(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2017-516328
(P2017-516328A)
(43)公表日　平成29年6月15日(2017.6.15)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5J104
G09C 1/00	(2006.01)	G09C	1/00	640E	
H04L 9/08	(2006.01)	H04L	9/00	601C	
G06F 21/33	(2013.01)	H04L	9/00	601F	
		G06F	21/33		

審査請求 未請求　予備審査請求 有　（全 51 頁）

(21)出願番号　特願2016-554858 (P2016-554858)
(86)(22)出願日　平成27年3月5日(2015.3.5)
(85)翻訳文提出日　平成28年8月31日(2016.8.31)
(86)国際出願番号　PCT/US2015/019006
(87)国際公開番号　WO2015/134771
(87)国際公開日　平成27年9月11日(2015.9.11)
(31)優先権主張番号　61/948,433
(32)優先日　平成26年3月5日(2014.3.5)
(33)優先権主張国　米国(US)
(31)優先権主張番号　14/638,290
(32)優先日　平成27年3月4日(2015.3.4)
(33)優先権主張国　米国(US)

(71)出願人　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　フィル・ティエン・グエン
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５・クアルコム・インコーポレイテッド

最終頁に続く

(54)【発明の名称】エンドユーザ連合ログインを使用した鍵交換暗号化チャネルにおける違反の検出

(57)【要約】
第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するためのシステムおよび方法を開示する。一態様では、第1のピアデバイスでは、ユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信し、第1の連合ログインプロバイダから第1の認証応答を受信し、第2のピアデバイスから第2の認証応答を受信し、第2の連合ログインプロバイダによる第2の認証応答を認証し、第1の認証応答を第2のピアデバイスに送信し、第2のピアデバイスが連合ログインプロバイダによる第1の認証応答を認証したことを示す肯定応答を第2のピアデバイスから受信し、第1のピアデバイスが第2の認証応答を認証したことを示す肯定応答を第2のピアデバイスに送信し、第2のピアデバイスからの肯定応答に基づいて鍵交換を認証する。

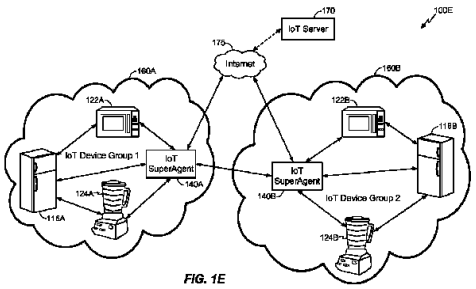


FIG. 1E

【特許請求の範囲】
【請求項１】
第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証する方法であって、
前記第1のピアデバイスによって、前記第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信するステップであって、前記第2のピアデバイスは、前記ユーザの前記連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信するステップと、
前記第1のピアデバイスによって、前記第1の連合ログインプロバイダから第1の認証応答を受信するステップであって、前記第2のピアデバイスは、前記第2の連合ログインプロバイダから第2の認証応答を受信するステップと、
前記第1のピアデバイスによって、前記第2のピアデバイスから前記第2の認証応答を受信するステップと、
前記第1のピアデバイスによって、前記第2の連合ログインプロバイダによる前記第2の認証応答を認証するステップと、
前記第1のピアデバイスによって、前記第1の認証応答を前記第2のピアデバイスに送信するステップであって、前記第2のピアデバイスは、前記第1の連合ログインプロバイダによる前記第1の認証応答を認証するステップと、
前記第1のピアデバイスによって、前記第2のピアデバイスが前記第1の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスから受信するステップと、
前記第1のピアデバイスによって、前記第1のピアデバイスが前記第2の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスに送信するステップと、
前記第1のピアデバイスによって、前記第2のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するステップであって、前記第2のピアデバイスは、前記第1のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するステップとを含む方法。
【請求項２】
前記第1の認証応答を受信するステップが、前記第1の認証応答によるHTMLリダイレクトを受信するステップを含む、請求項1に記載の方法。
【請求項３】
前記第1のピアデバイスは、前記HTMLリダイレクトに従うのではなく前記第1の認証応答を前記第2のピアデバイスに送信する、請求項2に記載の方法。
【請求項４】
前記ユーザの前記連合ログイン証明書および前記第1の識別子を前記第1の連合ログインプロバイダに送信する前に前記鍵交換を使用して前記第1のピアデバイスと前記第2のピアデバイスとの間にセキュアなセッションを確立するステップをさらに含む、請求項1に記載の方法。
【請求項５】
前記セキュアなセッションが、Diffie-Hellman鍵交換を使用して確立される、請求項4に記載の方法。
【請求項６】
前記第1の連合ログインプロバイダと前記第2の連合ログインプロバイダは異なる連合ログインプロバイダであり、前記第1の連合ログインプロバイダおよび前記第2の連合ログインプロバイダは、OpenIDプロバイダ、OAuthプロバイダ、またはFaceConnectプロバイダを含む、請求項1に記載の方法。
【請求項７】
前記第1の連合ログインプロバイダと前記第2の連合ログインプロバイダは同じ連合ログインプロバイダである、請求項1に記載の方法。
【請求項８】
前記第1のピアデバイスはコントローラピアデバイスを備え、前記第2のピアデバイスは被制御側デバイスを備える、請求項1に記載の方法。
【請求項９】

前記第1のピアデバイスによって、前記鍵交換に関する第1の公開鍵を生成するステップと、
前記第1のピアデバイスによって、前記第1の公開鍵を前記第2のピアデバイスに送信するステップと、
前記第1のピアデバイスによって、前記第2のピアデバイスから第2の公開鍵を受信するステップとを含む、請求項1に記載の方法。
【請求項１０】
前記第1の識別子は、前記第1の公開鍵、前記第1の公開鍵と前記第2の公開鍵との組合せ、前記第1の公開鍵と前記第2の公開鍵のハッシュ、または擬似ランダム関数(PRF)を使用して算出される前記第1の公開鍵と前記第2の公開鍵のベリファイアを含む、請求項9に記載の方法。
【請求項１１】
前記第1の識別子と前記第2の識別子は同じ識別子であり、前記第1の識別子と前記第2の識別子は、共通のハッシュまたは算出されたベリファイアを含む、請求項1に記載の方法。
【請求項１２】
前記第1の識別子と前記第2の識別子はそれぞれに異なる識別子であり、前記第1の識別子は、前記第1のピアデバイスによって生成される第1の公開鍵を含み、前記第2の識別子は、前記第2のピアデバイスによって生成される第2の公開鍵を含む、請求項1に記載の方法。
【請求項１３】
前記第2のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するステップは、前記第2のピアデバイスからの前記肯定応答を受信するステップに基づいて前記鍵交換を認証するステップを含む、請求項1に記載の方法。
【請求項１４】
第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するための装置であって、
前記第1のピアデバイスによって、前記第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信するように構成された論理であって、前記第2のピアデバイスは、前記ユーザの前記連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する論理と、
前記第1のピアデバイスによって、前記第1の連合ログインプロバイダから第1の認証応答を受信するように構成された論理であって、前記第2のピアデバイスは、前記第2の連合ログインプロバイダから第2の認証応答を受信する論理と、
前記第1のピアデバイスによって、前記第2のピアデバイスから前記第2の認証応答を受信するように構成された論理と、
前記第1のピアデバイスによって、前記第2の連合ログインプロバイダによる前記第2の認証応答を認証するように構成された論理と、
前記第1のピアデバイスによって、前記第1の認証応答を前記第2のピアデバイスに送信するように構成された論理であって、前記第2のピアデバイスは、前記第1の連合ログインプロバイダによる前記第1の認証応答を認証する論理と、
前記第1のピアデバイスによって、前記第2のピアデバイスが前記第1の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスから受信するように構成された論理と、
前記第1のピアデバイスによって、前記第1のピアデバイスが前記第2の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスに送信するように構成された論理と、
前記第1のピアデバイスによって、前記第2のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するように構成された論理であって、前記第2のピアデバイスは、前記第1のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証する論理とを備える装置。

【請求項１５】
前記第1の認証応答を受信するように構成された前記論理は、前記第1の認証応答によるHTMLリダイレクトを受信するように構成された論理を含む、請求項14に記載の装置。
【請求項１６】
前記第1のピアデバイスは、前記HTMLリダイレクトに従うのではなく前記第1の認証応答を前記第2のピアデバイスに送信する、請求項15に記載の装置。
【請求項１７】
前記ユーザの前記連合ログイン証明書および前記第1の識別子を前記第1の連合ログインプロバイダに送信する前に前記鍵交換を使用して前記第1のピアデバイスと前記第2のピアデバイスとの間にセキュアなセッションを確立するように構成された論理をさらに備える、請求項14に記載の装置。
【請求項１８】
前記セキュアなセッションは、Diffie-Hellman鍵交換を使用して確立される、請求項17に記載の装置。
【請求項１９】
前記第1の連合ログインプロバイダと前記第2の連合ログインプロバイダは異なる連合ログインプロバイダであり、前記第1の連合ログインプロバイダおよび前記第2の連合ログインプロバイダは、OpenIDプロバイダ、OAuthプロバイダ、またはFaceConnectプロバイダを含む、請求項14に記載の装置。
【請求項２０】
前記第1の連合ログインプロバイダと前記第2の連合ログインプロバイダは同じ連合ログインプロバイダである、請求項14に記載の装置。
【請求項２１】
前記第1のピアデバイスはコントローラピアデバイスを備え、前記第2のピアデバイスは被制御側デバイスを備える、請求項14に記載の装置。
【請求項２２】
前記第1のピアデバイスによって、前記鍵交換に関する第1の公開鍵を生成するように構成された論理と、
前記第1のピアデバイスによって、前記第1の公開鍵を第2のピアデバイスに送信するように構成された論理と、
前記第1のピアデバイスによって、前記第2のピアデバイスから前記第2の認証応答を受信するように構成された論理とをさらに備える、請求項14に記載の装置。
【請求項２３】
前記第1の識別子は、前記第1の公開鍵、前記第1の公開鍵と前記第2の公開鍵との組合せ、前記第1の公開鍵と前記第2の公開鍵のハッシュ、または擬似ランダム関数(PRF)を使用して算出される前記第1の公開鍵と前記第2の公開鍵のベリファイアを含む、請求項22に記載の装置。
【請求項２４】
前記第1の識別子と前記第2の識別子は同じ識別子であり、前記第1の識別子と前記第2の識別子は、共通のハッシュまたは算出されたベリファイアを含む、請求項14に記載の装置。
【請求項２５】
前記第1の識別子と前記第2の識別子はそれぞれに異なる識別子であり、前記第1の識別子は、前記第1のピアデバイスによって生成される第1の公開鍵を含み、前記第2の識別子は、前記第2のピアデバイスによって生成される第2の公開鍵を含む、請求項14に記載の装置。
【請求項２６】
前記第2のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するように構成された前記論理は、前記第2のピアデバイスからの前記肯定応答を受信することに基づいて前記鍵交換を認証するように構成された論理を備える、請求項14に記載の装置。

【請求項２７】
第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するための装置であって、
前記第1のピアデバイスによって、前記第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信するための手段であって、前記第2のピアデバイスは、前記ユーザの前記連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する手段と、
前記第1のピアデバイスによって、前記第1の連合ログインプロバイダから第1の認証応答を受信するための手段であって、前記第2のピアデバイスは、前記第2の連合ログインプロバイダから第2の認証応答を受信する手段と、
前記第1のピアデバイスによって、前記第2のピアデバイスから前記第2の認証応答を受信するための手段と、
前記第1のピアデバイスによって、前記第2の連合ログインプロバイダによる前記第2の認証応答を認証するための手段と、
前記第1のピアデバイスによって、前記第1の認証応答を前記第2のピアデバイスに送信するための手段であって、前記第2のピアデバイスは、前記第1の連合ログインプロバイダによる前記第1の認証応答を認証する手段と、
前記第1のピアデバイスによって、前記第2のピアデバイスが前記第1の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスから受信するための手段と、
前記第1のピアデバイスによって、前記第1のピアデバイスが前記第2の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスに送信するための手段と、
前記第1のピアデバイスによって、前記第2のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するための手段であって、前記第2のピアデバイスは、前記第1のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証する手段とを備える装置。
【請求項２８】
前記ユーザの前記連合ログイン証明書および前記第1の識別子を前記第1の連合ログインプロバイダに送信する前に前記鍵交換を使用して前記第1のピアデバイスと前記第2のピアデバイスとの間にセキュアなセッションを確立するための手段をさらに備える、請求項27に記載の装置。
【請求項２９】
第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するための非一時的コンピュータ可読記憶媒体であって、
前記第1のピアデバイスによって、前記第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信するための少なくとも1つの命令であって、前記第2のピアデバイスは、前記ユーザの前記連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第1の連合ログインプロバイダから第1の認証応答を受信するための少なくとも1つの命令であって、前記第2のピアデバイスは、前記第2の連合ログインプロバイダから第2の認証応答を受信する少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第2のピアデバイスから前記第2の認証応答を受信するための少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第2の連合ログインプロバイダによる前記第2の認証応答を認証するための少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第1の認証応答を前記第2のピアデバイスに送信するための少なくとも1つの命令であって、前記第2のピアデバイスは、前記第1の連合ログインプロバイダによる前記第1の認証応答を認証する少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第2のピアデバイスが前記第1の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスから受信するための少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第1のピアデバイスが前記第2の認証応答を認証

したことを示す肯定応答を前記第2のピアデバイスに送信するための少なくとも1つの命令と、

前記第1のピアデバイスによって、前記第2のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するための少なくとも1つの命令であって、前記第2のピアデバイスは、前記第1のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証する少なくとも1つの命令とを含む非一時的コンピュータ可読記憶媒体。

【請求項３０】

前記ユーザの前記連合ログイン証明書および前記第1の識別子を前記第1の連合ログインプロバイダに送信する前に前記鍵交換を使用して前記第1のピアデバイスと前記第2のピアデバイスとの間にセキュアなセッションを確立するための少なくとも1つの命令をさらに含む、請求項29に記載の非一時的コンピュータ可読記憶媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願の相互参照

本特許出願は、本出願の譲受人に譲渡され、その全体が参照により本明細書に明確に組み込まれる、2014年3月5日に出願された「USING END-USER FEDERATED LOGIN TO DETECT A BREACH IN A DIFFIE-HELLMAN KEY EXCHANGE ENCRYPTED CHANNEL」という名称の米国仮出願第61/948,433号の利益を主張する。

【０００２】

本明細書において説明する様々な実施形態は概して、エンドユーザ連合ログインを使用して鍵交換暗号化チャネルにおける違反を検出することに関する。

【背景技術】

【０００３】

インターネットは、標準インターネットプロトコルスイート(たとえば、伝送制御プロトコル(TCP)およびインターネットプロトコル(IP))を使用して互いに通信する、相互接続されたコンピュータならびにコンピュータネットワークのグローバルシステムである。モノのインターネット(IoT)は、コンピュータおよびコンピュータネットワークだけでなく、日常の物が、IoT通信ネットワーク(たとえば、アドホックシステムまたはインターネット)を介して読取り可能、認識可能、位置特定可能、アドレス指定可能、および制御可能であり得るという発想に基づく。

【０００４】

いくつかの市場動向がIoTデバイスの開発を推進している。たとえば、増大するエネルギーコストは、政府によるスマートグリッドに対する戦略投資、ならびに電気自動車および公共充電ステーションなど、将来の消費に対するサポートを推進している。増大する医療費および老齢人口は、遠隔/コネクテッドヘルスケア(connected health care)およびフィットネスサービスの開発を推進している。住居内の技術革命は、「N」プレイ(たとえば、データ、音声、ビデオ、セキュリティ、エネルギー管理など)をマーケティングして、ホームネットワークを拡張するサービスプロバイダによる統合を含めて、新しい「スマート」サービスの開発を推進している。企業設備の運転費を削減するための手段として、建造物はよりスマートかつより便利になっている。

【０００５】

IoT用のいくつかの重要なアプリケーションが存在する。たとえば、スマートグリッドおよびエネルギー管理の領域では、公益事業会社は住居および事業に対するエネルギーの配給を最適化することができるのに対して、カスタマはエネルギー使用をより良好に管理することができる。住居およびビルディングオートメーションの領域では、スマートホームおよびスマート建造物は、住居もしくは事務所内の、電化製品からプラグイン電気自動車(PEV)セキュリティシステムまで、事実上、どのようなデバイスまたはシステムに対しても集中制御し得る。資産管理の分野では、企業、病院、工場、および他の大型組織は、価値が高い設備、患者、車両などの位置を正確に追跡することができる。ヘルスおよびウ

ェルネスの領域では、医師は患者の健康を遠隔で監視することができるのに対して、人々はフィットネスルーチンの進捗を追跡することができる。

【発明の概要】

【課題を解決するための手段】

【０００６】

以下では、エンドユーザ連合ログインを使用して鍵交換暗号化チャネルにおける違反を検出するための本明細書において開示する機構に関連する1つまたは複数の態様および/または実施形態に関する簡略化された概要を示す。したがって、以下の概要は、すべての考えられる態様および/または実施形態に関連する包括的な概説と見なされるべきではなく、また、以下の概要は、すべての考えられる態様および/または実施形態に関連する重要な、または決定的な要素を特定するか、任意の特定の態様および/または実施形態に関連付けられる範囲を定めると見なされるべきでもない。したがって、以下の概要は、以下に提示される詳細な説明に先立って、本明細書において開示される機構に関連する1つまたは複数の態様および/または実施形態に関連する特定の概念を簡略化された形で提示することが唯一の目的である。

【０００７】

第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するためのシステムおよび方法を開示する。第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証する方法は、第1のピアデバイスによって、第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信するステップであって、第2のピアデバイスが、ユーザの連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信するステップと、第1のピアデバイスによって、第1の連合ログインプロバイダから第1の認証応答を受信するステップであって、第2のピアデバイスが、第2の連合ログインプロバイダから第2の認証応答を受信するステップと、第1のピアデバイスによって、第2のピアデバイスから第2の認証応答を受信するステップと、第1のピアデバイスによって、第2の連合ログインプロバイダによる第2の認証応答を認証するステップと、第1のピアデバイスによって、第1の認証応答を第2のピアデバイスに送信するステップであって、第2のピアデバイスが、第1の連合ログインプロバイダによる第1の認証応答を認証するステップと、第1のピアデバイスによって、第2のピアデバイスが第1の認証応答を認証したことを示す肯定応答を第2のピアデバイスから受信するステップと、第1のピアデバイスによって、第1のピアデバイスが第2の認証応答を認証したことを示す肯定応答を第2のピアデバイスに送信するステップと、第1のピアデバイスによって、第2のピアデバイスからの肯定応答に基づいて鍵交換を認証するステップであって、第2のピアデバイスが第1のピアデバイスからの肯定応答に基づいて鍵交換を認証するステップとを含む。

【０００８】

第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するための装置は、第1のピアデバイスによって、第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信するように構成された論理であって、第2のピアデバイスが、ユーザの連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する論理と、第1のピアデバイスによって、第1の連合ログインプロバイダから第1の認証応答を受信するように構成された論理であって、第2のピアデバイスが、第2の連合ログインプロバイダから第2の認証応答を受信する論理と、第1のピアデバイスによって、第2のピアデバイスから第2の認証応答を受信するように構成された論理と、第1のピアデバイスによって、第2の連合ログインプロバイダによる第2の認証応答を認証するように構成された論理と、第1のピアデバイスによって、第1の認証応答を第2のピアデバイスに送信するように構成された論理であって、第2のピアデバイスが、第1の連合ログインプロバイダによる第1の認証応答を認証する論理と、第1のピアデバイスによって、第2のピアデバイスが第1の認証応答を認証したことを示す肯定応答を第2のピアデバイスから受信するように構成された論理と、第1のピアデバイスによって、第1のピアデバイスが第2の認証応答を認証したことを示す肯定応答を第2のピアデバイスに送信するように構成さ

れた論理と、第1のピアデバイスによって、第2のピアデバイスからの肯定応答に基づいて鍵交換を認証するように構成された論理であって、第2のピアデバイスが第1のピアデバイスからの肯定応答に基づいて鍵交換を認証する論理とを含む。

【０００９】

第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するための装置は、第1のピアデバイスによって、第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信するための手段であって、第2のピアデバイスが、ユーザの連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する手段と、第1のピアデバイスによって、第1の連合ログインプロバイダから第1の認証応答を受信するための手段であって、第2のピアデバイスが、第2の連合ログインプロバイダから第2の認証応答を受信する手段と、第1のピアデバイスによって、第2のピアデバイスから第2の認証応答を受信するための手段と、第1のピアデバイスによって、第2の連合ログインプロバイダによる第2の認証応答を認証するための手段と、第1のピアデバイスによって、第1の認証応答を第2のピアデバイスに送信するための手段であって、第2のピアデバイスが、第1の連合ログインプロバイダによる第1の認証応答を認証するための手段と、第1のピアデバイスによって、第2のピアデバイスが第1の認証応答を認証したことを示す肯定応答を第2のピアデバイスから受信するための手段と、第1のピアデバイスによって、第1のピアデバイスが第2の認証応答を認証したことを示す肯定応答を第2のピアデバイスに送信するための手段と、第1のピアデバイスによって、第2のピアデバイスからの肯定応答に基づいて鍵交換を認証するための手段であって、第2のピアデバイスが第1のピアデバイスからの肯定応答に基づいて鍵交換を認証する手段とを含む。

【００１０】

第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するための非一時的コンピュータ可読記憶媒体は、第1のピアデバイスによって、第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信するための少なくとも1つの命令と、第2のピアデバイスが、ユーザの連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信するための少なくとも1つの命令と、第1のピアデバイスによって、第1の連合ログインプロバイダから第1の認証応答を受信するための少なくとも1つの命令であって、第2のピアデバイスが、第2の連合ログインプロバイダから第2の認証応答を受信する少なくとも1つの命令と、第1のピアデバイスによって、第2のピアデバイスから第2の認証応答を受信するための少なくとも1つの命令と、第1のピアデバイスによって、第2の連合ログインプロバイダによる第2の認証応答を認証するための少なくとも1つの命令と、第1のピアデバイスによって、第1の認証応答を第2のピアデバイスに送信するための少なくとも1つの命令であって、第2のピアデバイスが、第1の連合ログインプロバイダによる第1の認証応答を認証する少なくとも1つの命令と、第1のピアデバイスによって、第2のピアデバイスが第1の認証応答を認証したことを示す肯定応答を第2のピアデバイスから受信するための少なくとも1つの命令と、第1のピアデバイスによって、第1のピアデバイスが第2の認証応答を認証したことを示す肯定応答を第2のピアデバイスに送信するための少なくとも1つの命令と、第1のピアデバイスによって、第2のピアデバイスからの肯定応答に基づいて鍵交換を認証するための少なくとも1つの命令であって、第2のピアデバイスが第1のピアデバイスからの肯定応答に基づいて鍵交換を認証する少なくとも1つの命令とを含む。

【００１１】

本明細書において開示される機構に関連付けられる他の目的および利点は、添付の図面および詳細な説明に基づいて、当業者に明らかになるであろう。

【００１２】

本開示の態様およびその付随する利点の多くに関するより完全な理解は、以下の詳細な説明を参照しながら、本発明を限定するためではなく単に例示するために提示される添付の図面とともに考察することによって、本開示の態様およびその付随する利点の多くがより深く理解されるようになるときに容易に得られるであろう。

【図面の簡単な説明】
【００１３】
【図１Ａ】本開示の一態様によるワイヤレス通信システムのハイレベルシステムアーキテクチャを示す図である。
【図１Ｂ】本開示の別の態様によるワイヤレス通信システムのハイレベルシステムアーキテクチャを示す図である。
【図１Ｃ】本開示の一態様によるワイヤレス通信システムのハイレベルシステムアーキテクチャを示す図である。
【図１Ｄ】本開示の一態様によるワイヤレス通信システムのハイレベルシステムアーキテクチャを示す図である。
【図１Ｅ】本開示の一態様によるワイヤレス通信システムのハイレベルシステムアーキテクチャを示す図である。
【図２Ａ】本開示の態様による例示的なモノのインターネット(IoT)デバイスを示す図である。
【図２Ｂ】本開示の態様による例示的な受動IoTデバイスを示す図である。
【図３】本開示の態様による、機能を実現するように構成された論理を含む通信デバイスを示す図である。
【図４】本開示の様々な態様による例示的なサーバを示す図である。
【図５】本開示の一態様による、発見可能なピアツーピア(P2P)サービスをサポートすることのできるワイヤレス通信ネットワークを示す図である。
【図６】本開示の一態様による、様々なデバイスが通信するのに利用することができる近接度ベースの分散バスを確立するために発見可能なP2Pサービスを使用し得る例示的な環境を示す図である。
【図７】本開示の一態様による、様々なデバイスが通信するのに利用することができる近接度ベースの分散バスを確立するために発見可能なP2Pサービスを使用し得る例示的なメッセージシーケンスを示す図である。
【図８】本開示のセキュリティサービスのための例示的なシステムアーキテクチャを示す図である。
【図９】本開示の一態様による、OpenIDプロバイダを認証に使用するための例示的なフローを示す図である。
【図１０】本開示の一態様による、2つのクライアント間にセキュアなチャネルを確立するための例示的なフローを示す図である。
【図１１】本開示の一態様による、図8に示す、コントローラと、バンドリングされたセキュリティブリッジを含む被制御側との間のOpenID検証を示す図である。
【図１２】本開示の一態様による、図8に示す、コントローラと、バンドリングされたセキュリティブリッジを含まない被制御側との間のOAuth検証を示す図である。
【図１３】本開示の一態様による、第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するための例示的なフローを示す図である。
【図１４】本明細書で教示する通信をサポートするように構成された装置のサンプル態様の簡略ブロック図である。
【発明を実施するための形態】
【００１４】
本開示は、第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するためのシステムおよび方法を対象とする。一態様では、第1のピアデバイスは、第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信し、第2のピアデバイスは、ユーザの連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する。第1のピアデバイスは、第1の連合ログインプロバイダから第1の認証応答を受信し、第2のピアデバイスは、第2の連合ログインプロバイダから第2の認証応答を受信する。第1のピアデバイスは、第2のピアデバイスから第2の認証応答を受信し、第2の連合ログインプロバイダによる第2の認証応答を認証し、第1の認証応答を

第2のピアデバイスに送信し、第2のピアデバイスは、第1の連合ログインプロバイダによる第1の認証応答を認証する。第1のピアデバイスは、第2のピアデバイスが第1の認証応答を認証したことを示す肯定応答を第2のピアデバイスから受信し、第1のピアデバイスが第2の認証応答を認証したことを示す肯定応答を第2のピアデバイスに送信し、第2のピアデバイスからの肯定応答に基づいて鍵交換を認証し、第2のピアデバイスは、第1のピアデバイスからの肯定応答に基づいて鍵交換を認証する。

【００１５】

これらの態様およびその他の態様が、本開示の例示的な実施形態に関する特定の例を示すために以下の説明および関連する図面において開示される。代替的実施形態は、この開示を読むと当業者には明らかであり、本開示の範囲または趣旨を逸脱することなく構築され、実践され得る。加えて、本明細書で開示する態様および実施形態の関連する詳細を不明瞭にしないように、よく知られている要素は詳細には説明されず、または省略され得る。

【００１６】

「例示的」という言葉は、本明細書では「例、事例、または例示として機能すること」を意味するために使用される。本明細書で「例示的」として説明するいかなる実施形態も、必ずしも他の実施形態よりも好ましいか、または有利であると解釈されるべきではない。同様に、「実施形態」という用語は、すべての実施形態が、論じられた特徴、利点または動作モードを含むことを要求しない。

【００１７】

本明細書で使用される用語は、特定の実施形態のみを説明しており、本明細書で開示されるいずれかの実施形態を限定すると解釈されるべきではない。本明細書で使用される単数形「a」、「an」、および「the」は、文脈が別段に明確に示すのでなければ、複数形をも含むものとする。さらに、「含む(comprises)」、「含んでいる(comprising)」、「含む(includes)」、および/または「含んでいる(including)」という用語は、本明細書で使用すると、述べられた特徴、整数、ステップ、動作、要素、および/または構成要素の存在を明示するが、1つまたは複数の他の特徴、整数、ステップ、動作、要素、構成要素、および/またはそれらのグループの存在または追加を排除しないことが理解されよう。

【００１８】

さらに、多くの態様について、たとえばコンピューティングデバイスの要素によって実施されるべき、動作のシーケンスに関して説明する。本明細書で説明する様々な動作は、特定の回路(たとえば、特定用途向け集積回路(ASIC))によって、1つまたは複数のプロセッサによって実行されるプログラム命令によって、あるいは両方の組合せによって実施され得ることは認識されよう。さらに、本明細書で説明されるこれらの一連の動作は、実行されると、関連するプロセッサに本明細書において説明される機能を実行させることになる対応する1組のコンピュータ命令を記憶した、任意の形のコンピュータ可読記憶媒体内で完全に具現されるものと見なされ得る。したがって、本開示の様々な態様は、特許請求される主題の範囲内にすべて入ることが企図されているいくつかの異なる形で具現され得る。さらに、本明細書で説明される実施形態ごとに、任意のそのような実施形態の対応する形は、本明細書において、たとえば、説明される動作を実行する「ように構成された論理」として説明される場合がある。

【００１９】

本明細書で使用する「モノのインターネットデバイス」(すなわち「IoTデバイス」)という用語は、アドレス指定可能なインターフェース(たとえば、インターネットプロトコル(IP)アドレス、Bluetooth(登録商標)識別子(ID)、近距離無線通信(NFC:near-field communication)IDなど)を有し、有線またはワイヤレス接続を通じて1つまたは複数の他のデバイスに情報を送信することができる任意の物(たとえば、電化製品、センサーなど)を指すことができる。IoTデバイスは、クイックレスポンス(QR)コード、無線周波数識別(RFID)タグ、NFCタグなどの受動通信インターフェース、または、モデム、トランシーバ、送信機-受信機などの能動通信インターフェースを有し得る。IoTデバイスは、中央処理装置(C

PU)、マイクロプロセッサ、ASICなどの中に組み込まれること、および/あるいは、それらによって制御/監視されることが可能であり、ローカルアドホックネットワークまたはインターネットなどのIoTネットワークに接続するように構成された特定の属性セット(たとえば、IoTデバイスがオンであるか、もしくはオフであるか、開いているか、もしくは閉じているか、アイドルであるか、もしくはアクティブであるか、タスク実行のために利用可能であるか、もしくはビジーであるかなど、冷房機能であるか、もしくは暖房機能であるか、環境監視機能であるか、もしくは環境記録機能であるか、発光機能であるか、音響放射機能であるかなど、デバイスの状態またはステータス)を有し得る。たとえば、IoTデバイスは、これらのデバイスがIoTネットワークと通信するためのアドレス指定可能通信インターフェースを備える限り、冷蔵庫、トースター、オーブン、電子レンジ、冷凍庫、皿洗い機、パラボラアンテナ(dishes)、手工具、洗濯機、衣類乾燥機、加熱炉、空調機、温度自動調整器、テレビジョン、照明設備、掃除機、スプリンクラー、電気メータ、ガスメータなどを含み得るが、これらに限定されない。IoTデバイスはまた、セルフォン、スマートフォン、デスクトップコンピュータ、ラップトップコンピュータ、タブレットコンピュータ、携帯情報端末(PDA)などを含み得る。したがって、IoTネットワークは、通常はインターネット接続性を有しないデバイス(たとえば、皿洗い機など)に加えて、「レガシー」インターネットアクセス可能デバイス(たとえば、ラップトップコンピュータまたはデスクトップコンピュータ、セルフォンなど)の組合せから構成され得る。

【００２０】

図1Aは、本開示の一態様によるワイヤレス通信システム100Aのハイレベルシステムアーキテクチャを示す。ワイヤレス通信システム100Aは、テレビジョン110と、屋外空調機112と、温度自動調整器114と、冷蔵庫116と、洗濯機および乾燥機118とを含む、複数のIoTデバイスを含む。

【００２１】

図1Aを参照すると、IoTデバイス110～118は、図1Aにエアインターフェース108および直接有線接続109として示す物理通信インターフェースまたは物理通信レイヤを介してアクセスネットワーク(たとえば、アクセスポイント125)と通信するように構成される。エアインターフェース108は、IEEE 802.11など、ワイヤレスインターネットプロトコル(IP)に準拠し得る。図1Aは、エアインターフェース108を介して通信するIoTデバイス110～118と、直接有線接続109を介して通信するIoTデバイス118とを示すが、各IoTデバイスは、有線接続もしくはワイヤレス接続、または両方を介して通信することができる。

【００２２】

インターネット175は、いくつかのルーティングエージェントおよび処理エージェント(便宜上、図1Aには示されていない)を含む。インターネット175は、標準インターネットプロトコルスイート(たとえば、伝送制御プロトコル(TCP)およびIP)を使用して、異種のデバイス/ネットワークの間で通信する、相互接続されたコンピュータならびにコンピュータネットワークのグローバルシステムである。TCP/IPは、データが、宛先において、どのようにフォーマッティング、アドレス指定、送信、経路指定、および受信されるべきかを指定するエンドツーエンド接続性を提供する。

【００２３】

図1Aでは、デスクトップコンピュータまたはパーソナルコンピュータ(PC)などのコンピュータ120は、(たとえば、Ethernet(登録商標)接続またはWi-Fiもしくは802.11ベースのネットワークを介して)インターネット175と直接接続するとして示される。コンピュータ120は、(たとえば、有線接続性とワイヤレス接続性の両方を有するWiFiルータ用の)アクセスポイント125自体などに相当してよいモデムまたはルータとの直接接続など、インターネット175との有線接続を有し得る。代替的に、有線接続を介して、アクセスポイント125およびインターネット175に接続されるのではなく、コンピュータ120は、エアインターフェース108または別のワイヤレスインターフェースを介してアクセスポイント125に接続されてよく、エアインターフェース108を介してインターネット175にアクセスしてよい。デスクトップコンピュータとして例示されているが、コンピュータ120は、ラップトップ

コンピュータ、タブレットコンピュータ、PDA、スマートフォンなどであり得る。コンピュータ120は、IoTデバイスであり得、かつ/またはIoTデバイス110～118のネットワーク/グループなど、IoTネットワーク/グループを管理するための機能を含み得る。

【００２４】

アクセスポイント125は、たとえば、FiOS、ケーブルモデム、デジタル加入者線(DSL)モデムなど、光通信システムを介して、インターネット175に接続され得る。アクセスポイント125は、標準インターネットプロトコル(たとえば、TCP/IP)を使用して、IoTデバイス110～120およびインターネット175と通信することができる。

【００２５】

図1Aを参照すると、IoTサーバ170は、インターネット175に接続されるように示されている。IoTサーバ170は、複数の構造的に別々の複数のサーバとして実装され得るか、または代替的には、単一のサーバに対応し得る。一態様では、IoTサーバ170は、(点線によって示されるように)オプションであり、IoTデバイス110～120のグループは、ピアツーピア(P2P)ネットワークであり得る。そのような場合、IoTデバイス110～120は、エアインターフェース108および/または直接有線接続109を介して互いに直接通信することができる。代替的に、または追加として、IoTデバイス110～120の一部またはすべては、エアインターフェース108および直接有線接続109に依存しない通信インターフェースで構成され得る。たとえば、エアインターフェース108がWiFiインターフェースに対応する場合、IoTデバイス110～120のうちの1つもしくは複数は、互いに、または他のBluetooth(登録商標)対応デバイスもしくはNFC対応デバイスと直接通信するためのBluetooth(登録商標)インターフェースあるいはNFCインターフェースを有し得る。

【００２６】

ピアツーピアネットワークでは、サービス発見方式は、ノードの存在、その能力、およびグループメンバーシップをマルチキャストすることができる。ピアツーピアデバイスは、この情報に基づいて、関連性および後続の相互作用を確立することができる。

【００２７】

本開示の一態様によれば、図1Bは、複数のIoTデバイスを含む別のワイヤレス通信システム100Bのハイレベルアーキテクチャを示す。一般に、図1Bに示すワイヤレス通信システム100Bは、上でより詳細に説明した、図1Aに示すワイヤレス通信システム100Aと同じ、ならびに/または実質的に同様の様々な構成要素(たとえば、エアインターフェース108および/もしくは直接有線接続109を介してアクセスポイント125と通信するように構成された、テレビジョン110と、屋外空調機112と、温度自動調整器114と、冷蔵庫116と、洗濯機および乾燥機118とを含む様々なIoTデバイス、インターネット175に直接接続する、かつ/あるいはアクセスポイント125を通してインターネット175に接続するコンピュータ120、ならびにインターネット175を介してアクセス可能なIoTサーバ170など)を含み得る。したがって、説明を簡潔かつ簡単にするために、同じまたは同様の詳細が図1Aに示したワイヤレス通信システム100Aに関して上ですでに提供されている限り、図1Bに示すワイヤレス通信システム100B内のいくつかの構成要素に関する様々な詳細は本明細書で省略される場合がある。

【００２８】

図1Bを参照すると、ワイヤレス通信システム100Bは、代替的に、IoTマネージャ130またはIoTマネージャデバイス130と呼ばれる場合もあるスーパーバイザデバイス130を含み得る。したがって、以下の説明が「スーパーバイザデバイス」130という用語を使用する場合、IoTマネージャ、グループ所有者、または同様の用語に対するいずれの参照もスーパーバイザデバイス130、あるいは同じもしくは実質的に同様の機能を提供する別の物理的構成要素または論理的構成要素を指す場合があることを当業者は諒解されよう。

【００２９】

一実施形態では、スーパーバイザデバイス130は、一般に、ワイヤレス通信システム100B内の様々な他の構成要素を観測、監視、制御、あるいは管理することができる。たとえば、スーパーバイザデバイス130は、エアインターフェース108および/または直接有線接

続109を介してアクセスネットワーク(たとえば、アクセスポイント125)と通信して、ワイヤレス通信システム100B内の様々なIoTデバイス110～120に関連付けられた属性、活動、もしくは他の状態を監視または管理することができる。スーパーバイザデバイス130は、インターネット175に対して、および、オプションで、(点線として示される)IoTサーバ170に対して、有線接続またはワイヤレス接続を有し得る。スーパーバイザデバイス130は、様々なIoTデバイス110～120に関連付けられた属性、活動、もしくは他の状態をさらに監視または管理するために使用され得る情報をインターネット175および/あるいはIoTサーバ170から取得することができる。スーパーバイザデバイス130は、独立型デバイスであってよく、または、コンピュータ120など、IoTデバイス110～120のうちの1つであってもよい。スーパーバイザデバイス130は、物理デバイスであってよく、または物理デバイス上で実行するソフトウェアアプリケーションであってもよい。スーパーバイザデバイス130は、IoTデバイス110～120に関連付けられた、監視される属性、活動、または他の状態に関する情報を出力して、それらに関連付けられた属性、活動、または他の状態を制御あるいは管理するための入力情報を受信することができるユーザインターフェースを含み得る。したがって、スーパーバイザデバイス130は、一般に、様々な構成要素を含むことが可能であり、ワイヤレス通信システム100B内の様々な構成要素を観測、監視、制御、あるいは管理するために様々な有線通信インターフェースおよびワイヤレス通信インターフェースをサポートし得る。

【００３０】

図1Bに示すワイヤレス通信システム100Bは、ワイヤレス通信システム100Bに結合され得るか、あるいはワイヤレス通信システム100Bの一部であり得る(能動IoTデバイス110～120と対照的な)1つまたは複数の受動IoTデバイス105を含み得る。一般に、受動IoTデバイス105は、短距離インターフェースを介して問い合わされたとき、その識別子と属性とを別のデバイスに提供することができる、バーコード付きデバイス、Bluetooth(登録商標)デバイス、無線周波数(RF)デバイス、RFIDタグ付きデバイス、赤外線(IR)デバイス、NFCタグ付きデバイス、または任意の他の適切なデバイスを含み得る。能動IoTデバイスは、受動IoTデバイスの属性の変化を検出すること、記憶すること、通信すること、それらの変化に作用することなどが可能である。

【００３１】

たとえば、受動IoTデバイス105は、各々、RFIDタグまたはバーコードを有するコーヒーカップとオレンジジュースの容器とを含み得る。キャビネットIoTデバイスおよび冷蔵庫IoTデバイス116は、各々、RFIDタグもしくはバーコードを読み取って、コーヒーカップおよび/またはオレンジジュースの容器の受動IoTデバイス105がいつ追加あるいは除去されたかを検出することができる適切なスキャナまたはリーダーを有し得る。キャビネットIoTデバイスがコーヒーカップの受動IoTデバイス105の除去を検出し、冷蔵庫IoTデバイス116がオレンジジュースの容器の受動IoTデバイスの除去を検出すると、スーパーバイザデバイス130は、キャビネットIoTデバイスおよび冷蔵庫IoTデバイス116において検出された活動に関する1つまたは複数の信号を受信することができる。スーパーバイザデバイス130は、次いで、ユーザがコーヒーカップからオレンジジュースを飲んでいる、およびまたはコーヒーカップからオレンジジュースを飲みたいことを推定することができる。

【００３２】

上記は何らかの形のRFIDタグ通信インターフェースまたはバーコード通信インターフェースを有するとして受動IoTデバイス105を説明しているが、受動IoTデバイス105は、そのような通信能力を有しない、1つもしくは複数のデバイスまたは他の物理的対象物を含み得る。たとえば、あるIoTデバイスは、受動IoTデバイス105を識別するために、受動IoTデバイス105に関連付けられた形状、サイズ、色、および/もしくは他の観測可能な特徴を検出することができる適切なスキャナ機構またはリーダー機構を有し得る。このようにして、任意の適切な物理的対象物はその識別情報および属性を通信して、ワイヤレス通信システム100Bの一部になることができ、スーパーバイザデバイス130を用いて観測、監視、制御、あるいは管理され得る。さらに、受動IoTデバイス105は、図1Aのワイヤレス通信シス

テム100Aに結合され得るか、あるいはその一部であり得、実質的に同様の形で、観測、監視、制御、または管理され得る。

【００３３】

本開示の別の態様によれば、図1Cは、複数のIoTデバイスを含む別のワイヤレス通信システム100Cのハイレベルアーキテクチャを示す。一般に、図1Cに示すワイヤレス通信システム100Cは、上でより詳細に説明した、図1Aおよび図1Bにそれぞれ示したワイヤレス通信システム100Aならびに100Bと同じ、かつ/または実質的に同様の様々な構成要素を含み得る。したがって、説明を簡潔かつ簡単にするために、同じまたは類似の詳細が、それぞれ、図1Aおよび図1Bに示したワイヤレス通信システム100Aならびに100Bに関して上ですでに提供されている限り、図1Cに示すワイヤレス通信システム100C内のいくつかの構成要素に関する様々な詳細は本明細書で省略される場合がある。

【００３４】

図1Cに示す通信システム100Cは、IoTデバイス110～118とスーパーバイザデバイス130との間の例示的なピアツーピア通信を示す。図1Cに示すように、スーパーバイザデバイス130は、IoTスーパーバイザインターフェースを介してIoTデバイス110～118の各々と通信する。さらに、IoTデバイス110および114、IoTデバイス112、114、および116、ならびにIoTデバイス116および118は、互いに直接通信する。

【００３５】

IoTデバイス110～118はIoTグループ160を構成する。IoTデバイスグループ160は、ユーザのホームネットワークに接続されたIoTデバイスなど、ローカルに接続されたIoTデバイスのグループである。示さないが、複数のIoTデバイスグループは、インターネット175に接続されたIoT SuperAgent140を介して互いに接続されること、および/または通信することが可能である。ハイレベルで、スーパーバイザデバイス130はグループ内通信を管理するのに対して、IoT SuperAgent140はグループ間通信を管理することができる。別個のデバイスとして示すが、スーパーバイザデバイス130およびIoT SuperAgent140は、同じデバイス(たとえば、図1Aのコンピュータ120など、独立型デバイスもしくはIoTデバイス)であり得るか、またはその中に存在し得る。代替的に、IoT SuperAgent140は、アクセスポイント125の機能に対応し得るか、またはその機能を含み得る。さらに別の代替として、IoT SuperAgent140は、IoTサーバ170などのIoTサーバの機能に対応し得るか、またはその機能を含み得る。IoT SuperAgent140は、ゲートウェイ機能145をカプセル化することができる。

【００３６】

各IoTデバイス110～118は、スーパーバイザデバイス130をピアとして扱って、属性/スキーマ更新をスーパーバイザデバイス130に送信することができる。IoTデバイスが別のIoTデバイスと通信する必要があるとき、IoTデバイスは、スーパーバイザデバイス130にそのIoTデバイスに対するポインタを要求し、次いで、ピアとしてターゲットIoTデバイスと通信することができる。IoTデバイス110～118は、共通メッセージングプロトコル(CMP)を使用して、ピアツーピア通信ネットワークを介して互いに通信する。2つのIoTデバイスがCMP対応であり、共通通信トランスポートを介して接続される限り、それらのIoTデバイスは互いに通信することができる。プロトコルスタック内で、CMPレイヤ154は、アプリケーションレイヤ152の下にあり、トランスポートレイヤ156および物理レイヤ158の上にある。

【００３７】

本開示の別の態様によれば、図1Dは、複数のIoTデバイスを含む別のワイヤレス通信システム100Dのハイレベルアーキテクチャを示す。一般に、図1Dに示すワイヤレス通信システム100Dは、それぞれ、上でより詳細に説明した、図1A～図1Cに示したワイヤレス通信システム100A～100Cと同じ、かつ/または実質的に類似した様々構成要素を含み得る。したがって、説明を簡潔かつ簡単にするために、同じまたは類似の詳細がそれぞれ図1A～図1Cに示したワイヤレス通信システム100A～100Cに関して上ですでに提供されている限り、図1Dに示すワイヤレス通信システム100D内のいくつかの構成要素に関する様々な詳細は本明

細書で省略される場合がある。

【００３８】

インターネット175は、IoTの概念を使用して調整され得る「リソース」である。しかしながら、インターネット175は、調整されるリソースのほんの一例であり、任意のリソースがIoTの概念を使用して調整され得る。調整され得る他のリソースは、電気、ガス、ストレージ、セキュリティなどを含むが、これらに限定されない。IoTデバイスは、リソースに接続され得、それによって、リソースを調整するか、またはリソースはインターネット175を介して調整され得る。図1Dは、天然ガス、ガソリン、湯、および電気など、いくつかのリソース180を示し、リソース180は、インターネット175に加えて調整され得るか、またはインターネット175を介して調整され得る。

【００３９】

IoTデバイスは、互いに通信して、リソース180の使用を調整することができる。たとえば、トースター、コンピュータ、およびヘアドライヤなどのIoTデバイスは、Bluetooth(登録商標)通信インターフェースを介して互いに通信して、その電気(リソース180)使用を調整することができる。別の例として、デスクトップコンピュータ、電話、およびタブレットコンピュータなどのIoTデバイスは、Wi-Fi通信インターフェースを介して通信して、インターネット175(リソース180)に対するそのアクセスを調整することができる。さらに別の例として、ストーブ、衣類乾燥機、および湯沸かし器などのIoTデバイスは、Wi-Fi通信インターフェースを介して通信して、そのガス使用を調整することができる。代替的に、または追加として、各IoTデバイスは、IoTデバイスから受信された情報に基づいて、そのリソース180の使用を調整するための論理を有する、IoTサーバ170などのIoTサーバに接続され得る。

【００４０】

本開示の別の態様によれば、図1Eは、複数のIoTデバイスを含む別のワイヤレス通信システム100Eのハイレベルアーキテクチャを示す。一般に、図1Eに示すワイヤレス通信システム100Eは、上でより詳細に説明した、それぞれ、図1A～図1Dに示したワイヤレス通信システム100A～100Dと同じ、かつ/または実質的に類似した様々構成要素を含み得る。したがって、説明を簡潔かつ簡単にするために、同じまたは類似の詳細がそれぞれ図1A～図1Dに示したワイヤレス通信システム100A～100Dに関して上ですでに提供されている限り、図1Eに示すワイヤレス通信システム100E内のいくつかの構成要素に関する様々な詳細は本明細書で省略される場合がある。

【００４１】

通信システム100Eは、2つのIoTデバイスグループ160Aおよび160Bを含む。複数のIoTデバイスグループは、インターネット175に接続されたIoT SuperAgentを介して互いに接続されること、および/または互いに通信することが可能である。ハイレベルで、IoT SuperAgentは、IoTデバイスグループ内のグループ間通信を管理することができる。たとえば、図1Eで、IoTデバイスグループ160Aは、IoTデバイス116A、122A、および124Aと、IoT SuperAgent140Aとを含むのに対して、IoTデバイスグループ160Bは、IoTデバイス116B、122B、および124Bと、IoT SuperAgent140Bとを含む。したがって、IoT SuperAgent140Aおよび140Bは、インターネット175と接続して、インターネット175を介して互いと通信すること、ならびに/またはIoTデバイスグループ160Aおよび160B間の通信を促すために互いと直接通信することができる。さらに、図1Eは、IoT SuperAgent140Aおよび140Bを介して互いと通信する2つのIoTデバイスグループ160Aおよび160Bを示すが、任意の数のIoTデバイスグループが、IoT SuperAgentを使用して互いと好適に通信することができることを当業者は諒解されよう。

【００４２】

図2Aは、本開示の態様によるIoTデバイス200Aのハイレベルな例を示す。外観および/または内部構成要素はIoTデバイス間でかなり異なる場合があるが、大部分のIoTデバイスは、ディスプレイとユーザ入力のための手段とを含み得る、ある種のユーザインターフェースを有することになる。ユーザインターフェースがないIoTデバイスは、図1A～図1Bにお

けるエアインターフェース108など、有線ネットワークまたはワイヤレスネットワークを介してリモートで通信され得る。

【００４３】

図2Aに示すように、IoTデバイス200Aに関する例示的な構成では、IoTデバイス200Aの外部ケーシングは、当技術分野で知られているように、構成要素の中でも、ディスプレイ226と、電源ボタン222と、2つの制御ボタン224Aおよび224Bとで構成され得る。ディスプレイ226は、タッチスクリーンディスプレイであり得、その場合、制御ボタン224Aおよび224Bは必要でない場合がある。IoTデバイス200Aの一部として明示的に示されてはいないが、IoTデバイス200Aは、限定はしないが、Wi-Fiアンテナ、セルラーアンテナ、衛星位置システム(SPS)アンテナ(たとえば、全地球測位システム(GPS)アンテナ)などを含む、1つまたは複数の外部アンテナおよび/または外部ケーシングに内蔵される1つのまたは複数の内蔵アンテナを含むことができる。

【００４４】

IoTデバイス200AなどのIoTデバイスの内部構成要素は異なるハードウェア構成によって具体化され得るが、内部ハードウェア構成要素のための基本的なハイレベル構成は図2Aにプラットフォーム202として示されている。プラットフォーム202は、図1A～図1Bのエアインターフェース108ならびに/または有線インターフェースなど、ネットワークインターフェースを介して送信されたソフトウェアアプリケーション、データ、および/またはコマンドを受信ならびに実行することができる。プラットフォーム202は、ローカルに記憶されたアプリケーションを独立して実行してもよい。プラットフォーム202は、一般に、プロセッサ208と呼ばれることになる、マイクロコントローラ、マイクロプロセッサ、特定用途向け集積回路、デジタル信号プロセッサ(DSP)、プログラマブル論理回路、または他のデータ処理デバイスなど、1つもしくは複数のプロセッサ208に動作可能に結合された有線通信および/あるいはワイヤレス通信のために構成された1つもしくは複数のトランシーバ206(たとえば、Wi-Fiトランシーバ、Bluetooth(登録商標)トランシーバ、セルラートランシーバ、衛星トランシーバ、GPS受信機またはSPS受信機など)を含み得る。プロセッサ208は、IoTデバイス内のメモリ212内でアプリケーションプログラミング命令を実行することができる。メモリ212は、読取り専用メモリ(ROM)、ランダムアクセスメモリ(RAM)、電気消去可能プログラマブルROM(EEPROM)、フラッシュカード、またはコンピュータプラットフォームに共通の任意のメモリのうちの1つもしくは複数を含み得る。1つもしくは複数の入出力(I/O)インターフェース214は、プロセッサ208が、示すようなディスプレイ226、電源ボタン222、制御ボタン224Aおよび224Bなどの様々なI/Oデバイス、ならびにIoTデバイス200Aに関連付けられたセンサー、アクチュエータ、リレー、バルブ、スイッチなどの任意の他のデバイスと通信すること、ならびにそれらから制御することを可能にするように構成され得る。プラットフォーム202は、メモリ212に記憶された実行可能なモジュールであってもよい鍵交換認証モジュール216と、プロセッサ208に組み込まれるかまたは結合されたハードウェア/ファームウェアモジュールとをさらに含んでもよい。

【００４５】

したがって、本開示の一態様は、本明細書に記載された機能を実行する能力を含むIoTデバイス(たとえば、IoTデバイス200A)を含むことができる。当業者によって諒解されるように、様々な論理要素は、本明細書で開示する機能を実現するように個別の要素、プロセッサ(たとえば、プロセッサ208)上で実行されるソフトウェアモジュール、またはソフトウェアとハードウェアとの任意の組合せにおいて具現されてもよい。たとえば、トランシーバ206、プロセッサ208、メモリ212、I/Oインターフェース214、および/または鍵交換認証モジュール216をすべて協調的に使用して、本明細書において開示する様々な機能をロードし、記憶し、実行してもよく、したがって、これらの機能を実行するための論理は様々な要素に分散されてもよい。代替的に、機能は、鍵交換認証モジュール216などの1つの離散構成要素に組み込むことが可能である。したがって、図2AにおけるIoTデバイス200Aの特徴は、単に例示にすぎないものと見なされ、本開示は、示された特徴または構成に限定されない。

【００４６】
たとえば、IoTデバイス200Aは、IoTデバイス200Aと第2のピアデバイスとの間の鍵交換を認証するように構成された第1のピアデバイスである場合、本明細書において説明するように、トランシーバ206、プロセッサ208、鍵交換認証モジュール216、および場合によっては入出力インターフェース214は、IoTデバイス200Aのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに協働的に送信し、第2のピアデバイスは、ユーザの連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する。IoTデバイス200Aは、第1の連合ログインプロバイダから第1の認証応答を受信し、第2のピアデバイスは、第2の連合ログインプロバイダから第2の認証応答を受信する。IoTデバイス200Aは、第2のピアデバイスから第2の認証応答を受信し、第2の連合ログインプロバイダによる第2の認証応答を認証し、第1の認証応答を第2のピアデバイスに送信し、第2のピアデバイスは、第1の連合ログインプロバイダによる第1の認証応答を認証する。IoTデバイス200Aは、第2のピアデバイスが第1の認証応答を認証したことを示す肯定応答を第2のピアデバイスから受信し、IoTデバイス200Aが第2の認証応答を認証したことを示す肯定応答を第2のピアデバイスに送信し、第2のピアデバイスからの肯定応答に基づいて鍵交換を認証し、第2のピアデバイスは、IoTデバイス200Aからの肯定応答に基づいて鍵交換を認証する。このシナリオでは、IoTデバイス200Aは、本明細書においてさらに説明するようにコントローラまたは非制御側デバイスであってもよい。

【００４７】
図2Bは、本開示の態様による受動IoTデバイス200Bのハイレベルな例を示す。一般に、図2Bに示す受動IoTデバイス200Bは、上でより詳細に説明した、図2Aに示したIoTデバイス200Aと同じ、かつ/または実質的に類似した様々構成要素を含み得る。したがって、説明を簡潔かつ簡単にするために、同じまたは類似の詳細が図2Aに示したIoTデバイス200Aに関して上ですでに提供されている限り、図2Bに示す受動IoTデバイス200B内のいくつかの構成要素に関する様々な詳細は本明細書で省略される場合がある。

【００４８】
図2Bに示す受動IoTデバイス200Bは、プロセッサ、内部メモリ、またはある種の他の構成要素を有しない場合があるという点で、一般に、図2Aに示すIoTデバイス200Aとは異なる場合がある。代わりに、一実施形態では、受動IoTデバイス200Bは、受動IoTデバイス200Bが、制御されたIoTネットワーク内で観測されること、監視されること、制御されること、管理されること、あるいは知られることを可能にする、I/Oインターフェース214または他の適切な機構だけを含み得る。たとえば、一実施形態では、受動IoTデバイス200Bに関連付けられたI/Oインターフェース214は、短距離インターフェースを介して問い合わされたとき、受動IoTデバイス200Bに関連付けられた識別子および属性を別のデバイス(たとえば、受動IoTデバイス200Bに関連付けられた属性に関する情報を検出すること、記憶すること、通信すること、その情報に作用すること、あるいはその情報を処理することができる、IoTデバイス200Aなどの能動IoTデバイス)に提供することができる、バーコード、Bluetooth(登録商標)インターフェース、無線周波数(RF)インターフェース、RFIDタグ、IRインターフェース、NFCインターフェース、または任意の他の適切なI/Oインターフェースを含み得る。

【００４９】
一態様では、IoTデバイス200Bは、IoTデバイス200Bと第2のピアデバイスとの間の鍵交換を認証するように構成された第1のピアデバイスである場合、本明細書において説明するように、トランシーバ206、プロセッサ208、鍵交換認証モジュール216、および場合によっては入出力インターフェース214は、IoTデバイス200Bのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに協働的に送信し、第2のピアデバイスは、ユーザの連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する。IoTデバイス200Bは、第1の連合ログインプロバイダから第1の認証応答を受信し、第2のピアデバイスは、第2の連合ログインプロバイダから第2の認証応答を受信する。IoTデバイス200Bは、第2のピアデバイスから第2の認証応答を受信し、第2の連合ログイ

ンプロバイダによる第2の認証応答を認証し、第1の認証応答を第2のピアデバイスに送信し、第2のピアデバイスは、第1の連合ログインプロバイダによる第1の認証応答を認証する。IoTデバイス200Bは、第2のピアデバイスが第1の認証応答を認証したことを示す肯定応答を第2のピアデバイスから受信し、IoTデバイス200Aが第2の認証応答を認証したことを示す肯定応答を第2のピアデバイスに送信し、第2のピアデバイスからの肯定応答に基づいて鍵交換を認証し、第2のピアデバイスは、IoTデバイス200Bからの肯定応答に基づいて鍵交換を認証する。このシナリオでは、IoTデバイス200Bは、本明細書においてさらに説明するように非制御側デバイスであってもよい。あらゆる受動IoTデバイスが鍵交換認証モジュール216を含むとは限らないので、鍵交換認証モジュール216は省略可能であるように示されている。

【００５０】

上記は何らかの形のRF、バーコード、または他のI/Oインターフェース214を有するとして受動IoTデバイス200Bを説明しているが、受動IoTデバイス200Bは、そのようなI/Oインターフェース214を有しないデバイスまたは他の物理的対象物を含み得る。たとえば、あるIoTデバイスは、受動IoTデバイス200Bを識別するために、受動IoTデバイス200Bに関連付けられた形状、サイズ、色、および/もしくは他の観測可能な特徴を検出することができる適切なスキャナ機構またはリーダー機構を有し得る。このようにして、任意の適切な物理的対象物は、その識別および属性を通信することができ、制御されたIoTネットワーク内で観測、監視、制御、あるいは管理され得る。

【００５１】

図3は、機能を実行するように構成される論理を含む通信デバイス300を示す。通信デバイス300は、限定はしないが、IoTデバイス110～120、IoTデバイス200A、インターネット175に結合された任意の構成要素(たとえば、IoTサーバ170)などを含む、上記の通信デバイスのうちのいずれかに対応し得る。したがって、通信デバイス300は、図1A～図1Bのワイヤレス通信システム100A～100Bを介して1つもしくは複数の他のエンティティと通信する(または通信を容易にする)ように構成された任意の電子デバイスに対応し得る。

【００５２】

図3を参照すると、通信デバイス300は、情報を受信および/または送信するように構成される論理305を含む。一例では、通信デバイス300がワイヤレス通信デバイス(たとえば、IoTデバイス200Aおよび/または受動IoTデバイス200B)に対応する場合には、情報を受信および/または送信するように構成される論理305は、ワイヤレストランシーバおよび関連ハードウェア(たとえば、RFアンテナ、モデム、変調器および/または復調器など)のようなワイヤレス通信インターフェース(たとえば、Bluetooth(登録商標)、Wi-Fi、Wi-Fi Direct、Long-Term Evolution (LTE) Directなど)を含むことができる。別の例では、情報を受信および/または送信するように構成された論理305は、有線通信インターフェース(たとえば、インターネット175にアクセスする手段となり得るシリアル接続、USBまたはFirewire接続、Ethernet(登録商標)接続など)に対応することができる。したがって、通信デバイス300が、何らかのタイプのネットワークベースのサーバ(たとえば、アプリケーション170)に対応する場合には、情報を受信および/または送信するように構成された論理305は、一例では、Ethernet(登録商標)プロトコルによってネットワークベースのサーバを他の通信エンティティに接続するEthernet(登録商標)カードに対応し得る。さらなる例では、情報を受信および/または送信するように構成された論理305は、通信デバイス300がそのローカル環境を監視する手段となり得る感知または測定ハードウェア(たとえば、加速度計、温度センサー、光センサー、ローカルRF信号を監視するためのアンテナなど)を含むことができる。情報を受信および/または送信するように構成された論理305は、実行されるときに、情報を受信および/または送信するように構成された論理305の関連ハードウェアがその受信機能および/または送信機能を実行できるようにするソフトウェアも含むことができる。しかしながら、情報を受信および/または送信するように構成された論理305は、ソフトウェアだけに対応するのではなく、情報を受信および/または送信するように構成された論理305は、その機能性を達成するためのハードウェアに少なくとも部分的

に依拠する。

【００５３】

図3を参照すると、通信デバイス300は、情報を処理するように構成される論理310をさらに含む。一例では、情報を処理するように構成される論理310は、少なくともプロセッサを含むことができる。情報を処理するように構成された論理310によって実施され得るタイプの処理の例示的な実装形態は、判断を行うこと、接続を確立すること、異なる情報オプション間で選択を行うこと、データに関係する評価を実施すること、測定動作を実施するために通信デバイス300に結合されたセンサーと対話すること、情報をあるフォーマットから別のフォーマットに(たとえば、.wmvから.aviへなど、異なるプロトコル間で)変換することなどを含むが、これらに限定されない。たとえば、情報を処理するように構成された論理310中に含まれるプロセッサは、汎用プロセッサ、DSP、ASIC、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、または本明細書において説明される機能を実行するように設計されたそれらの任意の組合せに対応し得る。汎用プロセッサはマイクロプロセッサとすることができるが、代替として、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械とすることができる。プロセッサはまた、コンピューティングデバイスの組合せ(たとえば、DSPおよびマイクロプロセッサの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成)として実現され得る。情報を処理するように構成された論理310は、実行されるとき、情報を処理するように構成された論理310の関連ハードウェアがその処理機能を実行できるようにするソフトウェアも含むことができる。しかしながら、情報を処理するように構成された論理310は、ソフトウェアだけに対応するのではなく、情報を処理するように構成された論理310は、その機能を達成するためにハードウェアに少なくとも部分的に依拠する。

【００５４】

図3を参照すると、通信デバイス300は、情報を記憶するように構成される論理315をさらに含む。一例では、情報を記憶するように構成される論理315は、少なくとも非一時的メモリおよび関連ハードウェア(たとえば、メモリコントローラなど)を含むことができる。たとえば、情報を記憶するように構成される論理315に含まれる非一時的メモリは、RAM、フラッシュメモリ、ROM、消去可能プログラマブルROM(EPROM)、EEPROM、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当該技術分野において知られている任意の他の形の記憶媒体に対応することができる。情報を記憶するように構成される論理315は、実行されるときに、情報を記憶するように構成される論理315の関連ハードウェアがその記憶機能を実行できるようにするソフトウェアも含むことができる。しかしながら、情報を記憶するように構成される論理315は、ソフトウェアだけに対応するのではなく、情報を記憶するように構成される論理315は、その機能を達成するためにハードウェアに少なくとも部分的に依拠する。

【００５５】

一態様では、通信デバイス300は、通信デバイス300と第2のピアデバイスとの間の鍵交換を認証するように構成された第1のピアデバイスである場合、本明細書において説明するように、情報の受信および/または送信を行うように構成された論理305、情報を処理するように構成された論理310、ならびに情報を記憶するように構成された論理315は、通信デバイス300のユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに協働的に送信し、第2のピアデバイスは、ユーザの連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する。通信デバイス300は、第1の連合ログインプロバイダから第1の認証応答を受信し、第2のピアデバイスは、第2の連合ログインプロバイダから第2の認証応答を受信する。通信デバイス300は、第2のピアデバイスから第2の認証応答を受信し、第2の連合ログインプロバイダによる第2の認証応答を認証し、第1の認証応答を第2のピアデバイスに送信し、第2のピアデバイスは、第1の連合ログインプロバイダによる第1の認証応答を認証する。通信デバイス300は、第2のピアデバイス

が第1の認証応答を認証したことを示す肯定応答を第2のピアデバイスから受信し、通信デバイス300が第2の認証応答を認証したことを示す肯定応答を第2のピアデバイスに送信し、第2のピアデバイスからの肯定応答に基づいて鍵交換を認証し、第2のピアデバイスは、通信デバイス300からの肯定応答に基づいて鍵交換を認証する。このシナリオでは、通信デバイス300は、本明細書においてさらに説明するようにコントローラまたは非制御側デバイスであってもよい。

【００５６】

図3を参照すると、通信デバイス300は、情報を提示するように構成された論理320をさらにオプションで含む。一例では、情報を提示するように構成される論理320は、少なくとも出力デバイスおよび関連ハードウェアを含むことができる。たとえば、出力デバイスは、ビデオ出力デバイス(たとえば、ディスプレイスクリーン、USB、HDMI(登録商標)のようなビデオ情報を搬送することができるポートなど)、オーディオ出力デバイス(たとえば、スピーカ、マイクロフォンジャック、USB、HDMI(登録商標)のようなオーディオ情報を搬送することができるポートなど)、振動デバイス、および/または、情報がそれによって出力のためにフォーマットされ得る、または通信デバイス300のユーザもしくは操作者によって実際に出力され得る任意の他のデバイスを含むことができる。たとえば、通信デバイス300が、図2Aに示したIoTデバイス200Aおよび/または図2Bに示した受動IoTデバイス200Bに対応する場合、情報を提示するように構成された論理320は、ディスプレイ226を含み得る。さらなる一例では、情報を提示するように構成される論理320は、ローカルユーザを有しないネットワーク通信デバイス(たとえば、ネットワークスイッチ、またはルータ、リモートサーバなど)のようないくつかの通信デバイスでは省くことができる。情報を提示するように構成された論理320は、実行されるとき、情報を提示するように構成された論理320の関連ハードウェアがその提示機能を実施できるようにするソフトウェアも含むことができる。しかしながら、情報を提示するように構成された論理320は、ソフトウェアだけに対応するのではなく、情報を提示するように構成された論理320は、その機能性を達成するためにハードウェアに少なくとも部分的に依拠する。

【００５７】

図3を参照すると、通信デバイス300は、ローカルユーザ入力を受信するように構成された論理325をさらにオプションで含む。一例では、ローカルユーザ入力を受信するように構成される論理325は、少なくともユーザ入力デバイスおよび関連ハードウェアを含むことができる。たとえば、ユーザ入力デバイスは、ボタン、タッチスクリーンディスプレイ、キーボード、カメラ、オーディオ入力デバイス(たとえば、マイクロフォン、もしくはマイクロフォンジャックなど、オーディオ情報を搬送することができるポートなど)、および/または情報がそれによって通信デバイス300のユーザもしくはオペレータから受信され得る任意の他のデバイスを含み得る。たとえば、通信デバイス300が図2Aに示すようなIoTデバイス200Aおよび/または図2Bに示すような受動IoTデバイス200Bに対応する場合、ローカルユーザ入力を受信するように構成された論理325は、ボタン222、224Aおよび224B、ディスプレイ226(タッチスクリーンの場合)などを含み得る。さらなる例では、ローカルユーザ入力を受信するように構成された論理325は、(たとえば、ネットワークスイッチまたはルータ、リモートサーバなど)ローカルユーザを有さないネットワーク通信デバイスのようないくつかの通信デバイスでは省略されることがある。ローカルユーザ入力を受信するように構成された論理325は、実行されるとき、ローカルユーザ入力を受信するように構成された論理325の関連ハードウェアがその入力受信機能を実施できるようにするソフトウェアも含むことができる。しかしながら、ローカルユーザ入力を受信するように構成された論理325は、ソフトウェアだけに対応するのではなく、ローカルユーザ入力を受信するように構成された論理325は、その機能性を達成するためにハードウェアに少なくとも部分的に依拠する。

【００５８】

図3を参照すると、305～325の構成された論理は、図3では別個のまたは相異なるブロックとして示されているが、それぞれの構成された論理がその機能を実行するためのハード

ウェアおよび/またはソフトウェアは、部分的に重複できることは理解されよう。たとえば、305～325の構成された論理の機能を容易にするために使用される任意のソフトウェアを、情報を記憶するように構成された論理315に関連する非一時的メモリに記憶することができ、それにより、305～325の構成された論理は各々、その機能(すなわち、この場合、ソフトウェア実行)を、情報を記憶するように構成された論理315によって記憶されたソフトウェアの動作に部分的に基づいて実行する。同様に、構成された論理のうちの1つに直接関連付けられるハードウェアは、時々、他の構成された論理によって借用または使用され得る。たとえば、情報を処理するように構成された論理310のプロセッサは、データを、情報を受信および/または送信するように構成された論理305によって送信される前に、適切な形式にフォーマットすることができ、それにより、情報を受信および/または送信するように構成された論理305は、その機能(すなわち、この場合、データの送信)を、情報を処理するように構成された論理310に関連付けられたハードウェア(すなわち、プロセッサ)の動作に部分的に基づいて実行する。

【００５９】

概して、別段に明示的に記載されていない限り、本開示全体にわたって使用される「ように構成された論理」という句は、ハードウェアにより少なくとも部分的に実施される態様を呼び出すものとし、ハードウェアから独立したソフトウェアだけの実施形態に位置づけるものではない。様々なブロックにおける構成された論理または「ように構成された論理」は、特定の論理ゲートまたは論理要素に限定されるのではなく、概して、本明細書に記載した機能性を、(ハードウェアまたはハードウェアとソフトウェアの組合せのいずれかを介して)実施するための能力を指すことが諒解されよう。したがって、様々なブロックに示す構成された論理または「ように構成された論理」は、「論理」という言葉を共有するにもかかわらず、必ずしも論理ゲートまたは論理要素として実装されるとは限らない。様々なブロックの論理間の他のやりとりまたは協働が、以下でより詳細に説明する態様の検討から、当業者には明らかになるであろう。

【００６０】

様々な実施形態は、図4に示すサーバ400などの、様々な市販のサーバデバイスのいずれにおいても実装され得る。一例では、サーバ400は、上記で説明したIoTサーバ170または本明細書においてさらに説明するようなOpenID/OAuth/FaceConnectプロバイダの1つの例示的な構成に相当し得る。図4では、サーバ400は、揮発性メモリ402と、ディスクドライブ403などの大容量の不揮発性メモリとに結合されたプロセッサ401を含む。サーバ400は、プロセッサ401に結合された、フロッピー(登録商標)ディスクドライブ、コンパクトディスク(CD)ドライブまたはDVDディスクドライブ406を含むことも可能である。サーバ400は、他のブロードキャストシステムコンピュータおよびサーバに、またはインターネットに結合されたローカルエリアネットワークなどのネットワーク407とのデータ接続を確立するための、プロセッサ401に結合されたネットワークアクセスポート404を含むことも可能である。図3の文脈において、図4のサーバ400は、通信デバイス300の1つの例示的な実装形態を示すが、情報を送信および/または受信するように構成された論理305は、ネットワーク407と通信するためにサーバ400によって使用されるネットワークアクセスポート404に相当し、情報を処理するように構成された論理310は、プロセッサ401に相当し、情報を記憶するように構成された論理315は、揮発性メモリ402、ディスク(disk)ドライブ403、および/またはディスク(disc)ドライブ406のうちの任意の組合せに相当することが諒解されよう。情報を提示するように構成されたオプションの論理320およびローカルユーザ入力を受信するように構成されたオプションの論理325は、図4には明示的に示さず、その中に含まれる場合もあれば、含まれない場合もある。したがって、図4は、通信デバイス300が、図2Aに示すようなIoTデバイスの実装形態に加えてサーバとして実装され得ることを説明するのを助ける。

【００６１】

概して、電話、タブレットコンピュータ、ラップトップコンピュータおよびデスクトップコンピュータ、特定の車両などのユーザ機器(UE)は、互いに(たとえば、Bluetooth(登

録商標)、ローカルWi-Fiなどによって)ローカルに接続するかまたは(たとえば、セルラーネットワーク、インターネットなどを介して)リモートに接続するように構成されてもよい。さらに、いくつかのUEは、デバイスが1対1の接続を確立するかまたは互いに直接通信するためにいくつかのデバイスを含むグループに同時に接続するのを可能にする特定のワイヤレスネットワーキング技法(たとえば、Wi-Fi、Bluetooth(登録商標)、Wi-Fi Directなど)を使用する近接度ベースのピアツーピア(P2P)通信をサポートしてもよい。そのために、図5は、発見可能なP2Pサービスをサポートすることができる例示的なワイヤレス通信ネットワークまたはWAN500を示す。たとえば、一実施形態では、ワイヤレス通信ネットワーク500は、様々な基地局510と他のネットワークエンティティとを含むLTEネットワークまたは別の適切なWANを備えてもよい。簡単のために、図5には、3つの基地局510a、510bおよび510c、1つのネットワークコントローラ530、ならびに1つのダイナミックホストコンフィギュレーションプロトコル(DHCP)サーバ540のみを示す。基地局510は、デバイス520と通信するエンティティであってもよく、Node B、evolved Node B(eNB)、アクセスポイントなどとも呼ばれることがある。各基地局510は、特定の地理的エリアに対して通信カバレージを実現し得、カバレージエリア内に位置するデバイス520のための通信をサポートし得る。ネットワーク容量を向上させるために、基地局510の全体的なカバレージエリアが複数の(たとえば、3つの)より小さいエリアに区分されてもよく、各々のより小さいエリアがそれぞれの基地局510によってサービスされてもよい。3GPPでは、「セル」という用語は、この用語が使用される状況に応じて、このカバレッジエリアにサービスしている基地局510および/または基地局サブシステム510のカバレッジエリアを指し得る。3GPP2では、「セクタ」または「セルセクタ」という用語は、このカバレッジエリアにサービスしている基地局510および/または基地局サブシステム510のカバレッジエリアを指し得る。明確にするために、本明細書の説明では3GPPの「セル」の概念が使用されることがある。

【００６２】

基地局510は、マクロセル、ピコセル、フェムトセル、および/または他のセルタイプの通信カバレッジを可能にすることができる。マクロセルは、比較的大きい地理的エリア(たとえば、半径数キロメートル)をカバーすることができ、サービスに加入しているデバイス520による無制限アクセスを可能にし得る。ピコセルは、比較的小さい地理的エリアをカバーすることができ、サービスに加入しているデバイス520による無制限アクセスを可能にし得る。フェムトセルは、比較的小さい地理的エリア(たとえば、家庭)をカバーすることができ、フェムトセルとの関連付けを有するデバイス520(たとえば、限定加入者グループ(CSG)中のデバイス)による限定アクセスを可能にし得る。図5に示す例では、ワイヤレスネットワーク500は、マクロセルのためのマクロ基地局510a、510b、および510cを含む。ワイヤレスネットワーク500は、ピコセルのためのピコ基地局510および/またはフェムトセルのためのホーム基地局510(図5には示されていない)も含み得る。

【００６３】

ネットワークコントローラ530は、基地局510のセットに結合することができ、これらの基地局510の調整および制御を行うことができる。ネットワークコントローラ530は、バックホールを介して基地局と通信することができる単一のネットワークエンティティまたはネットワークエンティティの集合であってもよい。また、基地局は、たとえば、直接またはワイヤレスバックホールまたはワイヤラインバックホールを介して間接的に、互いに通信し得る。DHCPサーバ540は、以下に説明するように、P2P通信をサポートすることができる。DHCPサーバ540は、ワイヤレスネットワーク500の一部であっても、またはインターネット接続共有(ICS)を介して実行されるワイヤレスネットワーク500の外部のサーバであっても、またはそれらの任意の適切な組合せであってもよい。DHCPサーバ540は、(図5に示されるように)別個のエンティティであってよく、または、基地局510、ネットワークコントローラ530、もしくは他の何らかのエンティティの一部であってもよい。いずれの場合も、DHCPサーバ540は、ピアツーピアの通信を望むデバイス520によって到達可能であり得る。

【００６４】
デバイス520はワイヤレスネットワーク500全体にわたって分散され得、各デバイス520は固定されてもまたは移動可能であってもよい。デバイス520はまた、ノード、ユーザ機器(UE)、局、移動局、端末、アクセス端末、加入者ユニットなどと呼ばれ得る。デバイス520は、セルラー電話、携帯情報端末(PDA)、ワイヤレスモデム、ワイヤレス通信デバイス、ハンドヘルドデバイス、ラップトップコンピュータ、コードレス電話、ワイヤレスローカルループ(WLL)局、スマートフォン、ネットブック、スマートブック、タブレットなどであってよい。デバイス520は、ワイヤレスネットワーク500内の基地局510と通信してもよく、さらに他のデバイス520とピアツーピア通信してもよい。たとえば、図5に示すように、デバイス520aとデバイス520bがピアツーピア通信してもよく、デバイス520cとデバイス520dがピアツーピア通信してもよく、デバイス520eとデバイス520fがピアツーピア通信してもよく、デバイス520gとデバイス520hとデバイス520iがピアツーピア通信し、一方、残りのデバイス520が基地局510と通信してもよい。さらに図5に示すように、デバイス520a、520d、520f、および520hは、たとえば、P2P通信を行っていないときに基地局510と通信するか、または場合によってはP2P通信と同時に基地局510と通信してもよい。
【００６５】
本明細書の説明では、WAN通信は、たとえば別のデバイス520などのリモートエンティティと通話するための、ワイヤレスネットワーク500におけるデバイス520と基地局510との間の通信を指し得る。WANデバイスは、WAN通信に関心を持っているか、WAN通信に関与しているデバイス520である。P2P通信は、基地局510を介さない、2つ以上のデバイス520間の直接通信を指す。P2Pデバイスは、P2P通信に関心を持っているかまたはP2P通信に関与しているデバイス520、たとえば、P2Pデバイスの近傍内の別のデバイス520に関するトラフィックデータを有するデバイス520である。2つのデバイスは、たとえば、各デバイス520が他のデバイス520を検出できる場合、互いに近傍に位置すると見なされてもよい。概して、デバイス520は、別のデバイス520と、P2P通信の場合は直接通信してもよく、WAN通信の場合は少なくとも1つの基地局510を介して通信してもよい。
【００６６】
一実施形態では、P2Pデバイス520間の直接通信はP2Pグループとして構成されてもよい。より詳細には、P2Pグループは概して、P2P通信に関心を持っているか、またはP2P通信に関与している2つ以上のデバイス520のグループを指し、P2Pリンクは、P2Pグループ用の通信リンクを指す。さらに、一実施形態では、P2Pグループは、P2Pグループオーナー(またはP2Pサーバ)と指定される1つのデバイス520と、P2PグループオーナーによってサービスされるP2Pクライアントと指定される1つまたは複数のデバイス520とを含んでもよい。P2Pグループオーナーは、WANとのシグナリングの交換、P2PグループオーナーとP2Pクライアントとの間のデータ送信の調整などのような、いくつかの管理機能を実行することができる。たとえば、図5に示すように、第1のP2Pグループは、基地局510aの対象となるデバイス520aおよび520bを含み、第2のP2Pグループは、基地局510bの対象となるデバイス520cおよび520dを含み、第3のP2Pグループは、異なる基地局510bおよび510cの対象となるデバイス520eおよび520fを含み、第4のP2Pグループは、基地局510cの対象となるデバイス520g、520h、および520iを含む。デバイス520a、520d、520f、および520hは、そのそれぞれのP2PグループにおけるP2Pグループオーナーであってもよく、デバイス520b、520c、520e、520g、および520iは、そのそれぞれのP2PグループにおけるP2Pクライアントであってもよい。図5の他のデバイス520は、WAN通信に関与していてもよい。
【００６７】
実施形態では、P2P通信は、P2Pグループ内でのみ行われ、かつ、P2Pグループに関連するP2PグループオーナーとP2Pクライアントとの間でのみ行われる。たとえば、同じP2Pグループ内の2つのP2Pクライアント(たとえば、デバイス520gおよび520i)が情報を交換することを望む場合、P2Pクライアントの一方がP2Pグループオーナー(たとえば、デバイス520h)に情報を送ってもよく、次いでP2PグループオーナーがP2Pクライアントに中継してもよい。一実施形態では、特定のデバイス520は、複数のP2Pグループに属してもよ

く、各P2Pグループ内でP2Pグループオーナーまたは P2Pクライアントのいずれかとして振る舞ってもよい。さらに、一実施形態では、特定のP2Pクライアントは、1つのP2Pグループのみに属するかまたは複数のP2Pグループに属し、任意の特定の瞬間に複数のP2PグループのいずれかにおけるP2Pデバイス520と通信してもよい。概して、通信は、ダウンリンクおよびアップリンク上での送信を通じて促進され得る。WAN通信では、ダウンリンク(または順方向リンク)は基地局510からデバイス520への通信リンクを指し、アップリンク(または逆方向リンク)はデバイス520から基地局510への通信リンクを指す。P2P通信では、P2Pダウンリンクは P2Pグループオーナーから P2Pクライアントへの通信リンクを指し、P2Pアップリンクは P2Pクライアントから P2Pグループオーナーへの通信リンクを指す。いくつかの実施形態では、2つ以上のデバイスが、WAN技法を使用して P2P通信するのではなく、Wi-Fi、Bluetooth(登録商標)、または Wi-Fi Directなどの技法を使用してより小さい P2Pグループを形成してワイヤレスローカルエリアネットワーク(WLAN)上で P2P通信してもよい。たとえば、Wi-Fi、Bluetooth(登録商標)、Wi-Fi Direct、またはその他のWLAN技法を使用する P2P通信では、2つ以上のモバイルフォン、ゲームコンソール、ラップトップコンピュータ、またはその他の適切な通信エンティティ間の P2P通信を可能にすることができる。

【００６８】

図6は、本開示の一態様による、様々なデバイス610、630、640が通信するのに利用することができる近接度ベースの分散バスを確立するために発見可能な P2Pサービスを使用し得る例示的な環境600を示す。たとえば、一実施形態では、ネットワーク化コンピューティング環境におけるアプリケーション間通信を有効化するのに使用されるソフトウェアバスを含んでもよい分散バス625を介したプロセス間通信プロトコル(IPC)フレームワークを使用して単一のプラットフォーム上でのアプリケーション同士などの間の通信を容易にすることができ、この場合、ネットワーク化コンピューティング環境におけるアプリケーション間通信では、各アプリケーションが分散バス625に登録して他のアプリケーションにサービスを提供し、他のアプリケーションが登録されているアプリケーションに関する情報を分散バス625に問い合わせる。そのようなプロトコルは、信号メッセージ(たとえば、通知)がポイントツーポイントメッセージであってもまたはブロードキャストメッセージであってもよく、メソッド呼出しメッセージ(たとえば、RPC)が同期メッセージであってもまたは非同期メッセージであってもよく、分散バス625(たとえば、「デーモン」バスプロセス)が様々なデバイス610、630、640間のメッセージルーティングに対処することができる、非同期通知およびリモートプロシージャ呼出し(RPC)を可能にすることができる。

【００６９】

一実施形態では、分散バス625は、様々なトランスポートプロトコル(たとえば、Bluetooth(登録商標)、TCP/IP、Wi-Fi、CDMA、GPRS、UMTSなど)によってサポートされてもよい。たとえば、一態様によれば、第1のデバイス610は、分散バスノード612と1つまたは複数のローカルエンドポイント614とを含んでもよく、分散バスノード612は、第1のデバイス610に関連するローカルエンドポイント614と第2のデバイス630および第3のデバイス640に関連するローカルエンドポイント634および644との間の、分散バス625を通じた(たとえば、第2のデバイス630および第3のデバイス640上の分散バスノード632および642を介した)通信を容易にすることができる。図7を参照しながら以下にさらに詳細に説明するように、分散バス625は、対称的マルチデバイスネットワークトポロジーをサポートしてもよく、デバイスドロップアウトの存在下でロバストな動作を可能にしてもよい。したがって、仮想分散バス625は、概して任意の下位トランスポートプロトコル(たとえば、Bluetooth(登録商標)、TCP/IP、Wi-Fiなど)とは無関係であってもよく、非セキュア(たとえば、オープン)からセキュア(たとえば、認証または暗号化)まで様々なセキュリティオプションを実現することができ、セキュリティオプションは、第1のデバイス610、第2のデバイス630、および第3のデバイス640間の自発的な接続を容易にしつつ、様々なデバイス610、630、640が互いの範囲に入るかまたは互いに近接したときに介入せずに使用され得る。

【００７０】

図7は、本開示の一態様による、第1のデバイス(「デバイスA」)710および第2のデバイ

ス(「デバイスB」)730が通信するのに利用することができる近接度ベースの分散バスを確立するために発見可能なP2Pサービスを使用し得る例示的なメッセージシーケンス700を示す。概して、デバイスAは、デバイスBとの通信を要求してもよく、デバイスAは、そのような通信を容易にするのを助けることができるバスノード712に加えて通信の要求を出し得るローカルエンドポイント714(たとえば、ローカルアプリケーション、サービスなど)を含んでもよい。さらに、デバイスB 730は、ローカルエンドポイント714が、デバイスA 710上のローカルエンドポイント714とデバイスB 730上のローカルエンドポイント734との間の通信を容易にするのを助けることができるバスノード732に加えて通信を試み得るローカルエンドポイント734を含んでもよい。

【００７１】

一実施形態では、メッセージシーケンスステップ754において、バスノード712および732は適切な発見機構を実行してもよい。たとえば、Bluetooth(登録商標)、TCP/IP、UNIX(登録商標)などによってサポートされる接続を発見するための機構が使用されてもよい。メッセージシーケンスステップ756において、デバイスA 710上のローカルエンドポイント714は、バスノード712を通じて利用可能なエンティティ、サービス、エンドポイントなどに接続することを要求してもよい。一実施形態では、この要求は、ローカルエンドポイント714とバスノード712との間の要求応答プロセスを含んでもよい。メッセージシーケンスステップ758において、分散メッセージバスが、バスノード712をバスノード732に接続し、それによってデバイスA 710とデバイスB 730との間のP2P接続を確立するように形成されてもよい。一実施形態では、バスノード712とバスノード732との間に分散バスを形成するための通信は、近接度ベースのP2Pプロトコル(たとえば、接続された製品間の相互運用性を実現するように設計されたAllJoyn(登録商標)ソフトウェアフレームワークおよび近位ネットワークを動的に作成し近位P2P通信を容易にするための様々な製造業者によるソフトウェアアプリケーション)を使用して容易にされてもよい。代替として、一実施形態では、サーバ(図示せず)はバスノード712とバスノード732との間の接続を容易にしてもよい。さらに、一実施形態では、バスノード712とバスノード732との間に接続を形成する前に適切な認証機構が使用されてもよい(たとえば、クライアントが認証コマンドを送って認証対話を開始することができるSASL認証)。さらに、メッセージシーケンスステップ758の間、バスノード712および732は、利用可能な他のエンドポイント(たとえば、図6のデバイスC 640上のローカルエンドポイント644)に関する情報を交換してもよい。そのような実施形態では、バスノードが維持する各ローカルエンドポイントが他のバスノードに通知されてもよく、この通知は、一意のエンドポイント名、トランスポートタイプ、接続パラメータ、または他の適切な情報を含んでもよい。

【００７２】

一実施形態では、メッセージシーケンスステップ760において、バスノード712およびバスノード732は、それぞれローカルエンドポイント734および714に関連する得られた情報を使用して、様々なバスノードを通じて利用可能な得られた実エンドポイントを表すことのできる仮想エンドポイントを作成してもよい。一実施形態では、バスノード712上のメッセージルーティングでは、実エンドポイントおよび仮想エンドポイントを使用してメッセージを送信してもよい。さらに、リモートデバイス(たとえば、デバイスA 710)上に存在するあらゆるエンドポイントに1つのローカル仮想エンドポイントがあってもよい。さらに、そのような仮想エンドポイントは、分散バス(たとえば、バスノード712とバスノード732との間の接続)を介して送られたメッセージを多重化しならびに/あるいは多重化解除してもよい。一態様では、仮想エンドポイントは、実エンドポイントと同様にローカルバスノード712または732からメッセージを受信してもよく、分散バスを介してメッセージを転送してもよい。したがって、仮想エンドポイントは、エンドポイント多重化分散バス接続からローカルバスノード712および732へメッセージを転送してもよい。さらに、一実施形態では、リモートデバイス上の仮想エンドポイントに対応する仮想エンドポイントは、任意の時点で特定のトランスポートタイプの所望のトポロジーに対処するように再接続されてもよい。そのような態様では、UNIX(登録商標)ベースの仮想エンドポイントは、ロ

ーカルと見なされることがあり、したがって、再接続の候補とは見なされないことがある。さらに、TCPベースの仮想エンドポイントは、1つのホップルーティングに関して最適化されてもよい(たとえば、各バスノード712および732は互いに直接接続されてもよい)。さらに、Bluetooth(登録商標)ベースの仮想エンドポイントは、Bluetooth(登録商標)ベースのマスタがローカルマスタノードと同じバスノードであってもよい単一ピコネット(たとえば、1つのマスタおよびn個のスレーブ)に関して最適化されてもよい。

【００７３】

メッセージシーケンスステップ762において、バスノード712とバスノード732は、762においてバス状態情報を交換してバスインスタンス同士をマージし、分散バスを介した通信を可能にしてもよい。たとえば、一実施形態では、バス状態情報は、周知の一意のエンドポイント名マッピング、整合規則、ルーティンググループ、または他の適切な情報を含んでもよい。一実施形態では、状態情報は、分散バスベースのローカル名と通信するローカルエンドポイント714および734とのインターフェースを使用してバスノード712インスタンスとバスノード732インスタンスとの間で伝達されてもよい。別の態様では、バスノード712およびバスノード732の各々は、分散バスへのフィードバックを可能にする役割を果たすローカルバスコントローラを維持してもよく、バスコントローラは、グローバルメソッド、引数、信号、およびその他の情報を分散バスに関連する規格に変換してもよい。メッセージシーケンスステップ764において、バスノード712およびバスノード732は、上述のようなバスノードノード接続の間に導入されるあらゆる変化に関してそれぞれのローカルエンドポイント714および734に通知する信号を伝達(たとえば、ブロードキャスト)してもよい。一実施形態では、新しいおよび/または削除されたグローバル名および/または変換後の名前が、名前オーナー変更後信号によって示されてもよい。さらに、(たとえば、名前衝突に起因して)ローカルに失われることがあるグローバル名が名前喪失信号によって示されてもよい。さらに、名前衝突に起因して転送されるグローバル名が名前オーナー変更後信号によって示されてもよく、バスノード712およびバスノード732が切り離された場合および/またはときに消える一意の名前が名前オーナー変更後信号によって示されてもよい。

【００７４】

上記に使用されたように、周知の名前を使用してローカルエンドポイント714および734を一意に記述してもよい。一実施形態では、デバイスA 710とデバイスB 730との間で通信が行われるとき、異なる周知の名前タイプが使用されてもよい。たとえば、バスノード712が直接接続されるデバイスA 710に関連するバスノード712上にのみデバイスローカル名が存在してもよい。別の例では、すべての既知のバスノード712および732上にグローバル名が存在してもよく、すべてのバスセグメント上に存在してもよい名前のオーナーは1人だけである。言い換えれば、バスノード712とバスノード732が連結され、衝突が起こると、オーナーのうちの1人がグローバル名を失うことがある。さらに別の例では、クライアントが仮想バスに関連する他のバスノードに接続されるときに変換後の名前が使用されてもよい。そのような態様では、変換後の名前はアペンデッドエンドを含んでもよい(たとえば、グローバルに一意の識別子「1234」を有する分散バスに接続された周知の名前「org.foo」を有するローカルエンドポイント714は「G1234.org.foo」と見なされてもよい)。

【００７５】

メッセージシーケンスステップ766において、バスノード712およびバスノード732は、エンドポイントバストポロジーの変更について他のバスノードに通知するための信号を伝達(たとえば、ブロードキャスト)してもよい。その後、ローカルエンドポイント714からのトラフィックは、仮想エンドポイントを通過してデバイスB 730上の意図されるローカルエンドポイント734に達してもよい。さらに、動作中に、ローカルエンドポイント714とローカルエンドポイント734との間の通信はルーティンググループを使用してもよい。一態様では、ルーティンググループは、エンドポイントが信号、メソッド呼出し、またはエンドポイントのサブセットからの他の適切な情報を受信するのを可能にしてもよい。したがって、ルーティング名は、バスノード712または732に接続されたアプリケーションによ

って決定されてもよい。たとえば、P2Pアプリケーションは、アプリケーションに組み込まれた一意で周知のルーティンググループ名を使用してもよい。さらに、バスノード712および732は、ローカルエンドポイント714および734のルーティンググループへの登録および/または登録解除をサポートしてもよい。一実施形態では、ルーティンググループは、現在のバスインスタンスよりも後のインスタンスまで持続しなくてもよい。別の態様では、アプリケーションは、分散バスに接続するたびにアプリケーションの好ましいルーティンググループの登録をしてもよい。さらに、グループはオープンであっても(たとえば、任意のエンドポイントが参加してよい)またはクローズドであっても(たとえば、グループの作成者がグループを修正してもよい)よい。さらに、バスノード712または732は、他のリモートバスノードにルーティンググループエンドポイントの追加、削除、またはその他の変更を通知するための信号を送ってもよい。そのような実施形態では、バスノード712または732は、グループにメンバーが追加されならびに/あるいはグループからメンバーが削除されたときはいつでも他のグループメンバーにルーティンググループ変更信号を送ってもよい。さらに、バスノード712または732は、最初にルーティンググループから削除されることなく分散バスから切り離されるエンドポイントにルーティンググループ変更信号を送ってもよい。

【００７６】

Table 1(表1)およびTable 2(表2)は、本開示において使用される様々な用語および頭字語を定義した表である。

【００７７】

【表１】

Table 1: 用語

用語	定義
AllJoyn フレームワーク	低レベルネットワーク概念および API の抽象化を可能にするオープンソースピアツーピアフレームワーク。
AllJoyn コントローラデバイス	コントローラとも呼ばれる。コントローラの制御インターフェースにアドバタイズする別の AllJoyn デバイスを制御することができる AllJoyn デバイス。
AllJoyn 被制御側デバイス	被制御側とも呼ばれる。他の AllJoyn デバイスから制御を受けることができるようにデバイス自体の制御インターフェースにアドバタイズする AllJoyn デバイス。
エンドユーザ	AllJoyn デバイスおよびアプリケーションと相互作用する物理的な人間。
代理	権利を付与する権利を与えること。
許可	権利を与えること。

【００７８】

【表２】

Table 2: 頭字語

頭字語	定義
AJ	AllJoyn
GUID	グローバルに一意の識別子(Globally Unique Identifier)。衝突の確率を無視できるように無作為に生成される 128 ビット識別子
TC	シンクライアント(Thin Client)
ECDHE	エフェメラル楕円曲線 Diffie-Hellman 鍵交換(Ephemeral Elliptic Curve Diffie-Hellman key exchange)

【００７９】
QUALCOMM Incorporated(登録商標)によって提供されるAlljoyn(商標)Security Serviceなどの近接度ベースのP2Pプロトコルセキュリティサービスの目標は、被制御側デバイス(または被制御側)が被制御側のコントローラとの関係に基づいてセキュアインターフェースおよび/またはセキュアオブジェクトへのアクセスを制限するのを可能にすることである。コントローラと被制御側との間のセキュアなチャネルに加えて、このようなセキュリティサービスは、証明書のデータベースおよびデバイスアプリケーションにアクセスするためのアクセス制御リスト(ACL)を管理する。
【００８０】
特定のコントローラがアクセス権を有する場合があるセキュアオブジェクトまたはセキュアインターフェースのいずれかのセットは「ロール」としてグループ化される。コントローラは、1つまたは複数のロールに対するアクセス権を有する場合がある。ロールは、被制御側の開発者によってセットアップされ、一般に開発後に構成不能になる。
【００８１】
あらゆる被制御側は1つまたは複数の所有者コントローラを有する場合がある。所有者コントローラは、セキュリティサービスデータベースを維持する役目を果たす。所有者コントローラは、他のコントローラを、たとえばOpenIDまたはローカルGUIDのいずれかによって識別することによって、他のコントローラへのアクセスを許可してもよい。
【００８２】
近接度ベースのP2Pプロトコルネットワーク上のすべてのデバイスが(OpenID検証に必要な)直接インターネットアクセスを有するとは限らないので、OpenID認証を必要とするすべてのネットワークがセキュリティブリッジサービス(SBS)を実行することが必要になる場合がある。SBSは、OpenID検証に関するローカル要求を得て、クラウドと通信することによって認証を実行する。
【００８３】
OpenIDは、人気がある多数のサービス(たとえば、Yahoo!(登録商標)およびGoogle(登録商標))を対象とするグローバル識別子(ID)である。OpenIDによって、消費者は、友人および家族のグローバル識別子を知るか、またはそれらのグローバル識別子を要求することができる。消費者がそのデバイスにアクセスするうえで識別情報および証明書を作成する必要もあるいは共有する必要もない。消費者が、様々なロケーションに関する識別情報を記憶する必要はない。
【００８４】
図8は、本開示の一態様による、OpenID/OAuth/FaceConnectプロバイダ830を認証に使用するための例示的なフローを示す図である。OpenID/OAuthプロバイダ830は、図4におけるサーバ400に相当してもよい。802において、クライアント810(IoTデバイス200Aがセルフォン、スマートフォン、デスクトップコンピュータ、ラップトップコンピュータ、タブレ

ットコンピュータ、PDAなどとして具現化されるときは図2AにおけるIoTデバイス200Aに相当してもよい)は、OpenID/OAuthプロバイダ830に認証要求(たとえば、HTTP GET)を送信する。804において、OpenID/OAuthプロバイダ830はクライアント810に認証応答(たとえば、HTTPリダイレクト)を送信する。

【００８５】

OpenID/OAuthプロバイダ830が応答をHTTPリダイレクトとして送信することに留意されたい。しかし、クライアント810がウェブブラウザではない場合、リダイレクトに従う必要はない。その代わり、リダイレクトから取り出される唯一の情報は署名になる。結果として、署名は、(ハッシュ/オブジェクトを含む)return_toとOpenID識別情報をバインドする。さらに、この交換にクライアント810の電子メールアドレスを含めることができる。

【００８６】

図9は、本開示のセキュリティサービスに関する例示的なシステムアーキテクチャを示す図である。図9に示すシステムは、アプリケーション912を実行するコントローラデバイス910と、アプリケーション922を実行する被制御側デバイス920と、OpenID/OAuthプロバイダ830とを含む。コントローラデバイス910は、「スマート」デバイスであってもよく、IoTデバイス200Aがセルフォン、スマートフォン、デスクトップコンピュータ、ラップトップコンピュータ、タブレットコンピュータ、PDAなどとして具現化されるときは図2AのIoTデバイス200Aに相当してもよい。被制御側デバイス920は、それぞれ図2Aおよび図2BにおけるIoTデバイス200Aまたは200Bなどの任意のIoTデバイスであってもよい。アプリケーション912および922は、暗号化されたチャネルを介して互いに通信することができるが、チャネルは、コントローラがOpenIDを認証し被制御側がOpenIDを検証するまで検証されない。

【００８７】

コントローラデバイス910および被制御側デバイス920はどちらも、本明細書において説明する機能を実行するためにそれぞれ鍵交換認証モジュール916および926を含んでもよい。鍵交換認証モジュール916/926は、図2A/2Bにおける鍵交換認証モジュール216に相当してもよい。

【００８８】

各アプリケーション912および922は、認証を目的として割り当てられたGUIDを有する。所与のアプリケーションに関するすべての暗号化関連データがGUIDによってインデックス付けされた鍵ストアに記憶される。代表的な暗号化データにはマスタシークレット、セッション鍵、およびグループ鍵が含まれる。本開示では、鍵ストアをDiffie-Hellman鍵、エンドユーザオープンID情報、および許可を記憶するように拡張する。

【００８９】

エンドユーザは、コントローラデバイス910などのコントローラを使用する際、OpenID/OAuthプロバイダ(OP)830などのOpenID/OAuthプロバイダとの認証手順を実行することにより、被制御側デバイス920などの特定の被制御側によってアプリケーション912を検証することができる。この手順では、アプリケーションの認証GUIDをユーザのOpenID識別情報に関連付ける。本明細書において説明する検証を実行するには、セキュリティサービスがエンドユーザのOpenID証明書にアクセス権を有する必要がある。セキュリティサービスは、エンドユーザが自分のOpenIDログインサイトに証明書を与えるときにエンドユーザのOpenID証明書を取得することができる。

【００９０】

暗号化鍵を交換する領域において、Diffie-Hellman鍵交換(DHE)は、2つのピアアプリケーション912および922間に暗号化されたチャネルを確立するための実際的な方法である。Diffie-Hellman鍵交換は、互いに事前知識を有さない2人の当事者が、非セキュアな通信チャネルを介して共有秘密鍵を協働で確立するのを可能にする。次いで、この鍵を使用して、対称鍵暗号を用いて以後の通信を暗号化することが可能である。しかし、この通信は中間者攻撃を受ける。

【００９１】

Diffie-Hellman鍵交換に関する通信違反を検出できる方法がある。本開示は、OpenIDまたはOAuthプロトコルなどのエンドユーザ連合ログインを使用してDiffie-Hellman鍵交換などの鍵交換機構を認証し、通信当事者が違反を検出できるようにする方法を提供する。開示された方法では、エンドユーザが(対話式にあるいは記憶されたログイン情報を用いて)自分のアカウントにログインする必要がある。ソースとは無関係に、エンドユーザのアカウントへのログインは、OpenIDプロトコル(例示的なプロバイダにはGoogle(登録商標)およびYahoo!(登録商標)が含まれる)またはOAuthプロトコル(例示的なプロバイダにはFacebook(登録商標)が含まれる)によって、アプリケーションへのアクセスを許可するために実行され、このログインでは、通信チャネルが違反していないことを検証するためにOpenIDプロトコルまたはOAuthプロトコルの署名機能を使用して両当事者しか知らないトークンに署名する。

【００９２】

図10は、本開示の一態様に従って図9におけるコントローラデバイス910と被制御側デバイス920との間に(たとえば、Diffie-Hellman交換によって)セキュアなチャネルを確立するための例示的なフローを示す。この場合、両方のクライアントが共通するもの(たとえば、Diffie-Hellmanセッションパラメータ)に署名しそれを検証する。代替的に、両方のクライアントが公開鍵に署名することが可能である。

【００９３】

図10を参照して示す機能は、各デバイスの鍵交換認証モジュール916/926によって各デバイスのプロセッサ、トランシーバ、および/または入出力インターフェースと協働して実行されてもよい。たとえば、鍵交換認証モジュールが実行可能なモジュールである場合、コントローラデバイス910/被制御側デバイス920のプロセッサはそれぞれ、鍵交換認証モジュール916/926の機能を実行してもよく、それによってトランシーバがOP820および被制御側デバイス920/コントローラデバイス910と通信する。

【００９４】

1002～1004において、コントローラデバイス910と被制御側デバイス920は、Diffie-Hellman鍵を交換し、共有される秘密を生成する。1002において、コントローラデバイス910は、そのDiffie-Hellman鍵(「A_PublicKey」として表される)を被制御側デバイス920に送信する。1004において、コントローラデバイス920は、そのDiffie-Hellman鍵(「B_PublicKey」として表される)をコントローラデバイス910に送信する。この交換の後で、コントローラデバイス910および被制御側デバイス920の各々は、交換用の識別子を生成する。これは、公開鍵自体、それらのハッシュ、または擬似ランダム関数(PRF)を使用して算出されるベリファイアのいずれかである。

【００９５】

1006において、コントローラデバイス910はOpenID/OAuthプロバイダ830に認証要求を送信する。要求は、1002～1004において交換用に生成された識別子を含む。OpenIDおよびOAuthの場合、識別子はreturn_toパラメータに埋め込まれる。図10の例では、交換される識別子は、「HASH(A_PK|B_PK)」として表される「A_PublicKey」と「B_PublicKey」のハッシュを含む。1008において、コントローラデバイス910はOpenID/OAuthプロバイダ830から署名された応答を受信する。署名は識別子をカバーする。

【００９６】

1010において、被制御側デバイス920は、1006においてコントローラデバイス910によって送信された要求とは無関係にOpenID/OAuthプロバイダ830に認証要求を送信する。この要求は、1002～1004において交換用に生成された識別子も含む。OpenIDおよびOAuthの場合、識別子はreturn_toパラメータに埋め込まれる。1012において、被制御側デバイス920はOpenID/OAuthプロバイダ830から署名された応答を受信する。署名は識別子をカバーする。

【００９７】

1014～1016において、コントローラデバイス910と被制御側デバイス920は署名された応答を交換する。1018～1020において、コントローラデバイス910と被制御側デバイス920の

両方が(独立に)OpenID/OAuthプロバイダ830との認証チェックを行う。このチェックでは、1014～1016におけるデータ交換が有効であり、したがって、識別子が有効であることを検証する。1022～1024において、コントローラデバイス910と被制御側デバイス920の両方が認証完全肯定応答を交換する。

【００９８】

図11は、OpenIDプロバイダ、すなわち、OpenIDプロバイダ830を使用する図10に示すフローの例である。具体的に言うと、図11は、図9に示すコントローラデバイス910と被制御側デバイス920との間のOpenID検証に関する例示的なフローを示し、この場合、被制御側デバイス920はバンドリングされたセキュリティブリッジ924を含む。図11に示すフローは、エンドユーザのOpenID証明書を検証するための手順を示す。図11の例では、コントローラデバイス910は、コントローラアプリケーションを含む、スマートフォンなどのスマートデバイスであると仮定される。コントローラデバイス920は、バンドリングされたセキュリティブリッジ924を使用してOpenIDプロバイダとの検証を行う。被制御側デバイス920の開発者は、セキュリティブリッジ924機能を被制御側デバイス920に含めるかどうかを決定してもよい。セキュリティブリッジ924は、HTTPSコードおよび保証されたインターネット接続に基づいてもよい。デバイス910および920は、図11の例では、コントローラおよび被制御側として示されているが、任意の2つのピアデバイスであってもよい。

【００９９】

図11を参照して示す機能は、各デバイスの鍵交換認証モジュール916/926によって各デバイスのプロセッサ、トランシーバ、および/または入出力インターフェースと協働して実行されてもよい。たとえば、鍵交換認証モジュールが実行可能なモジュールである場合、コントローラデバイス910/被制御側デバイス920のプロセッサはそれぞれ、鍵交換認証モジュール916/926の機能を実行してもよく、それによって、コントローラアプリケーション912/被制御側アプリケーション922、セキュリティブリッジ924、およびそれぞれのAlljoyn(商標)コアが図11に示す機能を実行する。

【０１００】

図11に示すフローは、1102から始まり、コントローラデバイス910上のコントローラアプリケーション912が、クライアント(CGUID)とサービス(SGUID)との間にDiffie-Hellmanを使用するセキュアなセッションを確立する。セキュアなチャネルが、まだ利用可能になっていない場合にのみセットアップされることに留意されたい。1104において、コントローラアプリケーション912が、たとえばコントローラデバイス910内のAllJoyn(商標)コアに両方の公開鍵(すなわち、Diffie-Hellman鍵)のハッシュに関する要求を送信する。1108において、コントローラアプリケーション912は、1106においてAllJoyn(商標)コアからハッシュを受信したことに応答して、WebViewクライアントまたは他の同様のクライアントをオープンする。たとえば、コントローラアプリケーション912は、Android上のWebViewClientまたはiOS上のUIWebViewを使用してウエブブラウザセッションをオープンする。

【０１０１】

1110において、WebViewクライアントをオープンした後、コントローラアプリケーション912は、WebViewクライアントにおけるOpenIDプロバイダ830にHTTPS「mode=checked_setup」メッセージを送信する。コントローラアプリケーション912は、OpenIDログイン要求におけるドメインwww.alljoyn-security.orgを使用してリターンアドレスにセッション鍵ハッシュを付加する。1112において、OpenIDプロバイダ830は、OpenIDログインページに関するHTMLコンテンツによって応答する。1114において、コントローラアプリケーション912は、エンドユーザに対してログインスクリーンを表示するか、あるいは代替的に、エンドユーザが以前にログイン時に記憶させたログイン情報にアクセスし、エンドユーザのOpenID証明書を受信する。さらに、エンドユーザが現在ログインされており、エンドユーザのOpenID証明書が依然として有効である場合、これらのOpenID証明書は、追加のログインを必要とせずに使用することが可能である。

【０１０２】

コントローラアプリケーション912は、エンドユーザのOpenID証明書を受信したことに

応答して、1116においてログインスクリーンコンテンツをOpenIDプロバイダ830にサブミットする。1118において、OpenIDプロバイダ830は、「mode=id_res」を含む認証応答ハッシュによるHTMLリダイレクトによって応答する。1120において、コントローラアプリケーション912は、リダイレクトを実行せず、その代わりに認証応答のコンテンツを抽出する。1122において、コントローラアプリケーション912は、OpenIDプロバイダ830によって署名された認証応答を、たとえば被制御側デバイス920上のAllJoyn(商標)コアに送信する。

【０１０３】

AllJoyn(商標)コアは、コントローラアプリケーション912から認証応答を受信したことに応答して、1124において、セッションハッシュを検証する。1120と1124の両方において、2つの公開鍵の完全性を確保するためにopenid.return_toフィールドにおけるセッションIDハッシュが検証される。1126において、AllJoyn(商標)コアは、関数ValidateOpenID(authResp)によって内部セキュリティブリッジ924を呼び出す。1128において、セキュリティブリッジ924は、OpenIDプロバイダ830を呼び出し、mode=check_authenticationを使用して認証署名を検証する。1130において、OpenIDプロバイダ830はメッセージ「is_valid:true」によって応答する。しかし、セッションハッシュがコントローラデバイス910において使用される値とは異なる場合、check_authorizationは署名チェックに失敗する。

【０１０４】

1132において、セキュリティブリッジ924は、グローバルID検証が「OK」であることを示すメッセージをAllJoyn(商標)コアに送信する。それに応答して、1134において、AllJoyn(商標)コアは、CGUIDをグローバルIDによって検証済みとマークし、1136において、グローバルID検証が「OK」であることを示すメッセージをコントローラアプリケーション912に送信する。

【０１０５】

図12は、OAuthプロバイダ、すなわち、Facebook(登録商標)などのOAuthプロバイダ830を使用する図10に示すフローの例である。具体的に言うと、図12は、図9に示すコントローラデバイス910と被制御側デバイス920との間のOAuth検証を示し、この場合、被制御側デバイス920は、図11とは異なり、バンドリングされたセキュリティブリッジを含まない。図12に示す例では、OAuthプロバイダはFacebook(登録商標)であるものとして示されている。被制御側アプリケーション922またはセキュリティブリッジ924は、Facebook(登録商標)アカウントの検証をサポートするために、Facebook(登録商標)アプリケーションIDを提供する必要がある。Facebook(登録商標)でもそのような情報が必要である。詳細には、Facebook(登録商標)では、OAuthログインスクリーンを呼び出すために登録されたアプリケーションIDが必要である。デバイス910および920は、図12の例では、コントローラおよび被制御側として示されているが、任意の2つのピアデバイスであってもよい。

【０１０６】

図12を参照して示す機能は、各デバイスの鍵交換認証モジュール916/926によって各デバイスのプロセッサ、トランシーバ、および/または入出力インターフェースと協働して実行されてもよい。たとえば、鍵交換認証モジュールが実行可能なモジュールである場合、コントローラデバイス910/被制御側デバイス920のプロセッサはそれぞれ、鍵交換認証モジュール916/926の機能を実行してもよく、それによって、コントローラアプリケーション912/被制御側アプリケーション922およびそれぞれのAlljoyn(商標)コアが図12に示す機能を実行する。

【０１０７】

図12に示すフローは、1202から始まり、コントローラアプリケーション912が、CGUIDとSGUIDとの間にDiffie-Hellmanを使用するセキュアなセッションを確立する。セキュアなチャネルが、まだ利用可能になっていない場合にのみセットアップされることに留意されたい。1204において、コントローラアプリケーション912が、たとえばコントローラデバイス910内のAllJoyn(商標)コアに両方の公開鍵のハッシュに関する要求を送信する。コントローラアプリケーション912は、1206においてAllJoyn(商標)コアからハッシュを受信したことに応答して、1208においてFacebook(登録商標)へのログオンを開始する。外部セキ

ュリティブリッジ924は、ログオン要求を受信したことに応答して、1210において、Facebook(登録商標)AppIDおよびアプリケーションコールバックURLを、たとえば被制御側デバイス920のAllJoyn(商標)コアに送信し、AllJoyn(商標)コアはこの情報をコントローラアプリケーション912に転送する。

【０１０８】

1212において、コントローラアプリケーション912は、WebViewクライアントまたは同様のクライアントをオープンし、1214において、AppIDを含むOAuth要求をWebViewクライアントにおけるFacebook(登録商標)サーバに送信する。たとえば、コントローラアプリケーション912は、Android上のWebViewClientまたはiOS上のUIWebViewを使用してウエブブラウザセッションをオープンする。コントローラアプリケーション912は、Facebook(登録商標)アプリケーションコールバックURLをredirect_uriとして使用して、セッション鍵ハッシュコールバックURLおよび状態フィールドを追加する。1216において、Facebook(登録商標)サーバは、Facebook(登録商標)ログインページに関するHTMLコンテンツによって応答する。1218において、コントローラアプリケーション912は、エンドユーザに対してログインスクリーンを表示し、エンドユーザのFacebook(登録商標)証明書を受信する。

【０１０９】

コントローラアプリケーション912は、エンドユーザの証明書を受信したことに応答して、1220において、ログインスクリーンコンテンツをFacebook(登録商標)サーバにサブミットする。1222において、Facebook(登録商標)サーバは、アクセストークンを含む認証応答によるHTMLリダイレクトによって応答する。1224において、コントローラアプリケーション912は、リダイレクトを実行せず、その代わりにコードに関して認証応答を抽出して解析する。コントローラアプリケーション912は、状態フィールドにおけるセッションIDハッシュも検証する。1226において、コントローラアプリケーション912は、このコードを被制御側デバイス920上のAllJoyn(商標)コアに送信する。

【０１１０】

AllJoyn(商標)コアは、コントローラアプリケーション912からコードを受信したことに応答して、1228において、関数ValidateFacebook(セッションハッシュ、コード)によって外部セキュリティブリッジ924を呼び出す。1230において、セキュリティブリッジ924は次に、要求「https://graph.facebook.com/oauth/access_token?redirect_uri=&code=」によってFacebook(登録商標)サーバを呼び出し、それに応答して、1232において、アクセストークンを受信する。コードをアクセストークンと交換することはOAuth特有の方法であることに留意されたい。さらに、アプリケーションコールバックURLとセッションハッシュとを含むredirect_uriが形成される。redirect_uriが、セッションハッシュを検証するコントローラと一致しない場合、access_tokenコールは失敗する。

【０１１１】

1234において、セキュリティブリッジ924は次に、要求「https://graph.facebook.com/me?scope=email&access_token=」によってFacebook(登録商標)サーバを呼び出し、それに応答して、1236において、エンドユーザのFacebook(登録商標)ユーザ名および電子メールを受信する。1238において、セキュリティブリッジ924は、エンドユーザのFacebook(登録商標)ユーザ名および電子メールを被制御側デバイス920のAllJoyn(商標)コアに送信し、1240において、AllJoyn(商標)コアがCGUIDをグローバルIDによって検証済みとマークする。1242において、AllJoyn(商標)コアは、グローバルID検証が「OK」であることを示すメッセージをコントローラアプリケーション912に送信する。

【０１１２】

諒解されるように、図11および図12は、様々なメッセージがコントローラデバイス910および/または被制御側デバイス920におけるAllJoyn(商標)コアと交換されることを示すが、これは例示的な実施形態にすぎず、他の通信プロトコルが使用されてもよい。

【０１１３】

以下の表は、コントローラデバイス910および被制御側デバイス920がグローバルIDプロバイダに提供する必要がある必要な情報データを表す。

【０１１４】
【表３】

Table 3: グローバル **ID** 検証に必要なアプリケーションデータ

グローバル **ID** プロバイダ	コントローラ	コントローラ/セキュリティブリッジ	エンドユーザフレンドリー**ID**
OpenID	なし	なし	電子メールアドレス
Facebook(登録商標)(OAuth を使用する)	なし	有効な Facebook(登録商標)アプリケーション ID およびアプリケーションシークレット	電子メールアドレス

【０１１５】
図13は、本開示の一態様による、第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するための例示的なフローを示す。図13に示すフローは、図9におけるコントローラデバイス910または被制御側デバイス920によって実行されてもよい。便宜上、図13に示すフローは、コントローラデバイス910によって実行されるものとして説明する。
【０１１６】
図13に示すフローは1302から始まり、第1のピアデバイスは、図10の1006、図11の1116、および図12の1220のように、第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信する。同様に、第2のピアデバイスは、図10の1010のように、ユーザの連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する。
【０１１７】
第1の連合ログインプロバイダおよび第2の連合ログインプロバイダは、同じ連合ログインプロバイダであってもあるいはそれぞれに異なる連合ログインプロバイダであってもよい。しかし、第1の連合ログインプロバイダと第2の連合ログインプロバイダの両方が、OpenID、OAuth、またはFaceConnectなどの同じ連合ログインプロトコルをサポートすべきである。
【０１１８】
第1の識別子と第2の識別子は、同じ識別子であってもあるいはそれぞれに異なる識別子であってもよい。第1の識別子と第2の識別子は、同じ識別子である場合、共通のハッシュまたは算出されたベリファイアであってもよい。第1の識別子と第2の識別子がそれぞれに異なる識別子である場合、第1の識別子は、第1のピアデバイスによって生成される第1の公開鍵であってもよく、第2の識別子は、第2のピアデバイスによって生成される第2の公開鍵であってもよい。
【０１１９】
1304において、第1のピアデバイスは、図10の1008、図11の1118、および図12の1222のように、第1の連合ログインプロバイダから第1の認証応答を受信する。同様に、第2のピアデバイスは、図10の1012のように、第2の連合ログインプロバイダから第2の認証応答を受信する。
【０１２０】
1306において、第1のピアデバイスは、図10の1016のように、第2のピアデバイスから第2の認証応答を受信する。
【０１２１】
1308において、第1のピアデバイスは、図10の1018のように、第2の連合ログインプロバイダによる第2の認証応答を認証する。
【０１２２】

1310において、第1のピアデバイスは、図10の1014のように、第1の認証応答を第2のピアデバイスに送信する。第2のピアデバイスは、図10の1020、図11の1126～1132、および図12の1228～1238のように、第1の連合ログインプロバイダによる第1の認証応答を認証する。

【０１２３】

1312において、第1のピアデバイスは、図10の1022、図11の1136、および図12の1242のように、第2のピアデバイスが第1の認証応答を認証したことを示す肯定応答を第2のピアデバイスから受信する。

【０１２４】

1314において、第1のピアデバイスは、図10の1024のように、第1のピアデバイスが第2の認証応答を認証したことを示す肯定応答を第2のピアデバイスに送信する。

【０１２５】

1316において、第1のピアデバイスは、第2のピアデバイスからの肯定応答に基づいて鍵交換を認証し、第2のピアデバイスは、第1のピアデバイスからの肯定応答に基づいて鍵交換を認証する。

【０１２６】

図14は、相互に関係する一連の機能モジュールとして表された、例示的なユーザデバイス装置1400を示す。送信するためのモジュール1402は、少なくともいくつかの態様では、たとえば、本明細書において説明したように図2Aにおけるトランシーバ206などの通信デバイスに相当してもよい。受信するためのモジュール1404は、少なくともいくつかの態様では、たとえば、本明細書において説明したように図2Aにおけるトランシーバ206などの通信デバイスに相当してもよい。受信するためのモジュール1406は、少なくともいくつかの態様では、たとえば、本明細書において説明したように図2Aにおけるトランシーバ206などの通信デバイスに相当してもよい。認証するためのモジュール1408は、少なくともいくつかの態様では、たとえば、本明細書において説明したように図2Aにおけるプロセッサ208とともに鍵交換認証モジュール216などの処理システムと協働する、図2Aにおけるトランシーバ206などの通信デバイスに相当してもよい。送信するためのモジュール1410は、少なくともいくつかの態様では、たとえば、本明細書において説明したように図2Aにおけるトランシーバ206などの通信デバイスに相当してもよい。受信するためのモジュール1412は、少なくともいくつかの態様では、たとえば、本明細書において説明したように図2Aにおけるトランシーバ206などの通信デバイスに相当してもよい。送信するためのモジュール1414は、少なくともいくつかの態様では、たとえば、本明細書において説明したように図2Aにおけるトランシーバ206などの通信デバイスに相当してもよい。認証するためのモジュール1416は、少なくともいくつかの態様では、たとえば、本明細書において説明したように図2Aにおけるプロセッサ208とともに鍵交換認証モジュール216などの処理システムと協働する、図2Aにおけるトランシーバ206などの通信デバイスに相当してもよい。

【０１２７】

図14のモジュールの機能は、本明細書の教示と矛盾しない様々な方法で実装されてもよい。いくつかの設計では、これらのモジュールの機能は、1つまたは複数の電気構成要素として実装されてもよい。いくつかの設計では、これらのブロックの機能は、1つまたは複数のプロセッサ構成要素を含む処理システムとして実装されてもよい。いくつかの設計では、これらのモジュールの機能は、たとえば、1つまたは複数の集積回路(たとえば、ASIC)の少なくとも一部分を使用して実装されてもよい。本明細書で説明するように、集積回路は、プロセッサ、ソフトウェア、他の関連の構成要素、またはそれらの何らかの組合せを含んでもよい。したがって、異なるモジュールの機能は、たとえば、集積回路の異なるサブセットとして実装されてもよく、あるいは1組のソフトウェアモジュールの異なるサブセットとして実装されてもよく、あるいはその組合せとして実装されてもよい。また、(たとえば、集積回路の、および/またはソフトウェアモジュールのセットの)所与のサブセットが、2つ以上のモジュールに関する機能の少なくとも一部分を実現する場合があることが諒解されよう。

【０１２８】
加えて、図14によって表される構成要素および機能ならびに本明細書で説明する他の構成要素および機能は、任意の適切な手段を使用して実装されてもよい。そのような手段はまた、少なくとも部分的に、本明細書で教示する対応する構造を使用して実装されてもよい。たとえば、図14の「ためのモジュール」構成要素とともに上記で説明した構成要素はまた、同様に指定された「ための手段」機能に相当してもよい。したがって、いくつかの態様では、そのような手段のうちの1つまたは複数は、プロセッサ構成要素、集積回路、または本明細書で教示する他の適切な構造のうちの1つまたは複数を使用して実装されてもよい。

【０１２９】
情報および信号が多種多様な異なる技術および技法のいずれかを使用して表すことができることを、当業者は理解されよう。たとえば上記説明全体を通して参照することができるデータ、命令、指令、情報、信号、ビット、記号およびチップは、電圧、電流、電磁波、磁界または粒子、光学場または粒子、あるいはそれらの任意の組合せによって表すことができる。

【０１３０】
さらに、本明細書で開示する態様に関連して説明した様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装され得ることを当業者は理解されよう。ハードウェアおよびソフトウェアのこの互換性を明確に示すために、様々な例示的な構成要素、ブロック、モジュール、回路、およびステップは、一般的にそれらの機能性に関してこれまで説明されてきた。そのような機能性がハードウェアとして実現されるか、またはソフトウェアとして実現されるかは、具体的な適用例および全体的なシステムに課される設計制約によって決まる。当業者は、説明される機能を具体的な応用形態ごとに様々な方法で実現することができるが、そのような実現の決定は、本開示の範囲からの逸脱を生じるものと解釈されるべきではない。

【０１３１】
本明細書に開示する態様と関連して説明する様々な例示的な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途用集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブルロジックデバイス、個別のゲートもしくはトランジスタロジック、個別のハードウェア部品、または本明細書に記載した機能を行うように設計されたこれらの任意の組合せを用いて、実装または実行され得る。汎用プロセッサを、マイクロプロセッサとすることができるが、代替案では、プロセッサを、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械とすることができる。プロセッサはまた、コンピューティングデバイスの組合せ(たとえば、DSPおよびマイクロプロセッサの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成)として実装され得る。

【０１３２】
本明細書において開示する態様に関連して説明した方法、シーケンス、および/またはアルゴリズムは、ハードウェアで、プロセッサによって実行されるソフトウェアモジュールで、またはその2つの組合せで直接具現され得る。ソフトウェアモジュールは、RAM、フラッシュメモリ、ROM、EPROM、EEPROM、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当技術分野で知られている任意の他の形態の記憶媒体内に存在し得る。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読取り、そこに情報を書込みできるようにプロセッサに結合される。代替案では、記憶媒体は、プロセッサに一体とされ得る。プロセッサおよび記憶媒体は、ASIC内に存在し得る。ASICはIoTデバイス内に存在し得る。代替として、プロセッサおよび記憶媒体は、ユーザ端末内に個別の構成要素として存在し得る。

【０１３３】

1つまたは複数の例示的な態様では、述べられる機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せで、実施され得る。ソフトウェアに実装される場合、機能は、1つまたは複数の命令またはコードとして、コンピュータ可読媒体上に記憶されるか、または、コンピュータ可読媒体を介して送信される場合がある。コンピュータ可読媒体は、ある場所から別の場所へのコンピュータプログラムの転送を可能にする任意の媒体を含む、コンピュータ記憶媒体と通信媒体の両方を含む。記憶媒体は、コンピュータによってアクセスできるすべての使用可能な媒体とすることができる。限定ではなく例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスク(disc)ストレージ、磁気ディスク(disk)ストレージもしくは他の磁気ストレージデバイス、あるいは命令もしくはデータ構造の形で所望のプログラムコードを担持しまたは記憶するのに使用でき、コンピュータによってアクセスできる任意の他の媒体を含むことができる。また、任意の接続は、適切にコンピュータ可読媒体と呼ばれる。たとえば、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用して、ウェブサイト、サーバ、または他のリモートソースからソフトウェアが送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。本明細書で使用するディスク(disk)およびディスク(disc)は、CD、レーザディスク(disc)、光ディスク(disc)、DVD、フロッピーディスク(disk)およびBlu-ray(登録商標)ディスク(disc)を含み、ディスク(disk)は、通常、データを磁気的に再生し、ディスク(disc)は、データをレーザで光学的に再生する。前述の組合せも、コンピュータ可読媒体の範囲内に含まれるべきである。

【０１３４】

上記の開示は本開示の例示的な態様を示すが、添付の特許請求の範囲によって規定される本開示の範囲から逸脱することなく、本明細書で様々な変更および修正が行われ得ることに留意されたい。本明細書で説明した本開示の態様による方法クレームの機能、ステップおよび/または動作は、特定の順序で実施される必要はない。さらに、本開示の要素は、単数形で記載または特許請求されている場合があるが、単数形に限定することが明示的に述べられていない限り、複数形が考えられる。

【符号の説明】

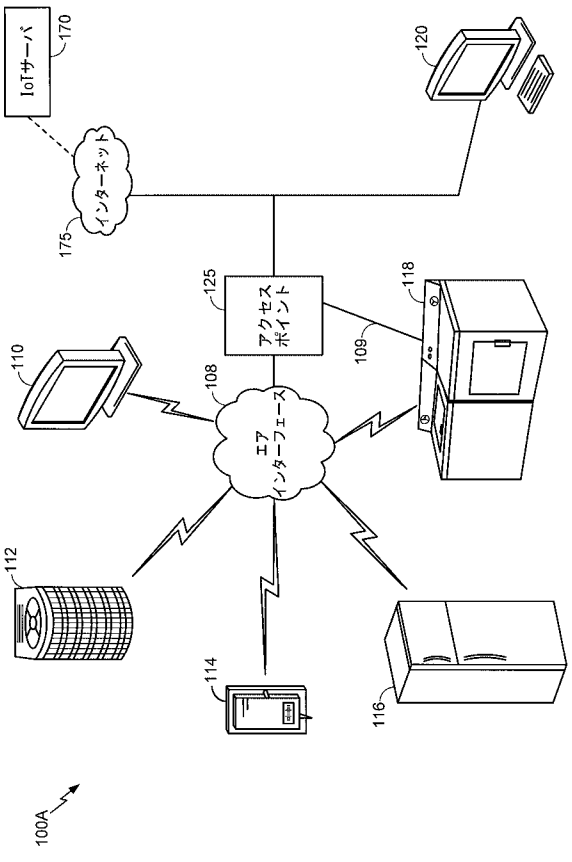
【０１３５】

100A、100B、100C　ワイヤレス通信システム
105　受動IoTデバイス
108　エアインターフェース
109　直接有線接続
110　テレビジョン、IoTデバイス
112　屋外空調機、IoTデバイス
114　温度自動調整器、IoTデバイス
116　冷蔵庫、IoTデバイス
116A、116B　IoTデバイス
118　洗濯機および乾燥機、IoTデバイス
120　コンピュータ
122A、122B　IoTデバイス
124A、124B　IoTデバイス
125　アクセスポイント
130　IoTマネージャ、スーパーバイザデバイス
140、140A、140B　IoT SuperAgent
145　ゲートウェイ機能
152　アプリケーションレイヤ
154　CMPレイヤ
156　トランスポートレイヤ

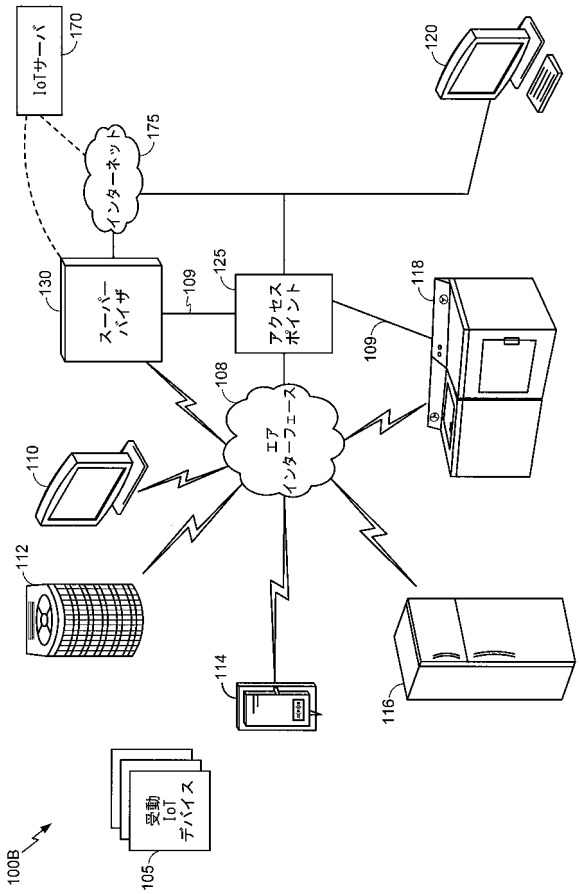
158 物理レイヤ
160 IoTグループ、IoTデバイスグループ
160A、160B IoTデバイス
170 IoTサーバ
175 インターネット
180 リソース
200A IoTデバイス
202 プラットフォーム
206 トランシーバ
208 プロセッサ
210 カメラ
212 メモリ
214 入出力(I/O)インターフェース
216 鍵交換認証モジュール
222、224A、224B ボタン
226 ディスプレイ
300 通信デバイス
305 論理
310 論理
315 論理
320 論理
325 論理
400 サーバ
401 プロセッサ
402 揮発性メモリ
403 ディスクドライブ
404 ネットワークアクセスポート
406 ディスクドライブ
407 ネットワーク
500 ワイヤレス通信ネットワーク、WAN、ワイヤレスネットワーク
510、510a、510b、510c 基地局
520 デバイス
530 ネットワークコントローラ
540 DHCPサーバ
600 例示的な環境
610 第1のデバイス
612 分散バスノード
614 ローカルエンドポイント
625 分散バス、仮想分散バス
630 第2のデバイス
632 分散バスノード
634 ローカルエンドポイント
640 第3のデバイス
642 分散バスノード
644 ローカルエンドポイント
700 例示的なメッセージシーケンス
710 第1のデバイス、デバイスA
730 第2のデバイス、デバイスB
712 バスノード
714 ローカルエンドポイント

732　バスノード
734　ローカルエンドポイント
810　クライアント
830　OpenID/OAuthプロバイダ
910　コントローラデバイス
912　コントローラアプリケーション
916　鍵交換認証モジュール
920　被制御側デバイス
922　被制御側アプリケーション
924　セキュリティブリッジ
1400　ユーザデバイス装置
1402　送信するためのモジュール
1404　受信するためのモジュール
1406　受信するためのモジュール
1408　認証するためのモジュール
1410　送信するためのモジュール
1412　受信するためのモジュール
1414　送信するためのモジュール
1416　認証するためのモジュール

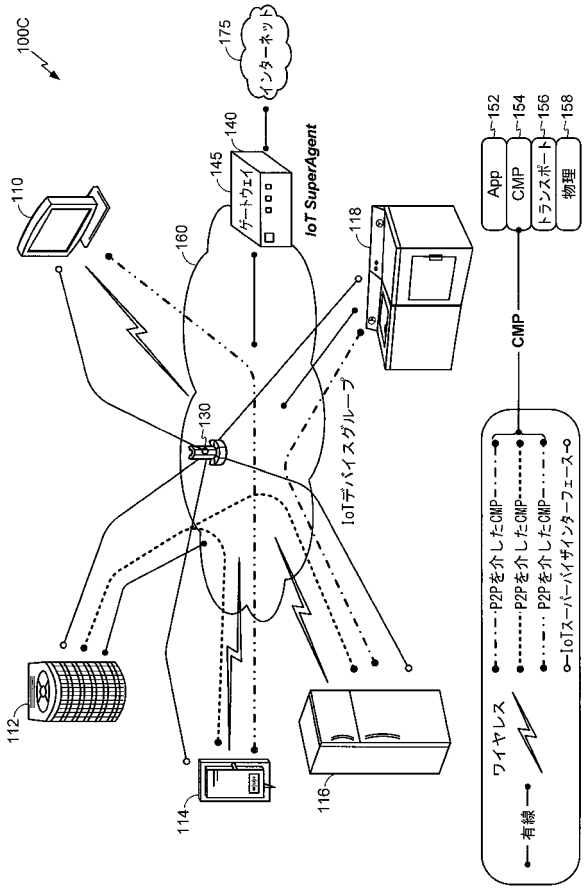
【図１Ａ】



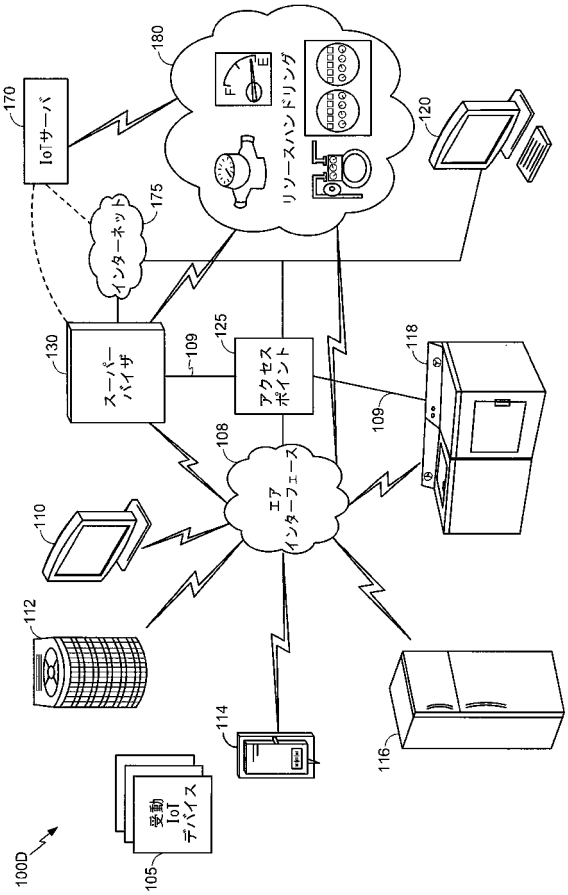
【図１Ｂ】



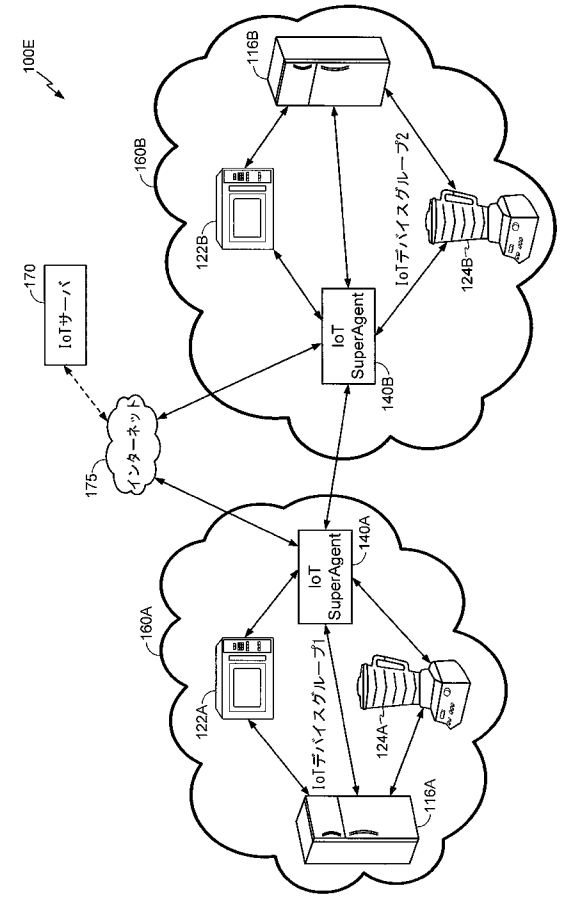
【図１Ｃ】



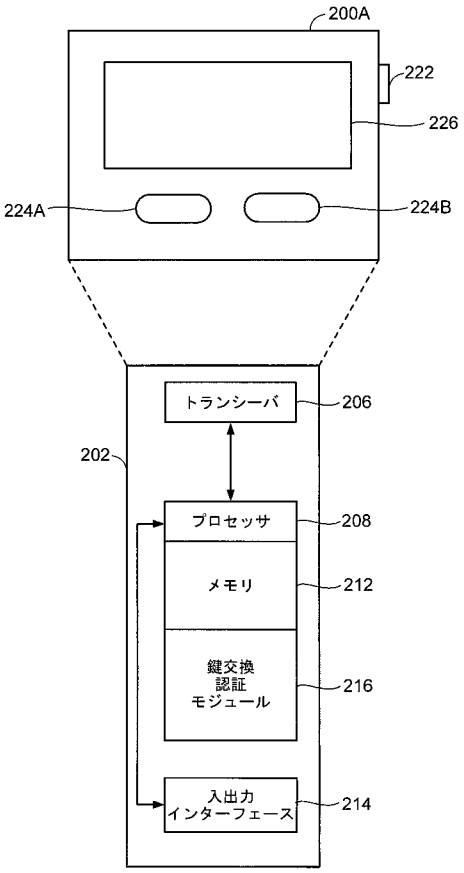
【図１Ｄ】



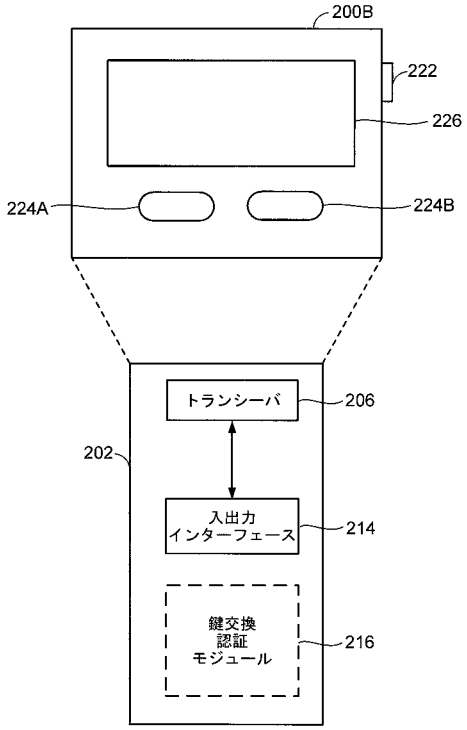
【図１Ｅ】



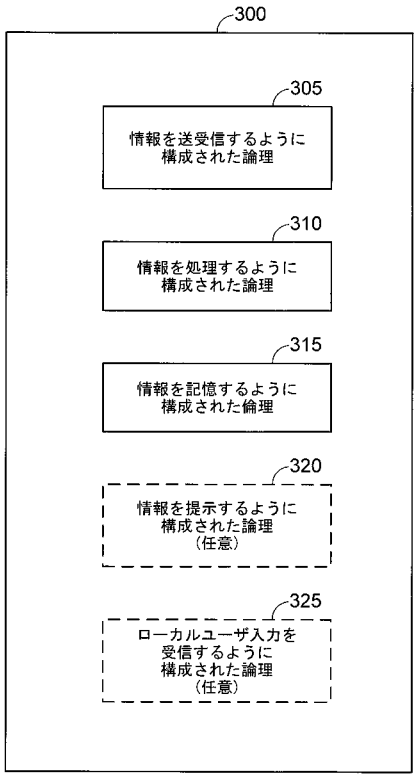
【図２Ａ】



【図２Ｂ】



【図３】



【図４】

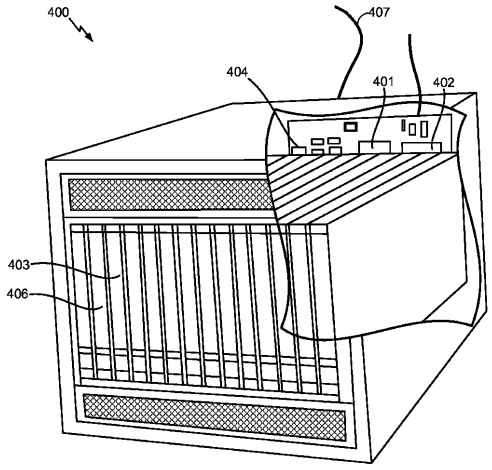
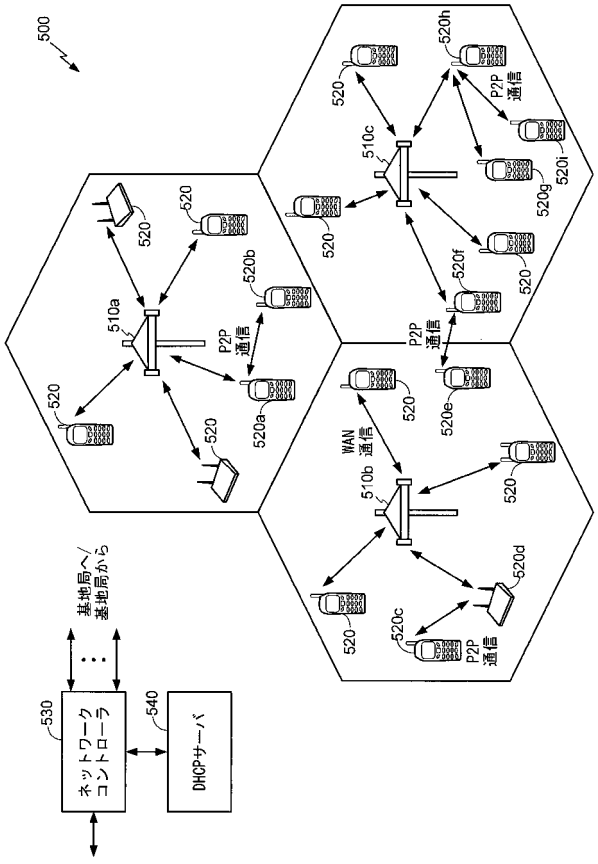
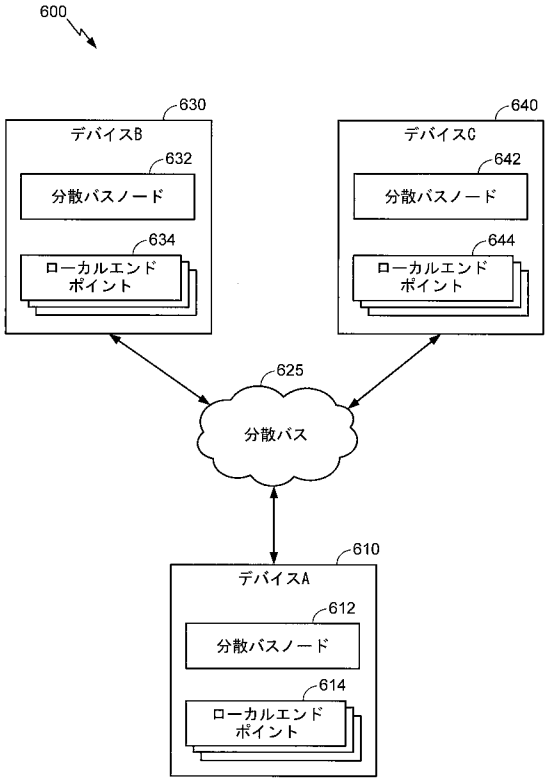


FIG. 4

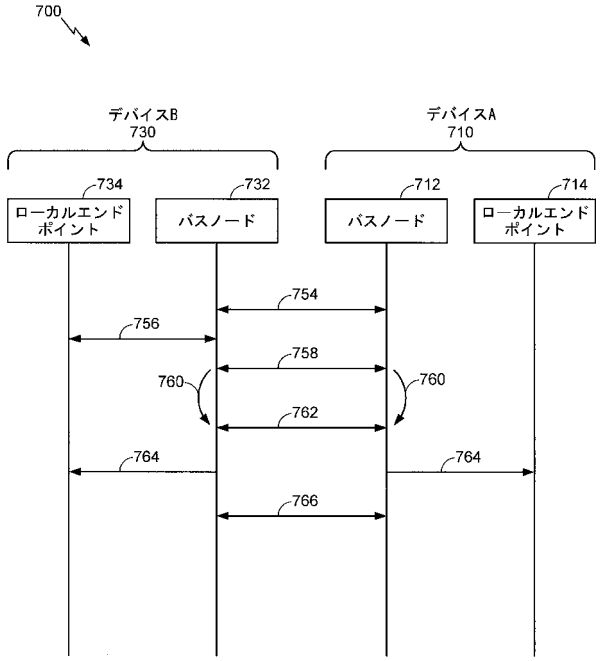
【図５】



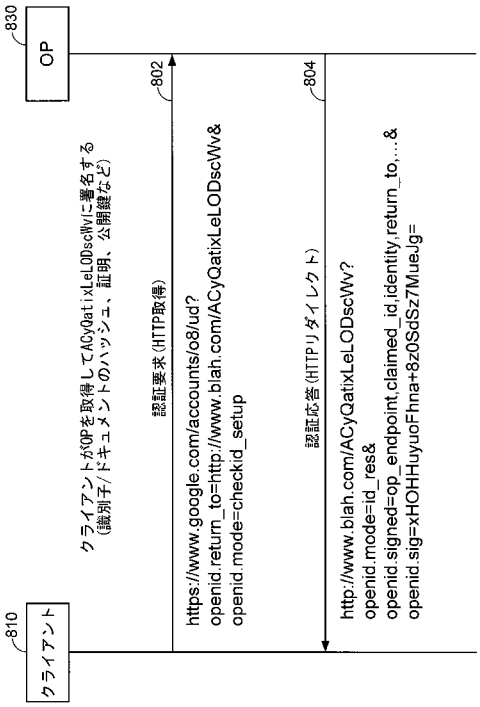
【図６】


600
630
デバイスB
632
分散バスノード
634
ローカルエンドポイント
640
デバイスC
642
分散バスノード
644
ローカルエンドポイント
625
分散バス
610
デバイスA
612
分散バスノード
614
ローカルエンドポイント

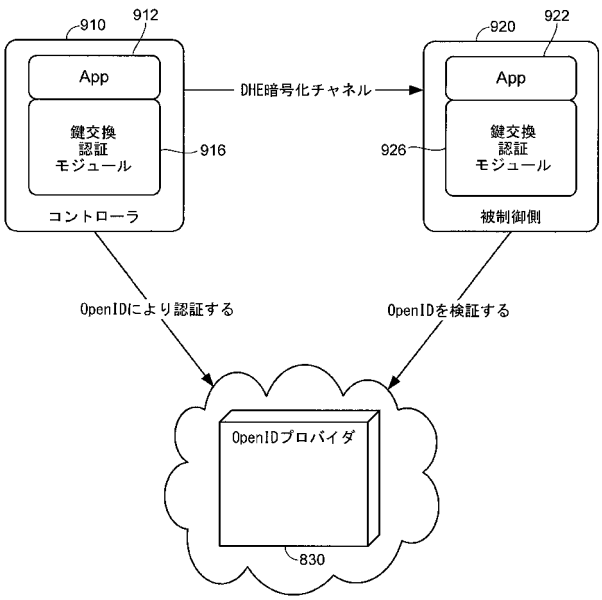
【図７】


700
デバイスB
730
デバイスA
710
734
ローカルエンドポイント
732
パスノード
712
パスノード
714
ローカルエンドポイント
754
756
758
760
760
762
764
764
766

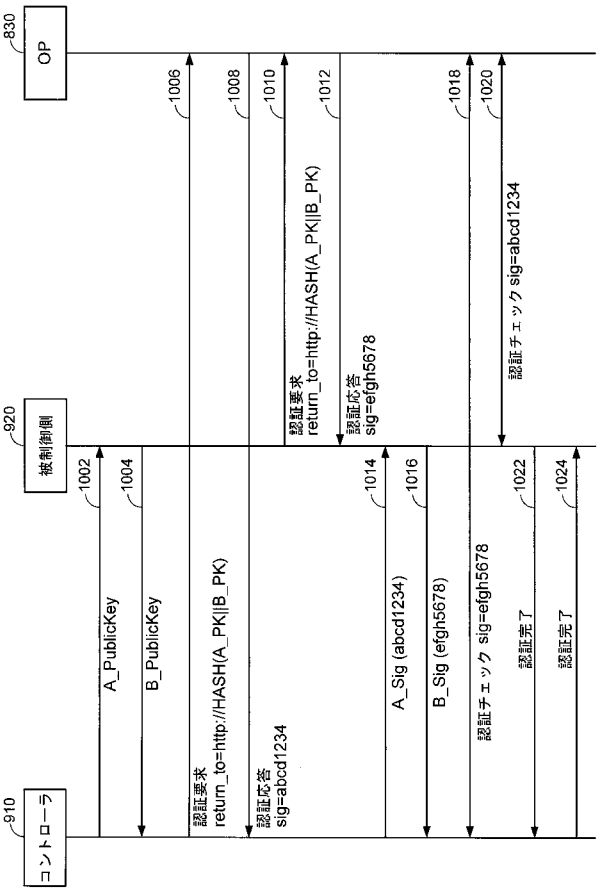
【図８】


830
OP
802
804
クライアントがOPを取得してACyQatixLeLODscWvに署名する
(識別子/ドキュメントのハッシュ、証明、公開鍵など)
認証要求(HTTP取得)
https://www.google.com/accounts/o8/ud?
openid.return_to=http://www.blah.com/ACyQatixLeLODscWv&
openid.mode=checkid_setup
認証応答(HTTPリダイレクト)
http://www.blah.com/ACyQatixLeLODscWv?
openid.mode=id_res&
openid.signed=op_endpoint,claimed_id,identity,return_to,...&
openid.sig=xHOHHuyuoFhna+8z0SdSz7MueJg=
810
クライアント

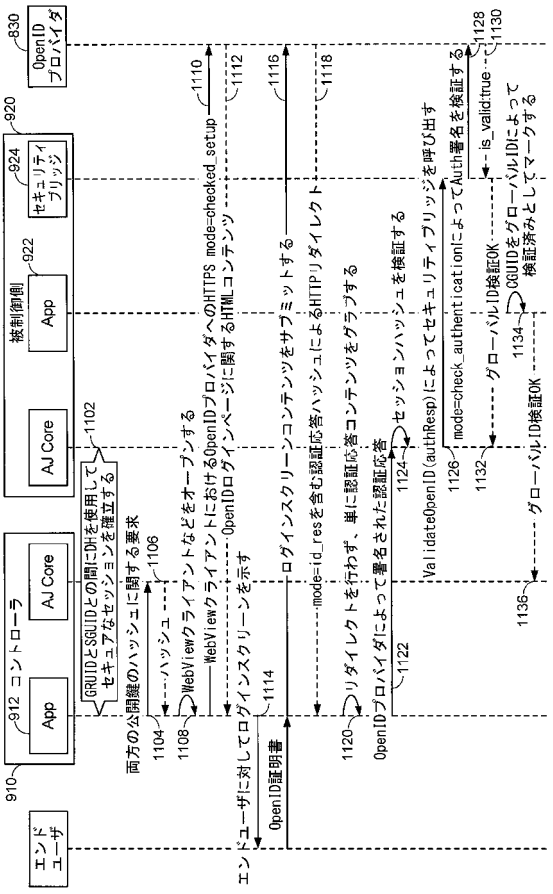
【図９】


910
912
App
鍵交換
認証
モジュール
916
コントローラ
DHE暗号化チャネル
920
922
App
鍵交換
認証
モジュール
926
被制御側
OpenIDにより認証する
OpenIDを検証する
OpenIDプロバイダ
830

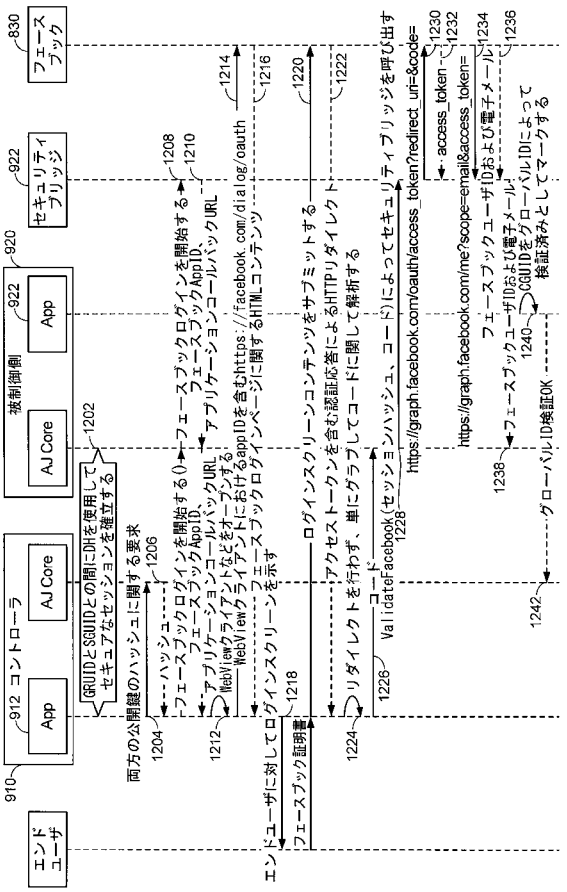
【図１０】



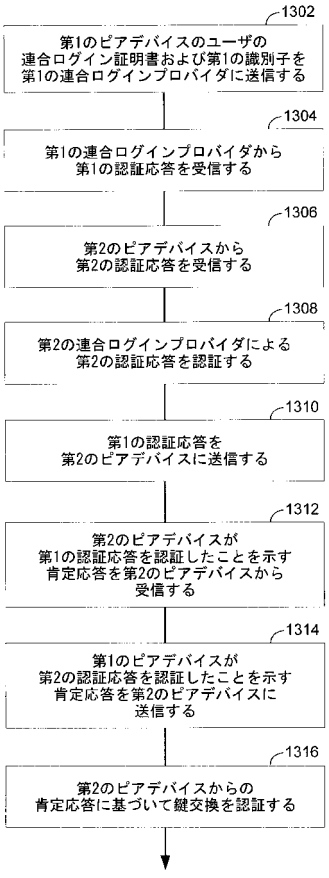
【図１１】



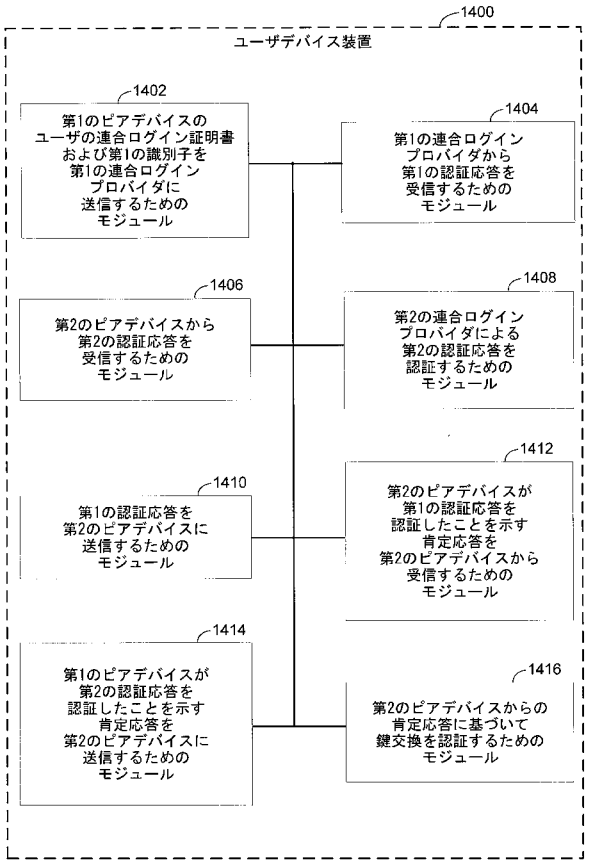
【図１２】



【図１３】



【図１４】



【手続補正書】
【提出日】平成28年9月6日(2016.9.6)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証する方法であって、
前記第1のピアデバイスによって、前記第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信するステップであって、前記第2のピアデバイスは、前記ユーザの前記連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信するステップと、
前記第1のピアデバイスによって、前記第1の連合ログインプロバイダから第1の認証応答を受信するステップであって、前記第2のピアデバイスは、前記第2の連合ログインプロバイダから第2の認証応答を受信するステップと、
前記第1のピアデバイスによって、前記第2のピアデバイスから前記第2の認証応答を受信するステップと、
前記第1のピアデバイスによって、前記第2の連合ログインプロバイダによる前記第2の認証応答を認証するステップと、
前記第1のピアデバイスによって、前記第1の認証応答を前記第2のピアデバイスに送信するステップであって、前記第2のピアデバイスは、前記第1の連合ログインプロバイダによる前記第1の認証応答を認証するステップと、
前記第1のピアデバイスによって、前記第2のピアデバイスが前記第1の認証応答を認証

したことを示す肯定応答を前記第2のピアデバイスから受信するステップと、
前記第1のピアデバイスによって、前記第1のピアデバイスが前記第2の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスに送信するステップと、
前記第1のピアデバイスによって、前記第2のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するステップであって、前記第2のピアデバイスは、前記第1のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するステップとを含む方法。
【請求項２】
前記第1の認証応答を受信するステップが、前記第1の認証応答によるHTMLリダイレクトを受信するステップを含む、請求項1に記載の方法。
【請求項３】
前記第1のピアデバイスは、前記HTMLリダイレクトに従うのではなく前記第1の認証応答を前記第2のピアデバイスに送信する、請求項2に記載の方法。
【請求項４】
前記ユーザの前記連合ログイン証明書および前記第1の識別子を前記第1の連合ログインプロバイダに送信する前に前記鍵交換を使用して前記第1のピアデバイスと前記第2のピアデバイスとの間にセキュアなセッションを確立するステップをさらに含む、請求項1に記載の方法。
【請求項５】
前記セキュアなセッションが、Diffie-Hellman鍵交換を使用して確立される、請求項4に記載の方法。
【請求項６】
前記第1の連合ログインプロバイダと前記第2の連合ログインプロバイダは異なる連合ログインプロバイダであり、前記第1の連合ログインプロバイダおよび前記第2の連合ログインプロバイダは、OpenIDプロバイダ、OAuthプロバイダ、またはFaceConnectプロバイダを含む、請求項1に記載の方法。
【請求項７】
前記第1の連合ログインプロバイダと前記第2の連合ログインプロバイダは同じ連合ログインプロバイダである、請求項1に記載の方法。
【請求項８】
前記第1のピアデバイスはコントローラピアデバイスを備え、前記第2のピアデバイスは被制御側デバイスを備える、請求項1に記載の方法。
【請求項９】
前記第1のピアデバイスによって、前記鍵交換に関する第1の公開鍵を生成するステップと、
前記第1のピアデバイスによって、前記第1の公開鍵を前記第2のピアデバイスに送信するステップと、
前記第1のピアデバイスによって、前記第2のピアデバイスから第2の公開鍵を受信するステップとを含む、請求項1に記載の方法。
【請求項１０】
前記第1の識別子は、前記第1の公開鍵、前記第1の公開鍵と前記第2の公開鍵との組合せ、前記第1の公開鍵と前記第2の公開鍵のハッシュ、または擬似ランダム関数(PRF)を使用して算出される前記第1の公開鍵と前記第2の公開鍵のベリファイアを含む、請求項9に記載の方法。
【請求項１１】
前記第1の識別子と前記第2の識別子は同じ識別子であり、前記第1の識別子と前記第2の識別子は、共通のハッシュまたは算出されたベリファイアを含む、請求項1に記載の方法。
【請求項１２】
前記第1の識別子と前記第2の識別子はそれぞれに異なる識別子であり、前記第1の識別子は、前記第1のピアデバイスによって生成される第1の公開鍵を含み、前記第2の識別子

は、前記第2のピアデバイスによって生成される第2の公開鍵を含む、請求項1に記載の方法。
【請求項１３】
前記第2のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するステップは、前記第2のピアデバイスからの前記肯定応答を受信するステップに基づいて前記鍵交換を認証するステップを含む、請求項1に記載の方法。
【請求項１４】
第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するための装置であって、
前記第1のピアデバイスによって、前記第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信するように構成された論理であって、前記第2のピアデバイスは、前記ユーザの前記連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する論理と、
前記第1のピアデバイスによって、前記第1の連合ログインプロバイダから第1の認証応答を受信するように構成された論理であって、前記第2のピアデバイスは、前記第2の連合ログインプロバイダから第2の認証応答を受信する論理と、
前記第1のピアデバイスによって、前記第2のピアデバイスから前記第2の認証応答を受信するように構成された論理と、
前記第1のピアデバイスによって、前記第2の連合ログインプロバイダによる前記第2の認証応答を認証するように構成された論理と、
前記第1のピアデバイスによって、前記第1の認証応答を前記第2のピアデバイスに送信するように構成された論理であって、前記第2のピアデバイスは、前記第1の連合ログインプロバイダによる前記第1の認証応答を認証する論理と、
前記第1のピアデバイスによって、前記第2のピアデバイスが前記第1の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスから受信するように構成された論理と、
前記第1のピアデバイスによって、前記第1のピアデバイスが前記第2の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスに送信するように構成された論理と、
前記第1のピアデバイスによって、前記第2のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するように構成された論理であって、前記第2のピアデバイスは、前記第1のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証する論理とを備える装置。
【請求項１５】
前記第1の認証応答を受信するように構成された前記論理は、前記第1の認証応答によるHTMLリダイレクトを受信するように構成された論理を含む、請求項14に記載の装置。
【請求項１６】
前記第1のピアデバイスは、前記HTMLリダイレクトに従うのではなく前記第1の認証応答を前記第2のピアデバイスに送信する、請求項15に記載の装置。
【請求項１７】
前記ユーザの前記連合ログイン証明書および前記第1の識別子が前記第1の連合ログインプロバイダに送信される前に前記鍵交換を使用して前記第1のピアデバイスと前記第2のピアデバイスとの間にセキュアなセッションを確立するように構成された論理をさらに備える、請求項14に記載の装置。
【請求項１８】
前記セキュアなセッションは、Diffie-Hellman鍵交換を使用して確立される、請求項17に記載の装置。
【請求項１９】
前記第1の連合ログインプロバイダと前記第2の連合ログインプロバイダは異なる連合ログインプロバイダであり、前記第1の連合ログインプロバイダおよび前記第2の連合ログインプロバイダは、OpenIDプロバイダ、OAuthプロバイダ、またはFaceConnectプロバイダを

含む、請求項14に記載の装置。
【請求項２０】
前記第1の連合ログインプロバイダと前記第2の連合ログインプロバイダは同じ連合ログインプロバイダである、請求項14に記載の装置。
【請求項２１】
前記第1のピアデバイスはコントローラピアデバイスを備え、前記第2のピアデバイスは被制御側デバイスを備える、請求項14に記載の装置。
【請求項２２】
前記第1のピアデバイスによって、前記鍵交換に関する第1の公開鍵を生成するように構成された論理と、
前記第1のピアデバイスによって、前記第1の公開鍵を第2のピアデバイスに送信するように構成された論理と、
前記第1のピアデバイスによって、前記第2のピアデバイスから第2の公開鍵を受信するように構成された論理とをさらに備える、請求項14に記載の装置。
【請求項２３】
前記第1の識別子は、前記第1の公開鍵、前記第1の公開鍵と前記第2の公開鍵との組合せ、前記第1の公開鍵と前記第2の公開鍵のハッシュ、または擬似ランダム関数(PRF)を使用して算出される前記第1の公開鍵と前記第2の公開鍵のベリファイアを含む、請求項22に記載の装置。
【請求項２４】
前記第1の識別子と前記第2の識別子は同じ識別子であり、前記第1の識別子と前記第2の識別子は、共通のハッシュまたは算出されたベリファイアを含む、請求項14に記載の装置。
【請求項２５】
前記第1の識別子と前記第2の識別子はそれぞれに異なる識別子であり、前記第1の識別子は、前記第1のピアデバイスによって生成される第1の公開鍵を含み、前記第2の識別子は、前記第2のピアデバイスによって生成される第2の公開鍵を含む、請求項14に記載の装置。
【請求項２６】
前記第2のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するように構成された前記論理は、前記第2のピアデバイスからの前記肯定応答の受信に基づいて前記鍵交換を認証するように構成された論理を備える、請求項14に記載の装置。
【請求項２７】
第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するための装置であって、
前記第1のピアデバイスによって、前記第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信するための手段であって、前記第2のピアデバイスは、前記ユーザの前記連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する手段と、
前記第1のピアデバイスによって、前記第1の連合ログインプロバイダから第1の認証応答を受信するための手段であって、前記第2のピアデバイスは、前記第2の連合ログインプロバイダから第2の認証応答を受信する手段と、
前記第1のピアデバイスによって、前記第2のピアデバイスから前記第2の認証応答を受信するための手段と、
前記第1のピアデバイスによって、前記第2の連合ログインプロバイダによる前記第2の認証応答を認証するための手段と、
前記第1のピアデバイスによって、前記第1の認証応答を前記第2のピアデバイスに送信するための手段であって、前記第2のピアデバイスは、前記第1の連合ログインプロバイダによる前記第1の認証応答を認証する手段と、
前記第1のピアデバイスによって、前記第2のピアデバイスが前記第1の認証応答を認証

したことを示す肯定応答を前記第2のピアデバイスから受信するための手段と、
前記第1のピアデバイスによって、前記第1のピアデバイスが前記第2の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスに送信するための手段と、
前記第1のピアデバイスによって、前記第2のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するための手段であって、前記第2のピアデバイスは、前記第1のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証する手段とを備える装置。
【請求項２８】
前記ユーザの前記連合ログイン証明書および前記第1の識別子を前記第1の連合ログインプロバイダに送信する前に前記鍵交換を使用して前記第1のピアデバイスと前記第2のピアデバイスとの間にセキュアなセッションを確立するための手段をさらに備える、請求項27に記載の装置。
【請求項２９】
第1のピアデバイスと第2のピアデバイスとの間の鍵交換を認証するための非一時的コンピュータ可読記憶媒体であって、
前記第1のピアデバイスによって、前記第1のピアデバイスのユーザの連合ログイン証明書および第1の識別子を第1の連合ログインプロバイダに送信するための少なくとも1つの命令であって、前記第2のピアデバイスは、前記ユーザの前記連合ログイン証明書および第2の識別子を第2の連合ログインプロバイダに送信する少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第1の連合ログインプロバイダから第1の認証応答を受信するための少なくとも1つの命令であって、前記第2のピアデバイスは、前記第2の連合ログインプロバイダから第2の認証応答を受信する少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第2のピアデバイスから前記第2の認証応答を受信するための少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第2の連合ログインプロバイダによる前記第2の認証応答を認証するための少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第1の認証応答を前記第2のピアデバイスに送信するための少なくとも1つの命令であって、前記第2のピアデバイスは、前記第1の連合ログインプロバイダによる前記第1の認証応答を認証する少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第2のピアデバイスが前記第1の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスから受信するための少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第1のピアデバイスが前記第2の認証応答を認証したことを示す肯定応答を前記第2のピアデバイスに送信するための少なくとも1つの命令と、
前記第1のピアデバイスによって、前記第2のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証するための少なくとも1つの命令であって、前記第2のピアデバイスは、前記第1のピアデバイスからの前記肯定応答に基づいて前記鍵交換を認証する少なくとも1つの命令とを含む非一時的コンピュータ可読記憶媒体。
【請求項３０】
前記ユーザの前記連合ログイン証明書および前記第1の識別子を前記第1の連合ログインプロバイダに送信する前に前記鍵交換を使用して前記第1のピアデバイスと前記第2のピアデバイスとの間にセキュアなセッションを確立するための少なくとも1つの命令をさらに含む、請求項29に記載の非一時的コンピュータ可読記憶媒体。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/019006

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L9/32 H04W12/06
ADD. H04W4/00

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)
H04L H04W

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, INSPEC, 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	MENEZES, VANSTONE, OORSCHOT: "Handbook of Applied Cryptography", 1997, CRC PRESS LLC, USA, XP001525013, pages 543-590, page 543 - page 590	1-30
A	EP 1 833 216 A1 (HITACHI LTD [JP]) 12 September 2007 (2007-09-12) abstract paragraph [0003] - paragraph [0011]	1-30
A	US 2011/314287 A1 (ESCOTT ADRIAN EDWARD [GB] ET AL) 22 December 2011 (2011-12-22) abstract paragraph [0008] - paragraph [0027]	1-30

☐ Further documents are listed in the continuation of Box C. ☒ 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
12 May 2015	20/05/2015

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	San Millán Maeso, J

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/019006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1833216 A1	12-09-2007	NONE	
US 2011314287 A1	22-12-2011	AR 081944 A1	31-10-2012
		AU 2011268205 A1	20-12-2012
		CA 2800941 A1	22-12-2011
		CN 102934470 A	13-02-2013
		EP 2583479 A1	24-04-2013
		JP 2013534754 A	05-09-2013
		KR 20130029103 A	21-03-2013
		RU 2013101768 A	27-07-2014
		SG 185662 A1	28-12-2012
		TW 201220793 A	16-05-2012
		UA 106299 C2	11-08-2014
		US 2011314287 A1	22-12-2011
		WO 2011159952 A1	22-12-2011

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

（特許庁注：以下のものは登録商標）
１．ＦＩＲＥＷＩＲＥ
２．ＡＮＤＲＯＩＤ

(72)発明者 キャメロン・アレン・ジョージ・マクドナルド
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５・クアルコム・インコーポレイテッド
(72)発明者 グレゴリー・バーンズ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５・クアルコム・インコーポレイテッド

Ｆターム(参考) 5J104 AA07 AA16 EA02 EA04 EA16 KA02 KA03 NA02 NA12 NA37
NA38 PA09