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

特許第6527179号
(P6527179)

(45)発行日　令和1年6月5日(2019.6.5)　(24)登録日　令和1年5月17日(2019.5.17)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601B
H04L	9/32	(2006.01)	H04L	9/00	675A
G09C	1/00	(2006.01)	G09C	1/00	640E

請求項の数 20　(全 40 頁)

(21)出願番号	特願2017-7876(P2017-7876)
(22)出願日	平成29年1月19日(2017.1.19)
(62)分割の表示	特願2014-533431(P2014-533431)の分割
原出願日	平成24年9月28日(2012.9.28)
(65)公開番号	特開2017-69989(P2017-69989A)
(43)公開日	平成29年4月6日(2017.4.6)
審査請求日	平成29年2月9日(2017.2.9)
(31)優先権主張番号	13/248,962
(32)優先日	平成23年9月29日(2011.9.29)
(33)優先権主張国	米国(US)
(31)優先権主張番号	13/248,953
(32)優先日	平成23年9月29日(2011.9.29)
(33)優先権主張国	米国(US)

(73)特許権者　506329306
アマゾン　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　９８１０８－１２２６
ワシントン州　シアトル　ピーオー　ボックス　８１２２６
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　グレゴリー　ビー．ロス
アメリカ合衆国　９８１０９－５２１０
ワシントン州　シアトル　テリー　アベニュー　ノース　４１０

最終頁に続く

(54)【発明の名称】パラメータベースのキー導出

(57)【特許請求の範囲】

【請求項１】

コンピュータで実施される方法であって、

第１のエンティティ装置から委任要求を受信するステップであって、当該委任要求は、第２のエンティティ装置にコンピューティングリソースへのアクセス特権を付与することを要求する、ステップと、

制限と、前記第１のエンティティ装置と共有される秘密信用情報とに基づいて、セッションキーを生成するステップであって、前記制限は、生成されるセッションキーに対する１つ以上の制限を示す情報である、ステップと、

前記セッションキーを前記第１のエンティティ装置に提供するステップと、

前記第２のエンティティ装置から、前記第２のエンティティ装置が前記コンピューティングリソースにアクセスするためのアクセス要求を受信するステップと、

前記セッションキーを使用して生成された第１のデジタル署名と前記第２のエンティティ装置から受信された第２のデジタル署名を比較して、前記アクセス要求を認証するステップと、

前記アクセス要求を履行するステップと、

を含む、コンピュータで実施される方法。

【請求項２】

前記制限は複数のキーゾーンのうちの１つのキーゾーンの識別に対応し、前記キーゾーンは、前記セッションキーが有効であるドメインを示す、請求項１に記載のコンピュータ

で実施される方法。
【請求項３】
前記委任要求は、前記セッションキーが生成される前記第１のエンティティ装置の識別を含み、
前記制限は、前記第１のエンティティ装置の前記識別に基づく、
請求項１に記載のコンピュータで実施される方法。
【請求項４】
前記制限は、前記第２のエンティティ装置に許容されるアクセス動作の範囲についての制限に対応する、請求項１に記載のコンピュータで実施される方法。
【請求項５】
前記アクセス要求は、前記第１のエンティティ装置によって提供される前記制限をさらに含み、
前記アクセス要求を認証するステップは、前記アクセス要求に含まれる前記制限に基づいて前記セッションキーが生成されたことを検証することを含む、
請求項１に記載のコンピュータで実施される方法。
【請求項６】
前記制限は前記セッションキーが有効である時間への制限に対応する、請求項１に記載のコンピュータで実施される方法。
【請求項７】
システムであって、
１つまたは複数のプロセッサと、
前記１つまたは複数のプロセッサによって実行されると、前記システムに、
第１のエンティティ装置から委任要求を受信し、当該委任要求は、第２のエンティティ装置にコンピューティングリソースへのアクセス特権を付与することを要求し、
前記委任要求の受信に応答して、
前記第１のエンティティ装置と前記システムとの間で共有される秘密信用情報と、セッション制限と、を暗号ハッシュアルゴリズムに通すことによって、セッションキーを生成し、前記セッション制限は、生成されるセッションキーに対する１つ以上の制限を示す情報であり、
前記セッションキーを前記第１のエンティティ装置に提供し、
前記第２のエンティティ装置から、前記第２のエンティティ装置が前記コンピューティングリソースにアクセスするためのアクセス要求を受信し、前記アクセス要求は、前記セッションキーに関連付けられており、
前記アクセス要求の受信に応答して、
前記セッションキーを使用して生成された第１のデジタル署名と前記第２のエンティティ装置から受信された第２のデジタル署名を比較して、前記アクセス要求を認証し、
前記アクセス要求を履行する
ことを実行させる命令を含むメモリと、
を備える、システム。
【請求項８】
前記アクセス要求を認証する前記命令は、前記システムに、前記アクセス要求が前記セッション制限に従っているかどうかを認証することを実行させる命令を含む、請求項７に記載のシステム。
【請求項９】
前記アクセス要求は第１のアクセス要求であり、前記命令は、前記システムに、
第３のエンティティ装置から第２のアクセス要求を受信して前記コンピューティングリソースにアクセスし、前記第２のアクセス要求は前記セッションキーに関連付けられており、
前記第２のアクセス要求の受信に応答して、
前記第１のデジタル署名と前記第３のエンティティ装置から受信された第３のデジ

タル署名とを比較することによって、前記第２のアクセス要求を認証し、
前記第３のエンティティ装置に、前記コンピューティングリソースへのアクセスを承諾することを実行させるさらなる命令を含む、請求項７に記載のシステム。
【請求項１０】
前記第１のエンティティ装置をさらに備え、前記第１のエンティティ装置は、１つまたは複数のコンピュータシステムによって実行されると、前記１つまたは複数のコンピュータシステムに、前記セッションキーを受信する結果として、前記秘密信用情報を前記第２のエンティティ装置に提供することなく前記セッションキーを前記第２のエンティティ装置に提供することを実行させる第１の命令で構成された前記１つまたは複数のコンピュータシステムを備える、請求項７に記載のシステム。
【請求項１１】
前記セッションキーを前記第２のエンティティ装置に提供する前記第１の命令は、前記１つまたは複数のコンピュータシステムに、前記第２のエンティティ装置が前記セッションキーを取得するために使用可能な情報を、前記第２のエンティティ装置がアクセス可能な電子的宛先に提供することを実行させる命令を含む、請求項１０に記載のシステム。
【請求項１２】
前記電子的宛先はＥメールアドレスである、請求項１１に記載のシステム。
【請求項１３】
前記システムに前記アクセス要求を認証することを実行させる前記命令は、前記システムに、前記暗号ハッシュアルゴリズムを第１の入力のセットおよび第２の入力のセットの両方に適用することを実行させる命令を含み、
前記第１の入力のセットは、前記秘密信用情報、前記アクセス要求、および前記セッション制限を含み、
前記第２の入力のセットは、前記セッションキーおよび前記アクセス要求を含む、
請求項７に記載のシステム。
【請求項１４】
前記暗号ハッシュアルゴリズムはハッシュベースのメッセージ認証符号関数である、請求項１３に記載のシステム。
【請求項１５】
前記アクセス要求は、前記第１のデジタル署名を前記アクセス要求とともに提供することによって、前記セッションキーに関連付けられる、請求項７に記載のシステム。
【請求項１６】
前記システムに前記アクセス要求を認証することを実行させる前記命令は、前記システムに、
前記暗号ハッシュアルゴリズムを前記秘密信用情報、前記アクセス要求、および前記セッション制限に適用してハッシュ結果を取得し、
前記ハッシュ結果を前記第２のデジタル署名と比較する
ことを実行させる命令を含む、請求項１５に記載のシステム。
【請求項１７】
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ると、前記コンピュータシステムに、少なくとも、
第１のエンティティ装置から第１の要求を受信し、当該第１の要求は、第２のエンティティ装置にコンピューティングリソースへのアクセス特権を付与することを要求し、
制限と、前記第１のエンティティ装置と前記コンピュータシステムとの間で共有される秘密信用情報とに基づいて、セッションキーを生成し、前記制限は、生成されるセッションキーに対する１つ以上の制限を示す情報であり、
コンピューティングリソースへのアクセス特権の占有を証明するために使用可能な前記セッションキーを前記第１のエンティティ装置に提供し、
前記コンピューティングリソースにアクセスするための第２の要求を受信し、当該第２の要求は、第２のエンティティ装置にコンピューティングリソースへのアクセスを提供

することを要求し、前記第２の要求は前記セッションキーに関連付けられており、
　前記セッションキーを使用して生成された第１のデジタル署名と前記第２のエンティティ装置から受信された第２のデジタル署名とを比較して、前記第２の要求を認証し、
　前記認証に依存して、前記コンピューティングリソースへのアクセスを提供することによって、前記第２の要求を履行する
　ことを実行させる実行可能命令が記憶された非一時的コンピュータ可読記憶媒体。
【請求項１８】
　前記コンピュータシステムに前記第２の要求を履行することを実行させる前記実行可能命令は、前記コンピュータシステムに、前記第２のエンティティ装置に前記秘密信用情報へのアクセスを提供せずに前記第２の要求を履行することを実行させる実行可能命令を含む、請求項１７に記載の非一時的コンピュータ可読記憶媒体。
【請求項１９】
　前記実行可能命令は、前記コンピュータシステムに、
　前記コンピューティングリソースへアクセスするための第３の要求を受信し、当該第３の要求は、第３のエンティティ装置に前記コンピューティングリソースへのアクセスを提供することを要求し、前記第３の要求は、前記セッションキーに関連付けられており、
　前記第１のデジタル署名と前記第３のエンティティ装置から受信された第３のデジタル署名とを比較することによって、前記第３の要求を認証し、
　前記認証に依存して、前記コンピューティングリソースへのアクセスを提供することによって前記第３の要求を履行する、
　ことを実行させる実行可能命令をさらに含む、請求項１７に記載の非一時的コンピュータ可読記憶媒体。
【請求項２０】
　前記第２の要求は、前記第２のデジタル署名を含み、
　前記第２の要求を認証することは、前記第２のデジタル署名の真正性を検証することをさらに含む、
　請求項１７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】
【背景技術】
【０００１】
　コンピューティング環境は多くの形態をとる。例として、組織は多くの場合、コンピューティングデバイスのネットワークを利用して、強固なサービスのセットをそれらのユーザに提供する。ネットワークは多くの場合、複数の地理的境界に及び、しばしば他のネットワークとつながっている。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および他者によって管理されるコンピューティングリソースの両方を使用してその事業を支援し得る。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ている間、データにアクセスおよび／または提供し得る。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、遠隔ネットワークを構成および操作し、それによってインフラコストを低減し、他の利益を得る。
【０００２】
　多様なコンピューティング環境は多種多様な応用に有用であることが証明されているが、そのような環境は多くの課題を提示する。例えば、ある組織的目標を増進させるためにコンピュータリソースを構成することは、別の組織的目標の増進に悪影響を及ぼし得る。例えば、コンピューティングリソースのセキュリティの効率的な管理は、多くの場合、データおよびサービスへの効率的なアクセスを犠牲にし得る。セキュリティと効率性の目標のバランスをとることは、極めて困難であり得、しばしば多大な労力とリソースを必要とする。
関連出願の相互参照
　本出願は、２０１１年９月２９日に提出された米国特許出願第１３／２４８，９６２号

、表題「ＰＡＲＡＭＥＴＥＲ　ＢＡＳＥＤ　ＫＥＹ　ＤＥＲＩＶＡＴＩＯＮ」（代理人整理番号９０２０４－８１３８８９（０２９４００ＰＣ））、２０１１年9月２９日に提出された同第１３／２４８，９５３号、表題「ＴＥＣＨＮＩＱＵＥＳ　ＦＯＲ　ＣＬＩＥＮＴ　ＣＯＮＳＴＲＵＣＴＥＤ　ＳＥＳＳＩＯＮＳ」（代理人整理番号９０２０４－８１８４７８（０３２３００ＵＳ））、および２０１１年9月２９日に提出された同第１３／２４８，９７３号、表題「ＫＥＹ　ＤＥＲＩＶＡＴＩＯＮ　ＴＥＣＨＮＩＱＵＥＳ」（代理人整理番号９０２０４－８１３８９０（０２９５００ＵＳ））に対する優先権を主張し、それらの全開示は、参照により本明細書に組み込まれる。

【図面の簡単な説明】

【０００３】

【図１】少なくとも１つの実施形態に従って、本開示の様々な態様を実現するために使用され得る、コンピューティング環境の例示説明となる実施例を示す。

【図２】少なくとも１つの実施形態に従って、複数のフォルトゾーンを管理するコンピューティングリソースプロバイダを含む、環境の例示説明となる実施例を示す。

【図３】少なくとも１つの実施形態に従って、図２のフォルトゾーン内の環境の例示説明となる実施例を示す。

【図４】少なくとも１つの実施形態に従って、図３に示される環境等の環境を支援するために使用され得る、コンピューティングリソース構成の例示説明となる実施例を示す。

【図５】少なくとも１つの実施形態に従って、コンピューティング環境に関与する様々な要素に異なる範囲の権限が割り当てられ得る例示の様式を示す図表である。

【図６】少なくとも１つの実施形態に従って、メッセージ署名検証プロセスの参加者間で情報が通信され得る例示の様式を示す図表である。

【図７】一実施形態に従って、メッセージに署名するためのプロセスの例示説明となる実施例を示すフローチャートである。

【図８】少なくとも１つの実施形態に従って、署名検証のためのプロセスの例示説明となる実施例を示すフローチャートである。

【図９】少なくとも１つの実施形態に従って、キーを配布する例示の様式を示す図表である。

【図１０】少なくとも１つの実施形態に従って、様々な範囲の権限を提供する様式で、キーを配布する例示の様式を示す図表である。

【図１１】少なくとも１つの実施形態に従って、キー導出のプロセスの例示説明となる実施例を示すフローチャートである。

【図１２】少なくとも１つの実施形態に従って、複数制限キー導出を示す図表である。

【図１３】少なくとも１つの実施形態に従って、署名を導出するための関数の例示説明となる実施例である。

【図１４】少なくとも１つの実施形態に従って、どのように複数キー導出が実行および使用され得るかの、例示説明となる実施例である。

【図１５】少なくとも１つの実施形態に従って、キーが導出され得る例示の様式を示す図表である。

【図１６】少なくとも１つの実施形態に従って、キーが導出され得る方法の別の実施例を示す図表である。

【図１７】少なくとも１つの実施形態に従って、キーが導出され得る方法のさらに別の実施例を示す図表である。

【図１８】少なくとも１つの実施形態に従って、セッションを開始するためのプロセスの例示説明となる実施例を示すフローチャートである。

【図１９】少なくとも１つの実施形態に従って、セッションキーを生成するためのプロセスの例示説明となる実施例を示すフローチャートである。

【図２０】少なくとも１つの実施形態に従って、セッションの間に１つ以上のコンピューティングリソースへのアクセスを得るためのプロセスの例示説明となる実施例を示すフローチャートである。

【図２１】少なくとも１つの実施形態に従って、１つ以上のコンピューティングリソースに対して要求されたアクセスを付与するかどうかを決定するためのプロセスの例示説明となる実施例を示すフローチャートである。
【図２２】少なくとも１つの実施形態に従って、権限を委任するためのプロセスの例示説明となる実施例を示すフローチャートである。
【図２３】少なくとも１つの実施形態に従って、権限の複数の委任の例示説明となる実施例を表す図表である。
【図２４】複数の権限からのキーを使用してキーが導出され得る様式の例示説明となる実施例を表す図表である。
【発明の概要】
【０００４】
以下の説明において、様々な実施形態が説明される。説明の目的で、実施形態の完全な理解を提供するために、特定の構成および詳細が記載される。しかしながら、実施形態が特定の詳細なしに実施され得ることも当業者には明らかとなるであろう。さらに、説明される実施形態を曖昧にしないために、良く知られた特徴は、省略または簡素化され得る。
【０００５】
本明細書において記載および提案される技法は、様々な実施形態に従って、キー生成のためのシステムおよび方法を含む。キーは、様々な目的で、例えば、メッセージ署名スキームにおける認証および参加に使用され得る。一実施形態において、コンピューティングリソースプロバイダは、サービスのユーザデバイスから受信された電子要求に少なくとも部分的に基づいて、コンピューティングサービスを顧客に提供する。サービスは、提供され得る任意の適切なサービスであってよく、限定するものではないが、データへのアクセス、操作を行うためのコンピューティングリソースへのアクセス、データストレージサービスへのアクセス等が挙げられる。
【０００６】
サービスが安全な様式で提供されることを保証するために、本開示の様々な実施形態は、要求が正規であることを保証するために、要求（「メッセージ」とも称される）を認証する技法を利用する。一実施形態において、要求は、以下でさらに詳述されるように、ハッシュメッセージ認証符号（ＨＭＡＣ）アルゴリズムまたは他の適切なアルゴリズムを使用して認証される。
【０００７】
一実施形態において、認証当事者（例えば、サービスのユーザまたはユーザの代わりに動作する当事者）および認証者（例えば、サービスのプロバイダまたはプロバイダの代わりに動作する当事者）の両方は、キーと称され得る秘密信用情報を共有する。認証者は、複数のユーザのために共有された秘密信用情報を記憶し得る。トランザクションの一部として、認証当事者は、共有された秘密信用情報を使用して要求に署名し得、それによって署名を形成する。署名は、要求とともに認証者に提供され得る。認証者は、共有された秘密信用情報のそれ自体のコピーを使用し得、受信された要求のための署名を生成し、生成された署名が受信された署名と一致するかどうかを比較することによって（例えば、受信された署名と同一であることによって）、共有された秘密信用情報を使用して要求が署名されたかどうかを決定する。共有された秘密信用情報を使用して要求が署名されたことが決定された場合、要求は本物であると見なされてよく、したがって要求が満たされるべきであることが決定され得る。
【０００８】
上記対話は対称であるため（すなわち、両方がそれらの役割を果たしているときに共通の情報を利用する）、認証者が保持する共有された秘密信用情報を使用して、両方が認証当事者を認証するか、またはそれらの代わりに動作することができる。結果として、これらの信用を保護するために高度のセキュリティが望ましい。高度のセキュリティを維持することは、マイナスの性能および可用性の結果を有し得る。例えば、高度のセキュリティを維持することは、キーストレージのための集中型システムを維持することを含み得る。

しかしながら、ユーザおよび／またはサービスの追加が集中型システムに大きな負荷をかけるため、そのような集中型システムは、スケーリングボトルネックを引き起こし得る。そのような集中型システムが機能しない場合、要求を認証することは困難または不可能であり得る。したがって、集中化は、セキュリティに対する利点およびサービスのスケーリングおよびサービスの可用性に対する欠点の両方を提供する。

【０００９】

一実施形態において、そのようなシステム（および他のシステム）のマイナスの影響は、認証当事者が共有された秘密信用情報を有し、したがって、アーチファクトとともに署名された要求において特定されるアクセスを得る権限が当てられている可能性が高いことを証明するために使用され得る、共有された秘密信用情報アーチファクトから導出する署名プロトコルを利用することによって低減される。一実施形態において、そのようなアーチファクトは、共有された信用情報自体の代わりに、共有された信用情報の導出に少なくとも部分的に基づく値を署名として許容するように認証者コンピュータシステムを構成することによって得られる。共有された信用情報の導出は、以下でより完全に記載されるように、その導出が共有された信用情報の実際の決定を可能にしないようにするものであり得る。

【００１０】

例えば、一実施形態において、認証当事者は、

ＨＭＡＣ（Ｍ，ＨＭＡＣ（Ｘ，ｃｒｅｄｅｎｔｉａｌ））

を伴う署名を行うことができ、Ｍはメッセージであり、ＨＭＡＣ（Ｘ，ｃｒｅｄｅｎｔｉａｌ）は、共有された秘密信用情報から導出されたアーチファクトである。Ｘの値は、認証当事者および認証者の両方に知られているなんらかの値であってよく、公的に入手可能であり得る。例えば、Ｘは現在の日付であってよく、既定の様式で符号化されて、ＨＭＡＣ（Ｘ，ｃｒｅｄｅｎｔｉａｌ）が、認証当事者および認証者によって一貫して計算されることを保証し得る。別の例として、Ｘは、アーチファクトが使用可能であるサービスの識別子であってよい。さらに別の実施例として、Ｘは、複数の意味論的意味を符号化し得、認証当事者および認証者の両方が一貫してアーチファクトを計算するような様式で提供され得る。意味論的意味は、キーの使用に対する制限であってよく、キーを形成する導出がこれ以上使用されるべきでないことを示す意味を含む。本パラグラフの前述の実施例を組み合わせると、Ｘは、「２０１１０８２５／ＤＤＳ」として符号化されてよく、スラッシュの左側の文字列は日付を表し、スラッシュの右側の文字列は、Ｘで計算されたアーチファクトが使用可能であるサービス名を表す。一般的に、Ｘは、認証当事者および認証者の両方に一貫して符号化された任意の値または一式の値であり得る。以下で論じられるように、ＨＭＡＣ関数以外の他の適切な関数が使用され得ることに留意すべきである。

【００１１】

ＨＭＡＣを利用する実施例に戻ると、一実施形態において、Ｘの値は、追加の利点を提供するために選択される。記述されるように、Ｘは、（必ずしもそうではないが）１つ以上の意味論的意味に対応し得る。一実施形態において、タイムスタンプ、サービス名、地域名等の意味論的意味を使用して、本開示の技法により形成されたアーチファクトが、Ｘから導出されたキーの使用に関する対応する制限を提供するシステムを提供する。このようにして、生成されたキーの漏洩が望ましくない当事者による認証を許可し得るにもかかわらず、キーを符号化するために使用される制限は、キーが漏洩されたときに、悪影響を最小限に抑えることを可能にする。例として、キーを導出するために使用される時間制限は、システムが、送信された署名が、署名送信時に有効であったキーで署名されたかどうかを確認するための効率的な方法を提供する。具体的な例として、現在の日付を使用してキーを導出させ、認証者システムがその現在の日付に送信された署名のみを許容する場合、認証者システムは、異なる日付で導出されたキーを使用して生成された署名が無効であることを決定する。同様に、特定のサービスの識別子で導出されたキーは、別のサービスとの併用で無効となる。他の実施例が以下に提供される。

【００１２】

記述されるように、本開示の様々な技法は、複数のパラメータを使用してキーを導出することを可能にする。一実施形態において、キーは、ＨＭＡＣ関数の複数の使用を通じて複数のパラメータから導出される。例えば、キーは以下のように計算されてよく、

K_S＝ＨＭＡＣ（…ＨＭＡＣ（ＨＭＡＣ（ＨＭＡＣ（Ｋ，P_1），P_2），P_3）…，P_N）

式中、Ｋは、共有された秘密信用情報であり、P_iはパラメータである。キー、Ｋｓを使用して署名を生成してもよく、

Ｓ＝ＨＭＡＣ（K_S，Ｍ）

式中、Ｍは、正規化され得るメッセージである。このようにして、キーは、階層化様式で導出され、キーの部分的導出が分散システムの様々な構成要素に伝えられることを可能にする。例えば、K_{P1}＝ＨＭＡＣ（Ｋ，P_1）が計算されて、分散システムの１つ以上の構成要素に伝えられてよい。K_{P1}を受信する構成要素は、K_{P2}＝ＨＭＡＣ（K_{P1}，P_2）を計算してよく、式中、P_2は、各構成要素に対して同じであり得るか、または一部または全部の構成要素に対して異なり得る。様々な構成要素によって計算されたK_{P2}の値は、その計算を分散システムの他の構成要素に伝えてよく、K_{P3}＝ＨＭＡＣ（K_{P2}，P_3）を計算し得る。各構成要素は、それが計算した結果、および他の構成要素によって算定および計算される可能な結果をキャッシュし得る。このようにして、導出されたキーの算定が分散システムの他の構成要素によって行われ得るため、共有された秘密キーを記憶するデータストア周辺のさらなるセキュリティが提供され得る。

【００１３】

本開示の技法は、セッションの開始も提供する。例えば、論じられるように、共有された秘密信用情報および１つ以上のパラメータが、キーを導出するために使用され得る。したがって、セッションのパラメータが、そのセッション中に使用され得る秘密情報を生成するために使用され得る。信用情報は、要求したユーザによって、またはいくつかの実施形態において、信用情報が伝えられ、１つ以上のコンピューティングリソースへのアクセスが委任されたユーザによって使用されてよい。そのような場合、そのようなアクセスの受任者は、共有された秘密信用情報ではなく、共有された秘密信用情報から導出されたキーを使用するため、より高レベルのセキュリティが維持され、受任者による将来の使用を防ぐために、共有された秘密信用情報を回転させる必要がない。以下でさらに詳述されるように、受任者は、本開示の技法を使用して委任者になってもよく、それらの多くは以下でさらに詳述される。

【発明を実施するための形態】

【００１４】

図１は、様々な実施形態に従って、本開示の態様を実現するための、例示の環境１００の態様を示す。当然のことながら、ウェブベース環境が説明の目的で使用されるが、様々な実施形態を実現するために異なる環境が適宜使用されてよい。環境は、電子クライアントデバイス１０２を含み、それには、適切なネットワーク１０４によって要求、メッセージ、または情報を送信および受信し、デバイスのユーザに情報を返信するように動作可能な任意の適切なデバイスを含み得る。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、携帯型メッセージングデバイス、ラップトップコンピュータ、セットトップボックス、パーソナルデータアシスタント、電子書籍リーダ等が挙げられる。ネットワークは、イントラネット、インターネット、セルラーネットワーク、ローカルエリアネットワーク、または任意の他のそのようなネットワークもしくはそれらの組み合わせを含む、任意の適切なネットワークを含むことができる。そのようなシステムに使用される構成要素は、選択されるネットワークおよび／または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および構成要素は、よく知られているため、本明細書において詳述されない。ネットワーク上の通信は、有線または無線接続、およびそれらの組み合わせによって使用可能であり得る。この例において、要求を受信し、それに応答してコンテンツを提供するために、環境がウェブサーバ１０６を含むので、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、当業者には明らかとなるように、同様の目的を果たす代替デバイスが

使用され得る。

【００１５】

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１０８およびデータストア１１０を含む。連鎖され得るか、または他の方法で構成されてよく、適切なデータストアからデータを取得する等のタスクを行うように相互にやりとりすることができる、いくつかのアプリケーションサーバ、階層、または他の要素、プロセス、もしくは構成要素が存在し得ることが理解されるべきである。本明細書において使用されるとき、「データストア」という用語は、データを記憶し、アクセスし、検索取得することができる、任意のデバイスまたはデバイスの組み合わせを指し、任意の組み合わせおよび数のデータサーバ、データベース、データストレージデバイス、およびデータストレージ媒体を、任意の標準、分散、またはクラスタ化環境に含み得る。アプリケーションサーバは、クライアントデバイスのための１つ以上のアプリケーションの態様を実行するために、必要に応じてデータストアと統合するための任意の適切なハードウェアおよびソフトウェアを含んでよく、アプリケーションのためのデータアクセスおよびビジネス論理の大部分を処理する。アプリケーションサーバは、データストアと協働してアクセス制御サービスを提供し、ユーザに伝送されるテキスト、グラフィック、オーディオ、および／またはビデオ等のコンテンツを生成することができ、この例ではＨＴＭＬ、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。全ての要求および応答の処理、ならびにクライアントデバイス１０２とアプリケーションサーバ１０８との間のコンテンツの送達は、ウェブサーバによって処理され得る。本明細書において論じられる構造化符号は、本明細書の他の部分で論じられる任意の適切なデバイスまたはホストマシン上で実行され得るため、ウェブサーバおよびアプリケーションサーバは必要とされず、単なる例示の構成要素であることが理解されるべきである。

【００１６】

データストア１１０は、特定の態様に関するデータを記憶するために、いくつかの別個のデータテーブル、データベース、または他のデータストレージ機構および媒体を含み得る。例えば、例示されるデータストアは、生産データ１１２およびユーザ情報１１６を記憶するための機構を含み、それらの情報は、生産サイドのコンテンツを提供するために使用され得る。データストアは、報告、分析、または他のそのような目的に使用され得る、ログデータ１１４を記憶するための機構を含むことも示される。例えば、ページ画像情報のため、および正しい情報にアクセスするためにデータストアに記憶される必要があり得る、多くの他の態様が存在し得ることを理解されるべきであり、必要に応じて上に列挙された機構のいずれにも、またはデータストア１１０内の追加の機構内にも記憶され得る。データストア１１０は、それと関連付けられた論理を通じて、アプリケーションサーバ１０８から命令を受信し、それに応答してデータを取得、更新、または他の方法で処理するように動作可能である。一実施例において、ユーザは、あるタイプのアイテムの検索要求を送信してもよい。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識別を検証してよく、カタログ詳細情報にアクセスして、そのタイプのアイテムに関する情報を得ることができる。次に情報は、例えば、ユーザデバイス１０２上のブラウザを介してユーザが見ることができるウェブページ上に列挙する結果において、ユーザに戻され得る。対象の特定のアイテムに関する情報は、ブラウザの専用ページまたはウィンドウ内で見ることができる。

【００１７】

各サーバは、通常、そのサーバの一般的な管理および操作のための実行可能なプログラム命令を提供するオペレーティングシステムを含み、通常、サーバのプロセッサによって実行されるとき、サーバがその意図される機能を実行することができる命令を記憶するコンピュータ可読ストレージ媒体（例えば、ハードディスク、ランダムアクセスメモリ、読み取り専用メモリ等）を含む。サーバのオペレーティングシステムおよび一般的な機能性に適切な実装は、既知であるか、または市販されており、特に本明細書における開示に照らして、当業者によって容易に実装される。

【００１８】
一実施形態における環境は、１つ以上のコンピュータネットワークまたは直接接続を使用して、通信リンクを介して相互接続されるいくつかのコンピュータシステムおよ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、当業者であれば、そのようなシステムが、図１に示されるよりも少数または多数の構成要素を有するシステム内で等しく良好に動作し得ることを理解するであろう。したがって、図１におけるシステム１００の描写は、性質的に例示的であると見なされるべきであり、本開示の範囲に限定するものではない。
【００１９】
図２は、少なくとも１つの実施形態に従って、複数のフォルトゾーン２０４を管理するコンピューティングリソースプロバイダ２０２を含む環境２００の例示説明となる実施例を示す。コンピューティングリソースプロバイダは、一実施形態において、１人以上の顧客２０６のためにコンピュータハードウェアを運用する組織である。コンピューティングリソースプロバイダは、様々な方法でコンピューティングリソースを提供し得る。例えば、一実施形態において、コンピューティングリソースプロバイダ２０２は、顧客２０６によって使用するための構成されるハードウェアを管理する。コンピューティングリソースプロバイダ２０２は、顧客２０６がハードウェアを使用してコンピューティングリソースを、プログラムによって構成することを可能にするインターフェースを提供する。例えば、コンピューティングリソースプロバイダは、顧客によってプログラムで制御される仮想コンピュータシステムを実行する、ハードウェアサーバを維持してよい。別の実施例として、コンピューティングリソースプロバイダ２０２は、高耐久性データストレージおよびブロックレベルのデータストレージ等の遠隔データストレージソリューションを提供するために、様々なデータストアを管理し得る。
【００２０】
フォルトゾーンは、一実施形態において、各フォルトゾーンが別のフォルトゾーンの故障に耐えるように、１つ以上のフォルト境界によって分離されるコンピューティングリソースの集合である。実施例として、各フォルトゾーン２０４は、別個のデータセンターであってよい。したがって、恐らく停電または他の妨害イベントに起因して１つのデータセンターが運転を中断した場合、他のデータセンターは、運転を継続し得る。フォルトゾーンはそれぞれ、異なる地理的場所にあってよく、フォルトゾーンのうちのいくつか、または全部が地政学的境界によって分離され得る。例えば、フォルトゾーンの２つ以上は異なる国にあってよい。例示の目的で、本開示は、フォルトゾーンがデータセンターである多数の例を提供することに留意すべきである。しかしながら、フォルトゾーンは、多数の他の方法で定義され得る。例えば、同じデータセンター内の別個の部屋は、様々な実施形態に従うと、別個のフォルトゾーンとして見なされ得る。別の実施例として、同じ場所にあるが、異なるバックアップ発電機により支援される、および／または異なるネットワークリソースにより支援されるコンピューティングリソースは、異なるフォルトゾーンとして見なされ得る。さらに別の実施例として、データセンターを、データセンターの各群がフォルトゾーンとして見なされ得るように群化してもよい。さらに、フォルトゾーンに障害が発生し得る多くの理由があり得、送電網の稼働、パブリックネットワークの稼働、電力の政治的主張に関する理由、および他の理由を含む。
【００２１】
一実施形態において、顧客２０６は、インターネット等のネットワーク２０８によってコンピューティングリソースプロバイダ２０２と通信する。顧客２０６は、フォルトゾーン２０４の１つ以上において構成されたリソースを有してよく、リソースを構成および操作するために、コンピューティングリソースプロバイダのウェブサービスアプリケーションプログラミングインターフェース（ＡＰＩ）を起動させるメッセージ等の電子メッセージを送信することによってリソースと通信し得る。顧客は、顧客のリソースに影響を及ぼす、可能性のある障害の影響を低下させるために、複数のフォルトゾーン内のリソースを利用してよい。コンピューティングリソースプロバイダ２０２のリソースを利用して公衆

がアクセス可能なウェブサイトを運営する顧客は、例えば、別個の複数フォルトゾーン内にウェブサーバおよび他のサーバを維持し、１つのフォルトゾーン内のサーバが故障した場合に、別のフォルトゾーン内のサーバにアクセスすることによって、公衆が依然としてウェブサイトにアクセスできるようにする。

【００２２】

図３は、フォルトゾーン３０２の内側の環境３００の例示説明となる実施例を示し、そのフォルトゾーンは、図２に例示されるコンピューティングリソースプロバイダのフォルトゾーンであり得る。フォルトゾーン３０２は、一実施形態において、顧客のために様々なサービスを提供するために使用されるコンピューティングリソースを含む。例えば、図３に示されるように、フォルトゾーン３０２は、永続的データストレージサービスを提供するために使用されるコンピューティングリソースを含み、顧客のために比較的大量のデータを安価に重複して記憶し得る。そのようなサービスは、大量のデータストレージおよび／またはデータストレージのセキュリティが必要とされるが、入力／出力性能が高優先度でない場合に使用され得る。フォルトゾーン３０６は、ブロックレベルのストレージデバイス、物理デバイス、および／または仮想デバイスの使用を顧客に提供する、ブロックデータストレージサービス３０６を含んでもよい。顧客は、例えば、ブロックレベルのストレージデバイスを、同じく顧客に利用されるコンピュータシステムに取り付けてもよい。コンピューティングサービスを顧客に提供し得る仮想コンピュータシステムサービス３０８も示される。一実施形態において、仮想コンピュータシステムサービス３０８は、コンピューティングリソースプロバイダによって維持される物理サーバ上の顧客のための仮想コンピュータシステムを実装することによって、コンピューティングサービスを提供するが、物理コンピュータシステムが顧客使用のために顧客に割り当てられる等の変型が可能である。仮想コンピュータシステムに関する一実施形態において、顧客は、それらのニーズに従って仮想コンピュータシステムをプログラムで管理してよい。例えば、図３に示されるように、顧客は、仮想コンピューティングサービスプロバイダの顧客のサーバ顧客に対する仮想コンピュータシステムサービス３０８の仮想コンピュータシステムを構成してもよい。仮想コンピュータシステムは、例えば、公衆がアクセス可能なウェブサイトを稼働するように構成されてよい。仮想コンピューティングリソースプロバイダの顧客およびその顧客の顧客は、様々な実施形態において、図２に関して上述のネットワーク２０８であり得る、ネットワーク３１０によりサービスと通信することによって、フォルトゾーン３０２内で運用される様々なサービスにアクセスしてよい。

【００２３】

図３に示される様々な実施形態が、図面に示され、本明細書に記載される全ての例示的な実施形態と同様に、性質的に例示であり、変型も本開示の範囲内であると見なされることに留意すべきである。例えば、例示されるものとは異なる他のサービスは、例示されるサービスに加えて、または代わりにフォルトゾーン３０２内で提供され得る。図３において省略（「・・・」）で示されるように、例えば、追加のサービスがフォルトゾーン３０２内で稼働され得る。さらに、いくつかのサービスは他のサービスを利用してもよい。例えば、複数のサービス（例えば、ブロックレベルのデータストレージサービス３０６および仮想コンピュータシステムサービス３０８）は、関連データベースサービス、電子メールサービス、および一般に、コンピューティングリソースプロバイダのリソースを使用して提供され得る任意のタイプのコンピューティングサービス等の他のサービスを提供するために一緒に利用されてよい。

【００２４】

図３に例示されるように、コンピューティングリソースプロバイダのサービスのそれぞれは、別個の検証手段３１２を含んでよい。検証手段は、コンピューティングデバイス、コンピューティングデバイスの集合、アプリケーションモジュール、または顧客によって、および可能性として他のコンピュータシステムによって行われた様々な証明を検証する他のリソースであってもよい。一実施形態において、検証手段３１２のそれぞれは、以下でさらに詳述されるように、本明細書において様々な実施形態に従って生成され、次にコ

ンピューティングリソースにアクセスする要求と併せて顧客によって提供されるメッセージ署名を検証する。キーおよび他の関連情報は、中央キー権限者から検証手段に伝播されて、検証手段が情報を検証することを可能にし得る。検証手段を有する各サービスは、特定の実施形態の例示説明となる実施例であるが、他の設定が本開示の範囲内であることに留意すべきである。例えば、単一の検証手段が、複数のサービス、ひいては全サービスを支援し得、さらには複数のフォルトゾーンを支援し得る。

【００２５】

図４は、少なくとも１つの実施形態に従って、図３に示される環境等の環境を支援するために使用され得る、コンピューティングリソース構成の例示説明となる実施例を示す。図４は、図３内のフォルトゾーンがデータセンターである特定の実施例を特定的に示す。したがって、図４に戻ると、データセンター４０２は、複数のサーバラック４０４～４０６を含んでよい。データセンター４０２は、図４に示されるデータセンター等の本開示の様々な実施形態において使用され得る、１つ以上のデータセンターの実施例である。サーバラック４０４とサーバラック４０６との間の省略（「・・・」）は、データセンター４０２が、任意の適切な数のサーバラックを含んでよいことを示すが、明確にするために、図４では２つのみが示される。各サーバラック４０４～４０６は、複数のサーバコンピュータ４０８～４１４および４１６～４２２に対する電力およびデータ通信等のサービスの維持に関与し得る。ここでも省略（「・・・」）は、サーバラック４０４～４０６が任意の適切な数のサーバコンピュータを含み得ることを示す。例えば、サーバコンピュータ４０８～４２２は、１つ以上の仮想コンピュータシステム（ＶＣＳ）サーバおよび／または１つ以上のデータストアサーバを含み得る。各サーバ４０８～４２２は、実装リソース専用ユニットに対応し得る。

【００２６】

図４において、各サーバラック４０４～４０６は、ラックスイッチ４２４～４２６を含むように描かれる。ラックスイッチ４２４および４２６は、デジタルデータのパケットと、それらそれぞれの一式のサーバコンピュータ４０８～４１４および４１６～４２２とのスイッチングに関与し得る。ラックスイッチ４２４～４２６は、データセンタースイッチング構造４２８に通信で接続され、次にデータセンター４０２を、インターネットを含む１つ以上の他のコンピュータネットワークに接続する、一式のエッジルータ４３０に通信で接続され得る。スイッチング構造は、１つ以上のスイッチング層に配列された１つ以上のスイッチタイプの複数の相互接続されたスイッチ４３２～４３８（明確にするために、図４では４つのみが示される）、ならびにルータ、ゲートウェイ、ブリッジ、ハブ、リピータ、ファイヤーウォール、コンピュータ、およびそれらの適切な組み合わせを含む、任意の適切な一式のネットワーキング構成要素を含み得る。少なくとも１つの実施形態において、ラックスイッチ４２４～４２６およびエッジルータ４３０は、スイッチング構造４２８の一部として見なされる。ラックスイッチ４２４～４２６、エッジルータ４３０、およびスイッチング構造４２８の構成要素は、図２のネットワークハードウェア２２４の例である。

【００２７】

上記のように、本開示の様々な実施形態は、異なる理由で付与される様々なレベルの権限を可能にする。図５は、コンピューティング環境に関与する様々な要素が、少なくとも１つの実施形態に従って、異なる範囲の権限を割り当てられ得る例示の様式を示す図表である。図５において、コンピューティングリソースプロバイダ５０２が示される。一実施形態において、コンピューティングリソースプロバイダ５０２は、図５に例示されるように、そのリソースに対して権限を有し、その権限をリソースの使用において、様々な参加者の間で分配することができる。本明細書における他の例示および説明と一致する例示の目的で、図５は、ドメインに対して権限を有するコンピューティングリソースプロバイダ５０２を示す。しかしながら、本開示の実施形態は、権限ドメインの他の所有者にも適用可能である。例えば、権限の所有者は、政府もしくは政府機関、別の機関の下部組織、または一般にいくつかのドメインに対して権限を有する任意のエンティティであってよい。

【００２８】
図５の例示説明となる実施例に戻ると、コンピューティングリソースプロバイダ５０２は、異なるサブエンティティが、異なるサブドメインに対して権限を有することを可能にすることによってその権限を管理する。例えば、この図に示されるように、コンピューティングリソースプロバイダのいくつかのフォルトゾーン５０４のそれぞれには、コンピューティングリソースプロバイダ５０２のドメインの対応するサブドメインが提供される。したがって、各フォルトゾーンは、それ自体のリソースに対して権限を有し得るが、別のフォルトゾーンのリソースに対しては権限を有さない（しかしながら、いくつかの例では、いくつかのサブドメインに対する権限が共有されてもよい）。したがって、一実施形態に従って、フォルトゾーンは、フォルトゾーン内のコンピューティングリソースへのアクセスをユーザに提供し得るが、別のフォルトゾーンのコンピューティングリソースへのアクセスは提供し得ない。
【００２９】
上記のように、各フォルトゾーンは、１つ以上のサービス５０６を含み得る。したがって、図５に示されるように、各サービスは、対応するフォルトゾーン５０６のドメインのサブドメインに対応可能であり得る。したがって、サービスは、一実施形態において、そのサービスによってアクセス可能なリソースへのアクセスを提供することができるが、他のサービスによってアクセス可能なリソースへのアクセスは提供できない。各サービスは、１人以上の顧客５０８に提供され得るため、各顧客は、対応するサービス５０６の権限のサブドメインに関与し得る。したがって、一実施形態において、顧客は、対応するサービスに関与するそれ自体のリソースへのアクセスを提供し得るが、別の顧客に対するアクセスは提供し得ない。具体的な例示説明となる実施例として、サービスが仮想コンピューティングリソースサービスである場合、顧客は、それ自体の仮想コンピュータシステムへのアクセス（例えば、パブリックアクセス）を提供し得るが、許可なしでは、他の顧客の仮想コンピュータシステムへのアクセスを提供することはできない。
【００３０】
記載のとおり、図５に示される権限の特定の割り当ては、例示説明の目的であり、多数の変型が本開示の範囲内であると見なされる。記載のとおり、本開示の実施形態は、コンピューティングリソースプロバイダによって管理されるドメインの外側にある権限のドメインに適用可能であり、サブドメインは、特定のニーズおよび環境に従って決定され得る。さらに、図５は、権限の最小サブドメインを有する仮想リソースプロバイダの顧客を示す。しかしながら、本開示の技術は、顧客ドメインを１つ以上のサブドメインに分割することを可能にし得る。
【００３１】
本開示の様々な実施形態は、メッセージ署名に関する。図６は、少なくとも１つの実施形態に従って、メッセージ署名検証プロセスの参加者の間で情報が通信され得る例示の様式を示す図表６００である。一実施形態において、キーソース６０２は、メッセージ送信者６０４および署名検証手段６０６の両方にキーを提供する。キーソースは、少なくともメッセージ送信者６０４および署名検証手段６０６にキーを提供するように構成されたコンピュータシステムであり得る。キーソースはまた、本明細書に記載される様々な実施形態を含む、様々な技術を使用してキーを生成し得るか、または別のソースから生成されたキーを得てもよい。メッセージ送信者６０４は、メッセージおよび署名を署名検証手段６０６に送信するように構成されたコンピュータシステム、または署名検証手段６０６に関連して動作する他の構成要素であり得る。メッセージ送信者６０４のコンピュータシステムは、例えば、コンピューティングリソースプロバイダの顧客のコンピュータシステムであり得る。署名検証手段６０６は、以下で論じられるように、メッセージおよび署名を受信し、その署名を分析してメッセージが本物であることを検証するように構成されたコンピュータシステムであり得る。つまり、署名検証手段６０６は、受信された署名およびメッセージを分析して、署名が正しいキーＫを使用して生成されたかどうかを決定し得る。図６は、キーソース６０２が、メッセージ送信者６０４と署名検証手段６０６とを分離す

ることを示すが、メッセージ送信者または署名検証手段のいずれかもキーソースであり得ることに留意すべきである。例えば、コンピューティングリソースプロバイダの顧客は、それら自身のキーを提供し得る。次に顧客キーは、署名の検証のために署名検証手段に提供されてよい。さらに、メッセージ送信者６０４および署名検証手段６０６は、それぞれ異なるキーをキーソース６０２から受信し得る。例えば、メッセージ送信者６０４は、キーを受容してよく、署名検証手段６０６は、本開示の様々な実施形態を使用して、メッセージ送信者６０４によって受信されたキーから導出されたキーを受信し得る。

【００３２】

図６に示されるように、署名検証手段６０６は、メッセージおよび対応する署名をメッセージ送信者６０４から受信する。メッセージは、例えば、コンピューティングサービス６０８へのアクセスの電子要求であり得る。メッセージは、例えば、ウェブサービスに対するＡＰＩコールを符号化し得る。署名およびメッセージの分析が、そのメッセージが本物であることを示す場合、次に署名検証手段は、メッセージ送信者が要求されたアクセスを有し得ることをサービス（またはそのサービスへのアクセスを制御する構成要素）を通知する。例えば、署名検証手段は、受信されたメッセージをサービスに渡し、そのサービスが要求を満たすことを可能にし得る。したがって、サービスは、上述の様々なサービス等の要求を満たすために動作可能なコンピュータシステムであってよい。図６の様々な構成要素および他の構成要素に関する様々な説明は、それらの構成要素が、ある動作を行うように構成されたコンピュータシステムとして実装され得るとして説明するが、構成要素は、その動作を行うように集約的に構成されたコンピューティングデバイスのネットワーク等の複数のコンピューティングデバイスをも含み得ることに留意されたい。

【００３３】

図７は、一実施形態に従って、メッセージに署名するためのプロセス７００の例示説明となる実施例を示すフローチャートである。プロセス７００（もしくは本明細書に記載される任意の他のプロセス、あるいはそれらの変型および／または組み合わせ）の一部または全部は、実行可能な命令を備えて構成された１つ以上のコンピュータシステムの制御下で行われてよく、１つ以上のプロセッサ上でハードウェアにより集約的に実行するコード（例えば、実行可能な命令、１つ以上のコンピュータプログラム、もしくは１つ以上のアプリケーション）、またはそれらの組み合わせとして実装されてよい。コードは、コンピュータ可読ストレージ媒体上で、例えば、１つ以上のプロセッサによって実行可能な複数の命令を含むコンピュータプログラムの形態で記憶されてもよい。コンピュータ可読ストレージ媒体は、非一時的であり得る。

【００３４】

一実施形態において、プロセス７００は、キーＫを得ること７０１を含む。キーは、任意の適切な様式で得ることができる。例えば、キーは、プロセス７００を行うコンピュータシステムによって生成されてよい。キーは、プロセス７００を行うコンピュータシステムによって電子的に受信され得る。一般的に、キーを得ることは、任意の適切な様式で行われてよい。キーは、利用される特定の署名アルゴリズムのための任意の適切なキーであってよい。例えば、ハッシュベースのメッセージ認証符号（ＨＭＡＣ）スキームが、セキュアハッシュアルゴリズム（ＳＨＡ）－２５６暗号ハッシュ関数とともに使用されている場合、キーは、例えば、６４バイト以下のシーケンス等のバイトシーケンスであり得る。異なる暗号ハッシュ関数、例えば、ＳＨＡ－２２４、ＳＨＡ－３８４、およびＳＨＡ－５１２も使用され得る。

【００３５】

一実施形態において、プロセスは、メッセージＭを正規化して、正規化されたメッセージM_cを形成することも含む。メッセージを正規化することは、検証手段がそのメッセージの署名が有効であるかどうかを検証することを可能にする形式で、メッセージ内に情報を配置することを含み得る。一般に、多くの情報通信プロトコルは、メッセージを成すビットを変換するが、そのメッセージは意味的に同一のままである。結果として、２つの意味的に同一のメッセージが、異なるビットセットを含んでよく、したがって異なる署名を

生じ得る。したがって、正規化は、署名が検証され得ることを保証する、単純な方法を可能にする。しかしながら、本開示のいくつかの実施形態は、メッセージの正規化を必要としないことに留意すべきである。例えば、利用される様々なプロトコルが、異なるビットセットを含む意味的に同一のメッセージを生じない場合、正規化は必須でない場合があり、省略されてよい。一般的に、正規化は、署名されたメッセージの操作なしに、署名検証が良好に行われ得るいかなる場合においても省略されてよい。

【００３６】

一実施形態において、署名は、ＨＭＡＣ（Ｋ，M_c）を計算することによって生成され、ＨＭＡＣ（）は、上述のようなＨＭＡＣ関数である。ＨＭＡＣ関数は、本開示の様々な実施形態に対してそれらを特に有用にするいくつかの特性を有する。例えば、ＨＭＡＣ関数は、コンピュータシステムによって効率的に計算することができ、それによって他のタスクに対して使用可能なコンピューティングリソースを残す。さらに、ＨＭＡＣ関数は原像計算困難性（非変換性）である。例えば、ＫがキーでありＭがメッセージである署名Ｓ＝ＨＭＡＣ（Ｋ，Ｍ）が与えられた場合、本質的にキーＫに関する情報は得られない。例えば、ＳからＫを決定することは、計算上不可能であるか、または少なくとも実践的はない。ＨＭＡＣ関数は第二原像計算困難性でもある。言い換えれば、Ｓ＝ＨＭＡＣ（Ｋ，Ｍ）およびＭが与えられた場合、Ｓ＝ＨＭＡＣ（Ｋ，Ｍ′）となるように、Ｍとは異なるメッセージＭ′を決定することは不可能であるか、または少なくとも計算上実践的でない。さらに、ＨＭＡＣ関数は、偽造困難性である。例えば、Ｓ＝ＨＭＡＣ（Ｋ，Ｍ）のオラクルが与えられた場合、そのオラクルをＮ回（Ｎは正の整数）クエリすることは、最大Ｎ個の署名－メッセージ対を可能にする。言い換えれば、一式の署名－メッセージ対が与えられた場合、キーを決定することや、またはそのセット内にないメッセージに対して正しい署名を生成する関数を決定することは不可能であるか、または計算上実践的でない。

【００３７】

ＨＭＡＣ関数は、様々な実施形態に対して特に有用であるが、他の関数も使用することができる。例えば、ＨＭＡＣ関数の上記特性を持つ任意の関数が使用されてもよい。さらに、必ずしも上記特性の全部（またはいずれか）を有するとは限らない他の関数は、例えば、セキュリティが最大の関心事でない場合、および／またはセキュリティが関心事であるが、他の機構を通じて維持される場合に使用され得る。様々な実施形態の様々な例示説明は、ＨＭＡＣ関数への特定の入力を示すが、変型も可能であることに留意すべきである。例えば、ＨＭＡＣ関数（または他の関数）の入力は異なり得る。上述のように、例えば、ある入力はキーである。しかしながら、この入力は、キーから導出され得るか、またはそうでなければ少なくとも部分的にキーに基づき得る。例示説明となる実施例として、入力は、接尾辞、接頭辞、またはその他としてキーに追加される、署名スキーム識別子（恐らくバージョン識別子）等の情報とともにキーを含み得る。別の実施例として、入力は、別のキーであり得る、キーの情報へのマッピングを使用することによって得られる情報であってよい。同様に、メッセージとして示される入力は、メッセージから導出され得る。本開示の範囲内であると考えられる別の例示の変型として、署名は、ＨＭＡＣ関数の出力ではないが、ＨＭＡＣ関数（または他の適切な関数）の出力から導出された１つ以上の値であり得る。いくつかの実施形態において、キーおよびメッセージは、逆順で関数に渡され得る。

【００３８】

図７の説明に戻り、署名がＨＭＡＣ（Ｋ，Ｍｃ）を計算することによって一旦生成されると、その署名およびメッセージＭは、署名を検証するコンピューティングデバイス、またはメッセージおよび署名の通信のためにインターフェースを提供するコンピューティングデバイス等の署名検証プロセスに関与する別のコンピューティングデバイスであり得る、受信者に提供される７０８。本明細書に明示的に記載される全ての実施形態と同様に、変型は、本開示の範囲内であると見なされる。例えば、正規化されたメッセージM_Cが、メッセージＭの代わりに、またはそれに加えて受信者に提供され得る。さらに、メッセージＭおよび署名を受信者に提供することは、キーをキー識別子と関連付けるデータストア

において、識別するために使用され得るキー識別子等の他の情報を提供することを含んでもよい。さらに、以下に論じられる、ポリシーを符号化するパラメータ等の他の情報が、メッセージMおよび署名とともに提供されてよい。

【００３９】

図８は、少なくとも一実施形態に従って、署名検証のためのプロセス８００の例示説明となる実施例を示すフローチャートである。図８に示されるプロセス８００は、図２に記載されるような検証手段によって行われてよい。さらに、プロセス８００は、署名およびメッセージの受信に応答して、例えば、図７のプロセス７００を行った別のコンピュータシステムに応答して行われてよい。一実施形態において、プロセス８００は、上述のように、キーＫを得ること８０２を含む。キーＫを得ることは、様々な実施形態において他の動作を含んでもよい。例えば、プロセス８００が、複数のキーから（例えば、コンピューティングリソースプロバイダの複数の顧客から）生成された署名を検証するコンピュータシステムによって使用される場合、キーＫを得ることは、データストア内の複数のキーからキーを選択することを含む。データストアは、様々なキーを、検証のための署名を送信するものと関連付けてよい。例えば、コンピューティングリソースプロバイダの各顧客は、データストアを参照し、適切なキーを識別するために使用されるキー識別子（または複数のキー識別子）を有してよい。キー識別子は、メッセージおよびその署名の送信に関連して送信され得るか、またはそうでなければログイン信用情報の送信時等に決定され得る。キー識別子の受信者（例えば、メッセージ検証手段）は、データストアを参照してキー識別子に対応するキーがデータストア内にあるかどうかを決定してよく、そうでない場合は、次に、例えば、本明細書に記載される技術を使用して、共有された秘密信用情報から直接または間接的にキーを導出することによってキー自体を生成してよい。これを可能にするために、受信者は、一実施形態において、受信者が既に持っている情報（例えば、共有された秘密信用情報から導出されたキー）からキーを導出するために必要な情報を符号化する、キー導出パスへのアクセスを有してよい。この情報は、署名の付いたメッセージの送信者から受信者に提供され得るか、またはそうでなければ受信者が入手できるようにし得る。例えば、受信者は、現在の日付で、その割り当てられた領域およびコードを使用してキーを自動的に生成するようにプログラム化され得る。一般的に、署名を生成するために使用されたキー（またはいくつかの実施形態では、署名を検証するために使用され得る別のキー）を得る任意の方法を使用することができる。受信者は、目前の要求、または受信者に既知である、ある種の他の特性に関して、許容できるキーおよび許容できないキー導出パスに関してポリシーを実施し得る。

【００４０】

一実施形態において、署名ＳおよびメッセージＭが受信される８０４。署名ＳおよびメッセージＭは、図７のプロセス７００を行ったコンピューティングデバイス等の送信者から電子的で受信され得る。次にメッセージＭは、一実施形態に従って、M_cを決定するように正規化される８０６。メッセージＭの正規化は、様々な実施形態において、署名Ｓが検証され得ることを保証する。したがって、一実施形態において、プロセス８００は、ＨＭＡＣ（Ｋ，M_c）を計算することによって署名Ｓ′を生成すること８０８を含む。一実施形態において、Ｓ′は、ＨＭＡＣ（Ｋ，M_c）に等しいが、Ｓ′は、様々な実施形態においてＨＭＡＣ（Ｋ，M_c）から導出され得る。例示の目的で、プロセス８００の残りは、Ｓ′＝ＨＭＡＣ（Ｋ，M_c）であるが、数値的変型が本開示の範囲内であるという前提で説明される。

【００４１】

したがって、一実施形態において、Ｓ′が受信された署名Ｓに等しいかどうかの決定が行われる８１０。言い換えれば、例えば、それがキーＫを使用して生成された署名であるため、受信された署名が十分であるかどうかの決定が行われる。したがって、一実施形態において、Ｓ′およびＳが等しくないことが決定された場合８１０、署名は検証されない８１２。しかしながら、Ｓ′がＳに等しい場合、署名が検証される８１４。署名が検証されたかどうかに応じて、適切な動作が行われ得る。例えば、メッセージが、コンピューテ

ィングリソースへのアクセスの要求であった場合、要求されたアクセスは（少なくとも一時的に）否定され得る。同様に、メッセージがコンピューティングリソースへのアクセスの要求であり、署名が検証された場合、要求されたアクセスが許可され得る。しかしながら、行われる適切な動作は、署名が受信および検証される理由（複数可）に応じて様々な実施形態において広く異なり得ることに留意すべきである。

【００４２】

上記のとおり、本開示の様々な実施形態は、多数の環境に適用する。多くの環境において、セキュリティ管理の様々な態様の集中管理を有することが有用である。図９は、例えば、少なくとも一実施形態に従って、キーを配布する例示の様式を示す図表９００である。図９において、中央キー権限者は、ある組織によって利用される様々なキーを含む、１つ以上のデータストア（集約的に「データストア」と称される）を維持する。キーは、例えば、組織のコンピューティングデバイスのユーザに対応し得る。ユーザ群の各ユーザには、例えば、１つ以上のキーが割り当てられてよい。一実施形態において、少なくともいくつかのキーが、組織の顧客（および／または顧客のユーザ）に対応する。例えば、一実施形態において、組織は、コンピューティングリソースプロバイダであり、コンピューティングリソースプロバイダの各顧客は、顧客のユーザが、コンピューティングリソースプロバイダによって維持されるコンピューティングリソースにアクセスすることを許可する１つ以上のキーに対応する。図７とともに上述の変型に従って、図８のプロセス８００の他の適合もまた、本開示の範囲内である。

【００４３】

図９に示されるように、キー権限者９０２は、キーを複数のキーゾーン９０４に伝播する。キーゾーンは、受信されたキーが有効である組織のドメインであり得る。例えば、図２を参照すると、各キーゾーン９０４は、データセンター等のフォルトゾーンに対応し得る。キーゾーンは、必ずしもそうとは限らないが、地理的に定義され得る。例えば、各キーゾーンは、国、地域、または他の地理的に定義された地域に対応し得る。キーゾーンは、他の方法で定義されてもよい。例えば、各キーゾーンは、コンピューティングリソースプロバイダによって組織の顧客に提供されるサービス等に対応し得る。キーゾーンは、示されてはいないが、サブゾーンを有し得る。例えば、キーゾーンは、国に対応し得る。その国の内には複数の地域が存在し得、それぞれキーゾーンのサブゾーンに対応する。キーは、そのような実施形態においてサブゾーンに伝播され得る。

【００４４】

図９に示されるように、キーゾーン９０４は、キーゾーンの１つ以上の検証手段９０６にキーを伝播し得る。例えば、キーゾーンがデータセンターに対応する場合、データセンターのコンピューティングデバイスは、そのデータセンター内でコンピューティングリソースによって支援される複数のサービスのそれぞれに対する検証手段にキーを伝播し得る。このように、検証手段を使用して、様々な要求に関連して送信された署名を検証することができる。これは、特に要求が行われるサービスからキー権限者９０２が地理的に遠位である場合、キー権限者自体のコンピューティングリソースが署名を検証するのを軽減し、待ち時間および帯域幅要件も減少させる。

【００４５】

キー伝播は様々な方法で行われてよい。一実施形態において、キーは、様々な受信者に対して、セキュアチャネルにより配布される。いくつかの実施形態において、キー権限者は、各キーゾーンに同一のキーを伝播する。またいくつかのキーは、複数のキーゾーンにおいて使用可能であり得る。キー権限者９０２は、複数のキーゾーンにおいて使用可能であるキーを、それらの複数のキーゾーンに伝播し得る一方で、それらのキーが使用できないキーゾーンにキーを伝播しないようにする。このようにして、コンピューティングリソースプロバイダの実施例において、キー権限者９０２は、顧客に対するキーを、その顧客がキーを使用できるキーゾーンのみに、例えば、顧客のコンピューティングリソースを維持するために使用されるデータセンター等に伝播し得る。

【００４６】

本開示の様々な実施形態はまた、多くの利益を提供する様式でキー伝播を提供する。図１０は、少なくとも一実施形態に従って、様々な権限の範囲を提供する様式でキーを配布する例示の様式を示す図表１０００である。図１０にあるように、図表１０００は、例えば、図９に関連する上記説明に従って、キーを直接または間接的に様々なキーゾーン１００４および検証手段１００６に伝播するキーＫを有するキー権限者１００２を含む。例示の目的で、図表１０００は、単一のキーＫ、およびＫから導出されたキーに関して説明されるが、本明細書に記載される実施形態では、キー権限者が多数のキーに対してそのような動作を行うときに適用される。

【００４７】

図１０に示されるように、キーＫは、Ｋから導出される他のキーの基礎として使用される。例えば、ＫからキーＫ$_1$が導出され、第１のキーゾーン（キーゾーン$_1$）に伝播される。したがって、キーＫ$_1$（またはキーＫ$_1$から導出されたキー）は、第１のキーゾーンにおいて使用可能であるが、Ｋ$_1$（またはキーＫ$_1$から導出されたキー）を有しない他のキーゾーンでは使用できない。同様に、多数の他のキーゾーンのそれぞれは、キーＫから導出された対応する異なるキーを受信する。図１０は、キー権限者１００２から対応するキーゾーンに伝播されるキーＫから導出されたキーを示すが、変型も可能であることを留意すべきである。例えば、キーＫは、キーゾーンに伝播されてよく、キーＫを受信する各キーゾーンは、キーＫを使用して１つ以上の対応するキーを導出し得る。例えば、「キーゾーン$_1$」と標識されるキーゾーン１００４は、キーＫを受信して、Ｋ$_1$を導出し得る。一般的に、キー導出および伝播に関与する様々なタスクは、様々な実施形態に例示されるものとは異なって行われてもよい。

【００４８】

図１０の例示説明となる実施例に示されるように、キーゾーン１００４によって受信されたキーを使用して、さらに伝播されるキーを導出する。例えば、「キーゾーン$_2$」と標識されるキーゾーン１００４を参照すると、キーＫから導出されるキーＫ$_2$を使用して追加のキーＫ$_2$′およびＫ$_2$′′を導出する。キーＫ$_2$′およびＫ$_2$′′は、署名を検証する際に検証手段１００６によって使用するために、対応する検証手段１００６に伝播される。したがって、Ｋ$_2$′を受信する検証手段は、一実施形態において、Ｋ$_2$′′を使用して生成された署名を検証することができるが、Ｋ$_2$′を受信しなかった検証手段は、署名を検証することができない。図９および１０に示される様式（またはその変型）でキーを伝播することによって利益が得られる。例えば、１つ以上の集中型検証手段の代わりに複数の場所にある多数の検証手段にキーを伝播することによって、より短い待ち時間が達成される。さらに、図１０を参照すると、導出されたキーを、次いで追加のキーを導出する他のデバイスに伝播することによって、複数の場所にある複数のデバイス上に計算を拡散することができ、それによってより迅速なキー導出およびフォルトトレランスの増加を可能にする。

【００４９】

キーの導出は、多数の方法で行われ得る。図１１は、少なくとも一実施形態に従って、キー導出のプロセス１１００の例示説明となる実施例を示すフローチャートである。一実施形態において、プロセス１００は、例えば、上述の様式でキーＫ$_i$を得ること１００２を含む。キーＫ$_i$は、上述のような任意の適切なキーであり得る。さらに、キーＫ$_i$は、必ずしもそうとは限らないが、例えば、プロセス１１００または別のプロセスの実行によって、別のキーから導出され得る。キーＫ$_i$を得ると、新たなキーがＫ$_i$から導出される。図１１の例示説明となる実施例において、新たなキーＫ$_{i+1}$は、ＨＭＡＣ（Ｋ$_i$，Ｒ$_{i+1}$）として計算され（または少なくとも部分的にそれに基づき）、式中、Ｒ$_{i+1}$は、キーＫ$_{i+1}$に対する１つ以上の制限を識別する情報である。Ｒ$_{i+1}$は、例えば、どこでキーＫ$_{i+1}$が使用可能であるかを示す情報を符号化するビットのシーケンスであり得る。例えば、Ｒ$_{i+1}$は、キーＫ$_{i+1}$が使用され得るキーゾーンを符号化し得る。制限は、地理、時間、ユーザ識別、サービス等に少なくとも部分的に基づいてよい。例となる制限は、以下の説明において提供される。

【００５０】
さらに、以下でさらに論じられるように、プロセス１１００は、キーを導出するために複数可使用されてもよい。例えば、プロセス１１００（またはその変型）を使用して生成されたキーは、同一または別の制限を使用して、別のキーを生成するために使用されてよい。図の用語を使用すると、R_{i+1}は、例えば、K_{i+1}が使用され得る場所を示す情報を符号化するビットのシーケンスであり得る。K_{i+1}は、プロセスの次の反復のためにキーK_iとなる。例えば、プロセス１１００を使用して地理的制限に基づいてキーを生成した場合、生成されたキーは、日付に基づく制限を有するキーを生成するために使用され得る。そのようなプロセスは、キーを導出するために複数の制限を使用するために複数回利用されてよい。以下でさらに完全に論じられるように、キーを導出するために複数の制限を使用することによって、１つ以上の検証手段が、署名を検証する間に、ポリシーを実施することができる。簡潔な例示的実施例として、署名検証プロセスの一部として、検証手段は、現在の日付の符号化等の制限を使用して、予想される署名を決定し得る。異なる日付で生成された署名が提供された場合、一実施形態に従うと、その署名の検証は失敗する。一般に、署名の使用がキーを導出するために使用された制限に準拠しない場合、一実施形態に従って、署名の検証は失敗し得る。

【００５１】
図１２は、少なくとも一実施形態に従った、複数の制限を使用するキーの導出の例示説明となる実施例を示す図表１２００である。図１２において、キーは、複数の制限を使用して導出される。この実施例において、キーおよび日付制限を使用して、日付キー（図ではＫｄａｔｅ）を決定する。図において、日付は、２０１１年７月１５日に対応して２０１１０７１５として符号化するが、日付は異なって符号化されてもよく、一般に、情報は、図に示されるものとは異なって符号化されてもよい。日付キーは、地域制限とともに使用されて、地域キー（Ｋｒｅｇｉｏｎ）を導出する。この実施例において、地域は、米国内のいくつかの地域の１つに対応し得る、地域識別子「ＵＳＡ－ｚｏｎｅ－１」で符号化される。Ｋｒｅｇｉｏｎキーは、サービス制限とともに使用され、サービスキーＫｓｅｒｖｉｃｅを導出する。この実施例において、サービスは、その頭字語ＶＣＳによって符号化された仮想コンピュータシステムサービスである。Ｋｓｅｒｖｉｃｅキーは、要求識別子とともに使用され、署名キー、つまりサービスに対する要求に署名するために使用されるキーを導出する。この実施例において、要求識別子は「ｖｃｓ＿ｒｅｑｕｅｓｔ」であり、ＶＣＳサービスに提出され得る特定タイプの要求に対応し得る。例えば、「ｖｃｓ＿ｒｅｑｕｅｓｔ」は、仮想コンピュータシステムを提供、停止、または別の方法で修正する要求に対応し得る。署名キーは、要求とともに送信され得る署名を生成するために使用される。署名は、上記のような任意の適切な様式で生成され得る。

【００５２】
図１２に示されるように、要求は、署名を生成するためのＨＭＡＣ関数への入力として、メッセージM_cを形成するように正規化され得る。当然のことながら、正規化が必須でない場合、およびＨＭＡＣ関数以外の関数が使用される場合を含む変型が、様々な実施形態に従って利用されてもよい。さらに、図１２は、一実施形態に従って、署名の導出の特定の例を示す。しかしながら、署名を導出する際に、より多数または少数の制限が使用されてよく、制限は、例示されるものとは異なる順序で使用されてもよい。さらに、図１２は署名の導出を示すが、全てのアプリケーションにおいて署名として見なされない場合がある他のオブジェクトを導出するためにこの技術が適用されてもよい。例えば、図１２（および他の場所）で示される技術は、一般にキーを導出するために使用され得る。

【００５３】
図１３は、少なくとも一実施形態に従って、署名を導出するための関数１３００の例示説明となる実施例である。図１３に示されるように、署名は以下のように計算される。
ＨＭＡＣ（ＨＭＡＣ（ＨＭＡＣ（ＨＭＡＣ（ＨＭＡＣ（Ｋ，ｄａｔｅ），ｒｅｇｉｏｎ），ｓｅｒｖｉｃｅ），ｐｒｏｔｏｃｏｌ），Ｍｃ）
この実施例において、Ｋはキーであり、「ｄａｔｅ」は日付の符号化であり、「ｒｅｇｉ

ｏｎ」は地域の識別子の符号化であり、「ｓｅｒｖｉｃｅ」はサービスの識別子の符号化であり、「ｐｒｏｔｏｃｏｌ」は、特定のメッセージ符号化プロトコルに対応し、M_cは正規化されたメッセージである。したがって、図１３に例示されるように、署名は、同一のＨＭＡＣ関数を複数回、それぞれ異なる制限をＨＭＡＣ関数への入力として用いて計算することによって計算される。署名キーは、この実施例において、
ＨＭＡＣ（ＨＭＡＣ（ＨＭＡＣ（ＨＭＡＣ（Ｋ，ｄａｔｅ），ｒｅｇｉｏｎ），ｓｅｒｖｉｃｅ），ｐｒｏｔｏｃｏｌ）
であり、それ自体はＨＭＡＣ関数を複数回、それぞれ異なる制限を用いて使用することによって導出される。

【００５４】

図１３の実施例において、様々な制限は、それぞれドメインを定義し、定義されたドメインの交点は、署名キーを用いて生成された署名が有効となる様式を定義する。この特定の実施例において、図１３に示される署名キーを用いて生成された署名は、特定された日付で、特定された地域において、特定されたプロトコルを使用して特定されたサービスに有効となる。したがって、要求が署名キーを使用するが、署名キーへの入力によって特定されたものとは異なる日付で署名される場合、要求への署名は、要求が特定されたサービスのために特定の地域において行われた場合であっても無効であると見なされ得る。

【００５５】

本明細書に記載される他の実施形態と同様に、変型は本開示の範囲内であると見なされる。例えば、図１３は、ＨＭＡＣ関数の反復使用を示す。署名を導出するために複数の関数が使用されてよく、いくつかの実施形態において、ＨＭＡＣ関数は、導出の全ての部分で使用されるわけではない。また記載されるように、異なる制限および異なる数の制限が、様々な実施形態において使用されてもよい。

【００５６】

キー導出は、様々な実施形態に従って、多くの方法で行われ得る。例えば、単一のコンピューティングデバイスが、いくつかの実施形態に従って、署名キーを計算することができる。他の実施形態に従うと、複数のコンピューティングデバイスが、署名キーを集約的に計算し得る。特定の例示説明となる実施例として、図１３を参照すると、１つのコンピュータが、
Ｋｒｅｇｉｏｎ＝ＨＭＡＣ（ＨＭＡＣ（Ｋ，ｄａｔｅ），ｒｅｇｉｏｎ）
を計算してよく、別のコンピュータが、
署名キー＝ＨＭＡＣ（Ｋｒｅｇｉｏｎ，Ｓｅｒｖｉｃｅ）
を計算し得る。

【００５７】

別の実施例として、別個のコンピュータシステムが、署名キーの計算において異なる層を実行し得る。前節の実施例を参照すると、単一のコンピュータがＫｒｅｇｉｏｎを計算する代わりに、１つのコンピュータが、
Ｋｄａｔｅ＝ＨＭＡＣ（Ｋ，ｄａｔｅ）
を計算してよく、別のコンピュータが、
Ｋｒｅｇｉｏｎ＝ＨＭＡＣ（Ｋｄａｔｅ，ｒｅｇｉｏｎ）
を計算し得る。

図１４は、少なくとも一実施形態に従って、複数のキー導出がどのように実行および使用され得るかの例示説明となる実施例である。特に、図１４は、署名キー（または様々な他の実施形態では他のキー）を集約的に計算するコンピュータシステムの分散セットの構成部員を示す例示の図表１５００を示す。図１４に示されるように、そのセットの各構成部員は、キーを生成して、生成されたキーを別のコンピュータシステムに提供する、キープロバイダコンピュータシステム１４０２である。例えば、Ｋｅｙ　Ｐｒｏｖｉｄｅｒ$_1$と標識されるキープロバイダは、（別のソースから、またはそのキー自体を生成することによって）キーＫを得て、キーおよび制限（R_1と標識される）を使用して、キーK_1を生成する。Ｋｅｙ　Ｐｒｏｖｉｄｅｒ$_1$は、キーK_1をＫｅｙ　Ｐｒｏｖｉｄｅｒ$_2$に渡し、そ

れがK_2および別の制限R_2を使用して別のキーK_2を生成する。Ｋｅｙ　Ｐｒｏｖｉｄｅｒ$_2$は、キーK_2をＫｅｙ　Ｐｒｏｖｉｄｅｒ$_3$に渡し、それがK_3および別の制限R_3を使用して、別のキーK_3を生成する。キープロバイダが特定の実施形態においていくつ存在するかに応じて、このプロセスは、Ｋｅｙ　Ｐｒｏｖｉｄｅｒ$_{N-1}$がキーK_{N-1}をＫｅｙ　Ｐｒｏｖｉｄｅｒ$_N$に渡すまで継続してよく、それがK_{N-1}および別の制限R_Nを使用して別の署名キーK_Nを生成する。キーK_Nは、次に検証手段コンピュータシステム１４０４に渡される。キーＫまたはＫから導出された任意のキー（複数可）（一般に図面ではK_iと称される）は、例えば、セキュアキー交換アルゴリズムを通じて、署名者コンピュータシステム１４０６に渡されてもよい。

【００５８】

署名者コンピュータシステム１４０６は、また、様々な実施形態において、例えば、制限R_1～R_Nが署名者に提供され、および／または公的に提供される場合、それ自体がK_Nを生成してもよい。さらに、署名者コンピュータシステム１４０６は、様々な実施形態において、それ自体がK_Nを導出するためにプロセスの一部のみを行い得る。例えば、署名者は、（恐らく適切なキープロバイダコンピュータシステムから）K_iを得てよく、いくつかの整数ｉはＮ未満であり、制限R_{i+1}～R_Nである。署名者は、次にK_iおよび制限R_{i+1}～R_Nを使用して署名キーK_Nを生成する。他の変型も本開示の範囲内であると見なされる。

【００５９】

署名者コンピュータシステム１４０６は、キーK_Nを使用して、検証手段１４０４によって検証されるメッセージを署名し得る。例えば、例示説明されるように、署名者１４０６は、署名Ｓ＝ＨＭＡＣ（K_N，M_C）を計算し、M_Cは、メッセージＭの正規化バージョンであり、これも検証手段に送信される。検証手段はK_Nを有するため、検証手段は、独立して、メッセージＭを正規化し、ＨＭＡＣ（K_N，M_C）を計算して、計算の結果が受信された署名Ｓと一致するかどうかを決定することができる。

【００６０】

図１４に示されるプロセスの変型、および本明細書に記載される他のプロセスは、ＨＭＡＣ関数の複数使用を伴うものとして示されるが、キーを導出するために複数の異なる関数が使用されてもよいことを留意すべきである。例えば、異なるタイプのメッセージ認証符号（ＭＡＣ）関数が、キーを導出する際に異なる時点で使用され得る。例えば、あるタイプのＭＡＣ関数の出力が、別のタイプのＭＡＣ関数への入力の基礎として使用され得る。一般に、他のタイプの関数が、キー導出プロセスにおいて、ＨＭＡＣ関数の代わりに、および／またはそれに加えて使用されてよく、様々な実施形態において、キーを導出するために同一タイプの関数を複数回使用する必要はなく、関数が要求されるたびに異なる関数が使用されてもよい。

【００６１】

図１５は、少なくとも一実施形態に従って、キーが複数の制限を使用して導出され得る例示の様式を示す図表１５００である。図１５に示される実施例は、コンピューティングリソースプロバイダの顧客等の顧客に関する。しかしながら、記載されるように、図１５に関連して説明される技術を含む本明細書に記載される技術は、多くの他の文脈において使用されてもよい。

【００６２】

示されるように、顧客キーK_{cust}は、一式の顧客長期キーの一部であり、それぞれが顧客によって一定期間、例えば、顧客がキーを更新する、新しいキーが割り当てられるか、またはそうでなければキーを変更するまで使用されるキーであってよい。キーは、１人以上の顧客によって無期限に使用されてもよい。顧客キーK_{cust}は、例えば、上に例示説明される様式で１つ以上の地域キーを導出するために使用される。例えば、図１５に示されるように、２つの地域キーが、例えば、ＨＭＡＣ（K_{cust}，ＵＳＡ‐Ｅ‐１）およびＨＭＡＣ（K_{cust}，ＵＳＡ‐Ｎ‐１）を計算することによって生成されてよく、式中、ＵＳＡ‐Ｅ‐１およびＵＳＡ‐Ｎ‐１は、それぞれの地域の識別子である。同様に、地域キーは

、日付キーを符号化するために使用される日付によって有効性が制限され得る日付キーを導出するために使用されてよい。日付キーのそれぞれは、例えば、上記の様式でサービスキーを導出するために使用され得る。

【００６３】

このように、様々な実施形態において、サービスキーは、その日付で、キーを符号化するために使用される地域内のみにおいて、それぞれのサービスと併せて使用され得る。新たな日付キーは、それぞれの日に生成されてよいが、地域キーおよび顧客長期キーは、より低頻度で生成され得る。例えば、図１５において、また本開示の他の場所で示される複数の制限キー導出は、多くの利点を提供する。例えば、署名キーが破られる場合（例えば、第三者によって不正に得られる場合）、図１５に関連して記載される様式でキーを導出することによって、セキュリティ違反は特定の領域、特定の日付、および特定のサービスに関連して制限される。他のサービスは影響を受けないままである。同様の利点は、キーが導出され得る他の方法で適用可能である。

【００６４】

図１６は、例えば、少なくとも一実施形態に従って、キーが導出され得る別の例示の様式を示す図表１６００である。図１６は、図１６のものに類似する様式で概念を示す。図１６においては、しかしながら、顧客長期キーが、日付キーを導出するために使用される。日付キーは、地域キーを導出するために使用される。地域キーは、サービスキーを導出するために使用される。導出は、本明細書に記載される様々な実施形態に従って達成され得る。

【００６５】

図１７は、少なくとも一実施形態に従って、キーが導出され得るさらに別の例示の様式を示す図表１７００である。図１７において、顧客長期キーが、月キーを導出するために使用される。月キーは、地域キーを導出するために使用される。地域キーは、日付キーを導出するために使用される。日付キーは、サービスキーを定義するために使用される。様々なキーの導出は、上記説明と一致する様式で行われてよい。

【００６６】

論じられるように、本開示の様々な技術は、セッションを生成する新規の方法を可能にする。セッションは、一式の１つ以上の動作が許可される期間であってよく、セッションの満了（または他の終了）によって、その一式の１つ以上の動作が許可されなくなる。図１８は、少なくとも一実施形態に従って、セッションを開始するためのプロセス１８００の例示説明となる実施例を示すフローチャートである。プロセス１８００は、任意の適切なコンピューティングデバイスによって、またはコンピューティングデバイスの任意の適切な集合によって全体的に行われてよい。例えば、プロセス１８００は、コンピューティングリソースプロバイダの顧客のクライアントデバイスによって行われ得る。別の実施例として、別の実施形態において、図３を参照すると、フォルトゾーンのサービスのうちの１つは、セッションサービスであってよく、そのサービスを提供することに関与する１つ以上のコンピューティングデバイスが、プロセス１８００を行い得る。

【００６７】

図１８に戻ると、一実施形態において、プロセス１８００は、キーＫを得ること１８０２を含む。キーＫは、例えば、上記の様式で、他のキーを使用して導出されたキー等の任意の適切なキーであり得る。例えば、キーＫは、プロセス１８００の実行に関与するコンピューティングデバイスに伝播されていてもよい。ある時点で（例えば、図に示されるように、キーＫを得るとき）、一実施形態において、セッションを開始する要求が受信され得る１８０４。要求は、上記のような電子要求であってよい。さらに、要求は、一実施形態において、本開示の様々な技術を使用して署名および検証される。また、要求は、プロセス１８００を実現するために使用される特定の環境に応じて、異なる要求であってよい。例えば、プロセス１８００がクライアントデバイス（例えば、コンピューティングリソースプロバイダの顧客の顧客デバイス）によって行われてセッションを生成する場合、そのセッションを開始する要求は、クライアントデバイスのモジュールによって受信されて

よい。

【００６８】

一実施形態において、セッションのためのセッションパラメータが決定される１８０６。セッションパラメータは、生成されるセッションに対する１つ以上の制限を示す情報であり得る。例示のパラメータとしては、限定するものではないが、期間、生成されるセッションキーの許容されるユーザの識別子、生成されるセッションキーが使用可能である１つ以上のサービス、セッションキーを使用して行われ得る動作に対する制限、上記の制限のいずれか、およびその他が挙げられる。パラメータは、生成されるセッションキーを伴う計算が一貫していることを保証する既定のフォーマット要件に従って電子的に符号化され得る。例えば、日付は、フォーマットＹＹＹＹＭＭＤＤで符号化される必要があり得る。他のパラメータは、それら独自のフォーマット要件を有し得る。さらに、セッションパラメータを決定することは、様々な方法で行われてよい。例えば、パラメータは、セッションのデフォルトパラメータであってよく、セッションキーが、セッション開始の要求者に許可された動作範囲に対して、既定の期間（例えば、２４時間の期間）のみ使用可能であるようにする。別の実施例として、パラメータは、受信された要求の一部として、またはそうでなければそれに関連して提供されてよい。例えば、パラメータは、要求者からのユーザ入力に従って生成され得、既定のスキームに従って符号化され得る。

【００６９】

一実施形態において、パラメータが決定されると、パラメータを使用して、セッションキーK_sを計算する１８０８。セッションキーK_sを計算することは、多数の方法で行われてよい。例えば、一実施形態において、セッションキーK_Sは、以下のように（またはそうでなければ少なくとも部分的に基づいて）計算されてよく、

ＨＭＡＣ（Ｋ，Ｓｅｓｓｉｏｎ＿Ｐａｒａｍｅｔｅｒｓ）

式中、Ｓｅｓｓｉｏｎ＿Ｐａｒａｍｅｔｅｒｓは、決定された１８０６パラメータの符号化である。Ｓｅｓｓｉｏｎ＿Ｐａｒａｍｅｔｅｒｓは、計算の一貫性を保証する既定の様式で符号化されてよい。セッションキーK_Sは、図１９に関連して以下に記載される様式等の他の方法で計算されてもよい。

【００７０】

一旦セッションキーK_Sが計算されると１８０８、一実施形態において、セッションキーK_Sは使用するために提供される。セッションキーを提供することは、様々な実施形態において多くの方法で行われ得る。例えば、セッションキーは、要求者がそのセッションキーを用いてメッセージに署名することを可能にするように、要求者のモジュールに提供されてよい。セッションキーは、他のデバイスがそのセッションキーを用いてメッセージに署名することを可能にするように、ネットワークにより別のデバイスに提供されてもよい。例えば、セッションキーは、セッションが開始される受任者に提供されてもよい。例えば、要求者は、セッションを開始する要求内で、またはそれに関連して受任者を特定していてもよい。セッションキーは、電子メールまたは他の電子アドレス等の要求者（すなわち、委任者）によって提供された情報に従って、電子的に提供されてよい。

【００７１】

記載されるように、図１９は、一実施形態に従って、署名を生成するために使用され得るプロセス１９００の例示説明となる実施例を示す。プロセス１９００は、図１８に関連して上述のプロセス１８００を行う１つ以上のコンピューティングデバイス等の１つ以上のコンピューティングデバイスによって行われ得る。プロセス１９００は、図１９に示されるように、上記のようにセッションパラメータを受信することを含む。得られたセッションパラメータを用いて、一実施形態において、中間キーK_{i+1}が、以下のように計算され１９０４、

K_{i+1}＝ＨＭＡＣ（K_i，P_i）

式中、K_iは、K_{i+1}の第１の計算のための図１８の記載におけるキーＫであってよく、P_iは、セッションパラメータのｉ番目のパラメータである。セッションパラメータは、キー署名の計算の一貫性を保証するために、既定の順序に従って順序付けされてよい。

【００７２】
一実施形態において、セッションキーを生成する際に使用される追加のパラメータがあるかどうかの決定が行われる１９０６。追加のパラメータがある場合、一実施形態において、指数ｉは１つ増加し１９０８、K_{i+1}が再度計算される１９０４。しかしながら、追加のパラメータがないと決定された場合は、次にK_SがK_{i+1}の値に設定される１９１０。
【００７３】
図２０は、少なくとも一実施形態に従って、セッション中に１つ以上のコンピューティングリソースへのアクセスを得るためのプロセス２０００の例示説明となる実施例を示すフローチャートである。図２０は、１つ以上のコンピューティングリソースへのアクセスを得るためのプロセス２０００を提示するが、本明細書に記載される他のプロセスと同様に、プロセス２０００は、署名プロセスが使用される任意の状況に対して修正されてよいことを留意すべきである。プロセス２０００は、図１に示されるクライアントコンピュータシステム、および／または本明細書の他の場所に記載される顧客コンピュータシステム等の１つ以上のコンピューティングリソースへのアクセスを要求するユーザのコンピュータ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２０００は、セッションキーK_Sを得ることを含む。セッションキーは、電子メッセージ等の任意の適切な様式で得ることができる。セッションキーは、１つ以上のコンピューティングリソースへのアクセスの委任者のコンピュータシステム、またはK_Sを生成するためのプロセスを行った１つ以上のコンピュータシステムと関連して動作するコンピュータシステム等の別のコンピュータシステムから得られてもよい。
【００７４】
一実施形態において、要求Ｒが生成される２００４。要求Ｒは、上記のようにメッセージであってよい。要求Ｒは、次に正規化され２００６、一実施形態において、署名は、例えば、その署名をＨＭＡＣ（K_S，R_C）として（またはそうでなければそれに少なくとも部分的に基づいて）計算することによって正規化されたメッセージから計算される２００８。署名が生成されると、署名Ｓおよび要求Ｒが提供される２０１０。例えば、上述のように、署名Ｓおよび要求Ｒは、要求を管理し、署名を検証することに関与するコンピュータシステムのインターフェースに電子的に提供され得る。署名Ｓおよび要求Ｒは、一般的な署名およびメッセージと同様に、単一の通信、別個の通信において一緒に、または複数の通信によって集約的に提供されてよい。他の情報が、署名Ｓおよび要求Ｒに関連して提供されてもよい。例えば、識別情報が、受信された署名を検証するために用いる署名を生成するために、検証手段が適切なキーを選択することを可能にするように提供され得る。識別は、例えば、比較のために署名を生成する際に使用されるべきキーの識別子であり得る。他の情報が、様々な実施形態において適宜提供および使用されてもよい。
【００７５】
図２１は、少なくとも一実施形態に従って、１つ以上のコンピューティングリソースに対して要求されたアクセスを許可するかどうかを決定するための、プロセス２１００の例示説明となる実施例を示すフローチャートである。図１２に示されるように、プロセス２１００は、署名キーK_sを得ること２１０２を含む。署名キーを得ることに関する本明細書における他の記述と同様に、署名キーは、例えば、その署名キーを別のソースから受信する、署名キーをメモリから検索取得する、署名キーを使用可能な情報から計算する等によって、様々な方法で得ることができる。
【００７６】
一実施形態において、受信された要求Ｒは、例えば、上記の様式で正規化されて、R_Cを形成する。本明細書に記載される他のプロセスと同様に、変型が可能であることに留意すべきである。例えば、プロセス２１００（または別のプロセス）の変型を行うコンピュータシステムは、単に正規化されたメッセージを受信してよく、正規化は、別のコンピューティングデバイスによって行われてもよい。図２１の説明に戻ると、署名Ｓ′が、ＨＭＡＣ（K_S，R_C）として（またはそうでなければそれに少なくとも部分的に基づいて）計算される。計算された署名キーＳ′を受信された署名Ｓと比較して２１１０、２つの署名

が同等であるかどうかを決定する。２つの署名が同等でないと決定された場合、セッションは、無効であると決定され２１１２、要求の却下等の適切な動作が行われ得る。２つの署名が同等であると決定された場合、セッションは有効であると見なされ２１１４、１つ以上のコンピューティングリソースへのアクセスを付与する等の適切な動作が行われ得る。

【００７７】

本開示の技術は、上述のように、権限の委任を許可するために使用されてよい。図２２は、少なくとも一実施形態に従って、権限を委任するためのプロセス２２００の例示説明となる実施例を示すフローチャートである。プロセス２２００は、コンピューティングデバイス、例えば、１つ以上のコンピューティングリソースへのアクセスを委任しようとするユーザのコンピューティングデバイス、またはコンピューティングリソースプロバイダのコンピューティングデバイス、あるいは任意の適切なコンピューティングデバイスによって行われてよい。図に示されるように、プロセス２２００は、セッションキーK_{si}を得ること２２０２を含む。得られたセッションキーK_{si}は、上記のキーが得られるものとして説明される様式等の任意の適切な方法で得られてよい。さらに、セッションキーは、１つ以上のコンピューティングリソースへのアクセスを委任するプロセスの一部として生成されたキーであってもよい。例えば、セッションキーは、プロセス２２００、またはその変型を行うことによって生成されていてもよい。

【００７８】

一実施形態において、セッションパラメータが決定される２００４。セッションパラメータは、図１８に関連して上述のような任意の適切な方法で決定されてよい。決定された２００４セッションパラメータを用いて、新たなセッションキー$K_{s(i+1)}$が、上述のように生成されてよく、図１９に関連して上述のものを含む。一旦生成されると、新たなセッションキーは、受任者に提供されてよい。例えば、セッションキーは、電子メッセージで受任者に送信されてよい。セッションキーは、直接または間接的に受任者に提供されてもよい。例えば、セッションキーは、委任者に付与されてもよく、その委任者は、セッションキーを１人以上の受任者に提供する責任を有し得る。他の情報が受任者に提供されてもよい。例えば、セッションパラメータは、受任者がセッションパラメータに署名を提供することができ、それによって受信者（例えば、検証手段）が、提供された署名が有効であるかどうかを検証するために予測された署名を生成することを可能にするように受任者に提供されてもよい。例えば、受信者は、パラメータを使用して、秘密信用情報からセッションキーまたはそこから導出されたキーを生成し、そのセッションキーを使用して、対応する署名されたメッセージの正規化バージョンのための署名を生成し得る。一般的に、パラメータは、受信者がメッセージの署名を検証することを可能にするように、任意の適切な様式で署名の受信者が使用できるようにしてよく、受信者が受任者から独立してパラメータへのアクセスを有する場合、受任者は必ずしもパラメータにアクセスする必要はない。

【００７９】

図２３は、例えば、特権がどのように複数回委任され得るかを示す図表２３００を示す。委任者２３０２は、１つ以上のアクセス特権を受任者２３０４に付与しようとする場合がある。しかしながら、受任者２３０４は、この実施例では、１つ以上の特権を別の受任者２３０６に提供しようとするかもしれない。したがって、この実施例では、受任者２３０４は委任者になり得る。同様に、受任者２３０６は、別の受任者にアクセスを提供しようとする場合があり、またその受任者は別の受任者にアクセスを許可しようとする等、最終的に１つ以上の特権がさらに別の受任者２３０８に付与される。

【００８０】

したがって、この実施例では、元の委任者２３０２は、上述のように、フォルトゾーンのサービスであり得るセッションベースの認証サービス２３１０に委任要求を送信する。これに応答して、一実施形態において、セッションベースの認証サービスは、例えば、図２２に関連して上述のように、セッションキーを生成して委任者２３０２に提供する。委

任者２３０２は次に、一実施形態において、セッションベースの認証サービス２３１０から受信したセッションキーを受任者２３０４に提供する。受任者２３０４は、セッションキーを別の受任者２３０６に提供し得る。このようにして、受任者２３０６は、受任者２３０４によって受信された特権の範囲を受信し、それは受任者２３０６に提供された特権の範囲と同一である。

【００８１】

しかしながら、図２３に示されるように、受任者２３０４は、委任要求をセッションベースの認証サービス２３１０に提出し、その委任要求に応答して、セッションベースの認証サービス２３１０によって生成されていた異なるセッションキーを受信し得る。受任者２３０４は、この新たなセッションキーを次の受任者２３０６に提供してよい。次の受任者２３０６は、そのセッションキーをさらに別の受任者に提供し得るか、または上記のように、委任要求をセッションベースの認証サービス２３１０に送信してもよく、セッションベースの認証サービス２３１０は、次にセッションキーを生成して、そのセッションキーを、委任要求を送信した受任者２３０６に提供する。図２３に示されるように、これは継続し得、受任者の１人以上は、自身が受信したセッションキーを使用しようと試み得る。

【００８２】

この特定の実施例において、受任者２３０８は、要求に関連して、セッションキーをコンピューティングリソース２３１２に提供する。上記のように、要求は、セッションキーを含み得るが、そのセッションキーは、要求とは別個に提供されてもよい。コンピューティングリソース２３１２は、上記のコンピューティングリソースのいずれか、または一般にいかなるコンピューティングリソースのでもあり得る。ポリシー管理サービス２３１４は、例えば上記の検証手段を含んでよく、コンピューティングリソースの要求時に、要求を検証し得る。コンピューティングリソース２３１２およびポリシー管理サービス２３１４は、図２３では別個に示されるが、単一の構成要素であってもよい。さらに、図２３は、セッションキーを生成するために使用される単一のセッションベースの認証サービス２３１０を示すが、様々な実施形態が異なるセッションベースの認証サービスを利用し得る。

【００８３】

上記のように、本明細書に提供される例示の実施例に加えて、多数の変型が本開示の範囲内であると見なされる。図２４は、一実施形態に従って、キーが複数の権限者からのキーを使用して導出され得る様式の例示説明となる実施例を表す図表２４００を示す。図２３において、顧客キーK_{cust}は、コンピューティングリソースプロバイダによって維持される一式の顧客キーから生じる。上記の実施形態と同様に、図２３は、コンピューティングリソースプロバイダに関連して例示説明となる実施例を論じたが、他の変型も本開示の範囲内であると見なされる。

【００８４】

図２４において、一式の権限キーが維持され、各権限キーは異なる権限ドメインに対応する。顧客キーK_{cust}から導出された各権限キーは、例えば、上記のように、異なるフォルトゾーンに伝播されてもよい。フォルトゾーンは、例えば、異なる行政区内のデータセンターであり得る。しかしながら、図２４は、単一の顧客キーK_{cust}から導出されたそれぞれの分割された権限キーを示すが、変型も可能であることに留意すべきである。例えば、分割された権限キーは、独立して導出されてもよい。別の実施例として、１つ以上の分割された権限キーは、共通キーから導出されてよく、１つ以上の他のキーは、別の共通キーから導出され得る等である。

【００８５】

一実施形態において、複数の権限者が、権限を組み合わせて、１つ以上のコンピューティングリソースへのアクセスを可能にすることができる。例えば、図２４に示されるように、分割された権限キーのサブセットを使用して、他のキーを導出してもよい。例えば、図２３に示されるように、Ａｕｔｈ１およびＡｕｔｈ２と標識される２つの権限キーを使

用して、統合された権限キーを導出する。統合された権限キーを導出するために、一実施形態において、例えば上記のように、ＨＭＡＣ（ｆ（Ａｕｔｈ１，Ａｕｔｈ２），Ｒ）の値が計算され、式中、Ｒはある種の制限である。この実施例において、ｆは分割された権限キーの関数であり、二次元を越え得る。例えば、３つの分割された権限キーＡｕｔｈ１、Ａｕｔｈ２、およびＡｕｔｈ３が、図２３に示されるように、関数ｆ（Ａｕｔｈ１，Ａｕｔｈ２，Ａｕｔｈ３）において使用され、統合された権限キーを、ＨＭＡＣ（ｆ（Ａｕｔｈ１，Ａｕｔｈ２，Ａｕｔｈ３），Ｒ）として（またはそうでなければそれに少なくとも部分的に基づいて）計算する。

【００８６】

異なる権限からのキーを構成する多くの変型も本開示の範囲内であると見なされる。例えば、一つの権限者が、本開示の様々な実施形態を使用して、キー（K_{spec}）を生成し得る（または生成している）。各権限K_{spec}は、部分的キーシードに対応してよく、そのK_{spec}を生成するために使用される制限の公的に使用可能な符号化（または他の方法でメッセージ署名者および署名検証手段が使用可能な符号化）であり得る。例えば、部分的キーシードは、（Ｋ１／２０１１０８ｉｏ／ｕｓａ‐ｅａｓｔ‐１／ＤＤＳ，Ｋ２／２０１１０８ｉｏ／ｏｒｇ＿ｎａｍｅ／ｊｐｌ／ＤＤＳ）であってよく、スラッシュ間の各文字列は制限である。そのような情報の符号化は、キーパスと称され得る。より一般的な実施例として、部分的キーシードは、X_1／…／X_nであってよく、各X_i（は１～ｎのｉ間）は、上記のパラメータ等のパラメータに対応する。適用可能な権限者からの部分的キーシードは、ｎ－タプルとして符号化されてよく、キーシードと称される。直上の実施例のｎ－タプルは、（$spec_1$，$spec_2$，…，$spec_n$）であってよく、各エントリは、対応するK_{spec}に対するキーパスである。キーシード（および／またはキーパス）は、キー保持者が署名／キーを生成することによって権限を与える精密なキー使用（全ての権限を与えられたキー間の完全な制限）を符号化することに留意すべきである。さらに、メッセージ署名者および署名検証手段の両方が使用可能な部分的キーシードを用いる場合、例えば、メッセージ署名者が、署名キーを生成するためにパラメータが使用された順序を特定する情報を有するため、したがって署名キーおよびメッセージを生成することができるため、キーおよび署名を生成するために使用されるパラメータの任意の順序が可能である。

【００８７】

次に適用可能な権限者、つまり、キーが生成される権限者のそれぞれに対するＨＭＡＣ（K_{spec}，ｋｅｙ‐ｓｅｅｄ）の値が得られ得るか、または計算され得る。この値は、様々な実施形態において、メッセージに署名するために署名キーを得るクライアントによって計算され得るか、または別のデバイスによって計算され、後次にそのクライアントに提供され得る。これらの値のそれぞれは、以下の考察の目的で、部分的キーと称され得る。これらの部分的キーのそれぞれの意味は、一実施形態において、以下の構成（および以下の構成の所与の変型）と組み合わされたときのみ、それらが有効であるということであり、組み合わされると、キーシード内で符号化された特化の交点を形成する。

【００８８】

署名キーを生成してメッセージに署名するために、以下の値を求め、

K_S＝ＨＭＡＣ（$partial\_key_1$＋…＋$partial\_key_n$，ｋｅｙ‐ｓｅｅｄ）

式中、「＋」は、式中記号で囲まれた部分的キーに対するいくつかの連想演算を意味し得る。「＋」記号は、例えば、部分的キーを含むビットに対する排他的ＯＲ（ＸＯＲ）操作であり得る。「＋」記号は、いくつかの他の適切な操作または関数を意味してもよい。

【００８９】

メッセージに署名するために使用される署名を検証するために、検証手段は、上述のように、各部分的キーを得て、上記のように部分的キーを組み合わせて署名キーを形成し、受信したメッセージに署名して、その結果を予想された結果と比較して署名を検証する。

【００９０】

本開示の例示の実施形態は、以下の付記を考慮して説明され得る。

付記１．　サービスを提供するためのコンピュータで実装される方法であって、
　実行可能な命令を備えて構成された１つ以上のコンピュータシステムの制御下で、
　認証当事者から、メッセージと、前記メッセージの署名と、前記認証当事者と共有される秘密信用情報から導出されたキーに関する一式の１つ以上の制限とを符号化している電子情報を受信することであって、前記署名は、ハッシュベースのメッセージ認証符号関数を前記メッセージ、前記秘密信用情報、および前記一式の１つ以上の制限に適用することによって決定可能であるが、前記ハッシュベースのメッセージ認証符号関数のみを有するが、前記一式の１つ以上の制限を有しない場合は決定できない、受信することと、
　前記一式の１つ以上の制限の少なくともサブセットを少なくとも部分的に使用して生成されたキーを得ることと、
　前記１つ以上のコンピュータシステムによって、
　　前記得られたキーに少なくとも部分的に基づく第１の入力と、
　　前記一式の１つ以上の制限に少なくとも部分的に基づく第２の入力と、
　を前記ハッシュベースのメッセージ認証符号関数に少なくとも入力することによって、ハッシュベースのメッセージ認証符号関数の値を計算することと、
　前記１つ以上のコンピュータシステムによって、かつ前記計算された値に少なくとも部分的に基づいて、前記署名が有効であるかどうかを決定することと、
　前記署名が有効であることが決定されたとき、１つ以上のコンピューティングリソースへのアクセスを提供することと、
　を含む、コンピュータで実装される方法。
付記２．　前記メッセージが、前記１つ以上のコンピューティングリソースへのアクセスの要求を含み、
　前記方法が、前記一式の１つ以上の制限が、前記要求が満たされるべきであることを示すかどうかを決定することを含み、
　前記１つ以上のコンピューティングリソースへのアクセスを提供することが、制限が、前記要求が満たされるべきであることを示すことを決定することを条件とする、付記１に記載のコンピュータで実装される方法。
付記３．　前記一式の１つ以上の制限を符号化する前記情報が、文書によって符号化され、前記一式の制限が、前記要求が満たされるべきであることを示すかどうかを決定することが、前記要求が受信される文脈に対して前記文書を評価することを含む、請求項２に記載のコンピュータで実装される方法。
付記４．　前記メッセージが、前記１つ以上のコンピューティングリソースのうちのコンピューティングリソースにアクセスする要求を含み、
　前記一式の１つ以上の制限を符号化する前記情報が、前記コンピューティングリソースを特定する情報を含み、
　前記１つ以上のコンピューティングリソースへのアクセスを提供することが、前記コンピューティングリソースが前記特定されたコンピューティングリソースと一致するとき、前記コンピューティングリソースへのアクセスを提供することを含む、付記１に記載のコンピュータで実装される方法。
付記５．　前記一式の１つ以上の制限を符号化する前記情報が、前記メッセージが有効である期間に対応し、
　前記署名が有効であるかどうかを決定することが、前記メッセージが前記対応する期間の間に送信されたかどうかに少なくとも部分的に基づく、付記１に記載のコンピュータで実装される方法。
付記６．　前記一式の１つ以上の制限を符号化する前記情報が、場所に少なくとも部分的に基づく制限に対応し、
　前記署名が有効であるかどうかを決定することが、前記１つ以上のコンピュータシステムのうちの少なくとも１つの場所が、前記対応する場所と一致するかどうかに少なくとも部分的に基づく、付記１に記載のコンピュータで実装される方法。
付記７．　サービスを提供するためのコンピュータで実装される方法であって、

実行可能な命令を備えて構成された１つ以上のコンピュータシステムの制御下で、
（ｉ）メッセージ、（ｉｉ）前記メッセージの第１の署名、および（ｉｉｉ）一式の１つ以上のパラメータを符号化している電子情報を得ることであって、前記第１の署名が、（ｉ）前記メッセージ、（ｉｉ）秘密信用情報、および（ｉｉｉ）前記一式の１つ以上のパラメータに少なくとも部分的に基づいて生成され、前記第１の署名がさらに、前記メッセージおよび前記秘密信用情報のみを有するが、前記一式の１つ以上のパラメータを有しない場合は決定できない、得ることと、
前記秘密信用情報および前記一式の１つ以上のパラメータのうちの少なくともサブセットに少なくとも部分的に基づいて、第２の信用情報を導出することと、
前記導出された第２の信用情報に少なくとも部分的に基づいて、第２の署名を生成することと、
前記第１の署名が、前記第２の署名と一致するかどうかを決定することと、
前記生成された第２の署名が、前記第１の署名と一致するとき、１つ以上のコンピューティングリソースへのアクセスを提供することと、
を含む、コンピュータで実装される方法。
付記８．　前記第２の信用情報を得ることが、前記秘密信用情報および前記一式の１つ以上のパラメータの前記少なくともサブセットを関数に入力することを含む、付記７に記載のコンピュータで実装される方法。
付記９．　前記関数が、対称メッセージ認証関数である、付記８に記載のコンピュータで実装される方法。
付記１０．　前記対称メッセージ認証関数が、ハッシュ関数である、付記９に記載のコンピュータで実装される方法。
付記１１．　前記秘密信用情報および前記１つ以上のパラメータの前記少なくともサブセットを前記関数に入力することが、ハッシュベースのメッセージ認証符号（ＨＭＡＣ）の一部として行われる、付記９に記載のコンピュータで実装される方法。
付記１２．　前記第２の署名を生成することが、前記関数の出力および前記一式の１つ以上のパラメータからのパラメータの両方を前記関数に入力することを含む、付記８に記載のコンピュータで実装される方法。
付記１３．　前記１つ以上のパラメータを符号化する前記情報が、前記一式の１つ以上のパラメータを符号化する電子文書を含む、付記７に記載のコンピュータで実装される方法。
付記１４．　前記第２の署名を生成することが、キーに少なくとも部分的に基づき、
前記一式の１つ以上のパラメータが、前記キーの使用に対する１つ以上の制限を含み、
前記１つ以上のコンピューティングリソースへのアクセスを提供することが、前記１つ以上の制限に従って行われる、付記８に記載のコンピュータで実装される方法。
付記１５．　前記キーが、前記秘密信用情報の関数への入力の結果に少なくとも部分的に基づく、付記１４に記載のコンピュータで実装される方法。
付記１６．　命令が記憶された非一時的コンピュータ可読ストレージ媒体であって、コンピュータシステムによって実行されるとき、少なくとも、
中間キーであって、少なくとも秘密信用情報および前記中間キーの使用のための１つ以上のパラメータから導出された中間キーを取得することと、
前記取得された中間キーに少なくとも部分的に基づいて、メッセージの署名をもたらす署名生成プロセスの少なくとも一部を適用することであって、前記署名生成プロセスが、前記署名生成プロセスによって、前記メッセージ、前記秘密信用情報、および前記署名を有するが、前記１つ以上の制限を欠くコンピューティングデバイスに対して前記署名が決定できないように構成される、適用することと、
前記メッセージ、前記署名、および前記１つ以上のパラメータを、前記１つ以上のパラメータおよび前記メッセージ、前記署名に少なくとも部分的に基づいて分析して、前記署名が有効であるかどうかを決定するように構成された別のコンピュータシステムに提供することと、

を前記コンピュータシステムに行わせる命令を記憶する、非一時的コンピュータ可読ストレージ媒体。
付記１７．　前記１つ以上のパラメータが、前記別のコンピュータシステムによって、少なくとも部分的に実施される、前記中間キーの使用に対する１つ以上の制限を符号化する、付記１６に記載の非一時的コンピュータ可読ストレージ媒体。
付記１８．　前記１つ以上の制限が、前記中間キーが使用可能である期間、前記中間キーが使用可能である場所、および前記中間キーがアクセスを得るために使用可能である１つ以上のサービスのうちの少なくとも１つに対応する、付記１６に記載の非一時的コンピュータ可読ストレージ媒体。
付記１９．　前記命令が、前記コンピュータシステムによって実行されるとき、前記コンピュータシステムが、前記秘密信用情報へアクセスをする必要なしに、前記署名を生成することを可能にする、付記１６に記載の非一時的コンピュータ可読ストレージ媒体。
付記２０．　前記一式の１つ以上のパラメータを有するとき、前記署名が、前記共有された秘密信用情報または前記中間キーのいずれかを使用して、前記署名生成プロセスによって決定可能である、付記１９に記載の非一時的コンピュータ可読ストレージ媒体。
付記２１．　前記中間キーを取得することが、ハッシュ関数のうちの少なくとも１つの出力が、前記パラメータのうちの少なくとも１つとともに、前記ハッシュ関数に入力されるアルゴリズムを行うことを含む、付記１９に記載の非一時的コンピュータ可読ストレージ媒体。
付記２２．　コンピュータシステムであって、
　１つ以上のプロセッサと、
　コンピュータシステムの１つ以上のプロセッサによって実行されるとき、前記コンピュータシステムに少なくとも、
　メッセージ、前記メッセージの署名、および１つ以上のパラメータを集約的に符号化している１つ以上の電子通信を受信することであって、前記署名が、前記秘密信用情報および前記１つ以上のパラメータに少なくとも部分的に基づいて生成される、符号化することと、
　前記１つ以上のパラメータに少なくとも部分的に基づいて、前記１つ以上のパラメータおよび前記秘密信用情報の少なくとも一部から導出されたが前記秘密信用情報を有しない、前記中間信用情報、前記メッセージおよび署名を分析して、前記署名が有効であるかどうかを決定することと、
　前記署名が有効であることを決定することを条件として１つ以上のアクションを行うことと、
　を行わせる命令を含む、メモリと、
を備える、コンピュータシステム。
付記２３．　前記メモリおよび１つ以上のプロセッサが、第１の地理的場所にある第１のサーバシステムの一部であり、
　前記コンピュータシステムが、第２の地理的場所にある第２のサーバシステムを備え、前記第２のサーバシステムが、前記秘密信用情報に少なくとも部分的に基づいて、異なる署名を生成するように構成され、
　前記第１のサーバシステムおよび第２のサーバシステムが、いずれも前記秘密信用情報を欠失し、
　前記メッセージおよび署名を分析することが、前記１つ以上のパラメータおよび前記中間信用情報の前記少なくとも一部を関数に入力することを含み、
　前記第１のサーバシステムおよび第２のサーバシステムがそれぞれ、前記関数を使用して前記メッセージから同じ署名が生成され得る情報を欠失する、付記２２に記載のコンピュータシステム。
付記２４．　前記コンピュータシステムが、サービスに対応し、
　前記１つ以上のアクションが、前記サービスへのアクセスを提供することを含む、付記２２に記載のコンピュータシステム。

付記２５．　前記１つ以上のパラメータが、前記サービスにアクセスする際に使用するための前記中間信用情報の使用を制限する、付記２４に記載のコンピュータシステム。
付記２６．　前記メッセージおよび署名を分析することが、ハッシュ関数を前記中間信用情報に適用することを含み、
　前記１つ以上のパラメータが、前記中間信用情報の使用に対する複数の制限を含み、
　前記コンピュータシステムが、前記制限を実施するように構成される、付記２２に記載のコンピュータシステム。
付記２７．　前記メッセージおよび署名を分析することが、ハッシュ関数を前記秘密信用情報から導出されたキーに適用することを含み、
　前記命令が、前記コンピュータシステムの前記１つ以上のプロセッサによって実行されるとき、前記コンピュータシステムに前記導出されたキーをキー権限者コンピュータシステムからさらに受信させる、付記２２に記載のコンピュータシステム。
付記２８．　前記コンピュータシステムに、前記キー権限者コンピュータシステムから前記導出されたキーをさらに受信させる前記命令が、前記コンピュータシステムに、前記メッセージの受信前に、前記キー権限者コンピュータシステムから前記導出されたキーを受信させる、付記２７に記載のコンピュータシステム。
付記２９．　前記中間信用情報が、前記コンピュータシステムとは異なる別のコンピュータシステムによって決定される、付記２２に記載のコンピュータシステム。
【００９１】
　様々な実施形態はさらに、多種多様な動作環境内で実装することができ、場合によっては、１つ以上のユーザコンピュータ、コンピューティングデバイス、または多数のアプリケーションのいずれかを操作するために使用することができる処理デバイスを含み得る。ユーザまたはクライアントデバイスは、標準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またはラップトップコンピュータ、ならびにモバイルソフトウェアを実行し、多数のネットワーキングおよびメッセージングプロトコルを支援することができるセルラー、ワイヤレス、および携帯型デバイス等の多数の汎用パーソナルコンピュータのいずれかを含むことができる。そのようなシステムは、開発およびデータベース管理等の目的で、多様な市販のオペレーティングシステムおよび他の既知のアプリケーションのうちのいずれかを実行する多数のワークステーションを含むこともできる。これらのデバイスは、ダミー端末、シンクライアント、ゲーミングシステム等の他の電子デバイス、およびネットワークを介して通信することができる他のデバイスを含むこともできる。
【００９２】
　大半の実施形態は、ＴＣＰ／ＩＰ、ＯＳＩ、ＦＴＰ、ＵＰｎＰ、ＮＦＳ、ＣＩＦＳ、およびＡｐｐｌｅＴａｌｋ等の多様な市販のプロトコルを使用する通信を支援するために、当業者によく知られている少なくとも１つのネットワークを利用する。ネットワークは、例えば、ローカルエリアネットワーク、広域ネットワーク、仮想プライベートネットワーク、インターネット、イントラネット、エクストラネット、公衆交換電話網、赤外線ネットワーク、ワイヤレスネットワーク、およびそれらの任意の組み合わせであり得る。
【００９３】
　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、ＨＴＴＰサーバ、ＦＴＰサーバ、ＣＧＩサーバ、データサーバ、Ｊａｖａサーバ、およびビジネスアプリケーションサーバを含む多様なサーバまたは中間階層アプリケーションのいずれかを実行することができる。サーバ（複数可）は、例えば、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つ以上のスクリプトまたはプログラムとして実装され得る１つ以上のウェブアプリケーションを実行することによって、ユーザデバイスからの要求に応答してプログラムまたはスクリプトを実行することも可能であり得る。サーバ（複数可）は、Ｏｒａｃｌｅ（登録商標）、Ｍｉｃｒｏｓｏｆｔ（登録商標）、Ｓｙｂａｓｅ（登録商標）、およびＩＢＭ（登録商標）から市販されているものを含むが、これらに限定されないデータベースサーバを含んでもよい。

【００９４】
環境は、上述のように、多様なデータストア、ならびに他のメモリおよびストレージ媒体を含み得る。これらは、例えば、コンピュータの１つ以上対してローカルである（および／またはその中に存在する）か、またはネットワーク全体のコンピュータのいずれかもしくは全てから遠隔にあるストレージ媒体上等の様々な場所に存在し得る。特定の一式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（「ＳＮＡ」）内に存在し得る。同様に、コンピュータ、サーバ、または他のネットワークデバイスに属した関数を行うための任意の必須ファイルは、必要に応じてローカルに、および／または遠隔的に記憶され得る。システムがコンピュータ化デバイスを含む場合、そのようなデバイスはそれぞれ、バスを介して電子的に連結され得るハードウェア要素を含むことができ、それらの要素は、例えば、少なくとも１つの中央演算装置（ＣＰＵ）、少なくとも１つの入力デバイス（例えば、マウス、キーボード、コントローラ、タッチスクリーン、またはキーパッド）、および少なくとも１つの出力デバイス（例えば、ディスプレイデバイス、プリンタ、またはスピーカ）を含む。そのようなシステムは、ディスクドライブ、光学ストレージデバイス、および固体ストレージデバイス（例えば、ランダムアクセスメモリ（「ＲＡＭ」）または読み取り専用メモリ（「ＲＯＭ」））、ならびにリムーバブルメディアデバイス、メモリカード、フラッシュカード等の１つ以上のストレージデバイスを含んでもよい。

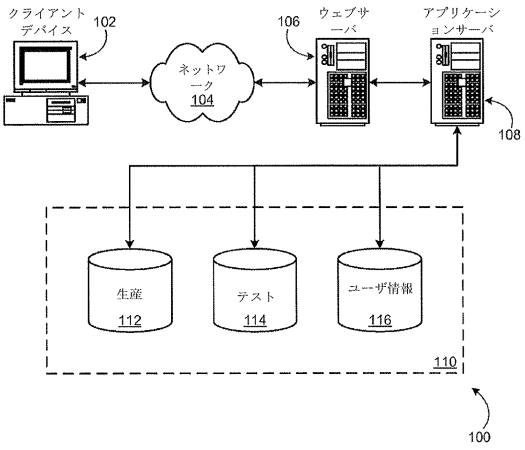
【００９５】
そのようなデバイスは、コンピュータ可読ストレージ媒体リーダ、通信デバイス（例えば、モデム、ネットワークカード（無線または有線）、赤外線通信デバイス等）、および上記のようなワーキングメモリを含むこともできる。コンピュータ可読ストレージ媒体リーダは、遠隔、ローカル、固定、および／またはリムーバブルストレージデバイスを表すコンピュータ可読ストレージ媒体、ならびにコンピュータ可読情報を一時的および／またはより永久的に含有、記憶、伝送、および検索取得するためのストレージ媒体と接続され得るか、またはそれらを受信するように構成され得る。システムおよび様々なデバイスは、通常、多数のソフトウェアアプリケーション、モジュール、サービス、または少なくとも１つのワーキングメモリデバイス内に位置する他の要素（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オペレーティングシステムおよびアプリケーションプログラムを含む）も含む。当然のことながら、代替実施形態は、上記のものからの多数の変型を有してもよい。例えば、カスタマイズされたハードウェアが使用されてもよく、および／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）、またはそれら両方において実現されてもよい。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てもよい。

【００９６】
符号または符号の一部を含むためのストレージ媒体およびコンピュータ可読媒体は、当該技術分野において既知であるか、または使用される任意の適切な媒体を含むことができ、例えば、限定するものではないが、コンピュータ可読命令、データ構造、プログラムモジュール、もしくは他のデータ等の情報の記憶および／または伝送のための任意の方法または技術において実装される揮発性および不揮発性、リムーバブルおよび非リムーバブル媒体が挙げられ、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリもしくは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）、または他の光学ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、または所望の情報を記憶するために使用することができ、かつシステムデバイスによってアクセスされ得る任意の他の媒体を含む。本明細書で提供される開示および教示に基づいて、当業者であれば、様々な実施形態を実現するための他の手段および／または方法を理解するであろう。

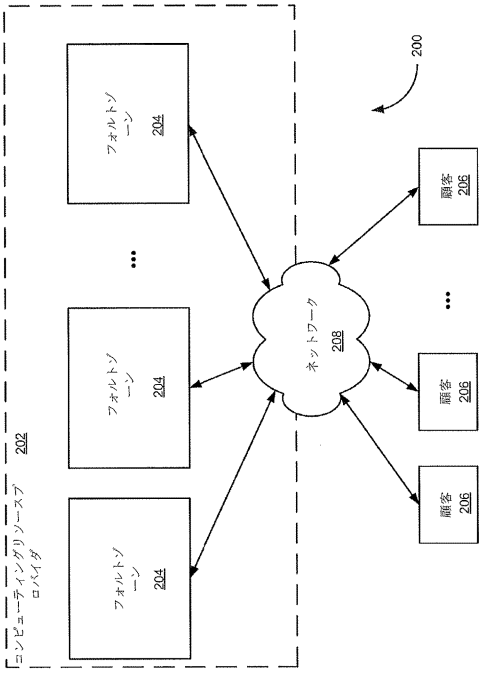
【００９７】
本明細書および図面は、したがって、制限的な意味ではなく例示説明として見なされるものである。しかしながら、請求項に記載される本発明の広義の趣旨および範囲から逸脱

することなく、様々な修正および変更がそこに行われ得ることは明らかとなるであろう。
【００９８】
他の変型も本開示の趣旨に含まれる。したがって、開示される技術は、様々な修正および代替構成を許すが、それらのある例示の実施形態が図面に示され、上で詳細に説明された。しかしながら、本発明を開示される特定の形態（複数可）に限定する意図はなく、反対に、添付の請求項において定義される、本発明の趣旨および範囲内に含まれる全ての修正、代替構成、および相当物を網羅することを意図することを理解すべきである。
【００９９】
開示される実施形態を説明する文脈における（特に以下の請求項の文脈における）用語「ａ」、「ａｎ」、および「ｔｈｅ」ならびに同様の指示語の使用は、本明細書において別段の指示がない限り、または文脈に明らかに矛盾するものでない限り、単数および複数の両方を網羅すると解釈される。用語「備える（ｃｏｍｐｒｉｓｉｎｇ）」、「有する（ｈａｖｉｎｇ）」、「含む（ｉｎｃｌｕｄｅｉｎｇ）」、および「含有する（ｃｏｎｔａｉｎｉｎｇ）」は、別段の記載がない限り、制限のない用語（すなわち、「含むが、それに限定されない」を意味するもの）として解釈される。用語「接続される（ｃｏｎｎｅｃｔｅｄ）」は、介在するもの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有される、そこに取り付けられる、または一緒に接合されるものと解釈される。本明細書における値の範囲の列挙は、本明細書において別段の指示がない限り、単にその範囲内に含まれるそれぞれ別個の値を個別に参照する簡略的な方法として機能することが意図され、各別個の値が、本明細書において個別に列挙されるかのように、本明細書に組み込まれる。本明細書に記載される全ての方法は、本明細書において別段の指示がない限り、または文脈と明らかに矛盾しない限り、任意の適切な順序で行われ得る。本明細書に提供される任意および全ての実施例、または例示的言語（例えば、「等」）の使用は、単に本発明の実施形態をさらに明らかにすることが意図され、別段の請求がない限り、本発明の範囲に対して制限を課すものではない。明細書におけるどの表現も、任意の請求されていない要素を本発明の実施に必須であると示すものと解釈されるべきではない。
【０１００】
本開示の好適な実施形態が、本明細書において、本発明を実行するために発明者らに既知の最良の形態を含んで説明される。それらの好適な実施形態の変型は、前記の説明を読むことで、当業者に明らかとなり得る。発明者らは、熟練者がそのような変型を必要に応じて用いることを予期し、また発明者らは、本発明が本明細書において特定的に説明されるものとは別の方法で実施されることを意図する。したがって、本発明は、適用可能な法律によって許可されるように、本明細書に添付される請求項に列挙される主題の全ての改変および相当物を含む。さらに、その全ての考えられる変型における上述の要素の任意の組み合わせが、本明細書において別段の指示がない限り、または文脈と明らかに矛盾しない限り、本発明によって包含される。
【０１０１】
本明細書において引用される出版物、特許出願、および特許を含む全ての参照文献は、各参照文献が参照により個別かつ特定的に組み込まれ、その全体が本明細書において記載されるのと同じ程度に、参照により本明細書に組み込まれる。

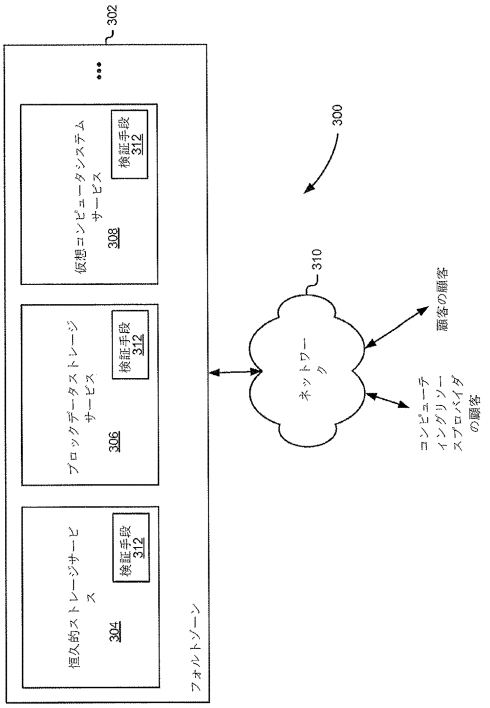
【図１】


クライアントデバイス
102
ネットワーク
104
106
ウェブサーバ
アプリケーションサーバ
108
生産
112
テスト
114
ユーザ情報
116
110
100

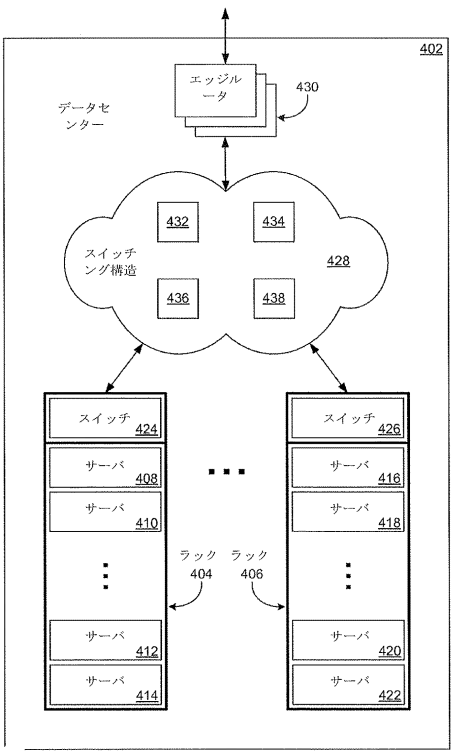
【図２】


200
フォルトゾーン
204
顧客
206
ネットワーク
208
202
コンピューティングリソースプロバイダ

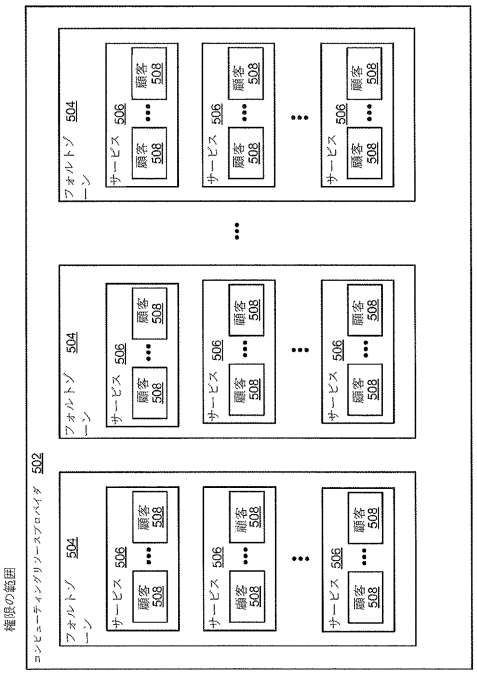
【図３】


302
仮想コンピュータシステムサービス
308
検証手段
312
ブロックデータストレージサービス
306
検証手段
312
恒久的ストレージサービス
304
検証手段
312
フォルトゾーン
300
310
ネットワーク
顧客の顧客
コンピューティングリソースプロバイダの顧客

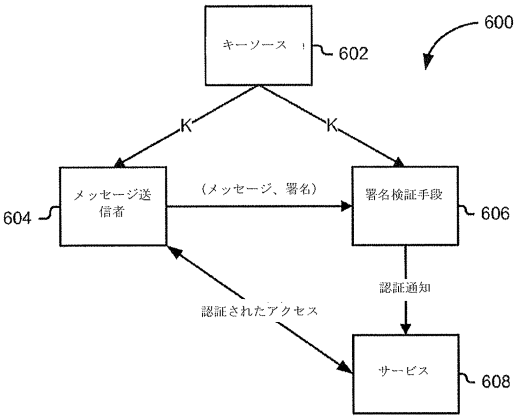
【図４】


402
データセンター
エッジルータ
430
432
434
428
スイッチング構造
436
438
スイッチ
424
サーバ
408
サーバ
410
サーバ
412
サーバ
414
ラック
404
ラック
406
スイッチ
426
サーバ
416
サーバ
418
サーバ
420
サーバ
422

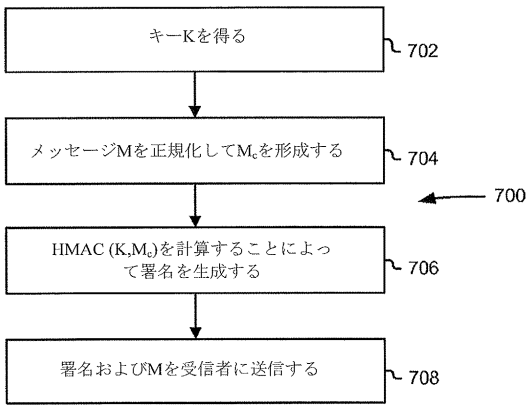
【図５】


権限の範囲
コンピューティングリソースプロバイダ
502
フォルトゾーン
504
サービス
506
顧客
508

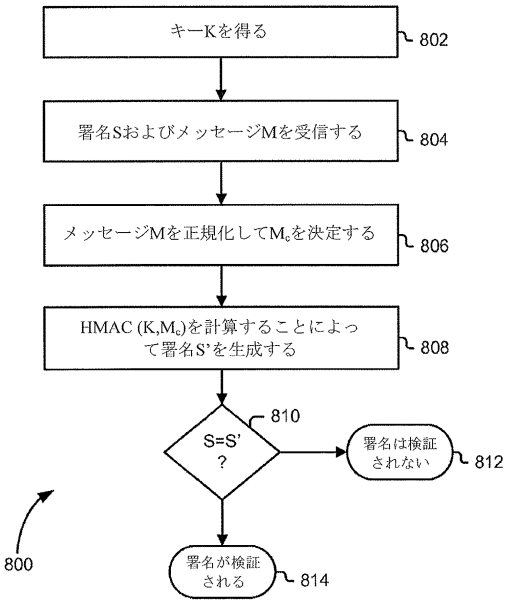
【図６】


600
キーソース
602
K
K
メッセージ送信者
604
(メッセージ、署名)
署名検証手段
606
認証通知
認証されたアクセス
サービス
608

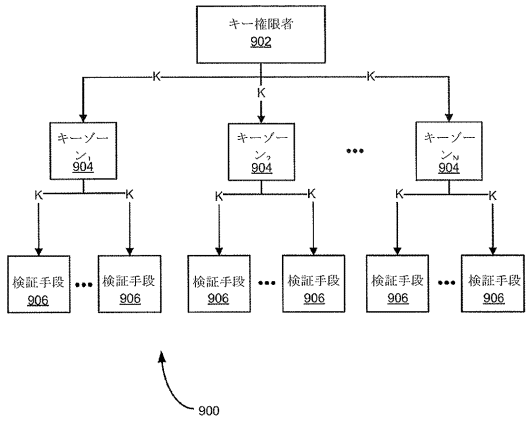
【図７】


キーKを得る
702
メッセージMを正規化してMcを形成する
704
700
HMAC (K,Mc)を計算することによって署名を生成する
706
署名およびMを受信者に送信する
708

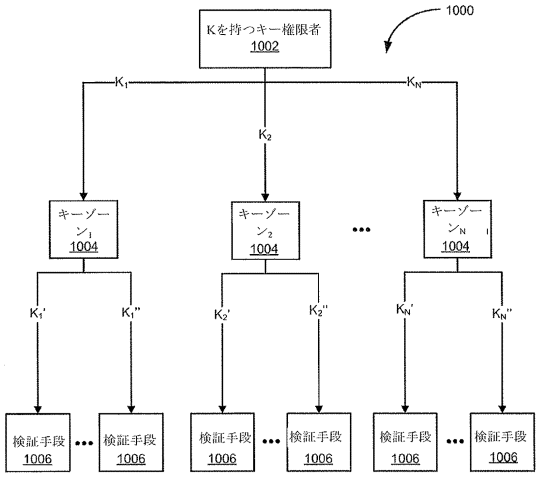
【図８】


キーKを得る
802
署名SおよびメッセージMを受信する
804
メッセージMを正規化してMcを決定する
806
HMAC (K,Mc)を計算することによって署名S'を生成する
808
S=S'
?
810
署名は検証されない
812
署名が検証される
814
800

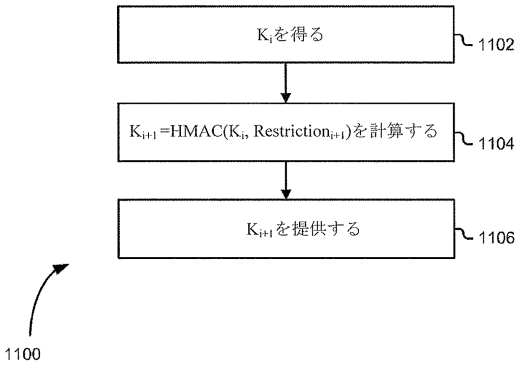
【図９】



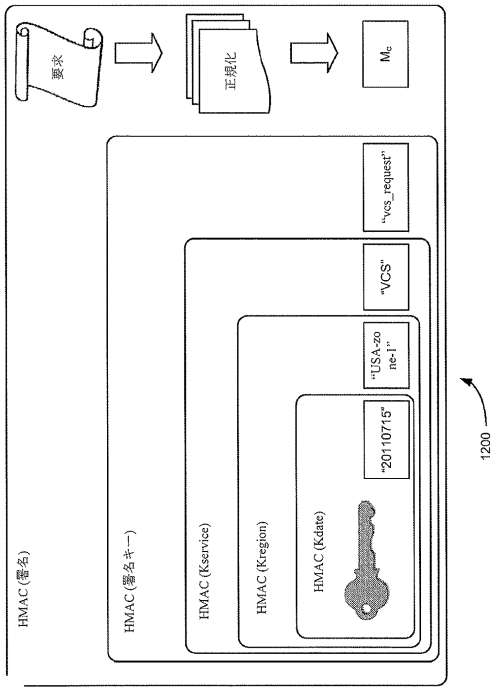
【図１０】



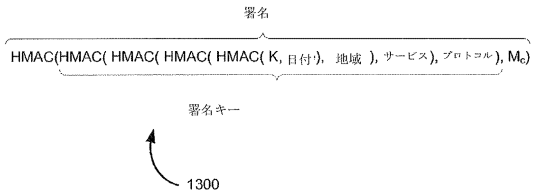
【図１１】



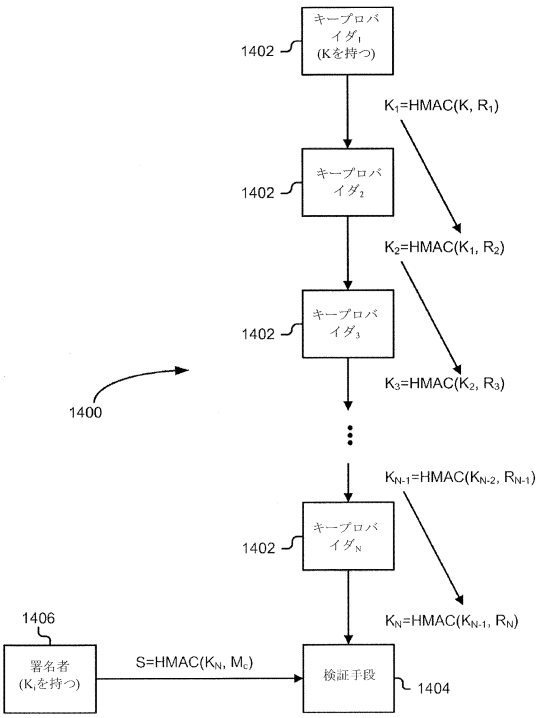
【図１２】



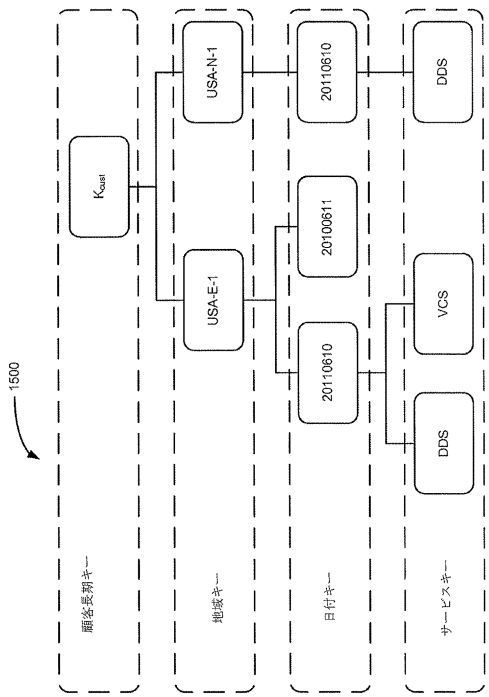
【図１３】



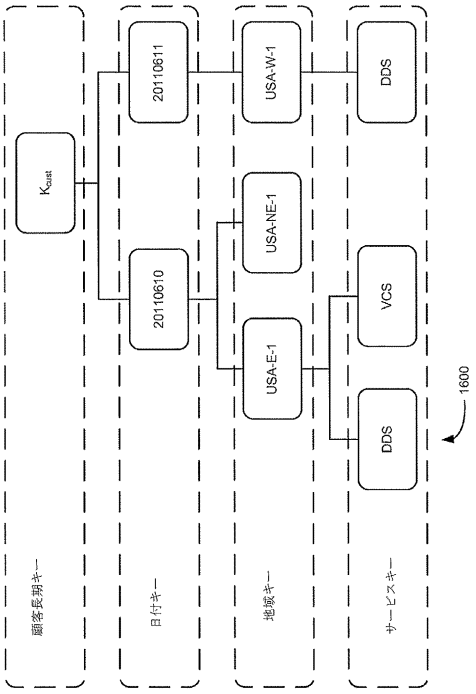
【図１４】



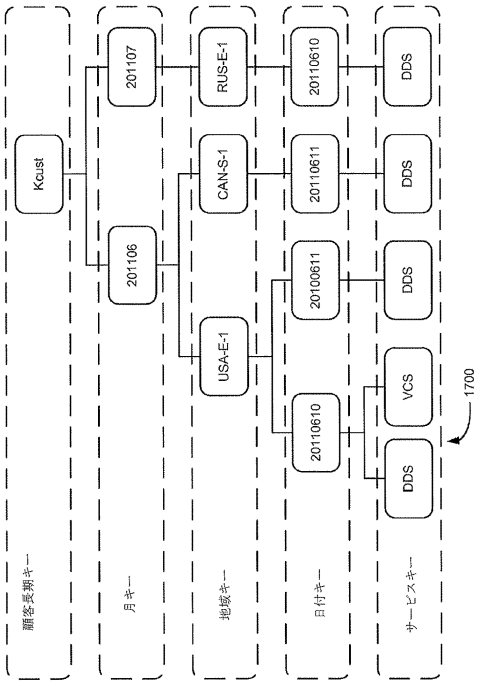
【図１５】



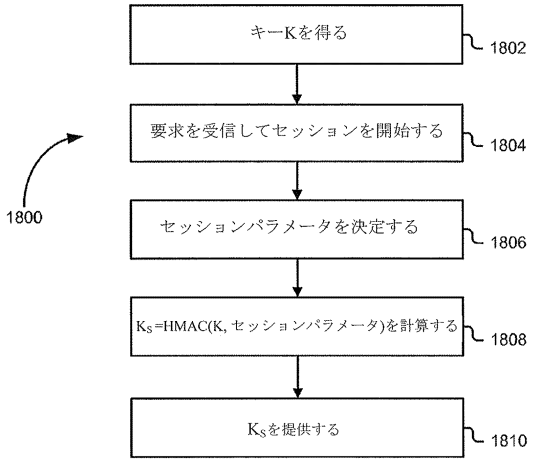
【図１６】



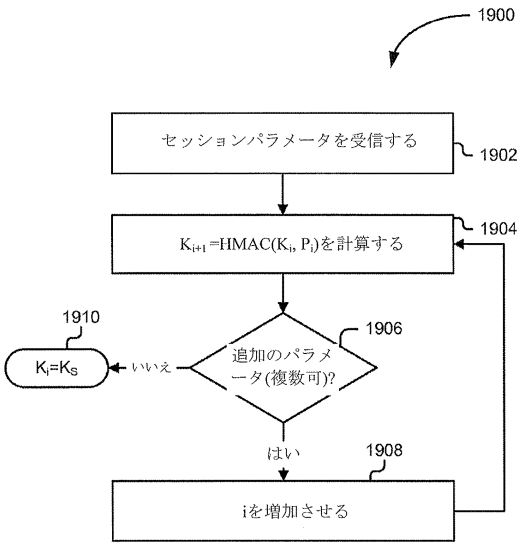
【図１７】



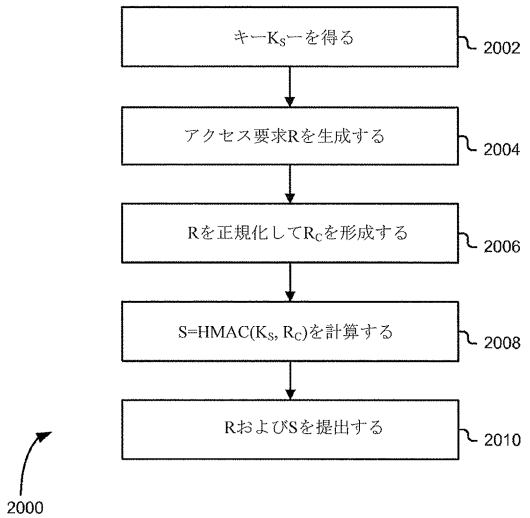
【図１８】



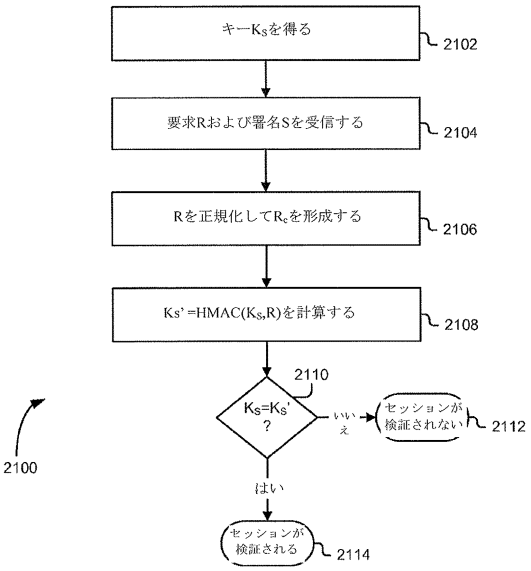
【図１９】



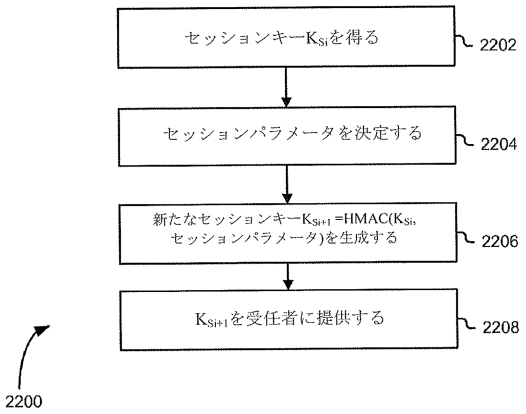
【図２０】



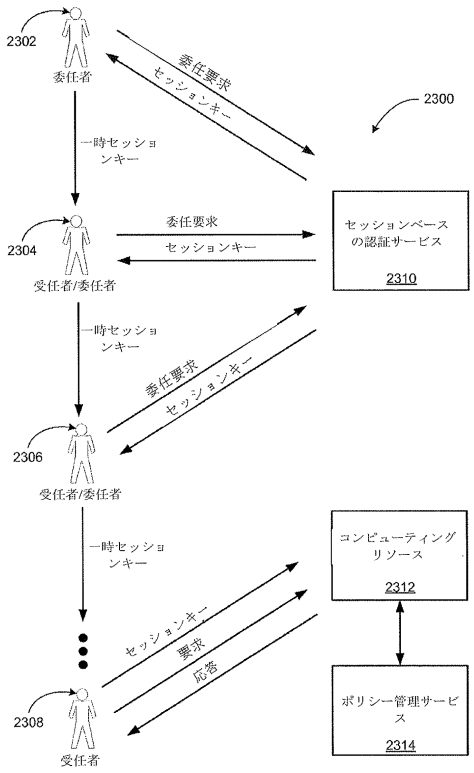
【図２１】



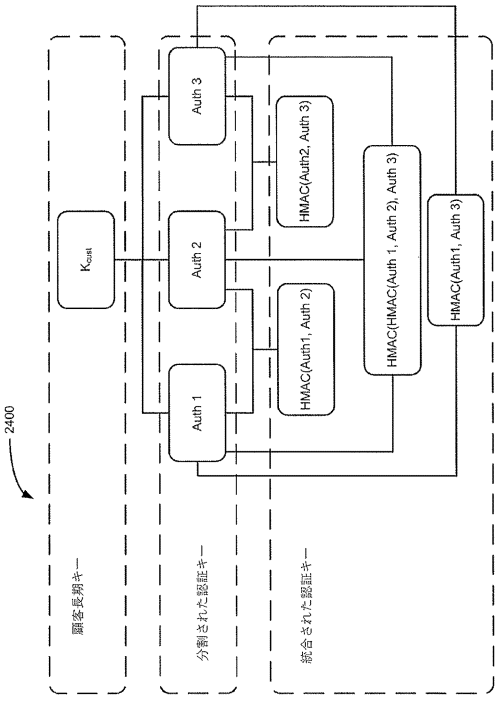
【図２２】



【図２３】



【図２４】



フロントページの続き

(31)優先権主張番号　13/248,973
(32)優先日　平成23年9月29日(2011.9.29)
(33)優先権主張国　米国(US)

(72)発明者　ブラッドリー　ジェフリー　ベーム
アメリカ合衆国　９８１０９－５２１０　ワシントン州　シアトル　テリー　アベニュー　ノース　４１０
(72)発明者　エリック　ディー．クラヘン
アメリカ合衆国　９８１０９－５２１０　ワシントン州　シアトル　テリー　アベニュー　ノース　４１０
(72)発明者　クリスティアン　エム．アイラック
アメリカ合衆国　９８１０９－５１１０　ワシントン州　シアトル　テリー　アベニュー　ノース　４１０
(72)発明者　ナザン　アール．フィッチ
アメリカ合衆国　９８１０９－５２１０　ワシントン州　シアトル　テリー　アベニュー　ノース　４１０
(72)発明者　エリック　ジェイソン　ブランドワイン
アメリカ合衆国　９８１０９－５２１０　ワシントン州　シアトル　テリー　アベニュー　ノース　４１０
(72)発明者　ケヴィン　ロス　オニール
アメリカ合衆国　９８１０９－５２１０　ワシントン州　シアトル　テリー　アベニュー　ノース　４１０

審査官　金沢　史明

(56)参考文献　特開２００３－０２２２５３（ＪＰ，Ａ）
特開２００３－０５８６５７（ＪＰ，Ａ）
特開２００７－１４９０１０（ＪＰ，Ａ）
特表２００６－５０８４７１（ＪＰ，Ａ）
特開２００７－２３３７０５（ＪＰ，Ａ）
特開２００７－２０６９６１（ＪＰ，Ａ）
特開２００６－２１７３２０（ＪＰ，Ａ）
米国特許出願公開第２００２／００９５５７０（ＵＳ，Ａ１）
米国特許出願公開第２００３／０１９６０８７（ＵＳ，Ａ１）