(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6656157号
(P6656157)
(45)発行日　令和2年3月4日(2020.3.4)　(24)登録日　令和2年2月6日(2020.2.6)

(51)Int.Cl.　F I
G06F 21/33 (2013.01)　G06F 21/33

請求項の数 14　(全 36 頁)

(21)出願番号　特願2016-542872(P2016-542872)
(86)(22)出願日　平成26年9月16日(2014.9.16)
(65)公表番号　特表2016-532984(P2016-532984A)
(43)公表日　平成28年10月20日(2016.10.20)
(86)国際出願番号　PCT/US2014/055874
(87)国際公開番号　WO2015/042046
(87)国際公開日　平成27年3月26日(2015.3.26)
審査請求日　平成28年3月9日(2016.3.9)
審判番号　不服2018-15262(P2018-15262/J1)
審判請求日　平成30年11月19日(2018.11.19)
(31)優先権主張番号　14/029,496
(32)優先日　平成25年9月17日(2013.9.17)
(33)優先権主張国・地域又は機関
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　100106541
弁理士　伊藤　信和
(72)発明者　スタルザー　マーク　エドワード
アメリカ合衆国　９８１０９－５２１０
ワシントン州　シアトル　テリー　アヴェニュー　ノース　４１０

最終頁に続く

(54)【発明の名称】ネットワーク接続自動化

(57)【特許請求の範囲】
【請求項１】
接続を認証するためのコンピュータ実装方法であって、
実行可能命令で構成された１つ又は複数のシステムの制御下で、コンピューティングリソースサービスプロバイダネットワークに接続されたコンピューティングリソースサービスプロバイダネットワークデバイスと当該コンピューティングリソースサービスプロバイダネットワークデバイスとは別に、カスタマネットワークに接続されたカスタマネットワークデバイスとの間の専用の物理ネットワーク接続を確立することと、
前記コンピューティングリソースサービスプロバイダによって運用される認証サービスが、前記コンピューティングリソースサービスプロバイダネットワークデバイスから前記物理ネットワーク接続を介して、前記カスタマネットワークデバイスを認証するための、カスタマの秘密キーに少なくとも部分的に基づいて生成された暗号認証情報を提供するよう前記カスタマネットワークデバイスに要求を送信することと、
前記コンピューティングリソースサービスプロバイダネットワークデバイスで、前記カスタマネットワークデバイスから前記暗号認証情報を受信することと、
前記コンピューティングリソースサービスプロバイダネットワークデバイスから、前記暗号認証情報を認証するために運用可能である認証サービスに、前記暗号認証情報を転送することと、
前記認証サービスが、カスタマの前記秘密キーを用いて予想カスタマデジタル署名を生成し、当該予想カスタマデジタル署名をもとに、受信した前記暗号認証情報が本物である

かを判断して前記暗号認証情報を認証することと、
前記認証サービスが前記暗号認証情報を無事に認証した結果として、前記カスタマネットワークデバイスから前記コンピューティングリソースサービスプロバイダネットワーク上のコンピューティングリソースサービスプロバイダの前記認証サービスとは異なる１つ又は複数のサービスに、専用の物理ネットワーク接続を経由して受信したネットワークトラフィックを送るように前記コンピューティングリソースサービスプロバイダネットワークデバイスを構成することと
を含む、コンピュータ実装方法。
【請求項２】
前記秘密キーが公開－秘密暗号キー組からの秘密キーである、請求項１に記載のコンピュータ実装方法。
【請求項３】
前記認証サービスが前記暗号認証情報を無事に認証した結果として、前記コンピューティングリソースサービスプロバイダネットワークデバイス上で前記カスタマのためにネットワークインタフェースを設定することをさらに含む、請求項１または請求項２に記載のコンピュータ実装方法。
【請求項４】
前記専用の物理ネットワーク接続が、前記カスタマから離れたコロケーションセンタでの物理接続に少なくとも部分的に基づいて確立され、前記物理接続が、前記カスタマネットワークデバイスのカスタマポートのセットから前記コンピューティングリソースサービスプロバイダネットワークデバイスのコンピューティングリソースサービスプロバイダポートのセットに接続される１本又は複数のケーブルを備える、請求項１ないし請求項３のいずれか一項に記載のコンピュータ実装方法。
【請求項５】
ある量の時間にわたって１回又は複数回、前記カスタマネットワークデバイスから追加の暗号認証情報を受信することをさらに含み、
前記カスタマネットワークデバイスから前記１つ又は複数のサービスへの前記ネットワークトラフィックを継続的に送ることが、前記追加の暗号認証情報を無事に認証することの条件とする、請求項１ないし請求項４のいずれか一項に記載のコンピュータ実装方法。
【請求項６】
前記暗号認証情報を提供するようにとの要求は、前記カスタマネットワークデバイス及び前記コンピューティングリソースサービスプロバイダネットワークデバイスによって使用される認証プロトコルに従って実行される、請求項１ないし請求項５のいずれか一項に記載のコンピュータ実装方法。
【請求項７】
前記暗号認証情報を提供するようにとの要求を送信する前に、前記コンピューティングリソースサービスプロバイダネットワークデバイスを欠いている通信チャネルを通して前記カスタマの前記秘密キーを受信することをさらに含む、請求項１ないし請求項６のいずれか一項に記載のコンピュータ実装方法。
【請求項８】
１台又は複数のプロセッサ、及び内部に前記１台又は複数のプロセッサによって実行させる命令が集約的に記憶された１つ又は複数の非一時的コンピュータ可読記憶媒体を含むシステムであって、
コンピューティングリソースサービスプロバイダネットワークに接続されたコンピューティングリソースサービスプロバイダネットワークデバイスと当該コンピューティングリソースサービスプロバイダネットワークデバイスとは別に、カスタマネットワークに接続されたカスタマネットワークデバイスとの間の専用の物理ネットワーク接続を確立させることと、
前記コンピューティングリソースサービスプロバイダによって運用される認証サービスが、前記コンピューティングリソースサービスプロバイダネットワークデバイスから前記

物理ネットワーク接続を介して、前記カスタマネットワークデバイスを認証するための、カスタマの秘密キーに少なくとも部分的に基づいて生成された暗号認証情報を提供するよう前記カスタマネットワークデバイスに要求を送信することと、
前記コンピューティングリソースサービスプロバイダネットワークデバイスに、前記カスタマネットワークデバイスから前記暗号認証情報を受信させることと、
前記コンピューティングリソースサービスプロバイダネットワークデバイスから、前記暗号認証情報を認証するために運用可能である認証サービスに、前記暗号認証情報を転送することと、
前記認証サービスが、カスタマの前記秘密キーを用いて予想カスタマデジタル署名を生成し、当該予想カスタマデジタル署名をもとに、受信した前記暗号認証情報が本物であるかを判断して前記暗号認証情報を認証することと、
前記認証サービスが前記暗号認証情報を無事に認証した結果として、前記カスタマネットワークデバイスから前記コンピューティングリソースサービスプロバイダネットワーク上のコンピューティングリソースサービスプロバイダの前記認証サービスとは異なる１つ又は複数のサービスに、専用の物理ネットワーク接続を経由して受信したネットワークトラフィックを送らせることと、を前記命令に含む、システム。
【請求項９】
前記カスタマネットワークデバイスから受信した前記暗号認証情報が本物であることを示す場合、再構成情報を前記コンピューティングリソースサービスプロバイダネットワークデバイスに送信し、それにより前記コンピューティングリソースサービスプロバイダネットワークデバイスに、カスタマネットワークデバイスから前記コンピューティングリソースサービスプロバイダの１つ又は複数の他のサービスにネットワークトラフィックを送らせることを前記命令に含み、
前記カスタマネットワークデバイスから受信した前記暗号認証情報が本物ではないことを示す場合、前記コンピューティングリソースサービスプロバイダネットワークデバイスに、前記カスタマネットワークデバイスから前記コンピューティングリソースサービスプロバイダの前記１つ又は複数の他のサービスへのネットワークトラフィックを拒否させることを前記命令に含む、請求項８に記載のシステム。
【請求項１０】
前記コンピューティングリソースサービスプロバイダに前記ネットワークトラフィックを拒否させることには前記カスタマネットワークデバイスから前記コンピューティングリソースサービスプロバイダの前記１つ又は複数の他のサービスへのネットワークトラフィックを拒否するための再構成情報を、前記コンピューティングリソースサービスプロバイダネットワークデバイスに送信することを含む、請求項９に記載のシステム。
【請求項１１】
前記カスタマネットワークデバイスから受信した前記暗号認証情報が本物であることを示す場合は、その結果として、前記コンピューティングリソースサービスプロバイダネットワークデバイス上で前記カスタマのためにネットワークインタフェースを設定することを前記命令にさらに含む、請求項９または請求項１０に記載のシステム。
【請求項１２】
前記専用の物理ネットワーク接続が前記カスタマから離れたコロケーションセンタでの、前記カスタマネットワークデバイスのカスタマポートのセットから前記コンピューティングリソースサービスプロバイダネットワークデバイスのコンピューティングリソースサービスプロバイダポートのセットに接続される１本又は複数のケーブルを備える物理接続に少なくとも部分的に基づくものである、請求項８ないし請求項１１のいずれか一項に記載のシステム。
【請求項１３】
前記暗号認証情報が、前記カスタマ及び前記コンピューティングリソースサービスプロバイダネットワークデバイスによって使用される認証プロトコルに従って前記専用の物理ネットワーク接続を通して送信される、請求項８ないし請求項１２のいずれか一項に記載

のシステム。
【請求項１４】
前記カスタマによって検証可能な第２の暗号情報をさらに生成させることと、
前記コンピューティングリソースサービスプロバイダネットワークデバイスを通して前記カスタマに前記暗号認証情報を送信させることと、を前記命令にさらに含む、請求項８ないし請求項１３のいずれか一項に記載のシステム。

【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本願は、すべての目的のために参照することにより、「ＩＮＴＥＲＦＡＣＥＳ　ＴＯ　ＭＡＮＡＧＥ　ＤＩＲＥＣＴ　ＮＥＴＷＯＲＫ　ＰＥＥＲＩＮＧＳ」という名称の、２０１１年１１月２９日に出願された米国特許出願番号第１３／３０６，７７５号、及び、「ＮＥＴＷＯＲＫ　ＣＯＮＮＥＣＴＩＯＮ　ＡＵＴＯＭＡＴＩＯＮ」という名称の、２０１３年９月１７日に出願された米国特許出願番号第１４／０２９，４９６号の全開示を組み込むものである。
【背景技術】
【０００２】
コンピューティングリソースサービスプロバイダ及び他のサービスプロバイダは多くの場合、専用のネットワーク接続を使用することによって自らのサービスへのアクセスをユーザに許可する。多くのユーザは、１つ又は複数のサービスにアクセスするために、例えば、コロケーション環境を活用してコンピューティングリソースサービスに直接的に接続する。それらの多くの優位点にも関わらず、コンピューティングリソースサービスプロバイダとカスタマとの間で専用の安全な接続を構成したとしても、それがすべてのリスクを免れているわけではないことがある。例えば、それを回避しようとする彼らの最善の努力にも関わらず、物理的な専用の接続でさえ、通信に対する権限のないアクセス及び／又は無作為のアクセスが可能である（例えば、パッチパネルでの）影響を受けやすい地点を有することがある。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】米国特許第２００７／０２３４０５４号
【発明の概要】
【課題を解決するための手段】
【０００４】
現在、コンピューティングリソースサービスプロバイダは、接続が安全であることを保証するために従来の認証方法を使用することがある。ただし、従来の認証方法は多くの場合、手動介入に頼り、本質的に柔軟性に乏しい。さらに、接続を安全に行うために使用される暗号技法は、接続への権限のないアクセスを得るために利用できるという脆弱性を有することがある。これらのリスクに適切に対応することは、専用接続に依存する組織にとって、及びコンピューティングリソースサービスプロバイダにとって追加費用となる。
【０００５】
本開示に係る多様な実施形態は、図面を参照して説明される。
【図面の簡単な説明】
【０００６】
【図１】多様な実施形態を実践できる環境の実施例を例示した図である。
【図２】多様な実施形態を実施できる環境の実施例を例示した図である。
【図３】少なくとも一実施形態に従ってコンピューティングリソースサービスプロバイダ

によって提供される１つ又は複数のサービスの実施例を例示した図である。
【図４】多様な実施形態を実践できる環境の実施例を例示した図である。
【図５】少なくとも一実施形態に従って物理接続が認証される環境の実施例を例示した図である。
【図６】少なくとも一実施形態に従って１つ又は複数のサービスとの接続が初期認証時に管理される環境の実施例を例示した図である。
【図７】少なくとも一実施形態に従って顧客とコンピューティングリソースサービスとの間に物理接続を確立するためのプロセスの実施例を例示した図である。
【図８】少なくとも一実施形態に従って初めて接続を認証するためのプロセスの実施例を例示した図である。
【図９】少なくとも一実施形態に従ってあらかじめ接続が確立された後に接続を認証するためのプロセスの実施例を例示した図である。
【図１０】少なくとも一実施形態に従って接続を認証するためのプロセスの実施例を例示した図である。
【図１１】多様な実施形態が実施できる環境を示す図である。
【発明を実施するための形態】
【０００７】
以下の説明では、多様な実施形態が説明される。説明のために、特定の構成及び詳細事項が、実施形態を完全に理解してもらうために示されている。しかしながら、また、実施形態が特定の詳細事項がなくても実践され得ることは当業者に明らかになるだろう。さらに、周知の特徴は説明されている実施形態を不明瞭にしないために省略又は簡略化されることがある。
【０００８】
本明細書に説明され、示唆されている技法はカスタマ（例えば、カスタマによって運用されているネットワーク）とコンピューティングリソースサービスプロバイダとの間の接続の認証に関するものである。実施形態では、コンピューティングリソースサービスプロバイダは、エンティティ（例えば、組織）とコンピューティングリソースサービスプロバイダとの間に直接的な接続を確立するためのエンティティからの要求を受信してよい。エンティティは、データストレージサービス、バーチャルコンピューティングシステムサービス、及び／又はデータベースサービス等の多様なサービスを運用することがある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であってよい。サービスの内の１つ又は複数のサービスを最適に使用するために、コンピューティングリソースサービスプロバイダは、カスタマが、直接的な接続、つまりコンピューティングリソースサービスプロバイダのコンピューティングリソースにカスタマのコンピューティングリソースを接続する物理的な通信接続を使用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ネットワークと通信できるようにしてよい。係る接続を確立するための技法例は、すべての目的のために参照することによりその全体が本明細書に組み込まれる「Ｉｎｔｅｒｆａｃｅｓ　ｔｏ　Ｍａｎａｇｅ　Ｄｉｒｅｃｔ　Ｎｅｔｗｏｒｋ　Ｐｅｅｒｉｎｇｓ」という名称の、２０１１年１１月２９日に出願された米国特許出願番号第１３／３０６，７７５号に説明されている。
【０００９】
コンピューティングリソースサービスプロバイダとカスタマとの間の接続を設定する前に、コンピューティングリソースサービスプロバイダは、コンピューティングリソースサービスプロバイダの従業員（例えば、データ技術者）が顧客とコンピューティングリソースサービスプロバイダとに関連付けられた物理的なルータを接続できるようにするために、授権書を作成してよい。この授権書は、コンピューティングリソースサービスプロバイダとの直接的な接続を確立するためにカスタマから受信された要求に応えて作成されてよい。
【００１０】
多様な実施形態では、コンピューティングリソースサービスプロバイダは、カスタマと

コンピューティングリソースサービスプロバイダとの間のネットワーク接続性を開始するために、接続時にカスタマルータに１つ又は複数の信号を送信してよい。これらの１つ又は複数の信号は、接続が正しく確立されたこと、及びカスタマがコンピューティングリソースサービスプロバイダに接続する権限を与えられた正しいエンティティであることを検証するために認証要求をさらに含んでよい。カスタマは、カスタマがコンピューティングリソースサービスプロバイダのコンピュータシステムにアクセスする権限を与えられていることを検証するために、コンピューティングリソースサービスプロバイダに応えて１つ又は複数の信号を送信してもよい。これらの１つ又は複数の信号は、１つ又は複数のカスタマコンピュータシステムを起源とする秘密暗号キー等の１つ又は複数の認証用クレデンシャルを使用して生成されるデジタル署名を含んでよい。この署名は、対称暗号アルゴリズム及び／又は非対称暗号アルゴリズムを使用して生成されてよい。コンピューティングリソースサービスプロバイダは、カスタマから受信された署名が本物であり、このカスタマに一致するかどうかを判断するために、カスタマ信号（又はカスタマ信号に少なくとも部分的に基づいた情報）を認証サービスに送信してよい。カスタマ信号が認証されない場合、コンピューティングリソースサービスプロバイダは多様なサービスへのアクセスを拒否してよい。それ以外の場合、カスタマはカスタマが使用することを選択した１つ又は複数のサービスへのアクセスを許可されてよい。

【００１１】

実施形態では、コンピューティングリソースサービスプロバイダは、接続が不正接続されていないことを保証するために、初期接続後に経時的にカスタマに１つ又は複数の認証要求を送信することがある。カスタマは、カスタマが接続を維持する権限を与えられている旨の証拠を提供するために、コンピューティングリソースサービスプロバイダに、ハッシュ関数及び暗号キーを使用して生成されたデジタル署名を含めてもよい、要求に対する応答を送信してよい。したがって、認証サービスを通して等、署名が検証される場合、コンピューティングリソースサービスプロバイダは接続を続行可能にしてよい。ただし、認証サービスが、カスタマがコンピューティングリソースサービスプロバイダによって提供されるサービスにアクセスする権限を有していることを検証できない場合、コンピューティングリソースサービスプロバイダは、カスタマがコンピューティングリソースサービスプロバイダに有効なデジタル署名を提供できるまで、カスタマのサービスへのアクセスを制限してよい。

【００１２】

実施形態では、カスタマは、接続が現在カスタマとコンピューティングリソースサービスプロバイダとの間にあることを検証するために、サービスに対する適切に構成されたＡＰＩコールを通して等、コンピューティングリソースサービスプロバイダに認証要求を送信する。コンピューティングリソースサービスプロバイダから受信された信号が本物ではない（例えば、コンピューティングリソースサービスプロバイダの代わりに有効なデジタル署名を含んでいない）場合、カスタマはコンピューティングリソースサービスプロバイダとの接続を制限する、又は終了さえしてもよい。それ以外の場合、カスタマは、要求時にコンピューティングリソースサービスプロバイダに認証用クレデンシャルを相互に与えてよいのであれば、コンピューティングリソースサービスプロバイダによって提供される多様なサービスへの自らのアクセスを続行してよい。

【００１３】

いくつかの実施形態では、カスタマは、、カスタマの通信が真にカスタマのコンピュータシステムを起源にしていることを認証サービスに検証させるために、サービスに対する適切に構成されたＡＰＩコールを通して等、コンピューティングリソースサービスプロバイダに認証要求を送信してよい。カスタマによって送信されるこの認証要求は、カスタマのアイデンティティを検証するためにコンピューティングリソースサービスプロバイダによって使用されてよいデジタル署名を含んでよい。デジタル署名が本物である場合、コンピューティングリソースサービスプロバイダは、コンピューティングリソースサービスプロバイダ用のデジタル署名を含んだ１つ又は複数の信号をカスタマに送信してよい。それ

に応じて、カスタマはこのデジタル署名を使用して、コンピュータリソースサービスプロバイダのアイデンティティを検証してよい。

【００１４】

このようにして、コンピューティングリソースサービスプロバイダ及びそのカスタマは、１台又は複数の物理的なルータを通して接続され、カスタマ又はコンピューティングリソースサービスプロバイダの信号を認証することに失敗した場合に接続が制限される、又は終了されることが保証され得る。さらに、本明細書に説明される技法は、更なる技術的な優位を容易にもたらす。例えば、いくつかの実施形態では、認証プロセスが、コンピューティングリソースサービスプロバイダ又はカスタマのどちらかによって管理されるコンピュータシステムによって実行されるため、接続を認証するために手動介入は要求されないことがある。したがって、これらの技法は、コンピューティングリソースサービスプロバイダ及びそのカスタマが安全な接続を保証する上で利用できる柔軟性を高め得る。さらに、代替認証プロセスの使用は、従来のルータ対ルータの認証技法の使用を排除し、従来の技法固有の脆弱性も潜在的に排除又は軽減し得る。更なる追加使用も本明細書に説明される多様な技法によって可能となる。

【００１５】

図１は、多様な実施形態を実践できる環境１００の実施例を例示する。環境１００で、コンピューティングリソースサービスプロバイダ１０２は、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に多様なコンピューティングリソースサービスを提供する。コンピューティングリソースサービスプロバイダ１０２は、１人又は複数のカスタマの代わりに多様なコンピューティングリソースをホストする組織であってよい。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は、ハードウェアサーバ、データストレージデバイス、ネットワークデバイス等の多様なコンピューティングハードウェアリソース、及びサーバラック、ネットワーキングケーブル等の他の設備をホストするために使用される１つ又は複数の施設を運用していてもよい。コンピューティングリソースハードウェアは、１つ又は複数のサービスを運用するためにそのコンピューティングハードウェアリソースを活用してよい。係るサービスは、物理的な設備において投資すべきカスタマの必要性を削減又は排除さえしつつ、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がコンピューティングリソースを遠隔で管理して当該カスタマによる運用をサポートできるようにするサービスを含んでもよい。サービス例として、多様なデータストレージサービス（オブジェクト単位のデータストレージサービス、アーカイブデータストレージサービス、データベースサービス等）、プログラム実行サービス、及び他のサービス等が含まれるが、これらに限定されるものではない。これらのサービスは、カスタマによって利用され、ウェブサイトの運営、組織をサポートする企業システムの運営、分散型計算、及び／又は他の活動を等の多種多様な活動をサポートするサービスであってもよい。

【００１６】

したがって、図１に示されるように、環境１００はカスタマ１０４を含む。カスタマ１０４は、コンピューティングリソースサービスプロバイダ１０２との直接的な接続を確立することによって少なくとも部分的に多様なサービスのいくらか又はすべてを活用する組織であってよい。コンピューティングリソースサービスプロバイダ１０２のカスタマ１０４は、コンピューティングリソースサービスプロバイダ１０２によって提供される多様なサービスを活用してよい。例えば、カスタマ１０４は、サービスに対して行われたバッチ要求、又はカスタマによる運用をサポートするためにサービスへのアクセスを要求するカスタマサーバ要求等、自動化されたプロセスを通してコンピューティングリソースサービスプロバイダ１０２によって提供されるサービスを活用してよい。カスタマ１０４は、コンピューティングリソースサービスプロバイダへの直接的な接続の設定を要求するためにコンピューティングリソースサービスプロバイダ１０２に接触してよい。コンピューティングリソースサービスプロバイダは、授権書を作成し、データ技術者を配置してもよく、あるいは、カスタマ１０２がカスタマ自身のデータ技術者もしくは第三者を利用してカスタマルータとコンピューティングリソースサービスプロバイダルータ１０６とを接続でき

るようにしてもよい。ルータは、遠隔場所に同様に設置してもよいデータセンタ又はコロケーションに設置してよい。ルータは例示の目的のために本開示を通して広範囲に使用されるが、本開示に例示される技法は概して他のネットワークデバイス（例えば、ゲートウェイデバイス等）にさらに適用してよい。

【００１７】

いったんカスタマ１０４とコンピューティングリソースサービスプロバイダルータ１０６との間の接続が確立されると、コンピューティングリソースサービスプロバイダルータはカスタマルータへの１つ又は複数の信号の送信を開始してよい。係る信号の一つは、カスタマ１０４がコンピューティングリソースサービスプロバイダ１０２に接続する権限を与えられていることを検証するために認証要求を含んでよい。この認証要求は、コンピューティングリソースサービスプロバイダ１０２によって維持され、運用される認証サービス１０８に起源してよい。認証サービス１０８は、受信されたカスタマデータをハッシュして、予想カスタマデジタル署名を生成するために必要となることがある暗号キーを入手するために、アカウントサービス（不図示）からカスタマ情報を入手するように構成されてよい。、カスタマのアイデンティティを検証するために、この予想カスタマデジタル署名を受信されたカスタマデジタル署名と比較してもよい。さらに、認証サービス１０８は、カスタマ１０４に認証要求を送信するためにコンピューティングリソースサービスプロバイダルータ１０６に実行可能なコマンドを送信するように構成されていてもよい。

【００１８】

認証要求に応えて、カスタマ１０４は、コンピューティングリソースサービスプロバイダルータ１０６に送信される１つ又は複数の信号を通して、追加のデータ（例えば、カスタマ識別番号、ポート番号等）とともにデジタル署名を含んだ１つ又は複数のデータパケットをコンピューティングリソースサービスプロバイダ１０２に提供してもよい。したがって、ルータ１０６は検証のために認証サービス１０８にこれらのデータパケットを送信してよい。認証サービス１０８は、予想カスタマデジタル署名を作成するために暗号キーとともにカスタマ１０４から受信された追加のデータをハッシュするように構成されてもよい。デジタル署名が一致する場合、認証サービス１０８は、カスタマがコンピューティングリソースサービスプロバイダ１０２によって提供される１つ又は複数の他のサービス１１０にアクセスできるようにするようにコンピューティングリソースサービスプロバイダルータ１０６を再構成してよい。これらの他のサービス１１０は、多様なデータストレージサービス（オブジェクト単位のデータストレージサービス、アーカイブデータストレージサービス、データサービス等）、プログラム実行サービス等を含んでよい。ただし、カスタマ１０４から受信されたデジタル署名が予想デジタル署名に一致しない場合、認証サービス１０８は他のサービス１１０へのアクセスを拒否してよい。

【００１９】

代わりに、カスタマ１０４は、コンピューティングリソースサービスプロバイダルータ１０６に１つ又は複数のデータパケットを送信することによって、サービスに対する適切に構成されたＡＰＩコールを通して等、認証プロセスを開始してよい。これらのデータパケットは秘密キーを使用して生成されたデジタル署名を含んでよく、秘密キーは、コンピューティングリソースサービスプロバイダ１０２によって処理されると、受信されたデジタル署名が本物であるかどうかを判断するために使用されてよい予想カスタマデジタル署名を生成するために、サービスプロバイダに暗号キーとともに受信されたデータをハッシュさせる。さらに、これらのデータパケットは、サービスプロバイダ１０２に、コンピューティングリソースサービスプロバイダのアイデンティティを検証するためにカスタマ１０４によって使用されてよい独自のデジタル署名を含んだ１つ又は複数のデータパケットを生成させてよい。このように、カスタマ１０４及びコンピューティングリソースサービスプロバイダ１０２の両方とも、直接的な物理接続を通して送信された信号の真正性を検証し得る。

【００２０】

いったんカスタマ１０４が１つ又は複数の他のサービス１１０へのアクセスを達成する

と、コンピューティングリソースサービスプロバイダ１０２は認証サービス１０８を使用して、接続が不正接続されていないことを保証するために１つ又は複数の認証要求をカスタマに送信してよい。接続が不正接続された可能性がある（例えば、カスタマ１０４から受信された認証用クレデンシャルが予想値に一致しない）旨の表示がある場合、コンピューティングリソースサービスプロバイダ１０２は、認証サービス１０８を通して、既存の接続に関して１つ又は複数のアクションを実行してよい。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１０２は、接続を制限するために１つ又は複数の実行可能命令をルータ１０６に送信するように認証サービス１０８を構成してよい。これは、カスタマ１０４に対して利用可能なネットワーク帯域幅を絞ること、又は他のサービス１１０へのアクセスを無効にすることを含んでよい。別の例では、認証サービス１０８は、アカウントサービス（不図示）を参照してカスタマ１０４の仕様に従って接続に対して１つ又は複数の制限を適用してよい。例えば、カスタマ１０４は、接続が不正接続される場合に所定のアクションが講じられることを、コンピューティングリソースサービスプロバイダ１０２への直接的な接続に対する初期の要求の間に指定していてもよい。コンピューティングリソースサービスプロバイダ１０２は、後の時点でカスタマ１０４がコンピューティングリソースサービスプロバイダに有効な認証用クレデンシャルを提供する場合、接続を復元してよい。

【００２１】

上述されたように、カスタマルータとコンピューティングリソースサービスプロバイダルータとの間の物理接続は、遠隔場所にしてもよいデータセンタ又はコロケーションで行われてよい。したがって、図２は多様な実施形態を実施できる環境の実施例を例示する。環境２００で、直接的な接続は、１人又は複数のカスタマ２０２とコンピューティングリソースサービスプロバイダ２１２との間で確立されていてもよい。上述されたように、カスタマ２０２は、コンピューティングリソースサービスプロバイダへの直接的な接続の設定を要求するためにコンピューティングリソースサービスプロバイダ２１２に接触してよい。したがって、コンピューティングリソースサービスプロバイダ２１２は、カスタマルータ２０６とコンピューティングリソースサービスプロバイダルータ２１０との間で物理接続を確立するためにデータ技術者を配置してよい。ルータ２０６、２１０は、さらには遠隔場所に設置してよいデータセンタ又はコロケーション２０４に設置してよい。

【００２２】

この例示した実施例で、１人又は複数のカスタマ２０２とコンピューティングリソースサービスプロバイダ２１２との間の直接的な接続は、カスタマルータ２０６とコンピューティングリソースサービスプロバイダルータ２１０との間にケーブルを設置することによって確立されてよい。図２に示されるルータ２０６、２１０は、ユーザが受取人にデータを送信する又はソースからデータを受信することができるように構成されたさまざまなポートを含んでよい。例えば、カスタマ及びプロバイダが光ファイバケーブルを使用して接続する実施形態では、ルータ２０６、２１０はいくつかの送信ポート及びいくつかの受信ポートを含んでよい。したがって、カスタマルータ２０６とコンピューティングリソースサービスプロバイダルータ２１０との間の接続は、ルータへの接続時に、カスタマ２０２及びコンピューティングリソースサービスプロバイダ２１２がデータを送信及び受信できるようにする複数のケーブルを含んでよい。

【００２３】

コロケーション２０４の構成に応じて、カスタマルータ２０６とコンピューティングリソースサービスプロバイダルータ２１０との間の直接的な物理接続（又は単に「物理接続」）は、１つ又は複数のパッチパネル２０８又は他の介入構造（例えば、非ルーティングデバイス、カプラ等）を含んでよい。例えば、１つ又は複数のパッチパネル２０８は、コロケーション２０４の運用者がより短い長さのケーブルを使用して、カスタマルータ２０６等の２台以上のデバイス及びコンピューティングリソースサービスプロバイダルータ２１０を接続できるようにしてよい。さらに、入力ポート／出力ポートはパッチパネル２０８から適宜名前を付けられてよいので、パッチパネル２０８は、接続を確立するために使

用されるポートの識別を簡略化するために使用されてよい。言い換えると、本開示の実施形態は、隣接するケーブルがカスタマ及びプロバイダルータを接続する実施形態に制限されない。いったん物理接続がコロケーション２０４でカスタマルータ２０６からコンピューティングリソースサービスプロバイダルータ２１０へ確立されると、コンピューティングリソースサービスプロバイダ２１２はコンピューティングリソースサービスプロバイダルータを通してカスタマルータに１つ又は複数の信号を送信し始めてよい。カスタマルータ２０６は、コンピューティングリソースサービスプロバイダ２１２から１つ又は複数の信号を受信すると、処理のためにカスタマ２０２に１つ又は複数の信号を送信してよい。上述されたように、１つ又は複数の信号は、カスタマ２０２によって運用されるコンピュータシステムに認証証拠を含んだ応答を送信させてよい認証要求を含んでよい。認証証拠は、デジタル署名又はカスタマ２０２のアイデンティティを確立するために必要な他のアカウント用クレデンシャルを含んでよい。認証のためのデジタル署名の使用は例示を目的とした本開示を通して広範囲に使用されるが、他の認証方法を使用してもよい。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２１２によって送信される認証要求は、カスタマグラフィックユーザインタフェースをパスワードに対するプロンプトによってカスタマ２０２のコンピュータシステム上に表示させてもよい、実行可能命令を含んでよい。したがって、カスタマ２０２は、接続を認証するためにプロンプトでパスワードをタイプ入力するように要求されることがある。

【００２４】

いったん接続が認証されると、コンピューティングリソースサービスプロバイダ２１２は、認証サービスを通して、カスタマ２０２と、コンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスとの間での通信を可能にするようにコンピューティングリソースサービスプロバイダルータ２１０を再構成してよい。後に、コンピューティングリソースサービスプロバイダ２１２は、接続が不正接続されていないことを検証するために、ルータ２１０を通してカスタマ２０２に１つ又は複数の信号を送信してよい。カスタマ２０２がコンピューティングリソースサービスプロバイダ２１２に適切な認証証拠を提供できない場合（例えば、無効なクレデンシャル、無効なデジタル署名、正しくないインターネットプロトコル（ＩＰ）アドレス、チェックサム不一致等）、コンピューティングリソースサービスプロバイダは、１つ又は複数のサービスへのカスタマ２０２のアクセスを制限するために認証サービスを通して再度コンピューティングリソースサービスプロバイダルータ２１０を再構成してよい。

【００２５】

同時に、カスタマ２０２は、接続が不正接続されていないことを検証するために、カスタマルータ２０６を通してコンピューティングリソースサービスプロバイダ２１２に１つ又は複数の信号を送信してよい。コンピューティングリソースサービスプロバイダ２１２が適切な認証証拠を提供できない場合、カスタマ２０２は、既存の接続を制限または終了さえするためにも、カスタマによって運用されている１つ又は複数のコンピュータシステムを通してカスタマルータ２０６に実行可能なコマンドを送信してよい。

【００２６】

上述されたように、コンピューティングリソースサービスプロバイダは、カスタマがその営業活動をサポートするために使用するであろういくつかのサービスを提供してよい。したがって、図３は、少なくとも一実施形態に従ってコンピューティングリソースサービスプロバイダ３０２によって提供される１つ又は複数のサービスの実施例を例示するものである。この実施例では、コンピューティングリソースサービスプロバイダ３０２は少なくとも５つのタイプのサービスを提供する。コンピューティングリソースサービスプロバイダ３０２によって提供されるサービスは、この例では、バーチャルコンピュータシステムサービス３０４、オブジェクト単位のデータストレージサービス３０６、データベースサービス３０８、アカウントサービス３１０、認証サービス３１２、及び１つ又は複数の他のサービス３１４を含む。ただし、本開示のすべての実施形態がすべての係るサービスを含むわけではなく、追加サービスは本明細書に明示的に説明されるサービスに加えて、

又は該サービスの代替策として提供されてもよい。

【００２７】

バーチャルコンピュータシステムサービス３０４は、コンピューティングリソースサービスプロバイダ３０２のカスタマの代わりに、バーチャルコンピューティングシステム上にバーチャルマシンインスタンスをインスタンス化するように構成されたコンピューティングリソースの集合体であってよい。コンピューティングリソースサービスプロバイダ３０２のカスタマはバーチャルコンピュータシステムのサービスと対話して、コンピューティングリソースサービスプロバイダ３０２によってホストされ、運用されている物理的なコンピューティングデバイス上でインスタンス化されるバーチャルコンピュータシステムを設定し、運用してよい。バーチャルコンピュータシステムは、ウェブサイトをサポートするサーバとして運用するため等、多様な目的に使用され得る。バーチャルコンピュータシステム用の他のアプリケーションは、データベースアプリケーション、電子商取引アプリケーション、業務アプリケーション、及び／又は他のアプリケーションをサポートするためのものであってよい。

【００２８】

オブジェクト単位のデータストレージサービス３０６は、カスタマのためにデータを記憶するために集合的に動作するコンピューティングリソースの集合体を含んでよい。オブジェクト単位のデータストレージサービス３０６に記憶されるデータは、データオブジェクトに編成されてもよい。データオブジェクトは、おそらくサイズに対する特定の制約を除き任意のサイズを有してよい。したがって、オブジェクト単位のデータストレージサービス３０６は、さまざまなサイズの多数のデータオブジェクトを記憶してよい。オブジェクト単位のデータストレージサービス３０６は、データストレージサービス３０６によって記憶されたデータオブジェクトと関連して他の動作を取り出す又は実行するためにカスタマによって使用されてもよい、データオブジェクトの識別子とデータオブジェクトを関連付けるキー値ストアとして運用してよい。データストレージサービスに対するアクセスは、適切に構成されたＡＰＩコールを通してであってもよい。

【００２９】

データベースサービス３０８は、１人又は複数のカスタマのために１つ又は複数のデータベースを実行するために集合的に運用するコンピューティングリソースの集合体であってもよい。コンピューティングリソースサービスプロバイダ３０２のカスタマは、適切に構成されたＡＰＩコールを活用することによってデータベースサービス３０８からデータベースを運用し、管理してよい。これは、さらにはカスタマがデータベースでの運用を維持し、潜在的に拡大縮小できるようにしてよい。

【００３０】

アカウントサービス３１０は、コンピューティングリソースサービスプロバイダ３０２のカスタマごとにカスタマアカウント情報を保持するために集合的に運用するコンピューティングリソースの集合体であってもよい。アカウントサービス３１０は、コンピューティングリソースサービスプロバイダ３０２のカスタマごとに、例えば、カスタマの名前、住所、電話番号、請求書作成の詳細、及び他の個人識別情報を含んでよい。さらに、アカウントサービス３１０は、暗号キー、又はカスタマがコンピューティングリソースサービスプロバイダ３０２によって提供される１つ又は複数のサービスにアクセスするための適正な許可を有していることを検証するために使用されてよい他のクレデンシャルを含んでよい。したがって、アカウントサービス３１０は、認証サービス３１２と連動して運用されることで、カスタマ接続を有効にし、カスタマが万一適切な認証証拠（例えば、デジタル署名、パスワード等）を提供できない場合に、コンピューティングリソースサービスプロバイダ３０２によって提供される１つ又は複数のサービスに対するアクセスを制限するように構成されてよい。カスタマは、必要に応じてアカウント情報を提供し、更新するために、インターネット等の１つ又は複数の通信ネットワークを通してアカウントサービス３１０と対話できてもよい。したがって、カスタマはアカウントサービス３１０にアクセスして、カスタマとコンピューティングリソースサービスプロバイダ３０２の両方ともが

物理接続を認証するために必要な暗号キーのコピーを有していることを保証するためにキー交換を実行してよい。

【００３１】

認証サービス３１２は、上述されたように、コンピューティングリソースサービスプロバイダ３０２とカスタマとの間の接続を認証し、検証するのに役立ててもよい。例えば、カスタマとコンピューティングリソースサービスプロバイダ３０２との間に（例えば、図２に示されるようにコロケーションに設置されたルータを使用することで）直接的な接続が確立された後、認証サービス３１２は、カスタマがコンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスにアクセスする許可を有していることを保証するために、カスタマに認証要求を送信してよい。したがって、認証サービス３１２は、カスタマから認証証拠を受け取り、提供された認証証拠が本物であるかを判断するために１つ又は複数の動作を実行するように構成されてもよい。例えば、認証サービス３１２はアカウントサービス３１０と対話して、提供された認証証拠（例えば、１つ又は複数の暗号キー、パスワード、カスタマ識別番号等）を検証するために必要なカスタマ情報を入手してもよい。認証証拠が適切ではない場合、認証サービス３１２は、カスタマが適切な認証証拠を提供できるまで１つ又は複数のサービスへのカスタマアクセスを制限するためにコンピューティングリソースサービスプロバイダ３０２のルータに１つ又は複数の実行可能なコマンドを送信してよい。認証サービス３１２は、カスタマとコンピューティングリソースサービスプロバイダ３０２との間の接続が不正接続されないことを保証するために、異なる時間にこの認証プロセスを実行するように構成されてもよい。

【００３２】

認証サービス３１２は、さらに、コンピューティングリソースサービスプロバイダ３０２にカスタマによって送信される認証要求に応えるように構成されていてもよい。例えば、カスタマとコンピューティングリソースサービスプロバイダ３０２との間に直接的な接続が確立された後、カスタマは、接続が本物であり、不正接続されていないことを検証するためにコンピューティングリソースサービスプロバイダに認証要求を送信することがある。認証サービス３１２は、当該要求を処理し、接続が本物であることを検証するために必要な認証証拠を提供してもよい。例えば、認証サービス３１２はアカウントサービス３１０にアクセスして、カスタマに関係するアカウント情報を見つけ、接続を認証するために必要とされる認証証拠のタイプを識別するように構成されてもよい。このようにして、認証サービス３１２は、カスタマとコンピューティングリソースサービスプロバイダ３０２との間の接続に追加のセキュリティを提供してよい。

【００３３】

コンピューティングリソースサービスプロバイダ３０２は、そのカスタマの必要性に基づいて１つ又は複数の他のサービス３１４をさらに保持してよい。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３０２は、ブロックレベルのデータストレージボリュームを活用することによって、カスタマのためにデータを記憶するために集合的に運用するコンピューティングリソースの集合体を含むことが可能なブロックレベルのデータストレージサービスを保持してよい。ストレージボリュームは、ブロックレベルカスタマインタフェースとともに、未処理のフォーマットされていないブロックストレージデバイスのように動作するように構成されてもよい。したがって、カスタマは、サービスに対する適正に構成されたＡＰＩコールを通して、ブロックレベルのデータストレージボリュームの上部にファイルシステムを作成するか、又はブロックレベルのストレージデバイス（例えば、ハードドライブ）としてボリュームを活用してよい。他のサービスは、オブジェクトレベルのアーカイブデータストレージサービス、他のサービスを管理するサービス、及び／又は他のサービスを含むが、これらに限定されるものではない。

【００３４】

上述されたように、コンピューティングリソースサービスプロバイダは、カスタマとコンピューティングリソースサービスプロバイダとの間の直接的な物理接続を認証するために認証サービスを活用してよい。ただし、接続を認証するための認証サービスの使用は他

のタイプの接続のために使用されてもよい。したがって、図４は、多様な実施形態を実践できる環境４００の実施例を例示したものである。環境４００で、カスタマはカスタマゲートウェイデバイス４０２を活用して、インターネット等の１つ又は複数の通信ネットワーク４０４を通してコンピューティングリソースサービスプロバイダ４０８と通信してよい。インターネットは例示目的の本開示を通して広範囲に使用されるが、本開示はこのように制限されるものではない。例えば、ゲートウェイデバイス４０２は、ローカルエリアネットワーク（ＬＡＮ）、イントラネット、エクストラネット、無線ネットワーク、及びこれらの任意の組合せを通してコンピューティングリソースサービスプロバイダ４０８と通信するために使用されてもよい。

【００３５】

カスタマゲートウェイデバイス４０２は、ネットワーク４０４への入口、つまり「ゲートウェイ」として働くように構成された任意のデバイスであってよい。カスタマゲートウェイ４０２は、カスタマコンピュータシステムで生じるデータを、意図された受取人（例えば、この場合、ネットワーク４０４を渡ってコンピューティングリソースサービスプロバイダ４０８）に送信されてよいデータパケットに変換するように構成されてもよい。さらに、カスタマゲートウェイデバイス４０２は、ネットワーク４０４を通して送信されるあらゆるデータパケットを受信し、これらのデータパケットをカスタマコンピュータシステムによって読み取り可能であるデータに変換するように構成されてもよい。例えば、カスタマゲートウェイデバイス４０２がインターネットを通してコンピューティングリソースサービスプロバイダ４０８に接続される場合、カスタマゲートウェイデバイス４０２は、伝送制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）等の通信プロトコルのセットを使用して、コンピューティングリソースサービスプロバイダ４０８にデータパケットを送信するように構成されてもよい。ＩＰ構成要素は、インターネットを通してカスタマコンピュータシステムからコンピューティングリソースサービスプロバイダ４０８へのルーティングを提供してもよい。これは、カスタマコンピュータシステム及びコンピューティングリソースサービスプロバイダ４０８のシステムに対応してよいＩＰアドレス（例えば、ＩＰｖ４アドレス又はＩＰｖ６アドレス）を使用することで成し遂げられてもよい。ＴＣＰ構成要素は、カスタマからコンピューティングリソースサービスプロバイダ４０８へのデータの正しい配信を検証することに対して責任を負うことがある。

【００３６】

カスタマコンピュータシステム及びコンピューティングリソースサービスプロバイダ４０８のコンピューティングシステムは追加のネットワークプロトコルをさらに使用して、データパケットのルーティングのために最も効率的な経路又は最も都合の良い経路を特定してよい。例えば、多様なコンピュータシステムは、ネットワーク４０４でルーティング情報を交換するためにボーダーゲートウェイプロトコル（ＢＧＰ）を活用してよい。カスタマコンピュータシステム及びコンピューティングリソースサービスプロバイダのコンピュータシステムはＢＧＰを使用して、ネットワーク４０４（例えば、インターネット）を渡って送信されるデータパケットを送受信するために利用できる利用可能なゲートウェイデバイス（例えば、ルータ）を決定してよい。このようにして、ＢＧＰを使用するコンピュータシステムは、コンピュータシステムに接続され、ネットワーク４０４をサポートする多様なルータを通してデータパケットを送信するためにＴＣＰ／ＩＰ依存することがある。

【００３７】

ネットワーク４０４を通してカスタマゲートウェイデバイス４０２をコンピューティングリソースサービスプロバイダ４０８に接続するために使用されるプロトコルは、カスタマ及びコンピューティングリソースサービスプロバイダが安全な接続４０６に参加する権限を与えられていることを検証するために必要なセキュリティプロトコルを含んでよい。安全な接続４０６は、１つ又は複数の安全なトンネル（例えば、１つ又は複数の暗号化方法を使用するインターネットプロトコルセキュリティ（ＩＰｓｅｃ）トンネルを通して運用される仮想プライベートネットワーク（ＶＰＮ）であってもよい。このようにして、初

期の接続がこのセキュリティプロトコルを使用してネットワーク４０４を通してカスタマとコンピューティングリソースサービスプロバイダ４０８との間で行われると、コンピューティングリソースサービスプロバイダは、カスタマがこの安全な接続４０６に参加する権限を有しているのかどうかを判断するために認証要求をカスタマに送信してよい。したがって、カスタマは、カスタマゲートウェイデバイス４０２を通して、コンピューティングリソースサービスプロバイダ４０８によって提供される認証サービスのＩＰアドレス及びセキュリティプロトコルに従う認証証拠（例えば、パスワード、デジタル署名等）を含んだデータパケットを送信してよい。

【００３８】

コンピューティングリソースサービスプロバイダ４０８によって提供される認証サービスはいったんカスタマゲートウェイデバイス４０２からデータパケットを受信すると、受信された認証クレデンシャルは、予想カスタマデジタル署名を生成するために、カスタマと関連付けられた暗号キーとともに、受信されたデータをハッシュするためにハッシュ関数を活用してよい。その結果、コンピューティングリソースサービスプロバイダ４０８は、これらの署名が一致するかどうかを判断するためにカスタマゲートウェイデバイス４０２から受信されたデジタル署名とこの予想カスタマデジタル署名を比較してよい。一致する場合、コンピューティングリソースサービスプロバイダ４０８は、カスタマが、コンピューティングリソースサービスプロバイダによって提供される１つ又は複数の他のサービスにアクセスするのを許可するように独自のゲートウェイデバイスを再構成してよい。しかし、デジタル署名が一致しない場合、１つ又は複数の他のサービスに送信されるいずれのデータパケットも拒否されてよい。さらに、カスタマはコンピューティングリソースサービスプロバイダ４０８に認証要求を送信するためにカスタマゲートウェイデバイス４０２を使用してよい。したがって、コンピューティングリソースサービスプロバイダ４０８は、カスタマコンピューティングシステムのＩＰアドレス、及びセキュリティプロトコルに従う認証クレデンシャル（例えば、デジタル署名、パスワード等）を含んだデータパケットを送信してよい。受信された認証クレデンシャルが不適切である場合、カスタマはコンピューティングリソースサービスプロバイダ４０８への安全な接続４０６を制限または終了するためにカスタマゲートウェイデバイス４０２に１つ又は複数の実行可能なコマンドを送信してよい。

【００３９】

図５は、少なくとも一実施形態に従って物理接続が認証される環境５００の実施例を例示する。環境５００で、カスタマはコンピューティングリソースサービスプロバイダとの直接的な接続を確立するためにコンピューティングリソースサービスプロバイダ５０４に要求を提示してよい。その結果、コンピューティングリソースサービスプロバイダ５０４はカスタマルータ５０２をコンピューティングリソースサービスプロバイダルータ５０６に物理的に接続するために授権書を作成してよい。図２に示されるように、データ技術者を物理接続を確立するために配置させてもよい。

【００４０】

カスタマルータ５０２とコンピューティングリソースサービスプロバイダ５０６の間でいったん物理接続が確立されると、コンピューティングリソースサービスプロバイダ５０４は、認証サービス５０８を活用して物理接続を通したカスタマ送信が権限を与えられたカスタマを起源とすることを検証してよい。したがって、認証サービス５０８は、コンピューティングリソースサービスプロバイダルータ５０６を通して認証要求を送信するように構成されてもよい。コンピューティングリソースサービスプロバイダルータ５０６は、カスタマからの応答を引き出すために、上述されたようにセキュリティプロトコルを使用してこの認証要求を送信するように構成されてよい。

【００４１】

したがって、カスタマルータ５０２はこの認証要求を受信し、処理のために１つ又は複数のカスタマコンピュータシステムに要求を送信してよい。１つ又は複数のカスタマコンピュータシステムは、カスタマが利用できる他のサービス５１２にアクセスするために必

要な任意の他の必須情報とともに、カスタマのアイデンティティを検証するために必要な認証証拠（例えば、パスワード、デジタル署名等）を含んだデータパケットを準備するように構成されてもよい。このデータパケットはカスタマルータ５０６に送信されてもよいが、これは認証証拠を含んだデータパケットを送信するためにセキュリティプロトコルを同様に活用してもよい。

【００４２】

コンピューティングリソースサービスプロバイダ５０６は、検証のために認証サービス５０８に受信されたカスタマデータパケットを送信してよい。従って、認証サービス５０８は、データパケットから認証証拠を抽出するように構成されてもよい。認証証拠は、受信されたデータのハッシュ、及びコンピューティングリソースサービスプロバイダによって保持され、カスタマに特有の暗号キーを使用して検証されることを必要とするであろうデジタル署名を含んでよい。このようにして、認証サービス５０８は、関連するカスタマ情報を入手するためにコンピューティングリソースサービスプロバイダ５０４によって管理されるアカウントサービス５１０と対話するように構成されてもよい。例えば、アカウントサービス５１０は、上述されたように、コンピューティングリソースサービスプロバイダ５０４のカスタマごとのカスタマアカウント情報を含んでよい。例えば、カスタマアカウントは、受信されたデジタル署名が本物であることを検証し、ひいては、コンピューティングリソースサービスプロバイダ５０４に直接的に接続されるカスタマコンピュータシステムのアイデンティティを検証するために予想カスタマデジタル署名を作成するために使用されてもよい１つ又は複数の暗号キーを含んでよい。したがって、アカウントサービス５１０は認証サービス５０８にこれらのキーを送信するように構成されてもよい。

【００４３】

認証サービス５０８は、予想カスタマデジタル署名を作成し、この署名をカスタマ認証証拠と一致させることを試みるために、カスタマから受信されるデータとともにアカウントサービス５１０からの暗号キーを使用してよい。デジタル署名間で結果的に一致する場合、認証サービス５０８は、カスタマがコンピューティングリソースサービスプロバイダ５０４によって提供される他のサービス５１２にアクセスできるようにするために、コンピューティングリソースサービスプロバイダルータ５０６に１つ又は複数の実行可能なコマンドを送信してよい。しかし、一致を確立できない場合、認証サービス５０８は、他のサービス５１２へのアクセスが拒否された理由を含んだカスタマへの情報メッセージを送信してよい。

【００４４】

別の実施形態では、いったんカスタマルータ５０２とコンピューティングリソースサービスプロバイダルータ５０６との間で物理接続が確立されると、カスタマはカスタマ情報及びデジタル署名を含んだ１つ又は複数のデータパケットを、カスタマのアイデンティティを検証するために使用されてもよい、サービスに対する１つ又は複数の適切に構成されたＡＰＩコール等を通して、生成してよい。これらのデータパケットは、認証プロトコルを使用した物理接続上でコンピューティングリソースサービスプロバイダルータ５０６に送信されてもよい。このルータ５０６は、さらなる処理のために認証サービス５０８にこれらのデータパケットを伝送するように構成されてもよい。

【００４５】

認証サービス５０８は、予想カスタマデジタル署名を作成するために必要な１つ又は複数の暗号キーを入手するためにアカウントサービス５１０と対話するように構成されてもよい。したがって、認証サービス５０８は、この予想カスタマデジタル署名を作成するために暗号キー及び受信されたカスタマデータをハッシュするように構成されてもよい。この署名と受信されたカスタマデジタル署名とを比較して、一致しているかどうかを判断してもよい。一致している場合、カスタマ送信は本物と見なされ、カスタマがコンピューティングリソースサービスプロバイダ５０４によって提供される１つ又は複数の他のサービス５１２にアクセスできるようにするために、認証サービス５０８からプロバイダルータ５０６に１つ又は複数の実行可能命令を送信させてもよい。例えば、カスタマ送信が本物

であると見なされる場合、コンピューティングリソースサービスプロバイダ５０４は、カスタマがこれらの他のサービス５１２にアクセスするために１つ又は複数のバーチャルインタフェースを設定できるようにしてよい。

【００４６】

さらに、カスタマアイデンティティの検証は、認証サービス５０８に、カスタマルータ５０２に送信されるであろうコンピューティングリソースサービスプロバイダ５０４のためのデジタル署名を含んだ１つ又は複数のデータパケットを生成させてもよい。これによって、カスタマがコンピューティングリソースサービスプロバイダ５０４のアイデンティティを検証できるようにしてよい。

【００４７】

カスタマの初期認証が行われた後、カスタマは直ちにコンピューティングリソースサービスプロバイダによって提供されるさまざまなサービスにアクセスすることができる。しかし、接続が不正接続されていないことを保証するために、カスタマとコンピューティングリソースサービスプロバイダとの間でさらなる認証要求が送信されてもよい。したがって、図６は、１つ又は複数のサービスを伴う接続が、少なくとも一実施形態に従って初期認証時に管理される環境６００の実施例を例示する。環境６００で、カスタマはコンピューティングリソースサービスプロバイダ６０４によって提供される１つ又は複数の他のサービス６１２にアクセスするためにカスタマルータ６０２を通して１つ又は複数の信号を送信してよい。したがって、これらの１つ又は複数の信号はコンピューティングリソースサービスプロバイダルータ６０６によって受信されて、１つ又は複数の他のサービス６１２に処理のため送信されてもよい。例えば、カスタマは、１つ又は複数のサービス６１２にアクセスするために必要となるであろうバーチャルインタフェースを設定するためにカスタマルータ６０２を活用してよい。このようにして、カスタマは自分の目的のために１つ又は複数のサービス６１２を活用することができる。

【００４８】

カスタマとコンピューティングリソースサービスプロバイダ６０４とその関連付けられた他のサービス６１２との間の対話中の任意の時点で、認証サービス６０８は、接続が不正接続されていないこと（例えば、第三者が接続を妨害している等）を保証するために、コンピューティングリソースサービスプロバイダルータ６０６及びカスタマルータ６０２を介してカスタマに認証要求を送信してよい。したがって、カスタマは、受信した認証要求を満たすために必要な認証証拠を送信するためにカスタマによって保持され、運用される１つ又は複数のコンピュータシステムを使用してよい。この認証証拠は、カスタマルータ６０２を通して送信されてもよい。図５に示される初期の認証プロセスにおけるように、認証証拠は、認証要求で要求されるパスワード、デジタル署名、又は任意の他のクレデンシャルを含んでよい。この認証証拠は、セキュリティプロトコルに従って構成された１つ又は複数のデータパケットで、コンピューティングリソースサービスプロバイダ６０４に送信されてもよい。

【００４９】

コンピューティングリソースサービスプロバイダルータ６０６は、この認証証拠を受信し、それに応じて検証のために認証サービス６０８に証拠を配信してよい。図５に示されるように、認証サービス６０８は、受信された認証証拠を評価するために必要な関連するカスタマ情報（例えば、暗号キー、カスタマアカウント用クレデンシャル等）を入手するためにアカウントサービス６１０と対話するように構成されてもよい。カスタマによって提供される認証証拠が本物であると確認されると、認証サービス６０８はカスタマによる他のサービス６１２への継続アクセスを可能にしてよい。ただし、提供された認証証拠がアカウントサービス６１０から入手される関連するカスタマ情報と適合しない場合、認証サービス６０８は、コンピューティングリソースサービスプロバイダ６０４によって提供される他のサービス６１２へのカスタマアクセスを制限するためにコンピューティングリソースサービスプロバイダルータ６０６に１つ又は複数の実行可能命令を送信してよい。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ルータ６０６は、カスタマが利

用できる接続帯域幅を削減する、又は接続もしくはバーチャルインタフェースを完全に終了するように構成されてもよい。代わりに、認証サービス６０８は、認証チャレンジが失敗した場合に講じられてよい１つ又は複数のアクションを識別するためにアカウントサービス６１０と再び対話するように構成されてもよい。例えば、カスタマは、コンピューティングリソースサービスプロバイダ６０４が、他のサービス６１２にアクセスしているカスタマであると主張しているユーザに関係するすべての活動を監視し、記録することを指定してよい。

【００５０】

代わりに、カスタマとコンピューティングリソースサービスプロバイダ６０４とその関連付けられた他のサービス６１２との間の対話中の任意の時点で、カスタマによって運用されるコンピュータシステムは、接続が不正接続されていないことを保証するためにコンピューティングリソースサービスプロバイダに１つ又は複数の認証要求を送信してよい。いったん要求がコンピューティングリソースサービスプロバイダルータ６０６によって受信されると、要求は処理のために認証サーバ６０８に送信されてもよい。認証サービス６０８は、カスタマ認証要求を満たす認証証拠を作成するために必要な１つ又は複数の暗号キーを含むが、これに限定されるものではない関連するカスタマ情報を入手するために、アカウントサービス６１０と対話するように構成されてもよい。例えば、認証サービス６０８は、デジタル署名を作成するためにデータ及び暗号キーをハッシュするハッシュ関数を使用するように構成されてもよい。したがって、認証サービス６０８は、コンピューティングリソースサービスプロバイダ６０６とカスタマルータ６０２との間の物理接続を介してカスタマコンピュータシステムに送信することのできる他のデータとともに認証証拠（例えば、デジタル署名）を含んでよい１つ又は複数のデータパケットを生成してよい。

【００５１】

コンピューティングリソースサービスプロバイダ６０４によって提供される認証証拠が不適切である場合、カスタマコンピューティングシステムは、カスタマルータ６０２に接続を終了させることのできる実行可能なコマンドを送信するように構成されてもよい。これは、データ技術者が物理接続を断つこと、又は物理接続を介した１つ又は複数の信号の送信の完全な停止に対する要求を生成することを含んでよい。しかし、コンピューティングリソースサービスプロバイダ６０４との接続が本当に本物であるように、認証証拠が適切である場合、、カスタマはそのビジネスをサポートするために必要な１つ又は複数の他のサービス６１２にアクセスするために物理接続を活用し続けてよい。

【００５２】

別の実施形態では、カスタマは、カスタマのアイデンティティを検証するために使用することのできる、サービスに対する１つ又は複数の適切に構成されたＡＰＩコール等を通して、暗号認証情報を含んだ追加のデータパケットを生成してよい。上述されたように、これらのデータパケットはコンピューティングリソースサービスプロバイダルータ６０６へ認証プロトコルを使用した物理接続を通して送信されてもよい。このルータ６０６は、さらなる処理のために認証サービス６０８にこれらのデータパケットを伝送するように構成されてもよい。

【００５３】

上述されたように、認証サービス６０８は、予想カスタマデジタル署名を作成するために必要な１つ又は複数の暗号キーを入手するためにアカウントサービス６１０と対話するように構成されてもよい。したがって、認証サービス６０８は、この予想カスタマデジタル署名を作成するために暗号キー及び受信されたカスタマデータをハッシュするように構成されてもよい。この署名と、受信されたカスタマデジタル署名とが比較され、一致するかどうかを判定してもよい。一致する場合、カスタマ送信は本物と見なされ、これにより認証サービス６０８は、コンピューティングリソースサービスプロバイダ６０４によって提供される１つ又は複数のサービス６１２への継続的なアクセスを可能とさせてよい。ただし、一致しない場合、認証サービス６０８は、上記に示されるように、既存の接続を制限するか、または終了さえするために１つ又は複数のアクションを実行してよい。

【００５４】
さらに、デジタル署名が一致する場合、認証サービス６０８は、カスタマルータ６０２に送信されてよいコンピューティングリソースサービスプロバイダ６０４のデジタル署名を含んだ１つ又は複数のデータパケットを生成してよい。これによって、カスタマが、現在の直接的な接続を継続するためにコンピューティングリソースサービスプロバイダ６０４のアイデンティティを検証できるようにしてよい。
【００５５】
上述されたように、直接的な接続は、カスタマがコンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスにアクセスできるようにするために、カスタマルータとコンピューティングリソースサービスプロバイダとの間に確立されてよい。したがって、図７は、少なくとも一実施形態に従ってカスタマとコンピューティングリソースサービスプロバイダとの間で物理接続を確立するためのプロセス７００の実施例を例示するものである。プロセス７００は、コンピューティングリソースサービスプロバイダ（例えば、認証サービス及びアカウントサービス）によって保持され、運用される１つ又は複数のサービスだけではなく、コンピューティングリソースサービスプロバイダによって運用されるさまざまなネットワーキング構成要素及びコンピューティング構成要素によって実行されてもよい。
【００５６】
カスタマは、カスタマルータとコンピューティングリソースサービスプロバイダとの間での直接的な物理接続の構築を要求するためにコンピューティングリソースサービスプロバイダに接触することができる。例えば、カスタマは、カスタマコンピューティングシステムとコンピューティングリソースサービスプロバイダのコンピューティングシステムとの間に専用のネットワーク接続を確立することを所望することがある。これによって、カスタマが自分の営業活動をサポートするためにコンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスにアクセスできるようにする。したがって、プロセス７００は、この直接的な接続を確立するためにカスタマからの要求をコンピューティングリソースサービスプロバイダが受信する７０２ことを含んでよい。
【００５７】
コンピューティングリソースサービスプロバイダはいったんカスタマから要求を受信すると、コンピューティングリソースサービスプロバイダは、コンピューティングリソースサービスプロバイダルータにカスタマルータを接続するために授権書を作成してよい７０４。図２に示されるように、カスタマルータ及びコンピューティングリソースサービスプロバイダルータはデータセンタ又はコロケーションセンタに設置してよい。このようにして、授権書はデータ技術者（例えば、コンピューティングリソースサービスプロバイダの従業員、カスタマ、又は契約第三者）にカスタマルータとコンピューティングリソースサービスプロバイダルータとの間に接続を確立する許可を与えてよい。
【００５８】
データ技術者は物理的なルータを接続する７０６ために１本又は複数のケーブルを使用してよい。これは、カスタマ及びコロケーションセンタ内のコンピューティングリソースサービスプロバイダルータ、及び、接続を確立するために必要とされる対応するポートを識別することを伴ってもよい。例えば、データ技術者は、カスタマルータの送受信ポートにケーブル（例えば、光ファイバ、銅、又は他の物質）一式の一方の端部を挿入し、コンピューティングリソースサービスプロバイダの送受信ポートに該ケーブルの他方の端部を接続してよい。コロケーションセンタが１つ又は複数のパッチパネルを含む場合、データ技術者はパッチパネルを通してカスタマルータから、及び最終的なパッチパネルポートからコンピューティングリソースサービスプロバイダルータにケーブルを接続してよい。データ技術者は、適正な接続性を保証するために診断ツールを使用するか、又はコンピューティングリソースサービスプロバイダに接触して、接続が確立されたことをコンピューティングリソースサービスプロバイダに知らせてもよい。
【００５９】

認証プロセスはポートと無関係であってよいことが留意されるべきである。例えば、実施形態では、カスタマは、そのカスタマのルータ、及び二次カスタマ又は三次カスタマ（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との既存の関係性を有するカスタマのカスタマ）によって保持され且つ運用されるルータを含むコロケーションセンタ内でケージを運用し、保持する。任意の時点で、カスタマは、カスタマルータとコンピューティングリソースサービスプロバイダとの間で物理接続を切断し、二次カスタマ又は三次カスタマによって維持されるルータとの物理接続を再接続してよい。二次カスタマ又は三次カスタマは、二次カスタマ又は三次カスタマと関連付けられ、コンピューティングリソースサービスプロバイダに認証証拠を提供するために使用されることが可能なクレデンシャルのセットを保持してよい。したがって、コンピューティングリソースサービスプロバイダは、適宜この物理接続を通してこの二次カスタマ又は三次カスタマとの物理接続を認証してよい。二次カスタマ又は三次カスタマは、それに応じて、以下に説明されるように、接続を認証するためにコンピューティングリソースサービスプロバイダに認証証拠を提供してよい。

【００６０】

多様な実施形態で、カスタマ及び／又はプロバイダは直接的な物理接続を確立するために使用されるネットワークデバイスポートを変更してよい。例えば、カスタマは、カスタマルータとコンピューティングリソースサービスプロバイダとの間で異なった接続を生じさせる、既存の物理接続のアップグレード（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ルータでの１ギガバイトポートから１０ギガバイトポートへの遷移）を要求してもよい。この例では、認証プロセスは、プロセスに対するいかなるシステム変更もなしに、いったん接続が確立されると繰り返されてもよい。これによって、認証プロセスがポートに無関係であることを保証することができる。

【００６１】

いったんコロケーションセンタでの物理的なルータが接続され、データ技術者によって接続が確認されると、コンピューティングリソースサービスプロバイダはルータを使用してカスタマルータに１つ又は複数の信号を送信７０８してよい。図５に関連して上記に示されたように、コンピューティングリソースサービスプロバイダは認証サービスを運用し、保持してもよく、この認証サービスは、カスタマがコンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスに接続する権限を与えられていることを検証するためにカスタマに認証要求を送信するように構成されてもよい。したがって、認証サービスはこの認証要求を含んだセキュリティプロトコルに従う１つ又は複数のデータパケットを生成するように構成されてもよい。これらのデータパケットは、コロケーションセンタで確立された物理接続を介してカスタマルータにコンピューティングリソースサービスプロバイダによって送信されてもよい。

【００６２】

カスタマルータがコンピューティングリソースサービスプロバイダからこれらの１つ又は複数のデータパケットを受信すると、カスタマルータは処理のためにカスタマコンピューティングシステムにこれらのデータパケットを送信してよい。認証要求に基づいて、カスタマコンピュータシステムはデジタル署名を生成するためにハッシュ関数及び暗号キーを活用するように構成されてもよい。デジタル署名は認証要求を満たすために必要な認証証拠を含んでよい。したがって、カスタマコンピュータシステムは、他のカスタマデータとともに要求を満たすために必要とされる認証証拠を含んだ１つ又は複数のデータパケットを生成するように構成されてもよい。これらのデータパケットは、認証情報の送信のために確立されたセキュリティプロトコルに従って作成されてよい。

【００６３】

カスタマ認証証拠を含んだデータパケットは、カスタマルータを使用して物理接続を通してコンピューティングリソースサービスプロバイダに送信されてもよい。したがって、コンピューティングリソースサービスプロバイダは、カスタマルータからカスタマデータパケットを含んだ信号を受信してよい７１０。カスタマルータを起源とする信号は、カス

タマからの信号を分解し、１つ又は複数のデータパケットを抽出するように構成してよいコンピューティングリソースサービスプロバイダルータによって受信されてもよい。認証サービスにアドレス指定可能なデータパケットは、処理のために認証サービスに送信されてもよい。

【００６４】

上述されたように、認証サービスはカスタマのアイデンティティを検証するために受信されたデータパケットからカスタマ認証証拠（例えば、デジタル署名）を抽出するように構成されてもよい。したがって、認証サービスは物理接続を通して受信されるデジタル署名を認証する７１２ことを試みてよい。上述されたように、認証サービスは関連するカスタマ情報を入手するためにアカウントサービスと対話するように構成されてもよい。例えば、認証サービスは、認証証拠を検証するためにアカウントサービスから１つ又は複数のカスタマ暗号キー（例えば、楕円曲線暗号法等の１つ又は複数の暗号方法を使用して生成されるカスタマキー）を入手してよい。例えば、認証サービスは、予想カスタマデジタル署名を作成するために、暗号キーとともに、受信されたカスタマデータをハッシュするように構成されてもよい。この予想カスタマデジタル署名がカスタマからの受信されたデジタル署名に一致する場合、信号は本物であり、カスタマアイデンティティは検証される。

【００６５】

カスタマによって提供される認証証拠が適切である（例えば、デジタル署名の一致が生じる）場合、認証サービスは、コンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスへのカスタマのアクセスを可能とする７１４ようにしてもよい。１つ又は複数のサービスに対するカスタマアクセスを可能にするために、認証サービスは、１つ又は複数の実行可能命令をコンピューティングリソースサービスプロバイダルータに送信して、カスタマが１つ又は複数のサービスにアクセスするために１つ又は複数の信号を送信できるようにルータを再構成するように構成されてもよい。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ルータは、１つ又は複数のサービスの受取人ＩＰアドレスを含んだいずれのデータパケットも１つ又は複数のサービスに配信できるように構成されてもよい。さらに、認証は、これらのサービスにアクセスするために使用されてよいバーチャルインタフェースをカスタマが設定できるようにするために、コンピューティングリソースサービスプロバイダルータに１つ又は複数の実行可能命令を送信するように構成されてもよい。このようにして、カスタマは、コンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスにアクセスできるようにしてよい。

【００６６】

上述されたように、認証サービスは、カスタマが、カスタマとコンピューティングリソースサービスプロバイダとの間の物理接続が確立された後にコンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスにアクセスする権限を有することを検証するように構成されてもよい。したがって、図８は、少なくとも一実施形態に従って初めて接続を認証するためのプロセス８００の実施例を例示する。上述されたように、コンピューティングリソースサービスプロバイダ及びカスタマはコロケーションセンタに設置するルータを使用することによって物理接続を確立してよい。いったん物理接続が確立されると、権限のない第三者が接続に干渉するかもしれいない（例えば、カスタマになりすまし、カスタマ情報にアクセスしようとする）というリスクがある。したがって、コンピューティングリソースサービスプロバイダは、カスタマが要求されたサービスにアクセスする権限を有することを検証するためにカスタマに認証要求を送信する８０２ように構成されてもよい認証サービスを含んでよい。

【００６７】

上述されたように、認証サービスは、物理接続を通して送信可能な認証要求を含んだ１つ又は複数のデータパケットを生成するように構成されてもよい。これらのデータパケットは、データパケットがカスタマコンピュータシステムによって処理され、送信が安全であるように、他の標準的なプロトコル（例えば、ＴＣＰ／ＩＰ、ＩＰｓｅｃ等）に加えて

セキュリティプロトコルに従ってさらに構成されてよい。したがって、認証サービスはこれらのデータパケットをコンピューティングリソースサービスプロバイダルータに送信し、同様にコンピューティングリソースサービスプロバイダルーがカスタマに当該データパケットを送信するように構成されてもよい。

【００６８】

カスタマは、コロケーションセンタのコンピューティングリソースサービスプロバイダに物理的に接続可能なカスタマルータを通してこれらのデータパケットを受信してよい。したがって、データパケットは処理のために１つ又は複数のカスタマコンピュータシステムに送信されてもよく、これによって１つ又は複数のコンピュータシステムは、カスタマがコンピューティングリソースサービスプロバイダによって提供されるサービスにアクセスする権限を有することを検証するために必要な認証証拠を含んだ要求に応えて１つ又は複数のデータパケットを生成してよい。認証サービスを使用して生成されるデータパケットの場合と同様に、１つ又は複数のカスタマコンピュータシステムは他の標準的なプロトコルに加えてセキュリティプロトコルに従って構成される１つ又は複数のデータパケットを生成するように構成されてもよい。したがって、これらのデータパケットは処理のためにカスタマルータからコンピューティングリソースサービスプロバイダに送信されてもよい。コンピューティングリソースサービスプロバイダは、カスタマから受信された１つ又は複数のデータパケットを認証サービスに送信してよい。

【００６９】

したがって、認証サービスは、カスタマから認証証拠を受信する８０４ように構成されてもよい。要求された認証証拠のタイプに基づいて、認証サービスは認証証拠を検証するために必要なカスタマアカウント情報を入手するためにアカウントサービスと対話するように構成されてもよい。例えば、認証サービスは、カスタマから受信されたデジタル署名が本物であるかどうかを判断するために使用されてもよい予想カスタマデジタル署名を生成するために、カスタマアカウントと関連付けられた暗号キーを入手してよい。

【００７０】

したがって、認証サービスは、暗号キーを使用して予想カスタマデジタル署名を作成し、これとカスタマから受信されたデジタル署名とを比較することで、これらが一致するかどうかを判断するように構成されてもよい。したがって、認証サービスは、カスタマ認証証拠が本物であるかどうかを判断する８０６ように構成されてもよい。カスタマから受信された認証証拠が認証サービスによって作成される予想カスタマデジタル署名に一致する場合、認証サービスはコンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスへの接続を確立してよい８０８。例えば、認証サービスは、コンピューティングリソースサービスプロバイダルータに１つ又は複数の実行可能命令を送信して、コンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスにアドレス指定されるカスタマから受信されたいずれのデータパケットも当該１つ又は複数のサービスに当該ルータにより送信されるように構成されてもよい。したがって、カスタマはそのビジネスをサポートするためにこれらのサービスにアクセスすることができるようになる。

【００７１】

しかしながら、カスタマから受信される認証証拠が認証サービスによって生成される予想カスタマデジタル署名に一致しない場合、認証サービスはコンピューティングリソースサービスプロバイダによって提供されるサービスへのカスタマのアクセスを拒否してよい８１０。例えば、認証サービスはコンピューティングリソースサービスプロバイダルータに１つ又は複数の実行可能なコマンドを送信して、ルータに、これらの１つ又は複数のサービスにアドレス指定されてよいカスタマからのいずれのデータパケットも当該ルータにより拒絶させるように構成されてもよい。あるいは、初期の物理接続中のコンピューティングリソースサービスプロバイダルータが１つ又は複数のサービスにアドレス指定されたいずれのデータパケットも自動的に拒絶するように構成されている場合、認証サービスは当該ルータにいずれの追加命令も送信しないことがある。したがって、ルータはカスタマ

からのこれらのデータパケットを拒絶し続けてよい。

【００７２】

いったんカスタマが１つ又は複数のサービスに無事に接続されると、カスタマはそのビジネスをサポートするためにこれらのサービスを活用し続けてよい。ただし、認証サービスは、接続が不正接続されていないことを保証するためにカスタマに認証要求を提示し続けるように構成されてもよい。したがって、図９は、接続が少なくとも一実施形態に従ってあらかじめ確立された後の接続を認証するためのプロセス９００の実施例を例示するものである。図８に示されるプロセスにおけるように、認証サービスはカスタマに認証要求を送信する９０２ように構成されてもよい。この認証要求は、１つ又は複数の通信プロトコル（例えば、ＴＣＰ／ＩＰ）、及び物理接続のセキュリティに必要なセキュリティプロトコルに従って構成された１つ又は複数のデータパケットで送信されてもよい。

【００７３】

上述されたように、カスタマはカスタマのさらなる営業活動に適するように構成された１つ又は複数のコンピュータシステムを運用してよい。したがって、これらの１つ又は複数のコンピュータシステムは認証要求を処理し、要求を満たすために必要な認証証拠を含んだ１つ又は複数のデータパケットを生成するように構成されてもよい。認証証拠は、上述されたように、１つ又は複数のカスタマクレデンシャル（例えば、パスワード、デジタル署名等）を含んでよい。認証要求を含んだデータパケットにおけるように、カスタマコンピューティングシステムを使用して生成されたデータパケットは１つ又は複数の通信プロトコル及びセキュリティプロトコルに適するように構成されてもよい。これらのデータパケットは、（例えば、コロケーションセンタの物理ケーブルを通して）直接的にコンピューティングリソースサービスプロバイダルータに接続されてよいカスタマルータを使用して配信されてもよい。

【００７４】

コンピューティングリソースサービスプロバイダルータは、このようにして認証証拠を含んだデータパケットを受信し９０４、コンピューティングリソースサービスプロバイダによって運用される認証サービスにこれらのデータパケットを送信するように構成されてもよい。したがって、認証サービスは、認証証拠を検証するために必要な情報を入手するためにコンピューティングリソースサービスプロバイダによって運用されるアカウントサービスと対話するように構成されてもよい。これによって、認証サービスが、カスタマ認証証拠が本物であるかどうかを判断する９０６ことができるようにしてもよい。例えば、認証サービスはカスタマから受信されたデジタル署名を検証するために使用されてよい予想カスタマデジタル署名を作成するために必要な１つ又は複数の暗号キーを入手してよい。

【００７５】

認証証拠が認証要求を満たす（例えば、提供されたカスタマデジタル署名が認証サービスによって作成された予想カスタマデジタル署名に適合する）場合、認証サービスは、カスタマが現在、コンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスにアクセスしているかどうかをさらに判断してよい９０８。コンピューティングリソースサービスプロバイダがカスタマとこれらのサービスとの間ですでに接続を確立している場合、認証サービスは、カスタマがこれらのサービスにアクセスできることが継続するように構成されてもよい。したがって、認証サービスは、接続が不正接続されていないことを保証するために別の認証要求をカスタマに送信する９０２ように構成されてもよい。これらの以後の要求は、認証サービスの構成に少なくとも部分的に基づいて後に行われてよい。

【００７６】

ただし、カスタマが現在コンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスにアクセスしていない場合、認証サービスはカスタマとこれらのサービスとの間に接続を確立してよい９１０。例えば、認証サービスは、１つ又は複数の実行可能命令をコンピューティングリソースサービスプロバイダルータに送信し、

カスタマコンピュータシステムを起源とするいずれのデータパケットも１つ又は複数のサービスに送信することを当該ルータに許可させるように構成されてもよい。これにより、カスタマは直ちに自らのビジネスを促進するためにこれらのサービスにアクセスすることができる。再び、いったん接続が確立されると、認証サービスは、接続が不正接続されていないことを保証するためにカスタマに認証要求を送信し続けてよい９０２。これらの以後の要求は、認証サービスの構成に応じて日次、週次、月次、又はさまざまな時間間隔で行われてよい。

【００７７】

認証サービスがカスタマからの受信された認証証拠を評価し、証拠が本物ではないと判断する場合、認証サービスは、コンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスへのカスタマのアクセスを制限するかどうかをさらに判断してよい９１２。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は、カスタマが、接続が不正接続されている場合にどのような対策が講じられ得るのかを定めることができるようにしてよい。例えば、カスタマは、潜在的な違反に基づいて接続が終了されるべきであることを指定してよい。別の例では、カスタマは、自称カスタマ（例えば、権限のない第三者等）とコンピューティングリソースサービスプロバイダとの間のすべての送信を記録する一方で、接続が中断されることなく続行できるようにすることを好むことがある。

【００７８】

したがって、認証サービスは、違反があった場合にカスタマの命令を参照し、これらの対策を実行するためにアカウントサービスと対話するように構成されてもよい。あるいは、カスタマが、講じられる対策を指定していない場合、認証サービスは１つ又は複数のデフォルト指示を参照して、接続に関して１つ又は複数の対策をサービスに実行させてもよい。カスタマの指示又はデフォルト指示が１つ又は複数のサービスへのアクセス制限を含む場合は、認証サービスはこれらのサービスへのカスタマのアクセスを制限する９１４方向へ進んでよい。例えば、認証サービスはコンピューティングリソースサービスプロバイダに１つ又は複数の実行可能命令を送信して、カスタマが利用できる利用可能な接続帯域幅を狭め、これによりカスタマがサービスにアクセスする能力を遅くするように構成されてもよい。あるいは、接続を完全に終了してもよい。サービスへのアクセスを制限するための他の方法が、さらに組み込まれてもよく、これらは本開示の範囲内であると見なせる。

【００７９】

カスタマとコンピューティングリソースサービスプロバイダとの間の接続がいったん制限されると、認証サービスはカスタマへ認証要求を送信し続けてよい９０２。したがって、カスタマが新しい認証要求に応えて適切な認証証拠を提供できる場合、認証サービスは１つ又は複数のサービスへのアクセスを復元するためにコンピューティングリソースサービスプロバイダルータに１つ又は複数の実行可能命令を送信してよい。このようにして、カスタマ及びコンピューティングリソースサービスプロバイダは接続に関わる問題を、それが権限のない第三者であれ、クレデンシャルの期限切れ又は何らかの他の問題であれ、解決し、接続を復元することができる。

【００８０】

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が、認証証拠が不適切である場合にいずれのアクションも講じるべきではないとカスタマが指定していた場合、コンピューティングリソースサービスプロバイダは接続が拘束されずに継続できるようにしてよい。したがって、認証サービスは、接続に関して問題が依然として残っているかどうかを判断するために認証要求を送信する９０２ことを続行するように構成されてもよい。例えば、認証サービスは、多数の認証要求でもなんら適切な認証証拠応答を生じさせなかった後には接続を終了するように構成されてもよい。

【００８１】

上述されたように、いったんカスタマルータとコンピューティングリソースサービスプ

ロバイダルータとの間の物理接続が確立されると、コンピューティングリソースサービスプロバイダは、カスタマのアイデンティティを検証し、接続が不正接続されていないことを保証するためにカスタマに１つ又は複数の認証要求を送信してよい。同様に、カスタマは、自分のビジネスをサポートするために使用可能な１つ又は複数のコンピューティングシステムを活用して、プロバイダのアイデンティティを検証するためにコンピューティングリソースサービスプロバイダに１つ又は複数の認証要求を送信してよい。したがって、図１０は、少なくとも一実施形態に従って接続を認証するためのプロセス１０００の実施例を例示するものである。

【００８２】

カスタマは、１つ又は複数のサービスに潜在的に影響を受けやすいカスタマデータを送信する前に、接続の他端で関係者のアイデンティティを検証することを所望することがある。したがって、カスタマはコンピューティングリソースサービスプロバイダに認証要求を送信する１００２ために１つ又は複数のコンピュータシステムを構成してもよい。上述されたように、カスタマコンピューティングシステムは、１つ又は複数の通信プロトコル、及び安全な接続を通してこれらのデータパケットを送信するために必要なセキュリティプロトコルに従って構成された１つ又は複数のデータパケットを生成するように構成されてもよい。これらのデータパケットは認証要求及びカスタマ識別データを含んでよい。したがって、カスタマコンピュータシステムはこれらのデータパケットを、これらのデータパケットを物理接続の他端のコンピューティングリソースサービスプロバイダに送信するように構成されてよいカスタマルータに伝送してよい。

【００８３】

したがって、認証要求は、処理のためにコンピューティングリソースサービスプロバイダによって運用される認証サービスに配信されてよい。認証サービスは、カスタマアカウントにアクセスし、要求を満たすために必要な情報を見つけ出すためにアカウントサービスと対話するように構成されてもよい。例えば、認証サービスは、認証証拠として使用され得るデジタル署名を作成するためにカスタマアカウントから暗号キーを入手してよい。認証サービスは、要求を満たし、コンピューティングリソースサービスプロバイダルータを通して１つ又は複数のカスタマコンピューティングシステムにこれらのデータパケットを送信するために必要な情報を含んだ１つ又は複数のデータパケットを生成するように構成されてもよい。このようにして、１つ又は複数のカスタマコンピュータシステムは、コンピューティングリソースサービスプロバイダから認証証拠を受信してよい１００４。

【００８４】

いったんカスタマコンピューティングシステムがコンピューティングリソースサービスプロバイダから認証証拠を入手すると、カスタマコンピューティングシステムは、証拠が本物であるかどうかを判断する１００６ために認証証拠を処理してよい。証拠が本当に本物であるかどうか判断するために、カスタマコンピューティングシステムは暗号キーを使用して予想認証サービスデジタル署名を作成し、このデジタル署名を認証サービスから受信されたデジタル署名と比較するように構成されてもよい。したがって、カスタマコンピュータシステムは予想コンピューティングリソースサービスプロバイダクレデンシャル（例えば、暗号キー、予想デジタル署名等）を設置又は生成し、これらのクレデンシャルを提供された証拠と比較してよい。受信された認証証拠が予想コンピューティングリソースサービスプロバイダクレデンシャルと一致しない場合、カスタマコンピュータシステムは接続を終了する１００８ために、再構成情報（例えば、実行可能命令）をカスタマルータに送信してよい。したがって、カスタマが潜在的な問題に対応できるようにする追加の送信は、コンピューティングリソースサービスプロバイダから受信されないことがある。

【００８５】

コンピューティングリソースサービスプロバイダから受信された認証証拠が有効である（例えば、予想認証サービスデジタル署名が受信されたデジタル署名に一致する）場合、カスタマは、さらなる送信を行うことを可能にし、コンピューティングリソースサービスプロバイダによって提供される１つ又は複数のサービスにアクセスし続けてよい。さらに

、カスタマコンピュータシステムは、接続が不正接続されていないことを保証するためにコンピューティングリソースサービスプロバイダに１つ又は複数の認証要求を送信１００２し続けるように構成されてもよい。

【００８６】

本開示の実施形態は、以下の節を鑑みて説明できる。

１．接続を認証するためのコンピュータ実装方法であって、

実行可能命令で構成された１つ又は複数のシステムの制御下で、

コンピューティングリソースサービスプロバイダネットワークデバイスで、及び安全な接続を通してコンピューティングリソースサービスプロバイダと接続されたカスタマデバイスから、カスタマの秘密キーに少なくとも部分的に基づいて生成される暗号認証情報を受信することと、

コンピューティングリソースサービスプロバイダネットワークデバイスから、暗号認証情報を認証するために運用可能である認証サービスに暗号認証情報を転送することと、

認証サービスが暗号認証情報を無事に認証した結果として、カスタマデバイスから認証サービスとは異なるコンピューティングリソースサービスプロバイダの１つ又は複数のサービスにネットワークトラフィックを送るようにコンピューティングリソースサービスプロバイダネットワークデバイスを構成することと

を含む、コンピュータ実装方法。

２．秘密キーが公開‐秘密暗号キー組からの秘密キーである、節１に記載のコンピュータ実装方法。

３．認証サービスが暗号認証情報を無事に認証した結果として、コンピューティングリソースサービスプロバイダネットワークデバイス上でカスタマのためにネットワークインタフェースを設定することをさらに含む、節１から２までのいずれか１節に記載のコンピュータ実装方法。

４．安全な接続が、コロケーションセンタでの物理接続に少なくとも部分的に基づいて確立され、物理接続が、カスタマポートのセットからコンピューティングリソースサービスプロバイダポートのセットに接続される１本又は複数のケーブルを含む、上記節のいずれか１節に記載のコンピュータ実装方法。

５．ある量の時間にわたって１回又は複数回、カスタマデバイスから追加の暗号認証情報を受信すること

をさらに含み、

カスタマデバイスから１つ又は複数のサービスへのネットワークトラフィックを継続的に送ることが、追加の暗号認証情報を無事に認証することを条件とする、上記節のいずれか１節に記載のコンピュータ実装方法。

６．安全な接続は公衆通信ネットワーク上での安全なトンネルを含む、上記節のいずれか１節に記載のコンピュータ実装方法。

７．該方法が、カスタマデバイス及びコンピューティングリソースサービスプロバイダネットワークデバイスによって使用される認証プロトコルに従って実行される、上記節のいずれか１節に記載のコンピュータ実装方法。

８．コンピューティングリソースサービスプロバイダネットワークデバイスを欠いている通信チャネルを通してカスタマの秘密キーを受信することをさらに含む、上記節のいずれか１節に記載のコンピュータ実装方法。

９．ネットワークデバイスであって、

認証サービスを含む１つ又は複数のサービスを含むプロバイダネットワークに接続される通信ポートを含む、ネットワークデバイスの外部から１つ又は複数の信号を受信するように構成される１つ又は複数の通信ポートと、

１つ又は複数の通信ポートと動作可能に結合される１台又は複数のプロセッサと

１台又は複数のプロセッサによって実行可能な命令を含むメモリであって、該１台又は複数のプロセッサによって実行されるときに、該１台又は複数のプロセッサに、

１つ又は複数の通信ポートに接続されたカスタマデバイスから、暗号認証情報を認証

するために運用可能である認証サービスへの接続を通して受信される暗号認証情報を転送させ、
　認証サービスが暗号情報を無事に認証した結果として認証サービスから再構成情報を受信して、ネットワークデバイスがカスタマデバイスからコンピューティングリソースサービスプロバイダの１つ又は複数のサービスにデータを転送できるようにさせ、
　再構成情報に従ってカスタマデバイスからコンピューティングリソースサービスプロバイダの１つ又は複数のサービスにデータを転送するように再構成させる、
　前記メモリと、
を含む、ネットワークデバイス。
　１０．カスタマデバイスから受信される暗号認証情報が、カスタマの秘密キーに少なくとも部分的に基づいて生成される、節９に記載のネットワークデバイス。
　１１．秘密キーが公開‐秘密暗号キーの組からの秘密キーである、節９から１０までに記載のネットワークデバイス。
　１２．接続は公衆通信ネットワーク上の安全なトンネルである、節９から１１までのネットワークデバイス。
　１３．命令によって、１台又は複数のプロセッサに、カスタマデバイスによって検証可能である暗号認証情報を認証サービスからカスタマデバイスにさらに送信させる、節９から１２のネットワークデバイス。
　１４．命令によって、１台又は複数のプロセッサに、カスタマデバイスから受信された追加の暗号認証情報を経時的に１回又は複数回、認証サービスにさらに転送させる、節９から１３までに記載のネットワークデバイス。
　１５．信号がカスタマデバイスから１つ又は複数の通信ポートに接続された１本又は複数の光ファイバケーブルを通して受信される、節９から１４までに記載のネットワークデバイス。
　１６．命令によって、１台又は複数のプロセッサに、再構成情報に少なくとも部分的に基づいて、カスタマデバイスからデータを処理するためのネットワークインタフェースをさらに設定させる、節９から１５までに記載のネットワークデバイス。
　１７．認証サービスの１台又は複数のプロセッサによって実行されるときに、認証サービスに、
　カスタマの秘密キーに少なくとも部分的に基づいて生成され、コンピューティングリソースサービスプロバイダネットワークデバイスとの安全な接続を通してカスタマから受信された暗号認証情報が本物であるかどうかの判断を下させ、
　判断に少なくとも部分的に基づいて１つ又は複数の対策を講じさせる
　命令を集合的に記憶させた１つ又は複数の非一時的コンピュータ可読記憶媒体であって、
　判断が、暗号認証情報が本物であることを示す場合、１つ又は複数の対策が再構成情報をコンピューティングリソースサービスプロバイダネットワークデバイスに送信し、それによりコンピューティングリソースサービスプロバイダネットワークデバイスに、カスタマデバイスからコンピューティングリソースサービスプロバイダの１つ又は複数の他のサービスにネットワークトラフィックを送らせることを含み、
　判断が、暗号認証情報が本物ではないことを示す場合、１つ又は複数の対策がコンピューティングリソースサービスプロバイダネットワークデバイスに、カスタマデバイスからコンピューティングリソースサービスプロバイダの１つ又は複数の他のサービスへのネットワークトラフィックを拒否させることを含む、
　１つ又は複数の非一時的コンピュータ可読記憶媒体。
　１８．コンピューティングリソースサービスプロバイダにネットワークトラフィックを拒否させることは、カスタマデバイスからコンピューティングリソースサービスプロバイダの１つ又は複数の他のサービスへのネットワークトラフィックを拒否するための再構成情報を、コンピューティングリソースサービスプロバイダネットワークデバイスに送信することを含む、節１７に記載の１つ又は複数の非一時的コンピュータ可読記憶媒体。

１９．秘密キーが公開‐秘密暗号キーの組からの秘密キーである、節１７から１８までに記載の１つ又は複数の非一時的コンピュータ可読記憶媒体。

２０．１つ又は複数の対策が、判断が、暗号認証情報が本物であることを示した結果として、コンピューティングリソースサービスプロバイダネットワークデバイス上でカスタマのためにネットワークインタフェースを設定することをさらに含む、節１７から１９までの１つ又は複数の非一時的コンピュータ可読記憶媒体。

２１．安全な接続がコロケーションセンタでの物理接続に少なくとも部分的に基づいて確立され、物理接続がカスタマポートのセットからコンピューティングリソースサービスプロバイダポートのセットに接続される１本又は複数のケーブルを含む、節１から１７までに記載の１つ又は複数の非一時的コンピュータ可読記憶媒体。

２２．安全な接続は公衆通信ネットワーク上で安全なトンネルを含む、節１７から２１までに記載の１つ又は複数の非一時的コンピュータ可読記憶媒体。

２３．暗号認証情報が、カスタマ及びコンピューティングリソースサービスプロバイダネットワークデバイスによって使用される認証プロトコルに従って安全な接続を通して送信される、節１７から２２までに記載の１つ又は複数の非一時的コンピュータ可読記憶媒体。

２４．命令によって、認証サービスに、カスタマによって検証可能な第２の暗号情報をさらに生成させ、コンピューティングリソースサービスプロバイダネットワークデバイスを通してカスタマに暗号認証情報を送信させる、節１７から２３までに記載の１つ又は複数の非一時的コンピュータ可読記憶媒体。

２５．命令によって、認証サービスに、継時的に１回又は複数回カスタマから受信される追加の暗号認証情報に少なくとも部分的に基づいて追加の判断をさらに下させる、節１７から２４までに記載の１つ又は複数の非一時的コンピュータ可読記憶媒体。

【００８７】

図１１は、多様な実施形態に従って態様を実装するための環境例１１００の態様を示す。理解されるように、ウェブに基づいた環境が説明のために使用されるが、多様な実施形態を実装するためには必要に応じて異なる環境が使用されてよい。環境は、適切なネットワーク１１０４上で要求、メッセージ、又は情報を送信及び受信し、装置のユーザに情報を伝え返すために運用可能な任意の適切なデバイスを含むことができる電子クライアントデバイス１１０２を含む。係るクライアントデバイスの例は、パーソナルコンピュータ、携帯電話、ハンドヘルドメッセージングデバイス、ラップトップコンピュータ、タブレットコンピュータ、セットトップボックス、パーソナルデータアシスタント、埋込式コンピュータシステム、電子ブックリーダー等を含む。ネットワークは、イントラネット、インターネット、セルラーネットワーク、ローカルエリアネットワーク、もしくは任意の他のこのようなネットワーク、又はそれらの組合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。係るシステムに使用される構成要素は、選択されたネットワーク及び／又は環境のタイプに少なくとも部分的に依存することができる。係るネットワークを介して通信するためのプロトコル及び構成要素は周知であり、本明細書に詳細に説明されない。ネットワーク上での通信は有線接続又は無線接続及びそれらの組合せによって行うことができる。この実施例では、要求を受信し、要求に応えてコンテンツを供給するためのウェブサーバ１１０６を環境が含むので、ネットワークはインターネットを含む。ただし、他のネットワークの場合、当業者に明らかになるように、類似する目的に役立つ代替デバイスが使用できるだろう。

【００８８】

例示的な環境は少なくとも１台のアプリケーションサーバ１１０８及びデータストア１１１０を含む。連結されているか、又はそれ以外の場合構成されてもよい、適切なデータストアからデータを入手する等のタスクを実行するために対話は可能な、いくつかのアプリケーションサーバ、層、又は他の要素、プロセスもしくは構成要素がある場合があることは理解されるべきである。サーバは、本明細書に使用されるように、ハードウェアデバイス又はバーチャルコンピュータシステム等の多様な方法で実装されてよい。いくつかの

状況では、サーバはコンピュータシステムで実行されているプログラマブルモジュールを指す場合がある。本明細書に使用されるように、用語「データストア」は、データを記憶し、アクセスし、取り出すことができる任意のデバイス又はデバイスの組合せを指すが、これらは、任意の標準的な環境、分散環境又はクラスタ環境でデータサーバ、データベース、データストレージデバイス、及びデータストレージ媒体の任意の組合せ及び数を含んでもよい。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に１つ又は複数のアプリケーションの態様を実行するために必要に応じてデータストアと統合し、データアクセス及びアプリケーションのためのビジネス論理のいくらか（大多数も）処理するための任意の適切なハードウェア及びソフトウェアを含むことができる。アプリケーションサーバはデータストアと協調してアクセス制御サービスを提供してよく、この例ではハイパーテキストマークアップ言語（「ＨＴＭＬ」）、拡張マークアップ言語（「ＸＭＬ」）、又は別の適切な構造化言語の形をとるウェブサーバによってユーザに提供されてよい、ユーザに伝送されるテキスト、グラフィック、音声、及び／又はビデオ等のコンテンツを生成できる。クライアントデバイス１１０２とアプリケーションサーバ１１０８との間でのコンテンツの配信だけではなく、すべての要求及び応答の処理もウェブサーバによって対処できる。本明細書で説明される構造化コードは本明細書の他の箇所に説明されるように任意の適切なデバイス又はホストマシン上で実行できるので、ウェブサーバ及びアプリケーションサーバが必須ではなく、単に構成要素例にすぎないことは理解されるべきである。さらに、単一のデバイスによって実行されるとして本明細書に説明される運用は、文脈から明確にならない限り、分散システムを形成してよい複数のデバイスによって集合的に実行されてよい。

【００８９】

データストア１１１０は、いくつかの別個のデータテーブル、データベース、又は本開示の特定の態様に関係するデータを記憶するための他のデータストレージ機構及びデータストレージ媒体を含むことができる。例えば、示されているデータストアは、生産側のためのコンテンツを供給するために使用できる生産データ１１１２及びユーザ情報１１１６を記憶するための機構を含んでよい。また、データストアは、報告、分析、又は他の係る目的のために使用できるログデータ１１１４を記憶するための機構を含むとして示されている。データストアに記憶されることを要求されるであろう多くの他の態様、例えば、ページ画像情報及びアクセス権情報等があり得ることは理解されるべきである。これらは、必要に応じて上記に挙げられた機構のいずれかに又はデータストア１１１０の追加機構に記憶できる。データストア１１１０は、データストアと関連付けられた論理を通して、アプリケーションサーバ１１０８から命令を受信し、命令に応えてデータを入手、更新、又はそれ以外の場合処理するために運用可能である。一例では、ユーザは、ユーザによって運用されるデバイスを通して、特定のタイプの項目に対する検索要求を提示する場合もある。この場合、データストアはユーザのアイデンティティを検証するためにユーザ情報にアクセスする可能性があり、そのタイプの項目についての情報を入手するためにカタログ詳細情報にアクセスできる。情報は、次いでユーザがユーザデバイス１１０２上のブラウザを介して閲覧することができるウェブページ上のリスト結果等で、ユーザに返されることがある。関心のある特定の項目のための情報は、ブラウザの専用のページ又はウィンドウで閲覧できる。ただし、本開示の実施形態は必ずしもウェブページの状況に制限されるものではなく、要求が必ずしもコンテンツに対する要求ではない一般的な要求の処理により一般的に適用可能であってよいことは留意されるべきである。

【００９０】

各サーバは、通常、そのサーバの一般的な管理及び運用のための実行可能プログラム命令を提供するオペレーティングシステムを含み、通常、サーバのプロセッサによって実行される時に、サーバがその意図される機能を実行できるようにする命令を記憶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、リードオンリーメモリ等）を含む。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のための適した実装は既知であり又は市販されており、特に本明細書の開示を鑑みて当業者によって

容易に実装される。

【００９１】

一実施形態における環境は、１つ又は複数のコンピュータネットワーク又は直接的な接続を利用して、通信リンクを介して相互接続されるいくつかのコンピュータシステム及び構成要素を活用する分散型コンピューティング環境である。ただし、係るシステムは、図１１に示されるよりも少ない数又は多い数の構成要素を有するシステムで等しくうまく運用できることが当業者によって理解されるであろう。したがって、図１１のシステム１１００の描写は、本来例示的であり、本開示の範囲を制限しないと解釈されるべきである。

【００９２】

多様な実施形態は、いくつかの場合に、多数のアプリケーションのいずれかを運用するために使用できる１台又は複数のユーザコンピュータ、コンピューティングデバイス、又は処理装置を含むことの可能なる多種多様の運用環境でさらに実装できる。ユーザ又はクライアントデバイスは、携帯電話向けソフトウェアを実行し、多数のネットワーキングプロトコル及びメッセージングプロトコルをサポートできるセルラーデバイス、無線デバイス並びにハンドヘルドデバイスだけではなく、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、又はタブレットコンピュータ等の多数の汎用パーソナルコンピュータの内のいずれかを含むことができる。また、係るシステムは、開発及びデータベース管理等のためにさまざまな市販のオペレーティングシステム及び他の既知のアプリケーションのいずれかを実行する多数のワークステーションを含むことができる。また、これらのデバイスは、ダミー端末、シンクライアント、ゲーム機、及びネットワークを介して通信できる他のデバイス等の他の電子デバイスを含むことができる。

【００９３】

本開示の多様な実施形態は、伝送制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）、オープンシステムインターコネクション（「ＯＳＩ」）モデルの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」）、共通インターネットファイルシステム（「ＣＩＦＳ」）、及びＡｐｐｌｅＴａｌｋ等のさまざまな市販のプロトコルのいずれかを使用して通信をサポートするための当業者によく知られている少なくとも１つのネットワークを活用する。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、公衆交換電話ネットワーク、赤外線ネットワーク、無線ネットワーク、及び任意のそれらの組合せとすることができる。

【００９４】

ウェブサーバを活用する実施形態で、ウェブサーバはハイパーテキスト転送プロトコル（「ＨＴＴＰ」）サーバ、ＦＴＰサーバ、共通ゲートウェイインタフェース（「ＣＧＩ」）サーバ、データサーバ、Ｊａｖａ（登録商標）サーバ、及び業務アプリケーションサーバを含んださまざまなサーバ又は中間階層アプリケーションのいずれかを実行できる。また、サーバ（複数の場合がある）は、１つ又は複数のスクリプト、又は、Ｊａｖａ（登録商標）、Ｃ、Ｃ＃、若しくはＣ＋＋等の任意のプログラミング言語又はＰｅｒｌ、Ｐｙｔｈｏｎ、若しくはＴＣＬ等の任意のスクリプト言語、並びに、それらの組み合わせで書かれるプログラムとしても実装され得る、１つ又は複数のウェブアプリケーションを実行すること等によって、ユーザデバイスからの要求に応えてプログラム又はスクリプトを実行できることがある。サーバ（複数の場合がある）は、Ｏｒａｃｌｅ（登録商標）、Ｍｉｃｒｏｓｏｆｔ（登録商標）、Ｓｙｂａｓｅ（登録商標）、及びＩＢＭ（登録商標）から市販されるものを制限なく含む、データベースサーバを含んでもよい。

【００９５】

環境は、上述されたさまざまなデータストア、並びに他のメモリ及び記憶媒体を含むことができる。これらは、コンピュータの内の１台又は複数台に対して局所的に（及び／又は常駐する）又はネットワーク全体のコンピュータのいずれか若しくはすべてから遠隔の

記憶媒体上等、さまざまな場所に常駐できる。特定の組の実施形態では、情報は当業者によく知られているストレージエリアネットワーク（「ＳＡＮ」）に常駐してよい。同様に、コンピュータ、サーバ、又は他のネットワークデバイスに起因する機能を実行するために必要ないずれのファイルも、必要に応じてローカルに及び／又は遠隔に記憶されてよい。システムがコンピュータ化されたデバイスを含む場合、それぞれの係るデバイスはバスを介して電気的に結合されてよいハードウェア要素を含むことができ、該要素は、例えば、少なくとも１台の中央演算処理装置（「ＣＰＵ」又は「プロセッサ」）、少なくとも１台の入力デバイス（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、又はキーボード）、及び少なくとも１台の出力デバイス（例えば、ディスプレイデバイス、プリンタ、又はスピーカ）を含む。また、係るシステムは、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だけではなく、ディスクドライブ、光学式記憶デバイス等の１台又は複数のストレージデバイス、及びランダムアクセスメモリ（「ＲＡＭ」）又はリードオンリーメモリ（「ＲＯＭ」）等の固体記憶装置も含んでよい。

【００９６】

また、係るデバイスは、上述されたようにコンピュータ可読記憶媒体読取装置、通信デバイス（例えば、モデム、ネットワークカード（無線又は有線）、赤外線通信デバイス等）、及び作業メモリを含むことができる。コンピュータ可読記憶媒体読取装置は、一時的に及び／又はより恒久的にコンピュータ可読情報を含む、記憶する、送信する、及び取り出すための記憶媒体だけではなく、遠隔ストレージデバイス、ローカルストレージデバイス、固定ストレージデバイス及び／又はリムーバブルストレージデバイスを典型とするコンピュータ可読記憶媒体と接続できる、又は受け入れるように構成できる。また、システム及び多様なデバイスは、通常、クライアントアプリケーション又はウェブブラウザ等のオペレーティングシステム及びアプリケーションプログラムを含む、少なくとも１台の作業メモリデバイスの中に位置する多数のソフトウェアアプリケーション、モジュール、サービス、又は他の要素を含む。代替的実施形態は、上述されたものから多数の変形形態を有することがあることは理解されるべきである。例えば、カスタマイズされたハードウェアが使用される可能性もある、及び／又は特定の要素がハードウェア、（アプレット等の高移植性ソフトウェアを含んだ）ソフトウェア、又は両方で実装される可能性がある。さらに、ネットワーク入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利用されてよい。

【００９７】

コード又はコードの部分を含むための記憶媒体及びコンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、電気的消去可能プログラム可能型読取専用メモリ（「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リードオンリーメモリ（「ＣＤ－ＲＯＭ」）、デジタル多用途ディスク（ＤＶＤ）、もしくは他の光学式記憶、磁気カセット、磁気テープ、磁気ディスク記憶装置、もしくは他の磁気記録装置、もしくは所望される情報を記憶するために使用することができ、システムデバイスによってアクセスできる任意の他の媒体を含む、コンピュータ可読命令、データ構造、プログラムモジュール、又は他のデータ等の情報の記憶及び／又は送信のための任意の方法又は技術で実装される揮発性媒体及び不揮発性媒体、リムーバブル媒体及び非リムーバブル媒体等であるが、これらに限定されるものではない記憶媒体及び通信媒体を含んだ、当技術分野で既知の又は使用されている任意の適切な媒体を含むことができる。本明細書に提供される開示及び教示に基づいて、当業者は多様な実施形態を実装するための適切な他のやり方及び／又は方法を理解するであろう。

【００９８】

本明細書及び図面は、したがって制限的な意味ではなく例示的な意味で見なされるべきである。しかしながら、多様な修正及び変更が、特許請求の範囲に明記される本発明のより広い精神及び範囲から逸脱することなくそれらに対して加えられ得ることは明らかである。

【００９９】

他の変形形態は本開示の精神の範囲内である。したがって、開示されている技法は多様な修正及び代替の構成の影響を受けやすいが、そのうちの所定の例示実施形態が図面に示され、詳細に上記に説明されている。ただし、開示されている特定の１つ又は複数の形式に本発明を制限する意図はなく、逆に、添付の特許請求の範囲に定められる本発明の精神及び範囲に入るすべての修正、代替構成、及び同等物を対象として含むことが意図される。

【０１００】

開示される実施形態を説明する文脈での（特に以下の特許請求の範囲の文脈での）用語「ａ」及び「ａｎ」及び「ｔｈｅ」並びに類似の指示対象の使用は、本明細書に別段の指示がない限り、又は明確に文脈に矛盾しない限り単数及び複数の両方ともを含むと解釈されるべきである。用語「備える」、「有する」、「含む」、及び「含有する」は特に断りのない限りオープンエンド用語（つまり、「～を含むが、これに限定されるものではない」を意味する）として解釈されるべきである。用語「接続される」は、修飾されておらず、物理接続を指している時、介在する何かがあったとしても、部分的に又は完全に中に含まれる、取り付けられる、又はともに接合されるとして解釈されるべきである。本明細書での値の範囲の列挙は、本明細書で別段の指示がない限り範囲に入るそれぞれ別々の値を個別に参照する簡単な方法として役立つことを単に意図とし、それぞれの別々の値は、あたかもそれが個々に本明細書で列挙されているかのように本明細書中に組み込まれる。用語「セット」（例えば「項目のセット」）又は「サブセット」の使用は、特に断りのない限り又は文脈に矛盾しない限り、１つ又は複数のメンバを含んだ空ではない集合体として解釈されるべきである。さらに、特に断りのない限り又は文脈に矛盾しない限り、対応するセットの用語「サブセット」は必ずしも対応するセットの適正なサブセットを示すのではなく、サブセット及び対応するセットは等しいことがある。

【０１０１】

形式「Ａ、Ｂ、及び、Ｃの内の少なくとも１つ」の句、又は「Ａ、Ｂ及びＣの内の少なくとも１つ」等の接続言語は、特に明記されない限り又は明確に文脈に矛盾しない限り、それ以外の場合、項目、用語等がＡもしくはＢもしくはＣ、又はＡ及びＢ及びＣのセットの任意の空ではないサブセットのどちらかであってよいことを提示するために一般に使用される文脈で理解される。例えば、上記の接続句で使用される３つのメンバを有するセットの例示的実施例で、「Ａ、Ｂ、及び、Ｃの内の少なくとも１つ」及び「Ａ、Ｂ及びＣの内の少なくとも１つ」は以下のセットの内のいずれかを指す。｛Ａ｝、｛Ｂ｝、｛Ｃ｝、｛Ａ，Ｂ｝、｛Ａ，Ｃ｝、｛Ｂ，Ｃ｝、｛Ａ，Ｂ，Ｃ｝。したがって、係る接続言語は、特定の実施形態が、Ａの少なくとも１つ、Ｂの少なくとも１つ、及びＣの少なくとも１つがそれぞれ存在することを必要とすることを暗示することを概して意図していない。

【０１０２】

本明細書に説明されるプロセスの運用は、本明細書で別段の指示がない限り又は明確に文脈に矛盾しない限り任意の適した順序で実行できる。本明細書に説明されるプロセス（又はプロセスの変形及び／又は組合せ）は、実行可能命令で構成された１つ又は複数のコンピュータシステムの制御下で実行されてよく、ハードウェア又はハードウェアの組合せによって１台又は複数のプロセッサで集合的に実行するコード（例えば、実行可能命令、１つ又は複数のコンピュータプログラム、又は１つ又は複数のアプリケーション）として実装されてよい。コードは、例えば、１台又は複数のプロセッサによって実行可能な複数の命令を含んだコンピュータプログラムの形でコンピュータ可読記憶媒上に記憶されてよい。コンピュータ可読記憶媒体は非一時的であってよい。

【０１０３】

本明細書に提供されるありとあらゆる例、又は例示的な言語（例えば「等」）の使用は単に本発明の実施形態をよりよく明らかにすることだけを意図し、別段に請求されない限り、本発明の範囲に対する制限を示さない。明細書中の言語は、本発明の実践にとって必須であるいかなる非請求要素も示すとして解釈されるべきではない。

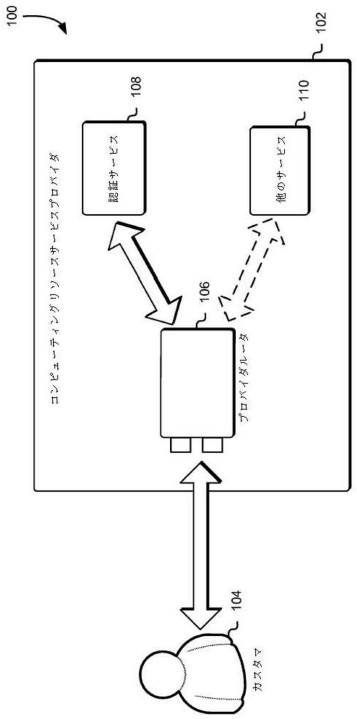
【０１０４】

本発明を実施するために本発明者に既知の最良の形態を含んだ本開示の好ましい実施形態が本明細書に説明されている。それらの好ましい実施形態の変形形態は上記明細書を読むと当業者に対して明らかにすることができる。本発明者は、当業者が係る変形形態を必要に応じて利用することを予想し、本発明者は、本開示の実施形態が本明細書に具体的に説明されるのとは別のやり方で実践されることを意図する。したがって、本開示の範囲は、適用可能な規則によって許される、本明細書に添付される特許請求の範囲に列挙される主題のすべての修正形態及び同等物を含む。さらに、そのすべての考えられる変形形態における上述された要素のいかなる組み合わせも、本明細書に別段に指示されない限り又は明確に文脈に矛盾しない限り本開示の範囲によって包含される。

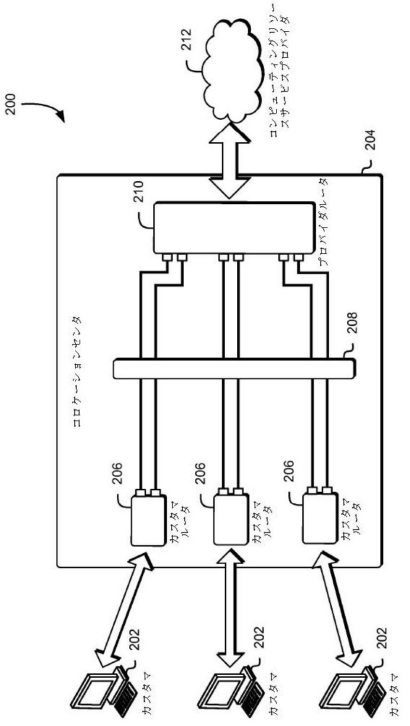
【０１０５】

本明細書に引用される公報、特許出願、及び特許を含むすべての参考文献は、各参考文献が個々に及び明確に参照することにより組み込まれるために示され、その全体として本明細書に明記されるかのように同程度まで、参照することにより本明細書に組み込まれる。

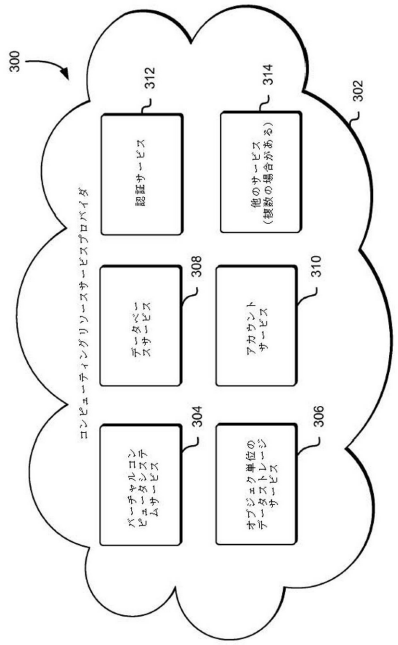
【図１】



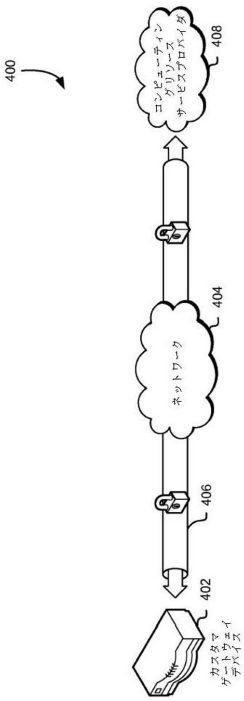
【図２】



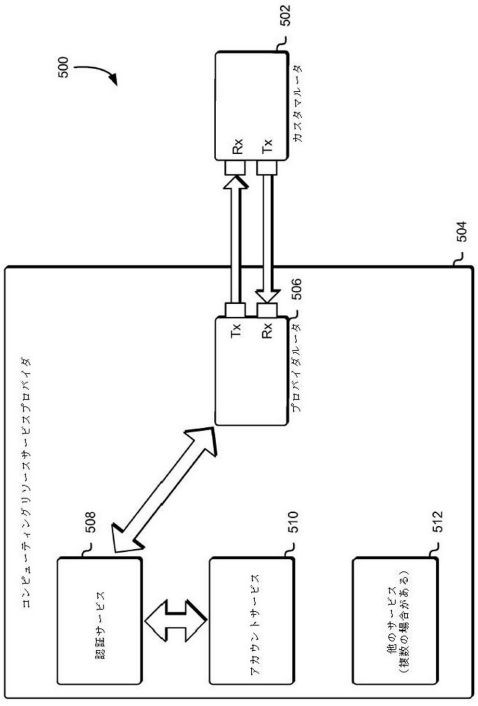
【図３】


300
302
コンピューティングリソースサービスプロバイダ
312
認証サービス
314
他のサービス
（複数の場合がある）
308
データベース
サービス
310
アカウント
サービス
304
バーチャルコンピュータシステム
サービス
306
オブジェクト単位の
データストレージ
サービス

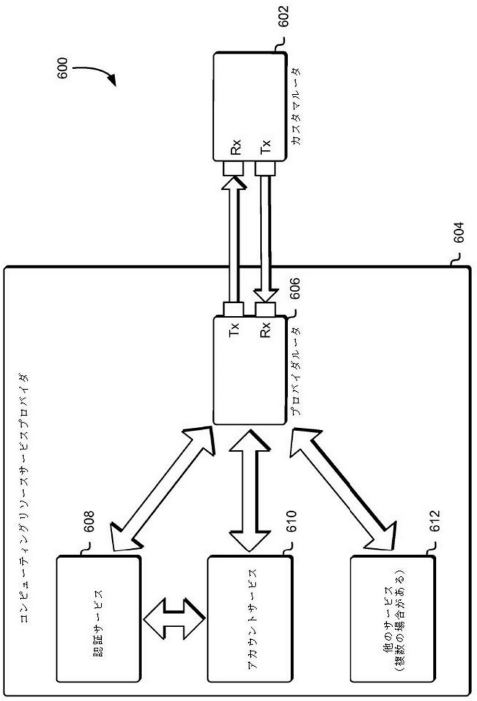
【図４】


400
408
コンピューティング
リソース
サービスプロバイダ
404
ネットワーク
406
402
カスタマー
ゲートウェイ
デバイス

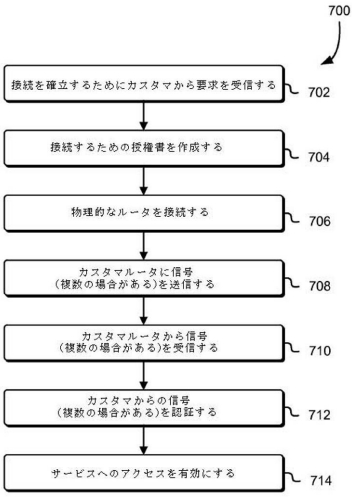
【図５】


500
502
Rx
Tx
カスタマルータ
504
Tx
Rx
506
プロバイダルータ
コンピューティングリソースサービスプロバイダ
508
認証サービス
510
アカウントサービス
512
他のサービス
（複数の場合がある）

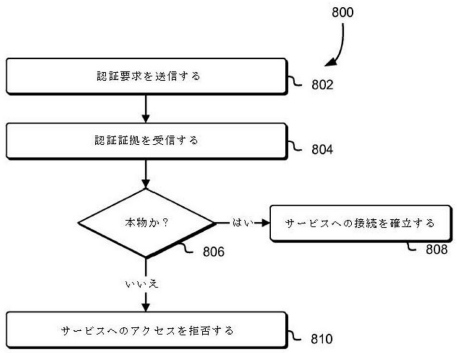
【図６】


600
602
Rx
Tx
カスタマルータ
604
Tx
Rx
606
プロバイダルータ
コンピューティングリソースサービスプロバイダ
608
認証サービス
610
アカウントサービス
612
他のサービス
（複数の場合がある）

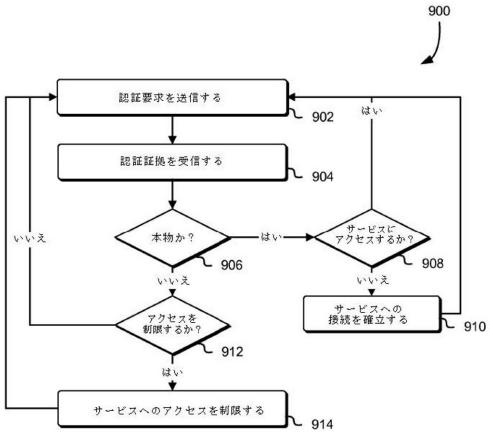
【図７】


700
接続を確立するためにカスタマから要求を受信する
702
接続するための授権書を作成する
704
物理的なルータを接続する
706
カスタマルータに信号
(複数の場合がある)を送信する
708
カスタマルータから信号
(複数の場合がある)を受信する
710
カスタマからの信号
(複数の場合がある)を認証する
712
サービスへのアクセスを有効にする
714

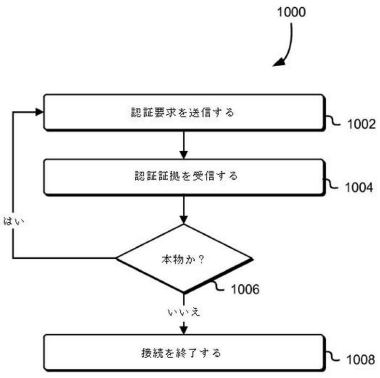
【図８】


800
認証要求を送信する
802
認証証拠を受信する
804
本物か？
806
はい
サービスへの接続を確立する
808
いいえ
サービスへのアクセスを拒否する
810

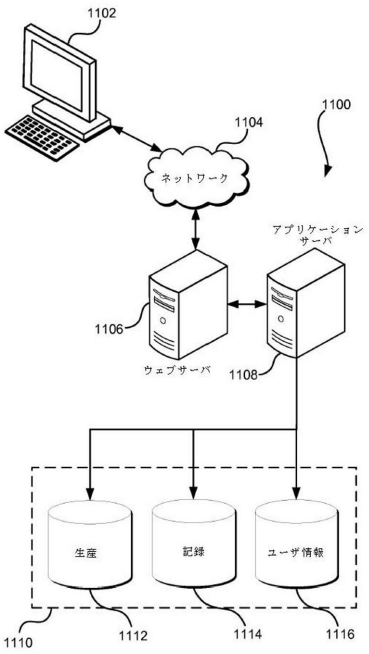
【図９】


900
認証要求を送信する
902
認証証拠を受信する
904
本物か？
906
はい
サービスに
アクセスするか？
908
はい
いいえ
いいえ
サービスへの
接続を確立する
910
アクセスを
制限するか？
912
はい
いいえ
サービスへのアクセスを制限する
914

【図１０】


1000
認証要求を送信する
1002
認証証拠を受信する
1004
本物か？
1006
はい
いいえ
接続を終了する
1008

【図１１】


1102
1100
1104
ネットワーク
アプリケーション
サーバ
1106
ウェブサーバ
1108
生産
記録
ユーザ情報
1110
1112
1114
1116

フロントページの続き

(72)発明者　アーレン　クリスチャン　アーサー
アメリカ合衆国　９８１０９－５２１０　ワシントン州　シアトル　テリー　アヴェニュー　ノース　４１０

合議体
審判長　田中　秀人
審判官　仲間　晃
審判官　松平　英

(56)参考文献　特開２００２－１０８８１８（ＪＰ，Ａ）
特開２００４－３１８５８２（ＪＰ，Ａ）
特開２００５－３３３３５０（ＪＰ，Ａ）
米国特許出願公開第２００５／００６３４００（ＵＳ，Ａ１）
米国特許出願公開第２００７／０２３４０５４（ＵＳ，Ａ１）
国際公開第２０１３／０８１９６２（ＷＯ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/33