(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2017-535097
(P2017-535097A)
(43)公表日　平成29年11月24日(2017.11.24)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
H04M 11/00	(2006.01)	H04L	9/00	601F	5K067
H04W 12/04	(2009.01)	H04M	11/00	302	5K201
G06F 21/44	(2013.01)	H04W	12/04		
		G06F	21/44		

審査請求 未請求　予備審査請求 有　（全 30 頁）

(21)出願番号　特願2017-509628 (P2017-509628)
(86)(22)出願日　平成27年8月12日 (2015.8.12)
(85)翻訳文提出日　平成29年4月17日 (2017.4.17)
(86)国際出願番号　PCT/US2015/044894
(87)国際公開番号　WO2016/028572
(87)国際公開日　平成28年2月25日 (2016.2.25)
(31)優先権主張番号　14/463,276
(32)優先日　平成26年8月19日 (2014.8.19)
(33)優先権主張国　米国 (US)

(71)出願人　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100158805
弁理士　井関　守三
(74)代理人　100112807
弁理士　岡田　貴志

最終頁に続く

(54)【発明の名称】ポイントオブセールデバイスを使用したネットワークアクセス認証

(57)【要約】
ユーザデバイス（１０２）は、ネットワークアクセスのために、例えばゲストネットワークアクセスのために、構成されることができる。一例では、第１のデバイス（１０４）は、第１のデバイス（１０２）を使用する取引の指示を受信する。第１のデバイス（１０２）は、取引の指示を受信することに応答して、ネットワークアクセスを求める要求をネットワークのアクセスポイント（１０６）に通信する。第１のデバイス（１０４）は次いで、アクセスポイント（１０６）から第１のキーを受信する。第１のデバイス（１０４）は、第１のキーをユーザデバイス（１０２）に提供する。ユーザデバイス（１０２）は、ネットワークへのネットワークアクセスを取得するために、第１のキーを使用することになる。

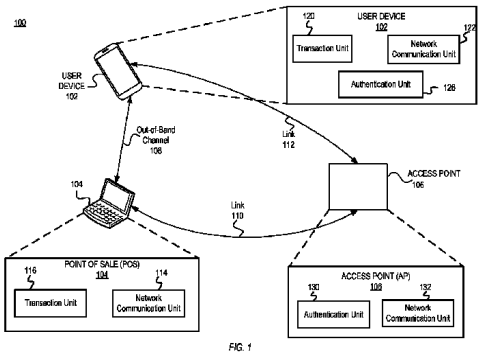

FIG. 1

【特許請求の範囲】
【請求項１】
ネットワークアクセスのための方法であって、
ネットワークの第１のデバイスにおいて、前記第１のデバイスを使用する取引の指示を受信することと、
前記取引の前記指示を受信することに応答して、ネットワークアクセスを求める要求を前記ネットワークのアクセスポイントに通信することと、
前記アクセスポイントから第１のキーを受信することと、
前記第１のキーをユーザデバイスに提供することと、
を備え、
ここにおいて、前記ユーザデバイスは、前記ネットワークアクセスを取得するために前記第１のキーを使用することになる、
方法。
【請求項２】
前記ユーザデバイスは、前記第１のキーに少なくとも部分的に基づいて第２のキーを生成するために、前記アクセスポイントと通信することになり、
前記ユーザデバイスはさらに、前記第２のキーにさらに基づいて前記ネットワークへのアクセスを取得するために、前記アクセスポイントと通信することになる、
請求項１に記載の方法。
【請求項３】
前記第１のキーは非対称キーであり、
前記第２のキーは対称キーである、
請求項２に記載の方法。
【請求項４】
前記第２のキーは、
ペアワイズマスターキー（ＰＭＫ）、
ペアワイズ一時キー（ＰＴＫ）、または、
事前共有キー（ＰＳＫ）
のうちの１つを備える、請求項２に記載の方法。
【請求項５】
前記第１のキーは、帯域外（ＯＯＢ）チャネルを使用して前記ユーザデバイスに提供される、請求項１に記載の方法。
【請求項６】
前記ＯＯＢチャネルは、
光チャネル、
近距離無線通信（ＮＦＣ）チャネル、
セルラチャネル、および、
Ｂｌｕｅｔｏｏｔｈチャネル、
から成るグループのうちの少なくとも１つのメンバを備える、請求項５に記載の方法。
【請求項７】
前記アクセスポイントは、前記第１のキーおよび第２のキーを含む第１のキーのペアを生成することになり、
前記第１のキーは公開キーであり、前記第２のキーは秘密キーであり、
前記ユーザデバイスは、第３のキーおよび第４のキーを備える第２のキーのペアを生成することになり、
前記第３のキーは公開キーであり、前記第４のキーは秘密キーであり、
前記ユーザデバイスは、前記第１のキーのペアおよび前記第２のキーのペアに基づいて、前記ネットワークアクセスを取得するために、前記アクセスポイントと通信することになる、
請求項１に記載の方法。

【請求項８】
前記取引は、前記ユーザデバイスと前記第１のデバイスとの間のものである、請求項１に記載の方法。
【請求項９】
前記第１のキーが前記ユーザデバイスに提供されるとき、前記アクセスポイントによって生成された前記第１のキーのフォーマットが維持される、
請求項１に記載の方法。
【請求項１０】
前記アクセスポイントは、前記ネットワークアクセスを求める前記要求を受信することに応答して、前記第１のキーを生成することになり、
前記第１のキーは対称キーである、
請求項１に記載の方法。
【請求項１１】
前記ユーザデバイスはさらに、前記第１のキーに少なくとも部分的に基づいて前記ネットワークアクセスを取得するために、前記アクセスポイントと通信することになる、請求項１に記載の方法。
【請求項１２】
コンピューティングデバイスであって、
プロセッサと、
プログラム命令を記憶したメモリと、
を備え、
前記プログラム命令は、前記コンピューティングデバイスに、
前記コンピューティングデバイスを使用する取引の指示を受信することと、
前記取引の前記指示を受信することに応答して、ネットワークアクセスを求める要求をネットワークのアクセスポイントに通信することと、
前記アクセスポイントから第１のキーを受信することと、
前記第１のキーをユーザデバイスに提供することと、
を行わせるように前記プロセッサによって実行可能であり、
ここにおいて、前記ユーザデバイスは、前記ネットワークアクセスを取得するために前記第１のキーを使用することになる、
コンピューティングデバイス。
【請求項１３】
前記ユーザデバイスは、前記第１のキーに少なくとも部分的に基づいて第２のキーを生成するために、前記アクセスポイントと通信することになり、
前記ユーザデバイスはさらに、前記第２のキーにさらに基づいて前記ネットワークへのアクセスを取得するために、前記アクセスポイントと通信することになる、
請求項１２に記載のコンピューティングデバイス。
【請求項１４】
前記第１のキーは非対称キーであり、
前記第２のキーは対称キーである、
請求項１３に記載のコンピューティングデバイス。
【請求項１５】
前記第２のキーは、
ペアワイズマスターキー（ＰＭＫ）、
ペアワイズ一時キー（ＰＴＫ）、または、
事前共有キー（ＰＳＫ）
のうちの１つを備える、請求項１３に記載のコンピューティングデバイス。
【請求項１６】
前記第１のキーは、帯域外（ＯＯＢ）チャネルを使用して前記ユーザデバイスに提供される、請求項１２に記載のコンピューティングデバイス。

【請求項１７】
前記アクセスポイントは、前記第１のキーおよび第２のキーを含む第１のキーのペアを生成することになり、
前記第１のキーは公開キーであり、前記第２のキーは秘密キーであり、
前記ユーザデバイスは、第３のキーおよび第４のキーを備える第２のキーのペアを生成することになり、
前記第３のキーは公開キーであり、前記第４のキーは秘密キーであり、
前記ユーザデバイスは、前記第１のキーのペアおよび前記第２のキーのペアに基づいて、前記ネットワークアクセスを取得するために、前記アクセスポイントと通信することになる、
請求項１２に記載のコンピューティングデバイス。
【請求項１８】
前記取引は、前記ユーザデバイスと前記第１のデバイスとの間のものである、請求項１２に記載のコンピューティングデバイス。
【請求項１９】
前記第１のキーが前記ユーザデバイスに提供されるとき、前記アクセスポイントによって生成された前記第１のキーのフォーマットが維持される、
請求項１２に記載のコンピューティングデバイス。
【請求項２０】
前記アクセスポイントは、前記ネットワークアクセスを求める前記要求を受信することに応答して、前記第１のキーを生成することになり、
前記第１のキーは対称キーである、
請求項１２に記載のコンピューティングデバイス。
【請求項２１】
ネットワークアクセスのための方法であって、
ネットワークの第１のデバイスによって、ネットワークアクセスを求める要求を前記ネットワークのアクセスポイントに通信することと、
前記第１のデバイスにおいて、前記アクセスポイントから第１のキーを受信することと、
ユーザデバイスとの支払取引を処理することと、
ここにおいて、前記支払取引を処理することは、
前記第１のキーを前記ユーザデバイスに提供することと、
前記ユーザデバイスから第２のキーを受信することと、
を備え、
前記ユーザデバイスは、前記ネットワークアクセスを取得するために、前記第１のキーを使用することになり、
前記第２のキーを前記アクセスポイントに提供することと、
を備える、方法。
【請求項２２】
前記ユーザデバイスは、前記第１のキーおよび前記第２のキーに少なくとも部分的に基づいて第３のキーを生成するために、前記アクセスポイントと通信することになり、
前記ユーザデバイスはさらに、前記第３のキーにさらに基づいて前記ネットワークアクセスを取得するために、前記アクセスポイントと通信することになる、
請求項２１に記載の方法。
【請求項２３】
前記支払取引を処理することはさらに、前記ユーザデバイスから支払データを受信することを備える、
請求項２１に記載の方法。
【請求項２４】
前記アクセスポイントは、前記支払取引の処理より前に、前記第１のキーを生成するこ

とになる、
請求項２１に記載の方法。
【請求項２５】
前記第１のキーは、帯域外（ＯＯＢ）チャネルを使用して前記ユーザデバイスに提供される、請求項２２に記載の方法。
【請求項２６】
コンピューティングデバイスであって、
プロセッサと、
プログラム命令を記憶したメモリと、
を備え、
前記プログラム命令は、前記コンピューティングデバイスに、
ネットワークアクセスを求める要求をネットワークのアクセスポイントに通信することと、
前記アクセスポイントから第１のキーを受信することと、
ユーザデバイスとの支払取引を処理することと、
ここにおいて、前記支払取引を処理することは、
前記第１のキーを前記ユーザデバイスに提供することと、
前記ユーザデバイスから第２のキーを受信することと、
を備え、
前記ユーザデバイスは、前記ネットワークアクセスを取得するために、前記第１のキーを使用することになり、
前記第２のキーを前記アクセスポイントに提供することと、
を行わせるように前記プロセッサによって実行可能である、コンピューティングデバイス。
【請求項２７】
前記ユーザデバイスは、前記第１のキーおよび前記第２のキーに少なくとも部分的に基づいて第３のキーを生成するために、前記アクセスポイントと通信することになり、
前記ユーザデバイスはさらに、前記第３のキーにさらに基づいて前記ネットワークアクセスを取得するために、前記アクセスポイントと通信することになる、
請求項２６に記載のコンピューティングデバイス。
【請求項２８】
前記支払取引を処理することはさらに、前記ユーザデバイスから支払データを受信することを備える、
請求項２６に記載のコンピューティングデバイス。
【請求項２９】
前記第１のキーは、帯域外（ＯＯＢ）チャネルを使用して前記ユーザデバイスに提供される、請求項２６に記載のコンピューティングデバイス。
【請求項３０】
前記アクセスポイントは、前記支払取引の処理より前に、前記第１のキーを生成することになる、
請求項２６に記載のコンピューティングデバイス。
【発明の詳細な説明】
【関連出願】
【０００１】
[0001] 本出願は、２０１４年８月１９日に出願された米国出願第１４／４６３，２７６号の優先権利益を主張する。
【背景技術】
【０００２】
[0002] 本開示の実施形態は、一般に、通信システムの分野に関し、より具体的には、通信ネットワーク内で使用するために通信デバイスを構成することに関する。

【０００３】
[0003] ユーザは時に、インターネットおよび他のネットワークリソースへのアクセスを得るために、コンピューティングデバイスをゲストネットワークへ接続することを望み得る。ゲストネットワークへ接続するために、ユーザは、ユーザのコンピューティングデバイスに、ゲストネットワークのアクセスポイント（ＡＰ）を通して利用可能なネットワークリソースへのアクセスを得させるための認証プロシージャに参加し得る。１つの認証プロシージャは、ユーザが、ユーザのコンピューティングデバイスにパスフレーズを入力することを含む。しかしながら、ユーザがコンピューティングデバイスにパスフレーズを入力することは、大抵は厄介である。さらに、ユーザは、パスフレーズを他者と共有することができ、そのことでパスフレーズは、より安全でなくなる。

【０００４】
[0004] 別の認証プロシージャは、ユーザのコンピューティングデバイス上のブラウザを、認証のためのキャプティブポータル（a captive portal）にリダイレクトすることを含む。しかしながら、このプロシージャは、認証処理より前にブラウザにロードされているウェブページに関する未定義の挙動をもたらす可能性がある。この未定義の挙動を避けるために、ユーザは典型的には、ブラウザ上でキャプティブポータルをロードするために、認証プロシージャの間に忘れずにブラウザをリフレッシュまたはリスタートしなければならない。加えて、キャプティブポータルは、パケットスニファで悪用される可能性がある（exploited with a packet sniffer）。上述された認証プロシージャの両方は、ユーザ認証のためにパスワードに頼る。これらのパスワードは、典型的には弱く、悪意のパーティ（a hostile party）によって推測される可能性がある。一旦パスワードが知られると、悪意のパーティは、正当なＡＰに成りすます不正なＡＰ（a rogue AP）をセットアップすることができ、それによりユーザへのセキュリティ脅威がもたらされる。

【発明の概要】
【０００５】
[0005] ネットワークアクセスのために、例えばゲストネットワークアクセスのために、ユーザデバイスを構成する様々な実施形態が開示される。一実施形態では、第１のデバイスは、第１のデバイスを使用する取引の指示を受信する。第１のデバイスは、取引の指示を受信することに応答して、ネットワークアクセスを求める要求をネットワークのアクセスポイントに通信する。第１のデバイスは次いで、アクセスポイントから第１のキーを受信する。第１のデバイスは、第１のキーをユーザデバイスに提供する。ユーザデバイスは、ネットワークへのネットワークアクセスを取得するために、第１のキーを使用することになる。

【０００６】
[0006] 別の実施形態では、ネットワークの第１のデバイスは、ネットワークアクセスを求める要求をネットワークのアクセスポイントに通信する。第１のデバイスは、アクセスポイントから第１のキーを受信する。第１のデバイスは、第１のキーをユーザデバイスに提供すること、およびユーザデバイスから第２のキーを受信することを含む、ユーザデバイスとの支払取引を処理する。ユーザデバイスは、ネットワークへのネットワークアクセスを取得するために、第１のキーを使用することになる。第１のデバイスは、第２のキーをアクセスポイントに提供する。

【０００７】
[0007] いくつかの実施形態では、ネットワークアクセスのための方法は、ネットワークの第１のデバイスにおいて、第１のデバイスを使用する取引の指示を受信することと、取引の指示を受信することに応答して、ネットワークアクセスを求める要求をネットワークのアクセスポイントに通信することと、アクセスポイントから第１のキーを受信することと、第１のキーをユーザデバイスに提供することと、を備え、ここにおいて、ユーザデバイスは、ネットワークアクセスを取得するために、第１のキーを使用することになる。

【０００８】
[0008] いくつかの実施形態では、ユーザデバイスは、第１のキーに少なくとも部分的

に基づいて第２のキーを生成するために、アクセスポイントと通信することになり、ユーザデバイスはさらに、第２のキーにさらに基づいてネットワークへのアクセスを取得するために、アクセスポイントと通信することになる。

【０００９】

[0009] いくつかの実施形態では、第１のキーは非対称キーであり、第２のキーは対称キーである。

【００１０】

[0010] いくつかの実施形態では、第２のキーは、ペアワイズマスターキー（ＰＭＫ：pairwise master key）、ペアワイズ一時キー（ＰＴＫ：pairwise transient key）、または事前共有キー（ＰＳＫ：pre-shared key）のうちの１つを備える。

【００１１】

[0011] いくつかの実施形態では、第１のキーは、帯域外（ＯＯＢ：out-of-band）チャネルを使用してユーザデバイスに提供される。

【００１２】

[0012] いくつかの実施形態では、ＯＯＢチャネルは、光チャネル、近距離無線通信（ＮＦＣ：Near Field Communication）チャネル、セルラチャネル、およびＢｌｕｅｔｏｏｔｈ（登録商標）チャネルから成るグループのうちの少なくとも１つのメンバを備える。

【００１３】

[0013] いくつかの実施形態では、アクセスポイントは、第１のキーおよび第２のキーを含む第１のキーのペアを生成することになり、ここで、第１のキーは公開キーであり、第２のキーは秘密キー（a private key）であり、ユーザデバイスは、第３のキーおよび第４のキーを備える第２のキーのペアを生成することになり、ここで、第３のキーは公開キーであり、第４のキーは秘密キーであり、ユーザデバイスは、第１のキーのペアおよび第２のキーのペアに基づいてネットワークアクセスを取得するために、アクセスポイントと通信することになる。

【００１４】

[0014] いくつかの実施形態では、取引は、ユーザデバイスと第１のデバイスとの間のものである。

【００１５】

[0015] いくつかの実施形態では、第１のキーがユーザデバイスに提供されるとき、アクセスポイントによって生成された第１のキーのフォーマットが維持される。

【００１６】

[0016] いくつかの実施形態では、アクセスポイントは、ネットワークアクセスを求める要求を受信することに応答して、第１のキーを生成することになり、第１のキーは対称キーである。

【００１７】

[0017] いくつかの実施形態では、ユーザデバイスはさらに、第１のキーに少なくとも部分的に基づいてネットワークアクセスを取得するために、アクセスポイントと通信することになる。

【００１８】

[0018] いくつかの実施形態では、コンピューティングデバイスは、プロセッサと、プログラム命令を記憶したメモリとを備え、プログラム命令は、コンピューティングデバイスに、コンピューティングデバイスを使用する取引の指示を受信することと、取引の指示を受信することに応答して、ネットワークアクセスを求める要求をネットワークのアクセスポイントに通信することと、アクセスポイントから第１のキーを受信することと、第１のキーをユーザデバイスに提供することと、を行わせるようにプロセッサによって実行可能であり、ここにおいて、ユーザデバイスは、ネットワークアクセスを取得するために、第１のキーを使用することになる。

【００１９】

[0019] いくつかの実施形態では、ユーザデバイスは、第１のキーに少なくとも部分的

に基づいて第２のキーを生成するために、アクセスポイントと通信することになり、ユーザデバイスはさらに、第２のキーにさらに基づいてネットワークへのアクセスを取得するために、アクセスポイントと通信することになる。

【００２０】

[0020] いくつかの実施形態では、第１のキーは非対称キーであり、第２のキーは対称キーである。

【００２１】

[0021] いくつかの実施形態では、第２のキーは、ペアワイズマスターキー（ＰＭＫ）、ペアワイズ一時キー（ＰＴＫ）、または事前共有キー（ＰＳＫ）のうちの１つを備える。

【００２２】

[0022] いくつかの実施形態では、第１のキーは、帯域外（ＯＯＢ）チャネルを使用してユーザデバイスに提供される。

【００２３】

[0023] いくつかの実施形態では、アクセスポイントは、第１のキーおよび第２のキーを含む第１のキーのペアを生成することになり、ここで、第１のキーは公開キーであり、第２のキーは秘密キーであり、ユーザデバイスは、第３のキーおよび第４のキーを備える第２のキーのペアを生成することになり、ここで、第３のキーは公開キーであり、第４のキーは秘密キーであり、ユーザデバイスは、第１のキーのペアおよび第２のキーのペアに基づいてネットワークアクセスを取得するために、アクセスポイントと通信することになる。

【００２４】

[0024] いくつかの実施形態では、取引は、ユーザデバイスと第１のデバイスとの間のものである。

【００２５】

[0025] いくつかの実施形態では、第１のキーがユーザデバイスに提供されるとき、アクセスポイントによって生成された第１のキーのフォーマットが維持される。

【００２６】

[0026] いくつかの実施形態では、アクセスポイントは、ネットワークアクセスを求める要求を受信することに応答して、第１のキーを生成することになり、第１のキーは対称キーである。

【００２７】

[0027] いくつかの実施形態では、ネットワークアクセスのための方法は、ネットワークの第１のデバイスによって、ネットワークアクセスを求める要求をネットワークのアクセスポイントに通信することと、第１のデバイスにおいて、アクセスポイントから第１のキーを受信することと、ユーザデバイスとの支払取引を処理すること、ここで、支払取引を処理することは第１のキーをユーザデバイスに提供することおよびユーザデバイスから第２のキーを受信することを備え、ユーザデバイスはネットワークアクセスを取得するために第１のキーを使用することになる、と、第２のキーをアクセスポイントに提供することと、を備える。

【００２８】

[0028] いくつかの実施形態では、ユーザデバイスは、第１のキーおよび第２のキーに少なくとも部分的に基づいて第３のキーを生成するために、アクセスポイントと通信することになり、ユーザデバイスはさらに、第３のキーにさらに基づいてネットワークアクセスを取得するために、アクセスポイントと通信することになる。

【００２９】

[0029] いくつかの実施形態では、支払取引を処理することはさらに、ユーザデバイスから支払データを受信することを備える。

【００３０】

[0030] いくつかの実施形態では、アクセスポイントは、支払取引の処理より前に第１

のキーを生成することになる。
【００３１】
[0031] いくつかの実施形態では、第１のキーは、帯域外（ＯＯＢ）チャネルを使用してユーザデバイスに提供される。
【００３２】
[0032] いくつかの実施形態では、コンピューティングデバイスは、プロセッサと、プログラム命令を記憶したメモリとを備え、プログラム命令は、コンピューティングデバイスに、ネットワークアクセスを求める要求をネットワークのアクセスポイントに通信することと、アクセスポイントから第１のキーを受信することと、ユーザデバイスとの支払取引を処理すること、ここで、支払取引を処理することは第１のキーをユーザデバイスに提供することおよびユーザデバイスから第２のキーを受信することを備え、ユーザデバイスはネットワークアクセスを取得するために第１のキーを使用することになる、と、第２のキーをアクセスポイントに提供することと、を行わせるようにプロセッサによって実行可能である。
【００３３】
[0033] いくつかの実施形態では、ユーザデバイスは、第１のキーおよび第２のキーに少なくとも部分的に基づいて第３のキーを生成するために、アクセスポイントと通信することになり、ユーザデバイスはさらに、第３のキーにさらに基づいてネットワークアクセスを取得するために、アクセスポイントと通信することになる。
【００３４】
[0034] いくつかの実施形態では、支払取引を処理することはさらに、ユーザデバイスから支払データを受信することを備える。
【００３５】
[0035] いくつかの実施形態では、第１のキーは、帯域外（ＯＯＢ）チャネルを使用してユーザデバイスに提供される。
【００３６】
[0036] いくつかの実施形態では、アクセスポイントは、支払取引の処理より前に第１のキーを生成することになる。
【図面の簡単な説明】
【００３７】
[0037] 添付の図面を参照することによって、本願の実施形態はさらに理解され得、また数多くのオブジェクト、特徴および利点が当業者に明らかとなり得る。
【図１】[0038] 図１は、ネットワークアクセスのためにデバイスを構成するための例示的なシステムの図である。
【図２】[0039] 図２は、例示的なネットワークアクセス認証処理を例示するフローダイアグラムを示す。
【図３】図３は、例示的なネットワークアクセス認証処理を例示するフローダイアグラムを示す。
【図４】[0040] 図４は、ネットワークアクセス認証処理の動作の実施形態を例示する図である。
【図５】[0041] 図５は、ネットワークアクセス認証処理の動作の別の実施形態を例示する図である。
【図６】[0042] 図６は、ネットワークアクセス認証処理の動作の別の実施形態を例示する図である。
【図７】[0043] 図７は、ネットワーク通信のためのインタフェースを含む電子デバイスの例示的な実施形態のブロック図である。
【発明を実施するための形態】
【００３８】
[0044] 以下の説明は、本開示の技法を具現化する例示的なシステム、方法、技法、命令シーケンス、およびコンピュータプログラム製品を含む。しかしながら、説明される実

施形態は、これらの特定の詳細なしに実行され得ることは理解される。例えば、いくつかの例は８０２．１１通信プロトコルを使用してワイヤレスローカルエリアネットワーク（ＷＬＡＮ）へのネットワークアクセスを取得することに言及するが、他の実施形態では、ここに説明されたネットワークアクセス動作は、他の好適な通信プロトコル（例えば、イーサネット（登録商標）、電力線通信（ＰＬＣ）、ロングタームエボリューション（ＬＴＥ（登録商標））、３Ｇ、４Ｇ等）をインプリメントする（implement）他のタイプのネットワークへのネットワークアクセスを取得するために実行されることができる。他の事例では、周知の命令インスタンス、プロトコル、構造および技法は、本説明を不明瞭にしないために、詳細には示されていない。

【００３９】

[0045] ポイントオブセール（ＰＯＳ：Point-of-Sale）デバイスは、アクセスポイント（ＡＰ）とユーザデバイス（例えば、スマートフォン）との間のネットワークアクセス認証処理を容易にするために使用されることができる。ＰＯＳデバイスは、ＡＰとユーザデバイスとの間で１つまたは複数のキーを交換するために使用されることができる。以下に説明されるように、これらのキーは、ユーザデバイスを認証するためのネットワークアクセス認証処理の間に使用されることができる。ユーザデバイスが認証されると、ネットワークアクセス（例えば、ゲストネットワークアクセス）が、認証されたユーザデバイスに提供されることができる。例えば、ネットワークアクセスは、ワイヤレスネットワーク（例えば、ＷＬＡＮ）またはワイヤード（wired）ネットワーク（例えば、イーサネットまたは電力線）を介して提供されることができる。

【００４０】

[0046] 一実施形態では、ＰＯＳデバイスは、例えば、商品またはサービスの購入のための顧客と商人（a merchant）との間の取引を処理することができる。取引の指示を受信すると、ＰＯＳデバイスは、ＡＰからネットワークアクセス（例えば、ゲストネットワークアクセス）を要求することができる。ＡＰは、ＡＰキーのペアを生成し、ＰＯＳデバイスにＡＰキーのペアのうちの公開キーを提供することができる。ＰＯＳデバイスは、帯域外（ＯＯＢ）チャネル上で、受信された公開キーをユーザデバイスに提供することができる。一旦ユーザデバイスがＡＰ公開キーを受信すると、ユーザデバイスおよびＡＰは、ＡＰキーのペアに基づいて、キー確立処理を開始することができる。キー確立処理は、安全キー（例えば、ペアワイズマスターキー（ＰＭＫ））を生成するために使用されることができる。安全キーは、ネットワークセキュリティ処理の間にユーザデバイスを認証するために使用されることができる。このように、ユーザデバイスは、厄介かつ安全でない（cumbersome and unsecure）パスフレーズを使用することなく、そして信用できないおよび不安定な（unreliable and unstable）キャプティブポータルを使用することなく、ネットワークアクセスのために認証されることができる。

【００４１】

[0047] 一実施形態では、顧客と商人（またはサービスプロバイダ）との間の取引は、ユーザデバイスのためのネットワークアクセス認証をトリガすることができる。別の実施形態では、ユーザデバイスは、顧客と商人との間の取引の間にネットワークアクセスのために構成されることができる。商人は典型的に、取引を処理するためにポイントオブセール（ＰＯＳ）デバイスを使用する。顧客は典型的に、ユーザデバイスを有し、それは、ＰＯＳデバイスを用いて取引を完了するために使用され得る。さらに、実施形態は、ゲストネットワークアクセスに限定されない。用途に応じて、ユーザデバイスは、別のタイプのネットワークアクセス、例えば、フルネットワークアクセス、管理者ネットワークアクセス、一時的なネットワークアクセス（a temporary network access）、契約者ネットワークアクセス等を提供されることができる。上述のネットワークアクセス認証処理の様々な態様はさらに、以下で説明される。

【００４２】

[0048] 図１は、いくつかの実施形態にしたがって、ネットワークアクセスのためにデバイスを構成するためのシステム１００の図である。図１に示されたシステム１００にお

いて、ユーザデバイス１０２は、ポイントオブセール（ＰＯＳ）デバイス１０４との顧客取引に関与することができる。ユーザデバイス１０２は、取引ユニット１２０、ネットワーク通信ユニット１２２、および認証ユニット１２６を含む。ＰＯＳデバイス１０４は、ネットワーク通信ユニット１１４、および取引ユニット１１６を含む。アクセスポイント（ＡＰ）１０６は、ネットワークアクセス（例えば、ゲストネットワークアクセス）をユーザデバイス１０２に提供するように構成される。ＡＰ１０６は、認証ユニット１３０およびネットワーク通信ユニット１３２を含む。デバイス１０２、１０４、および／または１０６の各々の１つまたは複数のユニットは、図７を参照して以下に説明されるようなソフトウェアおよび／またはハードウェアを使用してインプリメントされることができることに留意されたい。例えば、デバイス（例えば、デバイス１０４）のプロセッサは、ユニット（例えば、取引ユニット１１６）のうちの１つまたは複数に関連する機能性（functionality）をインプリメントするために、デバイスのメモリに記憶された命令を実行し得る。

【００４３】

[0049] ユーザデバイス１０２は、通信ネットワークを通してデータを転送することができる、如何なる技術的に実現可能な（technically feasible）電子デバイスの形もとることができる。例えば、ユーザデバイス１０２は、ユーザによってトランスポートされることができる、スマートフォン、ラップトップ、ネットブック、タブレットコンピュータ、スマートウォッチ、および同様のもののような、モバイルデバイスであることができる。ＰＯＳデバイス１０４は、専用商人コンピュータであり、ＡＰ１０６は、専用ＡＰであることができる。また、ＰＯＳデバイス１０４および／またはＡＰ１０６は、スマートフォン、ラップトップ、ネットブック、タブレットコンピュータ、スマート電気機器（appliance）、および同様のもののような電子デバイスを使用してインプリメントされることができる。

【００４４】

[0050] ＰＯＳデバイス１０４は、リンク１１０を介してＡＰ１０６に通信可能に結合される。ＰＯＳデバイス１０４のネットワーク通信ユニット１１４は、リンク１１０を介してＡＰ１０６のネットワーク通信ユニット１３２と通信することによって、ネットワークアクセス認証処理の一部を容易にすることができる。例えば、ＰＯＳデバイス１０４は、ネットワークアクセスを要求するためにＡＰ１０６と通信し、ＡＰ１０６の認証ユニット１３０にキーを生成させることができる。ユーザデバイス１０２は、リンク１１２を介してＡＰ１０６とのネットワークアクセス認証処理の別の部分を実行することができる。例えば、ユーザデバイス１０２は、リンク１１２を介して認証ユニット１３０とのネットワークセキュリティ処理および／またはキー確立処理を実行するために、認証ユニット１２６を使用することができる。リンク１１０および１１２は、ＩＥＥＥ８０２．１１、ロングタームエボリューション（ＬＴＥ）、３Ｇ、４Ｇ等のようなワイヤレスネットワークを使用してインプリメントされることができる。リンク１１０および１１２はまた、イーサネットまたは電力線等のようなワイヤードネットワーキング技術を使用してインプリメントされることができる。

【００４５】

[0051] ネットワーク通信ユニット１１４、１２２、および１３２の各々は、ＺｉｇＢｅｅ（登録商標）、ＩＥＥＥ８０２．１１、および／またはＢｌｕｅｔｏｏｔｈ（登録商標）プロトコルをインプリメントするワイヤレスインタフェースを含むことができる。いくつかの実施形態では、ネットワーク通信ユニット１１４、１２２、および１３２はまた、イーサネットプロトコルおよび／または電力線通信（ＰＬＣ）プロトコル（例えば、ＨｏｍｅＰｌｕｇ（登録商標）規格によって説明されるプロトコルのような）をインプリメントするワイヤードインタフェースを含み得る。いくつかの実施形態では、ネットワーク通信ユニット１１４、ネットワーク通信ユニット１３２、およびネットワーク通信ユニット１２２は、１つまたは複数の無線トランシーバ、アナログフロントエンド（ＡＦＥ：analog front end）ユニット、アンテナ、プロセッサ、メモリ、他の論理、および／または

通信プロトコルおよび関連する機能性をインプリメントするための他のコンポーネントを含むことができる。

【００４６】

[0052] ユーザデバイス１０２は、帯域外（ＯＯＢ）チャネル１０８を介してＰＯＳデバイス１０４の取引ユニット１１６と通信するために、取引ユニット１２０を使用することができる。例えば、システム１００内のデバイスが、通信のためにＩＥＥＥ８０２．１１プロトコルをインプリメントする場合、取引ユニット１２０は、Ｂｌｕｅｔｏｏｔｈプロトコル（すなわち、Ｂｌｕｅｔｏｏｔｈチャネル）、近距離無線通信（ＮＦＣ（登録商標）：Near Field Communication）プロトコル（すなわち、ＮＦＣチャネル）、赤外線プロトコル（すなわち、赤外線チャネル）等を使用して、ＯＯＢチャネル１０８を介して取引ユニット１１６と通信することができる。ＰＯＳデバイス１０４の取引ユニット１１６はまた、例えばＰＯＳデバイス１０４のディスプレイ上に表示されるイメージまたは紙のレシートを使用するなどして、光チャネルを使用して、情報（例えば、（１つまたは複数の）キー）を、ＯＯＢチャネル１０８を介してユーザデバイス１０２の取引ユニット１２０に提供することができる。取引ユニット１１６はまた、ＰＯＳデバイス１０４のディスプレイあるいはその同等物上にＱＲコード（登録商標）またはバーコードを表示することによって、ＱＲコードまたはバーコードを使用して、例えば、紙のレシート上に情報をプリントすることができる。取引ユニット１１６はまた、電子メール、ショートメッセージングサービス（ＳＭＳ）、および／またはマルチメディアメッセージングサービス（ＭＭＳ）を介するなどして、セルラチャネルを使用して、ＯＯＢチャネル１０８を介して取引ユニット１２０に情報を提供することができる。電子メールはまた、Ｂｌｕｅｔｏｏｔｈチャネルを使用するなどして、異なるチャネルを使用して送信されることもできることに留意されたい。

【００４７】

[0053] ＰＯＳデバイス１０４は、顧客と商人との間の顧客取引を処理することができる。顧客取引は、ＰＯＳデバイス１０４を使用した商人からの商品またはサービスの顧客購入を含むことができる。顧客取引は、ユーザデバイス１０２を使用して、またはユーザデバイス１０２を使用することなく、実行されることができる。いくつかの例では、顧客取引は、例えば、ＰＯＳデバイス１０４への支払を手動で提供する顧客などによって、ＰＯＳデバイス１０４を使用するがユーザデバイス１０２を使用せずに、実行されることができる。いくつかの例では、顧客取引はまた、支払取引を含むことができ、例えば、ここで、ユーザデバイス１０２は、ＯＯＢチャネル１０８を介して商品またはサービスの代金を払うために使用される。顧客取引は、データ（例えば、顧客のコンタクトおよび／または支払データ）を転送すること、および／またはユーザデバイス１０２とＰＯＳデバイス１０４との間でファイルすること（files between）を含むことができる。

【００４８】

[0054] ＰＯＳデバイス１０４は、顧客取引の指示を受信することができる。指示は、ユーザデバイス１０２によって（例えば、取引ユニット１２０によって）生成されることができ、ＰＯＳデバイス１０４に（例えば、ＯＯＢチャネル１０８上で）通信されることができる。指示は、メッセージ、通知、制御パケット等としてインプリメントされることができる。いくつかのインプリメンテーション（implementations）では、顧客取引の指示は、ユーザデバイス１０２によって生成される代わりに、クレジットカードまたはスマートカードリーダからＰＯＳデバイス１０４によって受信される支払データを含むことができる。例えば、受信される支払データは、クレジットカードまたはスマートカード情報を含むことができる。別の例では、顧客取引の指示は、顧客取引を処理する際にＰＯＳデバイス１０４の取引ユニット１１６によって局所的に生成されることができる。例えば、ＰＯＳデバイス１０４のメモリ内の所定の位置におけるフラグは、取引ユニット１１６が（例えば、顧客から支払を受けるなどの）手動の顧客取引を処理するとき、顧客取引を示すように設定されることができる。

【００４９】

[0055] 顧客取引を処理することに加えて、ＰＯＳデバイス１０４は、ネットワークアクセス（例えば、ゲストネットワークアクセス）をユーザデバイス１０２に提供するために、ネットワークアクセス認証処理を開始することができる。一実施形態では、ＰＯＳデバイス１０４の取引ユニット１１６は、例えば、商品またはサービスの購入のための、顧客と商人との間の顧客取引を処理する。顧客取引の指示を受信すると、ネットワーク通信ユニット１１４は、ＡＰ１０６からユーザデバイス１０２に関するネットワークアクセスを要求することができる。ネットワーク通信ユニット１１４は、例えばリンク１１０を使用して、ネットワークを介してネットワーク通信ユニット１３２にネットワークアクセス要求を通信することができる。

【００５０】

[0056] ネットワークアクセス要求を受信した後に、ＡＰ１０６の認証ユニット１３０は、ＡＰ公開キーおよびＡＰ秘密キーを含むＡＰキーのペアを生成することができる。ＡＰ１０６は、例えばリンク１１０を使用して、ＡＰ公開キーをネットワーク通信ユニット１１４に提供するために、通信ユニット１３２を使用することができる。１つのインプリメンテーションでは、ＡＰキーのペアは、一時的なキーのペア（an ephemeral key pair）である、すなわち、キー確立処理が実行されるたびに新しいキーのペアが生成される。ＡＰ１０６は、図４を参照して以下に説明されるように、キー確立処理の間にＡＰ秘密キーを使用することができる。

【００５１】

[0057] 取引ユニット１１６は、ＯＯＢチャネル１０８上でＡＰ公開キーを取引ユニット１２０に提供することができる。例えば、取引ユニット１１６は、ＡＰ公開キーを（例えばＱＲコードを使用して）レシート上にプリントすることができるか、ＡＰ公開キーを取引ユニット１２０に電子メールで送る（email）か、あるいはテキストメッセージで送る（text）（すなわち、ＳＭＳまたはＭＭＳを使用して）ことができる。一旦ユーザデバイス１０２がＡＰ公開キーを受信すると、認証ユニット１２６および認証ユニット１３０は、以下により詳細に説明されるように、キー確立処理を開始する。

【００５２】

[0058] 上の例を続けて、認証ユニット１２６は、デバイス秘密キーおよびデバイス公開キーを含むデバイスキーのペアを生成することができる。ユーザデバイス１０２は、図４を参照して以下に説明されるように、キー確立処理の間にデバイス秘密キーを使用することができる。キー確立処理は、認証ユニット１２６がリンク１１２を介してデバイス公開キーを認証ユニット１３０に提供することを含む、アソシエーション要求を実行することを含むことができる。キー確立処理は、認証ユニット１２６および認証ユニット１３０が、例えばペアワイズマスターキー（ＰＭＫ）等の安全キーを生成することを含む。

【００５３】

[0059] 認証ユニット１２６および認証ユニット１３０は次いで、キー確立処理に基づいて、ネットワークセキュリティ処理を開始する。認証ユニット１２６および認証ユニット１３０は、ＷＰＡ２認証のようなネットワークセキュリティ処理を実行するために、安全キーを使用することができる。一旦ネットワークセキュリティ処理が完了すると、ネットワークアクセスは、リンク１１２を介してＡＰ１０６によって、あるいは別のリンクおよび／または別のＡＰを介して、ユーザデバイス１０２に提供されることができる。

【００５４】

[0060] ネットワークアクセス認証処理の別の実施形態では、公開キーの交換は、図６を参照して以下に説明されるように、ユーザデバイス１０２とＰＯＳデバイス１０４との間の顧客取引の間に実行される。顧客取引（例えば、支払取引）は、ＯＯＢチャネル１０８上で、取引ユニット１２０と取引ユニット１１６との間で行われることができる。例えば、支払取引は、顧客が、ＮＦＣプロトコルまたはＢｌｕｅｔｏｏｔｈプロトコルのような通信プロトコルを使用して、ＯＯＢチャネル１０８を介してＰＯＳ１０８に支払を提供するために、ユーザデバイス１０２を使用することを含むことができる。顧客取引が開始されることより前に、認証ユニット１３０は、ＡＰキーのペアを生成し、次いでＰＯＳデ

バイス１０４にＡＰキーのペアのうちのＡＰ公開キーを提供することができる。さらに、顧客取引が開始することより前に、認証ユニット１２６はまた、デバイス公開キーおよびデバイス秘密キーを含むデバイスキーのペアを生成することができる。

【００５５】

[0061] 顧客取引の一部として、取引ユニット１１６は、取引ユニット１２０からデバイス公開キーを受信し、取引ユニット１２０は、取引ユニット１１６からＡＰ公開キーを受信する。ネットワーク通信ユニット１１４は、デバイス公開キーをネットワーク通信ユニット１３２に通信することができる。一旦ユーザデバイス１０２がＡＰ公開キーを受信し、ＡＰ１０６がデバイス公開キーを受信すると、認証ユニット１２６および認証ユニット１３０は、キー確立処理を開始する。上述した実施形態と同様に、キー確立処理は、安全キー（例えば、ＰＭＫ）の生成を含むことができる。認証ユニット１２６および認証ユニット１３０は、ネットワークセキュリティ処理を実行するために、安全キーを使用することができる。一旦ネットワークセキュリティ処理が完了すると、ユーザデバイス１０２は、ＡＰ１０６によってネットワークアクセスを提供されることができる。

【００５６】

[0062] ネットワークアクセス認証処理のさらに別の実施形態では、図５を参照して以下に説明されるように、（ＰＭＫのような）安全キーの直接の交換が利用される。ＰＯＳデバイス１０４の取引ユニット１１６は、顧客と商人との間の顧客取引を処理する。顧客取引の指示を受信すると、ＰＯＳデバイス１０４は（例えば、リンク１１０を使用して）、ＡＰ１０６からネットワークアクセスを要求する。ネットワークアクセス要求を受信すると、認証ユニット１３０は、安全キーを生成する。認証ユニット１３０は、リンク１１０上で、安全キーをネットワーク通信ユニット１１４に提供する。取引ユニット１１６は次いで、ＯＯＢチャネル１０８を介して安全キーを取引ユニット１２０に提供する。例えば、取引ユニット１１６は、安全キーを（例えば、ＱＲコードを使用して）レシート上にプリントすることができるか、安全キーを取引ユニット１２０に電子メールで送るか、あるいはテキストメッセージで送る（すなわち、ＳＭＳまたはＭＭＳを使用して）ことができる。認証ユニット１２６および認証ユニット１３０は次いで安全キーを使用して、すなわち、リンク１１２を介して、ネットワークセキュリティ処理を開始することができる。この実施形態および他の実施形態の例示的な動作は、以下の図面を参照してより詳細に説明される。

【００５７】

[0063] 図２は、いくつかの実施形態にしたがって、ネットワークアクセス認証処理を例示するフローダイアグラム２００を表す。フローダイアグラム２００は、（限定ではなく例示のために）図１に説明されたシステムおよびコンポーネントを参照して説明される。例示的な動作は、ＰＯＳデバイス１０４のネットワーク通信ユニット１１４および取引ユニット１１６のような、システム１００における１つまたは複数のコンポーネントによって実行されることができる。

【００５８】

[0064] ブロック２０２から初めて、ＰＯＳデバイス１０４は、ＰＯＳデバイス１０４を使用する顧客取引の指示を受信する。図１を参照して上述したように、指示は、メッセージ、通知、または制御パケットとしてインプリメントされることができる。指示は、顧客取引に関連するデータを含むことができる。

【００５９】

[0065] 図１を参照して上にも述べたように、顧客取引は、商品またはサービスの購入のための取引であることができる。１つのインプリメンテーションでは、顧客は、ユーザデバイス１０２を使用することなく、ＰＯＳデバイス１０４に支払を手動で提供することができる。顧客は、例えば、クレジットカードまたはスマートカードを使用して支払データをＰＯＳデバイス１０４に提供することができる。一例では、クレジットカードまたはスマートカードから受信される支払データは、顧客取引の指示であることができる。別の例では、ＰＯＳデバイス１０４は、受信される支払データを処理すると、顧客取引の指示

を生成することができる。

【００６０】

[0066] 別のインプリメンテーションでは、顧客は、例えば、ＰＯＳデバイス１０４を用いた電子支払取引を開始するためのユーザデバイス１０２のディスプレイ中のオプションを選択することなどによって、ユーザデバイス１０２を使用して購入される商品の代金を払うことができる。取引ユニット１１６は、ＯＯＢチャネル１０８上でまたは別のチャネルを介して、ユーザデバイス１０２の取引ユニット１２０から顧客取引の指示を受信することができる。例えば、取引ユニット１１６は、取引ユニット１２０から支払データを受信することができる。

【００６１】

[0067] ブロック２０４に進んで、顧客取引の指示を受信することに応答して、ＰＯＳデバイス１０４は、ネットワークアクセスを求める要求をＡＰ１０６に通信する。例えば、ＰＯＳデバイス１０４のネットワーク通信ユニット１１４は、リンク１１０を介して、ネットワークアクセスを求める要求を、ＡＰ１０６のネットワーク通信ユニット１３２に通信することができる。

【００６２】

[0068] 一実施形態では、図４を参照して以下に説明されるように、ＡＰ１０６は、ネットワークアクセスを求める要求を受信すると、ＡＰキーのペアを生成することができる。別の実施形態では、図５を参照して以下に説明されるように、ＡＰ１０６は、ネットワークアクセスを求める要求を受信すると、安全キーを生成することができる。

【００６３】

[0069] ブロック２０６に進んで、ＰＯＳデバイス１０４は、ＡＰ１０６からキーを受信する。例えば、ネットワーク通信ユニット１１４は、リンク１１０を介してネットワーク通信ユニット１３２からキーを受信する。図４の実施形態では、ＰＯＳデバイス１０４は、ＡＰキーのペアのうちのＡＰ公開キーを受信する。図５の実施形態では、ＰＯＳデバイス１０４は、安全キーを受信する。

【００６４】

[0070] ブロック２０８に進んで、ＰＯＳデバイス１０４は、ユーザデバイス１０２にキーを提供する。ユーザデバイス１０２は、ネットワークへのネットワークアクセスを取得するために、キーを使用するように構成される。キーは、キーのフォーマットを変えることなく、ユーザデバイス１０２に提供されることができる。ＰＯＳデバイス１０４はよって、キーをユーザデバイス１０２に提供するとき、（ＡＰ１０６によって生成された）受信されるキーの一貫性を維持する。

【００６５】

[0071] 図４の実施形態では、ＰＯＳデバイス１０４は、ＡＰ公開キーをユーザデバイス１０２に提供することができる。例えば、取引ユニット１１６は、ＯＯＢチャネル１０８上で、ＡＰ公開キーを取引ユニット１２０に提供することができる。一旦ユーザデバイス１０２がＡＰ公開キーを受信すると、認証ユニット１２６および認証ユニット１３０は、キー確立処理を開始し、次いでＡＰキーのペア（すなわち、ＡＰ１０６によって生成されたキーのペア）に基づいて、ネットワークセキュリティ処理を開始する。

【００６６】

[0072] 図５の実施形態では、ＰＯＳデバイス１０４は、安全キーをユーザデバイス１０２に提供することができる。例えば、取引ユニット１１６は、ＯＯＢチャネル１０８を介して、安全キーを取引ユニット１２０に提供することができる。認証ユニット１２６および認証ユニット１３０は、例えば、リンク１１２を介して、安全キーを使用して、ネットワークセキュリティ処理を開始することができる。

【００６７】

[0073] 図３は、いくつかの実施形態にしたがって、ネットワークアクセス認証処理を例示するフローダイアグラム３００を表す。フローダイアグラム３００は、（限定ではなく例示のために）図１に説明されたシステムおよびコンポーネントを参照して説明される

。例示的な動作は、ＰＯＳデバイス１０４のネットワーク通信ユニット１１４および取引ユニット１１６のような、システム１００における１つまたは複数のコンポーネントによって実行されることができる。

【００６８】

[0074] ブロック３０２から始めて、ＰＯＳデバイス１０４は、ネットワークアクセスを求める要求をＡＰ１０６に通信する。例えば、ネットワーク通信ユニット１１４は、リンク１１０を介して、ネットワークアクセスを求める要求をＡＰ１０６のネットワーク通信ユニット１３２に通信することができる。一実施形態では、図６を参照して以下に説明されるように、ＡＰ１０６は、ネットワークアクセスを求める要求を受信すると、ＡＰキーのペアを生成することができる。

【００６９】

[0075] ブロック３０４に進んで、ＰＯＳデバイス１０４は、ＡＰ１０６からＡＰキーのペアのうちのＡＰ公開キーを受信する。例えば、ネットワーク通信ユニット１１４は、リンク１１０を介して、ネットワーク通信ユニット１３２からＡＰ公開キーを受信することができる。

【００７０】

[0076] ブロック３０６に進んで、ＰＯＳデバイス１０４は、ユーザデバイス１０２との支払取引を処理する。例えば、ユーザデバイス１０２は、ＰＯＳデバイス１０４からの商品の代金を払うために使用されることができる支払アプリケーションを含むことができる。顧客は、例えば支払の形態を選択するために、支払アプリケーションにおいて電子支払を選択することができる。ユーザデバイス１０２における支払アプリケーションは次いで、支払取引を開始することができる。支払取引は、例えばＮＦＣプロトコルまたはＢｌｕｅｔｏｏｔｈプロトコル等を使用して、ＯＯＢ１０８を介して取引ユニット１２０と取引ユニット１１６との間で実行されることができる。

【００７１】

[0077] 支払取引を処理することは、ＰＯＳデバイス１０４がＡＰ公開キーをユーザデバイス１０２に提供すること、およびユーザデバイス１０２からデバイスキーのペアのうちのデバイス公開キーを受信することを含む。例えば、取引ユニット１１６は、ＯＯＢチャネル１０８を介して、支払取引の支払データと共に取引ユニット１２０からデバイス公開キーを受信することができる。支払取引の一部として、取引ユニット１１６は、ＯＯＢチャネル１０８を介して、ＡＰ公開キーを取引ユニット１２０に通信することができる。

【００７２】

[0078] ＰＯＳデバイス１０４は、ブロック３０６の、ユーザデバイス１０２からの支払取引を処理することより前に、（ブロック３０２の）ネットワークアクセスを求める要求を通信すること、およびＡＰ１０６からＡＰ公開キーを受信することができることに留意されたい。しかしながら、一実施形態では、ＰＯＳデバイス１０４は、（ブロック３０６の）ユーザデバイス１０２からの支払取引を処理することと事実上同時に、（ブロック３０４の）ＡＰ１０６からＡＰ公開キーを受信することができる。

【００７３】

[0079] ブロック３０８に進んで、ＰＯＳデバイス１０４は、デバイス公開キーをＡＰ１０６に提供することができる。例えば、ネットワーク通信ユニット１１４は、デバイス公開キーをネットワーク通信ユニット１３２に提供することができる。図６を参照して以下でより詳細に説明されるように、一旦ユーザデバイス１０２がＡＰ公開キーを受信すると、認証ユニット１２６および認証ユニット１３０は、ＡＰキーのペアおよびデバイスキーのペアに基づいて、キー確立処理およびネットワークセキュリティ処理を開始する。

【００７４】

[0080] 図４は、いくつかの実施形態にしたがって、ネットワークアクセス認証処理の間に、ユーザデバイス１０２、ＰＯＳデバイス１０４およびＡＰ１０６によって実行される動作を示す、メッセージフローダイアグラムである。

【００７５】

[0081] ＰＯＳデバイス１０４は、４０２Ａまたは４０２Ｂ（破線で示される）の何れかを介して、ＰＯＳデバイス１０４を使用する顧客取引の指示を受信する。４０２Ａにおいて、ＰＯＳデバイス１０４は、ユーザデバイス１０２から顧客取引の指示を受信することができる。顧客取引の指示（例えば、支払データ）は、ＯＯＢ１０８のような帯域外（ＯＯＢ）チャネル上で通信されることができる。

【００７６】

[0082] 代替的に、４０２Ｂにおいて、ＰＯＳデバイス１０４は、ユーザデバイス１０２を使用することなく提供される支払データの一部として顧客取引の指示を受信することができる。例えば、顧客は、ユーザデバイス１０２を使用することなくＰＯＳデバイス１０４に支払を手動で提供することができる。顧客取引の指示は、例えばクレジットカードまたはスマートカード情報等の、受信される支払データであることができる。ＰＯＳデバイス１０４はまた、支払データを受信または処理すると、顧客取引の指示（例えば、フラグ）を局所的に生成および記憶することができる。

【００７７】

[0083] ４０４において、顧客取引の指示を受信すると、ＰＯＳデバイス１０４は、ネットワークアクセス要求をＡＰ１０６に通信する。ネットワーク通信ユニット１１４は、例えばリンク１１０を使用して、ネットワークを介してネットワーク通信ユニット１３２にネットワークアクセス要求を通信することができる。

【００７８】

[0084] ４０６において、ネットワークアクセス要求を受信すると、ＡＰ１０６は、ＡＰキーのペアを生成する。ＡＰキーのペアは、ＡＰ秘密キーおよびＡＰ公開キーを含むことができる。一実施形態では、ＡＰキーのペアは非対称キーのペアである。

【００７９】

[0085] ４０８において、ＡＰ１０６は、ＡＰキーのペアのうちの公開キーをＰＯＳデバイス１０４に通信する。ネットワーク通信ユニット１３２は、例えばリンク１１０を使用して、ネットワークを介して公開キーをネットワーク通信ユニット１１４に通信することができる。

【００８０】

[0086] ４１０において、ＰＯＳデバイス１０４は、ＡＰキーのペアのうちの公開キーをユーザデバイス１０２に通信する。ＰＯＳデバイス１０４は、ＯＯＢチャネルを介して公開キーをユーザデバイス１０２に通信することができる。一実施形態では、４１０のＯＯＢチャネルは、４０２で使用されるＯＯＢチャネルと同じであることができる。別の実施形態では、４１０で使用されるＯＯＢチャネルは、４０２で使用されるＯＯＢチャネルとは異なる。

【００８１】

[0087] ４１２において、ユーザデバイス１０２およびＡＰ１０６は、キー確立処理を開始する。４１２のキー確立処理は、ユーザデバイス１０２がアソシエーション要求をＡＰ１０６に通信することを含むことができる。４１２のキー確立処理はまた、ユーザデバイス１０２がデバイスキーのペアのうちのデバイス公開キーをＡＰ１０６に通信することを含むことができる。いくつかのインプリメンテーションでは、ユーザデバイス１０２は、４１２のキー確立処理を開始することより前に、または、４１２のキー確立処理の間に、デバイス公開キーおよびデバイス秘密キーを含むデバイスキーのペアを生成することができる。例えば、ユーザデバイス１０２は、４０２において顧客取引を通信する際、４１０においてＡＰ公開キーを受信する際、または４１２においてアソシエーション要求を実行する際等に、デバイスキーのペアを生成することができる。

【００８２】

[0088] ４１４Ａにおいて、ユーザデバイス１０２は、受信されたＡＰ公開キーに少なくとも部分的に基づいて、安全キーを生成する。同様に、４１４Ｂにおいて、ＡＰ１０６は、受信されたデバイス公開キーに少なくとも部分的に基づいて、安全キーを生成する。一実施形態では、ユーザデバイス１０２によっておよびＡＰ１０６によって生成された安

全キーは、対称キーである。一実施形態では、ユーザデバイス１０２およびＡＰ１０６は、４１２のアソシエーション要求に少なくとも部分的に基づいて、同時に対称キーを生成する。一実施形態では、４１４Ａおよび４１４Ｂにおいて、ユーザデバイス１０２およびＡＰ１０６は、ユーザデバイス１０２およびＡＰ１０６の両方によってその後記憶される、単一の安全キーを生成する。

【００８３】

[0089] ユーザデバイス１０２およびＡＰ１０６は、ユーザデバイス１０２とＡＰ１０６との間の、ＤＨ（Diffie-Hellman）、ＳＡＥ（Simultaneous Authentication of Equals）、Ｗｉ－Ｆｉプロテクテッドセットアップ（ＷＰＳ：Wi-Fi Protected Setup）または、任意の他の技術的に実現可能なキー確立処理に少なくとも部分的に基づいて、（１つまたは複数の）安全キーを生成することができる。（１つまたは複数の）安全キーは、ネットワークセキュリティ処理で使用されるために、続いて直接的に使用されるか、またはキー導出アルゴリズム（a key derivation algorithm）を使用して導出されることができる。ネットワークセキュリティ処理は、Ｗｉ－Ｆｉプロテクテッドアクセス（Wi-Fi Protected Access）（商標）（ＷＰＡ（商標）またはＷＰＡ２（商標））によって、あるいはＷＥＰ（Wired Equivalent Privacy）によって指定された４ウェイハンドシェイク認証（a 4-way handshake authentication）のような、（１つまたは複数の）対称キーに頼った認証プロトコルを使用してインプリメントされることができる。安全キーは、ペアワイズマスターキー（ＰＭＫ）、ペアワイズ一時キー（ＰＴＫ）、または事前共有キー（ＰＳＫ）としてインプリメントされることができる。

【００８４】

[0090] ４１６において、ユーザデバイス１０２およびＡＰ１０６は、ネットワークセキュリティ処理を実行する。ネットワークセキュリティ処理は、（１つまたは複数の）安全キー、または、（１つまたは複数の）ＰＭＫキーのようなそれの派生物（a derivative）を使用して、実行される。例えば、ユーザデバイス１０２およびＡＰ１０６は、ＷＰＡまたはＷＰＡ２プロトコル、ＷＥＰプロトコル、あるいは他のネットワークセキュリティ処理にしたがって、（１つまたは複数の）安全キーを使用して、ネットワークセキュリティ処理を実行することができる。ＷＥＰおよびＷＰＡ／ＷＰＡ２は典型的にはＷＬＡＮネットワークと共に使用されるが、他のネットワークおよび／またはネットワークセキュリティ処理の使用も考慮されていることに留意されたい。

【００８５】

[0091] ４１８Ａにおいて、ユーザデバイス１０２は、（１つまたは複数の）安全キーを使用して、ネットワークアクセスのためにＡＰ１０６を認証する。例えば、認証ユニット１２６は、４１６のネットワークセキュリティ処理に基づいて、ＡＰ１０６を認証する。４１８Ｂにおいて、ＡＰ１０６は、（１つまたは複数の）安全キーを使用して、ネットワークアクセスのためにユーザデバイス１０２を認証する。例えば、認証ユニット１３０は、４１６のネットワークセキュリティ処理に基づいて、ユーザデバイス１０２を認証する。４１８Ａおよび４１８Ｂの相互認証処理からネットワークアクセスを取得した後で、ユーザは、ブラウザまたはユーザデバイス１０２上で実行中の他のアプリケーションを介して、インターネットまたは他のネットワークリソースにアクセスすることができる。

【００８６】

[0092] いくつかの実施形態では、公開キー自体の代わりに公開キーのハッシュが通信されることに留意されたい。ハッシング（hashing）の使用は、暗号セキュリティ（cryptographic security）の追加的なレイヤ（layer）を提供し得る。例えば、４０８において、ＡＰ１０６は、ＡＰキーのペアのうちのＡＰ公開キーのハッシュをＰＯＳデバイス１０４に通信することができる。４１０において、ＰＯＳデバイス１０４は、ＡＰ公開キーのハッシュをユーザデバイス１０２に通信することができる。ユーザデバイス１０２は、次いでキー確立処理４１２内で受信されたＡＰ公開キーが、受信されたハッシュに一致したことを確かめ（verify）、そして４１２を進めることができる（proceed with）。

【００８７】

[0093] 図５は、いくつかの実施形態にしたがって、ユーザデバイス１０２、ＰＯＳデバイス１０４、およびＡＰ１０６によって実行される動作を示すメッセージフローダイアグラムである。

【００８８】

[0094] ＰＯＳデバイス１０４は、５０２Ａまたは５０２Ｂ（破線で示される）の何れかを介してＰＯＳデバイス１０４を使用する顧客取引の指示を受信する。５０２Ａにおいて、ＰＯＳデバイス１０４は、ユーザデバイス１０２から顧客取引の指示を受信することができる。顧客取引の指示（例えば、支払データ）は、ＯＯＢチャネル上で通信されることができる。

【００８９】

[0095] 代替的に、５０２Ｂにおいて、ＰＯＳデバイス１０４は、ユーザデバイス１０２を使用することなく提供される支払データの一部として顧客取引の指示を受信することができる。例えば、４０２Ｂを参照して上述した技法と同様に、ＰＯＳデバイス１０４は、クレジットカードまたはスマートカードを介して顧客から支払を受けることができる。顧客取引の指示は、例えばクレジットカードまたはスマートカード情報等の、受信される支払データであることができる。ＰＯＳデバイス１０４はまた、支払データを受信または処理すると、顧客取引の指示（例えば、フラグ）を局所的に生成および記憶することができる。

【００９０】

[0096] ５０４において、顧客取引の指示を受信すると、ＰＯＳデバイス１０４は、ネットワークアクセス要求をＡＰ１０６に通信する。ネットワーク通信ユニット１１４は、例えばリンク１１０を使用して、ネットワークを介してネットワーク通信ユニット１３２にネットワークアクセス要求を通信することができる。

【００９１】

[0097] ５０６において、ネットワークアクセス要求を受信すると、ＡＰ１０６は、安全キーを生成する。図４および図６を参照して説明される実施形態とは対照的に、ＡＰ１０６は単独で、すなわちキー確立処理を使用することなく、および／または、ユーザデバイス１０２とＡＰ１０６との間で交換される非対称キーに基づいて認証プロトコルをインプリメントすることなく、安全キーを生成することに留意されたい。一実施形態では、安全キーは対称キーである。安全キーは、ペアワイズマスターキー（ＰＭＫ）、ペアワイズ一時キー（ＰＴＫ）、または事前共有キー（ＰＳＫ）としてインプリメントされることができる。

【００９２】

[0098] ５０８において、ＡＰ１０６は、安全キーをＰＯＳデバイス１０４に通信する。ネットワーク通信ユニット１３２は、リンク１１０を使用することによって、安全キーをネットワーク通信ユニット１１４に通信することができる。

【００９３】

[0099] ５１０において、ＰＯＳデバイス１０４は、安全キーをユーザデバイス１０２に通信する。ＰＯＳデバイス１０４は、ＯＯＢチャネルを介して、安全キーをユーザデバイス１０２に通信することができる。一実施形態では、４１０のＯＯＢチャネルは、５０２で使用されるＯＯＢチャネルと同じであることができる。別の実施形態では、５１０のＯＯＢチャネルは、５０２で使用されるＯＯＢチャネルとは異なる。

【００９４】

[00100] ５１２において、ユーザデバイス１０２およびＡＰ１０６は、ネットワークセキュリティ処理を実行する。ネットワークセキュリティ処理は、安全キーまたはキー導出アルゴリズムを使用して取得される安全キーの派生物を使用して、実行される。例えば、ユーザデバイス１０２およびＡＰ１０６は、Ｗｉ－Ｆｉプロテクテッドアクセス（ＷＰＡ）またはＷＰＡ２プロトコル、ＷＥＰ（Wired Equivalent Privacy）プロトコル、または他のネットワークセキュリティ処理にしたがって、安全キーを使用して、ネットワークセキュリティ処理を実行することができる。ＷＥＰおよびＷＰＡ／ＷＰＡ２は典型的には

ＷＬＡＮネットワークと共に使用されるが、他のネットワークおよび対応するネットワークセキュリティ処理の使用も考慮されていることに留意されたい。

【００９５】

[00101] ５１４Ａにおいて、ユーザデバイス１０２は、安全キーを使用して、ネットワークアクセスのためにＡＰ１０６を認証する。例えば、認証ユニット１２６は、５１２のネットワークセキュリティ処理に基づいて、ＡＰ１０６を認証する。５１４Ｂにおいて、ＡＰ１０６は、（１つまたは複数の）安全キーを使用して、ネットワークアクセスのためにユーザデバイス１０２を認証する。例えば、認証ユニット１３０は、５１２のネットワークセキュリティ処理に基づいて、ユーザデバイス１０２を認証する。

【００９６】

[00102] 図６は、いくつかの実施形態にしたがって、ユーザデバイス１０２、ＰＯＳデバイス１０４およびＡＰ１０６によって実行される動作を示すメッセージフローダイアグラムである。

【００９７】

[00103] ６０２において、ＰＯＳデバイス１０４は、ネットワークアクセス要求をＡＰ１０６に通信する。ネットワーク通信ユニット１１４は、リンク１１０を使用することによって、ネットワークアクセス要求をネットワーク通信ユニット１３２に通信することができる。

【００９８】

[00104] ６０４において、ネットワークアクセス要求を受信すると、ＡＰ１０６は、ＡＰキーのペアを生成する。ＡＰキーのペアは、ＡＰ秘密キーおよびＡＰ公開キーを含むことができる。一実施形態では、ＡＰキーのペアは非対称キーのペアである。

【００９９】

[00105] ６０６において、ＡＰ１０６は、ＡＰキーのペアのうちの公開キーをＰＯＳデバイス１０４に通信する。ネットワーク通信ユニット１３２は、リンク１１０を使用することによって、公開キーをネットワーク通信ユニット１１４に通信することができる。

【０１００】

[00106] ６０８において、ユーザデバイス１０２およびＰＯＳデバイス１０４は、支払取引を実行する。支払取引６０８は、ユーザデバイス１０２が、６１２において、支払データをＰＯＳデバイス１０４に通信することを含む。支払データは、顧客の銀行から商人の銀行に送られた金銭（money being transferred）を示すことができ、それは、そのような支払取引の認証のための他の情報を含み得る。ユーザデバイス１０２は、例えばＮＦＣプロトコルまたはＢｌｕｅｔｏｏｔｈプロトコル等を使用して、ＯＯＢチャネル１０８上で支払データを通信することができる。例えば、ユーザデバイス１０２は、ＰＯＳデバイス１０４に支払を提供するために使用されることができる支払アプリケーションを含むことができる。支払アプリケーションは、ＰＯＳデバイス１０４への支払を許可するために、金融機関（例えば顧客の銀行）と通信することができる。支払アプリケーションは次いで、支払認証をＰＯＳデバイス１０４に提供することができる。

【０１０１】

[00107] ６０８の支払取引はまた、ユーザデバイス１０２が、６１４において、デバイスキーのペアのうちのデバイス公開キーをＰＯＳデバイス１０４に通信することを含む。ユーザデバイス１０２は、６０８において支払取引を実行することより前に、デバイスキーのペアを生成することができる。ユーザデバイス１０２は、デバイスキーのペアのうちのデバイス秘密キーを保持する、すなわち、デバイス秘密キーを他のデバイスに通信することがない可能性がある。支払取引６０８はまた、ＰＯＳデバイス１０４が、ＡＰキーのペアのうちのＡＰ公開キーをユーザデバイス１０２に通信することを含む。

【０１０２】

[00108] 一実施形態では、６１４において、ユーザデバイス１０２は、ユーザデバイス１０２が支払データ６１２を通信するために使用したのと同じＯＯＢチャネル上で、デバイス公開キーをＰＯＳデバイス１０４に通信することができる。一実施形態では、６１

６において、ＰＯＳデバイス１０４は、例えばＮＦＣプロトコルまたはＢｌｕｅｔｏｏｔｈプロトコル等を使用して、６１２における支払データの通信、および／または、６１４におけるデバイス公開キーの通信と同じＯＯＢチャネル上で、ＡＰ公開キーをユーザデバイス１０２に通信することができる。

【０１０３】

[00109] ６１８において、ＰＯＳデバイス１０４は、デバイス公開キーをＡＰ１０６に通信する。例えば、ネットワーク通信ユニット１１４は、リンク１１０を介して、デバイス公開キーをネットワーク通信ユニット１３２に通信する。

【０１０４】

[00110] ６２０において、ユーザデバイス１０２およびＡＰ１０６は、キー確立処理を開始する。６２０のキー確立処理は、ユーザデバイス１０２がアソシエーション要求をＡＰ１０６に通信することを含むことができる。

【０１０５】

[00111] ６２２Ａにおいて、ユーザデバイス１０２は、受信されたＡＰ公開キーに少なくとも部分的に基づいて、安全キーを生成する。同様に、６２２Ｂにおいて、ＡＰ１０６は、受信されたデバイス公開キーに少なくとも部分的に基づいて、安全キーを生成する。一実施形態では、ユーザデバイス１０２によっておよびＡＰ１０６によって生成された安全キーは、対称キーである。一実施形態では、ユーザデバイス１０２およびＡＰ１０６は、６２０のキー確立処理のアソシエーション要求に少なくとも部分的に基づいて、対称キーを同時に生成する。一実施形態では、４１４Ａおよび４１４Ｂにおいて、ユーザデバイス１０２およびＡＰ１０６は、ユーザデバイス１０２およびＡＰ１０６の両方によってその後記憶される、単一の安全キーを生成する。

【０１０６】

[00112] 図４の４１４Ａおよび４１４Ｂを参照して上述した技法と同様に、６２２Ａにおいておよび６２２Ｂにおいて、それぞれ、ユーザデバイス１０２およびＡＰ１０６は、ＤＨ（Diffie-Hellman）、ＳＡＥ（Simultaneous Authentication of Equals）、Ｗｉ－Ｆｉプロテクテッドセットアップ（ＷＰＳ：Wi-Fi Protected Setup）、または任意の他の技術的に実現可能なキー確立処理に少なくとも部分的に基づいて、（１つまたは複数の）安全キーを生成することができる。（１つまたは複数の）安全キーは、ペアワイズマスターキー（ＰＭＫ）、ペアワイズ一時キー（ＰＴＫ）、または事前共有キー（ＰＳＫ）としてインプリメントされることができる。

【０１０７】

[00113] 図４の４１６を参照して上述した技法と同様に、６２４において、ユーザデバイス１０２およびＡＰ１０６は、ネットワークセキュリティ処理を実行することができる。ネットワークセキュリティ処理は、（１つまたは複数の）安全キー、例えば（１つまたは複数の）ＰＭＫキーを使用して、実行される。例えば、ユーザデバイス１０２およびＡＰ１０６は、Ｗｉ－Ｆｉプロテクテッドアクセス（ＷＰＡ）またはＷＰＡ２プロトコル、ＷＥＰ（Wired Equivalent Privacy）プロトコル、または他のネットワークセキュリティ処理にしたがって、安全キーを使用してネットワークセキュリティ処理を実行することができる。ＷＥＰおよびＷＰＡ／ＷＰＡ２は典型的にはＷＬＡＮネットワークと共に使用されるが、他のネットワークおよび対応するネットワークセキュリティ処理の使用も考慮されていることに留意されたい。

【０１０８】

[00114] ６２６Ａにおいて、ユーザデバイス１０２は、（１つまたは複数の）安全キーを使用して、ネットワークアクセスのためにＡＰ１０６を認証する。例えば、認証ユニット１２６は、６２４のネットワークセキュリティ処理に基づいて、ＡＰ１０６を認証する。６２６Ｂにおいて、ＡＰ１０６は、（１つまたは複数の）安全キーを使用して、ネットワークアクセスのためにユーザデバイス１０２を認証する。例えば、認証ユニット１３０は、６２４のネットワークセキュリティ処理に基づいて、ユーザデバイス１０２を認証する。

【０１０９】
[00115] 図４を参照して上述した技法と同様に、公開キー自体の代わりに公開キーのハッシュが通信されることができる。例えば、６０８において、ＡＰ１０６は、ＡＰキーのペアのうちのＡＰ公開キーのハッシュをＰＯＳデバイス１０４に通信することができる。同様に、６１８において、ＰＯＳデバイス１０４は、デバイスキーのペアのうちのデバイス公開キーのハッシュをＡＰ１０６に通信することができる。
【０１１０】
[00116] 本開示に照らして理解されるように、図２および図３の、および／または、図４から図６のフローダイアグラムは、本開示の代替的な態様を導き出すために修正され得る。また、本開示のこの態様におけるいくつかの動作は、逐次的な順序で示される。しかしながら、ある特定の動作は示されるものとは異なる順序で起こり得、ある特定の動作は同時に実行され得、ある特定の動作は他の動作と組み合わされ得、およびある特定の動作は本開示の別の態様では欠け得る。
【０１１１】
[00117] 当業者に認識されることになるように、本開示の複数の態様は、システム、方法、またはコンピュータプログラム製品として具現化され得る。したがって、本開示の複数の態様は、完全なるハードウェア実施形態、ソフトウェア実施形態（ファームウェア、常駐ソフトウェア、マイクロ－コード等を含む）、あるいは、本明細書において、すべて「回路」、「モジュール」、「ユニット」または「システム」と概して称され得る複数のソフトウェアおよびハードウェア態様を組み合わせた実施形態の形をとり得る。さらに、本開示の複数の態様は、コンピュータ読み取り可能なプログラムコードを統合（embodied）した１つまたは複数のコンピュータ読み取り可能な媒体に統合されたコンピュータプログラム製品の形をとり得る。
【０１１２】
[00118] １つまたは複数の非一時的なコンピュータ読み取り可能な媒体の如何なる組み合わせも、利用され得る。非一時的なコンピュータ読み取り可能な媒体は、一時的な（transitory）、伝播信号を唯一の例外として、すべてのコンピュータ読み取り可能な媒体を備える。非一時的なコンピュータ読み取り可能な媒体は、コンピュータ読み取り可能な記憶媒体であり得る。コンピュータ読み取り可能な記憶媒体は、例えば、それらに限定されるわけではないが、電子、磁気、光学、電磁気、赤外線、または半導体システム、装置、またはデバイス、あるいは、前述のものの任意の適切な組合せであり得る。コンピュータ読み取り可能な記憶媒体のより具体的な例（完全に網羅されてはいないリスト）は、１つまたは複数のワイヤを有する電気的な接続、ポータブルコンピュータディスケット、ハードディスク、ランダムアクセスメモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、消去可能なプログラム可能な読み取り専用メモリ（ＥＰＲＯＭまたはフラッシュメモリ）、光ファイバ、ポータブルコンパクトディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、光学記憶デバイス、磁気記憶デバイス、または前述のもの任意の適切な組み合わせを含み得る。本文書の文脈では、コンピュータ読み取り可能な記憶媒体は、命令実行システム、装置、またはデバイスに関連して使用されるか、あるいは命令実行システム、装置、またはデバイスによって使用されるための、プログラムを含むまたは記憶することができる、如何なる有形の媒体でもあり得る。
【０１１３】
[00119] 本開示の複数の態様に関する動作を実行するためのコンピュータ読み取り可能な媒体上に埋め込まれたコンピュータプログラムコードは、例えばＪａｖａ（登録商標）、Ｓｍａｌｌｔａｌｋ、Ｃ＋＋または同様のもの等のオブジェクト指向プログラミング言語（an object oriented programming language）、ならびに、例えば「Ｃ」プログラミング言語または同様のプログラミング言語等の従来の手続きプログラミング言語（conventional procedural programming languages）を含む、１つまたは複数のプログラミング言語の如何なる組み合わせでも書かれ得る。プログラムコードは、完全にユーザのコンピュータで、部分的にユーザのコンピュータで、スタンドアロンソフトウェアパッケージ

として、部分的にユーザのコンピュータでかつ部分的にリモートコンピュータで、あるいは完全にリモートコンピュータまたはサーバで、実行し得る。後者の状況では、リモートコンピュータは、ローカルエリアネットワーク（ＬＡＮ）またはワイドエリアネットワーク（ＷＡＮ）を含む任意のタイプのネットワークを通してユーザのコンピュータに接続され得るか、または接続は、（例えば、インターネットサービスプロバイダを使用してインターネットを通して）外部のコンピュータに、成され得る。

【０１１４】

[00120] 本開示の複数の態様は、本開示の実施形態にしたがった方法、装置（システム）およびコンピュータプログラム製品のフローチャート例示および／またはブロック図を参照して説明される。フローチャート例示および／またはブロック図の各ブロック、およびフローチャート例示および／またはブロック図における複数のブロックの組み合わせは、コンピュータプログラム命令によってインプリメントされることができることは理解されることになる。これらのコンピュータプログラム命令は、機械を製造（produce）するために、汎用コンピュータ、特殊目的コンピュータ、または他のプログラム可能なデータ処理装置のプロセッサに、そのコンピュータまたは他のプログラム可能なデータ処理装置のプロセッサを介して実行する命令がフローチャートおよび／またはブロック図のブロックまたは複数のブロックに指定された機能／アクトをインプリメントするための手段を作り出すように、提供され得る。

【０１１５】

[00121] これらのコンピュータプログラム命令はまた、コンピュータ読み取り可能な媒体内に記憶された命令が、フローチャートおよび／またはブロック図のブロックまたは複数のブロックに指定された機能／アクトをインプリメントする命令を含む製品を製造（produce）するように、コンピュータ、他のプログラム可能なデータ処理装置または他のデバイスに、特定の方法で機能するよう指示する（direct）ことができる、コンピュータ読み取り可能な媒体内に、記憶され得る。

【０１１６】

[00122] コンピュータプログラム命令はまた、コンピュータ、他のプログラム可能なデータ処理装置、または他のデバイスにロードされ、そのコンピュータ、他のプログラム可能な装置、または他のデバイス上で一連の動作ステップを実行させて、そのコンピュータまたは他のプログラム可能な装置上で実行する命令がフローチャートおよび／またはブロック図のブロックまたは複数のブロックに指定された機能／アクトをインプリメントするためのプロセスを提供するように、コンピュータによってインプリメントされるプロセスを作り出し得る（produce）。

【０１１７】

[00123] 図７は、電子デバイス７００の１つの実施形態のブロック図である。電子デバイス７００は、以下でさらに説明されるように、図１－６に関し上で説明された、ユーザデバイス、ＰＯＳデバイス、またはＡＰの動作を実行することおよび機能性をインプリメントすることができる。電子デバイスは、プロセッサ７０２（場合によっては複数のプロセッサ、複数のコア、複数のノードを含む、および／または、マルチスレッディングをインプリメントする、等の）を含む。電子デバイスは、メモリ７０６を含む。メモリ７０６は、システムメモリ（例えば、キャッシュ、ＳＲＡＭ、ＤＲＡＭ、ゼロキャパシタＲＡＭ、ツイントランジスタＲＡＭ、ｅＤＲＡＭ、ＥＤＯ ＲＡＭ、ＤＤＲ ＲＡＭ、ＥＥＰＲＯＭ（登録商標）、ＮＲＡＭ、ＲＲＡＭ（登録商標）、ＳＯＮＯＳ、ＰＲＡＭ等のうちの１つまたは複数）であり得るか、または機械読み取り可能な媒体の、上で既に説明された、可能性のある実現のうちの任意の１つまたは複数であり得る。電子デバイスはまた、バス７１０（例えば、ＰＣＩ、ＩＳＡ、ＰＣＩ－Ｅｘｐｒｅｓｓ、Ｈｙｐｅｒトランスポート（登録商標）、インフィニバンド（登録商標）、ＮｕＢｕｓ等）、ならびに、ワイヤレスネットワークインタフェース（例えば、ＷＬＡＮインタフェース、Ｂｌｕｅｔｏｏｔｈ（登録商標）インタフェース、ＷｉＭＡＸインタフェース、ＺｉｇＢｅｅ（登録商標）インタフェース、ワイヤレスＵＳＢインタフェース等）およびワイヤードネットワークイ

ンタフェース（例えば、ＰＬＣインタフェース、イーサネットインタフェース等）のうちの少なくとも１つを含むネットワークインタフェース７０４、を含む。

【０１１８】

[00124] いくつかの実施形態では、ネットワークインタフェース７０４は、ネットワーク通信ユニット７１４を含み得る。また、ネットワークインタフェース７０４は、オプションとして、取引ユニット７１６および認証ユニット７１８（破線で示される）を含み得る。例えば、電子デバイス７００がユーザデバイス（例えば、図１のユーザデバイス１０２）である場合、ネットワークインタフェース７０４は、ネットワーク通信ユニット７１４、取引ユニット７１６、および認証ユニット７１８を含み得る。別の例では、電子デバイス７００がＰＯＳデバイス（例えば、図１のＰＯＳデバイス１０４）である場合、ネットワークインタフェース７０４は、ネットワーク通信ユニット７１４および取引ユニット７１６を含み得る。さらに別の例では、電子デバイス７００がＡＰ（例えば、図１のＡＰ１０６）である場合、ネットワークインタフェース７０４は、ネットワーク通信ユニット７１４および認証ユニット７１８を含み得る。いくつかの実施形態では、ネットワークインタフェース７０４、プロセッサ７０２、およびメモリ７０６は、図１－６において上述した機能性をインプリメントすることができる。例えば、ネットワークインタフェース７０４、プロセッサ７０２、およびメモリ７０６は、ネットワーク通信ユニット７１４、取引ユニット７１６、および／または認証ユニット７１８の機能性をインプリメントすることができる。

【０１１９】

[00125] これらの機能性のうちの何れの１つも、部分的に（または完全に）ハードウェア内でおよび／またはプロセッサユニット７０２上でインプリメントされ得ることにさらに留意されたい。例えば、機能性は、特定用途向け集積回路を用いて、プロセッサユニット７０２内でインプリメントされる論理において、周辺デバイスまたはカード上のコプロセッサ（a co-processor）において、等のようにしてインプリメントされ得る。さらに、実現は、より少ないコンポーネントまたは図７には例示されていない追加的なコンポーネント（例えば、ビデオカード、オーディオカード、追加的なネットワークインタフェース、周辺デバイス等）を含み得る。プロセッサユニット７０２、（１つまたは複数の）記憶デバイス、およびネットワークインタフェース７０４は、バス７１０に結合される。バス７１０に結合されているものとして例示されているが、メモリユニット７０６は、プロセッサユニット７０２に結合され得る。

【０１２０】

[00126] 実施形態は、様々なインプリメンテーションおよび実施を参照して説明されるが、これらの実施形態は例示的なものであること、および本開示の範囲はそれらに限定されないことは、理解されることになる。一般に、ここに説明されたネットワークアクセス（例えばゲストネットワークアクセス）のためにデバイスを構成することを容易にするための技法は、任意のハードウェアシステムまたは複数のハードウェアシステムと一致するファシリティを用いてインプリメントされ得る。多くの変形、修正、追加、および改善が可能である。

【０１２１】

[00127] 複数形の事例が、単一の事例としてここに説明されるコンポーネント、動作、または構造について提供され得る。最後に、様々なコンポーネント、動作およびデータストア間の境界は、いくぶん恣意的であり、特定の動作は、具体的な例示的な構成の文脈で例示される。機能性の他の割り振りが想定されており、本開示の範囲に含まれ得る。一般に、例示的な構成における別々のコンポーネントとして提示された構造および機能性は、組み合わされた構造またはコンポーネントとしてインプリメントされ得る。同様に、単一のコンポーネントとして提示された構造および機能性は、別々のコンポーネントとしてインプリメントされ得る。これらのおよび他の変形、修正、追加、および改善は、本開示の範囲に含まれ得る。

【図１】

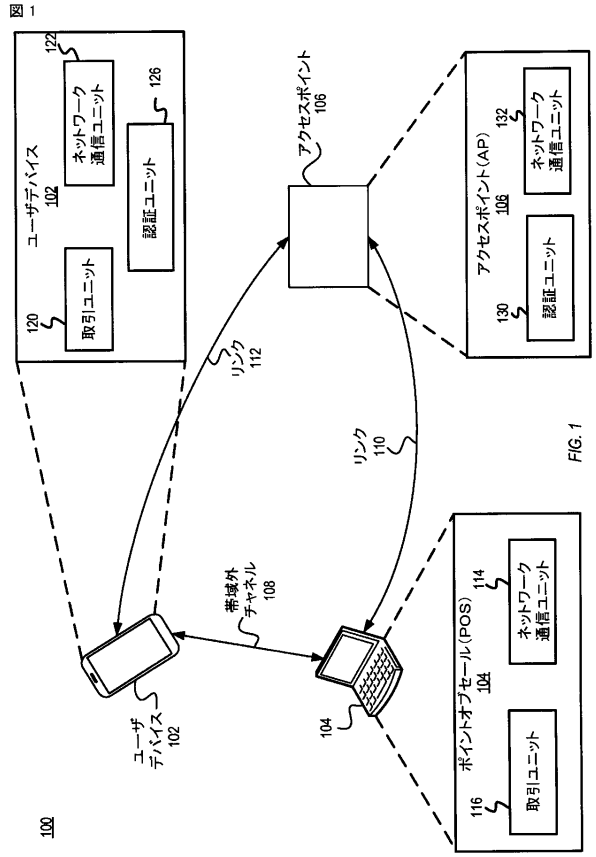

FIG. 1

【図２】

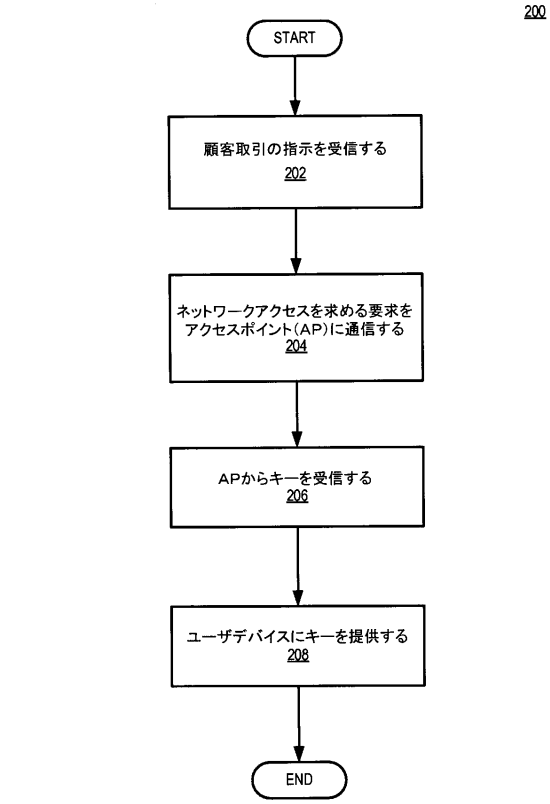

FIG. 2

【図３】

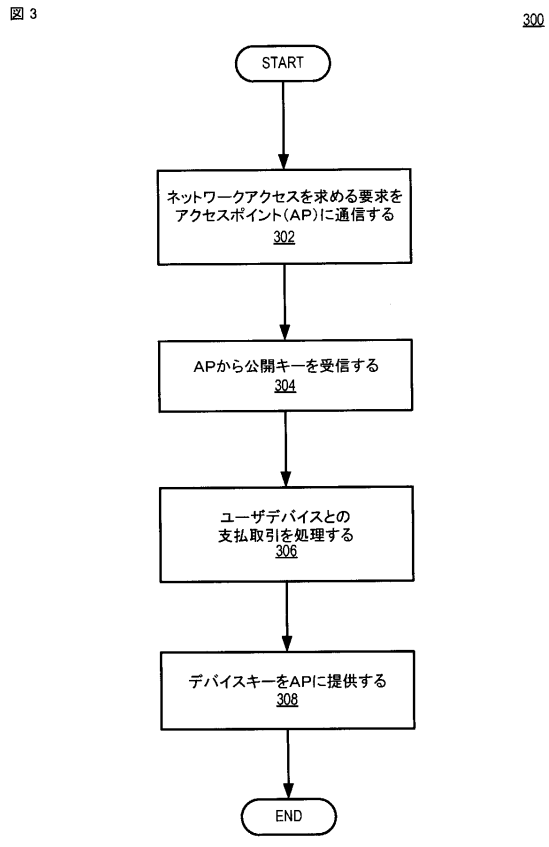

FIG. 3

【図４】

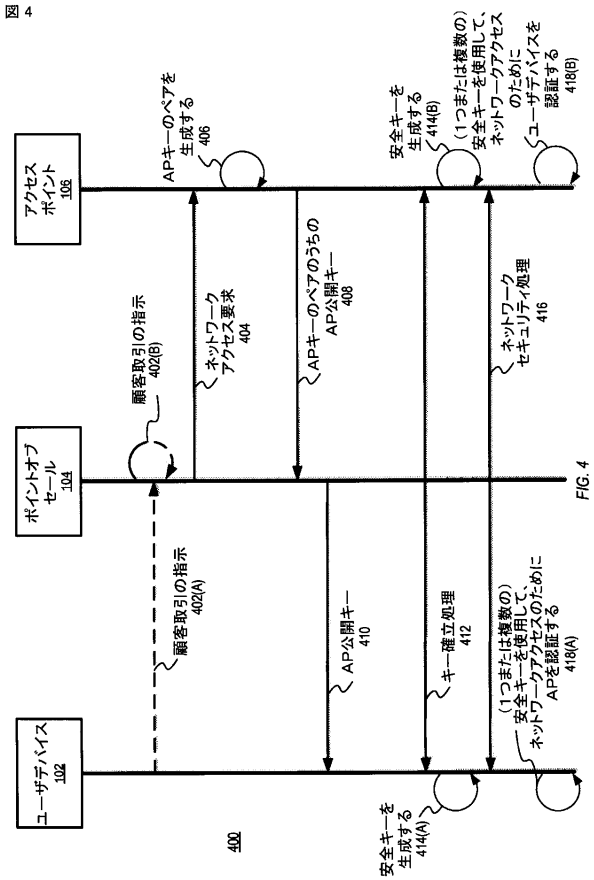

FIG. 4

【図５】

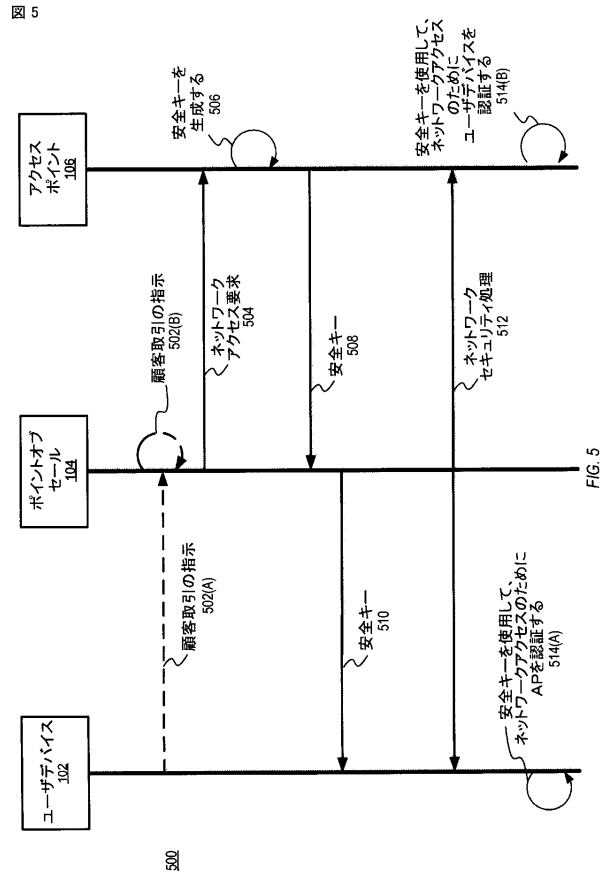

FIG. 5

【図６】

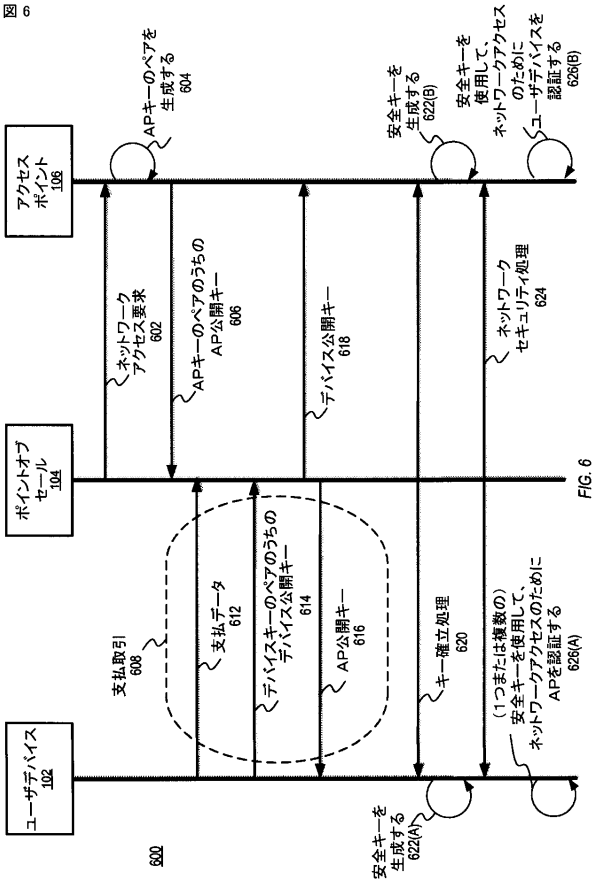

FIG. 6

【図７】

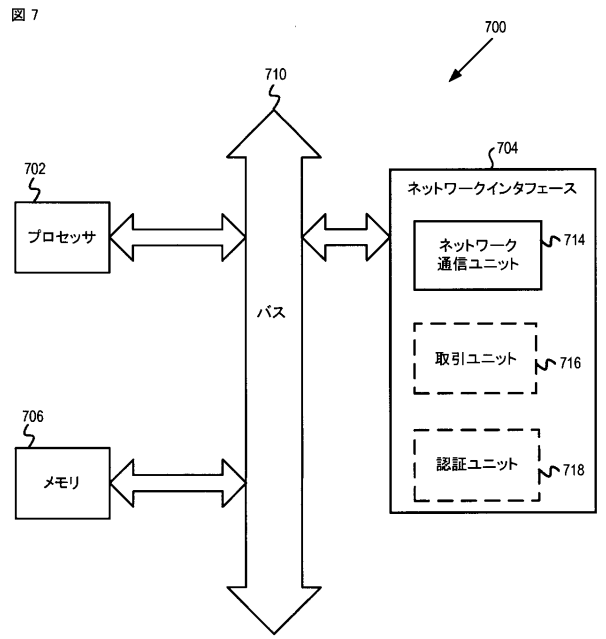

FIG. 7

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/044894

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/04 H04W12/06
ADD. G06Q20/32 H04W84/12

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)
H04W G06F G06Q

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 2013/036231 A1 (SUUMAEKI JAN [FI]) 7 February 2013 (2013-02-07) abstract paragraph [0006] - paragraph [0090] paragraph [0137] - paragraph [0206] paragraph [0237] - paragraph [0259] figures 1A-1J, 6A-6,7 -----	1-30
A	US 2012/284193 A1 (BHARGHAVAN VADUVUR [US] ET AL) 8 November 2012 (2012-11-08) abstract paragraph [0003] paragraph [0011] - paragraph [0038] figure 2 -----	1-30
	-/--	

[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
28 October 2015	05/11/2015

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	Spranger, Stephanie

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/044894

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004/240412 A1 (WINGET NANCY CAM [US]) 2 December 2004 (2004-12-02) abstract paragraph [0018] - paragraph [0024] paragraph [0034] - paragraph [0044] figure 4 -----	1-30

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/044894

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013036231 A1	07-02-2013	EP 2740315 A1	11-06-2014
		US 2013036231 A1	07-02-2013
		WO 2013021094 A1	14-02-2013
US 2012284193 A1	08-11-2012	NONE	
US 2004240412 A1	02-12-2004	AU 2004244634 A1	09-12-2004
		CA 2520772 A1	09-12-2004
		CN 1836404 A	20-09-2006
		EP 1639756 A2	29-03-2006
		US 2004240412 A1	02-12-2004
		US 2007280169 A1	06-12-2007
		WO 2004107780 A2	09-12-2004

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．ＳＭＡＬＬＴＡＬＫ

(72)発明者 ベノワ、オリビエ・ジャン
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ティンナコーンスリスプハプ、ピーラポル
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５

Ｆターム(参考) 5J104 AA16 EA16 EA23 NA02 NA37
5K067 AA21 BB04 DD17 EE02 EE10 HH36
5K201 AA08 AA09 BA17 EB07 EC08 ED05 ED08 EF05