(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2019-508763
(P2019-508763A)
(43)公表日　平成31年3月28日(2019.3.28)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/62	***(2013.01)***	G06F	21/62	318	5J104
H04L 9/32	***(2006.01)***	H04L	9/00	675A	5K067
G06F 21/31	***(2013.01)***	G06F	21/31		
H04W 84/10	***(2009.01)***	H04W	84/10	110	
H04W 76/10	***(2018.01)***	H04W	76/10		

審査請求 有　予備審査請求 未請求　（全 65 頁）　最終頁に続く

(21)出願番号　特願2018-520424 (P2018-520424)
(86)(22)出願日　平成28年12月15日 (2016.12.15)
(85)翻訳文提出日　平成30年5月21日 (2018.5.21)
(86)国際出願番号　PCT/US2016/066896
(87)国際公開番号　WO2017/131887
(87)国際公開日　平成29年8月3日 (2017.8.3)
(31)優先権主張番号　62/288,960
(32)優先日　平成28年1月29日 (2016.1.29)
(33)優先権主張国　米国 (US)

(71)出願人　502208397
グーグル　エルエルシー
アメリカ合衆国　カリフォルニア州　９４０４３　マウンテン　ビュー　アンフィシアター　パークウェイ　１６００
(74)代理人　110001195
特許業務法人深見特許事務所
(72)発明者　ビルギッソン，アーナー
アメリカ合衆国、９４０４３　カリフォルニア州、マウンテン・ビュー、アンフィシアター・パークウェイ、１６００
(72)発明者　グートニク，エフゲニー
アメリカ合衆国、９４０４３　カリフォルニア州、マウンテン・ビュー、アンフィシアター・パークウェイ、１６００
最終頁に続く

(54)【発明の名称】ローカルデバイス認証

(57)【要約】
開示される実施形態では、たとえば、リソースデバイスはマスターアクセストークンを生成および維持し得、マスターアクセストークンはコンピューティングシステムに送信され得る。コンピューティングシステムは、さまざまなアクセス制約に従って、リソースデバイスへの制限のあるアクセスをクライアントデバイスに与えるデータをリソースデバイスのオーナーのデバイスから受信し得る。コンピューティングシステムは、アクセス制約を特定するマスターアクセストークンの制限のあるバージョンを生成し、クライアントデバイスに提供し得る。クライアントデバイスは、直接的なワイヤレス接続を介してリソースデバイスにローカルアクセストークンを提示し得、リソースデバイスは当該トークンを照合し、コンピューティングシステムとの通信なしで、要求されたアクセスを与え得る。

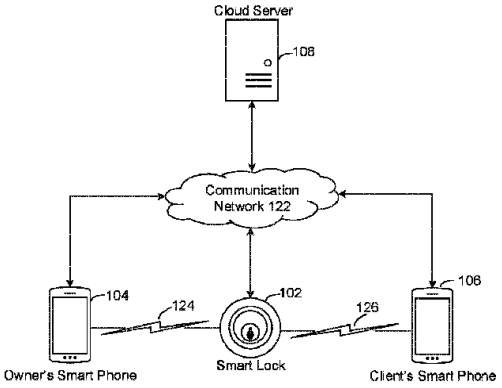

FIG. 1

【特許請求の範囲】
【請求項１】
コンピュータによって実現される方法であって、
装置の１つ以上のプロセッサによって、リソースデバイスについてのマスターアクセストークンを取得することと、
前記１つ以上のプロセッサによって、クライアントデバイスに関連付けられるユーザを識別することと、
前記１つ以上のプロセッサによって、前記ユーザが前記リソースデバイスへの制限のあるアクセスを受けることを承認されていることを決定することと、
前記決定することに応答して、前記１つ以上のプロセッサによって、前記マスターデバイストークンに基づいてローカルアクセストークンを生成することとを含み、前記ローカルアクセストークンは、前記リソースデバイスがネットワーク接続を有することを必要とすることなく、前記リソースデバイスへのアクセスを与えるように構成されており、さらに
前記１つ以上のプロセッサによって、前記リソースデバイスについての前記ローカルアクセストークンを前記クライアントデバイスに提供することを含む、方法。
【請求項２】
前記決定することは、前記リソースデバイスのオーナー、または、前記リソースデバイスへのアクセスをコントロール可能なエンティティのうちの少なくとも一方によって、前記ユーザが前記リソースデバイスへの前記制限のあるアクセスを受けることを承認されていることを決定することを含む、請求項１に記載の方法。
【請求項３】
前記識別することは、前記リソースデバイスへの前記制限のあるアクセスを取得するための要求を前記クライアントデバイスから受信することを含み、前記要求は、前記ユーザの識別子または前記クライアントデバイスの識別子のうちの少なくとも１つを含んでおり、
前記識別することはさらに、前記要求に応答して、前記リソースデバイスについての前記ローカルアクセストークンを前記クライアントデバイスに提供することを含む、請求項１または請求項２に記載の方法。
【請求項４】
前記方法はさらに、
受信した前記要求の少なくとも部分に基づいて前記クライアントデバイスを識別することと、
前記クライアントデバイスが前記リソースデバイスへの前記制限のあるアクセスを受けることを承認されていることを決定することとを含み、
前記生成することは、前記クライアントデバイスが前記制限のあるアクセスを受けることを承認されていることを決定することに応答して、前記ローカルアクセストークンを生成することを含む、請求項３に記載の方法。
【請求項５】
前記リソースデバイスについてのアクセスコントロールリストを取得することをさらに含み、前記アクセスコントロールリストは、前記リソースデバイスへの対応する制限のあるアクセスを受けることを承認されている１人以上のユーザを識別する、請求項１に記載の方法。
【請求項６】
前記装置は、ローカルメモリに前記アクセスコントロールリストを格納するように構成される、請求項５に記載の方法。
【請求項７】
前記決定することは、
前記１人以上の承認されているユーザが、前記クライアントデバイスに関連付けられる前記ユーザを含むということを、前記アクセスコントロールリストに基づいて決定するこ

と、
前記１人以上の承認されているユーザが前記ユーザを含むということを決定することに応答して、前記クライアントデバイスの前記ユーザが前記制限のあるアクセスを受けることを承認されていることを確証することとを含む、請求項５または請求項６に記載の方法。
【請求項８】
前記方法はさらに、オーナーデバイスからアクセスコントロールデータを受信することを含み、前記オーナーデバイスは前記リソースデバイスのオーナーに関連付けられており、前記アクセスコントロールデータは、前記ユーザが前記リソースデバイスへの前記制限のあるアクセスを受けることを承認しており、
前記方法はさらに、前記クライアントデバイスの前記ユーザを承認されたユーザであると識別するために前記アクセスコントロールリストの少なくとも部分を修正することを含む、請求項５～７のいずれか１項に記載の方法。
【請求項９】
前記アクセスコントロールデータはアクセスパラメータを含み、前記アクセスパラメータは、前記ユーザに与えられる前記制限のあるアクセスの範囲を確証し、
前記方法はさらに、前記アクセスパラメータを含むように前記アクセスコントロールリストの少なくとも部分を修正することを含む、請求項８に記載の方法。
【請求項１０】
前記アクセスパラメータは、前記ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含む、請求項９に記載の方法。
【請求項１１】
前記アクセスコントロールリストは、前記ユーザに関連付けられる１つ以上のアクセスパラメータを識別しており、前記アクセスパラメータは、前記ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含む、請求項５に記載の方法。
【請求項１２】
前記ローカルアクセストークンはマカロンを含み、前記マカロンは、１つ以上のキャビアートと、対応するキーとを含み、
前記生成することは、
前記アクセスコントロールリストに基づいて、前記ユーザに関連付けられる前記アクセスパラメータを識別することと、
前記ローカルアクセストークンについての失効時間を確証することと、
前記失効時間および識別された前記アクセスパラメータを前記ローカルアクセストークンの前記１つ以上のキャビアート内に統合する動作を実行することとを含む、請求項１１に記載の方法。
【請求項１３】
前記ユーザの前記ローカルアクセストークンについて確証される前記失効時間を統合するように前記アクセスコントロールリストの少なくとも部分を修正することをさらに含む、請求項１２に記載の方法。
【請求項１４】
前記ローカルアクセストークンは、前記クライアントデバイスに関連付けられる前記ユーザまたは前記クライアントデバイスのうちの少なくとも一方を識別するデータを含んでおり、
前記生成することは、前記ローカルアクセストークンにデジタル署名を適用することを含む、請求項１～７のいずれか１項に記載の方法。
【請求項１５】

前記ローカルアクセストークンはマカロンを含み、前記マカロンは、１つ以上のキャビアートと、対応するキーとを含み、
前記対応するキーは、適用される前記デジタル署名を含んでおり、
前記生成することはさらに、前記１つ以上のキャビアートの少なくとも部分へのＭＡＣアルゴリズムの適用に基づき、前記デジタル署名を生成することを含む、請求項１４に記載の方法。
【請求項１６】
前記１つ以上のキャビアートは、前記トークンの失効日時、前記ユーザに割り当てられる役割、または、前記ユーザもしくは前記クライアントデバイスのうちの少なくとも一方を識別する前記データのうちの少なくとも１つを含む、請求項１５に記載の方法。
【請求項１７】
前記ローカルアクセストークンはデジタル証明書を含む、請求項１～１１のいずれか１項に記載の方法。
【請求項１８】
前記取得することは、前記リソースデバイスから前記マスターアクセストークンを受信することを含み、
前記生成することは、受信した前記マスターアクセストークンの少なくとも部分に基づいて前記ローカルアクセストークンを生成することを含む、請求項１～７のいずれか１項に記載の方法。
【請求項１９】
前記マスターアクセストークンは第１のマカロンを含み、前記第１のマカロンは、１つ以上の第１のキャビアートと、対応する第１のキーとを含み、
前記ローカルアクセストークンは第２のマカロンを含み、前記第２のマカロンは、１つ以上の第２のキャビアートと、対応する第２のキーとを含む、請求項１８に記載の方法。
【請求項２０】
前記ローカルアクセストークンを生成することは、前記１つ以上の第２のキャビアートを生成することを含み、
前記第２のキャビアートの第１の部分は前記第１のキャビアートを含み、
前記第２のキャビアートの第２の部分は、前記ローカルアクセストークンの失効日時と、前記ユーザの前記制限のあるアクセスに関連付けられる１つ以上のアクセスパラメータとを含み、前記アクセスパラメータは、前記ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含む、請求項１９に記載の方法。
【請求項２１】
前記リソースデバイスからマスターデバイストークンを受信することをさらに含み、前記マスターデバイストークンは、前記クライアントデバイスが前記リソースデバイスの識別性を照合することを可能にし、さらに、
前記決定することに応答して、前記マスターデバイストークンの少なくとも部分に基づいてローカルデバイストークンを生成することと、
前記クライアントデバイスに前記ローカルデバイストークンを提供することとを含む、請求項１に記載の方法。
【請求項２２】
少なくとも１つのプロセッサと、
実行可能な命令を格納するメモリとを含み、
前記命令は、前記少なくとも１つのプロセッサによって実行されると、前記少なくとも１つのプロセッサに、
リソースデバイスについてのマスターアクセストークンを取得するステップと、
クライアントデバイスに関連付けられるユーザを識別するステップと、
前記ユーザが前記リソースデバイスへの制限のあるアクセスを受けることを承認され

ていることを決定するステップと、
前記決定することに応答して、前記マスターデバイストークンに基づいてローカルアクセストークンを生成するステップとを行わせ、前記ローカルアクセストークンは、前記リソースデバイスがネットワーク接続を有することを必要とすることなく、前記リソースデバイスへのアクセスを与えるように構成されており、
前記命令はさらに、前記少なくとも１つのプロセッサによって実行されると、前記少なくとも１つのプロセッサに、
前記リソースデバイスについての前記ローカルアクセストークンを前記クライアントデバイスに提供するステップを実行させる、装置。
【請求項２３】
前記少なくとも１つのプロセッサはさらに、前記リソースデバイスのオーナー、または、前記リソースデバイスへのアクセスをコントロール可能なエンティティのうちの少なくとも一方によって、前記ユーザが前記リソースデバイスへの前記制限のあるアクセスを受けることを承認されていることを決定するステップを実行する、請求項２２に記載の装置。
【請求項２４】
前記少なくとも１つのプロセッサはさらに、前記リソースデバイスへの前記制限のあるアクセスを取得するための要求を前記クライアントデバイスから受信するステップを実行し、前記要求は、前記ユーザの識別子または前記クライアントデバイスの識別子のうちの少なくとも１つを含んでおり、
前記少なくとも１つのプロセッサはさらに、前記要求に応答して、前記リソースデバイスについての前記ローカルアクセストークンを前記クライアントデバイスに提供するステップを実行する、請求項２２または請求項２３に記載の装置。
【請求項２５】
前記少なくとも１つのプロセッサはさらに、
受信した前記要求の少なくとも部分に基づいて前記クライアントデバイスを識別するステップと、
前記クライアントデバイスが前記リソースデバイスへの前記制限のあるアクセスを受けることを承認されていることを決定するステップと、
前記クライアントデバイスが前記制限のあるアクセスを受けることを承認されていることを決定することに応答して、前記ローカルアクセストークンを生成するステップとを実行する、請求項２４に記載の装置。
【請求項２６】
前記少なくとも１つのプロセッサはさらに、前記リソースデバイスについてのアクセスコントロールリストを取得するステップを実行し、前記アクセスコントロールリストは、前記リソースデバイスへの対応する制限のあるアクセスを受けることを承認されている１人以上のユーザを識別する、請求項２２に記載の装置。
【請求項２７】
前記装置は、ローカルメモリに前記アクセスコントロールリストを格納するように構成される、請求項２６に記載の装置。
【請求項２８】
前記少なくとも１つのプロセッサはさらに、
前記１人以上の承認されているユーザが、前記クライアントデバイスに関連付けられる前記ユーザを含むということを、前記アクセスコントロールリストに基づいて決定するステップと、
前記１人以上の承認されているユーザが前記ユーザを含むということを決定することに応答して、前記クライアントデバイスの前記ユーザが前記制限のあるアクセスを受けることを承認されていることを確証するステップとを実行する、請求項２６または請求項２７に記載の装置。
【請求項２９】

前記少なくとも１つのプロセッサはさらに、オーナーデバイスからアクセスコントロールデータを受信するステップを実行し、前記オーナーデバイスは前記リソースデバイスのオーナーに関連付けられており、前記アクセスコントロールデータは、前記ユーザが前記リソースデバイスへの前記制限のあるアクセスを受けることを承認しており、
前記少なくとも１つのプロセッサはさらに、前記クライアントデバイスの前記ユーザを承認されたユーザであると識別するために前記アクセスコントロールリストの少なくとも部分を修正するステップを実行する、請求項２６～２８のいずれか１項に記載の装置。
【請求項３０】
前記アクセスコントロールデータはアクセスパラメータを含み、前記アクセスパラメータは、前記ユーザに与えられる前記制限のあるアクセスの範囲を確証し、
前記少なくとも１つのプロセッサはさらに、前記アクセスパラメータを含むように前記アクセスコントロールリストの少なくとも部分を修正するステップを実行する、請求項２９に記載の装置。
【請求項３１】
前記アクセスパラメータは、前記ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含む、請求項３０に記載の装置。
【請求項３２】
前記アクセスコントロールリストは、前記ユーザに関連付けられる１つ以上のアクセスパラメータを識別しており、前記アクセスパラメータは、前記ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含む、請求項２６に記載の装置。
【請求項３３】
前記ローカルアクセストークンはマカロンを含み、前記マカロンは、１つ以上のキャビアートと、対応するキーとを含み、
前記少なくとも１つのプロセッサはさらに、
前記アクセスコントロールリストに基づいて、前記ユーザに関連付けられる前記アクセスパラメータを識別するステップと、
前記ローカルアクセストークンについての失効時間を確証するステップと、
前記失効時間および識別された前記アクセスパラメータを前記ローカルアクセストークンの前記１つ以上のキャビアート内に統合する動作を実行するステップと実行する、請求項３２に記載の装置。
【請求項３４】
前記少なくとも１つのプロセッサはさらに、前記ユーザの前記ローカルアクセストークンについて確証される前記失効時間を統合するように前記アクセスコントロールリストの少なくとも部分を修正するステップを実行する、請求項３３に記載の装置。
【請求項３５】
前記ローカルアクセストークンは、前記クライアントデバイスに関連付けられる前記ユーザまたは前記クライアントデバイスのうちの少なくとも１つを識別するデータを含み、
前記少なくとも１つのプロセッサはさらに、前記ローカルアクセストークンにデジタル署名を適用するステップを実行する、請求項２２～２８のいずれか１項に記載の装置。
【請求項３６】
前記ローカルアクセストークンはマカロンを含み、前記マカロンは、１つ以上のキャビアートと、対応するキーとを含み、
前記対応するキーは、適用された前記デジタル署名を含み、
前記少なくとも１つのプロセッサはさらに、前記１つ以上のキャビアートの少なくとも部分へのＭＡＣアルゴリズムの適用に基づき、前記デジタル署名を生成するステップを実行する、請求項３５に記載の装置。

【請求項３７】
前記１つ以上のキャビアートは、前記トークンの失効日時、前記ユーザに割り当てられる役割、または、前記ユーザもしくは前記クライアントデバイスのうちの少なくとも一方を識別する前記データのうちの少なくとも１つを含む、請求項３６に記載の装置。
【請求項３８】
前記ローカルアクセストークンはデジタル証明書を含む、請求項２２～３５のいずれか１項に記載の装置。
【請求項３９】
前記少なくとも１つのプロセッサはさらに、
前記リソースデバイスから前記マスターアクセストークンを受信するステップと、
受信した前記マスターアクセストークンの少なくとも部分に基づいて前記ローカルアクセストークンを生成するステップとを実行する、請求項２２～２８のいずれか１項に記載の装置。
【請求項４０】
前記マスターアクセストークンは第１のマカロンを含み、前記第１のマカロンは、１つ以上の第１のキャビアートと、対応する第１のキーとを含み、
前記ローカルアクセストークンは第２のマカロンを含み、前記第２のマカロンは、１つ以上の第２のキャビアートと、対応する第２のキーとを含み、
前記少なくとも１つのプロセスはさらに、前記１つ以上の第２のキャビアートを生成するステップを実行し、前記第２のキャビアートの第１の部分は前記第１のキャビアートを含み、前記第２のキャビアートの第２の部分は、前記ローカルアクセストークンの失効日時と、前記ユーザの前記制限のあるアクセスに関連付けられる１つ以上のアクセスパラメータとを含み、前記アクセスパラメータは、前記ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含む、請求項３９に記載の装置。
【請求項４１】
前記少なくとも１つのプロセッサはさらに、前記リソースデバイスからマスターデバイストークンを受信するステップを実行し、前記マスターデバイストークンは、前記クライアントデバイスが前記リソースデバイスの識別性を照合することを可能にし、
前記少なくとも１つのプロセッサはさらに、
前記決定することに応答して、前記マスターデバイストークンの少なくとも部分に基づいてローカルデバイストークンを生成するステップと、
前記クライアントデバイスに前記ローカルデバイストークンを提供するステップとを実行する、請求項２２に記載の装置。
【請求項４２】
命令を格納する有形の一時的でないコンピュータ読取可能媒体であって、前記命令は、装置の少なくとも１つのプロセッサによって実行されると、方法を実行し、
前記方法は、
リソースデバイスについてのマスターアクセストークンを取得することと、
クライアントデバイスに関連付けられるユーザを識別することと、
前記ユーザが前記リソースデバイスへの制限のあるアクセスを受けることを承認されていることを決定することと、
前記決定することに応答して、前記マスターデバイストークンに基づいてローカルアクセストークンを生成することとを含み、前記ローカルアクセストークンは、前記ローカルアクセストークンを有効化するために前記リソースデバイスがネットワーク接続を有することを必要とすることなく、前記リソースデバイスへのアクセスを与えるように構成されており、
前記方法はさらに、
前記リソースデバイスについての前記ローカルアクセストークンを前記クライアントデ

バイスに提供することを含む、有形の一時的でないコンピュータ読取可能媒体。
【請求項４３】
コンピュータによって実現される方法であって、
リソースデバイスの１つ以上のプロセッサによって、クライアントデバイスとのセキュアなワイヤレス接続を確立することと、
前記１つ以上のプロセッサによって、前記クライアントデバイスからのアクセストークンに由来するトークンデータと、前記クライアントデバイスによる前記リソースデバイスへのアクセスの要求とを受信することと、
前記１つ以上のプロセッサによって、ネットワークを介して通信することなく、受信した前記トークンデータが、前記リソースデバイスへのアクセスを承認する有効なトークンに由来すると決定することと、
前記１つ以上のプロセッサによって、前記ネットワークを介して通信することなく、前記アクセストークンが、前記クライアントデバイスによって要求される前記アクセスを提供するのに十分なアクセスのレベルを承認していると決定することと、
受信した前記トークンデータが有効なトークンに由来すると決定することと、前記アクセストークンが前記電子デバイスによって要求される前記アクセスを提供するのに十分なアクセスのレベルを承認していると決定することとに応答して、前記１つ以上のプロセッサによって、前記クライアントデバイスによって要求される前記リソースデバイスへの前記アクセスを提供することとを含む、方法。
【請求項４４】
前記セキュアなワイヤレス接続は、前記クライアントデバイスと前記リソースデバイスとの間の直接的なワイヤレス接続を含む、請求項４３に記載の方法。
【請求項４５】
前記直接的なワイヤレス接続は、ブルートゥースローエナジー（ＢＬＥ： Bluetooth Low Energy）接続を含む、請求項４４に記載の方法。
【請求項４６】
前記確立することは、前記クライアントデバイスからキャビアートデータおよびランダムデータを受信することを含み、前記キャビアートデータは、前記クライアントデバイスによってローカルデバイストークンから抽出され、
前記確立することはさらに、
受信した前記キャビアートおよびランダムデータの少なくとも部分に基づいてキー値を計算することと、
計算された前記キー値を前記クライアントデバイスに送信することと、
計算された前記キー値と、前記ローカルデバイストークンに基づいて前記クライアントデバイスによって計算される付加的なキー値との間の対応に基づき、前記クライアントデバイスとの前記セキュアなワイヤレス接続を確立することとを含む、請求項４３～４５のいずれか１項に記載の方法。
【請求項４７】
計算された前記キー値を、セッションキーとして確証することをさらに含む、請求項４６に記載の方法。
【請求項４８】
前記キャビアートデータおよびランダムデータは、共有された対称キーを使用して暗号化されており、
前記確立することはさらに、
受信した前記キャビアートデータおよびランダムデータを復号化することと、
前記共有された対称キーを使用して、計算された前記キー値を暗号化することと、
暗号化された前記キー値を前記クライアントデバイスに送信することとを含む、請求項４６または請求項４７に記載の方法。
【請求項４９】
アクセストークンはマカロンを含み、前記マカロンは、１つ以上のキャビアートと、対

応するキーとを含む、請求項４３～４５のいずれか１項に記載の方法。
【請求項５０】
ネットワークを介して通信することなく、受信した前記トークンデータが有効なトークンに由来すると決定するステップは、
受信した前記トークンデータから前記１つ以上のキャビアートを抽出することと、
抽出された前記キャビアートと、前記リソースデバイスによって維持されるマスターアクセストークンとに基づき、受信した前記トークンデータのコピーを計算することと、
受信した前記トークンデータが、計算された前記コピーに対応すると決定することと、
受信した前記トークンデータが、計算された前記コピーに対応する場合、受信した前記トークンデータが有効なトークンに由来すると確証することとを含む、請求項４９に記載の方法。
【請求項５１】
ネットワークを介して通信することなく、受信した前記トークンデータが有効なトークンに由来すると決定するステップはさらに、
抽出された前記キャビアートの少なくとも部分に基づいて、受信した前記トークンデータについてのアクセスのチェーンを識別することと、
受信した前記トークンデータについての前記アクセスのチェーンを照合することとを含む、請求項５０に記載の方法。
【請求項５２】
前記１つ以上のキャビアートは、前記アクセストークンの失効日時と、前記リソースデバイスのオーナーによって前記クライアントデバイスに割り当てられる役割と、１つ以上のアクセスパラメータとを含み、
前記アクセスパラメータは、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含み、
前記リソースデバイスへのアクセスの前記要求は、前記リソースデバイスの１つ以上の要求される機能を識別する、請求項４９～５１のいずれか１項に記載の方法。
【請求項５３】
前記アクセストークンが前記十分なアクセスのレベルを承認していると決定するステップは、
前記失効日時に基づいて、前記アクセストークンが失効していないと決定することと、
前記リソースデバイスの要求される機能へアクセスするために前記クライアントデバイスによって必要とされる役割を識別することと、
必要とされる前記役割が、割り当てられる前記役割と一貫していると決定することと、
前記１つ以上の要求される機能が前記１つ以上のアクセスパラメータと一貫していると決定することと、
（ｉ）前記アクセストークンが失効していないという決定と、（ｉｉ）必要とされる前記役割が、割り当てられる前記役割と一貫しているという決定と、（ｉｉｉ）１つ以上の要求される機能が前記１つ以上のアクセスパラメータと一貫しているという決定とに応答して、前記アクセストークンが、前記要求されるアクセスを提供するのに十分なアクセスのレベルを承認していると確証することとを含む、請求項５２に記載の方法。
【請求項５４】
前記リソースデバイスは、クラウドサーバに関連付けられるコンピュータシステム、サードパーティ認証サービス、または、前記リソースデバイスのオーナーのデバイスのうちの少なくとも１つにアクセスコントロールの決定を委任しており、
前記少なくとも１つのコンピュータシステム、サードパーティ認証サービス、または、オーナーデバイスは、前記アクセストークンを生成し、前記クライアントデバイスに前記アクセストークンを提供する、請求項４３～５３のいずれか１項に記載の方法。
【請求項５５】
前記ネットワークを介して通信することなく、前記確立するステップ、前記受信するス

テップおよび前記提供するステップを実行することをさらに含む、請求項４３に記載の方法。
【請求項５６】
リソースデバイスであって、
少なくとも１つのプロセッサと、
実行可能な命令を格納するメモリとを含み、前記命令は、前記少なくとも１つのプロセッサによって実行されると、前記少なくとも１つのプロセッサに、
クライアントデバイスとのセキュアなワイヤレス接続を確立するステップと、
前記クライアントデバイスからのアクセストークンに由来するトークンデータと、前記クライアントデバイスによる前記リソースデバイスへのアクセスの要求とを受信するステップと、
ネットワークを介して通信することなく、受信した前記トークンデータが、前記リソースデバイスへのアクセスを承認する有効なトークンに由来していると決定するステップと、
前記ネットワークを介して通信することなく、前記アクセストークンが、前記クライアントデバイスによって要求される前記アクセスを提供するのに十分なアクセスのレベルを承認していると決定するステップと、
受信した前記トークンデータが有効なトークンに由来すると決定することと、前記アクセストークンが前記電子デバイスによって要求される前記アクセスを提供するのに十分なアクセスのレベルを承認していると決定することとに応答して、前記クライアントデバイスによって要求される前記リソースデバイスへのアクセスを提供するステップとを実行させる、リソースデバイス。
【請求項５７】
前記セキュアなワイヤレス接続は、前記クライアントデバイスと前記リソースデバイスとの間の直接的なワイヤレス接続を含む、請求項５６に記載のリソースデバイス。
【請求項５８】
前記直接的なワイヤレス接続は、ブルートゥースローエナジー（ＢＬＥ： Bluetooth Low Energy）接続を含む、請求項５７に記載のリソースデバイス。
【請求項５９】
前記少なくとも１つのプロセッサはさらに、
前記クライアントデバイスからキャビアートデータおよびランダムデータを受信するステップを実行し、前記キャビアートデータは、前記クライアントデバイスによってローカルデバイストークンから抽出され、
前記少なくとも１つのプロセッサはさらに、
受信した前記キャビアートおよびランダムデータの少なくとも部分に基づいてキー値を計算するステップと、
計算された前記キー値を前記クライアントデバイスに送信するステップと、
計算された前記キー値と、前記ローカルデバイストークンに基づいて前記クライアントデバイスによって計算される付加的なキー値との間の対応に基づき、前記クライアントデバイスとの前記セキュアなワイヤレス接続を確立するステップとを実行する、請求項５６～５８のいずれか１項に記載のリソースデバイス。
【請求項６０】
前記少なくとも１つのプロセッサはさらに、計算された前記キー値を、セッションキーとして確証するステップを実行する、請求項５９に記載のリソースデバイス。
【請求項６１】
前記キャビアートデータおよびランダムデータは、共有された対称キーを使用して暗号化されており、
前記少なくとも１つのプロセッサはさらに、
受信した前記キャビアートデータおよびランダムデータを復号化するステップと、
前記共有された対称キーを使用して、計算された前記キー値を暗号化するステップと、

暗号化された前記キー値を前記クライアントデバイスに送信するステップとを実行する、請求項５９または請求項６０に記載のリソースデバイス。

【請求項６２】

アクセストークンはマカロンを含み、前記マカロンは、１つ以上のキャビアートと、対応するキーとを含む、請求項５６～５８のいずれか１項に記載のリソースデバイス。

【請求項６３】

前記少なくとも１つのプロセッサはさらに、

前記アクセストークンからの前記１つ以上のキャビアートを識別するステップと、

抽出された前記キャビアートと、前記リソースデバイスによって維持されるマスターアクセストークンとに基づき、受信した前記トークンデータのコピーを計算するステップと、

受信した前記トークンデータが計算された前記コピーに対応すると決定するステップと、

受信した前記トークンデータが計算された前記コピーに対応する場合、受信した前記トークンデータが有効なトークンに由来すると確証するステップとを実行する、請求項６２に記載のリソースデバイス。

【請求項６４】

前記少なくとも１つのプロセッサはさらに、

抽出された前記キャビアートの少なくとも部分に基づいて、前記アクセストークンについてのアクセスのチェーンを識別するステップと、

受信した前記トークンについての前記アクセスのチェーンを照合するステップとを実行する、請求項６３に記載のリソースデバイス。

【請求項６５】

前記１つ以上のキャビアートは、前記アクセストークンの失効日時と、前記リソースデバイスのオーナーによって前記クライアントデバイスに割り当てられる役割と、１つ以上のアクセスパラメータとを含み、

前記アクセスパラメータは、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含み、

前記リソースデバイスへのアクセスの前記要求は、前記リソースデバイスの１つ以上の要求される機能を識別する、請求項６２～６４のいずれか１項に記載のリソースデバイス。

【請求項６６】

前記少なくとも１つのプロセッサはさらに、

前記失効日時に基づいて、前記アクセストークンが失効していないと決定するステップと、

前記リソースデバイスの要求される機能へアクセスするために前記クライアントデバイスによって必要とされる役割を識別するステップと、

必要とされる前記役割が、割り当てられる前記役割と一貫していると決定するステップと、

前記１つ以上の要求される機能が前記１つ以上のアクセスパラメータと一貫していると決定するステップと、

（ｉ）前記アクセストークンが失効していないという決定と、（ｉｉ）必要とされる前記役割が、割り当てられる前記役割と一貫しているという決定と、（ｉｉｉ）１つ以上の要求される機能が前記１つ以上のアクセスパラメータと一貫しているという決定とに応答して、前記アクセストークンが、前記要求されるアクセスを提供するのに十分なアクセスのレベルを承認していると確証するステップとを実行する、請求項６５に記載のリソースデバイス。

【請求項６７】

前記リソースデバイスは、クラウドサーバに関連付けられるコンピュータシステム、サ

ードパーティ認証サービス、または、前記リソースデバイスのオーナーのデバイスのうちの少なくとも１つにアクセスコントロールの決定を委任しており、
前記少なくとも１つのコンピュータシステム、サードパーティ認証サービス、または、オーナーデバイスは、前記アクセストークンを生成し、前記クライアントデバイスに前記アクセストークンを提供する、請求項５６～６６のいずれか１項に記載のリソースデバイス。
【請求項６８】
前記少なくとも１つのプロセッサはさらに、前記ネットワークを介して通信することなく、前記確立するステップ、前記受信するステップおよび前記提供するステップを実行する、請求項５６～６７のいずれか１項に記載のリソースデバイス。
【請求項６９】
命令を格納する有形の一時的でないコンピュータ読取可能媒体であって、前記命令は、クライアントデバイスの少なくとも１つのプロセッサによって実行されると、方法を実行し、前記方法は、
クライアントデバイスとのセキュアなワイヤレス接続を確立することと、
前記クライアントデバイスからのアクセストークンに由来するトークンデータと、前記クライアントデバイスによる前記リソースデバイスへのアクセスの要求とを受信することと、
ネットワークを介して通信することなく、受信した前記トークンデータが、前記リソースデバイスへのアクセスを承認する有効なトークンに由来していると決定することと、
前記ネットワークを介して通信することなく、前記アクセストークンが、前記クライアントデバイスによって要求される前記アクセスを提供するのに十分なアクセスのレベルを承認していると決定することと、
受信した前記トークンデータが有効なトークンに由来すると決定することと、前記アクセストークンが前記電子デバイスによって要求される前記アクセスを提供するのに十分なアクセスのレベルを承認していると決定することとに応答して、前記クライアントデバイスによって要求される前記リソースデバイスへの前記アクセスを提供することとを含む、コンピュータ読取可能媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願への相互参照
この出願は、２０１６年１月２９日に出願された米国仮特許出願第６２／２８８，９６０号の優先権および完全な利益を主張しており、その全内容が本願明細書において参照により援用される。
【０００２】
分野
この明細書は、ローパワーネットワークを介するワイヤレス通信に関する技術を記載する。
【背景技術】
【０００３】
背景
スマートロック、スマート家電（たとえば洗濯機、ストーブ、冷蔵庫など）、スマートサーモスタット、ならびに、リモートコントロール、リモートセンシングおよびリモートオペレーションが可能である他のデバイスといったローパワーデバイスが、ますます一般的になっており、日常生活へ統合されている。これらのデバイスの処理能力の制限と、これらのデバイスが動作する（たとえばブルートゥース（登録商標）ローエナジー（ＢＬＥ：Bluetooth low energy）ネットワークのような）ローパワーネットワークによるデータ転送に課される帯域幅の制限とにより、多くの一般的なローパワーデバイスは、従来のアクセスコントロールプロセスを実現することができない場合がある。

【発明の概要】
【課題を解決するための手段】
【０００４】
概要
開示される実施形態は、スマートロック、スマート家電（たとえば洗濯機、ストーブ、冷蔵庫など）、スマートサーモスタット、ならびに、リモートオペレーションおよびリモートコントロールが可能である他のデバイスといったローパワーデバイスが、クラウドネットワークを維持するコンピューティングシステムのような１つ以上の付加的なデバイスにアクセスコントロールの決定を委任することを可能にするコンピュータ化されたプロセスに関する。開示される実施形態によると、ローパワーデバイス（たとえばリソースデバイス）が、１つ以上のマスタートークンを生成しローカルに格納し得る。マスタートークンの例としては、他のデバイスがローパワーデバイスの識別性を照合することを可能にするマスターデバイストークンと、他のデバイスがローパワーデバイスにアクセス可能にすることを確証するマスターアクセストークンとがある。リソースデバイスはたとえば、コンピューティングシステムにそのマスタートークンを送信することによって、コンピューティングシステムのうちの１つにそのアクセスコントロールの決定を委任し得る。コンピューティングシステムは、受信したマスタートークンを格納し得るとともに、リソースデバイスにアクセスすることが承認されたデバイスと、承認されたアクセスにリソースデバイスのオーナーによって課されるさまざまな制限および制約とを識別するアクセスコントロールリストをリソースデバイスに代わって維持し得る。
【０００５】
リソースデバイスにアクセスするためのクライアントデバイスからの要求を受信すると、コンピューティングシステムは、いくつかの局面において、オーナーがリソースデバイスへの制限のあるアクセスをクライアントデバイスに与えたことを確証するだけでなく、要求されたアクセスが、リソースデバイスのオーナーによって課されるさまざまな制限および制約と一貫していることを確証し得る。当該与えられた制限のあるアクセスを促進するために、コンピュータシステムは、マスターデバイストークンに基づいたローカルデバイストークンと、マスターアクセストークンに基づいたローカルアクセストークンとを生成または作り出し（mint）得る。ローカルデバイストークンは、クライアントデバイスが、たとえばローパワーＢＬＥネットワークのような直接的なデバイスツーデバイスワイヤレス接続を介して、リソースデバイスとのセキュアな直接的な接続を確立することを可能にし得る。また、ローカルアクセストークンは、さまざまな課された制約および制限を特定する「短命な（short-lived）」トークンであり得る。クライアントデバイスは、ローパワーネットワークを介してリソースデバイスにこれらのローカルトークンを提示し得、コンピューティングデバイスとの通信なしでまたはネットワークアクセスなしで、課された制約および制限に従ってアクセスをネゴシエーションし得る。
【０００６】
１つの一般的な局面では、コンピュータによって実現される方法は、装置の１つ以上のプロセッサによって、リソースデバイスについてのマスターアクセストークンを取得することと、１つ以上のプロセッサによって、クライアントデバイスに関連付けられるユーザを識別することと、１つ以上のプロセッサによって、ユーザがリソースデバイスへの制限のあるアクセスを受けることを承認されていることを決定することとを含む。決定することに応答して、上記方法は、１つ以上のプロセッサによって、マスターデバイストークンに基づいてローカルアクセストークンを生成し得る。いくつかの局面において、ローカルアクセストークンは、リソースデバイスがネットワーク接続を有することを必要とすることなく、リソースデバイスへのアクセスを与えるように構成され得る。上記方法はさらに、１つ以上のプロセッサによって、リソースデバイスについてのローカルアクセストークンをクライアントデバイスに提供することを含む。リソースデバイスはローパワーリソースデバイスであり得る。
【０００７】

いくつかの実現例では、開示される方法は、リソースデバイスのオーナー、または、リソースデバイスへのアクセスをコントロール可能なエンティティのうちの少なくとも一方によって、ユーザがリソースデバイスへの制限のあるアクセスを受けることを承認されていることを決定することを含み得る。

【０００８】

いくつかの実現例では、開示される方法は、リソースデバイスについて制限のあるアクセスを取得するための要求をクライアントデバイスから受信することと、要求に応答して、リソースデバイスについてのローカルアクセストークンをクライアントデバイスに提供することとを含み得る。ある局面では、当該要求は、ユーザの識別子またはクライアントデバイスの識別子のうちの少なくとも１つを含み得る。リソースデバイスについてのローカルアクセストークンは、要求に応答して、クライアントデバイスに提供され得る。

【０００９】

いくつかの実現例において、開示される方法は、受信した要求の少なくとも部分に基づいてクライアントデバイスを識別することと、クライアントデバイスがリソースデバイスへの制限のあるアクセスを受けることを承認されていることを決定することと、クライアントデバイスが制限のあるアクセスを受けることを承認されていることを決定することに応答して、ローカルアクセストークンを生成することとを含み得る。

【００１０】

いくつかの実現例では、開示される方法は、リソースデバイスについてのアクセスコントロールリストを取得することを含み得る。いくつかの局面では、アクセスコントロールリストは、リソースデバイスへの対応する制限のあるアクセスを受けることを承認されている１人以上のユーザを識別し得る。

【００１１】

いくつかの実現例では、装置は、ローカルメモリにアクセスコントロールリストを格納するように構成される。

【００１２】

いくつかの実現例では、開示される方法は、１人以上の承認されているユーザが上記ユーザを含むということを、アクセスコントロールリストに基づいて決定することと、１人以上の承認されているユーザが上記ユーザを含むということを決定することに応答して、クライアントデバイスのユーザが制限のあるアクセスを受けることを承認されていることを確証することとを含み得る。

【００１３】

いくつかの実現例では、開示される方法は、リソースデバイスのオーナーに関連付けられるオーナーデバイスからアクセスコントロールデータを受信することと、クライアントデバイスのユーザを承認されたユーザであると識別するためにアクセスコントロールリストの少なくとも部分を修正することとを含み得る。いくつかの局面では、アクセスコントロールデータは、ユーザがリソースデバイスへの制限のあるアクセスを受けることを承認し得る。

【００１４】

いくつかの実現例では、アクセスコントロールデータはアクセスパラメータを含み得、アクセスパラメータは、ユーザに与えられる制限されたアクセスの範囲を確立し得る。開示される方法はさらに、アクセスパラメータを含むようにアクセスコントロールリストの少なくとも部分を修正することを含み得る。

【００１５】

いくつかの実現例では、アクセスパラメータは、ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含み得、アクセスコントロールリストは、ユーザに関連付けられる１つ以上のアクセスパラメータを識別し得る。

【００１６】

いくつかの実現例において、ローカルアクセストークンは、１つ以上のキャビアートおよび対応するキーを含むマカロンを含み得、開示される方法は、アクセスコントロールリストに基づいて、ユーザに関連付けられるアクセスパラメータを識別し、ローカルアクセストークンについての失効時間を確証し、失効時間および識別されたアクセスパラメータをローカルアクセストークンの１つ以上のキャビアート内に統合する動作を実行し得る。

【００１７】

いくつかの実現例では、開示される方法は、ユーザのローカルアクセストークンについて確証される失効時間を統合するようにアクセスコントロールリストの少なくとも部分を修正することを含み得る。

【００１８】

いくつかの実現例では、ローカルアクセストークンは、ユーザまたはクライアントデバイスの少なくとも一方を識別するデータを含み得、開示される方法はローカルアクセストークンにデジタル署名を適用することを含み得る。

【００１９】

いくつかの実現例では、ローカルアクセストークンはたとえば、１つ以上のキャビアートおよび対応するキーを含むマカロンを含み得、対応するキーは、適用されたデジタル署名を含み得、開示される方法は、１つ以上のキャビアートの少なくとも部分へのＭＡＣアルゴリズムの適用に基づき、デジタル署名を生成することを含み得る。

【００２０】

いくつかの実現例では、１つ以上のキャビアートは、トークンの失効日時、ユーザに割り当てられる役割、または、ユーザもしくはクライアントデバイスのうちの少なくとも一方を識別するデータのうちの少なくとも１つを含み得る。

【００２１】

いくつかの実現例では、ローカルアクセストークンはデジタル証明書を含み得る。

いくつかの実現例では、開示される方法は、リソースデバイスからマスターアクセストークンを受信することと、マスターアクセストークンの少なくとも部分に基づいてローカルアクセストークンを生成することとを含み得る。

【００２２】

いくつかの実現例では、マスターアクセストークンはたとえば、１つ以上の第１のキャビアートおよび対応する第１のキーを有する第１のマカロンを含み得、ローカルアクセストークンは第２のマカロンを含み得、第２のマカロンは、１つ以上の第２のキャビアートと、対応する第２のキーとを含む。

【００２３】

いくつかの実現例では、第２のキャビアートは、第１のキャビアートと、ローカルアクセストークンの失効日時と、ユーザの制限のあるアクセスに関連付けられる１つ以上のアクセスパラメータとを含み得、当該アクセスパラメータは、ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含み得る。

【００２４】

いくつかの実現例では、開示される方法は、クライアントデバイスがリソースデバイスの識別性を照合することを可能にするマスターデバイストークンをリソースデバイスから受信することと、決定することに応答して、マスターデバイストークンの少なくとも部分に基づいてローカルデバイストークンを生成することと、クライアントデバイスにローカルデバイストークンを提供することとを含み得る。

【００２５】

別の一般的な局面では、コンピュータによって実現される方法は、リソースデバイスの１つ以上のプロセッサによって、クライアントデバイスとのセキュアなワイヤレス接続を確立することと、１つ以上のプロセッサによって、クライアントデバイスからのアクセストークンに由来するトークンデータと、クライアントデバイスによるリソースデバイスへ

のアクセスの要求とを受信することと、１つ以上のプロセッサによって、ネットワークを介して通信することなく、受信したトークンデータが、リソースデバイスへのアクセスを承認する有効なトークンに由来すると決定することと、１つ以上のプロセッサによって、ネットワークを介して通信することなく、アクセストークンが、クライアントデバイスによって要求されるアクセスを提供するのに十分なアクセスのレベルを承認していると決定することを含む。受信したトークンデータが有効なトークンに由来すると決定することと、アクセストークンが電子デバイスによって要求されるアクセスを提供するのに十分なアクセスのレベルを承認していると決定することとに応答して、上記方法はさらに、１つ以上のプロセッサによって、クライアントデバイスによって要求されるリソースデバイスへのアクセスを提供することとを含み得る。

【００２６】

いくつかの実現例では、セキュアなワイヤレス接続は、クライアントデバイスとリソースデバイスとの間の直接的なワイヤレス接続を含み得る。

【００２７】

いくつかの実現例では、直接的なワイヤレス接続は、ブルートゥースローエナジー（ＢＬＥ：Bluetooth Low Energy）接続を含み得る。

【００２８】

いくつかの実現例では、開示される方法はさらに、クライアントデバイスからキャビアートデータおよびランダムデータを受信することを含み、キャビアートデータは、クライアントデバイスによってローカルデバイストークンから抽出され、上記方法はさらに、受信したキャビアートおよびランダムデータの少なくとも部分に基づいてキー値を計算することと、計算されたキー値をクライアントデバイスに送信することと、計算されたキー値と、ローカルデバイストークンに基づいてクライアントデバイスによって計算される付加的なキー値との間の対応に基づき、クライアントデバイスとのセキュアなワイヤレス接続を確立することとを含み得る。

【００２９】

いくつかの実現例では、開示される方法は、計算されたキー値を、セッションキーとして確証することを含み得る。

【００３０】

いくつかの実現例では、キャビアートデータおよびランダムデータは、共有された対称キーを使用して暗号化され得、開示される方法は、受信したキャビアートデータおよびランダムデータを復号化することと、共有された対称キーを使用して、計算されたキー値を暗号化することと、暗号化されたキー値をクライアントデバイスに送信することとを含む。

【００３１】

いくつかの実現例では、リソースデバイスは、クラウドサーバに関連付けられるコンピュータシステム、サードパーティ認証サービス、または、リソースデバイスのオーナーのデバイスのうちの少なくとも１つにアクセスコントロールの決定を委任しており、少なくとも１つのコンピュータシステム、サードパーティ認証サービス、または、オーナーデバイスは、アクセストークンを生成し、クライアントデバイスにアクセストークンを提供する。

【００３２】

いくつかの実現例では、開示される方法は、ネットワークを介して通信することなく、確立するステップ、受信するステップおよび提供するステップを実行することを含み得る。

【００３３】

いくつかの実現例では、アクセストークンは、１つ以上のキャビアートおよび対応するキーを有するマカロンを含む。

【００３４】

いくつかの実現例では、ネットワークを介して通信することなく、受信したトークンデ

ータが有効なトークンに由来すると決定するステップは、受信したトークンデータから１つ以上のキャビアートを抽出することと、抽出されたキャビアートと、リソースデバイスによって維持されるマスターアクセストークンとに基づき、受信したトークンデータのコピーを計算することと、受信したトークンデータが、計算されたコピーに対応すると決定することと、受信したトークンデータが、計算されたコピーに対応する場合、受信したトークンデータが有効なトークンに由来すると確証することとを含み得る。

【００３５】

いくつかの実現例では、ネットワークを介して通信することなく、受信したトークンデータが有効なトークンに由来すると決定するステップは、抽出されたキャビアートの少なくとも部分に基づいて、受信したアクセストークンについてのアクセスのチェーンを識別することと、受信したトークンについてのアクセスのチェーンを照合することとをさらに含み得る。

【００３６】

いくつかの実現例では、１つ以上のキャビアートは、アクセストークンの失効日時と、リソースデバイスのオーナーによってクライアントデバイスに割り当てられる役割と、１つ以上のアクセスパラメータとを含み得、アクセスパラメータは、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含み、リソースデバイスへのアクセスの要求は、リソースデバイスの１つ以上の要求される機能を識別する。

【００３７】

いくつかの実現例では、アクセストークンが十分なアクセスのレベルを承認していると決定するステップは、失効日時に基づいて、アクセストークンが失効していないと決定することと、リソースデバイスの要求される機能へアクセスするためにクライアントデバイスによって必要とされる役割を識別することと、必要とされる役割が、割り当てられる役割と一貫していると決定することと、１つ以上の要求される機能が１つ以上のアクセスパラメータと一貫していると決定することと、（ｉ）アクセストークンが失効していないという決定と、（ｉｉ）必要とされる役割が、割り当てられる役割と一貫しているという決定と、（ｉｉｉ）１つ以上の要求される機能が１つ以上のアクセスパラメータと一貫しているという決定とに応答して、アクセストークンが、要求されるアクセスを提供するのに十分なアクセスのレベルを承認していると確証することを含み得る。

【００３８】

いくつかの実現例では、リソースデバイスは、クラウドサーバに関連付けられるコンピュータシステム、サードパーティ認証サービス、または、リソースデバイスのオーナーのデバイスのうちの少なくとも１つにアクセスコントロールの決定を委任しており、少なくとも１つのコンピュータシステム、サードパーティ認証サービス、または、オーナーデバイスは、アクセストークンを生成し、クライアントデバイスにアクセストークンを提供する。

【００３９】

他の実施形態において、対応するシステム、デバイスおよびコンピュータプログラムは、コンピュータストレージデバイス上でエンコードされる方法のアクションを実行するように構成され得る。１つ以上のプロセッサを有するデバイスは、デバイスにインストールされたソフトウェア、ファームウェア、ハードウェアまたはそれらの組み合わせによりそのように構成され得、当該ソフトウェア、ファームウェア、ハードウェアまたはそれらの組み合わせは、動作において当該デバイスに上記アクションを実行させる。１つ以上のコンピュータプログラムは、デバイスによって実行されると、デバイスにアクションを実行させる命令を有することによって、そのように構成され得る。

【００４０】

本願明細書において開示される技術の実現例は、以下の利点の１つ以上を提供し得る。デバイスはリモートシステムにアクセスコントロールの決定を委任し得る。これにより、デバイスについて洗練されたセキュリティおよびアクセスコントロールが可能になる一方

、デバイス上での電力需要、処理需要およびネットワーク帯域幅需要が低減される。当該システムにより、特定の許可または制約が与えられることを可能にするきめ細かいアクセスコントロールが可能になる。さらに、当該システムにより、さまざまな条件あるいは制約に従って、承認されたユーザが、他者に制限のあるアクセスを委任することが可能になる。さらに、リモートシステムがユーザまたはデバイスに認証を与える決定をしているが、当該セキュリティスキームは、リモートシステムとセキュアにされるデバイスとの間の通信が必要ではないように構成されている。すなわち、アクセスが要求されると、セキュアにされるデバイスは、要求を行った側が、その後にリモートシステムと通信することなく承認されるかどうか決定し得る。これにより、当該認証スキームは、ネットワーク接続がない状態でも有効である。さらに、ネットワーク接続がなくても認証を実行する能力により、電力需要が低減され得、これは小さいデバイスまたはバッテリ給電のデバイスに特に有利である。

【００４１】

この明細書に記載される主題の１つ以上の実施形態の詳細は、添付の図面および以下の説明において記載される。当該主題の他の潜在的な特徴、局面および利点は、説明、図面および請求の範囲から明白になるであろう。

【図面の簡単な説明】

【００４２】

【図１】例示的なコンピューティングシステムの図である。

【図２】デバイス間での、アクセスコントロールの決定の委任を促進するデータの例示的な交換を示す図である。

【図３】リソースデバイスから１つ以上のコンピューティングデバイスにアクセスコントロールの決定を委任するための例示的なプロセスのフローチャートの図である。

【図４】クライアントデバイスによるリソースデバイスのトークンベースのアクセスを促進するデータの例示的な交換を示す図である。

【図５】リソースデバイスへのアクセスを与えるための例示的なプロセスのフローチャートの図である。

【図６】この明細書に記載されるシステムおよび方法を実現するために使用され得るコンピューティングデバイスのブロック図である。

【発明を実施するための形態】

【００４３】

さまざまな図面における同様の参照番号および参照符号は同様の要素を示す。

詳細な説明

図１は、リソースデバイスから１つ以上の他のデバイスおよび／またはコンピュータシステムにアクセスコントロールの決定を委任し、かつ、ネットワークアクセスを必要とすることなく、リソースデバイスにアクセスを与えるデバイス固有のトークンを提供するための例示的なシステム１００を示す。たとえば、システム１００は、リソースデバイス１０２と、オーナーデバイス１０４と、クライアントデバイス１０６と、コンピューティングシステム１０８と、システム１００のコンポーネントのうちの１つ以上を相互接続することが可能である通信ネットワーク１２２とを含み得る。

【００４４】

さらに、ある局面では、システム１００は、システム１００の１つ以上のコンポーネントを直接的に接続することができる１つ以上のローカルワイヤレス通信ネットワーク（たとえばワイヤレスピアツーピア接続など）を含み得る。たとえば、図１において、システム１００は、リソースデバイス１０２およびオーナーデバイス１０４を直接的に接続するローカルワイヤレス通信ネットワーク１２４を含み得、付加的または代替的には、リソースデバイス１０２およびクライアントデバイス１０６を直接的に接続するローカルワイヤレス通信ネットワーク１２６を含み得る。しかしながら、開示される実施形態は、これらの例示的なローカルワイヤレス通信ネットワークに限定されず、他の局面において、システム１００は、システム１００のコンポーネントに適切な付加的または代替的な数のロー

カルワイヤレス通信ネットワークを含んでもよい。

【００４５】

一般に、リソースデバイス１０２は、たとえばルートキーといった、リソースデバイス１０２のみが知っている秘密を生成または維持し得る。リソースデバイス１０２は、ルートキーに由来するマスターキーまたはマスタートークンを生成する。その後、リソースデバイス１０２は、信頼された機構（trusted authority）にマスタートークンを送信して、当該信頼された機構にアクセス管理権を委任する。いくつかの実現例では、当該信頼された機構は、コンピューティングシステム１０８のような、インターネットによってアクセス可能なリモートサーバシステムである。委任が完了した後、信頼された機構は、リソースデバイス１０２とコンタクトすることなく、リソースデバイス１０２にアクセスするための任意数のアクセスキーあるいはアクセストークンを生成することが可能になる。リソースデバイス１０２は、新しいアクセストークンが生成される時に、オフまたはオフラインであり得る。

【００４６】

その後、別のパーティがリソースデバイス１０２へのアクセスを要求する際には、要求を行ったパーティーは、信頼された機構から取得されるアクセストークンを提示する。アクセストークンから、リソースデバイス１０２は、（ｉ）アクセストークンがデバイスルートキーに由来しているということと、（ｉｉ）アクセストークンが適切なアクセス管理機構によって発行されたものであるということとを照合することが可能である。さらに、リソースデバイス１０２は、アクセストークンを提示したものに与えられるアクセス権、権限および制約を決定することが可能である。これにより、リソースデバイス１０２は、アクセストークンに基づいて、アクセス管理権が委任された信頼された機構と通信することなく、アクセスを提供するべきかどうかと、どの範囲のアクセスを提供するべきかどうかとを決定することを可能になる。

【００４７】

いくつかの局面において、リソースデバイス１０２は、（たとえば、ローパワーマイクロコントローラユニット（ＭＣＵ： microcontroller unit）および／またはシステムオンチップ（ＳｏＣ：system-on-chip）によって動作される）ローパワーデバイスを含み得、当該ローパワーデバイスは、通信ネットワーク１２２を介してシステム１００のコンポーネントとの通信を確立するように構成され得、付加的または代替的には、ローカルワイヤレス通信ネットワーク１２４および１２６を介して直接的な接続を確立するように構成され得る。たとえば、ローパワーデバイスは、バッテリ給電のデバイス、またはそうでなければ、電力が抑制されているデバイスであり得る。例として、リソースデバイス１２２は、ワイヤレススピーカーのセットと、ワイヤレスプリンタまたは他の電子デバイスと、スマートロックと、スマート家電（たとえば冷蔵庫、ストーブおよび／または洗濯機）と、スマートサーモスタットまたは他のセンサと、たとえばネットワーク１２２を介したコンピューティングシステム１０８との通信、ローカルワイヤレス通信ネットワーク１２４を介したオーナーデバイス１０４との直接的な通信、付加的または代替的には、ローカルワイヤレス通信ネットワーク１２６を介したクライアントデバイス１０６との直接的な通信を確立することが可能である任意の付加的または代替的なデバイス（たとえばインターネットオブシングス（ＩＯＴ： Internet-of-Things）接続デバイス）とを含み得るが、これらに限定されない。いくつかの実現例において、リソースデバイス１０２は、ＷｅａｖｅまたはμＷｅａｖｅプロトコルに従って「サーバ」デバイスとして機能し得る。

【００４８】

オーナーデバイス１０４およびクライアントデバイス１０６は、携帯電話と、スマートフォンと、タブレットコンピュータと、デスクトップコンピュータと、ラップトップコンピュータと、タブレットコンピュータと、ウェアラブルコンピュータと、音楽プレーヤと、ｅブックリーダと、ナビゲーションシステムと、または、通信ネットワーク１２２、ローカルワイヤレス通信ネットワーク１２４および／もしくはローカルワイヤレス通信ネットワーク１２６を介してシステム１００のコンポーネントとの通信を確立可能である任意

の他の適切なコンピューティングデバイスとを含み得るが、これらに限定されない。さらに、コンピューティングシステム１０８は、開示される実施形態に係る１つ以上のプロセスを実行するよう、メモリに格納されるソフトウェア命令を実行するように構成されるとともに、ネットワーク１２２を介してシステム１００の１つ以上のコンポーネントと通信するように構成される１つ以上のコンピュータシステムを含み得る。

【００４９】

さらに、ある局面では、ローカルネットワーク１２４および／または１２６は、ブルートゥースローエナジー（ＢＬＥ）ネットワークのようなワイヤレスパーソナルエリアネットワーク（ＰＡＮ： personal area network）を含み得る。他の局面において、開示される実施形態によると、ネットワーク１２２、付加的または代替的には、ローカルネットワーク１２４および１２６の１つ以上は、たとえば「Ｗｉ－Ｆｉ（登録商標）」ネットワークのようなワイヤレスローカルエリアネットワーク（ＬＡＮ： local area network）と、ＲＦネットワークと、ニアフィールド通信（ＮＦＣ： Near Field Communication）ネットワークと、複数のワイアレスＬＡＮを接続するワイヤレスメトロポリタンエリアネットワーク（ＭＡＮ： Metropolitan Area Network）と、たとえばインターネットのようなワイドエリアネットワーク（ＷＡＮ： wide area network）とを含み得るが、これらに限定されない。

【００５０】

いくつかの実施形態において、システム１００のコンポーネントは、クライアントデバイス１０６にアクセスコントロール権限を与えるとともに与えられたアクセスコントロール権限に従ってクライアントデバイス１０６がリソースデバイス１０２にアクセスすることを可能にするアクセスコントロールプロトコルを実現し得る。例として、従来のアクセスコントロールプロセスは、１つ以上の承認されたデバイス（たとえばクライアントデバイス１０６）と、これらの承認されたデバイスに提供されるアクセスのレベルとを識別するアクセスコントロールリスト（たとえばＡＣＬ）を維持するために、アクセス可能なデバイス（たとえばリソースデバイス１０２）を必要とし得る。デバイスからのアクセス要求を受信すると、アクセス可能なデバイスは、ＡＣＬを解析して、要求を行ったデバイスが承認されたデバイスかどうか決定し、承認されたデバイスであれば、要求を行ったデバイスに与えられるアクセスのレベルおよび／またはタイプを決定し得る。

【００５１】

しかしながら、上述したように、リソースデバイス１０２は、ローパワーＭＣＵおよびＳｏＣによって動作されるデバイスを含み得る。これらのローパワーＭＣＵおよび／またはＳｏＣは、相対的に低いクロック速度で動作し、制限のあるローカルメモリを含んでおり、これにより、これらのローパワーＭＣＵおよび／またはＳｏＣは、複数の承認されたデバイスについてＡＣＬを維持することができず、（たとえばクライアントデバイス１０６、または、システム１００における他のクライアントデバイスからの）個々の要求を処理および認証するのに十分なスピードでアクセスコントロールプロトコルを実行することができない。ローパワーＭＣＵおよび／またはＳｏＣによって課される制限に鑑みて、開示される実施形態に係るアクセスコントロールプロトコルは、リソースデバイス１０２からシステム１００の別のコンポーネントにアクセスコントロールの決定を委任し得、これにより、リソースデバイス１０２にアクセスすることが承認されたデバイスを識別し、リソースデバイス１０２への提示の際に、承認されたデバイスがリソースデバイス１０２の機能にアクセスすることを可能にするローカルトークンを生成または「作り出」し得る。

【００５２】

例として、リソースデバイス１０２、オーナーデバイス１０４およびクライアントデバイス１０６は各々、ネットワーク１２２を介してコンピューティングシステム１０８との通信を確立可能であり得、開示される実施形態に係るアクセスコントロールプロトコルは、リソースデバイス１０２がコンピューティングシステム１０８にアクセスコントロールの決定を委任することを可能にし得る。いくつかの局面において、本願明細書において記載されるように、コンピューティングシステム１０８は、クラウドサーバ（たとえばGoog

le Cloud（商標）によって維持されるサーバ）として機能し得、オーナーデバイス１０４（付加的または代替的には、リソースデバイス１０２へのアクセスをコントロールまたは管理するエンティティの任意の他のデバイス）から受信される入力に基づいて、リソースデバイス１０２に代わってＡＣＬを生成および維持し得る。さらに、以下に記載されるように、コンピューティングシステム１０８は、承認されたデバイス（たとえばクライアントデバイス１０６）がリソースデバイス１０２の識別性を照合すること可能にするとともにリソースデバイス１０２へのクライアントデバイス１０６のアクセスのレベル、タイプ、および期間を特定するローカルトークンを生成または作り出し得る。

【００５３】

ある局面において、コンピューティングシステム１０８にリソースデバイス１０２のアクセスコントロールの決定を委任するアクセスコントロールプロトコルを開始するために、（たとえば、リソースデバイス１０２へのアクセスを有するまたはコントロールするエンティティによって維持された）オーナーデバイス１０４は、ネットワーク１２４を介してリソースデバイス１０２を発見する１つ以上のプロセスを実行し得る。たとえば、リソースデバイス１１２は、ネットワーク１２４を介して動作するデバイスに対して発見可能であり得、ネットワーク１２４を介して動作するデバイスに、その発見可能状態を示すアドバタイズメントデータをブロードキャスト送信し得る。１つの場合において、リソースデバイス１０２はパブリック（publicly）に発見可能であり、また、ブロードキャスト送信されたアドバタイズメントデータは、リソースデバイス１０２のデバイス識別子（たとえばメディアアクセスコントロール（ＭＡＣ）アドレス、ＩＰアドレスなど）を含み得る。オーナーデバイス１０４によってデバイス識別子が受信されると、オーナーデバイス１０４は、リソースデバイス１０２を発見しペアリングし得、（たとえばネットワーク１２４を介する）リソースデバイス１０２との直接的なワイヤレス接続を確立し得る。

【００５４】

他の場合において、リソースデバイス１２２は、プライベート（privately）に発見可能であり、システム１００内で動作する１つ以上のプライベートネットワークにおける自身のメンバーシップを示すようアドバタイズメントデータ内にエフェメラル識別子（ＥＩＤ： ephemeral identifier）データを含み得る。たとえば、プライベートに発見可能である場合、リソースデバイス１０２は、特定された長さの乱数（たとえば１６ビットの乱数）を含むアドバタイズメントデータと、１つ以上のプライベートネットワークのメンバーの間で共有されるプライベート暗号キーを使用して生成されるその乱数のデジタル署名とをブロードキャスト送信し得る。いくつかの局面において、リソースデバイス１０２は、メッセージ認証コード（ＭＡＣ： message authentication code）アルゴリズム（たとえば１６バイトのタグ長さを有するＨＭＡＣ－ＳＨＡ２５６アルゴリズム）を上記乱数および共有されたプライベート暗号キーに適用することによって、デジタル署名を生成し得る。オーナーデバイス１０４は、アドバタイズメントデータを受信し、共有されるプライベート暗号キーを使用して乱数の付加的なデジタル署名を生成し、受信および生成されたデジタル署名がマッチする場合、リソースデバイス１０２を発見し、ネットワーク１２４を介するリソースデバイス１０２との直接的なワイヤレス接続を確立し得る。

【００５５】

発見およびペアリングが成功すると、オーナーデバイス１０４は、コンピューティングシステム１０８にリソースデバイス１０２を登録し開示される実施形態に係るアクセスコントロールプロセスを実現するよう、１つ以上のプロセス（たとえば「ブートストラッピング」プロセス）を実行し得る。例として、オーナーデバイス１０４は、ネットワーク１２２を介するコンピューティングシステム１０８との通信を確立し得、コンピューティングシステム１０８に１つ以上の認証クレデンシャルを提供し得る（たとえばクラウドサービスアカウントに関連付けられるログイン、パスワード、バイオメトリックデータ、トークン、デジタル証明書など）。コンピューティングシステム１０８は、いくつかの局面において、格納されたクラウドサービスアカウントデータ（たとえばGoogle Cloud（商標）のようなクラウドサービスのアカウントを有するユーザまたはＧＡＩＡ（商標）アカウン

トを有するユーザを示すデータ）に対して、受信した認証クレデンシャルを比較し得、これにより、オーナーデバイス１０４のユーザ（たとえばオーナーデバイス１０４のオーナーおよび／またはオーナーデバイス１０４へのアクセスをコントロールするエンティティ）を認証し得る。

【００５６】

認証が成功すると、オーナーデバイス１０４は、登録テンプレートを生成し、グラフィカルユーザインターフェイスを介して（たとえば実行されるモバイルアプリケーションを介しておよび／またはクラウドサービスに関連付けられるウェブページを介して）ユーザに提示し得る。登録テンプレートは、いくつかの局面において、開示される実施形態に係る１つ以上のアクセスコントロールプロセスのために、リソースデバイス１０２を登録するユーザの意図を示す。さらに、例として、オーナーデバイス１０４は、提示された登録テンプレートへユーザによって入力された登録データを受信し得る。当該登録データは、リソースデバイス１０２、オーナーデバイス１０４および／またはクラウドサービスのユーザのアカウントを識別するデータを含み得るがこれに限定されない。また、オーナーデバイス１０４は、１つ以上のセキュアな通信プロトコル（たとえばセキュアハイパーテキストトランスファプロトコル（ＨＴＴＰＳ）など）を使用して、登録データをコンピューティングシステム１０８にネットワーク１２２を介して送信し得る。

【００５７】

コンピューティングシステム１０８は、受信した登録データを処理し得、オーナーデバイス１０４、ユーザのクラウドサービスアカウント（たとえばユーザのＧＡＩＡ（商標）アカウント、ユーザのGoogle Cloud（商標）アカウント）、および、リソースデバイス１０２にリンクされる一意登録チケット識別子（unique registration ticket identifier）を生成し得る。コンピューティングシステム１０８は、いくつかの場合において、生成された登録チケット識別子をローカルメモリまたはデータレポジトリに格納し得、１つ以上のセキュアな通信プロトコル（たとえばセキュアハイパーテキストトランスファプロトコル（ＨＴＴＰＳ）など）を使用して、生成された登録チケット識別子をネットワーク１２２を介してオーナーデバイス１０４に送信し得る。

【００５８】

オーナーデバイス１０４は、コンピューティングシステム１０８から登録チケット識別子を受信し得、いくつかの局面において、共有されるプライベート暗号キーを使用して登録チケット識別子を暗号化し、暗号化された登録チケット識別子をネットワーク１２４を介してリソースデバイス１０２に送信し得る。リソースデバイス１０２は、暗号化された登録チケット識別子を受信および復号化し得、当該登録チケット識別子はローカルメモリまたはデータレポジトリに格納され得る。さらに、ある局面では、リソースデバイス１０２は、登録処理を完了するために、（たとえばＷｅａｖｅプロトコルにかかるPrivet APIのような適切なアプリケーションプログラミングインターフェイス（ＡＰＩ： application programming interface）への呼び出しを通じて）コンピューティングシステム１０８に登録チケット識別子を提供し得る。

【００５９】

コンピューティングシステム１０８は、ＡＰＩを通じて登録チケット識別子を受信し得、登録チケット識別子に基づいて、オーナーデバイス１０４およびクラウドサービスアカウントを識別し得る。当該識別に応答して、コンピューティングシステム１０８は、リソースデバイス１０２についての１つ以上の認証クレデンシャルを生成し得、リソースデバイス１０２についての１つ以上のアクセスコントロールリスト（たとえばＡＣＬ）を生成しローカルに格納し得る。以下に記載されるように、生成および格納されたＡＣＬは、たとえば、リソースデバイス１０２にアクセスすることが承認されているデバイスと、承認されたアクセスの範囲を定義、制限および／または制約する１つ以上のアクセスパラメータとを識別し得る。コンピューティングシステム１０８は、上記のセキュアな通信プロトコルのいずれかを使用して、生成された認証クレデンシャルをネットワーク１２２を介してリソースデバイス１０２に送信し得る。リソースデバイス１０２は、発行された認証ク

レデンシャルを受信し、ローカルメモリまたはデータレポジトリに格納し得、いくつかの局面において、発行された認証クレデンシャルに基づいて、コンピューティングシステム１０８は、リソースデバイス１０２とのセキュアな通信セッションを確立し得る。

【００６０】

登録が成功すると、リソースデバイス１０２、オーナーデバイス１０４、クライアントデバイス１０６およびコンピューティングシステム１０８は、開示される実施形態に係る１つ以上のアクセスコントロールプロトコルを実現する動作をまとめて実行し得る。たとえば、開示されるプロセスによって、リソースデバイス１０２は、コンピューティングシステム１０８（たとえばGoogle Cloud（商標）によって維持されるサーバのようなクラウドサーバ）にアクセスコントロールの決定を委任することが可能になり得、コンピューティングシステム１０８は、オーナーデバイス１０４によって課される１つ以上の制限および／または制約に従って、クライアントデバイス１０６にリソースデバイス１０２へのアクセスを提供する１つ以上のトークンを生成し得る。

【００６１】

これらおよび他のアクセスコントロールプロセスを実現するために、リソースデバイス１０２、オーナーデバイス１０４、クライアントデバイス１０６および／またはコンピューティングシステム１０８は、１つ以上の暗号キーおよびトークンを生成、受信および／または格納するように構成され得る。たとえば、本願明細書において記載される発見プロセスの間、リソースデバイス１０２はルート暗号キーを生成し得、当該ルート暗号キーは、リソースデバイス１０２がローカルメモリまたはデータレポジトリに格納し得、かつ、リソースデバイス１０２によって機密保持され得る。

【００６２】

さらに、ある局面において、リソースデバイス１０２、オーナーデバイス１０４および／またはクライアントデバイス１０６は、共有されるプライベート暗号キーのローカルコピーを格納してもよく、初期ハンドシェイクプロセスの間のネットワーク１２４を介するリソースデバイスとオーナーデバイス１０４との間の通信（およびネットワーク１２６を介するクライアントデバイス１０６との通信）を暗号化してもよく、これにより、パッシブリスナー（passive listener）からの如何なるデバイス固有の情報も不明瞭にされ得る。ある局面では、共有されるプライベート暗号キーは、格納されたルート暗号キーを使用してリソースデバイス１０２によって生成され得、リソースデバイス１０２は、ネットワーク１２４および１２６のそれぞれを介して、共有されるプライベート暗号キーをオーナーデバイス１０４および／またはクライアントデバイス１０６に提供し得る。他の局面において、リソースデバイス１１２は、初期の登録および／またはブートストラッピングプロセスの間に、付加的なデバイス（たとえばリソースデバイス１１２のオーナーによって保持されるデバイス）および／またはコンピューティングシステム１０８（たとえばGoogle Cloud（商標）によって維持されるサーバのようなクラウドサーバ）に、共有されるプライベート暗号キーを提供し得る。次いで、付加的なデバイスおよび／またはコンピューティングシステム１０８が、以下に記載されるもののような１つ以上のローカルアクセストークンの部分として、共有されるプライベート暗号キーをクライアントデバイス１０６に提供し得る。

【００６３】

開示される実施形態に係るデバイスおよびアクセストークンは、マカロン（macaroon）としてフォーマットされ得、マカロンは、バイト列（たとえばキャビアート（caveat））のシーケンスと、ネスト型の態様（nested fashion）で各キャビアートにメッセージ認証コード（ＭＡＣ）アルゴリズムを適用することによって再帰的に計算される認証タグ（たとえばデジタル署名）とを含む。以下に記載されるように、キャビアートは、デバイス識別子、デバイス固有の暗号キーの識別子、および／または、アクセス制約（たとえば、失効日時、時間的制約、権限レベル、再共有に対する制約、セッションベースの制約、時間的制約など）を含み得るが、これらに限定されない。さらに、以下に記載される付加的な局面において、以前に生成されたマカロンが、付加的なキャビアートを加え、かつ、キー

として以前のタグを使用して付加的なキャビアートに再帰的にＭＡＣアルゴリズムを適用することにより、（たとえばリソースデバイス１０２、オーナーデバイス１０４、コンピューティングシステム１０８などによって）拡張され得る。開示される実施形態に係るＭＡＣアルゴリズムは、１６バイトのタグ長さのＨＭＡＣ－ＳＨＡ２５６アルゴリズムと、クライアントデバイス１０６およびリソースデバイス１１２に適切な他のアルゴリズムとを含み得るがこれらに限定されない。

【００６４】

たとえば、リソースデバイス１０２は、上述したようにマカロンとしてフォーマットされ得るマスターデバイストークンおよびマスターアクセストークンを生成し得る。マスターデバイストークンのキャビアートは、リソースデバイス１０２（たとえばＭＡＣアドレスなど）の識別子と、リソースデバイス１０２によって生成されるランダムデータ（たとえばランダムノンス（nonce））とを含み得るが、これらに限定されない。付加的な場合において、マスターアクセストークンのキャビアートは、たとえば、リソースデバイス１０２のオーナーに関連付けられる役割または権限のレベル（たとえば最も高い利用可能な権限）と、ランダムノンスとを含み得る。リソースデバイス１０２はさらに、たとえば、格納されたルート暗号キーと、マスターデバイスおよびアクセストークンのそれぞれのキャビアートとに基づいて、（たとえば適切なＭＡＣアルゴリズムを使用して）マスターデバイスおよびアクセストークンについてのデジタル署名を生成し得る。（たとえば、マカロンのうちの対応するものについての認証タグとして機能し得る）生成されたデジタル署名は、いくつかの場合において、リソースデバイス１０２とシステム１００の他のコンポーネントとの間の送信の間に、悪意のあるパーティーがトークンの１つ以上を傍受し修正し得る可能性を低減し得る。

【００６５】

上述したように、開示される実施形態に係るアクセスコントロールプロトコルは、リソースデバイス１０２が、コンピューティングシステム１０８（たとえばGoogle Cloud（商標）によって維持されるサーバのようなクラウドサーバ）にそのアクセスコントロールの決定を委任することを可能にし得、これにより、オーナーデバイス１０４によって課される制限および制約に従って、１つ以上の付加的なデバイス（たとえばクライアントデバイス１０６）にアクセス権を提供し得る。この委任を促進するために、リソースデバイス１０２は、（たとえば、上で概説されたセキュアな通信プロトコルのいずれかを使用して）ネットワーク１２２を介してコンピューティングシステム１０８にマスターデバイスおよびアクセストークンを送信し得る。

【００６６】

コンピューティングシステム１０８は、いくつかの局面において、リソースデバイス１０２からマスターデバイスおよびアクセストークンを受信し得、マスターデバイスおよびアクセストークンをオーナーデバイス１０４（付加的または代替的にはオーナーデバイス１０４のユーザのクラウドサービスアカウント）に関連付け得、ローカルメモリまたはデータレポジトリにマスターデバイスおよびアクセストークンを格納し得る。ある局面において、図２を参照して記載されるように、コンピューティングシステム１０８は、リソースデバイス１０２の１つ以上の機能へのアクセスを、オーナーデバイス１０４によってそのアクセスに課される制限および／または制約に従ってクライアントデバイス１０６に付与するローカルデバイスおよびアクセストークンを生成し得る。

【００６７】

図２は、開示される実施形態に従った、リソースデバイス１０２からコンピューティングシステム１０８へのアクセスコントロールの決定の委任を促進するデータ２００の例示的な交換を示す概略図である。例として、上記の例示的な技術のいずれかを使用して、リソースデバイス１０２は、マカロンとしてフォーマットされ得るとともにリソースデバイス１０２からコンピューティングシステム１０８に送信され得るマスターデバイスおよびアクセストークンを生成し得る。しかしながら、開示される実施形態は、リソースデバイス１０２によって生成されるマスターデバイスおよびアクセストークンに限定されず、他

の局面において、オーナーデバイス１０４と、リソースデバイス１０２をコントロールするエンティティに関連付けられる別のデバイス（図１に示されない）と、さらに、システム１００内で動作可能あり委任されたアクセスに適切な任意の付加的または代替的なデバイスとによって、開示される実施形態に係るマスターデバイスおよびアクセストークンが生成され得る。

【００６８】

いくつかの局面において、上述したように、コンピューティングシステム１０８は、リソースデバイス１０２にアクセスすることを承認される１つ以上のデバイスを識別するアクセスコントロールリスト（たとえばＡＣＬ）と、さらに、承認されたアクセスの範囲を定義、制限および／または制約する１つ以上のアクセスパラメータとを生成および維持し得る。ある局面では、アクセスパラメータは、失効日時、セッションベースの制約（たとえば、単一の確立されている通信設定への委任されたアクセスを制限すること）、時間的制約（たとえば有効期間、有効な日時など）、承認されたアクセスのタイプに対する制約（たとえば、機能の使用、設定の修正など）、承認されたデバイス（たとえばオーナー、マネージャ、ユーザなど）に関連付けられる役割、承認されたデバイスがさらにアクセスを委任する能力（たとえば付加的なトークンを作り出すこと）、および／または、承認されたデバイスがオフラインで（たとえばネットワーク１２２へのアクセスなしで）リソースデバイス１０２へアクセスする能力を含み得るが、これらに限定されない。しかしながら、開示される実施形態は、これらの例示的なアクセスパラメータに限定されず、さらに別の局面において、開示される実施形態に係るＡＣＬは、コンピューティングシステム１０８、リソースデバイス１０２および承認されたデバイス（たとえばクライアントデバイス１０６）に適切な任意の付加的または代替的なアクセスパラメータを含み得る。さらに、アクセスパラメータのうちの１つ以上は、（たとえば、対応するユーザから受信される入力に基づいて）オーナーデバイス１０４によって確立され得、付加的または代替的には、リソースデバイス１０２および／または承認されたデバイス（たとえばクライアントデバイス１０６）のプロパティに基づいて、コンピューティングシステム１０８によって確立されるデフォルトパラメータを表わし得る。

【００６９】

ある実施形態では、オーナーデバイス１０４のユーザは、（たとえば、オーナーデバイス１０４によって実行されるモバイルアプリケーション、および／または、オーナーデバイス１０４によって提示のためにアクセスおよびレンダリングされるウェブページによって生成される）コンピューティングシステム１０８に関連付けられるグラフィカルユーザインターフェイス（ＧＵＩ）にアクセスし得る。いくつかの局面では、提示されるＧＵＩは、（たとえば１つ以上のＡＣＬ内において）リソースデバイス１０２にアクセスすることを承認されている１つ以上のデバイスを識別し得、承認されているデバイスの各々について１つ以上のアクセスパラメータを識別し得、さらに、ユーザがＡＣＬに付加的な承認されたデバイスを加え、当該付加的な承認されたデバイスについてアクセスパラメータを特定することを可能にし得る。

【００７０】

たとえば、オーナーデバイス１０４によって提示されるＧＵＩへ入力されると、ユーザは、（ｉ）クライアントデバイス１０６をリソースデバイス１０２にアクセスすることを承認されたデバイスであると識別し、かつ、（ｉｉ）クライアントデバイス１０６の承認されたアクセスの範囲を定義、制限および／または制約するアクセスパラメータのうちの１つ以上を特定する情報を提供し得る。いくつかの場合、クライアントデバイス１０６を識別する情報は、デバイス識別子、および／または、クライアントデバイス１０６を操作するユーザの識別子を含み得る。さらに、上述したように、当該情報は、失効日時、セッションベースの制約、時間的制約、承認されたアクセスのタイプ、役割、その後の委任に対する制約、オーナーデバイス１０４によって課されるオフラインのアクセスに対する制約を含むがこれらに限定されないアクセスパラメータを特定し得る。いくつかの場合、開示される実施形態によると、特定された役割は、オーナーデバイス１０４に関連付けられ

る同等の役割に相当するか、それより低くなければならない。

【００７１】

図２に示されるように、オーナーデバイス１０４は、ユーザによって入力される情報を受信し、当該情報をアクセスコントロールデータ２０１へとパッケージ化し得、アクセスコントロールデータ２０１は、上で概説されたセキュアな通信プロトコルのいずれかを使用してネットワーク１２２を介してコンピューティングシステム１０８に送信され得る。ある局面では、アクセスコントロールデータ２０１はさらに、コンピューティングシステム１０８がオーナーデバイス１０４および／またはオーナーデバイス１０４のユーザを認証することを可能にする１つ以上の認証クレデンシャル（たとえばユーザのクラウドサービスアカウントのユーザ名、パスワード、バイオメトリックデータなど）を含み得る。

【００７２】

コンピューティングシステム１０８は、オーナーデバイス１０４からアクセスコントロールデータ２０１を受信し得、１つ以上の認証クレデンシャルに基づいて、オーナーデバイス１０４および／またはオーナーデバイス１０４のユーザを認証し得る。さらに、いくつかの局面では、コンピューティングシステム１０８は、アクセスコントロールデータ２０１を解析して、新しく承認されたデバイス（たとえばクライアントデバイス１０６）を識別するデータと、クライアントデバイス１０６の承認されたアクセスの範囲を定義する１つ以上のアクセスパラメータとを取得し得る。コンピューティングシステム１０８は、ある実施形態において、リソースデバイス１０２に対応する格納されたＡＣＬの部分にアクセスし得、クライアントデバイス１０６を識別するデータと、さらに、クライアントデバイス１０６がリソースデバイス１０２にアクセスする能力（たとえばアップデートされたＡＣＬ２０２を生成すること）を定義、制限および／または制約するアクセスパラメータとを含むように、アクセスされたＡＣＬ部分をアップデートする。

【００７３】

さらに、いくつかの実施形態では、クライアントデバイス１０６のユーザはクラウドサービスアカウント（たとえばコンピューティングシステム１０８によって維持されるGoogle Cloud（商標）または別のクラウドサービス）に関連付けられ得、クライアントデバイス１０６は、コンピューティングシステム１０８によって発行される１つ以上の認証クレデンシャルをローカルに格納し得る。ある局面では、クライアントデバイス１０６は、（たとえばネットワーク１２２を介して、上で概説されたセキュアな通信プロトコルのいずれかを使用して）コンピューティングシステム１０８に認証データ２０３を送信し得る。認証データ２０３は、たとえば、クライアントデバイス１０６に発行される１つ以上の認証クレデンシャルを含み得、コンピューティングシステム１０８は、受信した認証クレデンシャルと、格納されたクラウドサービスアカウントデータ（たとえば有効なＧＡＩＡ（商標）アカウントを識別するデータ、有効なGoogle Cloud（商標）アカウントを識別するデータなど）との比較に基づいてクライアントデバイス１０６を認証し得る。

【００７４】

受信した認証クレデンシャルが、格納されたクラウドサービスアカウントデータとマッチしない場合、コンピューティングシステム１０８は、フェイルした認証の試みを示す結果データ２０４を生成し、クライアントデバイス１０４に送信し得る。しかしながら、コンピューティングシステム１０８は、受信した認証クレデンシャルを格納されたクラウドサービスアカウントデータの部分とマッチするものであった場合、コンピューティングシステム１０８は、認証プロセスを成功とみなして、認証の成功を確認する結果データ２０４をクライアントデバイス１０６へ送信し得る。

【００７５】

認証の成功に応答して、クライアントデバイス１０６は、リソースデバイス１０２にアクセスする要求（たとえばアクセス要求２０５）を生成し、（たとえばネットワーク１２２を介して、上で概説されたセキュアな通信プロトコルのいずれかを使用して）コンピューティングシステム１０８に送信し得る。アクセス要求２０５は、いくつかの局面において、リソースデバイス１０２の識別子を含み得る（たとえばＭＡＣアドレス、ＩＰアドレ

スなど）。他の局面において、開示される実施形態によると、アクセス要求２０５はデバイス固有でなくてもよく、その代わりに、オーナーデバイス１０４がクライアントデバイス１０６にアクセス権限を与えたすべてのデバイスへのアクセスを要求してもよい。上述したように、クライアントデバイス１０６は、上で概説されたセキュアな通信プロトコルのいずれかを使用して、コンピューティングシステム１０８にネットワーク１２２を介してアクセス要求２０５を送信し得る。

【００７６】

コンピューティングシステム１０８は、アクセス要求２０５を受信し得、リソースデバイス１０２への要求されたアクセスが、オーナーデバイス１０４によってクライアントデバイス１０６に与えられたアクセスのレベルと一貫しているかどうか決定し得る。たとえば、コンピューティングシステム１０８は、アクセス要求２０５を解析し、リソースデバイス１０２と、付加的または代替的には、クライアントデバイス１０６とを識別し得る。ある局面では、コンピューティングシステム１０８は、リソースデバイス１０２に対応するＡＣＬのローカルに格納されたコピーにアクセスし得、当該ＡＣＬにおけるエントリに基づいて、オーナーデバイス１０４がクライアントデバイス１０６にリソースデバイス１０２へのアクセスを与えたかどうか決定し得る。

【００７７】

コンピューティングシステム１０８は、ＡＣＬエントリに基づいて、そのオーナーデバイス１０４がクライアントデバイス１０６（および／またはクライアントデバイス１０６のユーザ）にリソースデバイス１０２へのアクセスを与えていなかったと決定するものであった場合、与えられたアクセスが存在しないことを示すエラーメッセージを生成し、クライアントデバイス１０６に送信し得る（図２に示さず）。しかしながら、コンピューティングシステム１０８は、オーナーデバイス１０４がクライアントデバイス１０６（および／またはクライアントデバイス１０６のユーザ）にリソースデバイス１０２へのアクセスを与えたと決定するものであった場合、クライアントデバイス１０６がリソースデバイス１０２の１つ以上の機能にアクセスする能力を一緒に促進するローカルデバイストークンおよびローカルアクセストークン（たとえば図２のローカルトークンデータ２０６）を生成し得る。

【００７８】

ある局面では、コンピューティングシステム１０８は、（たとえば、成功した登録プロセスの後でリソースデバイス１０２によって生成され、リソースデバイス１０２から受信されるような）マスターデバイスおよびアクセストークンの格納されたコピーにアクセスし得、マスターデバイスおよびアクセストークンのそれぞれに対する拡張（extension）に基づいて、ローカルデバイストークンおよびローカルアクセストークンを生成および「作り出し」得る。たとえば、上述したように、マスターデバイストークンはマカロンとしてフォーマットされ得、そのキャビアートは、リソースデバイス１０２（たとえばＭＡＣアドレスなど）の識別子と、リソースデバイス１０２によって生成されるランダムデータ（たとえばデバイス固有のランダムノンス（nonce））とを含み得るが、これらに限定されない。ローカルデバイストークンを生成するために、コンピューティングシステム１０８は、１つ以上の付加的なキャビアート（たとえばクライアントデバイス１０６のデバイス識別子、ランダムノンスとしての付加的なランダムデータなど）を加え、かつ、以前のタグをキーとして使用して、適切なＭＡＣアルゴリズムを当該付加的なキャビアートに再帰的に適用することにより、マスターデバイストークンを拡張し得る。

【００７９】

さらに例として、マスターアクセストークンもマカロンとしてフォーマットされ得、そのキャビアートは、リソースデバイスのオーナーに関連付けられる役割（たとえば最も高い利用可能な権限）、および／または、リソースデバイス１０２によって生成されるランダムデータ（たとえばデバイス固有のランダムノンス）を含み得るがこれらに限定されない。ある局面では、ローカルアクセストークンを生成するために、コンピューティングシステム１０８は、オーナーデバイス１０４によってリソースデバイス１０２へのクライア

ントデバイス１０６のアクセスに課される１つ以上の制限および／または制約を識別する付加的なキャビアート（すなわちＡＣＬに格納される１つ以上のアクセスパラメータ）を付加的なランダムデータ（たとえばランダムノンス）とともに加えることによって、マスターデバイストークンを拡張し得る。

【００８０】

たとえば、コンピューティングシステム１０８は、クライアントデバイス１０６がリソースデバイス１０２にアクセスする能力に対してオーナーデバイス１０４によって課される１つ以上の制限および／または制約を示すアクセスパラメータを抽出するよう、リソースデバイス１０２に対応するＡＣＬを処理し得る。上述したように、課された制限および制約は、失効日時、時間的な制限（たとえばアクセスについての有効な日時）、セッションベースの制約（たとえば、単一の確立された通信セッションに、委任されたアクセスを限定すること）、アクセスのタイプ（たとえば、機能の使用、設定の修正など）に対する制約、クライアントデバイス１０６の役割（たとえばオーナー、マネージャ、ユーザなど）、クライアントデバイス１０６がさらにアクセスを委任する能力（たとえば付加的なトークンを作り出すこと）、および／または、クライアントデバイス１０６がリソースデバイス１０２にオフラインで（たとえばネットワーク１２２へのアクセスなしで）アクセスする能力を含み得るが、これらに限定されない。その後、コンピューティングシステム１０８は、（たとえばマスターアクセストークンからの）以前のタグをキーとして使用して付加的なキャビアートセットに適切なＭＡＣアルゴリズムを適用することによって、ローカルアクセストークンについて新しいタグを生成し得る。

【００８１】

いくつかの局面では、生成されたローカルデバイスおよびアクセストークンは「短命」であり得（すなわちは１時間、１日などの期間に有効であり得）、コンピューティングシステム１０８は、生成されたローカルデバイスおよびアクセストークンをローカルメモリまたはデータレポジトリ内に格納し得る。さらに、開示される実施形態に係るＭＡＣアルゴリズムは、１６バイトのタグ長さのＨＭＡＣ－ＳＨＡ２５６アルゴリズムと、クライアントデバイス１０６、リソースデバイス１１２およびネットワーク１２２に適切な他のアルゴリズムとを含み得るがこれらに限定されない。その後、コンピューティングシステム１０８は、生成されたローカルデバイスおよびアクセストークン（たとえばローカルトークンデータ２０６）を含むデータを生成し得、上で概説されたセキュアな通信プロトコルのいずれかを用いてネットワーク１２２を介してクライアントデバイス１０６にローカルトークンデータ２０６を送信する。いくつかの局面では、クライアントデバイス１０６は、ネットワーク１２２を介してコンピューティングシステム１０８からローカルトークンデータ２０６を受信し得、ローカルデバイスおよびアクセストークンのコピーをローカルメモリまたはデータレポジトリ内に格納し得る。

【００８２】

図３は、開示される実施形態に従った、リソースデバイスから１つ以上のコンピューティングデバイスにアクセスコントロールの決定を委任する例示的なプロセス３００のフローチャートである。ある局面において、クラウドサーバ（たとえばコンピューティングシステム１０８）として動作するコンピュータシステムは、リソースデバイス（たとえばリソースデバイス１０２）がコンピュータコンピューティングシステム１０８にアクセスコントロールの決定を委任することを可能にし得るとともにリソースデバイス１０２のオーナーのデバイス（たとえばオーナーデバイス１０４）によって指定される１つ以上のクライアントデバイス（たとえばクライアントデバイス１０６）にリソースデバイス１０２にアクセスする権利を提供する例示的なプロセス３００のステップを実行し得る。

【００８３】

いくつかの局面において、開示される実施形態によると、オーナーデバイス１０４は、ネットワーク１２４を介して動作するリソースデバイス１０２を発見する動作を実行し得る。たとえば、リソースデバイス１０２は、ネットワーク１２４を介して動作するデバイスに対して発見可能であり得、ネットワーク１２４を介して動作するデバイスに、その発

見可能状態を示すアドバタイズメントデータをブロードキャスト送信し得る。ある局面では、リソースデバイス１０２はパブリックまたはプライベートに発見可能であり得、オーナーデバイス１０４は、上で記載された例示的な技術のいずれかを使用して、パブリックまたはプライベートに発見可能状態で、リソースデバイス１０２を発見し得る。

【００８４】

オーナーデバイス１０４のリソースデバイス１０２の発見の成功に応答して、コンピューティングシステム１０８は、リソースデバイス１０２を登録し、リソースデバイス１０２をリソースデバイス１０２のオーナーのクラウドサービスアカウント（たとえばＧＡＩＡ（商標）アカウント、Google Cloud（商標）アカウントなど）に関連付け、付加的または代替的には、オーナーデバイス１０４に関連付ける動作を実行し得る（たとえばステップ３０２）。たとえば、オーナーデバイス１０４は、ネットワーク１２２を介するコンピューティングシステム１０８との通信を確立し得、コンピューティングシステム１０８に１つ以上の認証クレデンシャルを提供し得る（たとえばユーザ名、パスワード、バイオメトリックデータ、トークン、デジタル証明書など）。コンピューティングシステム１０８は、いくつかの局面において、格納された認証データ（たとえば、格納されたＧＡＩＡ（商標）アカウントデータ、格納されたGoogle Cloud（商標）アカウントデータなど）に対して、受信した認証クレデンシャルを比較し得、これにより、オーナーデバイス１０４を認証する。

【００８５】

上述したように、オーナーデバイス１０４は、（たとえば、提示される登録テンプレートにオーナーデバイスのユーザによって入力されるデータに基づいて）コンピューティングシステム１０８へのリソースデバイス１０２の登録をサポートするデータを生成し得、オーナーデバイス１０４は、（たとえば、上記のセキュアな通信プロトコルのいずれかを使用して）ネットワーク１２２を介してコンピューティングシステム１０８に生成された登録データを送信し得る。生成された登録データは、リソースデバイス１０２、オーナーデバイス１０４、および／または、リソースデバイス１０２のオーナーに関連付けられるクラウドサービスアカウントを識別するデータを含み得るがこれらに限定されない。

【００８６】

コンピューティングシステム１０８は、ステップ３０２において登録データを受信し得、オーナーデバイス１０４、オーナーのクラウドサービスアカウント、および、リソースデバイス１０２にリンクされる一意登録チケット識別子を生成し得る。コンピューティングシステム１０８は、いくつかの場合において、生成された登録チケット識別子をローカルメモリまたはデータレポジトリに格納し得、１つ以上のセキュアな通信プロトコル（たとえばセキュアハイパーテキストトランスファプロトコル（ＨＴＴＰＳ）など）を使用して、生成された登録チケット識別子をネットワーク１２２を介してオーナーデバイス１０４に送信し得る。

【００８７】

オーナーデバイス１０４は、コンピューティングシステム１０８から登録チケット識別子を受信し得、いくつかの局面において、共有されるプライベート暗号キーを使用して登録チケット識別子を暗号化し、それから、暗号化された登録チケット識別子をネットワーク１２４を介してリソースデバイス１０２に送信し得る。リソースデバイス１０２は、暗号化された登録チケット識別子を受信（および、適切な場合、復号化）し得、当該登録チケット識別子はローカルメモリまたはデータレポジトリに格納され得る。さらに、ある局面では、リソースデバイス１０２は、登録処理を完了するために、（たとえばＷｅａｖｅプロトコルにかかるPrivet APIのような適切なアプリケーションプログラミングインターフェイス（ＡＰＩ： application programming interface）への呼び出しを通じて）コンピューティングシステム１０８に登録チケット識別子を提供し得る。

【００８８】

コンピューティングシステム１０８は、ＡＰＩを通じて登録チケット識別子を受信し得、登録チケット識別子に基づいて、（たとえばステップ３０２において）１つ以上の認証

クレデンシャルを生成し、リソースデバイス１０２に発行し得る。コンピューティングシステム１０８は、生成および発行された認証クレデンシャルをリソースデバイス１０２にネットワーク１２２を介して送信し得、リソースデバイス１０２は、発行された認証クレデンシャルを受信し、ローカルメモリまたはデータレポジトリに格納し得る。さらに、発行された認証クレデンシャルに基づいて、リソースデバイス１０２は、ネットワーク１２２を介してコンピューティングシステム１０８とのセキュアな通信セッションを確立し得る。

【００８９】

付加的な局面において、リソースデバイス１０２の登録に応答して、コンピューティングシステム１０８は、リソースデバイス１０２についてアクセスコントロールリスト（たとえばＡＣＬ）を生成しローカルに格納し得る（たとえばステップ３０４）。生成および格納されたＡＣＬは、たとえば、リソースデバイス１０２にアクセスすることを承認された１つ以上のデバイスと、オーナーデバイス１０４によって承認されたアクセスに課される制限および制約を定義する１つ以上のアクセスパラメータとを識別し得る。ある局面において、アクセスパラメータは、トークン失効日時、セッションベースの制約（たとえば、単一の確立した通信設定への委任されたアクセスを限定すること）、時間的制約（たとえば有効期間など）、アクセスのタイプに対する制約（たとえば、特定の機能の使用、設定の修正など）、承認されたデバイス（たとえばオーナー、マネージャ、ユーザなど）に割り当てられる役割または権限のレベル、承認されたデバイスがさらにアクセスを委任する能力（たとえばアクセスを再共有すること）、および／または、リソースデバイス１０２にオフラインで（たとえばネットワーク１２２へのアクセスなしで）アクセスするための承認されたデバイスの利用可能性を含み得るが、これらに限定されない。いくつかの場合において、コンピューティングシステム１０８は、生成および格納されたＡＣＬをオーナーデバイス１０４および／またはオーナーデバイス１０４に関連付けられるクラウドサービスアカウントに関連付け得、以下に記載されるように、コンピューティングシステム１０８は、オーナーデバイス１０４から受信されるアクセスコントロールデータに応答して、格納されたＡＣＬにアクセスし修正するプロセスを実行し得る。

【００９０】

ある局面では、リソースデバイス１０２は、コンピューティングデバイス１０８に自身のアクセスコントロールの決定を委任し得、コンピューティングデバイス１０８は、オーナーデバイス１０４によって課される制限および制約に従って、１つ以上の付加的なデバイス（たとえばクライアントデバイス１０６）とのアクセス権限を共有し得る。この委任を促進するために、リソースデバイス１０２は、（たとえば、発行された認証クレデンシャルに基づいて）コンピューティングシステム１０８とのセキュアな通信セッションを確立し得、（たとえば、上で概説されたセキュアな通信プロトコルのいずれかを使用して）ネットワーク１２２を介してコンピューティングシステム１０８にマスターデバイストークンおよびマスターアクセストークンのコピーを送信し得る。コンピューティングデバイス１０８は、いくつかの局面において、リソースデバイス１０２からマスターデバイスおよびアクセストークンを受信し得（たとえばステップ３０６）、受信したマスターデバイスおよびアクセストークンをローカルメモリまたはデータレポジトリに格納し得る。以下に記載されるように、コンピューティングシステム１０８は、リソースデバイス１０２へのアクセスを１つ以上のクライアントデバイス（たとえばクライアントデバイス１０６）に提供するローカルトークンを生成するよう、マスターデバイスおよび／またはアクセストークンの構造を修正し得る。

【００９１】

たとえば、上述したように、開示される実施形態に係るマスターデバイスおよびアクセストークンは、バイト列（たとえばキャビアート（caveat））のシーケンスと、ネスト型の態様（nested fashion）で各キャビアートにメッセージ認証コード（ＭＡＣ）アルゴリズムを適用することによって再帰的に計算される認証タグ（たとえばデジタル署名）とを有するマカロン（macaroon）としてフォーマットされ得る。マスターデバイストークンの

キャビアートは、リソースデバイス１０２（たとえばＭＡＣアドレスなど）の識別子と、リソースデバイス１０２によって生成されるランダムデータ（たとえばデバイス固有のランダムノンス（nonce））とを含み得るが、これらに限定されない。付加的な場合において、マスターアクセストークンのキャビアートは、たとえば、リソースデバイスのオーナーに関連付けられる役割または権限のレベル（たとえば最も高い利用可能な権限）と、デバイス固有のランダムノンスとを含み得る。さらに、トークンに適用されたデジタル署名は、いくつかの場合において、悪意のあるパーティーが傍受しキャビアートデータの部分に承認されていない修正を行い得る可能性を低減し得る。

【００９２】

ある局面において、コンピューティングシステム１０８は、オーナーデバイス１０４からアクセスコントロールデータ（たとえば図２のアクセスコントロールデータ２０１）を受信するように構成され得る（たとえばステップ３０８）。受信したアクセスコントロールデータはたとえば、（ｉ）リソースデバイス１０２にアクセスすることを承認されたデバイス（たとえばクライアントデバイス１０６）を識別するとともに、（ｉｉ）クライアントデバイス１０６の承認されたアクセスを定義、制限および／または制約するアクセスパラメータのうちの１つ以上を特定する情報を含み得る。いくつかの場合、オーナーデバイス１０４のユーザは、入力として、受信したアクセスコントロールデータの少なくとも部分を、（たとえば、オーナーデバイス１０４によって実行されるモバイルアプリケーション、および／または、オーナーデバイス１０４によって提示のためにアクセスおよびレンダリングされるウェブページによって生成される）コンピューティングシステム１０８に関連付けられるグラフィカルユーザインターフェイス（ＧＵＩ）に提供し得る。

【００９３】

例として、受信したアクセスコントロールデータは、クライアントデバイス１０６の識別子、および／または、クライアントデバイス１０６を操作するユーザの識別子を含み得る。さらに、上述したように、受信したアクセスコントロールデータは、セッションベースの制約と、時間的制約と、アクセスのタイプに対する制約と、役割または権限レベルと、その後の委任に対する制約と、オフラインのアクセスに関して、リソースデバイス１０２にアクセスするクライアントデバイス１０６の能力に対してオーナーデバイス１０４によって課される制約とを含むがこれらに限定されないアクセスパラメータを特定し得る。いくつかの場合、開示される実施形態に従うと、オーナーデバイス１０４のユーザによって特定される役割または権限レベルは、オーナーデバイス１０４の同等の権限レベルに相当するかそれより低くなければならない。付加的な局面では、受信したアクセスコントロールデータは、コンピューティングシステム１０８がオーナーデバイス１０４および／またはオーナーデバイス１０４のユーザを認証することを可能にする１つ以上の認証クレデンシャル（たとえばオーナーデバイス１０４に関連付けられるクラウドサービスアカウントのログイン名、パスワード、バイオメトリックデータなど）を含み得る。

【００９４】

ステップ３１０において、コンピューティングシステム１０８は、（たとえば、格納されたクラウドサービスアカウントデータに対する、受信した認証クレデンシャルの比較に基づいて）オーナーデバイス１０４を認証し、さらに、受信したアクセスコントロールデータを解析して、新しく承認されたデバイス（たとえばクライアントデバイス１０６）と、クライアントデバイス１０６のリソースデバイス１０２へのアクセスを定義、制限および／または制約する１つ以上のアクセスパラメータとを識別するように構成され得る。コンピューティングシステム１０８はさらに、ローカルに格納されたＡＣＬにアクセスし得、ステップ３１２において、クライアントデバイス１０６を識別するデータと１つ以上のアクセスパラメータ（たとえば図２のアップデートされたＡＣＬ２０２）とを含むように、アクセスされたＡＣＬの少なくとも部分を修正し得る。

【００９５】

いくつかの局面では、クライアントデバイス１０６のユーザはクラウドサービスアカウント（たとえばコンピューティングシステム１０８によって維持されるGoogle Cloud（商

標）または別のクラウドサービス）に関連付けられ得、クライアントデバイス１０６は、コンピューティングシステム１０８によって発行される１つ以上の認証クレデンシャルをローカルに格納し得る。クライアントデバイス１０６は、いくつかの場合、上で概説されたセキュアな通信プロトコルのいずれかを使用して、コンピューティングシステム１０８にネットワーク１２２を介して認証データ（たとえば図２の認証データ２０３）を送信し得る。コンピューティングシステム１０８は、クライアントデバイス１０６から認証データを受信し得（たとえばステップ３１４）、本願明細書において記載される例示的な技術のいずれかを使用して、受信した認証データと、格納されたクラウドサービスアカウントデータとの比較に基づいて、クライアントデバイス１０６を認証し得る（たとえばステップ３１６）。

【００９６】

コンピューティングシステム１０８は、格納されたクラウドサービスアカウントデータにクライアントデバイス１０６の認証クレデンシャルをマッチすることができなかった場合（たとえばステップ３１６においてＮＯ）、フェイルした認証を示すエラーデータを生成し、ネットワーク１２２を介してクライアントデバイス１０６に送信し得る（たとえばステップ３１８）。その後、例示的なプロセス３００はステップ３２０において完了する。

【００９７】

しかしながら、コンピューティングシステム１０８は、クライアントデバイスの認証クレデンシャルを、格納されたクラウドサービスアカウントデータの部分とマッチすることができた場合（たとえばステップ３１６においてＹＥＳ）、認証の成功の確認を生成し、ネットワーク１２２を介してクライアントデバイス１０６に送信し得る（たとえばステップ３２２）。

【００９８】

認証の成功に応答して、クライアントデバイス１０６は、リソースデバイス１０２へのローカルアクセスの要求（たとえばアクセス要求２０５）を生成し、コンピューティングシステム１０８に送信し得る。アクセス要求２０５は、いくつかの局面において、リソースデバイス１０２およびクライアントデバイス１０６の識別子を含み得る（たとえばＭＡＣアドレス、ＩＰアドレスなど）。

【００９９】

コンピューティングシステム１０８は、クライアントデバイス１０６からアクセス要求を受信し得（たとえばステップ３２４）、要求されたアクセスがオーナーデバイス１０４によってクライアントデバイス１０６に与えられたアクセスと一貫しているかどうか決定し得る（たとえばステップ３２６）。たとえば、コンピューティングシステム１０８は、ステップ３２６において、受信したアクセス要求を解析し、リソースデバイス１０２を識別し得、付加的または代替的には、クライアントデバイス１０６を識別し得る。コンピューティングシステム１０８はさらに、リソースデバイス１０２に対応するＡＣＬのローカルに格納されたコピーにアクセスし得、ＡＣＬのエントリに基づいて、オーナーデバイス１０４がクライアントデバイス１０６にリソースデバイス１０２へのアクセスを与えたかどうか決定し得る。

【０１００】

オーナーデバイス１０４がクライアントデバイス１０６へアクセスを与えることをフェイルした場合（たとえばステップ３２６においてＮＯ）、コンピューティングシステム１０８は、ステップ３１８に戻り、与えられたアクセスが存在しないことを示すエラーデータを生成し、ネットワーク１２２を介してクライアントデバイス１０６に送信し得る。次いで、例示的なプロセス３００はステップ３２０で完了する。

【０１０１】

代替的には、コンピューティングシステム１０８は、オーナーデバイス１０４がリソースデバイス１０２へのアクセスをクライアントデバイス１０６に与えたと決定した場合（たとえばステップ３２６においてＹＥＳ）、コンピューティングシステム１０８は、リソ

ースデバイス１０２へのクライアントデバイス１０６のアクセスを一緒に促進するローカルデバイストークンおよびローカルアクセストークン（たとえば図２のローカルトークン２０６）を生成し得る（たとえばステップ３２８）。ある局面では、ステップ３２８において、コンピューティングシステム１０８は、（たとえば、成功した登録プロセスの後でリソースデバイス１０２によって生成され、リソースデバイス１０２から受信されるような）マスターデバイスおよびアクセストークンのローカルに格納されたコピーにアクセスし得、マスターデバイスおよびアクセストークンのそれぞれに対する拡張（extension）に基づいて、ローカルデバイストークンおよびローカルデバイストークンを生成および「作り出し」得る。

【０１０２】

たとえば、上述したように、マスターデバイストークンはマカロンとしてフォーマットされ得、そのキャビアートは、リソースデバイス１０２（たとえばＭＡＣアドレスなど）の識別子と、リソースデバイス１０２によって生成されるランダムデータ（たとえばランダムノンス（nonce））とを含み得るが、これらに限定されない。ステップ３２８においてローカルデバイストークンを生成するために、コンピューティングシステム１０８は、１つ以上の付加的なキャビアート（たとえばクライアントデバイス１０６のデバイス識別子、ランダムノンスとしての付加的なランダムデータなど）を加えることにより、マスターデバイストークンを拡張し得、以前のタグをキーとして使用して、適切なＭＡＣアルゴリズムを当該付加的なキャビアートに再帰的に適用し得る。

【０１０３】

さらに例として、マスターアクセストークンもマカロンとしてフォーマットされ得、そのキャビアートは、リソースデバイスのオーナーに関連付けられる役割または権限レベル（たとえば最も高い利用可能な権限）、および／または、リソースデバイス１０２によって生成されるランダムデータ（たとえばランダムノンス）を含み得るがこれらに限定されない。ある局面では、ステップ３２８においてローカルアクセストークンを生成するために、コンピューティングシステム１０８は、オーナーデバイス１０４によってリソースデバイス１０２へのクライアントデバイス１０６のアクセスに課される１つ以上の制限および／または制約を識別する１つ以上の付加的なキャビアート（すなわちＡＣＬに格納される１つ以上のアクセスパラメータ）を付加的なランダムデータ（たとえばランダムノンス）とともに加えることによって、マスターアクセストークンを拡張し得る。

【０１０４】

たとえば、コンピューティングシステム１０８は、クライアントデバイス１０６がリソースデバイス１０２にアクセスする能力に対してオーナーデバイス１０４によって課される制限および／または制約を示すアクセスパラメータを抽出するよう、ローカルに格納されたＡＣＬを解析し得る。上述したように、課された制限および制約は、失効日時、時間的な制限（たとえばアクセスについての有効な日時）、セッションベースの制約（たとえば、単一の確立された通信セッションへの委任されたアクセスを限定すること）、アクセスタイプ（たとえば、使用、設定の修正など）に対する制約、クライアントデバイス１０６の役割（たとえばオーナー、マネージャ、ユーザなど）、クライアントデバイス１０６がさらにアクセスを委任する能力（たとえば付加的なトークンを作り出すこと）、および／または、クライアントデバイス１０６がリソースデバイス１０２にオフラインで（たとえばネットワーク１２２へのアクセスなしで）アクセスする能力を含み得るが、これらに限定されない。その後、コンピューティングデバイス１０８は、（たとえばマスターアクセストークンからの）以前のタグをキーとして使用して付加的なキャビアートセットに適切なＭＡＣアルゴリズムを適用することによって、ローカルアクセストークンについて新しいタグを生成し得る。

【０１０５】

その後、コンピューティングシステム１０８は、上で概説されたセキュアな通信プロトコルのいずれかを使用して、生成されたローカルデバイスおよびアクセストークン（たとえば図２のローカルトークンデータ２０６）をネットワーク１２２を介してクライアント

デバイス１０６に送信し得る（たとえばステップ３３０）。次いで、例示的なプロセス３００はステップ３２０で完了する。

【０１０６】

上記の実施形態において、コンピューティングシステム１０８は、クライアントデバイス１０６から受信されるアクセス要求に応答して、ローカルデバイスおよび／またはアクセストークンを生成するように構成され得る。他の局面において、開示される実施形態によると、コンピューティングシステム１０８はその代りに、特定されたまたは所定の間隔（たとえば、１時間ごと、１日ごとなど）において、または、１つ以上のイベント（たとえばオーナーデバイス１０４からの要求に応答したＡＣＬへの修正）の発生の検出に応答して、ローカルデバイスおよび／またはアクセストークンを作り出し格納するプロセスを実行し得る。付加的な局面において、コンピューティングシステム１０８はさらに、特定の時間もしくは所定時間において、または、上記のイベントのいずれかに応答して、（たとえば上記のセキュアな通信プロトコルのいずれかを使用してネットワーク１２２を介して）ローカルデバイスおよび／またはアクセストークンの付加的なバージョンをクライアントデバイス１０６に「プッシュ送信（push）」する動作を実行し得る。

【０１０７】

ある実施形態において、上記の例示的なプロセスにより、リソースデバイス１０２が、コンピューティングシステム１０８（たとえばGoogle Cloud（登録商標）によって維持されるサーバのようなクラウドサーバ）にアクセスコントロールの決定を委任することが可能になり、コンピューティングシステム１０８は、オーナーデバイス１０４によって課される１つ以上の制限および／または制約に従って、クライアントデバイス１０６にリソースデバイス１０２へのアクセスを提供し得る。たとえば、上述したように、コンピューティングシステム１０８は、クライアントデバイス１０６にローカルデバイストークンおよびローカルアクセストークンを提供し得る。付加的な実施形態では、以下に概説されるように、ローカルデバイスおよびアクセストークンによって、クライアントデバイス１０６は、（たとえばネットワーク１２６を介して）リソースデバイス１０２とのセキュアな直接的なワイヤレス接続を確立することと、オーナーデバイス１０４またはコンピューティングシステム１０８との付加的なネットワーク通信を必要とすることなく、オーナーデバイスによって課される制限および／または制約に従ってリソースデバイス１０２にアクセスすることとが可能である。

【０１０８】

いくつかの局面において、開示される実施形態によると、クライアントデバイス１０６は、ネットワーク１２６を介して動作するリソースデバイス１０２を発見する動作を実行し得る。たとえば、リソースデバイス１０２は、ネットワーク１２６を介して動作するデバイスに対して発見可能であり得、ネットワーク１２６を介して動作するデバイスに、その発見可能状態を示すアドバタイズメントデータをブロードキャスト送信し得る。ある局面では、リソースデバイス１０２はパブリックまたはプライベートに発見可能であり得、クライアントデバイス１０６は、上で記載された例示的な技術のいずれかを使用して、パブリックまたはプライベートに発見可能状態で、リソースデバイス１０２を発見し得る。

【０１０９】

クライアントデバイス１０６によるリソースデバイス１０２の発見の際、クライアントデバイス１０６およびリソースデバイス１０２は、上記ローエナジーＢＬＥネットワークのようなネットワーク１２６を介してセキュアな直接的な接続を確立するようプロセスを開始し得る。たとえば、クライアントデバイス１０６は、ローカルデバイストークンの受信および格納の際（たとえばコンピューティングシステム１０８から受信される際）、ランダムデータ（たとえばクライアント固有のランダムノンス）を生成し得、格納されたローカルトークンからキャビアートのシーケンスを抽出し得る。キャビアートの抽出されたシーケンスは、リソースデバイス１０２（たとえばＭＡＣアドレスなど）の識別子と、リソースデバイス１０２によって生成されるランダムデータ（たとえばデバイス固有のランダムノンス）とを含み得るがこれらに限定されない。

【０１１０】
ある局面において、クライアントデバイス１０６は、格納されたローカルのデバイストークンおよび生成されたクライアント固有のランダムノンスへのＭＡＣアルゴリズム（たとえば１６バイトのタグ長さのＨＭＡＣ－ＳＨＡ２５６アルゴリズム）の適用に基づき、対称な暗号キーの第１の値（たとえば第１のハッシュ）を計算するように構成され得る。さらに、図４を参照して以下に記載されるように、クライアントデバイス１０６は、リソースデバイス１０２が、（たとえばリソースデバイス１０２によって維持されるような）ルート暗号キーと、抽出されたキャビアートシーケンスと、生成されたクライアント固有のランダムノンスとに再帰的に適用されるＭＡＣアルゴリズムに基づき、対称な暗号キーの第２の値を計算することを要求し得、さらに、第１および第２の対称な暗号キーの比較に基づいてリソースデバイス１０２の識別性を照合し得る。

【０１１１】
図４は、開示される実施形態に従った、クライアントデバイス１０６によるリソースデバイス１０２のトークンベースのアクセスを促進するデータ４００の例示的な交換を示す概略図である。たとえば、クライアントデバイス１０６は、リソースデバイスが対称な暗号キーの第２の値を計算することを要求するデータ（たとえばキー要求データ４０１）をネットワーク１２６を介してリソースデバイス１０２に送信し得る。キー要求データ４０１は、キャビアートの抽出されたシーケンスおよびクライアント固有のランダムノンスを含み得るがこれらに限定されず、ある局面では、クライアントデバイス１０６は、上述したように、共有されたプライベート暗号キーを使用してキー要求データ４０１を暗号化し得る。しかしながら、開示される実施形態は、これらの例示的な暗号化スキームに限定されず、他の局面において、クライアントデバイス１０６は、キー要求データ４０１、クライアントデバイス１０６およびリソースデバイス１０２に適切な任意の付加的または代替的な暗号化スキームを使用して、キー要求データ４０１を暗号化し得る（または、代替的には、暗号化のないクリアな状態（in the clear）でキー要求データ４０１を送信し得る）。

【０１１２】
いくつかの局面において、リソースデバイス１０２は、キー要求データ４０１を受信（および適切な場合、復号化）し得、ルート暗号キー、抽出されたキャビアートシーケンス、および、生成されたクライアント固有のランダムノンスへのＭＡＣアルゴリズムの再帰的な適用に基づいて、対称な暗号キーの要求された第２の値を計算し得る。たとえば、ＭＡＣアルゴリズムは、１６バイトのタグ長さのＨＭＡＣ－ＳＨＡ２５６アルゴリズムを含み得る。リソースデバイス１０２は、いくつかの場合、ルート暗号キーおよび抽出されたキャビアートシーケンスへのＭＡＣアルゴリズムの第１の適用に基づいてハッシュ値を計算し得、計算されたハッシュ値およびクライアント固有のランダムノンスへのＭＡＣアルゴリズムの第２の適用に基づいて、対称な暗号キーの第２の値を計算し得る。リソースデバイス１０２は、いくつかの局面において、第２の暗号キー（たとえばキー値データ４０２）を含むキーデータをネットワーク１２６を介してクライアントデバイス１０６に送信し得る。いくつかの場合では、上述したように、リソースデバイス１０２は、共有されたプライベート暗号キーを使用して、また付加的または代替的には、キー値データ４０２、リソースデバイス１０２およびクライアントデバイス１０６に適切な任意の他の暗号化スキームを使用して、キーデータを暗号化し得る（または、代替的には、暗号化のないクリアな状態（in the clear）でキー要求データ４０１を送信し得る）。

【０１１３】
クライアントデバイス１０６は、キー値データ４０２を受信（適切な場合、復号化）して、対称な暗号キーの第２の値を取得し得る。対称な暗号キーの第２の値は、クライアントデバイス１０６が計算された第１の値に対して比較し得る。第１および第２の値がマッチしないとクライアントデバイス１０６が決定した場合、クライアントデバイス１０６は、リソースデバイス１０２へのフェイルした接続の試みを示す応答を送信し得（図４に示されない）、これにより、クライアントデバイス１０６との接続プロセスをキャンセルし

得、ネットワーク１２６を介して動作する他のデバイスとの発見プロセスを開始するために、リソースデバイス１０２に付加的なアドバタイズメントデータをブロードキャスト送信させ得る。

【０１１４】

代替的には、クライアントデバイス１０６が、対称な暗号キーの第１および第２の値の間のマッチを決定した場合、クライアントデバイス１０６は、リソースデバイス１０２の識別性を照合し得、ネットワーク１２６を介してリソースデバイス１０２とのセキュアな直接的な接続を確立し得る。ある局面において、リソースデバイス１０２の識別性を照合することによって（たとえばクライアントデバイス１０６が正しいデバイスとの接続を確立していることを照合することによって）、クライアントデバイス１０６は、攻撃者または悪意のあるパーティーが中間者攻撃（man-in-the-middle attack）を試みていないことを保証し得る。さらに、クライアントデバイス１０６およびリソースデバイス１０２によって計算される対称な暗号キーの第１および第２の値は、いくつかの局面において、格納されたローカルアクセストークンに従ってクライアントデバイス１０６がリソースデバイス１０２の１つ以上の機能にアクセスすることを可能にする通信を含む、確立した直接的なワイヤレス接続を介するクライアントデバイス１０６とリソースデバイス１０２との間の将来の通信を暗号化し得るセッションキー４０３を表わしている。

【０１１５】

ある局面では、クライアントデバイス１０６は、リソースデバイス１０２の１つ以上の機能にアクセスする要求（たとえばローカルアクセス要求データ４０４）を、確立されたワイヤレス接続を介してリソースデバイス１０２に送信し得る。クライアントデバイス１０６はたとえば、要求されたローカルアクセス（たとえば範囲、タイプおよび／またはアクセスの期間）を識別するデータを含み得、さらに、格納されたローカルアクセストークンのコピーを含み得る。リソースデバイス１０２は、ローカルアクセス要求データ４０４を受信（適切な場合は復号化）し得、ローカルアクセス要求データ４０４を解析して、ローカルアクセストークンと、要求されたアクセスを識別するデータとを取得し得る。いくつかの局面において、リソースデバイス１０２は、ローカルアクセストークンおよびその示された認証チェーンの有効性を確証し得、さらに、要求されたローカルアクセスが、（たとえばコンピューティングシステム１０８によってローカルアクセストークンの１つ以上のキャビアートに埋め込まれているような）ローカルアクセストークン内に含まれるアクセスパラメータと一貫しているかどうか決定し得る。

【０１１６】

たとえば、上述したように、コンピューティングシステム１０８は、リソースデバイス１０２によって生成および維持されるマスターアクセストークンの拡張に基づいて、ローカルアクセストークンを生成し得る。ある局面において、リソースデバイス１０２は、（たとえば、クライアントデバイス１０６のローカルアクセス権限を定義するアクセスパラメータを特定し得る）ローカルアクセストークンの受信したコピーからキャビアートのシーケンスを抽出し得、抽出されたキャビアートシーケンスおよび（たとえばリソースデバイス１０２によって生成および格納された）マスターアクセストークンにＭＡＣアルゴリズムを適用して、ローカルアクセストークンのデバイス固有のコピーを生成し得る。

【０１１７】

受信したものと、ローカルアクセストークンのデバイス固有のコピーとがマッチする（たとえば受信したものとローカルアクセストークンのデバイス固有のコピーとのタグがマッチする）場合、リソースデバイス１０２は、ローカルアクセストークンの受信したコピーの有効性を確証し得る。ある局面において、決定された有効性に応答して、リソースデバイス１０２は、クライアントデバイス１０６によって要求されるアクセスが、たとえば抽出されたキャビアートシーケンスのアクセスパラメータ内で特定されるようなオーナーデバイス１０４によって与えられるアクセスと一貫しているかどうか決定し得る。

【０１１８】

たとえば、リソースデバイス１０２は、クライアントデバイス１０６から受信されるア

クセス要求を解析して、１つ以上の要求された機能を識別し、要求された機能へアクセスするためにクライアントデバイス１０６に必要とされる役割を決定または識別し得る。さらに、上述したように、リソースデバイス１０２は、抽出されたキャビアートシーケンスに基づいて、ローカルアクセストークンがまだ失効していない（たとえば、アクセスパラメータにおいて特定される失効日時がまだ発生していない）ことを決定し得る。リソースデバイス１０２はさらに、（たとえばアクセスパラメータ内で特定される役割に基づいて）クライアントデバイス１０６に割り当てられる役割または権限のレベルを識別し得、オーナーデバイス１０４によってクライアントデバイス１０６に課される１つ以上の付加的な制約（たとえば時間的制約、アクセスのタイプに対する制約、オフラインでの使用およびその後の委任に対する制約など）を識別し得る。

【０１１９】

ある局面において、リソースデバイス１０２は、要求される機能にアクセスするのにクライアントデバイス１０６によって必要とされる役割が（たとえばオーナーデバイス１０４によって）クライアントデバイス１０６に割り当てられる役割と一貫しているかどうか決定し得、さらに、要求された機能は、オーナーデバイス１０４によって課される１つ以上の付加的な制約と一貫しているかどうか決定し得る。要求されたアクセスが割り当てられた役割および課された制約に一貫している場合、リソースデバイス１０２は、決定された一貫性を示すとともに要求されたアクセスの許可を確認するデータ（たとえばアクセス確認データ４０５）を生成し、ネットワーク１２６を介してクライアントデバイス１０６に送信し得、リソースデバイス１０２は、クライアントデバイス１０６に、要求されたアクセスを与え得る（たとえば与えられたアクセス４０６）。代替的には、リソースデバイス１０２は、要求されたアクセスが、割り当てられた役割および／または課された制約と一貫していないとみなすと、エラーメッセージ（図４に示されない）を生成し、ネットワーク１２６を介してクライアントデバイス１０６に送信し得る（たとえば、これは、要求されたアクセスを修正するようにクライアントデバイス１０６に促し得る）。次いで、クライアントデバイス１０６およびリソースデバイス１０２は、クライアントデバイス１０６のリソースデバイス１０２へのアクセスを促進する付加的なデータを交換し得る。

【０１２０】

図５は、開示される実施形態に従った、リソースデバイスへのアクセスをクライアントデバイスに与えるための例示的なプロセス５００のフローチャートである。ある局面では、リソースデバイス（たとえばリソースデバイス１０２）は、例示的なプロセス５００のステップを実行し得、これにより、リソースデバイス１０２は、アクセスを要求するクライアントデバイス（たとえばクライアントデバイス１０６）とのセキュアな直接的なワイヤレス接続を確立することと、当該直接的なワイヤレス接続を介してクライアントデバイス１０６によってリソースデバイス１０２に提示されるローカルアクセストークン（たとえばローカルアクセストークン）に基づいてクライアントデバイス１０６にアクセスを与えることとが可能になる。

【０１２１】

いくつかの局面では、リソースデバイス１０２は、クライアントデバイス１０６によって実行される照合動作に関連して、（たとえばステップ５０２において）上で記載された例示的な技術のいずれかを使用してネットワーク１２６を介してリソースデバイス１０２とクライアントデバイス１０６との間にセキュアかつ直接的なワイヤレス接続を確立する動作を実行し得る。たとえば上述したように、（たとえば、クライアントデバイス１０６によって計算されたような）対称な暗号キーのクライアント固有の値が、（たとえばリソースデバイス１０２によって計算されたような）対称的な暗号キーのデバイス固有の値に対応する場合、クライアントデバイス１０６およびリソースデバイス１０２は（たとえばステップ５０２において）一緒にネットワーク１２６を介してセキュアかつ直接的なワイヤレス接続を確立し得る。さらに、クライアントデバイス１０６およびリソースデバイス１０２はさらに一緒に、対称な暗号キーのクライアント固有の値およびデバイス固有の値のそれぞれをセッションキー（たとえば図４のセッションキー４０３）として確証し得、

当該セッションキーにより、クライアントデバイス１０６およびリソースデバイス１０２は（たとえばステップ５０２において確立されたような）セキュアで直接的なワイヤレス接続を介してその後の通信を暗号化し得る。

【０１２２】

いくつかの局面において、リソースデバイス１０２は、クライアントデバイス１０６から（たとえばステップ５０４において）確立されたワイヤレス接続を介して、リソースデバイス１０２の１つ以上の機能にアクセスする要求（たとえば図４のローカルアクセス要求データ４０４）を受信し得る。いくつかの局面では、受信した要求は、要求されたローカルアクセスを識別するデータ（たとえばアクセスの範囲、タイプおよび／または期間）を含み得、さらに、格納されたローカルアクセストークンのコピーを含み得る。

【０１２３】

リソースデバイス１０２は、受信した要求を解析して、ローカルアクセストークンおよび要求されたアクセスを識別するデータの少なくとも部分を取得し得、いくつかの局面では、ローカルアクセストークンおよびその示された認証チェーンの有効性を決定し得る（たとえばステップ５０６）。たとえば、上述したように、コンピューティングシステム１０８は、リソースデバイス１０２によって生成および維持されるマスターアクセストークンの拡張に基づき、ローカルアクセストークンを生成し得る。リソースデバイス１０２は、ある局面において、ローカルアクセストークンの受信した部分から（たとえば、クライアントデバイス１０６のローカルアクセス権限を定義するアクセスパラメータを特定し得る）キャビアートのシーケンスを抽出し得、抽出されたキャビアートシーケンスおよび（たとえば、リソースデバイス１０２によって生成および格納されたような）マスターアクセストークンにＭＡＣアルゴリズムを適用して、ローカルアクセストークンの受信した部分のデバイス固有のコピーを計算し得る。さらに、リソースデバイス１０２は、ローカルアクセストークンの受信および計算されたコピーの比較（たとえばマカロンの形態でのローカルアクセストークンの受信および計算されたコピーのタグの比較）に基づいて、ローカルアクセストークンの有効性を決定し得る（したがって、リソースデバイス１０２へのアクセスを承認する有効なトークンに受信した部分が由来すると決定し得る）。ある局面では、リソースデバイス１０２は、ローカルに格納されたデータに基づき、ネットワーク１２２を介したコンピューティングシステム１０８との通信なしで、受信したローカルアクセストークンの有効性を決定するように構成され得る。

【０１２４】

リソースデバイス１０２は、ローカルアクセストークンの受信したコピーがローカルアクセストークンの計算されたコピーとマッチしないと決定した場合（たとえばステップ５０６においてＮＯ）、無効のローカルアクセストークンを示すエラーデータを生成しクライアントデバイス１０６に送信し得る（たとえばステップ５０８）。次いで、例示的なプロセス５００はステップ５１０で完了する。

【０１２５】

しかしながら、リソースがローカルアクセストークンの受信および計算されたコピー間でのマッチを検出した場合（たとえばステップ５０６においてＹＥＳ）、リソースデバイス１０２は、ローカルアクセストークンの受信した部分が有効なトークンに由来するということを確証し得、したがって、ローカルアクセストークンの有効性を確証し得る（たとえばステップ５１２）。ある局面において、決定された有効性に応答して、リソースデバイス１０２は、たとえば、抽出されたキャビアートシーケンスのアクセスパラメータ内に特定されるように、クライアントデバイス１０６によって要求されるアクセスがオーナーデバイス１０４によって与えられるアクセスと一貫しているかどうか決定し得る（たとえばステップ５１４）。

【０１２６】

たとえば、ステップ５１４において、リソースデバイス１０２は、クライアントデバイス１０６から受信されたアクセス要求を解析して、１つ以上の要求された機能を識別し得るとともに、さらに、要求された機能にアクセスするためにクライアントデバイス１０６

に必要とされる役割を決定または識別し得る。さらに、リソースデバイス１０２は、キャビアートシーケンスの部分に基づいて、ローカルアクセストークンがまだ失効していない（たとえば、アクセスパラメータにおいて特定される失効日時がまだ発生していない）ことを決定し得る。ステップ５１４では、リソースデバイス１０２はさらに、（たとえば、アクセスパラメータ内で特定される役割に基づいて）クライアントデバイス１０６に割り当てられた役割または権限のレベルを識別し得、オーナーデバイス１０４によってクライアントデバイス１０６に課される１つ以上の付加的な制約（たとえば時間的制約、アクセスのタイプに対する制約、オフラインでの使用およびその後の委任に対する制約など）を識別し得る。

【０１２７】

ある局面において、リソースデバイス１０２はステップ５１６において、要求される機能にアクセスするためにクライアントデバイス１０６によって必要とされる役割が（たとえばオーナーデバイス１０４によって）クライアントデバイス１０６に割り当てられた役割と一貫しているかどうかを決定し得、さらに、要求された機能が、オーナーデバイス１０４によって課される（たとえばアクセスパラメータ内の）付加的な制限および制約と一貫しているかどうか決定し得る。リソースデバイス１０２は、必要とされる役割が割り当てられた役割と一貫していない（たとえば、要求された機能が「マネージャ」の役割を必要としており、オーナーデバイスがクライアントデバイス１０６により低い役割である「ユーザ」を割り当てた）こと、および／または、要求された機能が課された制限および制約と一貫していないことを決定すると（たとえばステップ５１６においてＮＯ）、リソースデバイス１０２はステップ５１８に戻り、エラーメッセージを生成しネットワーク１２６を介してクライアントデバイス１０６に送信し得る。次いで、例示的なプロセス５００はステップ５１０で完了する。

【０１２８】

代替的には、リソースデバイス１０２は、必要とされる役割が割り当てられた役割と一貫していると決定し、かつ、要求された機能が課された制限および制約と一貫していると決定すると（たとえばステップ５１６においてＹＥＳ）、決定された一貫性を示し要求されたアクセスの付与を確認するデータ（たとえば図４のアクセス確認データ４０５）を生成し、ネットワーク１２６を介してクライアントデバイス１０６に送信し得る（たとえばステップ５１８）。リソースデバイス１０２は、要求されたアクセスをクライアントデバイス１０６に与え得、要求された機能へのクライアントデバイス１０６のアクセスを促進する付加的なデータを交換し得る（たとえばステップ５２０）。次いで、例示的なプロセス５００はステップ５１０で完了する。

【０１２９】

開示された例示的な実施形態の１つ以上を使用して、リソースデバイス１０２を所有またはコントロールするエンティティのデバイス（たとえばオーナーデバイス１０４）は、（たとえばクライアントデバイス１０６を通じて）１つ以上のクライアントデバイスと、リソースデバイス１０２へのアクセスを共有し得る。上述したように、オーナーデバイス１０４は、ネットワーク１２２を介してコンピューティングシステム１０８との通信を確立し得、アクセス権限を有する１つ以上のエンティティを識別するデータ（たとえばクライアントデバイス１０６のデバイス識別子）を提供し、これらのアクセス権限を定義する制限および／または制約を特定し得る。しかしながら、開示される実施形態は、クライアントデバイス１０６へのアクセス権の提供を促進するためにオーナーデバイス１０４とクライアントデバイス１０６との間の直接的なワイヤレス接続も必要とせず、また、オーナーデバイス１０４に対してクライアントデバイス１０６に自身の識別性を照合または立証させることを必要としない。さらに、上記のある実施形態において、オーナーデバイス１０４は、共有されたアクセス権限を示すデータにより自身を認証し、当該共有されたアクセス権限を示すデータを、オフラインまたは電源オフされ得るリソースデバイス１０２およびクライアントデバイス１０６と独立したコンピューティングシステム１０８に提供し得る。

【０１３０】
さらに、上述したように、クライアントデバイス１０６は、ネットワーク１２２を介してコンピューティングシステム１０８に対して自身を認証し得、（たとえばオーナーデバイス１０４によって課されるとともにコンピューティングシステム１０８によって維持されるアクセスコントロールリスト（ＡＣＬ）に統合される制限および／または制約に従って）リソースデバイス１０２へのクライアントデバイス１０６のアクセスを促進するローカルデバイスおよびアクセストークンを取得し得る。クライアントデバイス１０６は、要求を行いこれらのトークンを取得するようネットワーク１２２を介してコンピューティングシステム１０８との通信を確立し得るが、開示される実施形態は、クライアントデバイス１０６が要求を行いこれらのトークンを取得するためにプロセスを実行する間に、ネットワーク１２２への接続のないオフラインであり得るリソースデバイス１０２およびオーナーデバイス１０４に対して要件を課さない。
【０１３１】
付加的な局面において、クライアントデバイス１０６およびリソースデバイス１０２は、リソースデバイス１０２の１つ以上の機能へのクライアントデバイス１０６のアクセスを照合および確証するために、ネットワーク１２６（たとえばローエナジーＢＬＥネットワーク）を介してデータを交換し得る。開示される実施形態は、クライアントデバイス１０６および／またはリソースデバイス１０２が上記の例示的なネゴシエーションプロセスの間にネットワーク１２２に接続されるべきであるという要件を課さず、さらに、リソースデバイス１０２は、オフラインかつクライアントデバイス１０６、オーナーデバイス１０４および／またはコンピューティングシステム１０８との通信がない状態で、（たとえばクライアントデバイス１０６によって提供されるような）ローカルアクセストークンの有効性を決定し得る。
【０１３２】
さらに、上述したように、ローカルデバイス認証およびローカルアクセストークンは、コンピューティングシステム１０８による生成の後すぐに失効する（たとえば生成または作り出された後の３０分、１時間、１日などで失効する）「短命な」トークンを表わし得る。他の局面において、開示される実施形態によると、オーナーデバイス１０４は、オフラインかつネットワーク１２２への接続がない間、リソースデバイス１０２にアクセスする許可を承認されたデバイス（たとえばクライアントデバイス１０６）に与え得る。たとえば、コンピューティングシステム１０８は、対応するローカルアクセストークンのキャビアートデータの部分内において、クライアントデバイス１０６に与えられるオフラインアクセスを、（たとえば、上記の例示的な技術のいずれかを使用して）特定し得る。さらに、ある実施形態において、コンピューティングシステム１０８は、クライアントデバイス１０６のリソースデバイス１０２のオフラインアクセスを促進するために、（たとえばコンピューティングシステム１０８による生成の後数日、数週間あるいは数ヶ月間で失効する「長命の」トークンを生成するよう）対応するローカルアクセストークンの失効日時を遅延し得る。
【０１３３】
さらに、ある例示的な実施形態において、オーナーデバイス１０４によってリソースデバイス１０２へのアクセスが与えられたデバイスのユーザ（たとえばクライアントデバイス１０６のユーザ）は、コンピューティングシステム１０８によって維持されるクラウドサービスのアカウント（たとえばＧＡＩＡ（商標）アカウントおよび／またはGoogle Cloud（商標）アカウント）を保持し得、また、リソースデバイス１０２に対応するアクセスコントロールリスト（ＡＣＬ）は、当該クラウドサービスアカウントにより許可される与えられたアクセスに関連付けられ得る。しかしながら、開示される実施形態は、クラウドサービスアカウントホルダーにアクセスを与えるプロセスに限定されず、さらに別の実施形態において、オーナーデバイス１０４は、承認されたデバイスにアクセス権限を与えるとともに承認されたデバイスのユーザによる帯域外通信メカニズムを識別するアクセスコントロールデータを送信し得、上述したようにローカルデバイスおよびアクセストークン

にアクセスし得る。たとえば、帯域外通信メカニズムは、ｅメールアドレスまたはアカウントと、ソーシャルメディアネットワーク（たとえばＦａｃｅｂｏｏｋ（商標）、Ｔｗｉｔｔｅｒ（商標）、Ｇｏｏｇｌｅ＋（商標）など）内のハンドルと、チャットネットワークまたはメッセージングサービス内のハンドル（たとえばＷｈａｔｓＡｐｐ（商標）ユーザ名）と、ＳＭＳおよび／ＭＭＳテキストメッセージを受信することができる電話番号とを含み得るがこれらに限定されない。

【０１３４】

ある局面において、開示される実施形態によると、コンピューティングシステム１０８は、対応するＡＣＬの部分内において、帯域外通信メカニズムを識別するデータを統合し得る。（たとえば上記の例示的な技術のいずれかを使用した）ローカルデバイスおよび／またはアクセストークンの生成の際、コンピューティングシステム１０８は、ＡＣＬの部分から帯域外通信メカニズムを識別し得、ローカルデバイスおよび／またはアクセストークンにアクセスしローカルに格納する能力をクライアントデバイス１０６に提供するＵＲＬを生成し得、帯域外通信メカニズムに従ってクライアントデバイス１０６にＵＲＬを送信し得る。

【０１３５】

たとえば、クライアントデバイス１０６のユーザは、（たとえばクライアントデバイス１０６のディスプレイユニット内でのタッチ、クリックなどによって）ＵＲＬをアクティベートし得、クライアントデバイス１０６は、ローカルデバイスおよび／またはアクセストークンのコピーを取得し得る。他の場合、クライアントデバイス１０６によって実行されるアプリケーションプログラム（たとえばＡｎｄｒｏｉｄ（商標）のためのＣｒｏｉｓｓａｎｔ（商標））は、受信したＵＲＬを自動的に認識し、ユーザの介在なしでバックグラウンドでローカルデバイスおよび／またはアクセストークンをフェッチし得る。いくつかの局面において、コンピューティングシステム１０８は、帯域外通信メカニズムによって抽出されるローカルデバイスおよび／またはアクセストークンに対して、より短い有効期間と、クライアントデバイス１０６によるアクセスの試みの回数に対する制限とを含む付加的な制約を課し得る。

【０１３６】

さらに、ある局面では、リソースデバイス１０２は、（たとえば、オーナーのオプトアウトにより）ネットワーク１２２を介してコンピューティングシステム１０８に接続され得ず、付加的または代替的には、（たとえばスマートロックなどのようなローパワーデバイスにおいて起こり得るように）ネットワーク１２２にアクセス不能であり得る。ネットワーク１２２へのアクセスが存在しない場合、リソースデバイス１０２はコンピューティングシステム１０８にアクセスコントロールの決定を委任不可能であり得、さらに、システム１０８上にマスターデバイスおよび／またはアクセストークンを格納不可能であり得るか、または、コンピューティングシステム１０８がマスターデバイスおよび／もしくはアクセストークンに基づいて付加的なローカルトークンを作り出すことを要求不可能であり得る。

【０１３７】

付加的な実施形態では、ネットワーク１２２へのアクセスが存在しない場合、リソースデバイス１０２は、オーナーデバイス１０４（付加的または代替的にはオーナーデバイス１０４によって特定される別のデバイス）にアクセスコントロールの決定を委任し得、オーナーデバイス１０４は、（たとえば、上記の例示的な発見プロセスの後ネットワーク１２４を介して送信されたような）マスターデバイスおよび／またはアクセストークンのコピーを維持し得る。付加的な局面において、オーナーデバイス１０４は、アクセスコントロールリストを確証、維持、および／または、アップデートし得、リソースデバイスへアクセスするための要求をクライアントデバイス１０６から受信し得、上記の例示的なプロセスのいずれかを使用して、さらにローカルデバイスおよび／またはアクセストークンを生成または作り出し得る。

【０１３８】

たとえば、開示される実施形態により、オーナーデバイス１０４は、任意の適切な帯域外通信メカニズムを使用して、作り出されたローカルデバイスおよび／またはアクセストークンを承認されたデバイス（たとえばクライアントデバイス１０６）と共有することが可能になる。たとえば、オーナーデバイス１０４は、格納されたローカルデバイスおよび／またはアクセストークンを表すＢＬＯＢおよび／またはＵＲＬを生成し得、任意の帯域外通信チャネルを使用してＢＬＯＢおよび／またはＵＲＬを送信し得る（たとえばテキストメッセージ、ｅメールメッセージ、直接的なチャットメッセージ、ソーシャルメディアメッセージングなど）。クライアントデバイス１０６は、ＢＬＯＢおよび／またはＵＲＬを受信し得、受信したＢＬＯＢおよび／またはＵＲＬを処理して、ローカルデバイスおよび／またはアクセストークンを取得しローカルメモリまたはデータレポジトリに格納し得る（たとえばユーザ介在を通じてまたはプログラムによって）。開示される実施形態は、暗号化されていない帯域外通信チャネルを介してＢＬＯＢおよび／またはＵＲＬを送信することにより、存在するトランスポートメカニズムを暗黙的に信頼し得る。

【０１３９】

さらに、上記のある実施形態において、リソースデバイス１０２は、強力なクラウドベースの認証に依拠する（たとえば、Google Cloud（商標）のようなクラウドサービスを維持する）コンピューティングシステム１０８へアクセスコントロールの決定を委任する。他の局面において、開示される実施形態によると、リソースデバイス１０２は、サードパーティ機構にこれらのアクセスコントロールの決定を委任し得、当該サードパーティ機構は、（たとえばリソースデバイス１０２から受信されるような）マスターデバイスおよび／またはアクセストークンを格納し得るとともに、新しいより制限されたトークンを生成して、上記の例示的なプロセスのいずれかを使用してさまざまなトランスポートを通じてそれらを共有し得る。ある局面では、サードパーティ認証機構は、トークン生成、トークン寿命および範囲に対するコントロールを行い得る。

【０１４０】

多くの例示的な実施形態が記載された。しかしながら、本開示の精神および範囲から逸脱することなくさまざまな変更がなされ得ることが理解されるであろう。たとえば、ステップが再順序付けされるか、加えられるか、または、除去された状態で、上に示されたフローのさまざまな形態が使用されてもよい。

【０１４１】

この明細書に記載される実施形態および機能的な動作のすべては、この明細書において開示される構造およびそれらの構造的等価物またはそれらの１つ以上の組み合わせを含むデジタル電子回路またはコンピュータソフトウェア、ファームウェアもしくはハードウェアにおいて、実現され得る。実施形態は、１つ以上のコンピュータプログラムプロダクトとして実現され得る。すなわち、データ処理装置による実行またはデータ処理装置の動作の制御のためにコンピュータ読取可能媒体上でエンコードされたコンピュータプログラム命令の１つ以上のモジュールとして実現され得る。コンピュータ読取可能媒体は、マシン読取可能なストレージデバイス、マシン読取可能なストレージ基板、メモリデバイス、マシン読取可能な伝播信号に影響を与える物質の組成、または、それらの１つ以上の組み合わせであり得る。コンピュータ読取可能媒体は一時的でないコンピュータ読取可能媒体であり得る。「データ処理装置」という用語は、例として、プログラマブルプロセッサ、コンピュータまたは複数のプロセッサもしくはコンピュータを含む、データを処理するためのすべての装置、デバイスおよびマシンを包含する。装置は、ハードウェアに加えて、対象のコンピュータプログラムのための実行環境を作り出すコードを含み得、当該コードの例としては、プロセッサファームウェア、プロトコルスタック、データベース管理システム、オペレーティングシステムまたはそれらの１つ以上の組み合わせを構成するコードがある。伝播信号は、人為的に生成された信号であり、たとえば、好適な受信装置への送信のために情報をエンコードするように生成される、マシンにより生成される電気信号、光学信号または電磁気信号である。

【０１４２】

コンピュータプログラム（プログラム、ソフトウェア、ソフトウェアアプリケーション、スクリプトまたはコードとしても公知）は、コンパイルされた言語あるいは解釈された（interpreted）言語を含む任意の形態のプログラミング言語で記述され得、スタンドアロンプログラムとして、または、モジュール、コンポーネント、サブルーチン、もしくは、コンピューティング環境において使用するのに好適な他のユニットとして、任意の形態で展開され得る。コンピュータプログラムは、必ずしもファイルシステムにおけるファイルに対応しない。プログラムは、対象のプログラムに専用の単一のファイルにおいて、または、複数の協調されたファイル（たとえばコードの１つ以上のモジュール、サブプログラムもしくは部分を格納するファイル）において、他のプログラムまたはデータ（たとえば、マークアップ言語文書に格納される１つ以上のスクリプト）を保持するファイルの部分に格納され得る。コンピュータプログラムは、１つのコンピュータ上で実行されるように展開され得るか、または、１つのサイトに位置しているかもしくは複数のサイトにわたって分散され通信ネットワークによって相互接続される複数のコンピュータ上で実行されるように展開され得る。

【０１４３】

この明細書に記載されるプロセスおよびロジックフローは、入力データについて動作し出力を生成するによって、機能を実行するよう１つ以上のコンピュータプログラムを実行する１つ以上のプログラマブルプロセッサによって実行され得る。プロセスおよびロジックフローはさらに、たとえばＦＰＧＡ（フィールドプログラマブルゲートアレイ）またはＡＳＩＣ（特定用途向け集積回路）のような特殊目的のロジック回路によって実行され得、装置も当該特殊目的のロジック回路によって実現され得る。

【０１４４】

コンピュータプログラムの実行に好適であるプロセッサは、例として、汎用マイクロプロセッサおよび特殊目的マイクロプロセッサの両方を含んでおり、さらに、任意の種類のデジタルコンピュータのいずれか１つ以上のプロセッサを含んでいる。一般に、プロセッサは、リードオンリメモリ、ランダムアクセスメモリ、または、その両方から命令およびデータを受信する。コンピュータの必須の要素は、命令を実行するためのプロセッサと、命令およびデータを格納するための１つ以上のメモリデバイスとである。一般に、コンピュータは、たとえば磁気ディスク、光磁気ディスクまたは光ディスクといったデータを格納するための１つ以上のマスストレージデバイスを含むか、または、当該マスストレージデバイスからデータを受信するか、当該マスストレージデバイスへデータを搬送するか、もしくは、その両方を行うように動作可能に結合される。しかしながら、コンピュータはそのようなデバイスを有する必要はない。さらに、コンピュータは、たとえばタブレットコンピュータ、携帯電話、携帯情報端末（ＰＤＡ）、モバイルオーディオプレイヤー、グローバルポジショニングシステム（ＧＰＳ）レシーバーといった別のデバイスに埋め込まれてもよい。コンピュータプログラム命令およびデータを格納するのに好適なコンピュータ読取可能媒体は、例として、たとえばＥＰＲＯＭ、ＥＥＰＲＯＭおよびフラッシュメモリデバイスといった半導体メモリデバイスと、たとえば内部ハードディスクまたはリムーバブルディスクといった磁気ディスクと、光磁気ディスクと、ＣＤ－ＲＯＭおよびＤＶＤ－ＲＯＭディスクとを含むすべての形態の不揮発性メモリ、媒体およびメモリデバイスを含む。プロセッサおよびメモリは、専用ロジック回路によって補足または専用ロジック回路に統合され得る。

【０１４５】

ユーザとのインタラクションを提供するために、実施形態は、たとえばＣＲＴ（陰極線管）またはＬＣＤ（液晶ディスプレイ）モニタ、タッチスクリーンディスプレイなどの情報をユーザに表示するためのディスプレイデバイスと、ユーザが入力をコンピュータに提供し得るキーボードおよびたとえばマウスまたはトラックボールのようなポインティングデバイスとを有するコンピュータ上で実現され得る。他の種類のデバイスは同様に、ユーザとのインタラクションを提供するために使用され得、たとえば、ユーザに提供されるフィードバックは、たとえば視覚フィードバック、聴覚フィードバックまたは触覚フィード

バックといった任意の形態の感覚フィードバックであり得、ユーザからの入力は、音響入力、スピーチ入力、または触覚入力を含む任意の形態で受信され得る。

【０１４６】

実施形態は、バックエンドコンポーネントをたとえばデータサーバとして含むコンピューティングシステムにおいて実現され得るか、または、たとえばアプリケーションサーバといったミドルウェアコンポーネントを含むコンピューティングシステムにおいて実現され得るか、または、たとえば、ユーザが開示された技術の実現例とインタラクションする際に使用可能なグラフィックユーザインターフェイスもしくはウェブブラウザを有するクライアントコンピュータといったフロントエンドコンポーネントを含むコンピューティングシステムにおいて実現され得るか、または、そのようなバックエンド、ミドルウェア、もしくはフロントエンドコンポーネントの１つ以上の任意の組合せを含むコンピューティングシステムにおいて実現され得る。システムのコンポーネントは、任意の形態または媒体のデジタルデータ通信（たとえば通信ネットワーク）によって相互に接続され得る。通信ネットワークの例として、ローカルエリアネットワーク（「ＬＡＮ」）、および、たとえばインターネットのようなワイドエリアネットワーク（「ＷＡＮ」）が挙げられる。

【０１４７】

コンピューティングシステムはクライアントおよびサーバを含み得る。クライアントおよびサーバは一般に互いにリモートであり、典型的に通信ネットワークを介してインタラクションする。クライアントとサーバとの関係は、それぞれのコンピュータ上で実行されて互いにクライアント－サーバ関係を有するコンピュータプログラムによって生じる。

【０１４８】

さらに、ここで議論されるシステムが、ユーザに関する個人情報を収集するか、または、個人情報を利用し得る状況の場合、ユーザには、たとえば、ユーザのソーシャルネットワーク、ソーシャルアクションもしくはアクティビティ、職業、ユーザのプレファレンス、または、ユーザの現在の場所に関する情報のような個人情報をプログラムまたは機能が収集するかどうかをコントロールするために機会が提供され得るか、または、ユーザにより関連するコンテンツサーバからコンテンツを受信するかどうかおよび／もしくはユーザにより関連するコンテンツサーバからコンテンツをどのように受信するかをコントロールするために機会が提供され得る。さらに、あるデータは、格納または使用される前に、１つ以上の態様で匿名化され得るので、個人を識別可能な情報が除去される。たとえば、ユーザについて個人が識別可能である情報を決定することができないようにユーザの識別性が匿名化され得るか、または、ユーザの特定の位置が決定され得ないように位置情報がどこで得られるユーザの地理的な位置が（たとえば都市、郵便番号または州レベルまで）一般化され得る。したがって、ユーザは、自身に関して情報がどのように収集されコンテンツサーバによって使用されるかについてコントロールを有し得る。

【０１４９】

この明細書は多くの詳細を含んでいるが、これらは限定として解釈されるべきでなく、むしろ特定の実施形態に特有の特徴の記載として解釈されるべきである。別個の実施形態の文脈でこの明細書において記載されるある特徴も、単一の実施形態において組み合わせて実現され得る。反対に、単一の実施形態の文脈で記載されるさまざまな特徴も、別々にあるいは任意の好適なサブコンビネーションで、複数の実施形態において実現され得る。さらに、特徴は、ある組み合わせにおいて作用するように記載され、最初はそういうものとして特許請求されている場合があるが、特許請求された組み合わせのうちの１つ以上の特徴が、ある場合において、当該組み合わせから削除され得、特許請求された組み合わせは、サブコンビネーションあるいはサブコンビネーションの変形に向けられ得る。

【０１５０】

同様に、動作は図面において特定の順序で示されているが、これは、そのような動作は示された特定の順序あるいはシーケンシャルな順序で実行される必要があると理解されるべきではなく、または、望ましい結果を達成するためにすべての示された動作が実行される必要があると理解されるべきではない。ある状況では、マルチタスクおよび並列処理が

有利であり得る。さらに、上に記載された実施形態におけるさまざまなシステムコンポーネントの分離は、すべての実施形態においてそのような分離が必要であると理解されるべきでなく、記載されたプログラムコンポーネントおよびシステムは一般に、単一のソフトウェアプロダクトに一緒に統合されてもよく、または、複数のソフトウェアプロダクトにパッケージングされてもよいということが理解されるべきである。

【０１５１】

このように、特定の実施形態が記載された。他の実施形態は添付の請求の範囲内にある。たとえば、請求の範囲において記載されるアクションは、異なる順序で実行されてもよく、それでも望ましい結果を達成し得る。

【０１５２】

図６は、クライアントまたはサーバもしくは複数のサーバのいずれかとして、この明細書において記載されるシステムおよび方法を実現するために使用され得るコンピューティングデバイス６００，６５０のブロック図である。コンピューティングデバイス６００は、ラップトップ、デスクトップ、ワークステーション、携帯情報端末、サーバ、ブレードサーバ、メインフレーム、および他の適切なコンピュータといった、さまざまな形態のデジタルコンピュータを表わすことを意図している。コンピューティングデバイス６５０は、携帯情報端末、セルラー電話、スマートフォン、および他の同様のコンピューティングデバイスといった、さまざまな形態のモバイルデバイスを表わすことを意図している。さらに、コンピューティングデバイス６００または６５０は、ユニバーサルシリアルバス（ＵＳＢ： Universal Serial Bus）フラッシュドライブを含み得る。ＵＳＢフラッシュドライブはオペレーティングシステムおよび他のアプリケーションを格納し得る。ＵＳＢフラッシュドライブは、別のコンピューティングデバイスのＵＳＢポートへ挿入され得るワイヤレス送信機またはＵＳＢコネクタのような入出力コンポーネントを含み得る。ここに示すコンポーネント、それらの接続および関係、ならびにそれらの機能は例示であることが意図されているに過ぎず、本文書に記載のおよび／または請求項に記載の本発明の実現例を限定することを意図していない。

【０１５３】

コンピューティングデバイス６００は、プロセッサ６０２、メモリ６０４、ストレージデバイス６０６、メモリ６０４および高速拡張ポート６１０に接続している高速インターフェイス６０８、ならびに低速バス６１４およびストレージデバイス６０６に接続している低速インターフェイス６１２を含む。コンポーネント６０２，６０４，６０６，６０８，６１０および６１２の各々はさまざまなバスを用いて相互に接続されており、共通のマザーボード上にまたは他の態様で適宜搭載され得る。プロセッサ６０２は、コンピューティングデバイス６００内で実行される命令を処理可能であり、この命令には、ＧＵＩのためのグラフィック情報を高速インターフェイス６０８に結合されているディスプレイ６１６などの外部入出力デバイス上に表示するためにメモリ６０４内またはストレージデバイス６０６上に格納されている命令が含まれる。他の実現例では、複数のプロセッサおよび／または複数のバスが、複数のメモリおよび複数種類のメモリとともに必要に応じて用いられ得る。また、複数のコンピューティングデバイス６００が接続され得、各デバイスは（たとえばサーババンク、ブレードサーバのグループ、またはマルチプロセッサシステムとして）必要な動作の一部を提供する。

【０１５４】

メモリ６０４は情報をコンピューティングデバイス６００内に格納する。一実現例では、メモリ６０４は１つまたは複数の揮発性メモリユニットである。別の実現例では、メモリ６０４は１つまたは複数の不揮発性メモリユニットである。また、メモリ６０４は、磁気ディスクまたは光ディスクといった別の形態のコンピュータ読取可能媒体であってもよい。

【０１５５】

ストレージデバイス６０６は、コンピューティングデバイス６００にマスストレージを提供可能である。一実現例では、ストレージデバイス６０６は、フロッピー（登録商標）

ディスクデバイス、ハードディスクデバイス、光ディスクデバイス、またはテープデバイス、フラッシュメモリもしくは他の同様のソリッドステートメモリデバイス、またはストレージエリアネットワークもしくは他のコンフィギュレーションにおけるデバイスを含む多数のデバイスといった、コンピュータ読取可能媒体であってもよく、または当該コンピュータ読取可能媒体を含んでいてもよい。コンピュータプログラムプロダクトが情報媒体内に有形に具体化され得る。また、コンピュータプログラムプロダクトは、実行されると上述のような１つ以上の方法を実行する命令を含み得る。情報媒体は、メモリ６０４、ストレージデバイス６０６、またはプロセッサ６０２上のメモリといった、コンピュータ読取可能媒体またはマシン読取可能媒体である。

【０１５６】

高速コントローラ６０８はコンピューティングデバイス６００のための帯域幅集約的な動作を管理するのに対して、低速コントローラ６１２はより低い帯域幅集約的な動作を管理する。そのような機能の割当ては例示に過ぎない。一実現例では、高速コントローラ６０８はメモリ６０４、ディスプレイ６１６に（たとえばグラフィックスプロセッサまたはアクセラレータを介して）、およびさまざまな拡張カード（図示せず）を受付け得る高速拡張ポート６１０に結合される。当該実現例では、低速コントローラ６１２はストレージデバイス６０６および低速拡張ポート６１４に結合される。さまざまな通信ポート（たとえばＵＳＢ、ブルートゥース、イーサネット（登録商標）、無線イーサネット）を含み得る低速拡張ポートは、キーボード、ポインティングデバイス、スキャナ、またはスイッチもしくはルータといったネットワーキングデバイスなどの１つ以上の入出力デバイスに、たとえばネットワークアダプタを介して結合され得る。

【０１５７】

コンピューティングデバイス６００は、図に示すように多数の異なる形態で実現されてもよい。たとえば、コンピューティングデバイス６００は標準的なサーバ６２０として、またはそのようなサーバのグループ内で複数回実現されてもよい。また、コンピューティングデバイス６００はラックサーバシステム６２４の一部として実現されてもよい。さらに、コンピューティングデバイス６００はラップトップコンピュータ６２２などのパーソナルコンピュータにおいて実現されてもよい。代替的には、コンピューティングデバイス６００からのコンポーネントは、デバイス６５０などのモバイルデバイス（図示せず）内の他のコンポーネントと組合されてもよい。そのようなデバイスの各々がコンピューティングデバイス６００，６５０の１つ以上を含んでいてもよく、システム全体が、互いに通信する複数のコンピューティングデバイス６００，６５０で構成されてもよい。

【０１５８】

コンピューティングデバイス６５０は、数あるコンポーネントの中でも特に、プロセッサ６５２、メモリ６６４、ディスプレイ６５４などの入出力デバイス、通信インターフェイス６６６、およびトランシーバ６６８を含む。また、デバイス６５０には、マイクロドライブまたは他のデバイスなどのストレージデバイスが提供されて付加的なストレージが提供されてもよい。コンポーネント６５０，６５２，６６４，６５４，６６６および６６８の各々はさまざまなバスを用いて相互に接続されており、当該コンポーネントのいくつかは共通のマザーボード上にまたは他の態様で適宜搭載され得る。

【０１５９】

プロセッサ６５２は、メモリ６６４に格納されている命令を含む、コンピューティングデバイス６５０内の命令を実行可能である。プロセッサは、別個の複数のアナログおよびデジタルプロセッサを含むチップのチップセットとして実現されてもよい。さらに、プロセッサは、多くのアーキテクチャのうちのいずれかを使用して実現され得る。たとえば、プロセッサ４１０は、ＣＩＳＣ（Complex Instruction Set Computers（複雑命令セットコンピュータ））プロセッサ、ＲＩＳＣ（Reduced Instruction Set Computer（簡略化命令セットコンピュータ））プロセッサ、または、ＭＩＳＣ（Minimal Instruction Set Computer（最小命令セットコンピュータ））プロセッサであり得る。プロセッサは、たとえば、ユーザインターフェイス、デバイス６５０が実行するアプリケーション、およびデバ

イス６５０による無線通信の制御といった、デバイス６５０の他のコンポーネントの協調を提供し得る。

【０１６０】

プロセッサ６５２は、ディスプレイ６５４に結合された制御インターフェイス６５８およびディスプレイインターフェイス６５６を介してユーザと通信し得る。ディスプレイ６５４は、たとえば、ＴＦＴディスプレイ（薄膜トランジスタ液晶ディスプレイ）もしくはＯＬＥＤ（有機発光ダイオード）ディスプレイ、または他の適切なディスプレイ技術であり得る。ディスプレイインターフェイス６５６は、ディスプレイ６５４を駆動してグラフィックおよび他の情報をユーザに提示するための適切な回路を含み得る。制御インターフェイス６５８はユーザからコマンドを受信し、当該コマンドをプロセッサ６５２に提出するために変換し得る。さらに、外部インターフェイス６６２が、デバイス６５０と他のデバイスとの隣接通信を可能にするために、プロセッサ６５２と通信した状態で提供されてもよい。外部インターフェイス６６２は、たとえば、ある実現例では有線通信を提供し、他の実現例では無線通信を提供してもよく、また、複数のインターフェイスが用いられてもよい。

【０１６１】

メモリ６６４は情報をコンピューティングデバイス６５０内に格納する。メモリ６６４は、１つもしくは複数のコンピュータ読取可能媒体、１つもしくは複数の揮発性メモリユニット、または１つもしくは複数の不揮発性メモリユニットの１つ以上として実現され得る。さらに、拡張メモリ６７４が提供され、たとえばＳＩＭＭ（Single In Line Memory Module）カードインターフェイスを含み得る拡張インターフェイス６７２を介してデバイス６５０に接続されてもよい。このような拡張メモリ６７４はデバイス６５０に余分のストレージスペースを提供し得るか、またはデバイス６５０のためのアプリケーションもしくは他の情報をさらに格納し得る。具体的には、拡張メモリ６７４は上述のプロセスを実行または補足するための命令を含み得、さらにセキュアな情報を含み得る。ゆえに、たとえば、拡張メモリ６７４はデバイス６５０のためのセキュリティモジュールとして提供されてもよく、デバイス６５０のセキュアな使用を許可する命令でプログラムされてもよい。さらに、ハッキング不可能なようにＳＩＭＭカード上に識別情報を置くといったように、セキュアなアプリケーションが付加的な情報とともにＳＩＭＭカードを介して提供されてもよい。

【０１６２】

メモリは、以下に記載のように、たとえばフラッシュメモリおよび／またはＮＶＲＡＭメモリを含み得る。一実現例では、コンピュータプログラムプロダクトが情報媒体内に有形に具体化される。コンピュータプログラムプロダクトは、実行されると上述のような１つ以上の方法を実行する命令を含む。情報媒体は、メモリ６６４、拡張メモリ６７４、またはプロセッサ６５２上のメモリといった、コンピュータ読取可能媒体またはマシン読取可能媒体であり、これは、たとえばトランシーバ６６８または外部インターフェイス６６２上で受信され得る。

【０１６３】

デバイス６５０は、必要に応じてデジタル信号処理回路を含み得る通信インターフェイス６６６を介して無線通信し得る。通信インターフェイス６６６は、とりわけ、ＧＳＭ（登録商標）音声通話、ＳＭＳ、ＥＭＳ、またはＭＭＳメッセージング、ＣＤＭＡ、ＴＤＭＡ、ＰＤＣ、ＷＣＤＭＡ（登録商標）、ＣＤＭＡ２０００、またはＧＰＲＳといった、さまざまなモードまたはプロトコル下の通信を提供し得る。そのような通信は、たとえば無線周波数トランシーバ６６８を介して起こり得る。さらに、ブルートゥース、Ｗｉ－Ｆｉ、または他のそのようなトランシーバ（図示せず）を用いるなどして、短距離通信が起こり得る。さらに、ＧＰＳ（全地球測位システム）レシーバモジュール６７０が付加的なナビゲーション関連および位置関連の無線データをデバイス６５０に提供し得、当該データはデバイス６５０上で実行されるアプリケーションによって適宜用いられ得る。

【０１６４】

また、デバイス６５０は、ユーザから口頭情報を受信して当該情報を使用可能なデジタル情報に変換し得る音声コーデック６６０を用いて可聴的に通信し得る。音声コーデック６６０も同様に、たとえばデバイス６５０のハンドセット内で、スピーカを介すなどしてユーザに可聴音を生成し得る。そのような音は音声電話からの音を含んでいてもよく、録音された音（たとえば音声メッセージ、音楽ファイル等）を含んでいてもよく、さらに、デバイス６５０上で実行されるアプリケーションが生成する音を含んでいてもよい。

【０１６５】

コンピューティングデバイス６５０は、図に示すように多数の異なる形態で実現されてもよい。たとえば、コンピューティングデバイス６５０はセルラー電話６８０として実現されてもよい。また、コンピューティングデバイス６５０は、スマートフォン６８２、携帯情報端末、または他の同様のモバイルデバイスの一部として実現されてもよい。

【０１６６】

本明細書に記載のシステムおよび技術のさまざまな実現例は、デジタル電子回路、集積回路、特別に設計されたＡＳＩＣ（特定用途向け集積回路）、コンピュータハードウェア、ファームウェア、ソフトウェア、および／またはそれらの組合せで実現され得る。これらのさまざまな実現例は、少なくとも１つのプログラマブルプロセッサを含むプログラマブルシステム上で実行可能および／または解釈可能な１つ以上のコンピュータプログラムにおける実現例を含んでいてもよく、当該プロセッサは専用であっても汎用であってもよく、ストレージシステム、少なくとも１つの入力デバイス、および少なくとも１つの出力デバイスからデータおよび命令を受信するように、かつこれらにデータおよび命令を送信するように結合されている。

【０１６７】

これらのコンピュータプログラム（プログラム、ソフトウェア、ソフトウェアアプリケーションまたはコードとしても公知）はプログラマブルプロセッサのためのマシン命令を含んでおり、高レベル手続きおよび／もしくはオブジェクト指向プログラミング言語で、ならびに／またはアセンブリ／マシン言語で実現され得る。本明細書において使用する「マシン読取可能媒体」、「コンピュータ読取可能媒体」という用語は、マシン命令および／またはデータをプログラマブルプロセッサに提供するために用いられる任意のコンピュータプログラムプロダクト、装置および／またはデバイス（たとえば磁気ディスク、光ディスク、メモリ、プログラマブルロジックデバイス（ＰＬＤ））を指し、マシン命令をマシン読取可能信号として受信するマシン読取可能媒体を含む。「マシン読取可能信号」という用語は、マシン命令および／またはデータをプログラマブルプロセッサに提供するために用いられる任意の信号を指す。

【０１６８】

ユーザとのインタラクションを提供するために、本明細書に記載のシステムおよび技術は、情報をユーザに表示するためのディスプレイデバイス（たとえばＣＲＴ（陰極線管）またはＬＣＤ（液晶ディスプレイ）モニタ）と、ユーザが入力をコンピュータに提供する際に使用可能なキーボードおよびポインティングデバイス（たとえばマウスまたはトラックボール）とを有するコンピュータ上で実現され得る。他の種類のデバイスを用いてユーザとのインタラクションを提供することもでき、たとえば、ユーザに提供されるフィードバックは任意の形態の感覚フィードバック（たとえば視覚フィードバック、聴覚フィードバック、または触覚フィードバック）であり得、ユーザからの入力は、音響入力、スピーチ入力、または触覚入力を含む任意の形態で受信され得る。

【０１６９】

本明細書に記載のシステムおよび技術は、バックエンドコンポーネントを（たとえばデータサーバとして）含むコンピューティングシステムにおいて実現され得るか、またはミドルウェアコンポーネント（たとえばアプリケーションサーバ）を含むコンピューティングシステムにおいて実現され得るか、またはフロントエンドコンポーネント（たとえば、ユーザが上記のシステムおよび技術の実現例とインタラクションする際に使用可能なグラフィックユーザインターフェイスもしくはウェブブラウザを有するクライアントコンピュ

ータ）を含むコンピューティングシステムにおいて実現され得るか、またはそのようなバックエンド、ミドルウェア、もしくはフロントエンドコンポーネントの任意の組合せを含むコンピューティングシステムにおいて実現され得る。システムのコンポーネントは、任意の形態または媒体のデジタルデータ通信（たとえば通信ネットワーク）によって相互に接続され得る。通信ネットワークの例は、ローカルエリアネットワーク（「ＬＡＮ」）、ワイドエリアネットワーク（「ＷＡＮ」）、（アドホックまたはスタティックメンバーを有する）ピアツーピアネットワーク、グリッドコンピューティングインフラストラクチャ、および、インターネットを含む。

【０１７０】

コンピューティングシステムはクライアントおよびサーバを含み得る。クライアントおよびサーバは一般に互いにリモートであり、典型的に通信ネットワークを介してインタラクションする。クライアントとサーバとの関係は、それぞれのコンピュータ上で実行されて互いにクライアントーサーバ関係を有するコンピュータプログラムによって生じる。

【０１７１】

本発明の多数の実施形態を説明した。しかしながら、本発明の精神および範囲から逸脱することなくさまざまな変更がなされ得ることが理解されるであろう。たとえば、ステップが再順序付けされるか、加えられるか、または、除去された状態で、上に示されたフローのさまざまな形態が使用されてもよい。さらにローカルデバイス認証のいくつかの適用例が記載されたが、多数の他の適用例が考えられるということが認識されるべきである。したがって、他の実施形態も添付の請求の範囲内にある。

【図１】

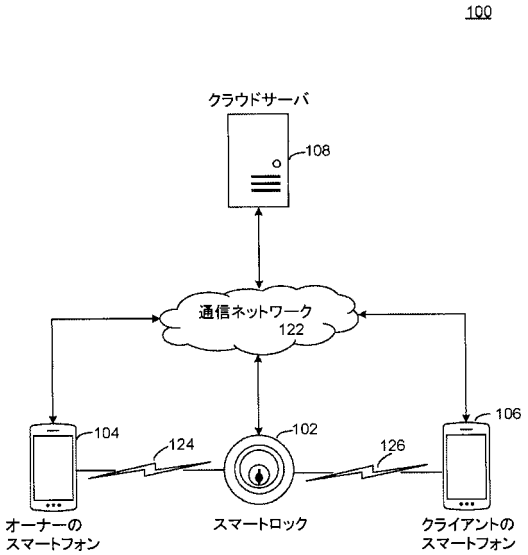

FIG. 1

【図２】

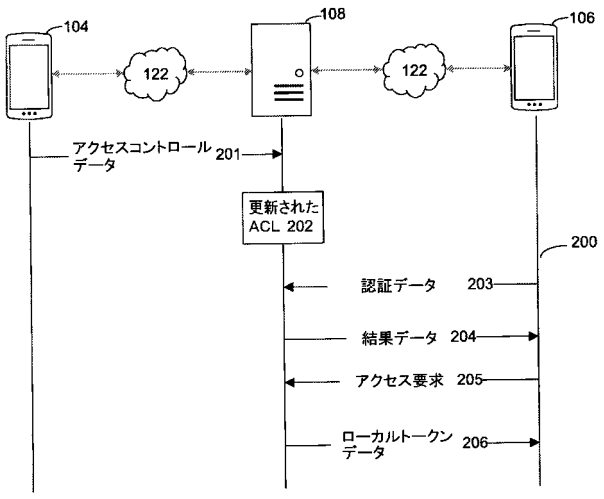

FIG. 2

【図３】

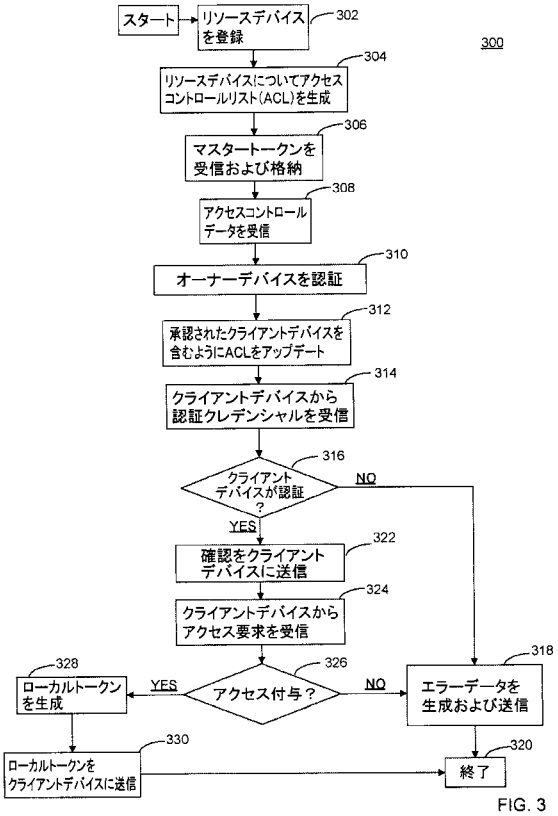

FIG. 3

【図４】

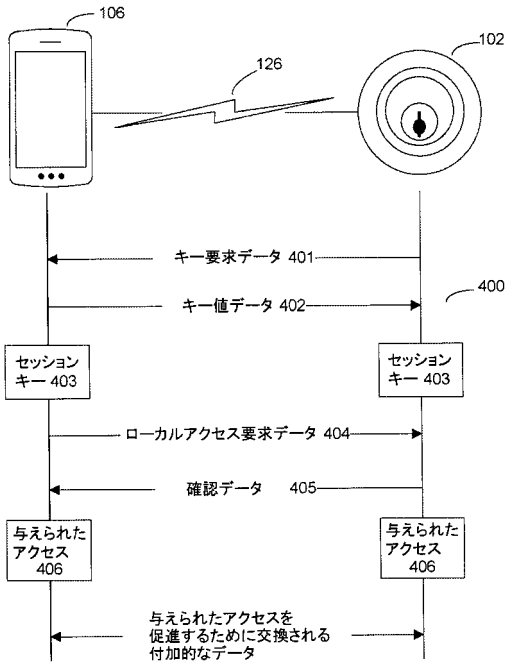

FIG. 4

【図５】

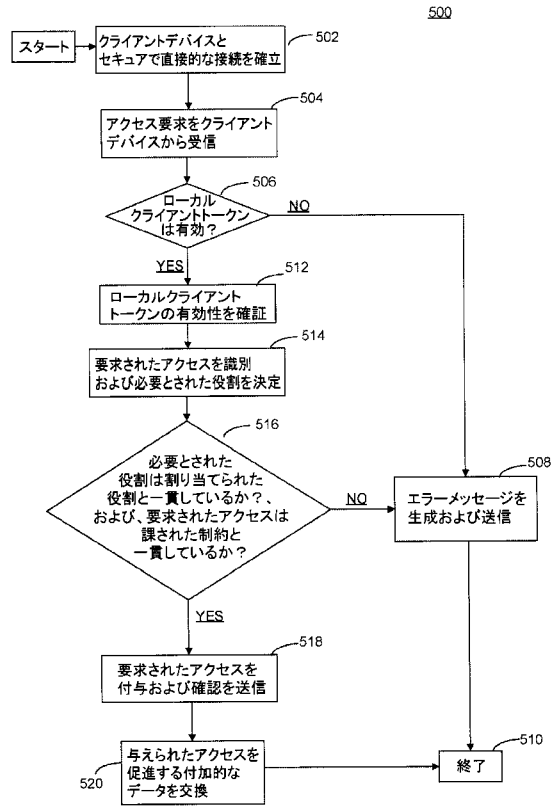

FIG. 5

【図６】

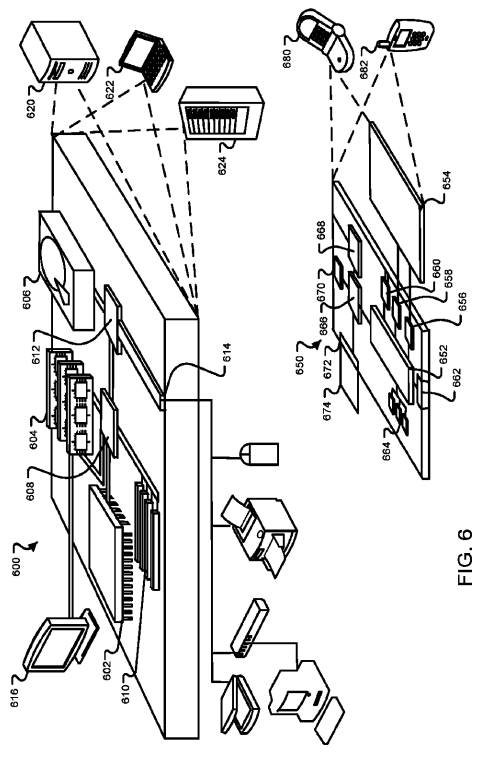

FIG. 6

【手続補正書】
【提出日】平成30年6月26日(2018.6.26)
【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】
コンピュータによって実現される方法であって、
装置の１つ以上のプロセッサによって、リソースデバイスについてのマスターアクセストークンを取得することと、
前記１つ以上のプロセッサによって、クライアントデバイスに関連付けられるユーザを識別することと、
前記１つ以上のプロセッサによって、前記ユーザが前記リソースデバイスへの制限のあるアクセスを受けることを承認されていることを決定することと、
前記決定することに応答して、前記１つ以上のプロセッサによって、前記マスターアクセストークンに基づいてローカルアクセストークンを生成することとを含み、前記ローカルアクセストークンは、前記リソースデバイスがネットワーク接続を有することを必要とすることなく、前記リソースデバイスへのアクセスを与えるように構成されており、さらに
前記１つ以上のプロセッサによって、前記リソースデバイスについての前記ローカルアクセストークンを前記クライアントデバイスに提供することを含む、方法。
【請求項２】
前記決定することは、前記リソースデバイスのオーナー、または、前記リソースデバイスへのアクセスをコントロール可能なエンティティのうちの少なくとも一方によって、前記ユーザが前記リソースデバイスへの前記制限のあるアクセスを受けることを承認されていることを決定することを含む、請求項１に記載の方法。
【請求項３】
前記識別することは、前記リソースデバイスへの前記制限のあるアクセスを取得するための要求を前記クライアントデバイスから受信することを含み、前記要求は、前記ユーザの識別子または前記クライアントデバイスの識別子のうちの少なくとも１つを含んでおり、
前記識別することはさらに、前記要求に応答して、前記リソースデバイスについての前記ローカルアクセストークンを前記クライアントデバイスに提供することを含む、請求項１または請求項２に記載の方法。
【請求項４】
前記方法はさらに、
受信した前記要求の少なくとも部分に基づいて前記クライアントデバイスを識別することと、
前記クライアントデバイスが前記リソースデバイスへの前記制限のあるアクセスを受けることを承認されていることを決定することとを含み、
前記生成することは、前記クライアントデバイスが前記制限のあるアクセスを受けることを承認されていることを決定することに応答して、前記ローカルアクセストークンを生成することを含む、請求項３に記載の方法。
【請求項５】
前記リソースデバイスについてのアクセスコントロールリストを取得することをさらに含み、前記アクセスコントロールリストは、前記リソースデバイスへの対応する制限のあるアクセスを受けることを承認されている１人以上のユーザを識別する、請求項１に記載の方法。

【請求項６】
前記装置は、ローカルメモリに前記アクセスコントロールリストを格納するように構成される、請求項５に記載の方法。
【請求項７】
前記決定することは、
前記１人以上の承認されているユーザが、前記クライアントデバイスに関連付けられる前記ユーザを含むということを、前記アクセスコントロールリストに基づいて決定することと、
前記１人以上の承認されているユーザが前記ユーザを含むということを決定することに応答して、前記クライアントデバイスの前記ユーザが前記制限のあるアクセスを受けることを承認されていることを確証することとを含む、請求項５または請求項６に記載の方法。
【請求項８】
前記方法はさらに、オーナーデバイスからアクセスコントロールデータを受信することを含み、前記オーナーデバイスは前記リソースデバイスのオーナーに関連付けられており、前記アクセスコントロールデータは、前記ユーザが前記リソースデバイスへの前記制限のあるアクセスを受けることを承認しており、
前記方法はさらに、前記クライアントデバイスの前記ユーザを承認されたユーザであると識別するために前記アクセスコントロールリストの少なくとも部分を修正することを含む、請求項５～７のいずれか１項に記載の方法。
【請求項９】
前記アクセスコントロールデータはアクセスパラメータを含み、前記アクセスパラメータは、前記ユーザに与えられる前記制限のあるアクセスの範囲を確証し、
前記方法はさらに、前記アクセスパラメータを含むように前記アクセスコントロールリストの少なくとも部分を修正することを含む、請求項８に記載の方法。
【請求項１０】
前記アクセスパラメータは、前記ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含む、請求項９に記載の方法。
【請求項１１】
前記アクセスコントロールリストは、前記ユーザに関連付けられる１つ以上のアクセスパラメータを識別しており、前記アクセスパラメータは、前記ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含む、請求項５に記載の方法。
【請求項１２】
前記ローカルアクセストークンはマカロンを含み、前記マカロンは、１つ以上のキャビアートと、対応するキーとを含み、
前記生成することは、
前記アクセスコントロールリストに基づいて、前記ユーザに関連付けられる前記アクセスパラメータを識別することと、
前記ローカルアクセストークンについての失効時間を確証することと、
前記失効時間および識別された前記アクセスパラメータを前記ローカルアクセストークンの前記１つ以上のキャビアート内に統合する動作を実行することとを含む、請求項１１に記載の方法。
【請求項１３】
前記ユーザの前記ローカルアクセストークンについて確証される前記失効時間を統合するように前記アクセスコントロールリストの少なくとも部分を修正することをさらに含む、請求項１２に記載の方法。

【請求項１４】
前記ローカルアクセストークンは、前記クライアントデバイスに関連付けられる前記ユーザまたは前記クライアントデバイスのうちの少なくとも一方を識別するデータを含んでおり、
前記生成することは、前記ローカルアクセストークンにデジタル署名を適用することを含む、請求項１～７のいずれか１項に記載の方法。
【請求項１５】
前記ローカルアクセストークンはマカロンを含み、前記マカロンは、１つ以上のキャビアートと、対応するキーとを含み、
前記対応するキーは、適用される前記デジタル署名を含んでおり、
前記生成することはさらに、前記１つ以上のキャビアートの少なくとも部分へのＭＡＣアルゴリズムの適用に基づき、前記デジタル署名を生成することを含む、請求項１４に記載の方法。
【請求項１６】
前記１つ以上のキャビアートは、前記ローカルアクセストークンの失効日時、前記ユーザに割り当てられる役割、または、前記ユーザもしくは前記クライアントデバイスのうちの少なくとも一方を識別する前記データのうちの少なくとも１つを含む、請求項１５に記載の方法。
【請求項１７】
前記ローカルアクセストークンはデジタル証明書を含む、請求項１～１１のいずれか１項に記載の方法。
【請求項１８】
前記取得することは、前記リソースデバイスから前記マスターアクセストークンを受信することを含み、
前記生成することは、受信した前記マスターアクセストークンの少なくとも部分に基づいて前記ローカルアクセストークンを生成することを含む、請求項１～７のいずれか１項に記載の方法。
【請求項１９】
前記マスターアクセストークンは第１のマカロンを含み、前記第１のマカロンは、１つ以上の第１のキャビアートと、対応する第１のキーとを含み、
前記ローカルアクセストークンは第２のマカロンを含み、前記第２のマカロンは、１つ以上の第２のキャビアートと、対応する第２のキーとを含む、請求項１８に記載の方法。
【請求項２０】
前記ローカルアクセストークンを生成することは、前記１つ以上の第２のキャビアートを生成することを含み、
前記第２のキャビアートの第１の部分は前記第１のキャビアートを含み、
前記第２のキャビアートの第２の部分は、前記ローカルアクセストークンの失効日時と、前記ユーザの前記制限のあるアクセスに関連付けられる１つ以上のアクセスパラメータとを含み、前記アクセスパラメータは、前記ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含む、請求項１９に記載の方法。
【請求項２１】
前記リソースデバイスからマスターアクセストークンを受信することをさらに含み、前記マスターアクセストークンは、前記クライアントデバイスが前記リソースデバイスの識別性を照合することを可能にし、さらに、
前記決定することに応答して、前記マスターアクセストークンの少なくとも部分に基づいてローカルアクセストークンを生成することと、
前記クライアントデバイスに前記ローカルアクセストークンを提供することとを含む、請求項１に記載の方法。

【請求項２２】
少なくとも１つのプロセッサと、
実行可能な命令を格納するメモリとを含み、
前記命令は、前記少なくとも１つのプロセッサによって実行されると、前記少なくとも１つのプロセッサに、
リソースデバイスについてのマスターアクセストークンを取得するステップと、
クライアントデバイスに関連付けられるユーザを識別するステップと、
前記ユーザが前記リソースデバイスへの制限のあるアクセスを受けることを承認されていることを決定するステップと、
前記決定することに応答して、前記マスターアクセストークンに基づいてローカルアクセストークンを生成するステップとを行わせ、前記ローカルアクセストークンは、前記リソースデバイスがネットワーク接続を有することを必要とすることなく、前記リソースデバイスへのアクセスを与えるように構成されており、
前記命令はさらに、前記少なくとも１つのプロセッサによって実行されると、前記少なくとも１つのプロセッサに、
前記リソースデバイスについての前記ローカルアクセストークンを前記クライアントデバイスに提供するステップを実行させる、装置。
【請求項２３】
前記少なくとも１つのプロセッサはさらに、前記リソースデバイスのオーナー、または、前記リソースデバイスへのアクセスをコントロール可能なエンティティのうちの少なくとも一方によって、前記ユーザが前記リソースデバイスへの前記制限のあるアクセスを受けることを承認されていることを決定するステップを実行する、請求項２２に記載の装置。
【請求項２４】
前記少なくとも１つのプロセッサはさらに、前記リソースデバイスへの前記制限のあるアクセスを取得するための要求を前記クライアントデバイスから受信するステップを実行し、前記要求は、前記ユーザの識別子または前記クライアントデバイスの識別子のうちの少なくとも１つを含んでおり、
前記少なくとも１つのプロセッサはさらに、前記要求に応答して、前記リソースデバイスについての前記ローカルアクセストークンを前記クライアントデバイスに提供するステップを実行する、請求項２２または請求項２３に記載の装置。
【請求項２５】
前記少なくとも１つのプロセッサはさらに、
受信した前記要求の少なくとも部分に基づいて前記クライアントデバイスを識別するステップと、
前記クライアントデバイスが前記リソースデバイスへの前記制限のあるアクセスを受けることを承認されていることを決定するステップと、
前記クライアントデバイスが前記制限のあるアクセスを受けることを承認されていることを決定することに応答して、前記ローカルアクセストークンを生成するステップとを実行する、請求項２４に記載の装置。
【請求項２６】
前記少なくとも１つのプロセッサはさらに、前記リソースデバイスについてのアクセスコントロールリストを取得するステップを実行し、前記アクセスコントロールリストは、前記リソースデバイスへの対応する制限のあるアクセスを受けることを承認されている１人以上のユーザを識別する、請求項２２に記載の装置。
【請求項２７】
前記装置は、ローカルメモリに前記アクセスコントロールリストを格納するように構成される、請求項２６に記載の装置。
【請求項２８】
前記少なくとも１つのプロセッサはさらに、

前記１人以上の承認されているユーザが、前記クライアントデバイスに関連付けられる前記ユーザを含むということを、前記アクセスコントロールリストに基づいて決定するステップと、

前記１人以上の承認されているユーザが前記ユーザを含むということを決定することに応答して、前記クライアントデバイスの前記ユーザが前記制限のあるアクセスを受けることを承認されていることを確証するステップとを実行する、請求項２６または請求項２７に記載の装置。

【請求項２９】

前記少なくとも１つのプロセッサはさらに、オーナーデバイスからアクセスコントロールデータを受信するステップを実行し、前記オーナーデバイスは前記リソースデバイスのオーナーに関連付けられており、前記アクセスコントロールデータは、前記ユーザが前記リソースデバイスへの前記制限のあるアクセスを受けることを承認しており、

前記少なくとも１つのプロセッサはさらに、前記クライアントデバイスの前記ユーザを承認されたユーザであると識別するために前記アクセスコントロールリストの少なくとも部分を修正するステップを実行する、請求項２６～２８のいずれか１項に記載の装置。

【請求項３０】

前記アクセスコントロールデータはアクセスパラメータを含み、前記アクセスパラメータは、前記ユーザに与えられる前記制限のあるアクセスの範囲を確証し、

前記少なくとも１つのプロセッサはさらに、前記アクセスパラメータを含むように前記アクセスコントロールリストの少なくとも部分を修正するステップを実行する、請求項２９に記載の装置。

【請求項３１】

前記アクセスパラメータは、前記ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含む、請求項３０に記載の装置。

【請求項３２】

前記アクセスコントロールリストは、前記ユーザに関連付けられる１つ以上のアクセスパラメータを識別しており、前記アクセスパラメータは、前記ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含む、請求項２６に記載の装置。

【請求項３３】

前記ローカルアクセストークンはマカロンを含み、前記マカロンは、１つ以上のキャビアートと、対応するキーとを含み、

前記少なくとも１つのプロセッサはさらに、

前記アクセスコントロールリストに基づいて、前記ユーザに関連付けられる前記アクセスパラメータを識別するステップと、

前記ローカルアクセストークンについての失効時間を確証するステップと、

前記失効時間および識別された前記アクセスパラメータを前記ローカルアクセストークンの前記１つ以上のキャビアート内に統合する動作を実行するステップと実行する、請求項３２に記載の装置。

【請求項３４】

前記少なくとも１つのプロセッサはさらに、前記ユーザの前記ローカルアクセストークンについて確証される前記失効時間を統合するように前記アクセスコントロールリストの少なくとも部分を修正するステップを実行する、請求項３３に記載の装置。

【請求項３５】

前記ローカルアクセストークンは、前記クライアントデバイスに関連付けられる前記ユーザまたは前記クライアントデバイスのうちの少なくとも１つを識別するデータを含み、

前記少なくとも１つのプロセッサはさらに、前記ローカルアクセストークンにデジタル

署名を適用するステップを実行する、請求項２２～２８のいずれか１項に記載の装置。
【請求項３６】
前記ローカルアクセストークンはマカロンを含み、前記マカロンは、１つ以上のキャビアートと、対応するキーとを含み、
前記対応するキーは、適用された前記デジタル署名を含み、
前記少なくとも１つのプロセッサはさらに、前記１つ以上のキャビアートの少なくとも部分へのＭＡＣアルゴリズムの適用に基づき、前記デジタル署名を生成するステップを実行する、請求項３５に記載の装置。
【請求項３７】
前記１つ以上のキャビアートは、前記ローカルアクセストークンの失効日時、前記ユーザに割り当てられる役割、または、前記ユーザもしくは前記クライアントデバイスのうちの少なくとも一方を識別する前記データのうちの少なくとも１つを含む、請求項３６に記載の装置。
【請求項３８】
前記ローカルアクセストークンはデジタル証明書を含む、請求項２２～３５のいずれか１項に記載の装置。
【請求項３９】
前記少なくとも１つのプロセッサはさらに、
前記リソースデバイスから前記マスターアクセストークンを受信するステップと、
受信した前記マスターアクセストークンの少なくとも部分に基づいて前記ローカルアクセストークンを生成するステップとを実行する、請求項２２～２８のいずれか１項に記載の装置。
【請求項４０】
前記マスターアクセストークンは第１のマカロンを含み、前記第１のマカロンは、１つ以上の第１のキャビアートと、対応する第１のキーとを含み、
前記ローカルアクセストークンは第２のマカロンを含み、前記第２のマカロンは、１つ以上の第２のキャビアートと、対応する第２のキーとを含み、
前記少なくとも１つのプロセッサはさらに、前記１つ以上の第２のキャビアートを生成するステップを実行し、前記第２のキャビアートの第１の部分は前記第１のキャビアートを含み、前記第２のキャビアートの第２の部分は、前記ローカルアクセストークンの失効日時と、前記ユーザの前記制限のあるアクセスに関連付けられる１つ以上のアクセスパラメータとを含み、前記アクセスパラメータは、前記ユーザに割り当てられる役割、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含む、請求項３９に記載の装置。
【請求項４１】
前記少なくとも１つのプロセッサはさらに、前記リソースデバイスからマスターアクセストークンを受信するステップを実行し、前記マスターアクセストークンは、前記クライアントデバイスが前記リソースデバイスの識別性を照合することを可能にし、
前記少なくとも１つのプロセッサはさらに、
前記決定することに応答して、前記マスターアクセストークンの少なくとも部分に基づいてローカルアクセストークンを生成するステップと、
前記クライアントデバイスに前記ローカルアクセストークンを提供するステップとを実行する、請求項２２に記載の装置。
【請求項４２】
命令を含むコンピュータプログラムであって、前記命令は、装置の少なくとも１つのプロセッサによって実行されると、方法を実行し、
前記方法は、
リソースデバイスについてのマスターアクセストークンを取得することと、
クライアントデバイスに関連付けられるユーザを識別することと、

前記ユーザが前記リソースデバイスへの制限のあるアクセスを受けることを承認されていることを決定することと、
前記決定することに応答して、前記マスターアクセストークンに基づいてローカルアクセストークンを生成することとを含み、前記ローカルアクセストークンは、前記ローカルアクセストークンを有効化するために前記リソースデバイスがネットワーク接続を有することを必要とすることなく、前記リソースデバイスへのアクセスを与えるように構成されており、
前記方法はさらに、
前記リソースデバイスについての前記ローカルアクセストークンを前記クライアントデバイスに提供することを含む、コンピュータプログラム。
【請求項４３】
コンピュータによって実現される方法であって、
リソースデバイスの１つ以上のプロセッサによって、クライアントデバイスとのセキュアなワイヤレス接続を確立することと、
前記１つ以上のプロセッサによって、前記クライアントデバイスからのアクセストークンに由来するトークンデータと、前記クライアントデバイスによる前記リソースデバイスへのアクセスの要求とを受信することと、
前記１つ以上のプロセッサによって、ネットワークを介して通信することなく、受信した前記トークンデータが、前記リソースデバイスへのアクセスを承認する有効なトークンに由来すると決定することと、
前記１つ以上のプロセッサによって、前記ネットワークを介して通信することなく、前記アクセストークンが、前記クライアントデバイスによって要求される前記アクセスを提供するのに十分なアクセスのレベルを承認していると決定することと、
受信した前記トークンデータが有効なトークンに由来すると決定することと、前記アクセストークンが前記クライアントデバイスによって要求される前記アクセスを提供するのに十分なアクセスのレベルを承認していると決定することとに応答して、前記１つ以上のプロセッサによって、前記クライアントデバイスによって要求される前記リソースデバイスへの前記アクセスを提供することとを含む、方法。
【請求項４４】
前記セキュアなワイヤレス接続は、前記クライアントデバイスと前記リソースデバイスとの間の直接的なワイヤレス接続を含む、請求項４３に記載の方法。
【請求項４５】
前記直接的なワイヤレス接続は、ブルートゥースローエナジー（ＢＬＥ：Bluetooth Low Energy）接続を含む、請求項４４に記載の方法。
【請求項４６】
前記確立することは、前記クライアントデバイスからキャビアートデータおよびランダムデータを受信することを含み、前記キャビアートデータは、前記クライアントデバイスによってローカルアクセストークンから抽出され、
前記確立することはさらに、
受信した前記キャビアートおよびランダムデータの少なくとも部分に基づいてキー値を計算することと、
計算された前記キー値を前記クライアントデバイスに送信することと、
計算された前記キー値と、前記ローカルアクセストークンに基づいて前記クライアントデバイスによって計算される付加的なキー値との間の対応に基づき、前記クライアントデバイスとの前記セキュアなワイヤレス接続を確立することとを含む、請求項４３～４５のいずれか１項に記載の方法。
【請求項４７】
計算された前記キー値を、セッションキーとして確証することをさらに含む、請求項４６に記載の方法。
【請求項４８】

前記キャビアートデータおよびランダムデータは、共有された対称キーを使用して暗号化されており、
前記確立することはさらに、
受信した前記キャビアートデータおよびランダムデータを復号化することと、
前記共有された対称キーを使用して、計算された前記キー値を暗号化することと、
暗号化された前記キー値を前記クライアントデバイスに送信することとを含む、請求項４６または請求項４７に記載の方法。
【請求項４９】
アクセストークンはマカロンを含み、前記マカロンは、１つ以上のキャビアートと、対応するキーとを含む、請求項４３～４５のいずれか１項に記載の方法。
【請求項５０】
ネットワークを介して通信することなく、受信した前記トークンデータが有効なトークンに由来すると決定するステップは、
受信した前記トークンデータから前記１つ以上のキャビアートを抽出することと、
抽出された前記キャビアートと、前記リソースデバイスによって維持されるマスターアクセストークンとに基づき、受信した前記トークンデータのコピーを計算することと、
受信した前記トークンデータが、計算された前記コピーに対応すると決定することと、
受信した前記トークンデータが、計算された前記コピーに対応する場合、受信した前記トークンデータが有効なトークンに由来すると確証することとを含む、請求項４９に記載の方法。
【請求項５１】
ネットワークを介して通信することなく、受信した前記トークンデータが有効なトークンに由来すると決定するステップはさらに、
抽出された前記キャビアートの少なくとも部分に基づいて、受信した前記トークンデータについてのアクセスのチェーンを識別することと、
受信した前記トークンデータについての前記アクセスのチェーンを照合することとを含む、請求項５０に記載の方法。
【請求項５２】
前記１つ以上のキャビアートは、前記アクセストークンの失効日時と、前記リソースデバイスのオーナーによって前記クライアントデバイスに割り当てられる役割と、１つ以上のアクセスパラメータとを含み、
前記アクセスパラメータは、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含み、
前記リソースデバイスへのアクセスの前記要求は、前記リソースデバイスの１つ以上の要求される機能を識別する、請求項４９～５１のいずれか１項に記載の方法。
【請求項５３】
前記アクセストークンが前記十分なアクセスのレベルを承認していると決定するステップは、
前記失効日時に基づいて、前記アクセストークンが失効していないと決定することと、
前記リソースデバイスの要求される機能へアクセスするために前記クライアントデバイスによって必要とされる役割を識別することと、
必要とされる前記役割が、割り当てられる前記役割と一貫していると決定することと、
前記１つ以上の要求される機能が前記１つ以上のアクセスパラメータと一貫していると決定することと、
（ｉ）前記アクセストークンが失効していないという決定と、（ｉｉ）必要とされる前記役割が、割り当てられる前記役割と一貫しているという決定と、（ｉｉｉ）１つ以上の要求される機能が前記１つ以上のアクセスパラメータと一貫しているという決定とに応答して、前記アクセストークンが、前記要求されるアクセスを提供するのに十分なアクセスのレベルを承認していると確証することとを含む、請求項５２に記載の方法。

【請求項５４】
前記リソースデバイスは、クラウドサーバに関連付けられるコンピュータシステム、サードパーティ認証サービス、または、前記リソースデバイスのオーナーのデバイスのうちの少なくとも１つにアクセスコントロールの決定を委任しており、
前記少なくとも１つのコンピュータシステム、サードパーティ認証サービス、または、オーナーデバイスは、前記アクセストークンを生成し、前記クライアントデバイスに前記アクセストークンを提供する、請求項４３～５３のいずれか１項に記載の方法。
【請求項５５】
前記ネットワークを介して通信することなく、前記確立するステップ、前記受信するステップおよび前記提供するステップを実行することをさらに含む、請求項４３に記載の方法。
【請求項５６】
リソースデバイスであって、
少なくとも１つのプロセッサと、
実行可能な命令を格納するメモリとを含み、前記命令は、前記少なくとも１つのプロセッサによって実行されると、前記少なくとも１つのプロセッサに、
クライアントデバイスとのセキュアなワイヤレス接続を確立するステップと、
前記クライアントデバイスからのアクセストークンに由来するトークンデータと、前記クライアントデバイスによる前記リソースデバイスへのアクセスの要求とを受信するステップと、
ネットワークを介して通信することなく、受信した前記トークンデータが、前記リソースデバイスへのアクセスを承認する有効なトークンに由来していると決定するステップと、
前記ネットワークを介して通信することなく、前記アクセストークンが、前記クライアントデバイスによって要求される前記アクセスを提供するのに十分なアクセスのレベルを承認していると決定するステップと、
受信した前記トークンデータが有効なトークンに由来すると決定することと、前記アクセストークンが前記クライアントデバイスによって要求される前記アクセスを提供するのに十分なアクセスのレベルを承認していると決定することとに応答して、前記クライアントデバイスによって要求される前記リソースデバイスへのアクセスを提供するステップとを実行させる、リソースデバイス。
【請求項５７】
前記セキュアなワイヤレス接続は、前記クライアントデバイスと前記リソースデバイスとの間の直接的なワイヤレス接続を含む、請求項５６に記載のリソースデバイス。
【請求項５８】
前記直接的なワイヤレス接続は、ブルートゥースローエナジー（ＢＬＥ：Bluetooth Low Energy）接続を含む、請求項５７に記載のリソースデバイス。
【請求項５９】
前記少なくとも１つのプロセッサはさらに、
前記クライアントデバイスからキャビアートデータおよびランダムデータを受信するステップを実行し、前記キャビアートデータは、前記クライアントデバイスによってローカルアクセストークンから抽出され、
前記少なくとも１つのプロセッサはさらに、
受信した前記キャビアートおよびランダムデータの少なくとも部分に基づいてキー値を計算するステップと、
計算された前記キー値を前記クライアントデバイスに送信するステップと、
計算された前記キー値と、前記ローカルアクセストークンに基づいて前記クライアントデバイスによって計算される付加的なキー値との間の対応に基づき、前記クライアントデバイスとの前記セキュアなワイヤレス接続を確立するステップとを実行する、請求項５６～５８のいずれか１項に記載のリソースデバイス。

【請求項６０】
前記少なくとも１つのプロセッサはさらに、計算された前記キー値を、セッションキーとして確証するステップを実行する、請求項５９に記載のリソースデバイス。
【請求項６１】
前記キャビアートデータおよびランダムデータは、共有された対称キーを使用して暗号化されており、
前記少なくとも１つのプロセッサはさらに、
受信した前記キャビアートデータおよびランダムデータを復号化するステップと、
前記共有された対称キーを使用して、計算された前記キー値を暗号化するステップと、
暗号化された前記キー値を前記クライアントデバイスに送信するステップとを実行する、請求項５９または請求項６０に記載のリソースデバイス。
【請求項６２】
アクセストークンはマカロンを含み、前記マカロンは、１つ以上のキャビアートと、対応するキーとを含む、請求項５６～５８のいずれか１項に記載のリソースデバイス。
【請求項６３】
前記少なくとも１つのプロセッサはさらに、
前記アクセストークンからの前記１つ以上のキャビアートを識別するステップと、
抽出された前記キャビアートと、前記リソースデバイスによって維持されるマスターアクセストークンとに基づき、受信した前記トークンデータのコピーを計算するステップと、
受信した前記トークンデータが計算された前記コピーに対応すると決定するステップと、
受信した前記トークンデータが計算された前記コピーに対応する場合、受信した前記トークンデータが有効なトークンに由来すると確証するステップとを実行する、請求項６２に記載のリソースデバイス。
【請求項６４】
前記少なくとも１つのプロセッサはさらに、
抽出された前記キャビアートの少なくとも部分に基づいて、前記アクセストークンについてのアクセスのチェーンを識別するステップと、
受信した前記トークンについての前記アクセスのチェーンを照合するステップとを実行する、請求項６３に記載のリソースデバイス。
【請求項６５】
前記１つ以上のキャビアートは、前記アクセストークンの失効日時と、前記リソースデバイスのオーナーによって前記クライアントデバイスに割り当てられる役割と、１つ以上のアクセスパラメータとを含み、
前記アクセスパラメータは、時間的制約、アクセスタイプに対する制約、オフラインアクセスに対する制約、または、前記クライアントデバイスがトークンを生成する能力に対する制約のうちの少なくとも１つを含み、
前記リソースデバイスへのアクセスの前記要求は、前記リソースデバイスの１つ以上の要求される機能を識別する、請求項６２～６４のいずれか１項に記載のリソースデバイス。
【請求項６６】
前記少なくとも１つのプロセッサはさらに、
前記失効日時に基づいて、前記アクセストークンが失効していないと決定するステップと、
前記リソースデバイスの要求される機能へアクセスするために前記クライアントデバイスによって必要とされる役割を識別するステップと、
必要とされる前記役割が、割り当てられる前記役割と一貫していると決定するステップと、
前記１つ以上の要求される機能が前記１つ以上のアクセスパラメータと一貫していると

決定するステップと、
（ｉ）前記アクセストークンが失効していないという決定と、（ｉｉ）必要とされる前記役割が、割り当てられる前記役割と一貫しているという決定と、（ｉｉｉ）１つ以上の要求される機能が前記１つ以上のアクセスパラメータと一貫しているという決定とに応答して、前記アクセストークンが、前記要求されるアクセスを提供するのに十分なアクセスのレベルを承認していると確証するステップとを実行する、請求項６５に記載のリソースデバイス。
【請求項６７】
前記リソースデバイスは、クラウドサーバに関連付けられるコンピュータシステム、サードパーティ認証サービス、または、前記リソースデバイスのオーナーのデバイスのうちの少なくとも１つにアクセスコントロールの決定を委任しており、
前記少なくとも１つのコンピュータシステム、サードパーティ認証サービス、または、オーナーデバイスは、前記アクセストークンを生成し、前記クライアントデバイスに前記アクセストークンを提供する、請求項５６～６６のいずれか１項に記載のリソースデバイス。
【請求項６８】
前記少なくとも１つのプロセッサはさらに、前記ネットワークを介して通信することなく、前記確立するステップ、前記受信するステップおよび前記提供するステップを実行する、請求項５６～６７のいずれか１項に記載のリソースデバイス。
【請求項６９】
命令を含むコンピュータプログラムであって、前記命令は、クライアントデバイスの少なくとも１つのプロセッサによって実行されると、方法を実行し、前記方法は、
クライアントデバイスとのセキュアなワイヤレス接続を確立することと、
前記クライアントデバイスからのアクセストークンに由来するトークンデータと、前記クライアントデバイスによるリソースデバイスへのアクセスの要求とを受信することと、
ネットワークを介して通信することなく、受信した前記トークンデータが、前記リソースデバイスへのアクセスを承認する有効なトークンに由来していると決定することと、
前記ネットワークを介して通信することなく、前記アクセストークンが、前記クライアントデバイスによって要求される前記アクセスを提供するのに十分なアクセスのレベルを承認していると決定することと、
受信した前記トークンデータが有効なトークンに由来すると決定することと、前記アクセストークンが前記クライアントデバイスによって要求される前記アクセスを提供するのに十分なアクセスのレベルを承認していると決定することとに応答して、前記クライアントデバイスによって要求される前記リソースデバイスへの前記アクセスを提供することとを含む、コンピュータプログラム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/066896

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/08
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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2015/002581 A1 (ERICSSON TELEFON AB L M [SE]) 8 January 2015 (2015-01-08)	43-45, 55-58, 68,69
A	page 1, line 4 - page 1, line 7 page 3, line 2 - page 5, line 20 page 6, line 1 - page 10, line 12 claims 1-27 figures 3-5	1-42, 46-54, 59-67

Y	US 2015/143471 A1 (KIM KYUNG-SU [KR] ET AL) 21 May 2015 (2015-05-21)	43-45, 55-58, 68,69
A	paragraph [0001] - paragraph [0016] paragraph [0026] paragraph [0052] - paragraph [0068] claims 31,35,36,40-44,50-52 figures 5,6	1-42, 46-54, 59-67

	-/--	

[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
27 February 2017	08/03/2017

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	Bakdi, Idir

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/066896

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ARNAR BIRGISSON ET AL: "Macaroons: Cookies with Contextual Caveats for Decentralized Authorization in the Cloud", PROCEEDINGS 2014 NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM, 23 February 2014 (2014-02-23), - 26 February 2014 (2014-02-26), XP055347395, Reston, VA DOI: 10.14722/ndss.2014.23212 ISBN: 978-1-891562-35-8 sections I - III -----	1-69

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/066896

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2015002581 A1	08-01-2015	CN 105359480 A	24-02-2016
		EP 3017581 A1	11-05-2016
		HK 1215335 A1	19-08-2016
		JP 2016526844 A	05-09-2016
		US 2016149869 A1	26-05-2016
		WO 2015002581 A1	08-01-2015
US 2015143471 A1	21-05-2015	KR 20130133987 A	10-12-2013
		US 2015143471 A1	21-05-2015
		WO 2013180356 A1	05-12-2013

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

フロントページの続き

(51)Int.Cl.		F I		テーマコード（参考）
Ｈ０４Ｗ 12/08	*(2009.01)*	Ｈ０４Ｗ	12/08	
Ｈ０４Ｗ 12/06	*(2009.01)*	Ｈ０４Ｗ	12/06	

(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,DJ,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,KH,KN,KP,KR,KW,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

（特許庁注：以下のものは登録商標）
１．ＢＬＵＥＴＯＯＴＨ

(72)発明者 チュー，ボー
アメリカ合衆国、９４０４３ カリフォルニア州、マウンテン・ビュー、アンフィシアター・パークウェイ、１６００
(72)発明者 ブカ，ビタリー
アメリカ合衆国、９４０４３ カリフォルニア州、マウンテン・ビュー、アンフィシアター・パークウェイ、１６００
(72)発明者 エダール，ジェイソン・リード
アメリカ合衆国、９４０４３ カリフォルニア州、マウンテン・ビュー、アンフィシアター・パークウェイ、１６００
(72)発明者 セメノフ，アレクセイ
アメリカ合衆国、９４０４３ カリフォルニア州、マウンテン・ビュー、アンフィシアター・パークウェイ、１６００
(72)発明者 ジャコビー，マッケンジー・リー
アメリカ合衆国、９４０４３ カリフォルニア州、マウンテン・ビュー、アンフィシアター・パークウェイ、１６００
(72)発明者 グプタ，ビカス
アメリカ合衆国、９４０４３ カリフォルニア州、マウンテン・ビュー、アンフィシアター・パークウェイ、１６００

Ｆターム(参考) 5J104 AA08 JA03 LA02 NA02 NA03 PA07 PA14
5K067 AA35 DD17 EE02 EE16 HH22