(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2018-533141
(P2018-533141A)
(43)公表日　平成30年11月8日(2018.11.8)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/41	(2013.01)	G06F	21/41		5B084
G06F 21/62	(2013.01)	G06F	21/62	345	
G06F 13/00	(2006.01)	G06F	13/00	510A	

審査請求 未請求　予備審査請求 有　（全 50 頁）

(21)出願番号　特願2018-520614 (P2018-520614)
(86)(22)出願日　平成28年3月31日 (2016.3.31)
(85)翻訳文提出日　平成30年6月18日 (2018.6.18)
(86)国際出願番号　PCT/US2016/025402
(87)国際公開番号　WO2017/069800
(87)国際公開日　平成29年4月27日 (2017.4.27)
(31)優先権主張番号　14/920,807
(32)優先日　平成27年10月22日 (2015.10.22)
(33)優先権主張国　米国 (US)

(71)出願人　502303739
オラクル・インターナショナル・コーポレイション
アメリカ合衆国カリフォルニア州９４０６５レッドウッド・シティー，オラクル・パークウェイ５００
(74)代理人　110001195
特許業務法人深見特許事務所
(72)発明者　マシュー，スティーブン
インド、５６００３５　カルナータカ、バンガロール、サージャプール・ロード、カーメララム・ポスト、ハドシダプラ・ビレッジ、チェサナ・メープル、エイ・ブロック、ナンバー・２０１

最終頁に続く

(54)【発明の名称】エンドユーザによって起動されるアクセスサーバ真正性チェック

(57)【要約】
１つ以上のリソースへのアクセスを制御するものなどのコンピューティングシステム（たとえばアクセス管理システム）の真正性をユーザが検証できるようにするための手法が開示される。ユーザは、クレデンシャル情報をアクセス管理システムに提供する前に、アクセス管理システムの真正性を判断することができる。ユーザには、クライアントシステムで、アクセス管理システムの認証を要求するためのインターフェイスが提示され得る。アクセス管理システムは、アクセス管理システムへ送り返すための一時アクセス情報を、クライアントシステムでユーザに提供してもよい。アクセス管理システムは、アクセス管理システムを立証するために、最近の個人情報をクライアントシステムでユーザに提供してもよい。個人情報が立証されると、アクセス管理システムはユーザに、セッションを確立するためのクレデンシャル情報の入力を促してもよい。

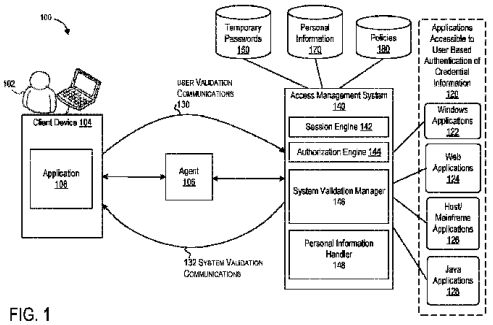

FIG. 1

【特許請求の範囲】
【請求項１】
方法であって、
アクセス管理システムのコンピューティングシステムが、ユーザによって操作されるコンピューティングデバイスから、前記アクセス管理システムの認証を求める検証要求を受信するステップを含み、前記検証要求は、前記ユーザに関連付けられたユーザ識別情報を含み、前記方法はさらに、
前記コンピューティングシステムが、前記ユーザ識別情報に基づいた前記ユーザに関連付けられた宛先へ、前記ユーザが前記アクセス管理システムを認証するための一時アクセス情報を送信するステップと、
前記コンピューティングシステムが、前記コンピューティングデバイスから、前記一時アクセス情報を含む第１の応答を受信するステップと、
前記第１の応答で受信された前記一時アクセス情報を立証すると、前記コンピューティングシステムが、前記ユーザについての個人情報を前記コンピューティングデバイスへ送信するステップと、
前記コンピューティングデバイスから第２の応答を受信するステップとを含み、前記第２の応答は、前記ユーザによる前記個人情報の確認を示し、前記第２の応答は、前記ユーザのクレデンシャルデータを含み、前記方法はさらに、
前記コンピューティングシステムが、前記コンピューティングデバイスからリソースにアクセスするための前記ユーザの認証を判断するステップを含み、前記認証は、前記第２の応答で受信された前記クレデンシャルデータと前記個人情報の前記確認とに基づいて判断される、方法。
【請求項２】
前記ユーザは前記コンピューティングデバイスから前記リソースへのアクセスを認証されていないと判断すると、前記コンピューティングデバイスへ、前記ユーザのクレデンシャル情報についての要求を送信するステップをさらに含み、
前記コンピューティングデバイスは、クレデンシャル情報についての前記要求に応答して前記検証要求を送信する、請求項１に記載の方法。
【請求項３】
前記宛先は、前記コンピューティングデバイスを含む、請求項１または２に記載の方法。
【請求項４】
前記宛先は、前記ユーザに関連付けられたデバイスを含み、前記デバイスは、前記コンピューティングデバイスとは異なる、請求項１または２に記載の方法。
【請求項５】
前記第１の応答は、前記宛先から受信される、請求項４に記載の方法。
【請求項６】
前記ユーザ識別情報は前記ユーザに関連付けられていると判断するステップと、
前記ユーザ識別情報に基づいて前記宛先を識別するステップとをさらに含む、請求項１～５のいずれか１項に記載の方法。
【請求項７】
前記一時アクセス情報は期間に関連付けられ、前記一時アクセス情報を立証することは、応答時間が前記期間内にあると判断することを含み、前記応答時間は、前記一時アクセス情報が前記コンピューティングデバイスへ送信された後に前記第１の応答を受信するための時間に基づく、請求項１～６のいずれか１項に記載の方法。
【請求項８】
前記第１の応答で受信された前記一時アクセス情報を立証すると、前記個人情報を送信する前に前記個人情報を生成するステップをさらに含む、請求項１～７のいずれか１項に記載の方法。
【請求項９】

前記個人情報は、前記一時アクセス情報が立証された後に判断される前記ユーザについての金融情報を含む、請求項８に記載の方法。
【請求項１０】
アクセス管理システムであって、
１つ以上のプロセッサと、
前記１つ以上のプロセッサと結合され、前記１つ以上のプロセッサによって読取可能なメモリとを含み、
前記メモリは、前記１つ以上のプロセッサによって実行されると、前記１つ以上のプロセッサに複数のステップを行なわせる１組の命令を格納し、前記複数のステップは、
ユーザによって操作されるコンピューティングデバイスから、前記アクセス管理システムの認証を求める検証要求を受信するステップを含み、前記検証要求は、前記ユーザに関連付けられたユーザ識別情報を含み、前記複数のステップはさらに、
前記ユーザ識別情報に基づいた前記ユーザに関連付けられた宛先へ、前記ユーザが前記アクセス管理システムを認証するための一時アクセス情報を送信するステップと、
前記コンピューティングデバイスから、前記一時アクセス情報を含む第１の応答を受信するステップと、
前記第１の応答で受信された前記一時アクセス情報を立証すると、前記ユーザについての個人情報を前記コンピューティングデバイスへ送信するステップと、
前記コンピューティングデバイスから第２の応答を受信するステップとを含み、前記第２の応答は、前記ユーザによる前記個人情報の確認を示し、前記第２の応答は、前記ユーザのクレデンシャルデータを含み、前記複数のステップはさらに、
前記コンピューティングデバイスからリソースにアクセスするための前記ユーザの認証を判断するステップを含み、前記認証は、前記第２の応答で受信された前記クレデンシャルデータと前記個人情報の前記確認とに基づいて判断される、アクセス管理システム。
【請求項１１】
前記１組の命令は、前記１つ以上のプロセッサによって実行されると、前記１つ以上のプロセッサに、
前記ユーザは前記コンピューティングデバイスから前記リソースへのアクセスを認証されていないと判断すると、前記コンピューティングデバイスへ、前記ユーザのクレデンシャル情報についての要求を送信するステップをさらに行なわせ、
前記コンピューティングデバイスは、クレデンシャル情報についての前記要求に応答して前記検証要求を送信する、請求項１０に記載のアクセス管理システム。
【請求項１２】
前記宛先は、前記ユーザに関連付けられたデバイスを含み、前記デバイスは、前記コンピューティングデバイスとは異なる、請求項１０または１１に記載のアクセス管理システム。
【請求項１３】
前記１組の命令は、前記１つ以上のプロセッサによって実行されると、前記１つ以上のプロセッサに、
前記ユーザ識別情報は前記ユーザに関連付けられていると判断するステップと、
前記ユーザ識別情報に基づいて前記宛先を識別するステップとをさらに行なわせる、請求項１０～１２のいずれか１項に記載のアクセス管理システム。
【請求項１４】
前記一時アクセス情報は期間に関連付けられ、前記一時アクセス情報を立証することは、応答時間が前記期間内にあると判断することを含み、前記応答時間は、前記一時アクセス情報が前記コンピューティングデバイスへ送信された後に前記第１の応答を受信するための時間に基づく、請求項１０～１３のいずれか１項に記載のアクセス管理システム。
【請求項１５】
前記１組の命令は、前記１つ以上のプロセッサによって実行されると、前記１つ以上のプロセッサに、

前記第１の応答で受信された前記一時アクセス情報を立証すると、前記個人情報を送信する前に前記個人情報を生成するステップをさらに行なわせ、
前記個人情報は、前記一時アクセス情報が立証された後に判断される前記ユーザについての金融情報を含む、請求項１０～１４のいずれか１項に記載のアクセス管理システム。
【請求項１６】
１組の命令を格納する、非一時的なコンピュータ読取可能媒体であって、前記１組の命令は、１つ以上のプロセッサによって実行されると、前記１つ以上のプロセッサに複数のステップを行なわせ、前記複数のステップは、
アクセス管理システムのコンピューティングシステムが、ユーザによって操作されるコンピューティングデバイスから、前記アクセス管理システムの認証を求める検証要求を受信するステップを含み、前記検証要求は、前記ユーザに関連付けられたユーザ識別情報を含み、前記複数のステップはさらに、
前記コンピューティングシステムが、前記ユーザ識別情報に基づいた前記ユーザに関連付けられた宛先へ、前記ユーザが前記アクセス管理システムを認証するための一時アクセス情報を送信するステップと、
前記コンピューティングシステムが、前記コンピューティングデバイスから、前記一時アクセス情報を含む第１の応答を受信するステップと、
前記第１の応答で受信された前記一時アクセス情報を立証すると、前記コンピューティングシステムが、前記ユーザについての個人情報を前記コンピューティングデバイスへ送信するステップと、
前記コンピューティングデバイスから第２の応答を受信するステップとを含み、前記第２の応答は、前記ユーザによる前記個人情報の確認を示し、前記第２の応答は、前記ユーザのクレデンシャルデータを含み、前記複数のステップはさらに、
前記コンピューティングシステムが、前記コンピューティングデバイスからリソースにアクセスするための前記ユーザの認証を判断するステップを含み、前記認証は、前記第２の応答で受信された前記クレデンシャルデータと前記個人情報の前記確認とに基づいて判断される、非一時的なコンピュータ読取可能媒体。
【請求項１７】
前記１組の命令は、前記１つ以上のプロセッサによって実行されると、前記１つ以上のプロセッサに、
前記ユーザは前記コンピューティングデバイスから前記リソースへのアクセスを認証されていないと判断すると、前記コンピューティングデバイスへ、前記ユーザのクレデンシャル情報についての要求を送信するステップをさらに行なわせ、
前記コンピューティングデバイスは、クレデンシャル情報についての前記要求に応答して前記検証要求を送信する、請求項１６に記載の非一時的なコンピュータ読取可能媒体。
【請求項１８】
前記宛先は、前記ユーザに関連付けられたデバイスを含み、前記デバイスは、前記コンピューティングデバイスとは異なる、請求項１６または１７に記載の非一時的なコンピュータ読取可能媒体。
【請求項１９】
前記１組の命令は、前記１つ以上のプロセッサによって実行されると、前記１つ以上のプロセッサに、
前記ユーザ識別情報は前記ユーザに関連付けられていると判断するステップと、
前記ユーザ識別情報に基づいて前記宛先を識別するステップとをさらに行なわせる、請求項１６～１８のいずれか１項に記載の非一時的なコンピュータ読取可能媒体。
【請求項２０】
前記１組の命令は、前記１つ以上のプロセッサによって実行されると、前記１つ以上のプロセッサに、
前記第１の応答で受信された前記一時アクセス情報を立証すると、前記個人情報を送信する前に前記個人情報を生成するステップをさらに行なわせ、

前記個人情報は、前記一時アクセス情報が立証された後に判断される前記ユーザについての金融情報を含む、請求項１６～１９のいずれか１項に記載の非一時的なコンピュータ読取可能媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願との相互参照

本願は、「エンドユーザによって起動されるアクセスサーバ真正性チェック」（END USER INITIATED ACCESS SERVER AUTHENTICITY CHECK）と題された、２０１５年１０月２２日に出願された米国非仮特許出願第１４／９２０，８０７号の利益および優先権を主張する。その内容全体は、あらゆる目的のために、ここに引用により援用される。

【背景技術】

【０００２】

背景

一般に、本願はデータ処理に関する。より具体的には、本願は、リソースへのアクセスを制御するコンピューティングシステムの真正性をユーザが検証できるようにするための手法に関する。

【０００３】

現代のビジネスは、事業活動にとって重大な情報を制御し生成するさまざまなアプリケーションおよびシステムに依拠している。異なるアプリケーションはしばしば異なるサービスおよび情報を提供しており、異なるユーザは各システムまたはアプリケーション内で異なるレベルの情報へのアクセスを必要とする場合がある。ユーザが与えられるアクセスのレベルは、ユーザの役割に依存し得る。たとえば、あるマネージャは、自分に報告する従業員についてのある情報へのアクセスを必要とし得るが、そのマネージャが、自分が報告する人々についての同じ情報にアクセスすることは、不適切であり得る。

【０００４】

以前は、性能があまり高くないアプリケーションは、アクセス管理ビジネスロジックをアプリケーションコードに直接取り入れていた。すなわち、各アプリケーションはユーザに、たとえば別個のアカウント、別個のポリシーロジック、および別個の許可を有するよう要求したであろう。さらに、これらのアプリケーションのうちの１つによってユーザが認証された場合、この認証は、企業における他のアプリケーションには知られないままである。なぜなら、第１のアプリケーションによる認証が行なわれたという事実が共有されないためである。このため、認証およびアクセス制御のために異なるシステムを使用するアプリケーション間には、信用という概念はない。技術者らは、１つの企業でアプリケーションごとにアクセス管理システムを有することは、自動車１台ごとにガソリンスタンドを有することによく似ているということに速やかに気付き、認証およびアクセス制御は共有リソースとしてより効率的に実現され管理されるであろうと判断した。これらの共有リソースは、アクセス管理システムとして知られるようになった。

【０００５】

アクセス管理システムは、ある特定のアクセス要求がある特定のリソースに与えられるべきかどうかに関する判断を下すために、ポリシーおよび他のビジネスロジックをしばしば使用する。アクセスが与えられるべきであるという判断が下されると、トークンが要求側に提供される。このトークンは、秘密データを守るドアを開けるために使用され得るキーに似ている。たとえば、ユーザは、給料情報といったある従業員についての情報を集めるために、人材データベースへのアクセスを試みるかもしれない。ユーザのウェブブラウザはアプリケーションに要求を行ない、それは認証を必要とする。ウェブブラウザがトークンを有していない場合、ユーザは、アクセス管理システムにログインするよう求められる。ユーザが認証されている場合、ユーザのブラウザは、人材アプリケーションにアクセスするために使用され得るトークンを表わすクッキーを受信する。

【０００６】

ある企業では、ユーザ（たとえば従業員）は典型的には、１つ以上の異なるシステムおよびアプリケーションへのアクセスを有するかもしれない。これらのシステムおよびアプリケーションの各々は、異なるアクセス制御ポリシーを利用し、異なるクレデンシャル（たとえば、ユーザ名およびパスワード）を必要とするかもしれない。シングルサインオン（single sign-on：ＳＳＯ）は、最初のログインの後に複数のシステムおよびアプリケーションへのアクセスをユーザに提供することができる。たとえば、ユーザが自分の作業用コンピュータにログインすると、ユーザは、システムおよびアプリケーションといった１つ以上の他のリソースへのアクセスも有し得る。あるアクセス管理システムは、リソースへのアクセスを判断するために、ユーザに自分のアイデンティティを立証するよう要求するかもしれない。ユーザは、「貴方が持っているもの」、「貴方が知っていること」、および「貴方が誰か」の組合せに基づいて、情報を要求されるかもしれない。

【０００７】

アクセス管理システムは、ユーザのクレデンシャルを立証するための情報をユーザに要求するために、クライアントデバイス上のグラフィカルユーザインターフェイスを用いてユーザに促すことができる。時折、ユーザに要求される情報は慎重に扱うべき機密情報を含む場合があり、それは、もし含まれると、個人のアイデンティティおよび個人情報（たとえば、金融情報またはアカウント情報）を脅かすおそれがある。その結果、ユーザは、情報を要求するシステムが実際にリソースへのアクセスを制御していることを確信しなければ、それらのリソースへのアクセスを得るためにサーバなどのシステムに機密情報を提供することをためらうかもしれない。

【０００８】

なりすましおよびフィッシングなどの手法を使用するアイデンティティ盗難における技術ベースの進歩の進行とともに、ユーザはより一層、クレデンシャルの要求元を立証する方法なしで自分のクレデンシャルを提供することを渋っている。たとえば、あるアクセス管理システムは、ユーザにプライベート情報を提供し、ユーザにそのプライベート情報に基づいてそのアクセス管理システムの真正性を判断させるかもしれない。しかしながら、このシナリオでは、なりすましおよびフィッシングシステムは、認証を要求するシステムが正当であるとユーザに信じさせようとするために使用され得る個人情報へのアクセスを有するかもしれない。別の例では、あるアクセス管理システムは、追加の立証のための特殊コードを用いて別のデバイスに連絡するかもしれない。しかしながら、なりすましシステムは、ユーザの連絡先情報へのアクセスを有するかもしれず、そのような情報を使用して追加の立証情報を送信するかもしれない。さらに別の例では、あるフィッシングまたはなりすましシステムは、アクセス管理システムによって制御されていない収集ページを通してクレデンシャル情報を取得することによって、ユーザをだまそうとするかもしれない。あるシナリオでは、クライアントシステム上で、悪質なブラウザプラグインが、ユーザからアクセスクレデンシャルを偽って要求するために、アクセス管理システムとして作用するよう起動されるかもしれない。

【０００９】

場合によっては、クライアントシステムを操作するユーザがアクセス管理システムを介してリソースにアクセスできるようにするために、クライアントシステムはワンタイムコード（たとえばパスワード）を受信してもよい。クライアントシステムは、不正侵入されたり盗まれたりした場合、クライアントシステムを操作するユーザがワンタイムコードを使用してリソースへの無認可アクセスを取得できるようにしてもよい。ユーザによって操作されるクライアントシステムとアクセス管理システムとの間の通信を傍受するために、アイデンティティ盗難のためのいくつかの手法が使用されてもよい。傍受された通信は、ユーザからアイデンティティまたはアクセス情報を請求するために使用されてもよい。

【００１０】

アクセス管理機能を提供するシステムの検証をユーザが起動できるようにする能力をユーザに提供するために、アクセス管理ソリューションが要求され得る。ユーザが、リソースにアクセスするためにクレデンシャル情報を要求するシステムの真正性を判断できるよ

うにするために、新しい手法が望まれる。
【発明の概要】
【課題を解決するための手段】
【００１１】
簡単な概要
本開示は一般に、リソースへのアクセスの管理に関する。１つ以上のリソースへのアクセスを制御するものなどのコンピューティングシステム（たとえばアクセス管理システム）の真正性をユーザが検証できるようにするために、ある手法が開示される。具体的には、ユーザがクレデンシャル情報をアクセス管理システムに提供する前に、ユーザがアクセス管理システムの真正性を判断できるようにするための手法が開示される。
【００１２】
ここに開示される実施形態は、ユーザが情報を使用してアクセス管理システムの真正性を立証できるようにする。情報は毎回異なるかもしれず、ユーザはこの最新情報を使用してアクセスサーバの真正性を立証することができる。アクセス管理システムとクライアントシステムとの間のデータの交換は、エンドユーザとアクセス管理システムとの間の３方向ハンドシェイクとして類推され得る。よって、ユーザが一時データを用いて自分を証明しない限り、アクセス管理システムは機密情報を漏らさないで済む。ここに説明される手法は、ユーザに一時データ（「貴方が持っているもの」）およびパスワード（「貴方が知っていること」）を要求することによって、盗まれたカードまたはモバイルデバイスの使用についてさらされるセキュリティリスクを防止する。３方向ハンドシェイクは、エンドユーザの視点からだけでなくアクセスサーバ側からも認証が無傷であることを保証する。
【００１３】
いくつかの実施形態では、ユーザには、クライアントシステムで、グラフィカルユーザインターフェイス（graphical user interface：ＧＵＩ）などのインターフェイスを提示することができ、それは、ユーザがアクセス管理システムの認証を要求できるようにする。インターフェイスは、アクセス管理システムによって制御されるリソースにアクセスするためにユーザからクレデンシャル情報が要求される前に、提示されてもよい。アクセス管理システムの真正性を立証することにより、ユーザは、無認可ユーザによって制御されるコンピューティングシステムにクレデンシャル情報が提供されないことを確信できる。ユーザがアクセス管理システムの真正性を検証できるようにすることにより、ユーザは、クレデンシャル情報および他の機密情報が無認可の当事者またはエンティティに漏洩されないことを保証できる。ユーザはまた、クレデンシャルが提供されるとそれらのクレデンシャルの受信者が所望のリソースへの無認可アクセスを得ることができるようなアクセス管理システム自体への不正侵入がなされなかったことを保証できる。
【００１４】
この発明の一局面では、システム検証を要求するためのインターフェイスが、システム検証を起動するためにユーザの識別情報を求めてもよい。識別情報は、アクセス管理システムがユーザを識別して、検証情報の通信のための連絡先情報を判断できるようにしてもよい。連絡先情報は、アクセス管理システムがシステム検証の一部として通信し得る１つ以上の宛先（たとえば、電子メールアドレスまたは異なるデバイス）に対応していてもよい。
【００１５】
システム検証中、アクセス管理システムは、時間などの１つ以上の基準によって制約される一時データ（たとえば一時アクセス情報）を送信してもよい。一時アクセス情報は、システム検証を要求するクライアントシステムへ、および／または、ユーザに関連付けられた任意の宛先へ送信されてもよい。アクセス管理システムは、システム検証プロセスの一部として、インターフェイスを介して一時アクセス情報を要求してもよい。アクセス管理システムは一時データを立証して、それがユーザへ送信されたものと一致するかどうかを判断することができる。
【００１６】

一時データが以前にユーザへ送信されたものと一致することを立証すると、アクセス管理システムは、システム検証の一部として、個人情報をユーザへ送信してもよい。個人情報は、無認可ユーザには知られないかもしれない、慎重に扱うべき機密情報（たとえば、現在の金融情報）を含み得る。個人情報は、クライアントシステムへ、および／または、ユーザに関連付けられた宛先へ送信されてもよい。インターフェイスを通して、ユーザは、個人情報が正しいかどうかを示すことができる。機密情報は、ユーザおよびアクセス管理システムにのみ知られているものであり得る。機密情報は、他の外部コンピューティングシステムが不正に傍受し、推測し、または取得することが不可能ではないにせよ可能性が低い情報を含み得る。

【００１７】

個人情報を立証すると、ユーザは、インターフェイスを通してクレデンシャル情報を提供することができる。クレデンシャル情報は、システム検証プロセスの一部としてユーザの認証を判断するために使用されてもよい。クレデンシャルに基づくユーザの検証が成功すると、アクセス管理システムは、リソースへのアクセスを可能にするようにユーザのためにセッションを確立してもよい。

【００１８】

いくつかの実施形態では、アクセス管理システムは、ここに説明される方法および動作を実現するように構成されたコンピューティングシステムを含んでいてもよい。さらに別の実施形態は、ここに説明される方法および動作のための命令を採用または格納するシステムおよび有形のマシン読取可能記憶媒体に関する。

【００１９】

少なくとも１つの実施形態では、方法は、ユーザによって操作されるコンピューティングデバイスから、アクセス管理システムの認証を求める検証要求を受信するステップを含んでいてもよく、検証要求は、ユーザに関連付けられたユーザ識別情報を含む。方法は、ユーザ識別情報に基づいたユーザに関連付けられた宛先へ、ユーザがアクセス管理システムを認証するための一時アクセス情報を送信するステップを含んでいてもよい。宛先は、コンピューティングデバイスであってもよい。宛先は、ユーザに関連付けられたデバイスであってもよい。デバイスは、コンピューティングデバイスとは異なっていてもよい。方法は、コンピューティングデバイスから、一時アクセス情報を含む第１の応答を受信するステップを含んでいてもよい。方法は、第１の応答で受信された一時アクセス情報を立証すると、コンピューティングシステムが、ユーザについての個人情報をコンピューティングデバイスへ送信するステップを含んでいてもよい。方法は、コンピューティングデバイスから第２の応答を受信するステップを含んでいてもよく、第２の応答は、ユーザによる個人情報の確認を示し、第２の応答は、ユーザのクレデンシャルデータを含む。方法は、コンピューティングデバイスからリソースにアクセスするためのユーザの認証を判断するステップを含んでいてもよい。認証は、第２の応答で受信されたクレデンシャルデータと個人情報の確認とに基づいて判断されてもよい。

【００２０】

いくつかの実施形態では、方法は、ユーザはコンピューティングデバイスからリソースへのアクセスを認証されていないと判断すると、コンピューティングデバイスへ、ユーザのクレデンシャル情報についての要求を送信するステップを含んでいてもよい。コンピューティングデバイスは、クレデンシャル情報についての要求に応答して検証要求を送信してもよい。

【００２１】

いくつかの実施形態では、第１の応答は、宛先から受信されてもよい。

いくつかの実施形態では、方法は、ユーザ識別情報はユーザに関連付けられていると判断するステップと、ユーザ識別情報に基づいて宛先を識別するステップとを含んでいてもよい。

【００２２】

いくつかの実施形態では、一時アクセス情報は期間に関連付けられる。一時アクセス情

報を立証することは、応答時間が期間内にあると判断することを含んでいてもよい。応答時間は、一時アクセス情報がコンピューティングデバイスへ送信された後に第１の応答を受信するための時間に基づいていてもよい。

【００２３】

いくつかの実施形態では、方法は、第１の応答で受信された一時アクセス情報を立証すると、個人情報を送信する前に個人情報を生成するステップを含んでいてもよい。

【００２４】

いくつかの実施形態では、個人情報は、一時アクセス情報が立証された後に判断されるユーザについての金融情報を含む。

【００２５】

前述の事項、ならびに他の特徴および実施形態は、以下の明細書、請求項、および添付図面を参照すれば、より明らかになるであろう。

【図面の簡単な説明】

【００２６】

本発明の例示的な実施形態を、以下の図面を参照して、以下に詳細に説明する。

【図１】一実施形態に従った、ユーザがアクセス管理システムの真正性を検証できるようにするためのシステムの高レベル図である。

【図２】一実施形態に従った、ユーザがアクセス管理システムの真正性を検証できるようにするためのシステムの高レベル図である。

【図３】一実施形態に従った、ユーザがアクセス管理システムの真正性を検証できるようにするための動作を示すシーケンス図である。

【図４】一実施形態に従った、ユーザがアクセス管理システムの真正性を検証できるようにするための動作を示すシーケンス図である。

【図５】一実施形態に従った、ユーザがアクセス管理システムの真正性を検証できるようにするためのプロセスを示すフローチャートである。

【図６】一実施形態に従った、ユーザがアクセス管理システムの真正性を検証できるようにするためのプロセスのグラフィカルユーザインターフェイス（ＧＵＩ）を示す図である。

【図７】一実施形態に従った、ユーザがアクセス管理システムの真正性を検証できるようにするためのプロセスのグラフィカルユーザインターフェイス（ＧＵＩ）を示す図である。

【図８】一実施形態に従った、ユーザがアクセス管理システムの真正性を検証できるようにするためのプロセスのグラフィカルユーザインターフェイス（ＧＵＩ）を示す図である。

【図９】一実施形態に従った、ユーザがアクセス管理システムの真正性を検証できるようにするためのプロセスのグラフィカルユーザインターフェイス（ＧＵＩ）を示す図である。

【図１０】一実施形態を実現するための分散型システムの簡略図である。

【図１１】本開示の一実施形態に従った、サービスがクラウドサービスとして提供され得るシステム環境の１つ以上のコンポーネントの簡略ブロック図である。

【図１２】本発明の一実施形態を実現するために使用され得る例示的なコンピュータシステムを示す図である。

【発明を実施するための形態】

【００２７】

詳細な説明

以下の記載では、説明の目的で、特定の詳細が、この発明の実施形態の完全な理解を提供するために述べられる。しかしながら、これらの特定の詳細がなくてもさまざまな実施形態が実践され得ることは明らかであろう。たとえば、実施形態を必要以上に詳細に記して不明瞭にすることがないように、回路、システム、アルゴリズム、構造、手法、ネットワーク、プロセス、および他のコンポーネントは、ブロック図の形のコンポーネントとし

て示されてもよい。図面および説明は、限定的であるよう意図されてはいない。

【００２８】

本開示は一般に、シングルサインオン（ＳＳＯ）アクセスの提供に関する。ＳＳＯセッションは、初期認証の後に、クレデンシャル情報（たとえば、ユーザ名およびパスワード）の認証に基づいて、１つ以上のシステムへのアクセスをユーザに提供してもよい。システムへのアクセスは、１つ以上のリソースへのアクセスを提供してもよい。リソースは、アプリケーション、文書、ファイル、電子コンテンツなどといった、コンピューティングシステムによって管理および／または格納される任意のアイテムを含んでいてもよい。リソースは、ユニフォームリソースロケータ（uniform resource locator：ＵＲＬ）、またはリソースのソースを示す他のデータによって識別されてもよい。

【００２９】

１つ以上のリソースへのアクセスを制御するものなどのコンピューティングシステム（たとえばアクセス管理システム）の真正性をユーザが検証できるようにするために、ある手法が開示される。具体的には、ユーザがクレデンシャル情報をアクセス管理システムに提供する前に、ユーザがアクセス管理システムの真正性を判断できるようにするための手法が開示される。

【００３０】

ここに開示される実施形態は、ユーザが情報を使用してアクセス管理システムの真正性を立証できるようにする。情報は毎回異なるかもしれず、ユーザはこの最新情報を使用してアクセスサーバの真正性を立証することができる。アクセス管理システムとクライアントシステムとの間のデータの交換は、エンドユーザとアクセス管理システムとの間の３方向ハンドシェイクとして類推され得る。よって、ユーザが一時データを用いて自分を証明しない限り、アクセス管理システムは機密情報を漏らさないで済む。ここに説明される手法は、ユーザに一時データ（「貴方が持っているもの」）およびパスワード（「貴方が知っていること」）を要求することによって、盗まれたカードまたはモバイルデバイスの使用についてさらされるセキュリティリスクを防止する。３方向ハンドシェイクは、エンドユーザの視点からだけでなくアクセスサーバ側からも認証が無傷であることを保証する。

【００３１】

ユーザがアクセス管理システムの真正性を検証できるようにするために、システム、方法、およびマシン読取可能媒体などのいくつかの実施形態が開示される。図１は、セッションでアクセス可能なリソースへのアクセスを有するユーザ（たとえばユーザ１０２）が、アクセス管理システム１４０の真正性を検証するためのプロセスを起動することができるシステム１００を示す。ユーザは、アクセス情報（たとえば、パスワードまたは機密情報）が無認可システムに漏洩されないことを保証するために、アクセス管理システムまたは任意のコンピューティングシステムの真正性の検証を望む場合がある。例示の目的で、ここに説明されるような「セッション」は、ＳＳＯセッションを含む。しかしながら、セッションは、ユーザへのアクセスを可能にする他のタイプのセッションを含んでいてもよい。アクセス管理システム１４０は、１つ以上のリソースへのアクセスを提供してもよい。アクセス管理システム１４０は、サインオンシステム、たとえばＳＳＯシステムを実現してもよく、それは、１つ以上のリソースへのＳＳＯアクセスを提供するためにＳＳＯセッションを確立することができる。

【００３２】

リソースは、ファイル、ウェブページ、文書、ウェブコンテンツ、コンピューティングリソース、またはアプリケーションを、何ら限定されることなく含んでいてもよい。たとえば、システム１００は、アプリケーション１２０、および／またはそれらのアプリケーション１２０を通してアクセス可能なコンテンツ、といったリソースを含んでいてもよい。リソースは、アプリケーションを使用して要求され、アクセスされてもよい。たとえば、アプリケーションは、要求されたリソースを識別するＵＲＬに基づいて、リソースサーバからウェブページへのアクセスを要求してもよい。リソースは、１つ以上のコンピューティングシステム、たとえば、ＳＳＯシステムでユーザ１０２を認証すると１つ以上のリ

ソースへのアクセスを提供するリソースサーバによって提供されてもよい。

【００３３】

クライアントデバイス、たとえばクライアントデバイス１０４を操作するユーザ１０２は、ユーザがアクセス管理システム（たとえばアクセス管理システム１４０）と対話できるようにするための入力を受け付ける１つ以上のインターフェイスを提示してもよい。インターフェイスの例は、図６～９を参照して説明されるグラフィカルユーザインターフェイス（ＧＵＩ）を含んでいてもよい。インターフェイスは、クライアントデバイス１０４上で実行されるアプリケーション、たとえばアプリケーション１０８を使用してアクセス可能であってもよい。ユーザ１０２がユーザ１０２の認証のためにアクセス管理システム１４０を用いたアクセスプロセスを起動する前に、インターフェイスは、アクセス管理システム１４０の真正性の検証を要求するための入力を受信してもよい。ユーザ１０２からアクセス管理システム１４０の検証を求める要求を受信すると、アクセス管理システム１４０は、ユーザがアクセス管理システム１４０を検証できるようにするように、アクセス管理システム１４０とユーザ１０２によって操作されるクライアントデバイス１０４とを通信に従事させるプロセスを起動してもよい。ユーザとアクセス管理システム１４０との間の通信は、アクセス管理システム１４０がユーザのためのアクセスを確立するために実際のユーザと通信していることを、アクセス管理システム１４０が立証できるようにする。通信は、クライアントデバイスとアクセス管理システム１４０との間に３方向ハンドシェイクを確立して、リソースへのアクセスをユーザに提供するための認証のためにユーザとアクセス管理システムとの間に信用を確立する。

【００３４】

アクセス管理システム１４０は、コンピューティングシステムによって実現されてもよい。コンピューティングシステムは、１つ以上のコンピュータおよび／またはサーバ（たとえば、１つ以上のアクセスマネージャサーバ）を含んでいてもよく、それらは、汎用コンピュータ、特殊サーバコンピュータ（例として、ＰＣサーバ、ＵＮＩＸ（登録商標）サーバ、ミッドレンジサーバ、メインフレームコンピュータ、ラックマウントサーバなどを含む）、サーバファーム、サーバクラスタ、分散サーバ、または任意の他の適切な構成、および／またはそれらの組合せであってもよい。アクセス管理システム１４０は、オペレーティングシステムもしくはさまざまな追加サーバアプリケーションおよび／または中間層アプリケーションのうちのいずれかを実行してもよく、ＨＴＴＰサーバ、ＦＴＰサーバ、ＣＧＩサーバ、Ｊａｖａ（登録商標）サーバ、データベースサーバなどを含む。例示的なデータベースサーバは、オラクル、マイクロソフトなどから商業的に利用可能なものを、何ら限定されることなく含む。アクセス管理システム１４０は、ハードウェア、ファームウェア、ソフトウェア、またはそれらの組合せを使用して実現されてもよい。

【００３５】

いくつかの実施形態では、アクセス管理システム１４０は、データセンターにクラスタとしてデプロイメントされた複数のコンピューティングデバイス（たとえばアクセスマネージャサーバ）によって実現されてもよく、それは、スケーラビリティおよび高可用性を可能にする。アクセスマネージャサーバクラスタを有する、そのような地理的に分散した複数のデータセンターは、マルチデータセンター（multi-data center：ＭＤＣ）システムを構成するために（有線または無線で）接続され得る。ＭＤＣシステムは、企業コンピュータネットワーク内のアクセスサーバの高可用性、負荷分散、および障害復旧要件を満たし得る。ＭＤＣシステムは、アクセス管理システム１４０のためのＳＳＯサービスをサポートするための単一の論理アクセスサーバとして機能してもよい。

【００３６】

アクセス管理システム１４０は、少なくとも１つのメモリと、１つ以上の処理部（またはプロセッサ）と、ストレージとを含んでいてもよい。処理部は、ハードウェア、コンピュータ実行可能命令、ファームウェア、またはそれらの組合せで適宜実現されてもよい。いくつかの実施形態では、アクセス管理システム１４０は、いくつかのサブシステムおよび／またはモジュールを含んでいてもよい。たとえば、アクセス管理システム１４０は、

セッションエンジン１４２と、認可エンジン１４４と、システム検証マネージャ１４６と、個人情報ハンドラ１４８とを含んでいてもよく、それらは各々、ハードウェア、ハードウェア上で実行されるソフトウェア（たとえば、プログラムコード、プロセッサによって実行可能な命令）、またはそれらの組合せで実現されてもよい。いくつかの実施形態では、ソフトウェアは、メモリ（たとえば、非一時的なコンピュータ読取可能媒体）、メモリデバイス、または何らかの他の物理メモリに格納されてもよく、１つ以上の処理部（たとえば、１つ以上のプロセッサ、１つ以上のプロセッサコア、１つ以上のＧＰＵなど）によって実行されてもよい。処理部のコンピュータ実行可能命令またはファームウェア実現化例は、ここに説明されるさまざま動作、機能、方法、および／またはプロセスを行なうように任意の好適なプログラミング言語で書かれたコンピュータ実行可能命令またはマシン実行可能命令を含んでいてもよい。メモリは、処理部上でロード可能および実行可能なプログラム命令、ならびに、これらのプログラムの実行中に生成されたデータを格納してもよい。メモリは、揮発性（ランダムアクセスメモリ（random access memory：ＲＡＭ）など）および／または不揮発性（読出専用メモリ（read-only memory：ＲＯＭ）、フラッシュメモリなど）であってもよい。メモリは、コンピュータ読取可能記憶媒体といった、任意のタイプの持続的記憶装置を使用して実現されてもよい。いくつかの実施形態では、コンピュータ読取可能記憶媒体は、悪質なコードを含む電子通信からコンピュータを保護するように構成されてもよい。コンピュータ読取可能記憶媒体は、その上に格納された命令を含んでいてもよく、命令は、プロセッサ上で実行されると、ここに説明される動作を行なう。

【００３７】

図１は、認証プロセスが起動される前に、ユーザ１０２（たとえば、クレデンシャル情報を提出するユーザ）が、アクセス管理システム１４０を検証するためにアクセス管理システム１４０との通信に従事することができる一例を示す。この例では、クライアントデバイス１０４を操作するユーザ１０２は、アプリケーション１０８などのリソース、たとえば、アプリケーション１２０またはアプリケーション１２０を通してアクセス可能なリソースのうちのいずれか１つへのアクセスを試みてもよい。ユーザ１０２についてのクレデンシャル情報の認証が成功すると、アプリケーション１２０はユーザ１０２にとってアクセス可能になってもよい。アプリケーション１２０のうちの１つがクライアントデバイス１０４でユーザ１０２にとってアクセス可能になる前に、ユーザ１０２は、アプリケーション１２０へのアクセスをユーザ１０２に提供するセッションのために認証されてもよい。クライアントデバイス１０４は、アクセス管理システム１４０からアクセスを要求することによって認証プロセスを起動してもよい。認証プロセスは、クライアントデバイス１０４が、ユーザのクレデンシャル情報を受信するための１つ以上のＧＵＩを表示すること、および、認証要求をアクセス管理システム１４０へ提出することを含んでいてもよい。認証は、ユーザ１０２のクレデンシャル情報の立証に基づいて確立されてもよい。

【００３８】

アプリケーションへのアクセスを試みる際に、ユーザ１０２は、アクセス管理システム１４０を介してユーザのアカウントへのアクセスを管理するアプリケーション（たとえばアプリケーション１０８）を動作させてもよい。たとえば、アプリケーション１０８は、図６～９に示すものなどのＧＵＩを提示し得るアクセス管理アプリケーションである。アプリケーション１０８を使用して、ユーザ１０２は、アクセス管理システム１４０の真正性（すなわち、アクセス管理システム１４０がユーザ１０２の認証を担当しているか）を判断するための検証プロセスを起動してもよい。検証プロセスは、クライアントデバイス１０４からアクセス管理システム１４０への１回以上の通信１３０（「ユーザ検証通信」）を含んでいてもよい。検証プロセスは、アクセス管理システム１４０から、検証プロセスを起動するユーザに関連付けられた１つ以上のクライアントデバイス、たとえばクライアントデバイス１０４への１回以上の通信１３２（「システム検証通信」）を含んでいてもよい。検証プロセスのいくつかの実施形態を、以下にさらに説明する。

【００３９】

クライアントデバイス１０４とアクセス管理システム１４０との間の通信は、ゲートウェイシステムを通して受信され得る。ゲートウェイシステムは、アクセス管理サービスをサポートしてもよい。たとえば、クライアントおよびアクセス管理システム１４０からの要求を平衡化し、および／または扱うために、シングルサインオン（ＳＳＯ）ゲートウェイが、エージェント１０６（たとえばウェブゲートエージェント）などの１つ以上のアクセスエージェントを実現してもよい。

【００４０】

少なくとも１つの実施形態では、検証プロセスは、アプリケーション１０８においてユーザ１０２によって起動されてもよい。アプリケーション１０８は、ユーザ１０２にクレデンシャル情報の入力を促す（プロンプト）ＧＵＩを提示してもよい。ユーザがもはや認証されない場合、クレデンシャル情報が要求されてもよい。セッションが無いこと、またはセッションの失効が、保護されるリソースのためにユーザ１０２からクレデンシャル情報を要求するよう、アクセス管理システム１４０を促してもよい。アプリケーション１０８は、ユーザ１０２がクレデンシャル情報を提供する前にアクセス管理システム１４０の検証を要求できるようにするＧＵＩを提示してもよい。システム検証要求が起動されると、アクセス管理システム１４０の検証を起動するために、ユーザ検証通信１３０（たとえばシステム検証要求）がクライアントデバイス１０４からアクセス管理システム１４０へ送信されてもよい。具体的には、システム検証は、アクセス管理システム１４０についての認証を扱うコンピューティングシステムの真正性を判断してもよい。

【００４１】

システム検証要求を受信すると、アクセス管理システム１４０のシステム検証マネージャ１４６は、システム検証を管理してもよい。システム検証マネージャ１４６は、ユーザ１０２による立証のための一時アクセス情報（たとえばワンタイムパスワード）を判断してもよい。一時アクセス情報は、１つ以上の基準（たとえば時間）によって制約されてもよい。一時アクセス情報の例は、パスワード、コード、トークン、キー、または、１つ以上の基準によって制約される他の情報を含んでいてもよい。一時アクセス情報は、システム検証要求を受信すると生成されてもよく、または、前もって生成されてもよい。アクセス管理システム１４０は、一時アクセス情報をデータストア１６０（「一時パスワード」）に格納してもよい。

【００４２】

システム検証マネージャ１４６は、システム検証通信１３２における一時アクセス情報を、ユーザ１０２によって受信されるようにクライアントデバイス１０４へ送信してもよい。ユーザ１０２は、一時アクセス情報を用いてユーザ検証通信１３０をアクセス管理システム１４０へ送信するように、クライアントデバイス１０４を操作することができる。アクセス管理システム１４０は、ユーザによって送り返された一時アクセス情報を立証して、それが以前にユーザ１０２へ送信されたものと一致するかどうかを判断することができる。

【００４３】

アクセス管理システム１４０の個人情報ハンドラ１４８は、ユーザのみによって知られているかまたはアクセス可能であり得る個人情報を生成してもよい。いくつかの実施形態では、個人情報は、検証されているアクセス管理システムの一部ではない第三者ソース（たとえば、金融システム、または個人情報を提供するシステム）のために取得されてもよい。ユーザ１０２は、前もってアクセス管理システム１４０に登録してもよく、１つ以上のソース、たとえば第三者システムから個人情報にアクセスするための情報を提供する。個人情報は、ユーザに関連付けられた最近の情報を含んでいてもよく、当該情報には、当該情報にアクセスする特権を有していない無認可ユーザはアクセスできないであろう。個人情報は、データストア、たとえばデータストア１７０（「個人情報」）に格納されてもよい。最近の個人情報は、たとえば、現在の金融記録（たとえば銀行記録）から取得された金融情報を含んでいてもよい。個人情報が現在の記録に基づくことを保証するために、個人情報ハンドラ１４８は、システム検証マネージャ１４６が一時アクセス情報を立証し

た後に個人情報を判断してもよい。

【００４４】

システム検証マネージャ１４６は、個人情報を含むシステム検証通信１３２をクライアントデバイス１０４へ送信してもよい。クライアントデバイス１０４は、個人情報を表示するためのインターフェイスを提示してもよく、そのインターフェイスを使用して、ユーザ１０２は、個人情報が正しいかどうかを示すことができる。個人情報が正しいことをユーザが示す場合、インターフェイスは、ユーザの認証を判断するためにクレデンシャル情報を受け付けてもよい。個人情報が正しくない場合、ユーザはそう示すことができ、クレデンシャル情報を提供しないと選択することができる。このため、個人情報の立証は、アクセス管理システム１４０が真正かどうかをユーザ１０２が判断できるようにする。個人情報が正しくない場合、ユーザ１０２は、アクセス管理システム１４０が真正ではないと判断することができ、それにより、ユーザがおそらく無認可のコンピューティングシステムへクレデンシャル情報を分配することが防止される。

【００４５】

クレデンシャル情報の認証成功に基づいて、リソース（たとえばアプリケーション１２０）がユーザ１０２にとってアクセス可能になってもよい。クレデンシャル情報を受信すると、セッションエンジン１４２は、要求されたリソース、たとえばアプリケーション１２０が、アクセスのためにクレデンシャルを必要とする保護（プロテクト）されたリソースかどうかを立証してもよい。セッションエンジン１４２は認可エンジン１４４に、リソースへのアクセスが保護されているかどうかを判断するよう要求してもよい。リソースへのアクセスが保護されていないと判断されると、セッションエンジン１４２は、リソースへのアクセスを与えてもよい。リソースへのアクセスが保護されていると判断されると、セッションエンジン１４２は、クレデンシャル情報に基づいてユーザ１０２の認証を判断してもよい。ユーザ１０２の認証が判断されると、認可エンジン１４４は、ユーザ１０２に許可されたアクセスに基づいて、ユーザ１０２がリソースへのアクセスを認可されているかどうかを判断してもよい。セッションエンジン１４２は、リソースへのアクセスがユーザ１０２によって許可されているかどうかを示すように、クライアントデバイス１０４へ通信を送信してもよい。アクセスが許可されているかどうかに基づいて、アプリケーション１０８がユーザ１０２にとってイネーブルにされてもよい。

【００４６】

アクセス管理システム１４０は、リソースへのアクセスの管理（たとえば、アクセスを与える／拒否すること）、自動サインオン、アプリケーションパスワード変更およびリセット、セッション管理、アプリケーションクレデンシャルプロビジョニング、ならびにセッションの認証を含む多くのＳＳＯサービスを提供してもよい。いくつかの実施形態では、アクセス管理システム１４０は、実行されている、またはクライアントデバイスからアクセスされている、ウィンドウズ（登録商標）アプリケーション、ウェブアプリケーション、Ｊａｖａ（登録商標）アプリケーション、およびメインフレーム／端末ベースのアプリケーションといったアプリケーション１２０のために、自動シングルサインオン機能性を提供することができる。上述のように、アクセス管理システム１２０は、クライアントデバイス（たとえばクライアントデバイス１０４）を操作するユーザ（たとえばユーザ１０２）の認証を行なってもよい。認証とは、ユーザを立証してユーザが本人であると判断するプロセスである。

【００４７】

いくつかの実施形態では、アクセス管理システム１４０は、リソースへのアクセスを制御するために、データストア１８０（「ポリシー」）に格納された１つ以上のポリシーを使用してもよい。ポリシー１８０は、所与のリソースについてアクセスが提供されるべきユーザを認証するために使用される認証技法を特定する認証ポリシーを含んでいてもよい。ポリシー１８０は、リソースアクセスが保護されるべき方法（たとえば、暗号化のタイプなど）を規定する。ポリシー１８０は、ユーザまたはユーザグループがリソースへのアクセスを有する条件を特定する認可ポリシーを含んでいてもよい。たとえば、アドミニス

トレータが、グループ内の特定のユーザのみが特定のリソースにアクセスすることを認可してもよい。アクセス管理システム１４０は、ポリシー１８０のうちの１つ以上に基づいて、ＳＳＯセッションについての認証を判断してもよい。

【００４８】

アクセス管理システム１４０はまた、追加ストレージを含むかまたは追加ストレージに結合されてもよく、追加ストレージは、メモリ記憶装置または他の非一時的なコンピュータ読取可能記憶媒体といった、任意のタイプの持続的記憶装置を使用して実現されてもよい。いくつかの実施形態では、ローカルストレージは、１つ以上のデータベース（たとえば、文書データベース、リレーショナルデータベース、または他のタイプのデータベース）、１つ以上のファイルストア、１つ以上のファイルシステム、もしくはそれらの組合せを含むかまたは実現してもよい。たとえば、アクセス管理システム１４０は、一時パスワード１６０、個人情報１７０、およびポリシー１８０などのデータを格納するための１つ以上のデータストアに結合されるかまたは当該１つ以上のデータストアを含む。メモリおよび追加ストレージはすべて、コンピュータ読取可能記憶媒体の例である。たとえば、コンピュータ読取可能記憶媒体は、コンピュータ読取可能命令、データ構造、プログラムモジュール、または他のデータといった情報を格納するための任意の方法または技術で実現された、揮発性または不揮発性のリムーバブルまたは非リムーバブル媒体を含んでいてもよい。

【００４９】

セッションエンジン１４２は、リソースにアクセスするためにユーザ１０２にとって有効なセッションが存在するかどうかを判断するための処理を扱ってもよい。セッションエンジン１４２は、保護されている要求されたリソースにアクセスするためにユーザ１０２にとって有効なセッションについてチェックする。セッションエンジン１４２は、ユーザ１０２に適用可能な１つ以上のアクセスポリシーの検討に基づいて、ユーザ１０２にとってのセッションの有効性を査定してもよい。ユーザ１０２にとって有効なセッションが存在しないという判断に基づいて、セッションエンジン１４２は、ユーザ１０２からクレデンシャル情報（「クレデンシャル」）を要求してもよい１０８。クレデンシャル情報の認証成功は、要求されたリソースを含み得る１つ以上のリソースへのアクセスをユーザに提供してもよい。

【００５０】

要求がクライアントデバイス１０４へ通信されてもよく、クライアントデバイス１０４はそれに応答して、ユーザ１０２に、セッションの認証を判断するためのユーザクレデンシャルの入力を促す。要求は、クレデンシャル情報を受信するためのウェブページまたはユーザインターフェイス（たとえば、ウェブページ、ポータル、またはダッシュボード）への情報（たとえばＵＲＬ）を含んでいてもよい。要求はクライアントデバイス１０４へ通信されてもよく、クライアントデバイス１０４はそれに応答して、ユーザ１０２に、セッションの認証を判断するためのユーザクレデンシャルの入力を促す。

【００５１】

セッションエンジン１４２は、ユーザ１０２についてのクレデンシャル情報を認証するための動作を行なってもよい。いくつかの実施形態では、セッションエンジン１４２は、ユーザの認証成功で確立されたセッションについての情報を格納してもよい。あるＳＳＯセッション（たとえばＳＳＯ認証セッション）について、そのＳＳＯセッションは、ユーザについてのクレデンシャル情報の認証成功に基づいて、ユーザにとってアクセス可能なすべてのリソースへのアクセスを可能にするＳＳＯセッションとして管理されてもよい。

【００５２】

いくつかの実施形態では、セッションエンジン１４２は、認証の範囲に関して認可エンジン１４４と通信してもよい。認可エンジン１４４は、保護されているリソースを判断できるとともに、認証セッション１５０に基づいて、あるセッションについて許可および／または制限されたリソースを判断できる。

【００５３】

いくつかの実施形態では、アクセス管理システム１４０は、アクセス管理システム１４０用に実現されたアクセスマネージャサーバのうちの任意の１つとクライアントデバイス１０４との間の通信のためのエージェント－サーバモデルに従って、システム１００で実現されてもよい。エージェント－サーバモデルは、エージェントコンポーネント（たとえばゲートウェイシステム）と、サーバコンポーネントとを含んでいてもよい。エージェントコンポーネントは、ホストシステム上にデプロイメントされてもよく、サーバコンポーネントは、サーバ、たとえばアクセスマネージャサーバ上にデプロイメントされてもよい。クライアントデバイス１０４を操作するユーザ１０２は、企業コンピュータネットワークを使用して、エージェント１０６を介してアクセス管理システム１４０と通信してもよい。クライアントデバイス１０４は、ワークステーション、パーソナルコンピュータ（ＰＣ）、ラップトップコンピュータ、スマートフォン、ウェアラブルコンピュータ、または他のネットワーク化された電子デバイスであってもよい。

【００５４】

エージェント１０６はアクセス制御を提供してもよく、また、アクセス管理システム１４０、およびアクセス管理システム１４０を通してアクセス可能な任意のリソースを、外部および内部ウェブベースの脅威から保護するように動作してもよい。アクセス管理システム１４０は、１つ以上のリソース、たとえばアプリケーション１２０へのアクセスを提供する、１つ以上のリソースコンピューティングシステム（たとえばリソースサーバ）と通信してもよい。エージェント１０６は、アクセス管理システム１４０のエージェントコンポーネントを実現するかまたは当該エージェントコンポーネントとして動作してもよく、また、サーバコンポーネントとして動作するサーバを含んでいてもよい。アクセス管理システム１４０によってアクセス可能な各リソースは、エージェント、たとえばエージェント１０６を通して保護されてもよい。エージェント１０６は、それによって保護された１つ以上のリソースについてのユーザ要求を傍受して、ユーザを認証するためにユーザクレデンシャルについてチェックしてもよい。エージェントは次に、アクセス管理システム１４０で、サーバ、たとえばアクセスマネージャサーバに連絡してもよい。アクセス管理サーバは、リソースが、アクセスのためにクレデンシャルを必要とする保護されたリソースかどうかを立証してもよい。リソースが保護されていないとアクセス管理サーバが判断した場合、エージェント１０６はユーザ１０２にアクセスを与えてもよい。リソースが保護されている場合、エージェント１０６はユーザ１０２に認証クレデンシャルを提供するよう要求してもよい。

【００５５】

いくつかの実施形態では、エージェント１０６とアクセス管理システム１４０との間の通信は、２つの異なる通信チャネルへと分割されてもよい。たとえば、前方チャネルを介する通信は、ハイパーテキスト転送プロトコルセキュア（hypertext transfer protocol secure：ＨＴＴＰＳ）プロトコルを使用してもよい。前方チャネル通信は、認証用のクレデンシャル収集動作のための通信といった、それほど頻繁でない通信を含んでいてもよい。後方チャネルを介する通信は、オープンアクセスプロトコル（open access protocol：ＯＡＰ）を使用してもよい。後方チャネル通信は、アクセス管理システム１４０によって管理されるリソースへのアクセス要求を含む、エージェントとサーバとの対話といった、より頻繁な通信を含んでいてもよい。各チャネルは、チャネルを通した通信のタイプ用に設計されたアクセストークンを使用して通信してもよい。アクセスフローは、２つのタイプのブラウザトークンを生成してもよい。第１のトークンはアクセス管理ＩＤトークン（たとえば、OAM_IDトークン）であり、それは、ＨＴＴＰを通して伝搬されているＳＳＯ要求を送達する。第２のトークンは、ＯＡＰを通して伝搬されているＳＳＯ要求を送達するために使用され得る認可トークン（たとえば、OAMAuthnトークン）である。ブラウザトークンは、クライアントデバイス１０４でホストクッキーとして格納されてもよい。

【００５６】

アクセス管理システム１４０は（たとえばエージェント１０６を使用して）、課題の形をした認証クレデンシャルについての要求を（たとえば、クライアントデバイス１０４で

のユーザのウェブブラウザを介して）ユーザ１０２に提示してもよい。いくつかの実施形態では、ユーザ１０２は、クライアントデバイス１０４上で実行されるクライアントを通して、またはクライアントデバイス１０４上のウェブブラウザを通して、ＳＳＯユーザインターフェイスにアクセスすることができる。ＳＳＯユーザインターフェイスは、アクセス管理システム１４０で実現されてもよい。アクセス管理システム１４０は、ＳＳＯユーザインターフェイス、またはＳＳＯユーザインターフェイスへのアクセスを可能にする情報（たとえばＵＲＬ）を、要求１０８を用いて送信してもよい。

【００５７】

いくつかの実施形態では、ＳＳＯユーザインターフェイスは、ユーザ１０２が通常利用するアプリケーションのリストを含み得る。ユーザ１０２は、ＳＳＯユーザインターフェイスを通して、アプリケーションに関連付けられた自分のクレデンシャルおよびポリシーを管理することができる。ユーザ１０２がＳＳＯユーザインターフェイスを通して、あるアプリケーション、たとえばアプリケーション１４０へのアクセスを要求すると、ユーザ１０２に適用可能な１つ以上のポリシー１８０からそのアプリケーション用のポリシータイプを判断するために、要求がクライアントデバイス１０４からアクセス管理システム１４０へ送信されてもよい。アクセス管理システム１４０は、ユーザにとって有効なセッションが存在するかどうかを判断してもよく、存在する場合、それは次に、ポリシータイプに基づいてユーザ１０２のクレデンシャル情報を判断することができる。

【００５８】

いくつかの実施形態では、要求は、ユーザ１０２がクレデンシャルの検索を認可されているかどうかを判断するために使用され得る、以前のログインからの認証クッキーを含んでいてもよい。認可されている場合、ユーザは、クレデンシャルを使用してアプリケーションにログインすることができる。いくつかの実施形態では、エージェント１０６は、ユーザが、アクセス管理システムによって提供されるＳＳＯサービスを使用してアプリケーション１２０にアクセスできるようにすることができる。アクセスは、まずＳＳＯユーザインターフェイスにアクセスしたり、またはクライアントデバイス１０４上で実行されるクライアントを使用したりすることなく、ウェブブラウザを通して直接提供されてもよい。ユーザ１０２が認可されていない場合、アクセス管理システムは、ユーザ１０２からクレデンシャルを要求してもよい１０８。ＳＳＯユーザインターフェイスは、クレデンシャル情報を含む入力を受信するためのインターフェイスを提示してもよい。クレデンシャル情報は、ユーザ１０２の認証を判断するためにアクセス管理システム１４０へ送信されてもよい１１０。

【００５９】

いくつかの実施形態では、オラクル・アクセス・マネジメント（Oracle Access Management）によって保護されたリソース、連合アプリケーション／リソース、およびフォーム記入アプリケーションといった、クレデンシャルタイプがサポートされ得る。クレデンシャルタイプの例は、スマートカード／近接型カード、トークン、公開キーインフラストラクチャ（public key infrastructure：ＰＫＩ）、ウィンドウズ・ログオン（Windows Logon）、軽量ディレクトリアクセスプロトコル（lightweight directory access protocol：ＬＤＡＰ）ログオン、生体認証入力などを含んでいてもよい。ＯＡＭによって保護されたリソースについては、ユーザ要求が認証され、次に、要求されたリソースに関連付けられたＵＲＬへ向けられ得る。連合アプリケーションについては、企業間（business to business：Ｂ２Ｂ）パートナーアプリケーションおよびＳａａＳアプリケーションを含む、連合パートナーおよびリソースへのリンクが提供され得る。フォーム記入アプリケーションについては、クレデンシャルがそれを通して提出され得るアプリケーションウェブページのフィールドを識別するために、テンプレートが使用され得る。

【００６０】

いくつかの実施形態では、認証クレデンシャルを提供するための入力を受信するＳＳＯユーザインターフェイスは、システム検証を起動するための１つ以上の対話型エレメントを含んでいてもよい。インターフェイスの例は、図６～９を参照して説明されるものを含

んでいてもよい。

【００６１】

ここで図２を参照して、ユーザ１０２がアクセス管理システム１４０の真正性を検証するためのプロセスを起動することができるシステム２００が示される。図２に示す例は、図１のエレメントを含んでいてもよい。システム２００によって示された例では、アクセス管理システム１４０の真正性を検証することは、アクセス管理システム１４０とアクセス管理システム１４０の検証を起動するクライアントデバイス１０４との間の１回以上の通信によって、および、アクセス管理システム１４０とクライアントデバイス２１０などの１つ以上の宛先との間の１回以上の通信によって、容易にされてもよい。宛先は、クライアントデバイス１０４に物理的に位置していなくてもよい。宛先は、データがそこで通信および／または受信され得る、電子メールアドレスまたは電話番号などの位置に対応していてもよい。宛先は、ユーザがアクセス管理システム１４０の検証を容易にすることができるように、クライアントデバイス１０４を操作するユーザにとってアクセス可能であってもよい。宛先は、ユーザが、アクセス管理システム１４０から情報を受信すること、および／またはアクセス管理システム１４０へ情報を送信することができるようにしてもよい。

【００６２】

宛先との通信は、当該通信が、クライアントデバイス１０４に位置していないデバイスとの通信であるように、および／または、クライアントデバイス１０４との通信とは異なる通信メカニズムが使用されるように、帯域外であると考えられてもよい。宛先との通信は、無認可ユーザがアクセス管理システム１４０の検証に使用される情報へのアクセスを取得することを防止するように、アクセス管理システム１４０の検証のための情報の安全な通信を可能にしてもよい。少なくとも１つの実施形態では、アクセス管理システム１４０の検証は、アクセス管理システム１４０が１回以上の通信２０２（「システム検証通信」）を１つ以上の宛先、たとえばクライアントデバイス２１０へ送信することを含んでいてもよい。アクセス管理システム１４０の検証は、宛先が１回以上の通信２０４（「ユーザ検証通信」）をアクセス管理システム１４０へ送信することを含んでいてもよい。

【００６３】

少なくとも１つの例では、アクセス管理システム１４０は、アクセス管理システム１４０の検証の一部として一時アクセス情報および／または個人情報などの情報を提供するために、１回以上のシステム検証通信２０２をクライアントデバイス２１０へ送信してもよい。クライアントデバイス１０４を操作するユーザは、情報の受信を確認するために、宛先にアクセスし、ユーザ検証通信２０４をアクセス管理システムへ送信することができる。ユーザは、アクセス管理システム１４０からの情報を取得するために宛先にアクセスし、宛先から取得された情報を用いてクライアントデバイス１０４からアクセス管理システム１４０へ応答することができる。このように、無認可ユーザがアクセス管理システム１４０の検証のための情報を取得することを防止するとは言わないまでも減少させるように、情報がアクセス管理システム１４０とユーザとの間で安全に通信され得る。クライアントデバイス１０４および宛先の使用はさらに、検証のための情報が受信および／または立証されることを保証する。いくつかの実施形態では、クライアントデバイス２１０などの宛先でのアプリケーション２０８は、アクセス管理システム１４０の検証のための情報の通信を容易にするためのインターフェイスを提供してもよい。

【００６４】

いくつかの実施形態では、アクセス管理システム１４０は、クライアントデバイス１０４を操作するユーザがアクセス管理システム１４０の検証のための１つ以上の宛先を登録できるようにする登録プロセスをサポートしてもよい。登録は、宛先についての情報を格納することを含んでいてもよい。登録された各宛先は、宛先を登録するユーザのユーザ識別情報とともに格納されてもよい。アクセス管理システム１４０は、ユーザによって提供されるユーザ識別情報に基づいて宛先を識別してもよい。ユーザは、アクセス管理システム１４０が基準に従って宛先と通信するように、宛先についての１つ以上の基準（たとえ

ば時間）を特定してもよい。ここで図３および図４を参照して、アクセス管理システム１４０の検証の例を示す。

【００６５】

いくつかの実施形態では、図３～９を参照して説明されるものなどは、フローチャート、フロー図、データフロー図、構造図、シーケンス図、またはブロック図として示されるプロセスとして説明され得る。シーケンス図またはフローチャートは動作を逐次プロセスとして説明し得るものの、動作の多くは並行して、または同時に行なわれてもよい。加えて、動作の順序は並べ替えられてもよい。プロセスは、その動作が完了すると終了するが、図面に含まれない追加のステップを有していてもよい。プロセスは、方法、機能、手順、サブルーチン、サブプログラムなどに対応してもよい。プロセスが機能に対応する場合、その終了は、その機能が呼出機能または主機能に戻ることに対応してもよい。

【００６６】

図３～９を参照して説明されるものなどの、ここに示されるプロセスは、１つ以上の処理部（たとえばプロセッサコア）によって実行されるソフトウェア（たとえば、コード、命令、プログラム）、ハードウェア、またはそれらの組合せで実現されてもよい。ソフトウェアは、メモリ（たとえば、メモリデバイス上、非一時的なコンピュータ読取可能記憶媒体上）に格納されてもよい。いくつかの実施形態では、ここにフローチャートで示されたプロセスは、アクセス管理システム、たとえば図１および図２のアクセス管理システム１４０のコンピューティングシステムによって実現され得る。この開示における特定の一連の処理ステップは、限定的であるよう意図されてはいない。代替的な実施形態に従って、他の順序のステップも行なわれてもよい。たとえば、本発明の代替的な実施形態は、上に概説されたステップを異なる順序で行なってもよい。また、図に示された個々のステップは、個々のステップへさまざまな順序で適宜行なわれ得る複数のサブステップを含んでいてもよい。図３～９に示される処理は単一のリソースへのアクセスに関して説明され得るが、そのような処理は複数のリソースのために行なわれてもよく、リソースがアクセスされるたびに、および／または、リソースへのアクセスのためにユーザの認証が判断される必要があるたびに、アクセス管理システムのコンピューティングシステムの検証が必要とされ得るようになっている。図３～９に示される処理は複数のセッションに関して説明されてもよく、それらの各々について、アクセス管理システムのコンピューティングシステムの検証が必要とされてもよい。さらに、特定のアプリケーションに依存して、追加のステップが追加または除去されてもよい。当業者であれば、多くの変形、修正、および代替物を認識するであろう。

【００６７】

いくつかの実施形態の一局面では、図３～９における各プロセスは、１つ以上の処理部によって行なわれ得る。処理部は、シングルコアまたはマルチコアプロセッサ、プロセッサの１つ以上のコア、またはそれらの組合せを含む、１つ以上のプロセッサを含んでいてもよい。いくつかの実施形態では、処理部は、グラフィックスプロセッサ、デジタル信号プロセッサ（digital signal processor：ＤＳＰ）などといった、１つ以上の専用コプロセッサを含み得る。いくつかの実施形態では、処理部のうちのいくつかまたはすべては、特定用途向け集積回路（application specific integrated circuit：ＡＳＩＣ）、またはフィールドプログラマブルゲートアレイ（field programmable gate array：ＦＰＧＡ）といった、カスタマイズされた回路を使用して実現され得る。

【００６８】

図３～４は、一実施形態に従った、ユーザがアクセス管理システム（たとえばアクセス管理システム１４０）の真正性を検証できるようにするための動作を示すシーケンス図を示す。図３は、ユーザが１つ以上のリソースにアクセスするために操作するクライアントデバイスから、ユーザがアクセス管理システムの真正性を検証できるようにするためのシーケンス図３００を示す。

【００６９】

ステップ３１２から始まって、ユーザは、クライアントデバイス３０２を操作して、ア

クセス管理システムによってアクセスが管理されているリソースへのアクセスを要求する（「要求されたリソース」）。アクセス管理システムのセッションエンジン３０６は、リソースへのアクセスを管理するように構成されてもよい。セッションエンジン３０６は、セッションを確立するためにクライアントデバイス３０２の認証を扱ってもよい。セッションエンジン３０６は、アクセス管理システムのサーバ（たとえば認証サーバ）上で実現されてもよい。たとえば、セッションエンジン３０６は、図１のセッションエンジン１４２を含むかまたは実現してもよい。

【００７０】

上述のように、リソースは、アプリケーション、または、アプリケーションを使用してアクセス可能なリソースであってもよい。図３の例では、クライアントデバイス３０２は、アプリケーション３０４を通してリソースへのアクセスを要求するように操作されてもよい。ステップ３１４で、アプリケーション３０４は、クライアントデバイス３０２によって要求されたリソースについてアクセスを要求してもよい。アプリケーション３０４は、アクセス管理システムと通信することによってアクセスを管理するアクセス管理アプリケーションであってもよい。ユーザは、ユーザの認証のために、アプリケーション３０４を介してアクセスクレデンシャルをアクセス管理システムへ提供することができる。ユーザの認証が成功すると、セッションエンジン３０６はセッション（たとえばＳＳＯセッション）を確立してもよい。セッションは、ユーザがクライアントデバイス３０２から１つ以上のリソースにアクセスできるようにしてもよい。

【００７１】

いくつかの実施形態では、リソースへのアクセスを求める要求は、ウェブゲートなどのエージェントによって扱われてもよい。エージェントは、サーバによって提供されるリソースへのアクセスを保護してもよい。クライアントデバイス３０２は、セッションエンジン３０６と直接、またはエージェントを介して間接的に通信することによって、アクセス管理システム１４０と通信してもよい。エージェントは、それによって保護された１つ以上のリソースについてのユーザ要求を傍受して、要求されたリソースへのアクセスを判断してもよい。エージェントは、アクセス管理システムによって制御されるリソースにアクセスするためのセッションについてユーザを認証するために、ユーザクレデンシャルについてチェックしてもよい。エージェントは、リソースが保護されているかどうかを判断してもよく、また、リソースが保護されている場合、クライアントデバイス３０２からアプリケーション３０４を介してリソースにアクセスできるようにするためにアクティブなセッションが存在するかどうかを判断してもよい。

【００７２】

セッションエンジン３０６は、セッションを確立するためにクライアントデバイス３０２の認証を扱ってもよい。リソースへのアクセスを求める要求を受信すると、ステップ３２０で、セッションエンジン３０６は、リソースにアクセスするために有効なセッションが必要とされるかどうかを判断してもよい。たとえば、セッションエンジン３０６は、リソースへのアクセスが保護されているかどうかを判断してもよい。リソースへのアクセスは、ユーザの認証に基づいていてもよい。セッションエンジン３０６は、有効なセッションがユーザにとってアクティブかどうかを判断してもよい。有効なセッションの存在は、ユーザが認証されたことを示してもよい。セッションエンジン３０６は、アクティブなセッションが、要求されたリソースなどのリソースへのアクセスを可能にするかどうかを判断してもよい。いくつかの実施形態では、認証は、あるリソースに特有であってもよい。いくつかの実施形態では、セッションエンジン３０６は、ユーザに適用可能な１つ以上のアクセスポリシーの検討に基づいて、ユーザにとってのセッションの有効性を査定してもよい。

【００７３】

ステップ３２２で、セッションエンジン３０６は、ユーザが、要求されたリソースへのアクセスを認証されていないと判断してもよい。セッションエンジン３０６は、ユーザにとって有効なセッションが存在しないと判断することによって、ユーザが認証されていな

いと判断してもよい。ユーザがリソースへのアクセスを認証されていないと判断すると、ステップ３３０で、セッションエンジン３０６は、ユーザクレデンシャル情報についての要求をクライアントデバイス３０２へ送信してもよい（「ユーザクレデンシャルについて要求する」）。クライアントデバイス３０２は、クレデンシャル情報についての要求を受信する。いくつかの実施形態では、ステップ３３０からの要求は、アプリケーション３０４を介して受信されてもよい。

【００７４】

ユーザクレデンシャルについての要求に応答して、クライアントデバイス３０２は、クライアントデバイスがクレデンシャル情報を受信できるようにするインターフェイスを提供してもよい。インターフェイスは、アプリケーション、たとえばアプリケーション３０４において提供されてもよい。インターフェイスの一例は、図６を参照して以下に説明される。インターフェイスは、ユーザのクレデンシャルを要求しているシステム（たとえば、セッションエンジン３０６を含むアクセス管理システム）の検証をユーザが要求できるようにするための１つ以上の対話型エレメントを含んでいてもよい。システムの検証を要求するために、インターフェイスは、要求に関連付けられたユーザを識別するユーザクレデンシャル（たとえばユーザ識別情報）をユーザが入力できるようにしてもよい。以下にさらに説明されるように、セッションエンジン３０６は、システムの検証に関連する通信のための宛先を判断するために、ユーザ識別情報を立証してもよい。ステップ３３２で、クライアントデバイス３０２は、システム検証についての要求を受信してもよい。クライアントデバイス３０２は、ユーザ識別情報を受信してもよい。ステップ３４０で、クライアントデバイス３０２は、システム検証についての要求をセッションエンジン３０６へ送信してもよい。要求は、ユーザ識別情報とともに送信されてもよい。

【００７５】

ステップ３５０で、セッションエンジン３０６は、システム検証を要求したユーザがシステム検証を要求できるかどうかを判断してもよい。セッションエンジン３０６は、ユーザ識別情報を立証するためにアクセスすることによって、アクセス管理システムを検証するためのシステム検証プロセスを開始してもよい。セッションエンジン３０６は、ユーザ識別情報が有効である（たとえば、存在する）かどうかを判断し、また、有効であると判断した場合、それがユーザに関連付けられているかどうかを判断することによって、ユーザ識別情報を立証してもよい。セッションエンジン３０６は、ユーザ識別情報を立証するために、アイデンティティ管理システムにアクセスしてもよい。

【００７６】

セッションエンジン３０６がユーザ識別情報を立証すると（すなわち、ユーザ識別情報が有効であると判断し、ユーザ識別情報がユーザに関連付けられていると判断すると）、セッションエンジン３０６は、ユーザ識別情報に関連付けられた通信優先度を、アイデンティティ管理システムから受信してもよい。通信優先度は、システム検証のための一時アクセス情報を受信するように指定された１つ以上の宛先を示してもよい。セッションエンジン３０６は、一時アクセス情報を提供するために宛先と通信することができる。

【００７７】

ステップ３５０で、セッションエンジン３０６は、アクセス管理システムのシステム検証を要求したユーザのための一時アクセス情報（たとえば、ワンタイムパスワード）を判断してもよい。一時アクセス情報は、システム検証のプロセスの一部として使用されてもよい。一時アクセス情報は、アクセス管理システムによって生成されてもよく、および／または、第三者システムから取得されてもよい。いくつかの実施形態では、一時アクセス情報は、システム検証についての要求に先立って生成されてもよい。一時アクセス情報は、一時アクセス情報の使用を制限された期間制限する１つ以上の制約に関連付けられてもよい。

【００７８】

ステップ３５２で、セッションエンジン３０６は、システム検証を要求したユーザへ一時アクセス情報を送信することができる。一時アクセス情報は、ユーザの通信優先度に基

づいて識別された１つ以上の宛先で、ユーザへ送信されてもよい。上述のように、通信優先度は、ユーザ識別情報を使用して検索されてもよい。いくつかの実施形態では、宛先は、システム検証を要求したクライアントデバイス（たとえばクライアントデバイス３０２）を含んでいてもよい。デフォルトにより（たとえば、ユーザが通信優先度を提供しなかった場合）、一時アクセス情報は、システム検証を要求したクライアントデバイス（たとえば３０２）へ送信され得る。一時アクセス情報は、１つ以上の通信システム、たとえばメッセージサービスを使用して、クライアントデバイスへ通信されてもよい。

【００７９】

ステップ３６０で、システム検証を要求したユーザは、クライアントデバイス３０２を操作してもよい。ユーザは、一時アクセス情報を取得するためにクライアントデバイス３０２を操作してもよい。クライアントデバイス３０２は、一時アクセス情報を受信する１つ以上の対話型エレメントを有するインターフェイスを提供してもよい。ユーザは、インターフェイスにおいて一時アクセス情報を提供するためにクライアントデバイス３０２を操作してもよい。クライアントデバイス３０２は、インターフェイスへ提供される一時アクセス情報を受信する。ステップ３６２で、クライアントデバイス３０２は、システム検証についてのプロセスを続けるために、一時アクセス情報をアクセス管理システム（たとえばセッションエンジン３０６）へ送信してもよい。

【００８０】

ステップ３７０で、セッションエンジン３０６は一時アクセス情報を立証してもよい。一時アクセス情報を立証することは、一時アクセス情報の制約が満たされているかどうかを判断することを含んでいてもよい。たとえば、一時アクセス情報が時間制限に関連付けられている場合、セッションエンジン３０６は、その時間制限に基づいて一時アクセス情報が失効したかどうかを判断することができる。制約が満たされていない場合（すなわち、一時アクセス情報が失効した場合）、一時アクセス情報はシステム検証のために受け付けられないかもしれない。一時アクセス情報を立証することは、一時アクセス情報が、ステップ３５２でクライアントデバイス３０２へ送信された一時アクセス情報と一致するかどうかを判断することを含んでいてもよい。一時アクセス情報は、システム検証を要求したユーザのユーザ識別情報と関連付けて格納されてもよい。

【００８１】

さらにステップ３７０で、セッションエンジン３０６は、システム検証の一部として個人情報を判断してもよい。一時アクセス情報が立証されると、個人情報が判断されてもよい。個人情報は、セッションエンジン３０６によって生成されてもよい。いくつかの実施形態では、個人情報は、検証されているアクセス管理システムの一部ではない第三者ソース（たとえば金融システム）のために取得されてもよい。個人情報は、ユーザに関連付けられた最近の情報を含んでいてもよく、当該情報には、ユーザ識別情報の保持者ではないユーザ（たとえば無認可ユーザ）はアクセスできないであろう。最近の情報は、たとえば、現在の金融記録（たとえば銀行記録）から取得された金融情報を含んでいてもよい。個人情報が現在の記録に基づくことを保証するために、セッションエンジン３０６は、一時アクセス情報を立証してから個人情報を判断してもよい。

【００８２】

ステップ３７２で、セッションエンジン３０６は、システム検証を要求したユーザに関連付けられたクライアントデバイスへ個人情報を送信してもよい。クライアントデバイスは、システム検証を要求したクライアントデバイスであってもよい。ユーザに関連付けられていることが知られているクライアントデバイスへ個人情報を送信することにより、セッションエンジン３０６は、個人情報が、個人情報へのアクセスを認可されていないユーザへ送信されないことを確信する。クライアントデバイス３０２を操作するユーザは、個人情報が、認可されたアクセス管理システムとして検証された信頼できるソースからのものであることを確信できる。ステップ３８０で、システム検証を要求したユーザに関連付けられたクライアントデバイスは、立証すべきユーザについての個人情報を表示してもよい。たとえば、個人情報は、インターフェイスに表示されてもよい。システム検証を要求

したクライアントデバイスは、個人情報を受信したクライアントデバイスであり得ると仮定される。個人情報はシステム検証の一部としてアクセス管理システムによって送信されるため、個人情報は、システム検証を要求したユーザに関して正確かつ最新のものであり得る。個人情報は、ユーザがシステム検証を要求した後で、ユーザについての個人情報の最近のクエリに基づいて判断されてもよい。

【００８３】

ステップ３８０で、クライアントデバイス３０２は、個人情報が正しいことを立証するための入力をユーザが提供できるようにするインターフェイスを、ユーザに提示してもよい。個人情報が正しいことが立証されると、クライアントデバイス３０２は、ユーザのユーザ識別情報に対応するクレデンシャル情報を受信するためのインターフェイスを、ユーザに提示してもよい。システム検証プロセスは、個人情報が正確であることが立証されるとユーザがクレデンシャル情報を提出することによって完了してもよい。クライアントデバイス３０２は、検証のために、クレデンシャル情報をセッションエンジン３０６へ送信してもよい（３８２）。

【００８４】

ステップ３９０で、セッションエンジン３０６は、ユーザについてのクレデンシャル情報を立証してもよい。クレデンシャル情報を立証することは、クレデンシャル情報が、ユーザのユーザ識別情報に関連付けられた、以前に確立されたクレデンシャル情報と一致しているかどうかを判断することを含んでいてもよい。クレデンシャル情報が正しいことを立証することに基づいて、ステップ３１２での要求されたリソースへのアクセスが与えられてもよい。ステップ３９２で、セッションエンジン３０６は、要求されたリソースへのアクセスを与えてもよい。アクセスが与えられることを示す情報を格納することによって、アクセスが与えられてもよい。セッションエンジン３０６は、与えられるアクセスについての情報を示すデータをクライアント３０２へ送信してもよい。いくつかの実施形態では、与えられるアクセスについてのデータは、アプリケーション３０４へ送信されてもよい。ステップ３９４で、アプリケーション３０４は、アクセスが与えられたことを示すセッションエンジン３０６からのデータを受信することに基づいて、リソース（たとえばアプリケーション３０４）へのアクセスを可能にしてもよい。

【００８５】

ここで図４を参照して、ユーザが、複数のクライアントデバイスを使用することからアクセス管理システムの真正性を検証できるようにするためのシーケンス図４００が示される。具体的には、シーケンス図４００は、アクセス管理システムのシステム検証が帯域外通信チャネルを使用して容易にされ得ることを示す。たとえば、図３を参照して説明されたシステム検証は、クライアントデバイス３０２から物理的に離れている宛先４１０（「帯域外宛先」）との帯域外通信を追加することによって強化されてもよい。たとえば、宛先４１０は、クライアントデバイス３０２を操作するユーザの制御下にある、クライアントデバイス３０２とは異なるクライアントデバイスであってもよい。宛先４１０はモバイル通信デバイスであってもよく、クライアントデバイス３０２はデスクトップコンピュータであってもよい。帯域外通信は、無認可ユーザ（たとえば、ハッカーまたはアイデンティティ泥棒）が個人情報および一時アクセス情報などの機密情報を取得することを防止するかまたはより困難にすることによって、システム検証プロセスのセキュリティを高め得る。

【００８６】

図３に示す例に基づいて、図４における例は、システム検証の一部としての帯域外宛先との通信を示す。帯域外宛先は、通信で送信された情報を漏洩することなく、ユーザがシステム検証の一部として重要な通信を受信および／または送信できるようにするために有用であり得る。ハッカーは宛先を知らないため、宛先との通信によってセキュリティが高められ得る。そのため、ハッカーは、個人情報および一時アクセス情報などの情報にアクセスしたり、当該情報を傍受したりすることができないであろう。

【００８７】

クライアントデバイス３０２を操作するユーザは、図３および図４に示すシステム検証などのプロセスのいずれかが起こる前に、アクセス管理システムに登録してもよい。ユーザは、システム検証のための１つ以上の宛先についての情報を含む、ユーザについての情報を提供することによって、登録してもよい。宛先についての情報は、ユーザによって制御される１つ以上のクライアントデバイスについてのデバイス情報、およびまたは、他のタイプの宛先についての任意の情報（たとえば、電子メールアカウント情報）を含んでいてもよい。ユーザについての情報は、ユーザ識別情報およびクレデンシャル情報と関連付けて格納されてもよい。いくつかの実施形態では、ユーザは、アクセス管理システムにとってアクセス可能であるアイデンティティ管理システムに情報を登録してもよい。登録は、ユーザが宛先についての情報を提供することを含んでいてもよい。アクセス管理システムは、システム検証のために、システム検証を起動するクライアントデバイス、および／または帯域外宛先のうちの１つ以上を介して、ユーザと通信してもよい。

【００８８】

図４に示す例は、図３と同様のエレメントを含んでいてもよい。クライアントデバイス３０２を操作するユーザは、セッションエンジン３０６を含むアクセス管理システムによって制御されるリソースへのアクセスを要求してもよい。要求されたリソースへのアクセス取得の一部として、ユーザは、アクセス管理システムのシステム検証を起動してもよい。システム検証が起動されると、セッションエンジン３０６は、システム検証プロセスの１つ以上のステップのために、帯域外宛先４１０を介してユーザと通信することができる。

【００８９】

いくつかの実施形態では、ステップ３５０で一時アクセス情報を判断した後に、セッションエンジン３０６は、クライアントデバイス３０２とは異なる１つ以上の宛先へ一時アクセス情報を送信してもよい。たとえば、ステップ４５２で、セッションエンジン３０６は、宛先４１０へ一時アクセス情報（たとえば一時パスワード）を送信してもよい。セッションエンジン３０６は、クライアントデバイス３０２への一時アクセス情報の送信に加えて、または当該送信の代わりに、宛先４１０へ一時アクセス情報を送信してもよい。一時アクセス情報がクライアントデバイス３０２へ送信されない場合、クライアントデバイス３０２を操作するユーザは、宛先４１０から一時アクセス情報を取得しなければならないかもしれない。ステップ４５４で、宛先、仮にデバイスは、一時アクセス情報をクライアントデバイス３０２へ送信することができる。または、宛先４１０がユーザにとってアクセス可能な場合、ユーザは、宛先４１０から一時アクセス情報を取得できてもよい。上述のように、一時アクセス情報は、システム検証プロセスの一部として、ユーザによってアクセス管理システムへ提供される。図４では、ステップ３６０で、クライアントデバイス３０２は一時アクセス情報を入力としてユーザから受信してもよく、または、ステップ４５４で宛先４１０から受信してもよい。

【００９０】

いくつかの実施形態では、システム検証の一部として、アクセス管理システムは、クライアントデバイス３０２への個人情報の送信に加えて、または当該送信の代わりに、１つ以上の帯域外宛先（たとえば宛先４１０）へ個人情報を送信してもよい。たとえば、ステップ３７０で個人情報を生成した後に、セッションエンジン３０６は個人情報を宛先４１０へ送信してもよい。システム検証のためのセキュリティを強化するために、個人情報は、無認可ユーザによるアクセスを防止するために帯域外宛先へ送信されてもよい。無認可ユーザは、宛先の存在に気づかないかもしれず、たとえそうであったとしても、個人情報がシステム検証プロセスに関連することに気づかないかもしれない。いくつかの実施形態では、個人情報は、システム検証を起動するクライアントデバイス３０２と個人情報を受信する１つ以上の宛先との間で共有されてもよい。

【００９１】

システム検証プロセスを続けると、個人情報は、どこで受信されても、それが正しいかどうかを判断するためにユーザによって査定されてもよい。いくつかの実施形態では、シ

ステム検証プロセスは、個人情報が正しいかどうかを示すための入力をユーザが提供できるようにするためのインターフェイス（たとえば、図８のインターフェイス）を提供することを含んでいてもよい。インターフェイスは、クライアントデバイス３０２または宛先４１０でユーザに提示されてもよい。図４の例では、ステップ３８０で、インターフェイスがユーザに提示されてもよい。ステップ３８０で、クライアントデバイス３０２は、クライアントデバイス３０２でのインターフェイスを介して、個人情報の検証を示す入力を受信することができる。

【００９２】

このため、システム検証の一部として１つ以上の宛先を提供することにより、アクセス管理システムのユーザは、システム検証中に無認可ユーザによって漏洩された情報はなかったことを確信できる。

【００９３】

図５は、一実施形態に従った、ユーザがアクセス管理システムの真正性を検証できるようにするためのプロセスのフローチャート５００を示す。いくつかの実施形態では、フローチャート５００に示すプロセスは、図１および図２のアクセス管理システム１４０によって実現されてもよい。

【００９４】

フローチャート５００は、ステップ５０２で、ユーザがクライアントデバイスからのアクセスについて認証されているかどうかを判断することによって始まってもよい。たとえば、アクセス管理システムは、ユーザが、ユーザによって要求されたリソースへのアクセスを認証されているかどうかを判断してもよい。認証は、ある特定のクライアントデバイス、たとえば、ユーザがそこからアクセスを要求するクライアントデバイスからのアクセスについて判断されてもよい。ユーザについての認証は、ユーザによって提供された（たとえば、ユーザによって操作されるクライアントデバイスから受信された）クレデンシャル情報（たとえば、ユーザＩＤおよびパスワード）に基づいて判断されてもよい。ユーザは、クレデンシャル情報の検証に基づいて、クライアントデバイスからのアクセスについて認証されてもよい。

【００９５】

いくつかの実施形態では、アクセス管理システムは、ユーザにとって有効なセッション（たとえばＳＳＯセッション）が存在するかどうかに基づいて、ユーザが認証されているかどうかを判断してもよい。ユーザは、有効なセッションが存在すると判断されると認証されてもよい。いくつかの実施形態では、有効なセッションが存在する場合、アクセス管理システムは、有効なセッションのためにユーザによって要求されたリソースへのアクセスをユーザが有するかどうかを判断してもよい。

【００９６】

ステップ５０４で、要求が、ユーザによって操作されるクライアントデバイスへ送信されてもよい。要求は、ユーザを認証するためのユーザのクレデンシャル情報について送信されてもよい。要求は、ユーザが認証されていない（たとえば、リソースへのアクセスを認証されていない）と判断されると送信されてもよい。

【００９７】

ステップ５０６で、検証要求がクライアントデバイスから受信されてもよい。検証要求は、アクセス管理システムのコンピューティングシステムの認証を要求するために提出されてもよい。認証が要求されるコンピューティングシステムは、ユーザからクレデンシャル情報を要求したのと同じコンピューティングシステムであってもよい。いくつかの実施形態では、ユーザは、図６を参照して以下にさらに説明されるもののようなＧＵＩを通して、検証要求を提出してもよい。ＧＵＩは、ユーザ識別情報を含む入力を受信してもよい。ユーザ識別情報は、検証要求に含まれてもよい。以下にさらに説明されるように、ユーザ識別情報は、アクセス管理システムが一時アクセス情報（たとえばワンタイムパスワード）の通信のための宛先を判断できるようにしてもよい。

【００９８】

ステップ５０８で、ユーザに関連付けられた宛先が識別されてもよい。宛先は、検証要求（たとえば、ステップ５０６で受信された検証要求）におけるユーザ識別情報に基づいて識別されてもよい。ユーザ識別情報は、ユーザＩＤ（たとえばユーザ名）、もしくは、ユーザを一意的に識別する他の情報（たとえば、電話番号または電子メールアドレス）を含んでいてもよい。一例では、アクセス管理システムは、アイデンティティ管理システムから、ユーザ識別情報によって識別されたユーザのプロファイルを検索してもよい。宛先は、ユーザとの通信のための１つ以上の宛先を示すそのプロファイルに基づいて識別されてもよい。宛先は、電子メールアドレス、モバイルデバイスの電話番号、または、情報が送信され得る任意の他の位置を含んでいてもよい。

【００９９】

ステップ５１０で、一時アクセス情報が宛先へ送信されてもよい。宛先は、検証要求におけるユーザ識別情報に基づいて識別されるものであってもよい。一時アクセス情報は、ユーザがコンピューティングシステムを認証するために送信されてもよい。一時アクセス情報は、一時アクセス情報の送信者を確認するためにユーザによって使用されるワンタイムパスワード（ＯＴＰ）であってもよい。一時アクセス情報は、アクセス管理システムのコンピューティングシステムが実際にアクセス管理システムの真正コンピューティングシステムであることをユーザが検証できるようにしてもよい。

【０１００】

アクセス管理システムによって管理されるユーザのアカウントを無認可アクセスから保護するために、アクセス管理システムは、クライアントデバイスとは異なる宛先でユーザと通信してもよい。宛先は、アクセス管理システムの検証を要求するクライアントデバイスから帯域外またはチャネル外であってもよい。宛先は、ユーザにとってアクセス可能なデバイス上にあってもよく、または、（たとえば、メモリにおける位置、または、リモートコンピューティングシステムでアクセス可能な位置で）ユーザにとってアクセス可能であってもよい。宛先は、それが、ユーザのアカウントへのアクセスを偽って得ようとする無認可システムによって知られないように、選択されてもよい。たとえば、宛先は、検証要求を送信するクライアントデバイス（たとえば端末）とは異なるクライアントデバイス（たとえばモバイルデバイス）である。別の例では、宛先は、一時アクセス情報を含む電子メールメッセージが送信され得る電子メールアドレスである。いくつかの実施形態では、宛先は、検証要求を送信してきたのと同じクライアントデバイスである。

【０１０１】

ステップ５１２で、クライアントデバイス（たとえば、検証要求を送信するクライアントデバイス）から応答が受信されてもよい。応答は、宛先へ送信された一時アクセス情報を含んでいてもよい。ユーザは、宛先から一時アクセス情報を取得してもよい。いくつかの実施形態では、宛先からユーザによって取得された一時アクセス情報を受信するために、図７を参照して示されるもののようなＧＵＩが、クライアントデバイスで提示されてもよい。一時アクセス情報は、ＧＵＩからの受信時に応答に含まれていてもよい。

【０１０２】

ステップ５１２で応答において受信された一時アクセス情報は、ステップ５１４で立証されてもよい。アクセス管理システムは、クライアントデバイスから受信された一時アクセス情報が、宛先へ送信された一時アクセス情報と同じであるか、すなわち一致するかどうかを判断してもよい。いくつかの実施形態では、一時アクセス情報は、それが１つ以上の制約（たとえば期間）に関連付けられるように、限定的または一時的であってもよい。一時アクセス情報は、宛先によって受信されるものの、制約が満たされない場合には有効ではないかもしれない。一時アクセス情報を立証することは、一時アクセス情報についての制約が満たされたかどうかを判断することを含んでいてもよい。

【０１０３】

ステップ５１６で、検証要求を送信したクライアントデバイスのユーザについての個人情報が、クライアントデバイスへ送信されてもよい。個人情報は、一時アクセス情報が制約を満たすことが立証されるとクライアントデバイスへ送信されてもよい。アクセス管理

システムの検証の一部として、アクセス管理システムは、ユーザが自分のクレデンシャルをアクセス管理システムへ提供する前にユーザがその真正性を立証できるようにするために、ユーザについての個人情報を提供してもよい。個人情報は、たとえば、ユーザのアカウントへのアクセスを偽って得るように設計されたフィッシングまたはハッキングコンピューティングシステムといった他のコンピューティングシステムにとってアクセスできなかったであろう最新情報を含んでいてもよい。個人情報は、アクセス管理システムによるアクセスについてユーザによって認可された１つ以上のソースによって供給されてもよい。個人情報の例は、金融情報（たとえば、最近の取引、最近の口座残高など）、もしくは、他の個人情報または機密情報を含んでいてもよい。個人情報は、無認可アクセスが起こる可能性が低くなるように、最近更新された情報を含んでいてもよい。

【０１０４】

個人情報は、クライアントデバイスによって受信されると、図８を参照して説明される例のように、クライアントデバイスによってＧＵＩに表示されてもよい。ＧＵＩを通して、ユーザは個人情報を、その真正性を確認するために立証してもよい。ＧＵＩは、ステップ５０６で検証要求とともに受信されたユーザ識別情報に関連付けられたユーザについての個人情報およびクレデンシャル情報（たとえばパスワード）の確認を受信するための１つ以上の対話型エレメントを含んでいてもよい。

【０１０５】

ステップ５１８で、アクセス管理システムの検証を要求したクライアントデバイスから、応答が受信されてもよい。応答は、ステップ５１６で送信された個人情報が正確であるという立証を示すＧＵＩを介して受信された入力に応答して、クライアントデバイスから受信されてもよい。応答は、個人情報を確認したユーザのクレデンシャルデータを含んでいてもよい。クレデンシャルデータは、ステップ５０６で受信されたユーザ識別情報に関連付けられたアカウントにアクセスするためのクレデンシャル情報（たとえばパスワード）を含んでいてもよい。

【０１０６】

ステップ５１８で応答を送信したユーザは、クライアントデバイスからリソースへのアクセスを判断するために認証されてもよい。ユーザは、ステップ５１８で受信されたクレデンシャルデータに基づいて認証されてもよい。クレデンシャルデータは、ユーザのユーザ識別情報についての格納されたクレデンシャル情報と比較され、それらが一致するかどうかが判断されてもよい。クレデンシャルデータが格納されたクレデンシャル情報と一致すると判断されると、ステップ５２０で、ユーザはリソースへのアクセスを認証されてもよい。ユーザが認証されると、ユーザのために、セッションが、リソースにアクセスするためにクライアントデバイスで確立されてもよい。いくつかの実施形態では、ユーザはさらに、ステップ５１８で受信された応答において確認を受信することに基づいて認証されてもよい。ユーザがクライアントデバイスからリソースにアクセスすることを認証されていると判断することに基づいて、アクセスがユーザに与えられてもよい。フローチャートはステップ５２２で終了する。

【０１０７】

図６～９は、一実施形態に従った、ユーザがアクセス管理システムの真正性を検証できるようにするためのインターフェイス（たとえばＧＵＩ）を示す。図６～９のＧＵＩの各々は、アプリケーション、たとえば図１のアプリケーション１０８に表示されてもよい。ＧＵＩ６００は、１つ以上のリソースへのアクセスを管理するアクセス管理アプリケーションによって表示されてもよい。ＧＵＩ６００は、クライアントデバイスによって生成されてもよく、ＧＵＩを生成するアクセス管理システムから受信されてもよく、またはそれらの組合せであってもよい。ＧＵＩ６００は、サービス（たとえばクラウドサービス）、またはネットワークアクセス可能なアプリケーションの一部として、ネットワークを介してアクセス管理システムによって提供されてもよい。少なくとも１つの例では、アクセス管理システムのオペレータは、ＧＵＩ６００と対話するようにクライアントデバイスを操作してもよい。

【０１０８】
ここで図６を参照すると、１つ以上のリソースにアクセスするためのセッション（たとえばＳＳＯセッション）を確立するためにユーザがクレデンシャル情報を入力できるようにするＧＵＩ６００が示される。ＧＵＩ６００は、セッションを提供するアカウントへのアクセスをユーザが得られるようにするための１つ以上の対話型エレメントを含んでいてもよい。たとえば、ＧＵＩ６００は、ユーザ識別情報（たとえばユーザ名）などのクレデンシャル情報を受信するための対話型エレメント６１０を含んでいてもよい。ＧＵＩ６００は、ユーザの認証のためのアクセスプロセス（たとえばログインプロセス）を起動するための入力を受信する対話型エレメント６３０を含んでいてもよい。アクセスプロセスは、ユーザが、アクセス管理システムによって管理されるアカウントにアクセスできるようにしてもよい。アクセスプロセスを起動することにより、図９に関して説明されるＧＵＩが、ユーザ識別情報に関連付けられたユーザによるアクセスを判断するための入力、たとえばクレデンシャル情報（たとえばパスワード）を受信するために表示されてもよい。
【０１０９】
いくつかの実施形態では、ＧＵＩ６００は、ＧＵＩ６００を介してクレデンシャル情報を要求するコンピューティングシステムの真正性を判断するための検証要求を起動するための入力を受信する対話型エレメント６２０を含んでいてもよい。検証要求を起動することにより、ユーザは、クレデンシャル情報を求めるコンピューティングシステムが実際に、クレデンシャル情報に関連付けられたアカウントへのアクセスを管理する真正（たとえば不正でない）システムであるかどうかを判断できるようにされてもよい。
【０１１０】
図７には、ユーザが一時アクセス情報（たとえばワンタイムパスワード）を入力できるようにするＧＵＩ７００が示される。上述のように、一時アクセス情報は、認証プロセスの一部として、アクセス管理システムのコンピューティングシステムからクライアントデバイスによって受信されてもよい。アクセス管理システムは、宛先、たとえば、アクセス管理システムの検証を要求したクライアントデバイスとは異なるデバイスへ一時アクセス情報を送信することによって、その真正性を確立してもよい。アクセス管理システムを検証するためのプロセスの一部として、アクセス管理システムは、クライアントデバイス（たとえば、検証要求を起動したクライアントデバイス）へ、宛先へ送信された一時アクセス情報を受信するよう、要求を送信してもよい。いくつかの実施形態では、クライアントデバイスは、対話型エレメント７１０を介して一時アクセス情報を受信するＧＵＩ７００を表示してもよい。ＧＵＩ７００は、一時アクセス情報をアクセス管理システムへ送信する（たとえば、提出する）ための入力を受信する対話型エレメント７２０を含んでいてもよい。一時アクセス情報は、アクセス管理システムへ提出されてもよい。アクセス管理システムは、一時アクセス情報のユーザの立証を確認することができる。アクセス管理システムは、一時アクセス情報が、宛先へ送信された一時アクセス情報と一致するかどうかを判断するために、一時アクセス情報を立証することができる。
【０１１１】
図８には、ユーザがアクセス管理システムの真正性を判断できるようにするＧＵＩ８００が示される。ＧＵＩ８００は、アクセス管理システムの検証を要求したユーザについての個人情報を表示してもよい。上述のように、アクセス管理システムは、アクセス管理システムの検証を要求するユーザによって操作されるクライアントデバイスへ、ユーザについての個人情報を送信してもよい。ユーザから受信された一時アクセス情報が立証されると、個人情報はユーザへ送信されてもよい。いくつかの実施形態では、個人情報は、アクセス管理システムの真正性を判断するための要求を起動するクライアントデバイスへ送信されてもよい。
【０１１２】
クライアントデバイスは、クライアントデバイスを操作するユーザによる立証のための個人情報を提供するために、ＧＵＩ８００を表示してもよい。個人情報は、アクセス管理システムの真正性を検証するためのプロセスの一部として提供されてもよい。ユーザは、

ＧＵＩ８００によって表示された個人情報を見て、それが正確かどうかを判断してもよい。ＧＵＩ８００は、個人情報が正確かどうかを示すための入力を受信するための１つ以上の対話型エレメントを含んでいてもよい。対話型エレメントは、ユーザが、個人情報の精度を確認するためにアクセス管理システムへ要求を提出できるようにしてもよい。いくつかの実施形態では、ＧＵＩ８００における対話型エレメントは、個人情報が表示されるユーザのアカウントにアクセスするためのアクセス要求（たとえばログイン要求）を送信するための入力を受信してもよい。たとえば、ＧＵＩ８００は、アカウントへのアクセスを要求するための入力を受信する対話型エレメント８２０を含んでいてもよい。対話型エレメント８２０を介して入力を受信すると、アクセス要求がアクセス管理システムへ提出されてもよい。ＧＵＩ８００は、個人情報が表示されるユーザのアカウントにアクセスするためのアクセス情報（たとえばパスワード）を受信するための対話型エレメント８１０を含んでいてもよい。アクセス情報は、図６を参照して説明されたＧＵＩで受信されたユーザ識別情報に対応してもよい。アクセス情報は、アクセス要求とともに、アクセス管理システムへ提出されてもよい。アクセス管理システムは、ＧＵＩ８００を使用して提出されたアクセス情報を立証することに基づいて、アカウントへのアクセスを判断することができる。

【０１１３】

図９は、ユーザに関連付けられたアカウントへのアクセスを要求するためのアクセス情報（たとえばパスワード）をユーザが提供できるようにするＧＵＩ９００を示す。アカウントは、アカウントに関連付けられたユーザＩＤによって識別されてもよい。ユーザ識別情報は、異なるＧＵＩ、たとえば図６を参照して説明されたＧＵＩ６００で提供されてもよい。ＧＵＩ９００は、図６の対話型エレメント６３０との対話によってアクセスプロセスが起動されると表示されてもよい。ＧＵＩ９００は、アカウントについてのクレデンシャル情報を受信するための対話型エレメント９１０を含んでいてもよい。対話型エレメント９２０は、クレデンシャル情報に基づいてログインプロセスを起動するように対話型であり得る。いくつかの実施形態では、ユーザがアクセス管理システムの真正性を検証しないと決めるとＧＵＩ９００が表示されてもよい。いくつかの実施形態では、ユーザがアクセスプロセスのためのクレデンシャル情報を提供するステップの数を減少させるために、ＧＵＩ９００とＧＵＩ６００とが組合されてもよい。

【０１１４】

図１０は、一実施形態を実現するための分散型システム１０００の簡略図を示す。図示された実施形態では、分散型システム１０００は１つ以上のクライアントコンピューティングデバイス１００２、１００４、１００６、および１００８を含み、それらは、１つ以上のネットワーク１０１０を通して、ウェブブラウザ、専用クライアント（たとえば、オラクル・フォームズ（Oracle Forms））などのクライアントアプリケーションを実行し、動作させるように構成される。サーバ１０１２は、ネットワーク１０１０を介して、リモートのクライアントコンピューティングデバイス１００２、１００４、１００６、および１００８と通信可能に結合されてもよい。

【０１１５】

さまざまな実施形態では、サーバ１０１２は、１つ以上のサービスまたはソフトウェアアプリケーションを実行するように適合されてもよい。ある実施形態では、サーバ１０１２は他のサービスも提供してもよく、または、ソフトウェアアプリケーションは非仮想環境および仮想環境を含み得る。いくつかの実施形態では、これらのサービスは、ウェブベースのサービスまたはクラウドサービスとして、もしくはソフトウェア・アズ・ア・サービス（Software as a Service：ＳａａＳ）モデルの下で、クライアントコンピューティングデバイス１００２、１００４、１００６、および／または１００８のユーザに提供されてもよい。クライアントコンピューティングデバイス１００２、１００４、１００６、および／または１００８を操作するユーザは次に、これらのコンポーネントによって提供されるサービスを利用するためにサーバ１０１２と対話するために、１つ以上のクライアントアプリケーションを利用してもよい。

【０１１６】
図１０に示す構成では、システム１０００のソフトウェアコンポーネント１０１８、１０２０および１０２２は、サーバ１０１２上で実現されるとして示されている。他の実施形態では、システム１０００のコンポーネントおよび／またはこれらのコンポーネントによって提供されるサービスのうちの１つ以上も、クライアントコンピューティングデバイス１００２、１００４、１００６、および／または１００８のうちの１つ以上によって実現されてもよい。クライアントコンピューティングデバイスを操作するユーザは次に、これらのコンポーネントによって提供されるサービスを使用するために、１つ以上のクライアントアプリケーションを利用してもよい。これらのコンポーネントは、ハードウェア、ファームウェア、ソフトウェア、またはそれらの組合せで実現されてもよい。分散型システム１０００とは異なり得るさまざまな異なるシステム構成が可能であることが理解されるべきである。図１０に示す実施形態はこのため、実施形態システムを実現するための分散型システムの一例であり、限定的であるよう意図されてはいない。

【０１１７】
クライアントコンピューティングデバイス１００２、１００４、１００６、および／または１００８は、さまざまなタイプのコンピューティングシステムを含んでいてもよい。たとえば、クライアントコンピューティングデバイスは、携帯型ハンドヘルドデバイス（たとえば、ｉＰｈｏｎｅ（登録商標）、携帯電話、ｉＰａｄ（登録商標）、コンピューティングタブレット、携帯情報端末（ＰＤＡ））、またはウェアラブルデバイス（たとえば、グーグル・グラス（Google Glass）（登録商標）頭部装着型ディスプレイ）を含んでいてもよく、マイクロソフト・ウィンドウズ・モバイル（Microsoft Windows Mobile）（登録商標）などのソフトウェア、および／または、ｉＯＳ、ウィンドウズ（登録商標）フォン、アンドロイド（登録商標）、ブラックベリー（登録商標）１０、パームＯＳなどのさまざまなモバイルオペレーティングシステムを実行する。デバイスは、さまざまなインターネット関連アプリ、電子メール、ショートメッセージサービス（short message service：ＳＭＳ）アプリケーションといった、さまざまなアプリケーションをサポートしてもよく、さまざまな他の通信プロトコルを使用してもよい。クライアントコンピューティングデバイスはまた、マイクロソフト・ウィンドウズ（登録商標）、アップル・マッキントッシュ（登録商標）、および／またはＬｉｎｕｘ（登録商標）オペレーティングシステムのさまざまなバージョンを実行するパーソナルコンピュータおよび／またはラップトップコンピュータを例として含む、汎用パーソナルコンピュータを含んでいてもよい。クライアントコンピューティングデバイスは、たとえばグーグル・クローム（Google Chrome）ＯＳなどのさまざまなＧＮＵ／Ｌｉｎｕｘオペレーティングシステムを何ら限定されることなく含む、商業的に入手可能なさまざまなＵＮＩＸ（登録商標）またはＵＮＩＸ様オペレーティングシステムのうちのいずれかを実行するワークステーションコンピュータであり得る。クライアントコンピューティングデバイスはまた、ネットワーク１０１０を通して通信可能である、シンクライアントコンピュータ、インターネット対応ゲーミングシステム（たとえば、Ｋｉｎｅｃｔ（登録商標）ジェスチャー入力デバイスを有する、または有さない、マイクロソフトＸｂｏｘゲーミングコンソール）、および／またはパーソナルメッセージングデバイスといった電子デバイスを含んでいてもよい。

【０１１８】
図１０の分散型システム１０００は４つのクライアントコンピューティングデバイスを有して示されているが、任意の数のクライアントコンピューティングデバイスがサポートされてもよい。センサを有するデバイスなどの他のデバイスが、サーバ１０１２と対話してもよい。

【０１１９】
分散型システム１０００におけるネットワーク１０１０は、ＴＣＰ／ＩＰ（transmission control protocol/Internet protocol：伝送制御プロトコル／インターネットプロトコル）、ＳＮＡ（systems network architecture：システムネットワークアーキテクチャ）、ＩＰＸ（Internet packet exchange：インターネットパケット交換）、アップル・ト

ーク（Apple Talk）などを何ら限定されることなく含む、利用可能なさまざまなプロトコルのうちのいずれかを使用してデータ通信をサポートできる、当業者にはよく知られた任意のタイプのネットワークであってもよい。単なる例として、ネットワーク１０１０は、ローカルエリアネットワーク（local area network：ＬＡＮ）、イーサネット（登録商標）、トークンリング（Token-Ring）に基づくネットワーク、ワイドエリアネットワーク、インターネット、仮想ネットワーク、仮想プライベートネットワーク（virtual private network：ＶＰＮ）、イントラネット、エクストラネット、公衆交換電話網（public switched telephone network：ＰＳＴＮ）、赤外線ネットワーク、無線ネットワーク（たとえば、電気電子技術者協会（the Institute of Electrical and Electronics：ＩＥＥＥ）８０２．１１プロトコルスイート、Bluetooth（登録商標）、および／または任意の他の無線プロトコルのうちのいずれかの下で動作するネットワーク）、ならびに／もしくは、これらのおよび／または他のネットワークの任意の組合せであり得る。

【０１２０】

サーバ１０１２は、１つ以上の汎用コンピュータ、専用サーバコンピュータ（ＰＣ（パーソナルコンピュータ）サーバ、ＵＮＩＸ（登録商標）サーバ、ミッドレンジサーバ、メインフレームコンピュータ、ラックマウントサーバなどを例として含む）、サーバファーム、サーバクラスタ、もしくは任意の他の適切な構成および／または組合せで構成されてもよい。サーバ１０１２は、仮想オペレーティングシステムを実行する１つ以上の仮想マシン、または仮想化を伴う他のコンピューティングアーキテクチャを含み得る。サーバのための仮想記憶装置を維持するために、論理記憶装置の１つ以上の柔軟なプールが仮想化され得る。仮想ネットワークは、ソフトウェア定義ネットワーキングを使用してサーバ１０１２によって制御され得る。さまざまな実施形態では、サーバ１０１２は、前述の開示で説明された１つ以上のサービスまたはソフトウェアアプリケーションを実行するように適合されてもよい。たとえば、サーバ１０１２は、本開示の一実施形態に従った上述のような処理を行なうためのサーバに対応していてもよい。

【０１２１】

サーバ１０１２は、上述のもののうちのいずれかを含むオペレーティングシステム、および商業的に入手可能な任意のサーバオペレーティングシステムを実行してもよい。サーバ１０１２はまた、さまざまな追加のサーバアプリケーションおよび／または中間層アプリケーションのうちのいずれかを実行してもよく、ＨＴＴＰ（hypertext transport protocol：ハイパーテキスト伝送プロトコル）サーバ、ＦＴＰ（file transfer protocol：ファイル転送プロトコル）サーバ、ＣＧＩ（common gateway interface：コモンゲートウェイインターフェイス）サーバ、ＪＡＶＡ（登録商標）サーバ、データベースサーバなどを含む。例示的なデータベースサーバは、オラクル、マイクロソフト、サイベース（Sybase）、ＩＢＭ（International Business Machines：インターナショナル・ビジネス・マシーンズ）などから商業的に入手可能なものを何ら限定されることなく含む。

【０１２２】

いくつかの実現化例では、サーバ１０１２は、クライアントコンピューティングデバイス１００２、１００４、１００６、および１００８のユーザから受信されたデータフィードおよび／またはイベント更新を分析して統合するための１つ以上のアプリケーションを含んでいてもよい。一例として、データフィードおよび／またはイベント更新は、センサデータアプリケーション、金融ティッカー、ネットワーク性能測定ツール（たとえば、ネットワーク監視およびトラフィック管理アプリケーション）、クリックストリーム分析ツール、自動車交通監視などに関連するリアルタイムイベントを含み得る、１つ以上の第三者情報源および連続データストリームから受信されたツイッター（登録商標）フィード、フェースブック（登録商標）更新またはリアルタイム更新を含んでいてもよいが、それらに限定されない。サーバ１０１２はまた、クライアントコンピューティングデバイス１００２、１００４、１００６、および１００８の１つ以上の表示装置を介してデータフィードおよび／またはリアルタイムイベントを表示するための１つ以上のアプリケーションを含んでいてもよい。

【０１２３】
分散型システム１０００はまた、１つ以上のデータベース１０１４および１０１６を含んでいてもよい。これらのデータベースは、本発明の実施形態によって使用される、ユーザ対話情報、使用パターン情報、適合ルール情報、および他の情報などの情報を格納するためのメカニズムを提供してもよい。データベース１０１４および１０１６は、さまざまな位置に存在していてもよい。例として、データベース１０１４および１０１６のうちの１つ以上は、サーバ１０１２に対してローカルな（および／または、サーバ１０１２内にある）非一時的記憶媒体上に存在していてもよい。それに代えて、データベース１０１４および１０１６は、サーバ１０１２からリモートであってもよく、ネットワークベースの接続または専用接続を介してサーバ１０１２と通信してもよい。一組の実施形態では、データベース１０１４および１０１６は、ストレージエリアネットワーク（storage-area network：ＳＡＮ）に存在していてもよい。同様に、サーバ１０１２に帰する機能を行なうための任意の必要なファイルが適宜、サーバ１０１２上にローカルに格納されてもよく、および／またはリモートに格納されてもよい。一組の実施形態では、データベース１０１４および１０１６は、ＳＱＬフォーマットのコマンドに応答してデータを格納し、更新し、検索するように適合された、オラクルによって提供されるデータベースなどのリレーショナルデータベースを含んでいてもよい。

【０１２４】
いくつかの実施形態では、クラウド環境が１つ以上のサービスを提供してもよい。図１１は、本開示の一実施形態に従った、サービスがクラウドサービスとして提供され得るシステム環境１１００の１つ以上のコンポーネントの簡略ブロック図である。図１１における図示された実施形態では、システム環境１１００は、クラウドサービスを提供するクラウドインフラストラクチャシステム１１０２と対話するためにユーザによって使用され得る１つ以上のクライアントコンピューティングデバイス１１０４、１１０６、および１１０８を含む。クラウドインフラストラクチャシステム１１０２は、サーバ１０１２について上述したものを含み得る１つ以上のコンピュータおよび／またはサーバを含んでいてもよい。

【０１２５】
図１１に示すクラウドインフラストラクチャシステム１１０２は、示されたもの以外のコンポーネントを有していてもよい、ということが理解されるべきである。また、図１１に示す実施形態は、この発明の一実施形態を取入れ得るクラウドインフラストラクチャシステムの単なる一例である。いくつかの他の実施形態では、クラウドインフラストラクチャシステム１１０２は、図示されたものよりも多い、または少ないコンポーネントを有していてもよく、２つ以上のコンポーネントを組合せてもよく、もしくは、異なる構成または配置のコンポーネントを有していてもよい。

【０１２６】
クライアントコンピューティングデバイス１１０４、１１０６、および１１０８は、クライアントコンピューティングデバイス１００２、１００４、１００６、および１００８について上述したものと同様のデバイスであってもよい。クライアントコンピューティングデバイス１１０４、１１０６、および１１０８は、クラウドインフラストラクチャシステム１１０２によって提供されるサービスを使用するためにクラウドインフラストラクチャシステム１１０２と対話するためにクライアントコンピューティングデバイスのユーザによって使用され得る、ウェブブラウザ、専用クライアントアプリケーション（たとえば、オラクル・フォームズ）、または何らかの他のアプリケーションといったクライアントアプリケーションを動作させるように構成されてもよい。例示的なシステム環境１１００は３つのクライアントコンピューティングデバイスを有して示されているが、任意の数のクライアントコンピューティングデバイスがサポートされてもよい。センサを有するデバイスなどの他のデバイスが、クラウドインフラストラクチャシステム１１０２と対話してもよい。

【０１２７】

ネットワーク１１１０は、クライアントコンピューティングデバイス１１０４、１１０６、および１１０８とクラウドインフラストラクチャシステム１１０２との間のデータの通信および交換を容易にしてもよい。各ネットワークは、ネットワーク１０１０について上述したものを含む、商業的に入手可能なさまざまなプロトコルのうちのいずれかを使用してデータ通信をサポートできる、当業者にはよく知られた任意のタイプのネットワークであってもよい。

【０１２８】

ある実施形態では、クラウドインフラストラクチャシステム１１０２によって提供されるサービスは、クラウドインフラストラクチャシステムのユーザにとってオンデマンドで利用可能にされる多数のサービスを含んでいてもよい。オンラインデータストレージおよびバックアップソリューション、ウェブベースの電子メールサービス、ホスト型オフィススイートおよび文書コラボレーションサービス、データベース処理、管理された技術サポートサービスなどを何ら限定されることなく含む、さまざま他のサービスも提供されてもよい。クラウドインフラストラクチャシステムによって提供されるサービスは、そのユーザの必要性を満たすために動的にスケール変更され得る。

【０１２９】

ある実施形態では、クラウドインフラストラクチャシステム１１０２によって提供されるサービスの特定のインスタンス化は、ここに「サービスインスタンス」と呼ばれる。一般に、クラウドサービスプロバイダのシステムから、インターネットなどの通信ネットワークを介してユーザに利用可能とされる任意のサービスは、「クラウドサービス」と呼ばれる。典型的には、パブリッククラウド環境では、クラウドサービスプロバイダのシステムを作り上げるサーバおよびシステムは、顧客自身の構内サーバおよびシステムとは異なっている。たとえば、クラウドサービスプロバイダのシステムは、アプリケーションをホストしてもよく、ユーザは、インターネットなどの通信ネットワークを介してオンデマンドでアプリケーションをオーダーし、使用してもよい。

【０１３０】

いくつかの例では、コンピュータネットワーククラウドインフラストラクチャにおけるサービスは、クラウドベンダーによってユーザに提供されるかまたは当該技術分野において他の態様で公知であるようなストレージ、ホスト型データベース、ホスト型ウェブサーバ、ソフトウェアアプリケーション、もしくは他のサービスへの、保護されたコンピュータネットワークアクセスを含んでいてもよい。たとえば、サービスは、インターネットを通した、クラウド上のリモートストレージへの、パスワードで保護されたアクセスを含み得る。別の例として、サービスは、ネットワーク化された開発者による私的使用のための、ウェブサービスベースのホスト型リレーショナルデータベースおよびスクリプト言語ミドルウェアエンジンを含み得る。別の例として、サービスは、クラウドベンダーのウェブサイト上でホストされる電子メールソフトウェアアプリケーションへのアクセスを含み得る。

【０１３１】

ある実施形態では、クラウドインフラストラクチャシステム１１０２は、セルフサービスで、サブスクリプションベースで、弾力的にスケーラブルで、信頼でき、高可用性で、かつ安全な態様で顧客に配信される、アプリケーション、ミドルウェアおよびデータベースサービス提供物一式を含んでいてもよい。そのようなクラウドインフラストラクチャシステムの一例は、本譲受人によって提供されるオラクル・パブリック・クラウド（Oracle Public Cloud）である。

【０１３２】

クラウドインフラストラクチャシステム１１０２はまた、「ビッグデータ」に関連する計算および分析サービスを提供してもよい。「ビッグデータ」という用語は一般に、大量のデータを視覚化し、傾向を検出し、および／または他の態様でデータと対話するためにアナリストおよび調査員によって格納され操作され得る、極めて大きいデータセットを指すために使用される。このビッグデータおよび関連するアプリケーションは、多くのレベ

ルで、および異なるスケールで、インフラストラクチャシステムによってホストおよび／または操作され得る。並列にリンクされた何十、何百、または何千ものプロセッサが、そのようなデータを提示するために、もしくは、当該データまたはそれが表わすものに対する外力をシミュレートするために、当該データに作用することができる。これらのデータセットは、データベースで編成されたもの、または他の態様で構造化モデルに従ったものなどの構造化データ、ならびに／もしくは、非構造化データ（たとえば、電子メール、画像、データｂｌｏｂ（バイナリラージオブジェクト）、ウェブページ、複合イベント処理）を伴い得る。より多い（またはより少ない）コンピューティングリソースを目標へ比較的迅速に集中させるために実施形態の能力を活用することにより、クラウドインフラストラクチャシステムは、企業、政府機関、研究組織、個人、同志の個人または組織のグループ、もしくは他のエンティティからの要望に基づいて、大きいデータセットに対してタスクを行なうために、より良好に利用可能であり得る。

【０１３３】

さまざまな実施形態では、クラウドインフラストラクチャシステム１１０２は、クラウドインフラストラクチャシステム１１０２によって提供されるサービスへの顧客のサブスクリプションを自動的にプロビジョニングし、管理し、追跡するように適合されてもよい。クラウドインフラストラクチャシステム１１０２は、異なるデプロイメントモデルを介してクラウドサービスを提供してもよい。たとえば、サービスは、クラウドインフラストラクチャシステム１１０２がクラウドサービスを販売する組織によって所有され（たとえば、オラクル・コーポレイションによって所有され）、サービスが一般大衆または異なる産業企業にとって利用可能とされる、パブリッククラウドモデルの下で提供されてもよい。別の例として、サービスは、クラウドインフラストラクチャシステム１１０２が単一の組織のためにのみ動作され、その組織内の１つ以上のエンティティのためのサービスを提供し得る、プライベートクラウドモデルの下で提供されてもよい。クラウドサービスはまた、クラウドインフラストラクチャシステム１１０２、およびクラウドインフラストラクチャシステム１１０２によって提供されるサービスが、関連するコミュニティにおけるいくつかの組織によって共有される、コミュニティクラウドモデルの下で提供されてもよい。クラウドサービスはまた、２つ以上の異なるモデルの組合せであるハイブリッドクラウドモデルの下で提供されてもよい。

【０１３４】

いくつかの実施形態では、クラウドインフラストラクチャシステム１１０２によって提供されるサービスは、ソフトウェア・アズ・ア・サービス（ＳａａＳ）カテゴリー、プラットフォーム・アズ・ア・サービス（Platform as a Service：ＰａａＳ）カテゴリー、インフラストラクチャ・アズ・ア・サービス（Infrastructure as a Service：ＩａａＳ）カテゴリー、または、ハイブリッドサービスを含むサービスの他のカテゴリーの下で提供される、１つ以上のサービスを含んでいてもよい。顧客は、クラウドインフラストラクチャシステム１１０２によって提供される１つ以上のサービスを、サブスクリプションオーダーを介してオーダーしてもよい。クラウドインフラストラクチャシステム１１０２は次に、顧客のサブスクリプションオーダーにおけるサービスを提供するために処理を行なう。

【０１３５】

いくつかの実施形態では、クラウドインフラストラクチャシステム１１０２によって提供されるサービスは、アプリケーションサービス、プラットフォームサービス、およびインフラストラクチャサービスを、何ら限定されることなく含んでいてもよい。いくつかの例では、アプリケーションサービスは、ＳａａＳプラットフォームを介して、クラウドインフラストラクチャシステムによって提供されてもよい。ＳａａＳプラットフォームは、ＳａａＳカテゴリーに該当するクラウドサービスを提供するように構成されてもよい。たとえば、ＳａａＳプラットフォームは、統合された開発およびデプロイメントプラットフォーム上にオンデマンドアプリケーション一式を構築し、配信するための能力を提供してもよい。ＳａａＳプラットフォームは、ＳａａＳサービスを提供するための基本ソフトウ

ェアおよびインフラストラクチャを管理し、制御してもよい。ＳａａＳプラットフォームによって提供されるサービスを利用することにより、顧客は、クラウドインフラストラクチャシステム上で実行されるアプリケーションを利用できる。顧客は、顧客が別々のライセンスおよびサポートを購入する必要なく、アプリケーションサービスを取得できる。さまざまな異なるＳａａＳサービスが提供されてもよい。例は、大型組織のための販売実績管理、企業統合、およびビジネス柔軟性についてのソリューションを提供するサービスを、何ら限定されることなく含む。

【０１３６】

いくつかの実施形態では、プラットフォームサービスは、ＰａａＳプラットフォームを介して、クラウドインフラストラクチャシステム１１０２によって提供されてもよい。ＰａａＳプラットフォームは、ＰａａＳカテゴリーに該当するクラウドサービスを提供するように構成されてもよい。プラットフォームサービスの例は、（オラクルなどの）組織が共有の共通アーキテクチャ上で既存のアプリケーションを統合できるようにするサービスと、プラットフォームによって提供される共有のサービスを活用する新しいアプリケーションを構築するための能力とを、何ら限定されることなく含んでいてもよい。ＰａａＳプラットフォームは、ＰａａＳサービスを提供するための基本ソフトウェアおよびインフラストラクチャを管理し、制御してもよい。顧客は、顧客が別々のライセンスおよびサポートを購入する必要なく、クラウドインフラストラクチャシステム１１０２によって提供されるＰａａＳサービスを取得できる。プラットフォームサービスの例は、オラクルＪａｖａ（登録商標）クラウドサービス（Java Cloud Service：ＪＣＳ）、オラクル・データベース・クラウド・サービス（Database Cloud Service：ＤＢＣＳ）などを、何ら限定されることなく含む。

【０１３７】

ＰａａＳプラットフォームによって提供されるサービスを利用することにより、顧客は、クラウドインフラストラクチャシステムによってサポートされるプログラミング言語およびツールを採用するとともに、デプロイメントされたサービスを制御することもできる。いくつかの実施形態では、クラウドインフラストラクチャシステムによって提供されるプラットフォームサービスは、データベースクラウドサービス、ミドルウェアクラウドサービス（たとえば、オラクル・フュージョン・ミドルウェア（Oracle Fusion Middleware）サービス）、およびＪａｖａクラウドサービスを含んでいてもよい。一実施形態では、データベースクラウドサービスは、組織がデータベースリソースをプールし、データベースクラウドの形をしたデータベース・アズ・ア・サービスを顧客に提供することを可能にする共有のサービスデプロイメントモデルをサポートしてもよい。ミドルウェアクラウドサービスは、顧客がさまざまなビジネスアプリケーションを開発してデプロイメントするためのプラットフォームを提供してもよく、Ｊａｖａクラウドサービスは、顧客がクラウドインフラストラクチャシステムにおいてＪａｖａアプリケーションをデプロイメントするためのプラットフォームを提供してもよい。

【０１３８】

クラウドインフラストラクチャシステムにおいて、さまざまな異なるインフラストラクチャサービスが、ＩａａＳプラットフォームによって提供されてもよい。これらのインフラストラクチャサービスは、ＳａａＳプラットフォームおよびＰａａＳプラットフォームによって提供されるサービスを利用する顧客のための、ストレージ、ネットワーク、ならびに他の基礎的コンピューティングリソースなどの基本コンピューティングリソースの管理および制御を容易にする。

【０１３９】

ある実施形態では、クラウドインフラストラクチャシステム１１０２はまた、クラウドインフラストラクチャシステムの顧客にさまざまなサービスを提供するために使用されるリソースを提供するためのインフラストラクチャリソース１１３０を含んでいてもよい。一実施形態では、インフラストラクチャリソース１１３０は、ＰａａＳプラットフォームおよびＳａａＳプラットフォームによって提供されるサービスを実行するためのサーバ、

ストレージ、およびネットワーキングリソース、ならびに他のリソースなどのハードウェアの予め統合され最適化された組合せを含んでいてもよい。

【０１４０】

いくつかの実施形態では、クラウドインフラストラクチャシステム１１０２におけるリソースは、複数のユーザによって共有され、要望ごとに動的に再割当てされてもよい。加えて、リソースは、異なる時間帯におけるユーザに割当てられてもよい。たとえば、クラウドインフラストラクチャシステム１１０２は、第１の時間帯における第１の一組のユーザが、特定数の時間、クラウドインフラストラクチャシステムのリソースを利用することを可能にし、次に、異なる時間帯に位置する別の一組のユーザへの同じリソースの再割当てを可能にして、それによりリソースの利用を最大化してもよい。

【０１４１】

ある実施形態では、クラウドインフラストラクチャシステム１１０２によるサービスのプロビジョニングを可能にするために、クラウドインフラストラクチャシステム１１０２の異なるコンポーネントまたはモジュールによって共有される、多くの内部共有サービス１１３２が提供されてもよい。これらの内部共有サービスは、セキュリティおよびアイデンティティサービス、統合サービス、企業リポジトリサービス、企業マネージャサービス、ウィルススキャニングおよびホワイトリストサービス、高可用性、バックアップおよび復元サービス、クラウドサポートを可能にするためのサービス、電子メールサービス、通知サービス、ファイル転送サービスなどを、何ら限定されることなく含んでいてもよい。

【０１４２】

ある実施形態では、クラウドインフラストラクチャシステム１１０２は、クラウドインフラストラクチャシステムにおけるクラウドサービス（たとえば、ＳａａＳ、ＰａａＳ、およびＩａａＳサービス）の包括的管理を提供してもよい。一実施形態では、クラウド管理機能性は、クラウドインフラストラクチャシステム１１０２によって受信された顧客のサブスクリプションをプロビジョニングし、管理し、追跡するための能力などを含んでいてもよい。

【０１４３】

一実施形態では、図１１に示すように、クラウド管理機能性は、オーダー管理モジュール１１２０、オーダーオーケストレーションモジュール１１２２、オーダープロビジョニングモジュール１１２４、オーダー管理および監視モジュール１１２６、ならびにアイデンティティ管理モジュール１１２８などの１つ以上のモジュールによって提供されてもよい。これらのモジュールは、汎用コンピュータ、専用サーバコンピュータ、サーバファーム、サーバクラスタ、もしくは任意の他の適切な構成および／または組合せであり得る、１つ以上のコンピュータおよび／またはサーバを含んでいてもよく、もしくはそれらを使用して提供されてもよい。

【０１４４】

例示的な動作では、ステップ１１３４で、クライアントコンピューティングデバイス１１０４、１１０６または１１０８などのクライアントデバイスを使用する顧客は、クラウドインフラストラクチャシステム１１０２によって提供される１つ以上のサービスを要求し、クラウドインフラストラクチャシステム１１０２によって提供される１つ以上のサービスについてサブスクリプションオーダーを出すことにより、クラウドインフラストラクチャシステム１１０２と対話してもよい。ある実施形態では、顧客は、クラウドユーザインターフェイス（User Interface：ＵＩ）、たとえばクラウドＵＩ１１１２、クラウドＵＩ１１１４および／またはクラウドＵＩ１１１６にアクセスし、これらのＵＩを介してサブスクリプションオーダーを出してもよい。顧客がオーダーを出したことに応答してクラウドインフラストラクチャシステム１１０２が受信したオーダー情報は、顧客と、顧客が申し込むつもりである、クラウドインフラストラクチャシステム１１０２によって提供される１つ以上のサービスとを識別する情報を含んでいてもよい。

【０１４５】

ステップ１１３６で、顧客から受信されたオーダー情報が、オーダーデータベース１１

１８に格納されてもよい。これが新しいオーダーである場合、そのオーダーのために新しい記録が作成されてもよい。一実施形態では、オーダーデータベース１１１８は、クラウドインフラストラクチャシステム１１０２によって動作され、他のシステムエレメントとともに動作される、いくつかのデータベースのうちの１つであり得る。

【０１４６】

ステップ１１３８で、オーダーを立証し、立証後にオーダーを予約するといった、オーダーに関連する請求および課金機能を行なうように構成され得るオーダー管理モジュール１１２０へ、オーダー情報が発送されてもよい。

【０１４７】

ステップ１１４０で、顧客によって出されたオーダーのためのサービスおよびリソースのプロビジョニングをオーケストレーションするように構成されたオーダーオーケストレーションモジュール１１２２へ、オーダーに関する情報が通信されてもよい。場合によっては、オーダーオーケストレーションモジュール１１２２は、プロビジョニングのためにオーダープロビジョニングモジュール１１２４のサービスを使用してもよい。ある実施形態では、オーダーオーケストレーションモジュール１１２２は、各オーダーに関連付けられたビジネスプロセスの管理を可能にし、オーダーがプロビジョニングへ進むべきかどうかを判断するためにビジネスロジックを適用する。

【０１４８】

図１１に示す実施形態に示されるように、ステップ１１４２で、新規サブスクリプションのオーダーを受信すると、オーダーオーケストレーションモジュール１１２２は、リソースを割当ててサブスクリプションオーダーを遂行するために必要とされるリソースを構成することを求める要求を、オーダープロビジョニングモジュール１１２４へ送信する。オーダープロビジョニングモジュール１１２４は、顧客によってオーダーされたサービスのためのリソースの割当てを可能にする。オーダープロビジョニングモジュール１１２４は、クラウドインフラストラクチャシステム１１０２によって提供されるクラウドサービスと、要求されたサービスを提供するためのリソースをプロビジョニングするために使用される物理的実装層との間の抽象化のレベルを提供する。これは、オーダーオーケストレーションモジュール１１２２が、サービスおよびリソースが実際にオンザフライでプロビジョニングされるか否か、または予めプロビジョニングされて要求時にのみ割当てられるか否かといった実装詳細から切り離され得るようにする。

【０１４９】

ステップ１１４４で、サービスおよびリソースが一旦プロビジョニングされると、要求されたサービスが現在使える状態であることを示す通知が、申し込んだ顧客へ送信されてもよい。場合によっては、要求されたサービスの使用を顧客が開始できるようにする情報（たとえばリンク）が、顧客へ送信されてもよい。

【０１５０】

ステップ１１４６で、顧客のサブスクリプションオーダーが、オーダー管理および監視モジュール１１２６によって管理され、追跡されてもよい。場合によっては、オーダー管理および監視モジュール１１２６は、申し込まれたサービスの顧客使用に関する使用統計を収集するように構成されてもよい。たとえば、統計は、使用されるストレージの量、転送されるデータの量、ユーザの数、システムアップタイムおよびシステムダウンタイムの量などについて収集されてもよい。

【０１５１】

ある実施形態では、クラウドインフラストラクチャシステム１１０２は、クラウドインフラストラクチャシステム１１０２においてアクセス管理および認証サービスなどのアイデンティティサービスを提供するように構成されたアイデンティティ管理モジュール１１２８を含んでいてもよい。いくつかの実施形態では、アイデンティティ管理モジュール１１２８は、クラウドインフラストラクチャシステム１１０２によって提供されるサービスを利用したい顧客についての情報を制御してもよい。そのような情報は、そのような顧客のアイデンティティを認証する情報と、さまざまなシステムリソース（たとえば、ファイ

ル、ディレクトリ、アプリケーション、通信ポート、メモリセグメントなど）に対してそれらの顧客がどのアクションを行なうことが認可されているかを記述する情報とを含み得る。アイデンティティ管理モジュール１１２８はまた、各顧客についての記述的情報と、その記述的情報が誰によってどのようにアクセスされ、修正され得るかについての記述的情報との管理を含んでいてもよい。

【０１５２】

図１２は、本発明の一実施形態を実現するために使用され得る例示的なコンピュータシステム１２００を示す。いくつかの実施形態では、コンピュータシステム１２００は、上述のさまざまなサーバおよびコンピュータシステムのうちのいずれかを実現するために使用されてもよい。図１２に示すように、コンピュータシステム１２００は、バスサブシステム１２０２を介して多くの周辺サブシステムと通信する処理部１２０４を含むさまざまなサブシステムを含む。これらの周辺サブシステムは、処理加速部１２０６と、Ｉ／Ｏサブシステム１２０８と、記憶サブシステム１２１８と、通信サブシステム１２２４とを含んでいてもよい。記憶サブシステム１２１８は、有形のコンピュータ読取可能記憶媒体１２２２と、システムメモリ１２１０とを含んでいてもよい。

【０１５３】

バスサブシステム１２０２は、コンピュータシステム１２００のさまざまなコンポーネントおよびサブシステムを意図されるように互いに通信させるためのメカニズムを提供する。バスサブシステム１２０２は単一のバスとして概略的に示されているが、バスサブシステムの代替的な実施形態は複数のバスを利用してもよい。バスサブシステム１２０２は、さまざまなバスアーキテクチャのうちのいずれかを使用するメモリバスまたはメモリコントローラ、周辺バス、およびローカルバスを含む、いくつかのタイプのバス構造のうちのいずれかであってもよい。たとえば、そのようなアーキテクチャは、ＩＥＥＥ　Ｐ１３８６．１規格で製造されるメザニンバスとして実現可能な、産業標準アーキテクチャ（Industry Standard Architecture：ＩＳＡ）バス、マイクロチャネルアーキテクチャ（Micro Channel Architecture：ＭＣＡ）バス、強化ＩＳＡ（ＥＩＳＡ）バス、ビデオエレクトロニクス標準組織（Video Electronics Standards Association：ＶＥＳＡ）ローカルバス、および周辺コンポーネント相互接続（Peripheral Component Interconnect：ＰＣＩ）バスなどを含んでいてもよい。

【０１５４】

処理サブシステム１２０４はコンピュータシステム１２００の動作を制御しており、また、１つ以上の処理部１２３２、１２３４などを含んでいてもよい。処理部は、シングルコアまたはマルチコアプロセッサ、プロセッサの１つ以上のコア、またはそれらの組合せを含む、１つ以上のプロセッサを含んでいてもよい。いくつかの実施形態では、処理サブシステム１２０４は、グラフィックスプロセッサ、デジタル信号プロセッサ（ＤＳＰ）などといった、１つ以上の専用コプロセッサを含み得る。いくつかの実施形態では、処理サブシステム１２０４の処理部のうちのいくつかまたはすべては、特定用途向け集積回路（ＡＳＩＣ）、またはフィールドプログラマブルゲートアレイ（ＦＰＧＡ）といった、カスタマイズされた回路を使用して実現され得る。

【０１５５】

いくつかの実施形態では、処理サブシステム１２０４における処理部は、システムメモリ１２１０に、またはコンピュータ読取可能記憶媒体１２２２上に格納された命令を実行することができる。さまざまな実施形態では、処理部は、さまざまなプログラムおよびコード命令を実行でき、同時に実行される複数のプログラムまたはプロセスを維持できる。任意の所与の時間において、実行されるべきプログラムコードのうちのいくつかまたはすべては、システムメモリ１２１０に、および／または、おそらく１つ以上の記憶装置上を含むコンピュータ読取可能記憶媒体１２２２上にあり得る。好適なプログラミングを通して、処理サブシステム１２０４は、さまざまな機能性を提供できる。

【０１５６】

ある実施形態では、コンピュータシステム１２００によって行なわれる処理全体を加速

するように、カスタマイズされた処理を行なうために、または、処理サブシステム１２０４によって行なわれる処理のうちのいくつかをオフロードするために、処理加速部１２０６が提供されてもよい。

【０１５７】

Ｉ／Ｏサブシステム１２０８は、コンピュータシステム１２００へ情報を入力するための、および／または、コンピュータシステム１２００から、またはコンピュータシステム１２００を介して情報を出力するための装置およびメカニズムを含んでいてもよい。一般に、「入力装置」という用語の使用は、コンピュータシステム１２００へ情報を入力するためのあらゆる可能なタイプの装置およびメカニズムを含むよう意図されている。ユーザインターフェイス入力装置は、たとえば、キーボード、マウスまたはトラックボールなどのポインティング装置、ディスプレイに組込まれたタッチパッドまたはタッチスクリーン、スクロールホイール、クリックホイール、ダイヤル、ボタン、スイッチ、キーパッド、音声コマンド認識システム付き音声入力装置、マイクロホン、および他のタイプの入力装置を含んでいてもよい。ユーザインターフェイス入力装置はまた、ユーザが入力装置を制御し、それと対話することを可能にする、マイクロソフトＫｉｎｅｃｔ（登録商標）運動センサなどの運動感知および／またはジェスチャー認識装置、マイクロソフトＸｂｏｘ（登録商標）３６０ゲームコントローラ、ジェスチャーおよび口頭コマンドを使用して入力を受信するためのインターフェイスを提供する装置を含んでいてもよい。ユーザインターフェイス入力装置はまた、ユーザから目の活動（たとえば、写真撮影中および／またはメニュー選択中の「まばたき」）を検出し、アイジェスチャーを入力装置（たとえば、グーグル・グラス（登録商標））への入力として変換する、グーグル・グラス（登録商標）まばたき検出器などのアイジェスチャー認識装置を含んでいてもよい。加えて、ユーザインターフェイス入力装置は、ユーザが音声コマンドを通して音声認識システム（たとえば、Ｓｉｒｉ（登録商標）ナビゲータ）と対話できるようにする音声認識感知装置を含んでいてもよい。

【０１５８】

ユーザインターフェイス入力装置の他の例は、３次元（３Ｄ）マウス、ジョイスティックまたはポインティングスティック、ゲームパッドおよびグラフィックタブレット、ならびに、スピーカ、デジタルカメラ、デジタルビデオカメラ、携帯型メディアプレイヤー、ウェブカメラ、画像スキャナ、指紋スキャナ、バーコードリーダ３Ｄスキャナ、３Ｄプリンタ、レーザー測距器、および視線追跡装置などの音声／視覚装置を、何ら限定されることなく含んでいてもよい。加えて、ユーザインターフェイス入力装置は、たとえば、コンピュータ断層撮影装置、磁気共鳴撮像装置、ポジトロン放出断層撮影装置、医療用超音波検査装置などの医療用撮像入力装置を含んでいてもよい。ユーザインターフェイス入力装置はまた、たとえば、ＭＩＤＩキーボード、デジタル楽器などの音声入力装置を含んでいてもよい。

【０１５９】

ユーザインターフェイス出力装置は、表示サブシステム、表示灯、または、音声出力装置などの非視覚的ディスプレイを含んでいてもよい。表示サブシステムは、陰極線管（cathode ray tube：ＣＲＴ）、液晶ディスプレイ（liquid crystal display：ＬＣＤ）またはプラズマディスプレイを使用するものなどのフラットパネル装置、投影装置、タッチスクリーンなどであってもよい。一般に、「出力装置」という用語の使用は、コンピュータシステム１２００からユーザまたは他のコンピュータへ情報を出力するためのあらゆる可能なタイプの装置およびメカニズムを含むよう意図されている。たとえば、ユーザインターフェイス出力装置は、モニタ、プリンタ、スピーカ、ヘッドホン、自動車ナビゲーションシステム、プロッタ、音声出力装置、およびモデムといった、テキスト、グラフィックスおよび音声／映像情報を視覚的に伝えるさまざまな表示装置を、何ら限定されることなく含んでいてもよい。

【０１６０】

記憶サブシステム１２１８は、コンピュータシステム１２００によって使用される情報

を格納するためのリポジトリまたはデータストアを提供する。記憶サブシステム１２１８は、いくつかの実施形態の機能性を提供する基本プログラミングおよびデータ構造を格納するための有形の非一時的なコンピュータ読取可能記憶媒体を提供する。処理サブシステム１２０４によって実行されると上述の機能性を提供するソフトウェア（プログラム、コードモジュール、命令）が、記憶サブシステム１２１８に格納されてもよい。ソフトウェアは、処理サブシステム１２０４の１つ以上の処理部によって実行されてもよい。記憶サブシステム１２１８はまた、本発明に従って使用されるデータを格納するためのリポジトリを提供してもよい。

【０１６１】

記憶サブシステム１２１８は、揮発性および不揮発性メモリデバイスを含む、１つ以上の非一時的メモリデバイスを含んでいてもよい。図１２に示すように、記憶サブシステム１２１８は、システムメモリ１２１０と、コンピュータ読取可能記憶媒体１２２２とを含む。システムメモリ１２１０は、プログラム実行中に命令およびデータを格納するための揮発性のメインランダムアクセスメモリ（ＲＡＭ）と、固定された命令が格納される不揮発性の読出専用メモリ（ＲＯＭ）またはフラッシュメモリとを含む、多くのメモリを含んでいてもよい。いくつかの実現化例では、起動中などにコンピュータシステム１２００内のエレメント間で情報を転送するのに役立つ基本ルーチンを含む基本入力／出力システム（basic input/output system：ＢＩＯＳ）が、典型的にはＲＯＭに格納されてもよい。ＲＡＭは典型的には、処理サブシステム１２０４によって現在動作され実行されているデータおよび／またはプログラムモジュールを含む。いくつかの実現化例では、システムメモリ１２１０は、スタティックランダムアクセスメモリ（ＳＲＡＭ）またはダイナミックランダムアクセスメモリ（ＤＲＡＭ）といった、複数の異なるタイプのメモリを含んでいてもよい。

【０１６２】

限定のためではなく例として、図１２に示すように、システムメモリ１２１０は、クライアントアプリケーション、ウェブブラウザ、中間層アプリケーション、リレーショナルデータベース管理システム（relational database management system：ＲＤＢＭＳ）などを含み得るアプリケーションプログラム１２１２と、プログラムデータ１２１４と、オペレーティングシステム１２１６と格納してもよい。例として、オペレーティングシステム１２１６は、マイクロソフト・ウィンドウズ（登録商標）、アップル・マッキントッシュ（登録商標）、および／またはＬｉｎｕｘオペレーティングシステムのさまざまなバージョン、商業的に入手可能なさまざまなＵＮＩＸ（登録商標）またはＵＮＩＸ様オペレーティングシステム（さまざまなＧＮＵ／Ｌｉｎｕｘオペレーティングシステム、グーグル・クローム（登録商標）ＯＳなどを何ら限定されることなく含む）、および／または、ｉＯＳ、ウィンドウズ（登録商標）フォン、アンドロイド（登録商標）ＯＳ、ブラックベリー（登録商標）１０ＯＳ、パーム（登録商標）ＯＳオペレーティングシステムなどのモバイルオペレーティングシステムを含んでいてもよい。

【０１６３】

コンピュータ読取可能記憶媒体１２２２は、いくつかの実施形態の機能性を提供するプログラミングおよびデータ構造を格納してもよい。処理サブシステム１２０４プロセッサによって実行されると上述の機能性を提供するソフトウェア（プログラム、コードモジュール、命令）が、記憶サブシステム１２１８に格納されてもよい。例として、コンピュータ読取可能記憶媒体１２２２は、ハードディスクドライブ、磁気ディスクドライブ、ならびに、ＣＤ　ＲＯＭ、ＤＶＤ、Ｂｌｕ－Ｒａｙ（登録商標）ディスク、または他の光学媒体などの光ディスクドライブ、といった不揮発性メモリを含んでいてもよい。コンピュータ読取可能記憶媒体１２２２は、Ｚｉｐ（登録商標）ドライブ、フラッシュメモリカード、ユニバーサルシリアルバス（universal serial bus：ＵＳＢ）フラッシュドライブ、セキュアデジタル（secure digital：ＳＤ）カード、ＤＶＤディスク、デジタルビデオテープなどを含んでいてもよいが、それらに限定されない。コンピュータ読取可能記憶媒体１２２２はまた、フラッシュメモリベースのソリッドステートドライブ（solid-state driv

e：ＳＳＤ）、企業フラッシュドライブ、ソリッドステートＲＯＭといった、不揮発性メモリに基づいたＳＳＤ、ソリッドステートＲＡＭ、ダイナミックＲＡＭ、スタティックＲＡＭ、ＤＲＡＭベースのＳＳＤ、磁気抵抗ＲＡＭ（ＭＲＡＭ）ＳＳＤといった、揮発性メモリに基づいたＳＳＤ、および、ＤＲＡＭベースのＳＳＤとフラッシュメモリベースのＳＳＤとの組合せを使用するハイブリッドＳＳＤを含んでいてもよい。コンピュータ読取可能媒体１２２２は、コンピュータシステム１２００のためのコンピュータ読取可能命令、データ構造、プログラムモジュール、および他のデータの格納を提供してもよい。

【０１６４】

ある実施形態では、記憶サブシステム１２１８はまた、コンピュータ読取可能記憶媒体１２２２にさらに接続され得るコンピュータ読取可能記憶媒体リーダ１２２０を含んでいてもよい。システムメモリ１２１０とともに、およびオプションでシステムメモリ１２１０と組合わされて、コンピュータ読取可能記憶媒体１２２２は、リモート、ローカル、固定および／またはリムーバブルの記憶装置に加えて、コンピュータ読取可能情報を格納するための記憶媒体を包括的に表わしてもよい。

【０１６５】

ある実施形態では、コンピュータシステム１２００は、１つ以上の仮想マシンを実行するためのサポートを提供してもよい。コンピュータシステム１２００は、仮想マシンを構成し管理することを容易にするためのハイパーバイザなどのプログラムを実行してもよい。各仮想マシンは、割当てられたメモリ、コンピュート（たとえばプロセッサ、コア）、Ｉ／Ｏ、およびネットワーキングリソースであってもよい。各仮想マシンは典型的には、それ自体のオペレーティングシステムを実行し、それは、コンピュータシステム１２００によって実行される他の仮想マシンによって実行されるオペレーティングシステムと同じであっても異なっていてもよい。したがって、潜在的に、複数のオペレーティングシステムが、コンピュータシステム１２００によって同時に実行されてもよい。各仮想マシンは一般に、他の仮想マシンから独立して実行される。

【０１６６】

通信サブシステム１２２４は、他のコンピュータシステムおよびネットワークへのインターフェイスを提供する。通信サブシステム１２２４は、コンピュータシステム１２００とは別のシステムからデータを受信し、別のシステムにデータを送信するためのインターフェイスとして機能する。たとえば、通信サブシステム１２２４は、コンピュータシステム１２００が、１つ以上のクライアントコンピューテイングデバイスとの間で情報を送受信するために、クライアントコンピューテイングデバイスへの通信チャネルをインターネットを介して確立できるようにしてもよい。

【０１６７】

通信サブシステム１２２４は、有線および／または無線通信プロトコル双方をサポートしてもよい。たとえば、ある実施形態では、通信サブシステム１２２４は、（たとえば、３Ｇ、４Ｇ、またはＥＤＧＥ（enhanced data rates for global evolution：エンハンスト・データレート・フォー・グローバル・エボリューション）、ＷｉＦｉ（ＩＥＥＥ８０２．１１ファミリー規格）、または他のモバイル通信技術、またはそれらの任意の組合せといった携帯電話技術、高度なデータネットワーク技術を使用した）無線音声および／またはデータネットワークにアクセスするための無線周波数（radio frequency：ＲＦ）トランシーバコンポーネント、全地球測位システム（global positioning system：ＧＰＳ）受信機コンポーネント、および／または他のコンポーネントを含んでいてもよい。いくつかの実施形態では、通信サブシステム１２２４は、無線インターフェイスに加えて、またはその代わりに、有線ネットワーク接続（たとえば、イーサネット）を提供できる。

【０１６８】

通信サブシステム１２２４は、データをさまざまな形で送受信することができる。たとえば、いくつかの実施形態では、通信サブシステム１２２４は、構造化および／または非構造化データフィード１２２６、イベントストリーム１２２８、イベント更新１２３０などの形をした入力通信を受信してもよい。たとえば、通信サブシステム１２２４は、ツイ

ッター（登録商標）フィード、フェースブック（登録商標）更新、リッチ・サイト・サマリー（Rich Site Summary：ＲＳＳ）フィードなどのウェブフィード、および／または１つ以上の第三者情報源からのリアルタイム更新といった、ソーシャルメディアネットワークおよび／または他の通信サービスのユーザからのデータフィード１２２６をリアルタイムで受信（または送信）するように構成されてもよい。

【０１６９】

ある実施形態では、通信サブシステム１２２４は、リアルタイムイベントのイベントストリーム１２２８および／またはイベント更新１２３０を含み得る、明確な終わりがなく本質的に連続的または無限であり得る連続データストリームの形をしたデータを受信するように構成されてもよい。連続データを生成するアプリケーションの例は、たとえば、センサデータアプリケーション、金融ティッカー、ネットワーク性能測定ツール（たとえば、ネットワーク監視およびトラフィック管理アプリケーション）、クリックストリーム分析ツール、自動車交通監視などを含んでいてもよい。

【０１７０】

通信サブシステム１２２４はまた、構造化および／または非構造化データフィード１２２６、イベントストリーム１２２８、イベント更新１２３０などを、コンピュータシステム１２００に結合された１つ以上のストリーミングデータソースコンピュータと通信し得る１つ以上のデータベースに出力するように構成されてもよい。

【０１７１】

コンピュータシステム１２００は、ハンドヘルド携帯デバイス（たとえば、ｉＰｈｏｎｅ（登録商標）携帯電話、ｉＰａｄ（登録商標）コンピューティングタブレット、ＰＤＡ）、ウェアラブルデバイス（たとえば、グーグル・グラス（登録商標）頭部装着型ディスプレイ）、パーソナルコンピュータ、ワークステーション、メインフレーム、キオスク、サーバラック、または任意の他のデータ処理システムを含む、さまざまなタイプのうちの１つであり得る。

【０１７２】

コンピュータおよびネットワークの絶えず変化する性質により、図１２に示されるコンピュータシステム１２００の説明は、単に特定の一例として意図される。図１２に示されるシステムよりも多い、または少ないコンポーネントを有する多くの他の構成が可能である。ここに提供される開示および教示に基づいて、当業者であれば、さまざまな実施形態を実現するための他のやり方および／または方法を理解するであろう。

【０１７３】

この発明の特定の実施形態が説明されてきたが、さまざまな修正、変更、代替構造、および均等物も、この発明の範囲内に包含される。修正は、開示された特徴のあらゆる関連する組合せを含む。本発明の実施形態は、ある特定のデータ処理環境内での動作に制限されず、複数のデータ処理環境内で自由に動作することができる。加えて、本発明の実施形態はある特定の一連のトランザクションおよびステップを使用して説明されてきたが、本発明の範囲が説明された一連のトランザクションおよびステップに限定されないことは、当業者には明らかであるはずである。上述の実施形態のさまざまな特徴および局面は、個々にまたはともに使用されてもよい。

【０１７４】

また、本発明の実施形態はハードウェアとソフトウェアとの特定の組合せを使用して説明されてきたが、ハードウェアとソフトウェアとの他の組合せも本発明の範囲内にあるということが認識されるべきである。本発明の実施形態は、ハードウェアでのみ、またはソフトウェアでのみ、またはそれらの組合せを使用して実現されてもよい。ここに説明されたさまざまなプロセスは、同じプロセッサ、または任意の組合せの異なるプロセッサ上で実現され得る。したがって、コンポーネントまたはモジュールが、ある動作を行なうように構成されると説明される場合、そのような構成は、たとえば、動作を行なうように電子回路を設計することによって、動作を行なうように（マイクロプロセッサなどの）プログラマブル電子回路をプログラミングすることによって、またはそれらの任意の組合せによ

って達成され得る。プロセスは、プロセス間通信用の従来の手法を含むもののそれらに限定されないさまざまな手法を使用して通信することができ、異なる対のプロセスが異なる手法を使用してもよく、または、同じ対のプロセスが異なる時間に異なる手法を使用してもよい。

【０１７５】

したがって、明細書および図面は、限定的な意味ではなく、例示としてみなされるべきである。しかしながら、追加、削減、削除、ならびに他の修正および変更が、請求項で述べられるようなより広範な精神および範囲から逸脱することなく、それらになされ得るということが明らかであろう。このため、特定の発明実施形態が説明されてきたが、これらは限定的であるよう意図されてはいない。さまざまな修正および均等物は、請求の範囲内にある。

【図１】

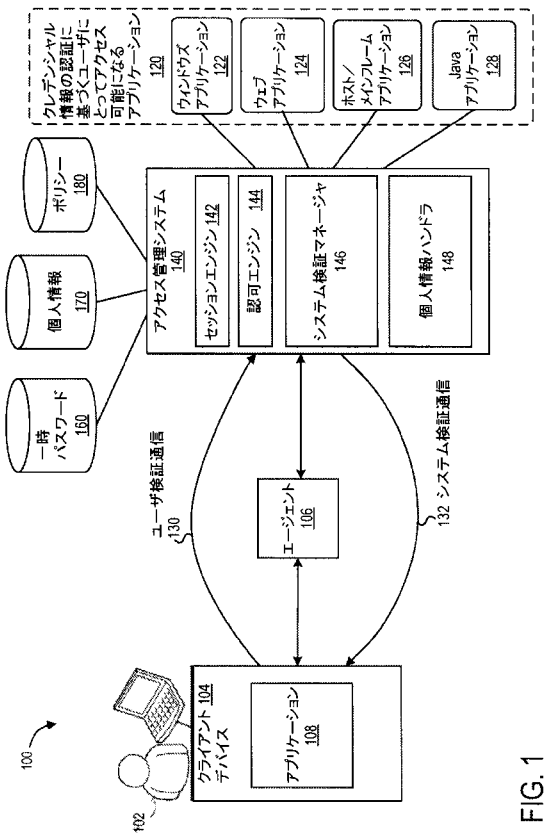

FIG. 1

【図２】

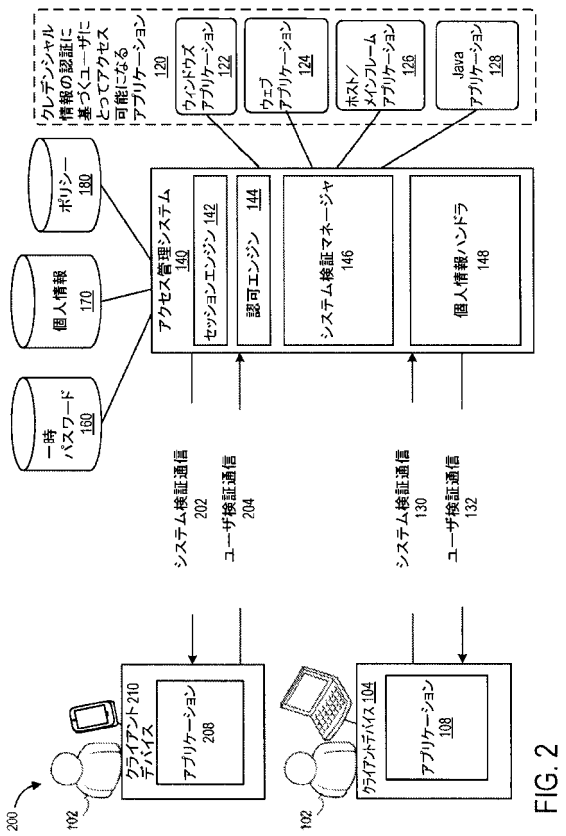

FIG. 2

【図３】

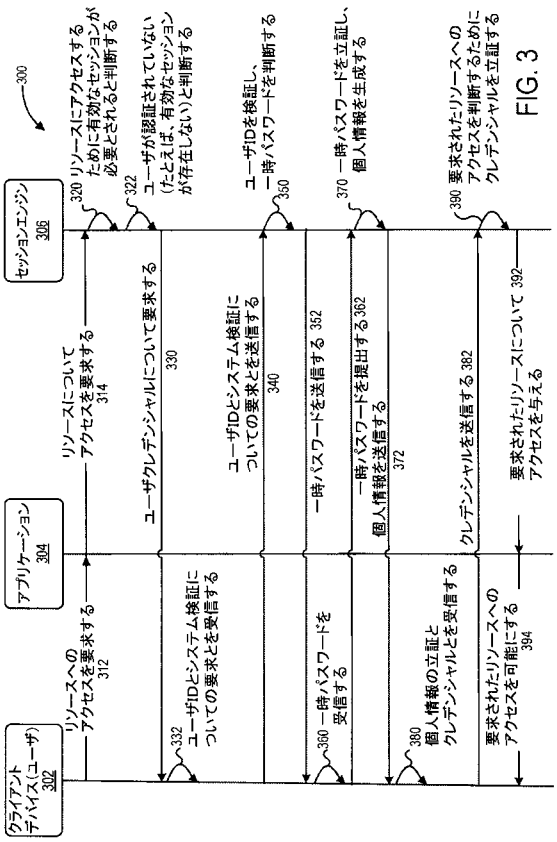

FIG. 3

【図４】

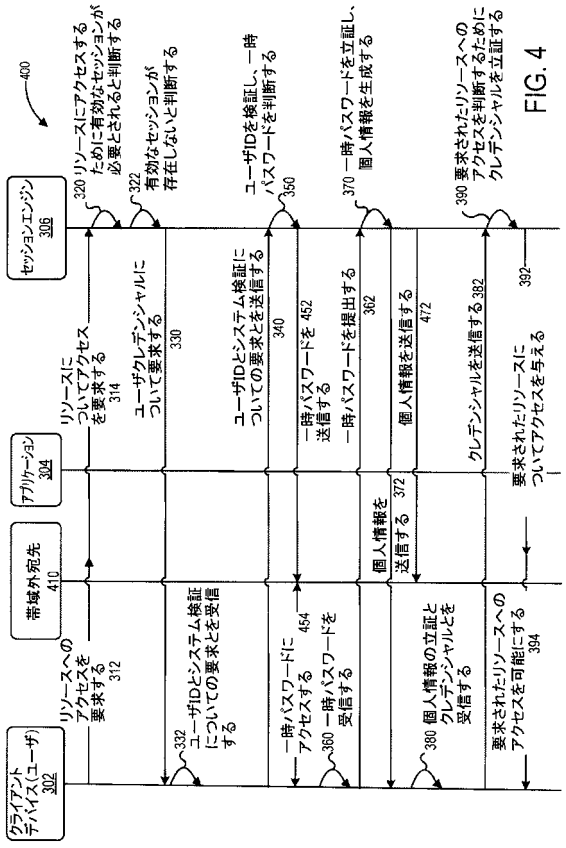

FIG. 4

【図５】

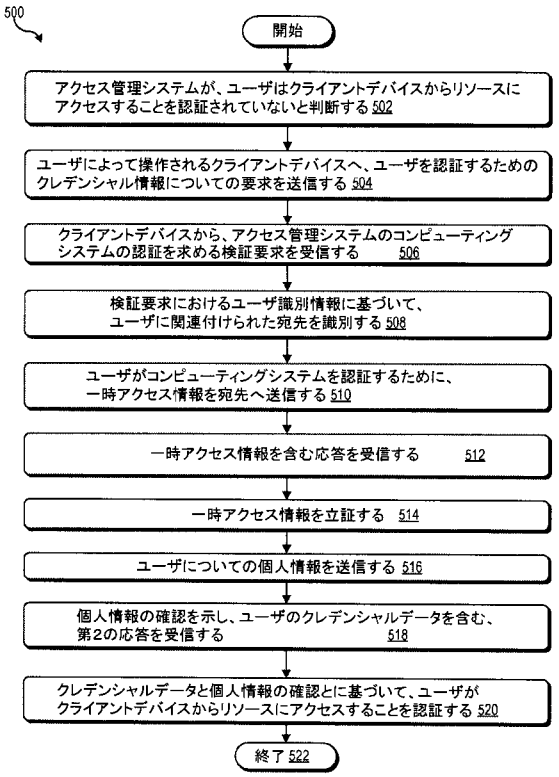

FIG. 5

【図６】

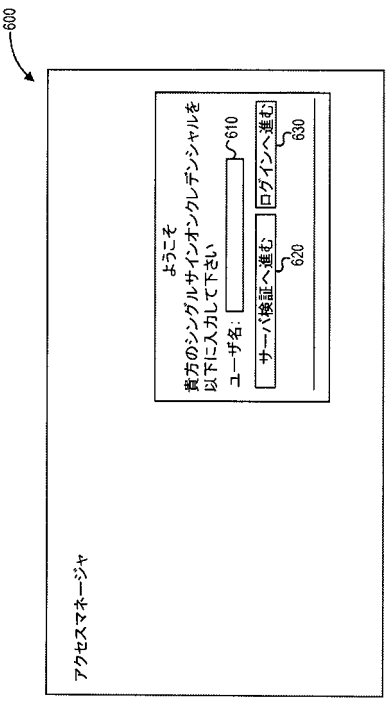

FIG. 6

【図７】

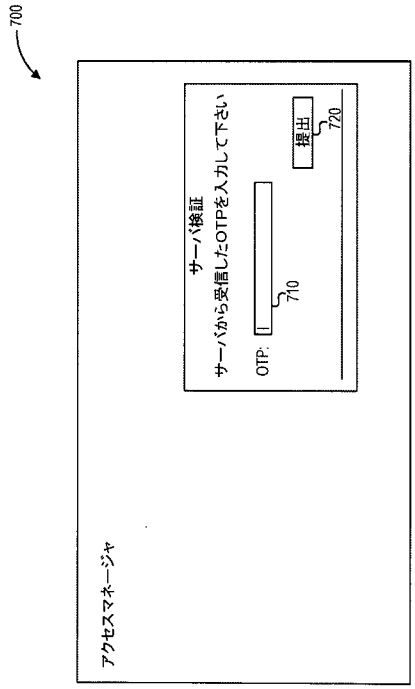

FIG. 7

【図８】

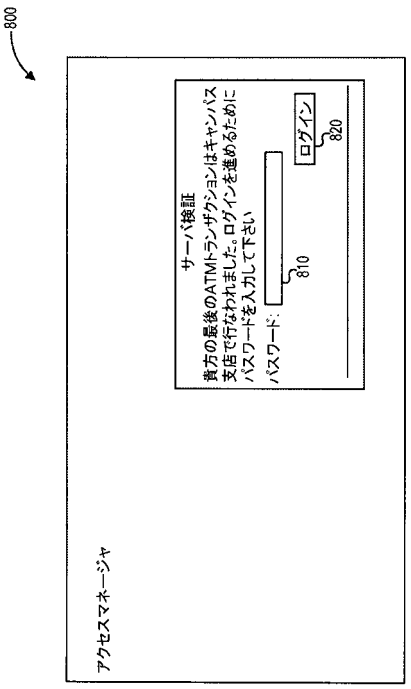

FIG. 8

【図９】

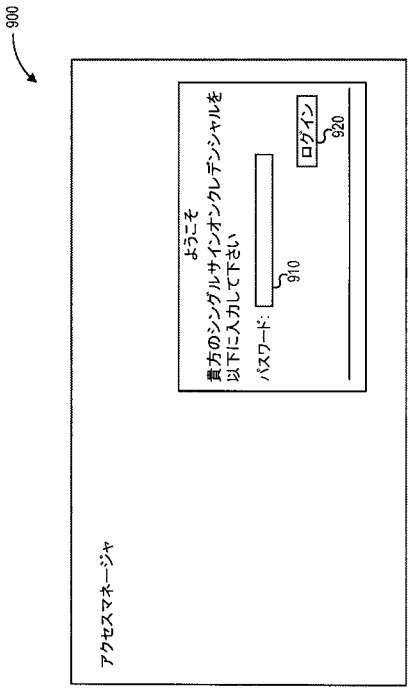

FIG. 9

【図１０】

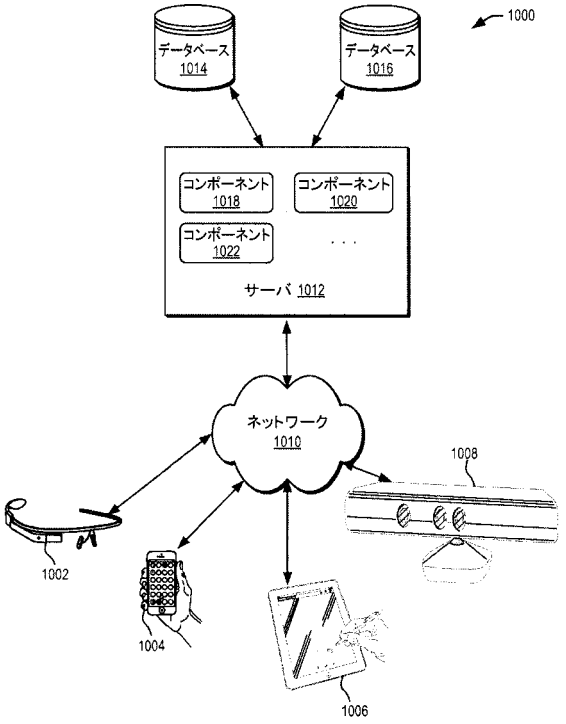

FIG. 10

【図１１】

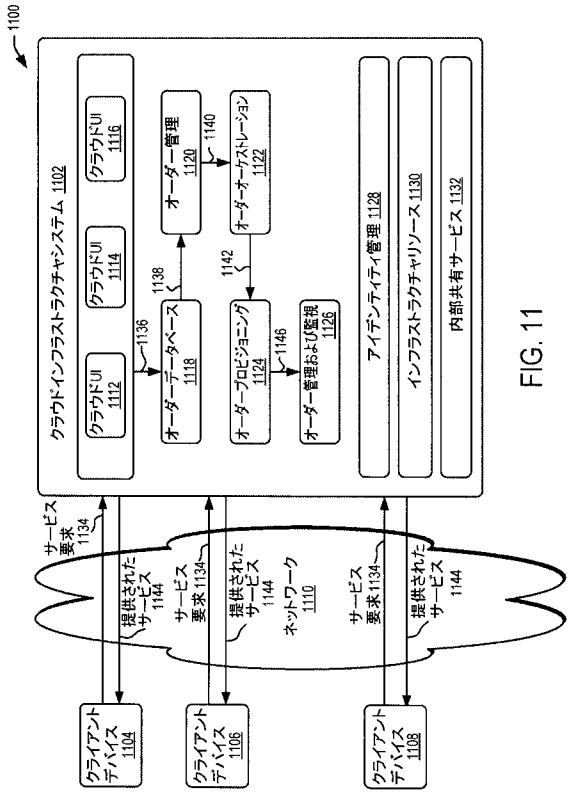

FIG. 11

【図１２】

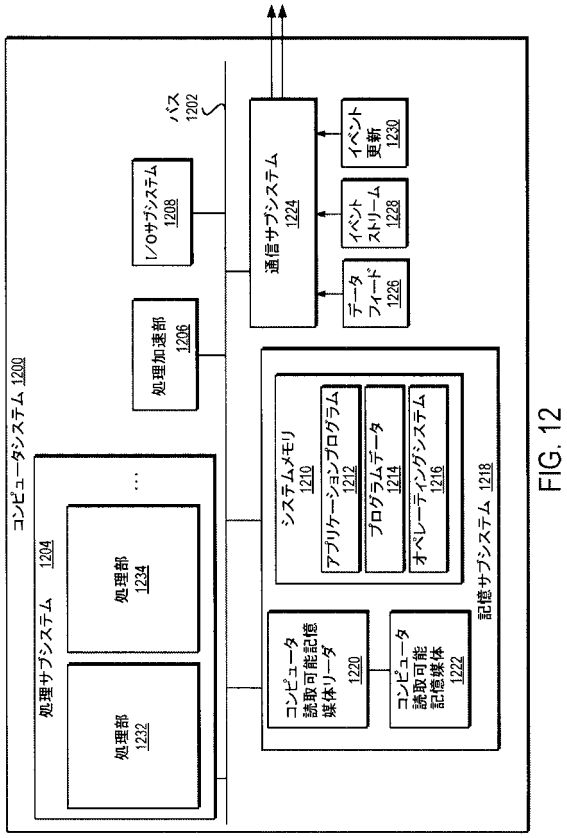

FIG. 12

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/025402

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/44 H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/136573 A1 (STEINBERG JOSEPH [US]) 14 June 2007 (2007-06-14) the whole document -----	1-20
X	Jim Youll: "Fraud Vulnerabilities in SiteKey Security at Bank of America", , 18 July 2006 (2006-07-18), XP055285038, Retrieved from the Internet: URL:http://cr-labs.com/publications/SiteKey-20060718.pdf [retrieved on 2016-06-30] the whole document ----- -/--	1-20

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 July 2016	18/07/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Mäenpää, Jari

3

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/025402

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	RACHNA DHAMIJA AND J D TYGAR: "Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks", HUMAN INTERACTIVE PROOFS, SECOND INTERNATIONAL WORKSHOP ON HUMAN INTERACTIVE PROOFS (HIP 2005),, 1 May 2005 (2005-05-01), pages 127-141, XP008130711, the whole document -----	1-20

3

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/025402

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007136573 A1	14-06-2007	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(72)発明者 サブラマンヤ，ラムヤ
インド、５６００７９ カルナータカ、バンガロール、バセイブシュワーラナガー、カーロスカー・コロニー・サード・ステージ、ナンバー・エス－５５
(72)発明者 クーテイ，ビピン・アナパラッカル
インド、６７１３１０ ケーララ、トリカープール、メイン・ロード、サンギース

Ｆターム(参考) 5B084 AA01 AA30 AB36 BA07 BB16 CD09 CD24 DB02 DC02