存在する場合、処理は正常に復号化され、プレインテキストを提供する。デジタル署名検証の実施例において、肯定的な応

答では、デジタル署名が正しい旨、及び、デジタル署名の正当性の検証に使用する鍵を信頼する旨の両方を示す。

【００５４】

応答は、セキュリティ期待値の評価に基づき生成され提供される（５１４）（例えば、ネットワークを介して送信される）。セキュリティ期待値を満たしている場合、処理を完了し、適切な応答（例えば、暗号文を解読し得られたプレインテキスト）を提供してもよい。いくつかの実施形態では、セキュリティ期待値を満たしていなければ（例えば、ＴＲＵＳＴＫＥＹアクションを許可するポリシが存在しない）、失敗に終わりクライアントに返してもよい。

【００５５】

図６は、複数の適用セキュリティポリシ間のコンフリクトを解消するプロセス６００の実施例を示す。プロセス６００は、暗号化サービスまたは暗号化サービスの構成要素など、任意の適切なシステムにより実施されてもよい。例えば、セキュリティポリシに関して実施する際、上記のポリシ実施モジュールが、プロセス６００を実施してもよい。いくつかの実施形態では、暗号化サービスは、要求を処理する際（例えば、図５に記載のプロセスに従って、図２に関し上記したように）、複数のセキュリティポリシを取得してもよい。複数のポリシが評価されると検出する（６０２）と、ポリシそれぞれを評価し（６０４）、個々のポリシ／期待値のそれぞれの結果を決定する。その後、個々のポリシの結果はそれぞれ、一時的媒体（例えば、ＲＡＭまたは一時的なキャッシュ）または持続的媒体（例えば、ハードディスクまたはネットワークストレージ）に記憶され、その後評価計算を実施してもよい。いくつかの実施形態では、並行してまたは分散して評価を実施してもよい。

【００５６】

全ての評価を完了すると、最初に、明示的なアクセス拒否エフェクトがあるかどうかを確認する（６０６）ことで、コンフリクトは解消される。明示的な拒否は、ＤＥＮＹエフェクトを有するセキュリティポリシに起因してもよい。明示的な拒否を検出すると、コンフリクトが解消された結果、リソースへのアクセス要求は拒否される。しかしながら、明示的な拒否が無く、少なくとも１つの許可エフェクトが検出された場合（６０８）、要求は許可される（６２２）。これは、コンフリクトが解消された結果、リソースへのアクセスを許可（６２２）することを意味する。

【００５７】

セキュリティ期待値の評価の際にも、同様のプロセスを実施してもよい。例えば、特定タイプのＡＰＩコール（例えば、ＤＥＣＲＹＰＴまたはＶＥＲＩＦＹ＿ＳＩＧＮＡＴＵＲＥ）では、セキュリティ期待値に明示されたエフェクトにより上書きされる場合がある要求を履行するデフォルト方法があってもよい。例えば、ＤＥＣＲＹＰＴに対するデフォルトでは、信頼する際使用する暗号鍵をセキュリティ期待値が要求しない限り、復号化された暗号文を提供するようにしてもよく、そういった要求を満たさない時には、要求は拒否されてもよい。別の実施例として、ＶＥＲＩＦＹ＿ＳＩＧＮＡＴＵＲＥのデフォルトでは、信頼性があると指定された鍵をセキュリティ期待値が要求しない限り、正確性の確認に使用する鍵の信頼性に関わらず、デジタル署名が正しいかどうかを示す応答を提供するようにしてもよい。そういったセキュリティ期待値であれば、デジタル署名の検証ができない旨を示す応答、または、いくつかの実施形態では、デジタル署名は正しいが信頼できない旨の応答を提供して、信頼性のない鍵を使用したデジタル署名の検証を求める要求を処理してもよい。要求履行のデフォルト様式は、多様な実施形態において、アカウントベース、及び／または他の方法により様々であってもよい。例えば、場合により、セキュリティ期待値が低位なセキュリティを明示的に許可しない限り、デフォルトでは高いセキュリティを保証してもよい（例えば、信頼性のない鍵でのデジタル署名の検証、または、信頼性のない鍵での復号化）。

【００５８】

図７は、多様な実施形態による態様を実施する例示的な環境７００の態様を示す。説明

のためにウェブベースの環境を使用するが、多様な環境を適切に用いて、多様な実施形態を実施してもよいことは理解されるであろう。当該環境は、適切なネットワーク７０４を介して要求、メッセージまたは情報を送信及び／または受信するよう動作可能な任意の適切なデバイスを含むことができ、いくつかの実施形態では、デバイスのユーザに情報を戻すことができる、電子クライアントデバイス７０２を含む。そういったクライアントデバイスの実施例には、パーソナルコンピュータ、携帯電話、携帯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、パーソナルデータアシスタント、埋め込みコンピュータシステム、電子ブックリーダなどがある。ネットワークは、イントラネット、インターネット、セルラネットワーク、ローカルエリアネットワーク、衛星ネットワーク、もしくは任意の他のそういったネットワーク、及び／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であり得る。そういったシステムに使用する構成要素は、選択されたネットワークタイプ及び／または環境タイプに少なくとも部分的に依存し得る。そういったネットワークを介した通信プロトコル及び構成要素は周知であり、本明細書では詳述しない。ネットワークを介した通信は、有線接続または無線接続、及びそれらの組み合わせにより実施可能となり得る。当該実施例では、ネットワークはインターネットを備え、当該環境は、要求を受信しそれに応答してコンテンツを提供するウェブサーバ７０６を備えているが、他のネットワークでは、同様の目的を果たす代替デバイスの使用が可能であることは、当業者には明らかであろう。

【００５９】

図の環境は、少なくとも１つのアプリケーションサーバ７０８及びデータストア７１０を備える。複数のアプリケーションサーバ、レイヤなどの要素、プロセス、または構成要素がある可能性があり、接続されるか構成され、適切なデータストアからデータを取得するなどのタスクを実施するために対話可能であることは、理解されたい。本明細書で使用するように、サーバは、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など、多様な方法で実施されてもよい。文脈上、サーバが、コンピュータシステム上で実行されるプログラミングモジュールを指すことがある。本明細書で使用するように、特段に指定がなく文脈上明白でない限り、用語「データストア」は、データの保存、取得及び検索が可能な任意のデバイスまたはデバイスの組み合わせを指し、任意の標準環境、分散化環境、仮想環境、またはクラスタ環境において、データサーバ、データベース、データストレージデバイス、及びデータ記憶媒体を任意に組み合わせ任意の数を含んでもよい。アプリケーションサーバは、データストアと一体化した任意の適切なハードウェア、ソフトウェア及びファームウェアを含むことができ、必要に応じ、アプリケーション用データアクセス及びビジネスロジックの一部または全てを処理し、クライアントデバイス用の１以上のアプリケーションの態様を実行する。アプリケーションサーバは、データストアと連携したアクセス制御サービスを提供してもよく、ユーザへの提供に使用可能なテキスト、グラフィックス、オーディオ、ビデオ、及び／または他のコンテンツを含むが、これらに限定されないコンテンツを生成することができ、ウェブサーバによりユーザに、ＨｙｐｅｒＴｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（「ＨＴＭＬ」）、Ｅｘｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（「ＸＭＬ」）、ＪａｖａＳｃｒｉｐｔ、Ｃａｓｃａｄｉｎｇ Ｓｔｙｌｅ Ｓｈｅｅｔｓ（「ＣＳＳ」）、または他の適切なクライアント側構造化言語の形式で提供されてもよい。クライアントデバイスに転送されるコンテンツは、クライアントデバイスにより処理されて、ユーザに聴覚的に、視覚的に、ならびに／または、感触、味覚及び／もしくは嗅覚を含む他の感覚により知覚可能な形式を含むが、これらに限定されない１以上の形式で、コンテンツを提供してもよい。クライアントデバイス７０２とアプリケーションサーバ７０８との間のコンテンツ配信だけでなく、全ての要求及び応答の処理は、ＰＨＰ：Ｈｙｐｅｒｔｅｘｔ Ｐｒｅｐｒｏｃｅｓｓｏｒ（「ＰＨＰ」）、Ｐｙｔｈｏｎ、Ｒｕｂｙ、Ｐｅｒｌ、Ｊａｖａ、ＨＴＭＬ、ＸＭＬ、または、本実施例において他の適切なサーバ側構造化言語を用いて、ウェブサーバにより処理され得る。本明細書で論じる構造化コードは、本明細書の他の箇所でも論じ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可能であるので、ウェブサーバ及びアプリケーションサ

ーバは必須ではなく、単に例示的な構成要素であることを理解されたい。さらに、本明細書で単体デバイスにより実施されるよう説明した処理は、文脈上特段に明白でない限り、分散化システム及び／または仮想システムを形成する場合がある複数のデバイスにより一体的に実施されてもよい。

【００６０】

データストア７１０は、本開示の特定の態様に関連するデータを保存するための、複数の別個のデータテーブル、データベース、データドキュメント、動的データ記憶方式、ならびに／または、他のデータ記憶機構及び媒体を含み得る。例えば、図のデータストアは、生産側用コンテンツの提供に使用可能な、生産データ７１２及びユーザ情報７１６の保存機構を含んでもよい。また、図のデータストアは、報告、解析または他のそういった目的のために使用され得るログデータ７１４の保存機構を含む。ページ画像情報及びアクセス権情報など、データストアに保存する必要があり、適切であるとして上記で挙げた機構のいずれか、または、データストア７１０に機構を追加して保存可能となる他の多くの態様が存在し得ることを理解されたい。データストア７１０は、関連するロジックを介して、アプリケーションサーバ７０８から命令を受信しそれに応答してデータを取得、更新または処理するよう動作可能である。アプリケーションサーバ７０８は、受信した命令に応答して静的データ、動的データ、または、静的データ及び動的データを組み合わせて提供してもよい。ウェブログ（ブログ）、ショッピングアプリケーション、ニュースサービス、及び、他のそういったアプリケーションで使用するデータなどの動的データは、本明細書で説明するようにサーバ側構造化言語により生成されてもよく、アプリケーションサーバ上で、または、アプリケーションサーバによる制御下で動作するコンテンツ管理システム（「ＣＭＳ」）により提供されてもよい。一実施例では、ユーザは、ユーザにより操作されるデバイスを介して、所定項目タイプの検索要求を出してもよい。この場合、データストアはユーザ情報にアクセスしてユーザのアイデンティティを検証してもよく、カタログ詳細情報にアクセスして当該タイプの項目に関する情報を取得し得る。その後、当該情報を、ユーザがユーザデバイス７０２上でブラウザを介して見ることができるウェブページ上の結果リストなどで、ユーザに返すことができる。注目する特定項目の情報は、ブラウザの専用ページまたはウィンドウで見ることができる。しかしながら、本開示の当該実施形態は、必ずしもウェブページのコンテキストに限定されず、一般的に要求処理に適用し、一般的に要求は必ずしもコンテンツに関する要求ではないことに留意する。

【００６１】

各サーバは、一般的に、当該サーバの一般的な管理及び処理について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備え、また一般的に、命令を保存するコンピュータ可読記憶媒体（例えば、ハードディスク、ランダムアクセスメモリ、読取専用メモリなど）を備え、当該命令はサーバのプロセッサにより実行されるとサーバがその意図する機能を実施できるようになる。サーバのオペレーティングシステム及び一般的な機能性に適した実施態様は、周知であるか市販されており、当業者であれば本明細書の開示に照らして容易に実施できる。

【００６２】

当該環境は、一実施形態では、１以上のコンピュータネットワークまたは直接接続を使い、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及び／または仮想コンピューティング環境である。しかしながら、当業者であれば、そういったシステムは、図７に示すより少ないまたは多い構成要素を備えるシステムにおいても同等に良好に動作可能であることは理解するものである。したがって、図７のシステム７００の描写は、本質的に例示とし、本開示の範囲を限定するものではない。

【００６３】

さらに、多様な実施形態が多種多様な動作環境において実施可能であり、場合により、多数のアプリケーションのいずれかの動作に使用可能な１以上のユーザコンピュータ、コンピューティングデバイス、または処理デバイスを備え得る。ユーザまたはクライアントデバイスは、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など、多数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し多数のネットワーク及びメッセージングプロトコルに対応可能なセルラデバイス、ワイヤレスデバイス、及び携帯デバイス、のいずれかを備え得る。また、そういったシステムは、多様な市販オペレーティングシステムのいずれか、ならびに、開発及びデータベース管理などのための他の既知のアプリケーションを実行する多数のワークステーションを備え得る。また、当該デバイスは、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デバイスなど他の電子デバイスを含み得る。また、当該デバイスは、仮想マシン、ハイパバイザ、及び、ネットワークを介して通信可能な他の仮想デバイスなど仮想デバイスを含み得る。

【００６４】

本開示の多様な実施形態は、多様な市販のプロトコルのいずれかを使用した通信をサポートし当業者には周知である少なくとも１つのネットワークを利用し、当該プロトコルには、伝送制御プロトコル／インターネットプロトコル（「ＴＣＰ／ＩＰ」）、ユーザデータグラムプロトコル（「ＵＤＰ」）、オープンシステム相互接続（「ＯＳＩ」）モデルの多様な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」）、カモンインターネットファイルシステム（「ＣＩＦＳ」）、及び、ＡｐｐｌｅＴａｌｋなどがある。ネットワークには、例えば、ローカルエリアネットワーク、広域ネットワーク、仮想プライベートネットワーク、インターネット、イントラネット、エクストラネット、公衆交換電話網、赤外線ネットワーク、無線ネットワーク、衛星ネットワーク、及び、それらの任意の組み合わせがあり得る。

【００６５】

ウェブサーバを利用する実施形態では、ウェブサーバは、ハイパーテキスト転送プロトコル（「ＨＴＴＰ」）サーバ、ＦＴＰサーバ、カモンゲートウェイインタフェース（「ＣＧＩ」）サーバ、データサーバ、Ｊａｖａサーバ、Ａｐａｃｈｅサーバ、及び、ビジネスアプリケーションサーバを含む、多様なサーバまたはミッドティアアプリケーションのいずれかを実行し得る。また、サーバ（複数可）は、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＋＋などのプログラミング言語のいずれか、または、Ｒｕｂｙ、ＰＨＰ、Ｐｅｒｌ、Ｐｙｔｈｏｎ、もしくはＴＣＬなどのスクリプト言語のいずれか、ならびにそれらの組み合わせで書かれた１以上のスクリプトまたはプログラムとして実施される場合がある１以上のウェブアプリケーションを実行するなどして、プログラムまたはスクリプトの実行を可能にしてもよい。また、サーバ（複数可）はデータベースサーバを含んでもよく、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データベースサーバを含むがこれらに限定されず、ＭｙＳＱＬ、Ｐｏｓｔｇｒｅｓ、ＳＱＬｉｔｅ、ＭｏｎｇｏＤＢ、及び、構造化または非構造化データの保存、検索、及び取得が可能な任意の他のサーバなどのオープンソースサーバを含む。データベースサーバは、テーブルベースサーバ、ドキュメントベースサーバ、非構造化サーバ、リレーショナルサーバ、非リレーショナルサーバ、または、これらのデータベースサーバ及び／もしくは他のデータベースサーバの組み合わせを含んでもよい。

【００６６】

当該環境は、上述したような多様なデータストア、ならびに他のメモリ及び記憶媒体を含み得る。これらは、コンピュータの１以上にローカルな（及び／もしくは常駐する）、または、ネットワーク経由の複数のコンピュータの一部または全てから離れた記憶媒体など、多様な場所に存在し得る。特定の実施形態セットでは、情報は、当業者には周知のストレージエリアネットワーク（「ＳＡＮ」）に存在してもよい。同様に、コンピュータ、サーバまたは他のネットワークデバイスによる機能の実施に必要なファイルは、適切にローカルに及び／またはリモートに保存されてもよい。システムがコンピュータ化デバイスを含む場合、そういったデバイスはそれぞれ、バスを介して電気接続される場合があるハ

ードウェア要素を含むことができ、当該要素は、例えば、少なくとも１つの中央処理装置（「ＣＰＵ」または「プロセッサ」）、少なくとも１つの入力デバイス（例えば、マウス、キーボード、コントローラ、タッチスクリーン、またはキーパッド）、及び少なくとも１つの出力デバイス（例えば、ディスプレイデバイス、プリンタ、またはスピーカ）を含む。また、そういったシステムは、ディスクドライブ、光記憶装置、及び、ランダムアクセスメモリ（「ＲＡＭ」）または読出専用メモリ（「ＲＯＭ」）などのソリッドステート記憶装置、ならびに、リムーバブルメディアデバイス、メモリカード、フラッシュカードなど、１以上のストレージデバイスを含んでもよい。

【００６７】

また、そういったデバイスは、コンピュータ可読記憶メディアリーダ、通信デバイス（例えば、モデム、ネットワークカード（無線または有線）、赤外線通信デバイスなど）、及び、上記のようなワーキングメモリを含み得る。コンピュータ可読記憶メディアリーダは、遠隔の、ローカルの、固定及び／または取り外し可能な記憶装置を表すコンピュータ可読記憶媒体、ならびに、一時的に及び／または永続的に、コンピュータ可読情報を含み、保存し、送信し、及び検索するための記憶媒体と接続するか、当該記憶媒体を収容するよう構成され得る。また、システム及び多様なデバイスは、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配置された多数のソフトウェアアプリケーション、モジュール、サービス、または他の要素を含む。代替の実施形態では、上記から多数の変形が可能であ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を使用する場合があり、及び／または、特定の要素をハードウェア、ソフトウェア（アプレットなどのポータブルソフトウェアを含む）、もしくはその両方に実施される場合もある。さらに、ネットワーク入力／出力デバイスなどの他のコンピューティングデバイスへの接続を使用してもよい。

【００６８】

コードまたはコードの一部を含む記憶媒体及びコンピュータ可読媒体は、記憶媒体及び通信媒体を含む、当該技術分野において周知されているか使用されている任意の媒体を含むことができ、当該記憶媒体及び通信媒体には、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もしくは他のデータなどの情報の保存及び／または送信する方法または技術において実施する、揮発性及び不揮発性で取り外し可能及び取り外し不可な媒体などがあるがこれらに限定されず、ＲＡＭ、ＲＯＭ、電気的消去可能プログラマブル読取専用メモリ（「ＥＥＰＲＯＭ」）、フラッシュメモリもしくは他のメモリ技術、コンパクトディスク読取専用メモリ（「ＣＤ－ＲＯＭ」）、デジタル多用途ディスク（「ＤＶＤ」）もしくは他の光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージもしくは他の磁気記憶装置、または、所望の情報の保存に使用することができシステムデバイスによりアクセス可能な任意の他の媒体を含む。当業者であれば、本明細書で提供する開示及び教示に基づいて、多様な実施形態を実施する他の方法及び／またはメソッドがわかるであろう。

【００６９】

したがって、本明細書及び図は、限定ではなく例示であるとみなすものである。しかしながら、特許請求に記載する本発明の広い趣旨及び範囲から逸脱することなく、多様な修正及び変更が可能であることは明らかである。

【００７０】

他の変形も本開示の趣旨の範囲内である。したがって、本開示技術では、多様な修正及び代替構成が可能であるが、図では所定の例示的な実施形態を示し、ここまで詳述してきた。しかしながら、開示した特定形式に本発明を限定する意図はなく、反対に、添付の特許請求に定めるように、本発明の趣旨及び範囲内でのあらゆる修正、代替構成及び等価物を包含することを意図する。

【００７１】

開示した実施形態を説明する文脈における（特に以下の請求項の文脈における）用語「

ａ」、及び「ａｎ」、及び「ｔｈｅ」、及び同様対象の使用は、本明細書で特段に記載せず文脈で明白に否定しない限り、単数形及び複数形の両方を包含するものと解釈される。用語「ｃｏｍｐｒｉｓｉｎｇ（備える）」、「ｈａｖｉｎｇ（有する）」、「ｉｎｃｌｕｄｉｎｇ（含む）」、及び「ｃｏｎｔａｉｎｉｎｇ（含有する）」は、特段に記載しない限り、非限定用語として解釈される（すなわち、「ｉｎｃｌｕｄｉｎｇ、ｂｕｔ ｎｏｔ ｌｉｍｉｔｅｄ ｔｏ（含むがこれに限定されない）」を意味する）。用語「ｃｏｎｎｅｃｔｅｄ（接続された）」は、変更されておらず物理的な接続を指す場合、介在するものがあっても、部分的にもしくは全体的に内包され、接続され、または結合されていると解釈される。本明細書での値の範囲の記載は、本明細書で特段に記載しない限り、単に、範囲内の各別個の値をそれぞれ意味する簡略法とすることを意図し、それぞれの別個の値は、本明細書にそれぞれ記載されているかのように本明細書に組み込まれる。特段に記載されず文脈で否定しない限り、用語「ｓｅｔ（セット）」（例えば、「ａ ｓｅｔ ｏｆ ｉｔｅｍｓ（項目セット）」、または「ｓｕｂｓｅｔ（サブセット）」の使用は、１以上の要素を含む非空コレクションとして解釈される。さらに、特段に記載されず文脈で否定しない限り、対応するセットについての用語「ｓｕｂｓｅｔ（サブセット）」は、必ずしも対応するセットの適切なサブセットを意味するものではないが、サブセット及び対応するセットは同一であってもよい。

【００７２】

特段に指定せず文脈で明白に否定しない限り、「ａｔ ｌｅａｓｔ ｏｎｅ ｏｆ Ａ、Ｂ、ａｎｄ Ｃ（Ａ、Ｂ、及びＣの少なくとも１つ）」、または「ａｔ ｌｅａｓｔ ｏｎｅ ｏｆ Ａ、Ｂ ａｎｄ Ｃ（Ａ、Ｂ及びＣの少なくとも１つ）」形式の句などの接続語句は、項目、用語などがＡまたはＢまたはＣのいずれかであるか、Ａ及びＢ及びＣのセットの任意の非空サブセットであることを示すために一般的に使用されるように、文脈上理解される。例えば、３つの要素を有するセットの例示的な実施例では、接続句「ａｔ ｌｅａｓｔ ｏｎｅ ｏｆ Ａ、Ｂ、ａｎｄ Ｃ（Ａ、Ｂ、及びＣの少なくとも１つ）」、及び「ａｔ ｌｅａｓｔ ｏｎｅ ｏｆ Ａ、Ｂ ａｎｄ Ｃ（Ａ、Ｂ及びＣの少なくとも１つ）」は、｛Ａ｝、｛Ｂ｝、｛Ｃ｝、｛Ａ、Ｂ｝、｛Ａ、Ｃ｝、｛Ｂ、Ｃ｝、｛Ａ、Ｂ、Ｃ｝のセットのいずれかを指す。このように、そういった接続語句は、一般的に、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のそれぞれの存在を所定の実施形態が要していると示す意図はない。

【００７３】

本明細書に記載するプロセス処理は、本明細書で特段に記載されず文脈で特段に明白に否定しない限り、任意の適切な順序で実施され得る。本明細書で説明するプロセス（またはその変形及び／またはそれらの組み合わせ）は、実行可能な命令で構成された１以上のコンピュータシステムの制御下で実施され、ハードウェアまたはその組み合わせにより１以上のプロセッサを一元的に実行するコード（例えば、実行可能な命令、１以上のコンピュータプログラム、または１以上のアプリケーション）として実施されてもよい。コードは、例えば、１以上のプロセッサにより実行可能な複数の命令を備えるコンピュータプログラムの形式で、コンピュータ可読記憶媒体に保存されてもよい。コンピュータ可読記憶媒体は、非一時的であってもよい。

【００７４】

本明細書で提供する実施例の一部及び全て、または例示的な用語（例えば「ｓｕｃｈ ａｓ（など）」）の使用は、単に本発明の実施形態をより分かり易く示すことを意図し、特段に請求しない限り、本発明の範囲の限定を提示するものではない。本明細書におけるいかなる文言も、本発明の実施に不可欠な、任意の非請求要素を示すものと解釈されるべきではない。

【００７５】

本開示の実施形態を、本発明を実行するために本発明者が知る最良形態を含め本明細書に記載する。当該実施形態の変形は、当業者であれば上記の内容を読めば明らかになるであろう。本発明者らは、当業者によりそういった変形が適切に使用されることを期待値し

ており、本発明者らは、本開示の実施形態が本明細書に具体的な記載とは異なって実施されることを意図する。したがって、本開示の範囲は、適用法令によって許容されるように、本明細書に添付された特許請求に挙げた主題のあらゆる変形及び均等物を含む。さらに、本明細書に特段に記載されず文脈で明白に否定しない限り、あらゆる可能な変形での上記要素の全ての組合せは、本開示の範囲に包含される。

【００７６】

明細書で引用する刊行物、特許出願及び特許を含む全ての参考文献は、各参考文献が個々に特異的に参照により組み入れられると記載され、本明細書にその全体が記載されているのと同程度に、参照により本明細書に組み込まれる。

【００７７】

本開示の実施形態は、以下の条項を考慮して記載され得る。

１．コンピュータ実施方法では、

サービスプロバイダのカスタマと関連するリクエスタから、履行により暗号化処理が実施されるウェブサービス要求を受信し、

前記ウェブサービス要求の情報の少なくとも一部に基づき、前記サービスプロバイダの複数のカスタマのための、前記サービスプロバイダにより管理される複数の暗号鍵から暗号鍵を選択し、

前記ウェブサービス要求に適用するセキュリティ期待値セットを決定し、前記セキュリティ期待値セットは、履行の際、前記選択暗号鍵が前記暗号化処理の実施に使用可能であるかどうかにかかわらず、前記暗号化処理の結果を信頼することを示す、前記選択暗号鍵に適用する条件セットを定め、

前記選択暗号鍵に対し前記セキュリティ期待値セットを評価し、

前記セキュリティ期待値セットの評価の少なくとも一部に基づき、前記ウェブサービス要求に対する応答を生成し、

前記生成応答を提供する、前記コンピュータ実施方法。

【００７８】

２．前記セキュリティ期待値セットは前記要求に指定される、条項１に記載のコンピュータ実施方法。

【００７９】

３．　前記方法ではさらに、

複数の保存ポリシドキュメントからの、前記要求に適用するポリシセットを決定し、

前記ポリシセットが前記要求の履行を許可するよう決定し、

前記セキュリティ期待値セットでは、前記決定ポリシセットから少なくとも一つのセキュリティ期待値を決定するよう決定する、条項１または２に記載のコンピュータ実施方法。

【００８０】

４．　前記方法ではさらに、

前記カスタマによりポリシの修正を許可されたエンティティから、前記カスタマに関連するポリシセットに対し前記セキュリティ期待値セットの実施を求めるウェブサービス要求を受信し、

前記セキュリティ期待値セットを含むよう前記ポリシセットを修正することで前記要求を履行する、条項３に記載のコンピュータ実施方法。

【００８１】

５．　前記暗号化処理は復号化またはデジタル署名検証である、条項３または４に記載のコンピュータ実施方法。

【００８２】

６．　システムであって、１以上のサービスを実施するよう構成された少なくとも１つのコンピューティングデバイスを備え、前記１以上のサービスは構成により、

クライアントから、暗号化処理の実施を求める要求を受信し、

前記システムにより管理される暗号鍵セットからの、前記暗号化処理を実施するための

暗号鍵を決定し、
前記要求に含まれる情報の少なくとも一部に基づき、前記暗号化処理の実施結果は前記クライアントにより信頼されるべきとする条件セットを決定し、
前記暗号鍵及び前記決定条件セットの少なくとも一部に基づき、前記要求に対する応答を生成し、
前記生成応答を前記クライアントに提供する、前記システム。
【００８３】
７．　前記１以上のサービスはさらに構成により、少なくとも１つの条件が前記要求に指定されることにより、前記条件セットの前記少なくとも１つの条件を決定する、条項６に記載のシステム。
【００８４】
８．　前記クライアントのアイデンティティが認証され、
前記１以上のサービスは、前記条件セットを決定するよう構成され、前記決定では少なくとも、
前記アイデンティティに適用するポリシセットのサブセットを選択し、
前記条件セットの少なくとも１つの条件を、前記少なくとも１つの条件が前記ポリシセットの前記サブセットに指定されることにより決定する、条項６または７に記載のシステム。
【００８５】
９．　前記システムはサービスプロバイダにより動作され、
前記ポリシセットは、前記アイデンティティに関連する前記サービスプロバイダのカスタマによりプログラムでの修正が可能である、条項８に記載のシステム。
【００８６】
１０．　前記システムは、前記暗号鍵セットのハードウェアベースの保護機能を有するデバイスであり、前記暗号鍵ではプレインテキスト形式に前記デバイスからプログラムでのエクスポートができない、条項６乃至９のいずれか１項に記載のシステム。
【００８７】
１１．　前記暗号鍵は、サービスプロバイダの第一カスタマに代わり前記システムにより管理され、
前記暗号鍵セットは、前記サービスプロバイダの第二カスタマに代わり前記システムにより管理される第二暗号鍵を備える、条項６乃至１０のいずれか１項に記載のシステム。
【００８８】
１２．　前記クライアントは、前記サービスプロバイダの第三カスタマにより動作される、条項１１に記載のシステム。
【００８９】
１３．　前記生成応答は、前記条件セットの評価結果を示す情報を含む、条項６乃至１２のいずれか１項に記載のシステム。
【００９０】
１４．　前記条件セットは、前記暗号鍵が、信頼性があると指定された暗号鍵セットからのものであることを求める、条項６乃至１３のいずれか１項に記載のシステム。
【００９１】
１５．　実行可能命令を保存し有する非一時的コンピュータ可読記憶媒体であって、前記実行可能命令は、コンピュータシステムの１以上のプロセッサにより実行されると、前記コンピュータシステムにサービスを提供させ、前記サービスは構成により、
暗号鍵に関係する暗号化処理に履行により関係する、リクエスタからの要求に含まれる情報の少なくとも一部に基づき、前記リクエスタが前記暗号化処理の結果を信頼すべきかどうかを決定するために前記暗号鍵に適用する条件セットを決定し、前記暗号鍵は、それぞれ前記暗号鍵セットの対応サブセットを有する複数のエンティティのための前記コンピュータシステムにより管理される暗号鍵セットからのものであり、
前記要求の履行方法を決定するために、前記決定条件セットを評価し、

前記決定条件セットの評価の結果、前記暗号鍵が信頼できると示し、前記暗号化処理を実施させ、前記暗号化処理の前記結果を前記要求に応答して提供させる、前記非一時的コンピュータ可読記憶媒体。

【００９２】

１６．　前記エンティティは、前記コンピュータシステムを動作させるサービスプロバイダのカスタマである、条項１５に記載の非一時的コンピュータ可読記憶媒体。

【００９３】

１７．　前記コンピュータシステムに前記条件セットを決定させる前記命令は、前記１以上のプロセッサにより実行されると、前記システムに、前記条件セットの少なくとも１つの条件を、前記要求を出すアイデンティティに関連するポリシから取得させる、条項１５または１６に記載の非一時的コンピュータ可読記憶媒体。

【００９４】

１８．　前記要求はウェブサービス要求である、条項１５乃至１７のいずれか１項に記載の非一時的コンピュータ可読記憶媒体。

【００９５】

１９．　前記１以上の条件は、前記暗号鍵に固有なプロパティの少なくとも一部に基づく、条項１５乃至１８のいずれか１項に記載の非一時的コンピュータ可読記憶媒体。

【００９６】

２０．　前記決定条件セットからの少なくとも１つの条件が前記要求により指定される、条項１５乃至１９のいずれか１項に記載の非一時的コンピュータ可読記憶媒体。

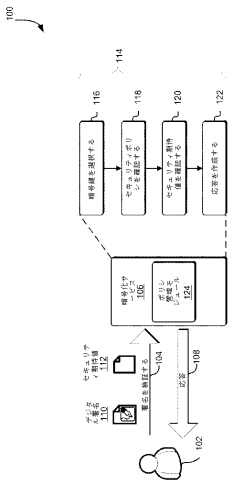
【００９７】

２１．　前記条件セットはブール演算子で繋がれた複数の条件を含む、条項２０に記載の非一時的コンピュータ可読記憶媒体。

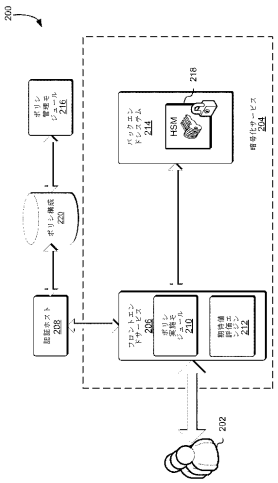
【００９８】

２２．　前記命令はさらに、前記１以上のプロセッサにより実行されると、前記決定条件セットの評価に必須として、前記コンピュータシステムに前記要求に適用するポリシセットを評価させる、条項１５乃至２１のいずれか１項に記載の非一時的コンピュータ可読記憶媒体。

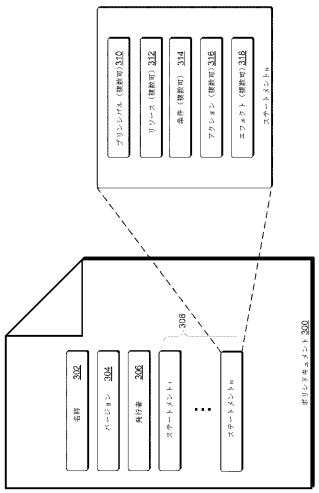
【図１】



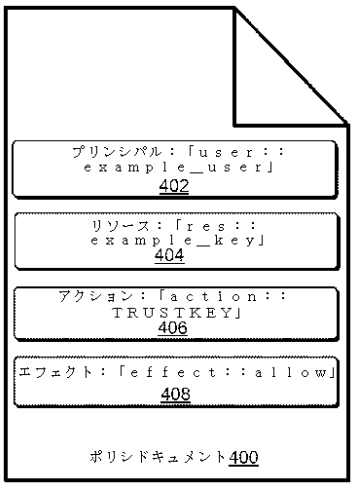
【図２】



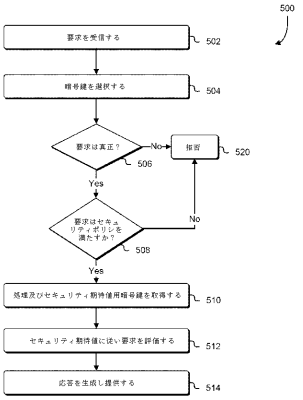
【図３】



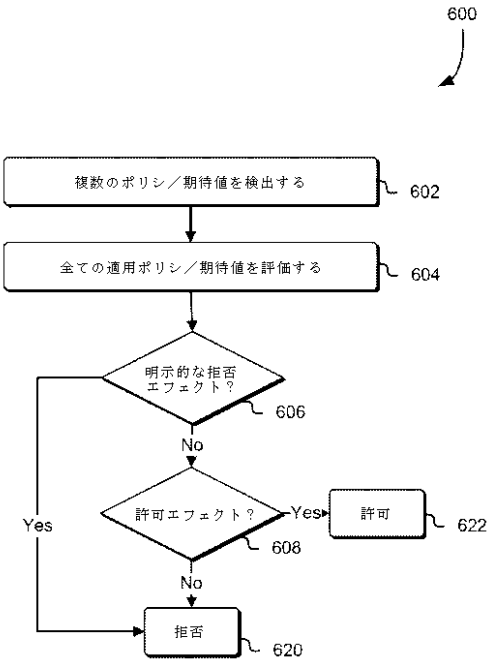
【図４】


プリンシパル：「ｕｓｅｒ：：ｅｘａｍｐｌｅ＿ｕｓｅｒ」
402
リソース：「ｒｅｓ：：ｅｘａｍｐｌｅ＿ｋｅｙ」
404
アクション：「ａｃｔｉｏｎ：：ＴＲＵＳＴＫＥＹ」
406
エフェクト：「ｅｆｆｅｃｔ：：ａｌｌｏｗ」
408
ポリシドキュメント400

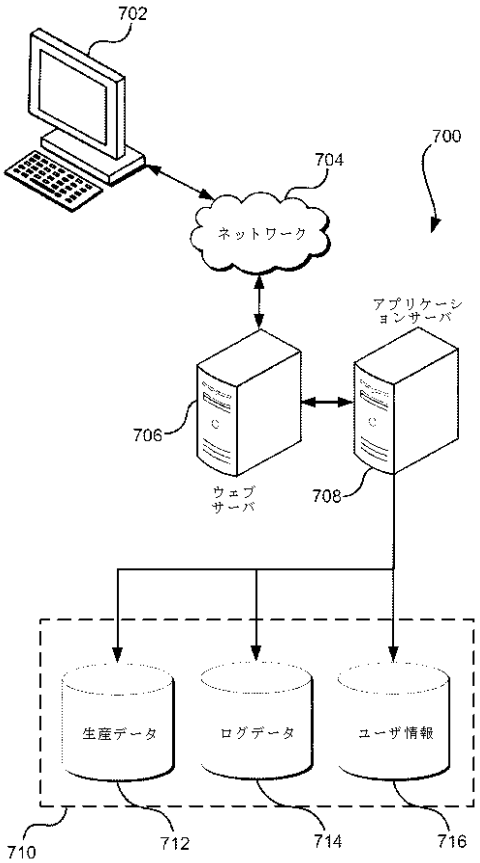
【図５】


500
要求を受信する
502
暗号鍵を選択する
504
要求は真正？
506
No
拒否
520
Yes
要求はセキュリティポリシを満たすか？
508
No
Yes
処理及びセキュリティ期待値用暗号鍵を取得する
510
セキュリティ期待値に従い要求を評価する
512
応答を生成し提供する
514

【図６】


600
複数のポリシ／期待値を検出する
602
全ての適用ポリシ／期待値を評価する
604
明示的な拒否エフェクト？
606
No
許可エフェクト？
608
Yes
許可
622
No
Yes
拒否
620

【図７】


702
700
704
ネットワーク
アプリケーションサーバ
706
ウェブサーバ
708
生産データ
ログデータ
ユーザ情報
710
712
714
716

フロントページの続き

(72)発明者　ロス、グレゴリー　ブランチェク
アメリカ合衆国、ワシントン州　９８１０８、シアトル　ピー．オー．ボックス　８１２２６　アマゾン　テクノロジーズ、インコーポレイテッド内

合議体
審判長　石井　茂和
審判官　山崎　慎一
審判官　月野　洋一郎

(56)参考文献　米国特許出願公開第２０１４／００５０３１７（ＵＳ，Ａ１）
米国特許出願公開第２０１４／０２５０４９１（ＵＳ，Ａ１）
特開２００３－２２４５６３（ＪＰ，Ａ）
特開２００５－５７４１７（ＪＰ，Ａ）
特表２００７－５０７１７５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L9/08
H04L9/14
G06F21/31