

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7607039号
(P7607039)

(45)発行日 令和6年12月26日(2024.12.26)

(24)登録日 令和6年12月18日(2024.12.18)

(51)国際特許分類		F I			
H 0 4 L	9/32 (2006.01)	H 0 4 L	9/32	2 0 0 E	
H 0 4 L	9/08 (2006.01)	H 0 4 L	9/08	B	
G 0 6 Q	20/38 (2012.01)	H 0 4 L	9/08	E	
G 0 6 Q	50/06 (2024.01)	H 0 4 L	9/32	2 0 0 A	
G 0 6 F	21/62 (2013.01)	G 0 6 Q	20/38	3 1 0	
請求項の数 19 (全43頁) 最終頁に続く					
(21)出願番号	特願2022-522931(P2022-522931)	(73)特許権者	513113895		
(86)(22)出願日	令和2年10月14日(2020.10.14)		ランディス・ギア イノベーションズ インコーポレイテッド		
(65)公表番号	特表2022-551994(P2022-551994 A)		LANDIS+GYR INNOVATIONS, INC.		
(43)公表日	令和4年12月14日(2022.12.14)		アメリカ合衆国 3 0 0 2 2 ジョージア州 アルファレッタ ミル クリーク アベニュー 3 0 0 0 0		
(86)国際出願番号	PCT/US2020/055636	(74)代理人	100145403		
(87)国際公開番号	WO2021/076669		弁理士 山尾 憲人		
(87)国際公開日	令和3年4月22日(2021.4.22)	(74)代理人	100135703		
審査請求日	令和5年10月4日(2023.10.4)		弁理士 岡部 英隆		
(31)優先権主張番号	16/656,615	(74)代理人	100189544		
(32)優先日	令和1年10月18日(2019.10.18)		弁理士 柏原 啓伸		
(33)優先権主張国・地域又は機関	米国(US)	(72)発明者	デシュムク, プシュベシュ クマール		最終頁に続く

(54)【発明の名称】 資源分配ネットワークにおける資源へのアクセスを制御するためのセキュアトークン

(57)【特許請求の範囲】

【請求項1】

ヘッドエンドシステム及びメータを備えるシステムであって、

前記ヘッドエンドシステムは、

メータに対して行われる支払いに基づくクレジット値による支払いベースのトークンを生成する要求を受信するステップであって、該クレジット値は、負のクレジット値限界と正のクレジット値限界との間の値をとるように構成される、受信するステップと、前記メータの識別子と前記クレジット値とに基づいて、前記支払いベースのトークンを生成するステップと、及び

メッシュネットワークに接続された前記メータに前記支払いベースのトークンを送信するステップと

を行うように構成され、

前記メータは、地理的位置に設置され、少なくとも前記メッシュネットワークを介して前記ヘッドエンドシステムと通信し、

前記メータは、

前記支払いベースのトークンを受信するステップと、

前記支払いベースのトークンを検証するステップであって、前記メータの識別子に関連する情報に基づいて、前記支払いベースのトークンが前記メータに対して生成されることを判定することを含む、検証するステップと、及び、

前記支払いベースのトークンが有効であると判定することに応答して、前記支払いベース

のトークンにて指定される前記クレジット値に基づいて、前記メータと関連付けられる残高を判定するステップと、
前記メータと関連付けられる残高に基づいて、資源分配ネットワークから、前記メータと関連付けられる構内を接続する又は切断するステップと
を行うように構成され、
前記ヘッドエンドシステムは、更に、
前記支払いベースのトークンを生成する前に、秘密鍵及びトークン受入パラメータを含むプロビジョニングデータを少なくとも前記メッシュネットワークを介して前記メータに送信するステップを行うように構成される、
システム。

10

【請求項 2】

前記支払いベースのトークンは、更に、少なくとも前記メータの識別子を暗号化することによって生成される完全性フィールドを含み、

前記支払いベースのトークンがメータに対して生成されることを判定するステップは、前記秘密鍵を使用して前記メータの識別子を暗号化して認証コードを生成するステップと、

前記認証コードと前記支払いベースのトークンの前記完全性フィールドとを比較するステップと、

前記認証コードが前記支払いベースのトークンの前記完全性フィールドと一致することを判定することに応答して、前記支払いベースのトークンが前記メータに対して生成されることを判定するステップと、及び、

20

前記認証コードが前記支払いベースのトークンの前記完全性フィールドと一致しないことを判定することに応答して、前記支払いベースのトークンが前記メータに対して生成されないことを判定するステップと

を含む、請求項 1 に記載のシステム。

【請求項 3】

前記ヘッドエンドシステムは、更に、前記支払いベースのトークンに対してシリアル番号を生成するステップを行うように構成され、前記支払いベースのトークンにトランザクション識別子を含み、

前記トランザクション識別子は、前記シリアル番号の少なくとも一部を構成し、

前記支払いベースのトークンの前記完全性フィールドは、更に、少なくとも前記支払いベースのトークンの前記シリアル番号と前記メータの識別子とを暗号化することにより生成され、並びに、

30

前記認証コードは、更に、少なくとも前記支払いベースのトークンの前記シリアル番号と前記メータの識別子とを暗号化することにより生成される、

請求項 2 に記載のシステム。

【請求項 4】

前記メータは、更に、

前記トークン受入パラメータに基づき、前記支払いベースのトークンに対する許容可能なウィンドウを判定するステップと、

前記支払いベースのトークンに関連付けられるシリアル番号が前記許容可能なウィンドウ内にあるかを判定するステップであって、前記支払いベースのトークンに関連付けられるシリアル番号が前記許容可能なウィンドウ内にあることを判定することに応答して、前記支払いベースのトークンにて指定される前記クレジット値に基づいて前記メータに関連付けられる残高を判定することが実行される、判定するステップと、及び、

40

前記支払いベースのトークンに関連付けられるシリアル番号が前記許容可能なウィンドウの外側にあることを判定することに応答して、前記支払いベースのトークンを拒否するステップと

を行うように構成されている、

請求項 1 又は 2 に記載のシステム。

【請求項 5】

50

前記トークン受入パラメータは、負のオフセットと正のオフセットとを含み、
前記支払いベースのトークンに対する許容可能なウィンドウを判定するステップは、
前記許容可能なウィンドウの下限を、前記メータで受信される従前の許容可能なセキュアトークンに関連付けられるシリアル番号から前記負のオフセットを引いたものとして判定するステップと、

前記許容可能なウィンドウの上限を、前記メータで受信される従前の許容可能なセキュアトークンに関連付けられるシリアル番号に前記正のオフセットを加えたものとして判定するステップと

によって、実行され、

前記従前の許容可能なセキュアトークンは、支払いベースのトークン、時間ベースのトークン、若しくはグローバルトークンの、いずれかである、

請求項 4 に記載のシステム。

【請求項 6】

前記支払いベースのトークンにて指定される前記クレジット値に基づいて前記メータに関連付けられる残高を判定することは、前記支払いベースのトークンにて指定される前記クレジット値が閾値未満であることを判定することに応答して、前記メータに関連付けられる現在の残高を減少させることを含み、

前記残高が前記閾値未満であることを判定することに応答して、前記資源分配ネットワークから前記構内を切断することが実行される、

請求項 1 又は 2 に記載のシステム。

【請求項 7】

前記支払いベースのトークンは、前記ヘッドエンドシステムから受信され、

前記メータは、更に、

前記支払いベースのトークンと、前記支払いベースのトークンのステータスと、前記メータのステータスと、前記メータに関連付けられる残高とのうちの 1 つ以上を含む応答を生成してヘッドエンドシステムに送信するステップを行うように構成され、

前記支払いベースのトークンのステータスが、受け入れられたステータス若しくは拒否されたステータスを含み、前記メータのステータスが、切断されたステータス若しくは接続されたステータスを含む、

請求項 1 又は 2 に記載のシステム。

【請求項 8】

前記支払いベースのトークンは、前記メータに結合されるデバイスから受信され、

前記メータは、更に、

前記支払いベースのトークンを含むイベントメッセージを生成して前記ヘッドエンドシステムに送信するステップ

を行うように構成されている、請求項 1 又は 2 に記載のシステム。

【請求項 9】

前記ヘッドエンドシステムは、更に、

前記イベントメッセージを受信することに応答して、前記イベントメッセージにて指定される前記支払いベースのトークンが前記ヘッドエンドシステムによって生成されたことを検証するステップと、

前記イベントメッセージにて指定される前記支払いベースのトークンが前記ヘッドエンドシステムによって生成されなかったことを判定することに応答して、前記支払いベースのトークンが前記ヘッドエンドシステムによって生成されなかったことを示す通知を前記メータに送信するステップと、

を行うように構成されており、

前記メータは、更に、

前記支払いベースのトークンが前記ヘッドエンドシステムによって生成されなかったことを示す通知を受信することに応答して、前記残高から前記クレジット値を除去するべく前記メータと関連付けられる前記残高を調整するステップと、

前記メータに関連付けられる前記調整された残高に基づいて、前記資源分配ネットワークから前記構内を接続する若しくは切断するステップを行うように構成されている、請求項 8 に記載のシステム。

【請求項 10】

方法であって、

支払いベースのトークンを生成する前に、ヘッドエンドシステムによって、秘密鍵及びトークン受入パラメータを含むプロビジョニングデータを少なくともメッシュネットワークを介してメータに送信するステップと、

前記メータによって、前記支払いベースのトークンを受信するステップであって、該メータは、該メータに関連付けられる構内の資源分配ネットワークへの接続を制御するように構成され、前記支払いベースのトークンは、前記メータの識別子と、前記メータのために行われる支払いに基づいて判定されるクレジット値とに基づいて生成され、前記クレジット値は、負のクレジット値限度から正のクレジット値限度までの値を取るように構成されている、受信するステップと、

10

前記メータによって、前記支払いベースのトークンを検証するステップであって、前記メータの識別子に関連する情報に基づいて、前記支払いベースのトークンが前記メータに対して生成されることを判定することを含む、検証するステップと、

前記支払いベースのトークンが有効であることを判定することに応答して、前記メータによって、前記支払いベースのトークンにて指定される前記クレジット値に基づいて、前記メータに関連付けられる残高を判定するステップと、

20

前記メータに関連付けられる残高に基づいて、前記メータによって、前記資源分配ネットワークから前記構内を接続する、若しくは切断するステップとを含む、方法。

【請求項 11】

更に、

前記メータに格納されるトークン受入パラメータに基づいて、前記支払いベースのトークンに対する許容可能なウィンドウを判定するステップであって、前記トークン受入パラメータは、前記支払いベースのトークンを受信する前に、リモートコンピューティングデバイスから受信される、判定するステップと、

前記支払いベースのトークンに関連付けられるシリアル番号が前記許容可能なウィンドウ内にあるかを判定するステップであって、前記支払いベースのトークンに関連付けられるシリアル番号が前記許容可能なウィンドウ内にあることを判定することに応答して、前記メータに関連付けられる残高を前記支払いベースのトークンにて指定される前記クレジット値に基づいて判定することが実行される、判定するステップと、

30

前記支払いベースのトークンに関連付けられるシリアル番号が前記許容可能なウィンドウの外側にあることを判定することに応答して、前記支払いベースのトークンを拒否するステップと

を含む、請求項 10 に記載の方法。

【請求項 12】

前記支払いベースのトークンは、更に、少なくとも前記メータの識別子と前記支払いベースのトークンの前記クレジット値とを暗号化することによって生成される完全性フィールドを含み、

40

前記支払いベースのトークンを検証するステップは、更に、

少なくとも前記メータの識別子と前記支払いベースのトークンの前記クレジット値とを暗号化して認証コードを生成するステップと、

前記認証コードと前記支払いベースのトークンの前記完全性フィールドとを比較するステップと、

前記認証コードが前記支払いベースのトークンの前記完全性フィールドと一致することを判定することに応答して、前記支払いベースのトークンが有効であることを判定するステップと、及び、

50

前記認証コードが前記支払いベースのトークンの前記完全性フィールドと一致しないことを判定することに応答して、前記支払いベースのトークンが無効であることを判定するステップと

を含む、請求項 10 又は 11 に記載の方法。

【請求項 13】

前記支払いベースのトークンは、更に、前記支払いベースのトークンに対するシリアル番号から導出されるトランザクション識別子を更に含み、

前記支払いベースのトークンの前記完全性フィールドは、更に、少なくとも前記支払いベースのトークンの前記シリアル番号と前記メータの前記識別子とを暗号化することにより生成され、及び、

前記認証コードは、少なくとも前記支払いベースのトークンの前記シリアル番号と前記メータの前記識別子を暗号化することによって生成される、

請求項 12 に記載の方法。

【請求項 14】

前記支払いベースのトークンにて指定される前記クレジット値に基づいて前記メータに関連付けられる残高を判定することは、前記支払いベースのトークンにて指定される前記クレジット値が閾値未満であることを判定することに応答して、前記メータに関連付けられる現在の残高を減少させることを含み、

前記残高が前記閾値未満であることを判定することに応答して、前記資源分配ネットワークから前記構内を切断することが実行される、

請求項 10 又は 11 に記載の方法。

【請求項 15】

前記支払いベースのトークンは、少なくとも前記メッシュネットワークを介して前記メータと接続するヘッドエンドシステムから受信され、

前記方法は、更に、

前記支払いベースのトークンと、前記支払いベースのトークンのステータスと、前記メータのステータスと、前記メータに関連付けられる残高とのうちの 1 つ以上を含む応答を生成して前記ヘッドエンドシステムに送信するステップを含む、

前記支払いベースのトークンのステータスが、受け入れられたステータス若しくは拒否されたステータスを含み、前記メータのステータスが、切断されたステータス若しくは接続されたステータスを含む、

請求項 10 又は 11 に記載の方法。

【請求項 16】

前記支払いベースのトークンが、前記メータに結合されるデバイスから受信され、

前記方法は、更に、

前記支払いベースのトークンの検証のために、前記支払いベースのトークンを含むイベントメッセージを生成してヘッドエンドシステムに送信するステップ

を含む、請求項 10 又は 11 に記載の方法。

【請求項 17】

方法であって、

支払いベースのトークンを生成する前に、ヘッドエンドシステムによって、秘密鍵及びトークン受入パラメータを含むプロビジョニングデータを少なくともメッシュネットワークを介してメータに送信するステップであって、該プロビジョニングデータは、支払いベースのトークンを受け入れるためのモードで前記メータを動作させるように構成されており、前記メータは、地理的位置における構内の資源分配ネットワークへの接続を制御するように構成される、送信するステップと、

前記メータに対して行われる支払いに基づくクレジット値による前記支払いベースのトークンを生成する要求を、前記ヘッドエンドシステムによって、受信するステップであって、該クレジット値は、負のクレジット値限界と正のクレジット値限界との間の値を取るように構成される、受信するステップと、

前記ヘッドエンドシステムによって、前記メータの識別子及び前記クレジット値に基づいて、前記支払いベースのトークンを生成するステップと、

前記ヘッドエンドシステムによって、前記支払いベースのトークンを、少なくとも前記メッシュネットワークを介して前記メータに送信するステップとを含み、

前記支払いベースのトークンは、前記メータと関連付けられる残高を更新するように、及び、前記メータに関連付けられる残高に基づいて前記資源分配ネットワークから前記構内を接続する若しくは切断するように、前記メータによって使用される、方法。

【請求項 18】

前記支払いベースのトークンは、更に、少なくとも前記メータの識別子と前記支払いベースのトークンのクレジット値とを暗号化することによって生成される完全性フィールドを含み、前記完全性フィールドは、前記支払いベースのトークンを検証するように、前記メータによって使用される、
請求項 17 に記載の方法。

【請求項 19】

更に、

特定の支払いベースのトークンを含むイベントメッセージを前記メータから受信することに応答して、前記イベントメッセージにおいて指定される前記特定の支払いベースのトークンが前記ヘッドエンドシステムによって生成されたことを検証するステップと、

前記イベントメッセージにおいて指定される前記特定の支払いベースのトークンが前記ヘッドエンドシステムによって生成されなかったことを判定することに応答して、前記支払いベースのトークンが前記ヘッドエンドシステムによって生成されなかったことを示す通知を前記メータに送信するステップとを含み、

前記通知は、前記残高から前記クレジット値を除去するべく前記メータと関連付けられる前記残高を調整するように、及び、前記メータに関連する前記調整された残高に基づいて前記資源分配ネットワークから前記構内を接続する若しくは切断するように、前記メータにより使用される、

請求項 17 又は 18 に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、一般に、資源分配ネットワークにおける資源へのアクセスを制御することに関する。より詳細には、本開示は、資源へのアクセスを制御するために、資源分配ネットワーク内のメータに対して異なる種類のデバイスレベルのセキュアトークンを生成し適用することに関する。

【背景技術】

【0002】

現在の高度計量インフラストラクチャ（AMI）において、支払い機構に関連付けられる複雑さおよび潜在的なセキュリティ問題のために、資源分配ネットワーク内のメータに支払いを適用するための選択肢は限られている。既存の支払い機構は、メータリングネットワークとは別のサードパーティ製オンライン支払いサービスなどに依存している。したがって、支払い機構のセキュリティは、電力会社や計測ネットワークがほとんど制御できないサードパーティによって実装されたセキュリティ機構に依存する。さらに、支払い機構は、メータリングネットワークから分離されているので、支払いが意図されたメータとは異なるメータに適用される可能性があるという点で、エラーが起こりやすい。

【0003】

さらに、現在のAMIは、一般に、ネットワークインフラストラクチャの問題がある、又は、顧客が時間内に支払いを行うことができない、状況を考慮する支払いバックアップ

10

20

30

40

50

機能を提供しない。これらの状況では、顧客が直面している可能性のある特別な条件にかかわらず、顧客のデバイスは、資源供給から切断される。

【発明の概要】

【0004】

支払いベースのトークン、時間ベースのトークン、またはグローバルトークンを生成し、メタリングシステム内の個々のメータに適用するための装置およびプロセスに関する態様および例が開示される。例えば、システムは、ヘッドエンドシステムと、地理的な場所に設置され、少なくともメッシュネットワークを介してヘッドエンドシステムと通信するメータとを含む。ヘッドエンドシステムは、メータに対して行われる支払いに基づいて、クレジット値を有する支払いに基づくトークンを生成する要求を受信するように構成される。クレジット値は、負のクレジット値限界と正のクレジット値限界との間の値を取るように構成される。ヘッドエンドシステムは、メータの識別子とクレジット値とに基づいて支払いベースのトークンを生成し、支払いベースのトークンをメータに送信するようにさらに構成される。メータは、支払いベースのトークンを受信し、更に、メータの識別子に関連する情報に基づいて支払いベースのトークンがメータのために生成されたことを判定することを含む、支払いベースのトークンを検証することを、行うように構成される。支払ベースのトークンが有効であることを判定することに応答して、メータは、支払ベースのトークンにおいて指定されるクレジット値に基づいてメータに関連付けられる残高を判定し、メータに関連付けられる残高に基づいて資源分配ネットワークからメータに関連付けられる構内を接続または切断するように、さらに構成される。

【0005】

別の実施例では、方法は、メータによって支払いベースのトークンを受信することを含む。メータは、資源分配ネットワークへのメータに関連付けられる構内の接続を制御するように構成される。支払いベースのトークンは、メータの識別子と、メータに対して行われる支払いに基づいて判定されるクレジット値とに基づいて、生成される。クレジット値は、負のクレジット値限界と正のクレジット値限界の間の値を取るように構成される。本方法は、支払ベースのトークンを検証することを更に含み、メータの識別子に関連する情報に基づいて、支払ベースのトークンがメータに対して生成されることを判定することを含む。本方法は、支払ベースのトークンが有効であることを判定することに応答して、支払ベースのトークンにおいて指定されるクレジット値に基づいて、メータに関連付けられる残高を判定することと、メータに関連付けられる残高に基づいて、資源分配ネットワークから構内を接続または切断することとを、さらに含む。

【0006】

さらなる実施例では、方法は、ヘッドエンドシステムによって、少なくともメッシュネットワークを介して、プロビジョニングデータをメータに送信することを含む。プロビジョニングデータは、支払いベースのトークンを受信するモードでメータを動作させるように構成される。メータは、地理的位置に設置され、地理的位置における構内の資源分配ネットワークへの接続を制御するように構成される。本方法は、ヘッドエンドシステムによって、メータに対して行われる支払いに基づくクレジット値を有する支払いベースのトークンを生成する要求を受信することをさらに含む。クレジット値は、負のクレジット値限界と正のクレジット値限界の間の値を取るように構成される。本方法はまた、ヘッドエンドシステムによって、メータの識別子とクレジット値とに基づいて、支払いベースのトークンを生成することと、ヘッドエンドシステムによって、支払いベースのトークンを、少なくともメッシュネットワークを介してメータに送信することとを含む。支払いベースのトークンは、メータによって使用されて、メータに関連付けられる残高を更新し、メータに関連付けられる残高に基づいて資源分配ネットワークから構内を接続または切断する。

【0007】

これらの例示的な態様および特徴は、現在説明されている主題を限定または定義するためではなく、本願で説明される概念の理解を助けるべく例を提供するために言及される。現在説明されている主題の他の態様、利点、および特徴は、本出願全体を検討した後に明

10

20

30

40

50

らかになるであろう。

【図面の簡単な説明】

【0008】

本開示のこれらおよび他の特徴、態様、および利点は、添付の図面を参照して以下の詳細な説明を読むと、よりよく理解される。

【0009】

【図1】図1は、本開示の或る実施例に係る、資源分配ネットワークにおけるメータでセキュアトークンを生成し適用するための例示的な動作環境を示すブロック図である。

【図2】図2は、本開示の或る実施例に係る、資源分配ネットワーク内のメータにおいて支払いベースのトークンを生成し適用するための例示的な動作環境を示す図である。

10

【図3】図3は、本開示の或る実施例に係る、ヘッドエンドシステムによって生成され、資源分配ネットワーク内のメータで適用される支払いベースのトークンの一例を示す図である。

【図4】図4は、本開示の或る実施例に係る、セキュアトークンが資源分配ネットワーク内のメータで受け入れられ適用され得るようにメータをプロビジョニングするためのプロセスの一例を示す図である。

【図5】図5は、本開示の或る実施例に係る、資源分配ネットワーク内のメータにおいて支払いベースのトークンを生成し適用するためのプロセスの一例を示す図である。

【図6】図6は、本開示の或る実施例に係る、資源分配ネットワーク内のメータにおいて時間ベースのトークンを生成し適用するための例示的な動作環境を示す図である。

20

【図7】図7は、本開示の或る実施例に係る、ヘッドエンドシステムによって生成され、資源分配ネットワーク内のメータで適用される支払いベースのトークンの一例を示す図である。

【図8】図8は、本開示の或る実施例に係る、資源分配ネットワーク内のメータにおいて支払いベースのトークンを生成し適用するためのプロセスの一例を示す図である。

【図9】図9は、本開示の或る実施例に係る、メータにおいてセキュアトークンを検証するためのプロセスの一例である。

【図10】図10は、本開示の或る実施例に係る、資源分配ネットワークにおけるメータでグローバルトークンを生成し適用するための例示的な動作環境を示す図である。

【図11】図11は、本開示の或る実施例に係る、グローバルトークンテーブルの一例を示す図である。

30

【図12】図12は、本開示の或る実施例に係る、資源分配ネットワーク内のメータで適用可能なグローバルトークンの例を示す。

【図13】図13は、本開示の或る実施例に係る、メータにおいてグローバルトークンを生成し適用するためのプロセスの一例を示す図である。

【図14】図14は、本開示の或る実施例に係る、メータでセキュアトークンを受信し処理するためのプロセスの一例を示す図である。

【図15】図15は、本明細書に提示する技法および技術の態様を実装するのに適したメータの一例を示すブロック図である。

【図16】図16は、本明細書に提示する技法および技術の態様を実装するのに適したヘッドエンドシステムの一例を示すブロック図である。

40

【発明を実施するための形態】

【0010】

資源分配ネットワーク内のメータにおいてセキュアトークンを生成し適用するためのシステムおよび方法が提供される。メータは、それぞれの場所での資源消費を測定するように構成され、さらに、メッシュネットワークを介してヘッドエンドシステムと通信している。ヘッドエンドシステムは、様々な種類のセキュアトークンを生成するように構成される。セキュアトークンは、支払いベースのトークン、時間ベースのトークン、またはグローバルトークンを含むことができる。支払いベースのトークンは、特定のメータに対して行われた支払いに応答して生成され、その支払いに対応するクレジット値を有する。支払

50

いベースのトークンは、資源供給への接続を維持すべきか切断すべきかを判定する、メータに関連付けられる残高を更新するために、メータにおいて適用され得る。時間ベースのトークンは、特定のメータに対して行われた要求に応答して生成され、それに関連付けられる時間期間を有する。時間ベースのトークンは、資源供給との接続を時間ベースのトークンで指定される時間期間だけ延長するために、メータに適用することができる。グローバルトークンは、特定のメータではなく、メータのグループに対して生成され、また、時間期間が関連付けられている。グローバルトークンは、グローバルトークンで指定される時間期間によって資源供給との接続を拡張するために、メータのグループ内の各メータで適用されることもできる。

【0011】

いくつかの実施例では、ヘッドエンドシステムは、特定のメータに対して行われた支払いに従って支払いベースのトークンを生成する要求を受信することに応答して、支払いベースのトークンを生成するように構成される。支払いベースのトークンは、支払いに対応するクレジット値を有する。クレジット値は、負のクレジット値限界と正のクレジット値限界とによってスパンされる範囲から取得される値である。ヘッドエンドシステムは、生成された支払いベースのトークンがメータに固有であるように、メータのシリアル番号などの特定のメータの識別子に基づいて、支払いベースのトークンを生成する。支払いベースのトークンはまた、クレジット値を含む。ヘッドエンドシステムは、メッシュネットワークを介して特定のメータに支払いベースのトークンを送信するようにさらに構成される。支払いベースのトークンを受信した後、メータは、支払いベースのトークンの完全性をチェックすることによって、トークンがメータに固有のものであることを検証することによって、及び他の動作を実行することによって、支払いベースのトークンを有効化する。支払いベースのトークンが有効である場合、メータは、支払いベースのトークンに指定されるクレジット値に基づいてメータに関連付けられる残高を判定し、メータに関連付けられる残高に基づいてメータの位置で資源供給を接続または切断するように構成される。

【0012】

他の実施例では、ヘッドエンドシステムは、特定のメータに対する時間ベースのトークンを生成する要求を受信することに応答して、時間ベースのトークンを生成するようにさらに構成される。時間ベースのトークンは、それに関連付けられる時間期間を有し、それは、ユーザによって要求されるか、又は或る規則に基づいてヘッドエンドシステムによって選択され得る。ヘッドエンドシステムは、メータのシリアル番号など、特定のメータの識別子に基づいて時間ベースのトークンを生成し、生成された時間ベースのトークンがメータに固有であり、他のメータで適用されないようにする。ヘッドエンドシステムは、ネットワーク150及びメッシュネットワークを介して特定のメータに時間ベースのトークンを送信することができる。時間ベースのトークンを受信した後、メータは、時間ベースのトークンの完全性をチェックし、トークンがメータに固有のものであることを検証するなど、支払いベースのトークンを検証するのと同様の方法で、時間ベースのトークンを検証する。時間ベースのトークンが有効である場合、メータは、メータに関連付けられる時間期間を判定し、少なくとも時間ベースのトークンで指定される時間期間の間、メータの位置で資源供給を接続するように構成される。

【0013】

さらなる実施例では、ヘッドエンドシステムは、或る地理的領域に関連付けられ、ヘッドエンドシステムによって管理される複数のメータに適用可能なグローバルトークンを生成するようにも構成される。例えば、ヘッドエンドシステムは、メッシュネットワーク及びヘッドエンドシステムが利用できなくなるような極端な気象条件などの特別な又は緊急の状況下で、電力会社による要求に応答して、グローバルトークンを生成することができる。一例では、グローバルトークンは、それに関連付けられる時間期間を有する。グローバルトークンは、メッシュネットワーク以外のブロードキャストチャネル、例えばラジオネットワーク、テレビネットワーク、または他の緊急通信メカニズム、例えばテキストメッセージングを通じてユーザに分配することができる。メータのユーザは、グローバルト

10

20

30

40

50

ークンをそれぞれのメータに手動で入力することができる。グローバルトークンを受信した後、メータは、グローバルトークンによって指定される時間期間を判定し、判定される時間期間の間、メータの位置で資源供給を接続することができる。

【0014】

本開示で説明される技術は、資源分配ネットワークにおいて適用されるトークンの精度およびセキュリティを高める。ここで生成される支払いベースのトークンは、デバイス固有であり、指定されるメータにのみ適用される。これは、間違ったメータに支払いを適用する機会を減少させ、また、攻撃者によって傍受されたトークンを無意味にする。さらに、ヘッドエンドシステムとメータが複数種類のセキュアトークンを生成し処理するように構成することで、資源分配ネットワークが緊急事態を含むさまざまな状況に対応できる柔軟性を大幅に向上させた。その結果、分配ネットワーク内のメータは、異なる状況に対してモードを切り替える必要がなく、それによって、メータにおける電力、メモリまたはコンピューティング資源などのリソース消費を低減することができる。

【0015】

図1は、資源分配ネットワーク内のメータにおいてセキュアトークンを生成し適用するための例示的な動作環境100を示す。環境100は、資源分配ネットワーク内のメータによって得られた測定データを配信するために、資源分配ネットワークに関連付けられるメッシュネットワーク140を含む。メッシュネットワーク140は、様々な地理的位置に配備された（本明細書では、個別にメータ112と呼ばれることもあり、集散的にメータ112と呼ばれることもある）複数のメータ112A～112Hを含む。メータ112は、電気メータ、ガスメータ、水メータ、蒸気メータなど、ユーティリティネットワークにおける任意のタイプのメータとすることができる。メータ112は、資源消費の特性など、資源分配ネットワークの様々な動作特性を測定するために実装され得る。例えば、電力分配ネットワークにおいて、メータ112は、ネットワークにおける電力使用量に関連する特性を監視し、測定することができる。資源分配ネットワークにおける電力使用に関連する例示的な特性は、平均または総電力消費、電力サージ、停電、および負荷変化を含む。

【0016】

メータ112は、収集したデータをメッシュネットワーク140を介して（本明細書では、個別にルートノード114と呼ぶことも、集散的にルートノード114と呼ぶこともある）ルートノード114Aおよび114Bへ送信する。ネットワーク140のルートノード114は、メータ112の管理、メータ112からのデータの収集、及びヘッドエンドシステム104へのデータの転送などの動作を実行するためにメータ112と通信するように構成されてもよい。ルートノード114は、それ自体がデータを測定し処理するためのノードとして機能するように構成することもできる。ルートノード114は、パーソナルエリアネットワーク（PAN）コーディネータ、ゲートウェイ、またはヘッドエンドシステム104と通信することができる他の任意のデバイスであってもよい。

【0017】

ルートノード114は、最終的に、インターネット、イントラネット、または任意の他のデータ通信ネットワークなどの別のネットワーク150を介して、生成および収集されたメータデータをヘッドエンドシステム104に送信する。ヘッドエンドシステム104は、ルートノード114からデータまたはメッセージのストリームを受信する中央処理システムとして機能することができる。ヘッドエンドシステム104は、収集されたデータを処理または分析することができる。処理されたデータに基づいて、ヘッドエンドシステム104は、請求、性能分析またはトラブルシューティングなどの様々な目的のために、電力会社に関連付けられるユーティリティシステム102とさらに通信する。図1は、ヘッドエンドシステム104及びユーティリティシステム102が別個のシステムであることを示しているが、いくつかの実施例では、これらは1つのシステムで実装されることができる。

【0018】

いくつかの実施例では、メータ112はまた、その地理的位置における、またはそうでなければメータ112に関連付けられる建物構内132の、資源分配ネットワークによって提供される資源供給130への接続を制御するように構成され得る。例えば、電力分配ネットワークにおいて、メータ112は、資源ネットワークの電力供給を建物構内132から接続または切断するために、スイッチ134のステータスを制御するように構成され得る。いくつかの実装では、メータ112は、メータ112のモードに基づいて、建物構内132と資源供給130（すなわち、資源分配ネットワーク）との接続を制御する。

【0019】

メータ112がクレジットモードである場合、メータ112は、建物構内132の資源供給130への接続を継続的に維持し、建物構内132における資源消費を測定する。メータ112は、測定された資源消費を他のデータとともにヘッドエンドシステム104に定期的送信し、ヘッドエンドシステム104はさらにデータをユーティリティシステム102に転送し、ユーザ120のための請求書を生成する。メータ112がプリペイモードである場合、メータ112は、メータ112に関連付けられるクレジット残高又はメータ112に対して指定される接続時間期間に基づいて、建物構内132の資源供給130への接続を制御する。メータ112は、メータ112に関連付けられるクレジット残高が正であるか、もしくは閾値残高値を超えている限り、またはメータ112に対して指定される接続時間持続時間が非ゼロであるか、もしくは閾期間値を超えている限り、建物構内132と資源供給130との間の接続を維持する。メータ112に関連付けられる残高が負になるか、閾値残高値を下回る、または接続時間期間がゼロになると、メータ112はスイッチ134を制御して、建物構内132を資源供給130から切り離すことになる。メータ112に関連付けられる残高または接続時間期間は、メータ112にセキュアトークンを適用することによって調整することができる。プリペイモードにおけるメータ112の動作に関する追加の詳細は、図2～図12に関して以下に提供される。

【0020】

さらなる実施例では、メータ112は、メータ112に関連付けられる様々な情報および資源に関連する特性を表示するように構成されたハンドヘルドデバイス106とも結合され得る。配電ネットワークの例では、ハンドヘルドデバイス106は、建物構内132における電力消費量、電力接続のステータス（例えば、接続又は切断）、メータのモード（例えば、前払いモード又は後払い／クレジットモード）、メータが前払いモードである場合にはメータに関連付けられる残高等を表示するように構成されてもよい。ハンドヘルドデバイス106は、ユーザ120からのユーザ入力を受け入れ、ユーザ入力をメータ112に送信するようにさらに構成される。図2～図12に関して後述するように、ユーザ入力は、セキュアトークンを含んでもよい。

【0021】

ハンドヘルドデバイス106は、任意の有線又は無線方式でメータ112に接続され得る。例えば、ハンドヘルドデバイス106は、ホームエリアネットワーク（HAN）を介してメータ112に接続されることができる。HANを実装するための適切なネットワークキングプロトコルの非限定的な例としては、ZigBee（登録商標）、Bluetooth（登録商標）、Wi-Fi（登録商標）などが挙げられる。HANの非限定的な例としては、電力線通信を介して実装されるHomePlug（登録商標）ネットワーク、同軸ケーブルを介して実装されるアプライアンスとネットワークデバイスとの間のネットワーク接続を提供するMultimedia over Coax Alliance（「MoCA」）ネットワーク、HomePNA Allianceネットワーク等が挙げられる。

【0022】

図1は特定のネットワークトポロジ（例えば、DODAGツリー）を描いているが、他のネットワークトポロジも可能であることを理解されたい（例えば、リングトポロジ、メッシュトポロジ、スタートポロジなど）。さらに、以下の説明では、1つのメータ112の態様に焦点を当てるが、メータが電力源へのアクセスを制御できる限り、メータ112

およびルートノード 114 を含むメッシュネットワーク内の任意のメータによって、本明細書に記載される技術を適用することができる。

【0023】

図 2 は、本開示の或る実施例に係る、資源分配ネットワーク内のメータにおいて支払いベースのトークンを生成し適用するための例示的な動作環境 200 を示す図である。環境 200 は、ユーティリティシステム 102 と、ヘッドエンドシステム 104 と、図 1 に関して上述したようなメータ 112 とを含む。環境 200 は、さらに、支払い処理システム 206、プリペイ自動販売機 208、またはサービスシステム 210 を含む。

【0024】

プリペイ自動販売機 208 は、ユーザ 120 が或るメータ 112 に向けて支払い 212 10
を行うことを可能にする自動化された機械である。複数のプリペイ自動販売機 208 は、ユーザ 120 がそれぞれの場所でメータに対する支払いを行うことができるように、資源分配ネットワークが展開されている地理的領域に展開され得る。サービスシステム 210 は、ユーザ 120 が支払い 212 を行うことを可能にする、例えば、電力会社またはサードパーティによってホストされるコンピューティングシステムを含む。例えば、サービスシステム 210 は、ユーザ 120 が支払い 212 を行うことができるウェブサイト又は電話サービスを提供するように構成されてもよい。

【0025】

支払い処理システム 206 は、支払い 212 を受け取り、支払い 212 を検証し、支払い 212 に関してヘッドエンドシステム 104 又はユーティリティシステム 102 に通知 20
するように構成されている。支払い処理システム 206 は、支払い 212 を処理または検証するために、銀行または信用組合などの金融機関に関連付けられることがある。代替的に、または追加的に、支払い処理システム 206 は、ヘッドエンドシステム 104 またはユーティリティシステム 102 と関連付けられ、さらに金融機関と通信して、支払い 212 を処理してもよい。支払い 212 は、現金、小切手、クレジットカード、デビットカードなどを用いて行われてもよい。

【0026】

資源分配ネットワーク内のメータ 112 が、支払いベースのトークン、時間ベースのトークン、およびグローバルトークンを含むセキュアトークンを受け入れ、処理するために、ヘッドエンドシステム 104 は、最初に、メータ 112 をプロビジョニングして、それらのモードをプリペイモードに切り替えるように構成される。いくつかの実施例では、プロビジョニングは、ヘッドエンドシステム 104 がプロビジョニングデータ 202 をプリペイモードに切り替えられるメータ 112 に送信することによって実行される。メータ 112 に送信されるプロビジョニングデータ 202 は、メータ 112 で受信されたセキュアトークンを検証するためにメータ 112 によって使用される秘密鍵を含むことができる。プロビジョニングデータ 202 は、セキュアトークンが有効であるか否かを判定するためにメータ 112 によって使用される他のパラメータをさらに含むことができる。例えば、プロビジョニングデータ 202 は、セキュアトークンの許容可能なウィンドウを判定するためのトークン受入パラメータを含むことができる。許容可能なウィンドウは、許容可能なセキュアトークンのシリアル番号の範囲を定義する。受信したセキュアトークンのシリアル番号がこの範囲内にある場合、セキュアトークンはメータ 112 で受け入れられ得るが、そうでなければ、メータ 112 はセキュアトークンを拒否することになる。セキュアトークンを検証することに関する追加の詳細は、図 9 に関して以下に提供される。図 10 ~ 図 12 に関して後述するように、プロビジョニングデータ 202 は、許容可能なグローバルトークンを列挙するグローバルトークンテーブルなど、グローバルトークンを処理するためにメータ 112 が使用するデータも含むことができる。

【0027】

プロビジョニングデータ 202 を受信した後、メータ 112 は、そのモードをプリペイモードに切り替え、プロビジョニングデータ 202 をローカルに保存する。いくつかの実装では、メータ 112 は、メータ 112 がプリペイモードに正常に切り替わり、そのモー 50

ドの下で適切に機能していることをヘッドエンドシステム104に知らせるために、プロビジョニング応答をヘッドエンドシステム104に送信するようにも構成される。別の実施例では、メータ112は、設置時にプリペイモードに設定される。その後、メータ112は、ヘッドエンドシステム104との最初の通信の間に、ヘッドエンドシステム104からプロビジョニングデータ202を受信する。

【0028】

メータ112のモードをプリペイモードに切り替えることは、メータ112のユーザの要求によって、または独自の決定に基づいて、電力会社によって要求され得ることに留意されたい。電力会社は、或るメータ112のモードを切り替える要求をトークン命令214に含め、その要求をユーティリティシステム102を介してヘッドエンドシステム104に送信することができる。要求に基づいて、ヘッドエンドシステム104は、切り替えられるべきメータ112のリストを判定し、上述したように、これらのメータの各々を規定する。いくつかの実施例では、セキュリティ上の理由から、プロビジョニングデータ202に含まれる秘密鍵は、他のメータ112に対する秘密鍵とは異なり、メータ112とヘッドエンドシステム104との間の通信に用いられる鍵とも異なっている。トークン受入パラメータなど、プロビジョニングデータ202に含まれる他のパラメータは、異なるメータ112に対して同じであっても異なってもよい。

【0029】

メータ112がプロビジョニングされ、プリペイモードに切り替わると、メータ112は、セキュアトークンを受け入れ、処理することができる。図2に示す例では、メータ112は、支払いベースのトークンを受け入れて処理することができる。時間ベースのトークンやグローバルトークンなどの他のタイプのセキュアトークンは、図6～図12に関して後述する。図2に示す例では、ユーザ120は、図1に関して上述したようにプリペイ自動販売機208またはサービスシステム210を使用して、または他の機構を介して、メータ112に対する支払い212を行うことができる。支払い212を受信すると、支払い処理システム206は、支払い212が有効な支払いであることを確認する。例えば、支払い処理システム206は、支払いに使用される銀行口座又はクレジットカード口座が実在する口座であり、ユーザ120がその口座に支払いをチャージする権限を有するユーザであることを検証し得る。支払い処理システム206は、検証プロセスが失敗した場合、ユーザ120に通知する。

【0030】

支払い処理システム206が、支払い212が有効であることを判定する場合、支払い処理システム206は、支払いベースのトークンの要求216を生成してヘッドエンドシステム104に送信する。支払いベースのトークンの要求216は、支払いベースのトークンが生成されるべきメータの識別子、(本明細書では支払い212の「クレジット値」とも呼ばれる)支払い212の金額、支払いが正か負か、および他の情報などの情報を含むことができる。正の支払いは、支払い処理システム206が、正のクレジット値がメータ112に関連付けられる口座に追加されることを判定したとき、例えば、ユーザ120がメータ112に関連付けられる口座にXドルを追加したときに発生する。負の支払いは、支払い処理システム206が、あるクレジット値をメータ112に関連付けられる口座から差し引くべきであることを判定したときに発生する。負の支払いは、例えば、以前に誤って行われた正の支払いを訂正するため、一時的に行われたクレジット値の調整を取り消すため、ユーザに対して返金を行うため等に利用することができる。

【0031】

支払いベースのトークンの要求216に基づいて、ヘッドエンドシステム104は、支払いベースのトークン204を生成する。支払いベースのトークン204は、トークンのタイプ、トークンに関連付けられるクレジット値、トークンのシリアル番号、トークンが生成されたメータなどの情報に基づいて生成される。これらのタイプの情報は、支払いベースのトークン204の1つ以上のフィールドに明示的に含まれてもよいし、支払いベースのトークン204に含まれる前に変換されてもよい。図3は、本開示の或る実施例に係

10

20

30

40

50

るヘッドエンドシステム104によって生成された支払いベースのトークン204の一例を示す。

【0032】

図3に示される例では、支払いベースのトークン204は、20桁の10進数に相当する66ビットを含む。支払いベースのトークン204の最初の2つのビットは、トークンタイプ302を表すために使用される。いくつかの実施例では、トークンタイプ302の値が0である場合、そのトークンは支払いベースのトークンである。トークンタイプ302の他の値は、他のタイプのセキュアトークンを示すために使用することができる。図3に示す支払いベースのトークン204の次の2ビットは、トークンのサブタイプ304を示し、次の20ビットは、0～10,000米ドル又は他の通貨の範囲であるクレジット値306を示す。

10

【0033】

いくつかの実施例では、サブタイプ304が値0を有する場合、トークン204はクレジット値の正の調整（アジャストメント）を表し、サブタイプ304が値1を有する場合、トークン204はクレジット値の負の調整（アジャストメント）を表す。言い換えれば、サブタイプ304が正の調整（アジャストメント）を示す場合、クレジット値306によって表される量が、メータ112に関連付けられる口座に追加されることになる。サブタイプ304が負の調整（アジャストメント）を示す場合、クレジット値306によって表される量は、メータ112に関連付けられる口座から差し引かれる。

【0034】

20

図3に示される支払いベースのトークン204は、10ビットを含むトランザクションID308のフィールドをさらに含む。いくつかの実施例では、トランザクションID308は、完全なトークン参照番号（TRN）の最下位10ビットを表す。TRNは、メータ112の連続したトークン番号を一意に表す2進数である。初期開始値の後、メータ112のために生成された各トークンは、単調に増加するシーケンシャルTRNを有することになる。いくつかの実施例では、TRNは0から4294967295までの32ビット数であり、トランザクションID308は、この32ビット数の最下位10ビットを表す。

【0035】

図3に示す支払いベースのトークン204はまた、ハッシュベースのメッセージ認証コード（HMAC）などの暗号化ツールを使用することによって一意に計算される完全性フィールド310を含む。完全性フィールド310は、暗号化ツールを適用して、支払いベースのトークン204のフィールド302～308、メータ112のシリアル番号、メータ112のネットワークID、及びトークンのTRNなどの資源分配ネットワーク内でトークンに固有である情報などのデータを暗号化することによって生成することができる。いくつかの実施例では、ヘッドエンドシステム104は、プロビジョニングデータ202に含まれる秘密鍵に基づいて、セキュアハッシュアルゴリズムSHA-256などのハッシュ関数を使用してHMACを生成する。このようにして、メータ112は、支払いベースのトークン204を受信した後、同じ秘密鍵を使用してHMACを生成し、生成されたHMACを受信した支払いベースのトークン204の完全性フィールド310に含まれるものと比較して、トークン204を検証しうる。HMACおよびSHA-256以外の暗号化ツールも、完全性フィールド310を生成するために使用できることを理解されたい。

30

40

【0036】

図2に戻って参照すると、ヘッドエンドシステム104が支払いベースのトークン204を生成した後、ヘッドエンドシステム104は、支払いベースのトークン204を支払い処理システム206または別のシステムに送り返し、そのシステムは、ユーザ120が支払いベースのトークン204のコピーを取得できるように、プリペイド自動販売機208またはサービスシステム210に転送することができる。あるいは、支払いベースのトークン204は、支払いベースのトークン204のコピーをユーザ120に提供するために、支払いベースのトークン204をプリペイド自動販売機208又はサービスシステム21

50

0に直接送信してもよい。いくつかの実施例では、支払いベースのトークン204は、支払い212の受信など、ユーザ120に送信される支払い212の確認に含まれてもよい。

【0037】

いくつかの実装では、プリペイ自動販売機208又はサービスシステム210で支払い212を提出するとき、ユーザ120は、生成された支払いベースのトークン204をメータ112に自動的に適用させることを望むかどうかとも質問される。この点に関してユーザ120によってなされた決定は、ヘッドエンドシステム104がそれに応じて行動できるように、支払いベースのトークンの要求216に含まれることが可能である。ユーザ120が、支払いベースのトークン204のメータ112への自動適用に同意する場合、ヘッドエンドシステム104は、支払いベースのトークン204をメッシュネットワーク140を介してメータ112に送信する。ユーザ120が支払いベースのトークン204の自動適用に同意しない場合、ヘッドエンドシステム104は、支払いベースのトークン204をメータ112に送らない。いくつかの実施例では、ユーザ120は、ヘッドエンドシステム104が支払いベースのトークン204をメータ112に自動的に適用することを許可するが、ある程度の遅延を伴うことを選択することができる。それらの例では、ヘッドエンドシステム104は、指定される量の時間期間を待ち、その後、メッシュネットワーク140を介してメータ112に支払いベースのトークン204を送信する。

【0038】

支払いベースのトークン204を適用するためにヘッドエンドシステム104に頼る代わりに、ユーザ120は、メータ112に関連付けられるハンドヘルドデバイス106を使用して支払いベースのトークン204を入力することができる。言い換えれば、ユーザ120は、ヘッドエンドシステム104による支払いベースのトークン204の自動適用を断り、ハンドヘルドデバイス106を介して支払い212を行った後に受け取った支払いベースのトークン204を入力することができる。これらの例では、ハンドヘルドデバイス106は、ユーザ120が支払いベースのトークン204を入力し、支払いベースのトークン204をメータ112に送信することができるユーザインターフェースを提示するように構成される。

【0039】

ハンドヘルドデバイス106から、又はヘッドエンドシステム104から、支払いベースのトークン204を受信すると、メータ112は、支払いベースのトークン204の検証を開始する。メータ112は、支払いベースのトークン204を解析して、支払いベースのトークン204に含まれるフィールドの各々を判定することができる。メータ112はさらに、プロビジョニングデータ202に含まれる秘密鍵を使用して、ヘッドエンドシステム104が完全性フィールド310を生成するために使用するのと同じ情報に基づいて、HMACなどの認証コードを生成する。この情報は、例えば、メータのシリアル番号、メータのネットワークID、TRN、及び支払いベースのトークン204の他のフィールド、すなわち、トークンタイプ302、サブタイプ304、クレジット値306、及びトランザクションID308を含むことが可能である。生成された認証コードが支払いベースのトークン204の完全性フィールド310と一致する場合、メータ112は、支払いベースのトークン204がヘッドエンドシステム104によって生成され、支払いベースのトークン204のコンテンツが変更されていないことを判定することができる。

【0040】

完全性フィールド310のHMACを生成するための入力に、メータ112のシリアル番号およびネットワークIDなどのメータ112の識別子を含めることによって、生成された支払いベースのトークン204は、意図されたメータ112に結びつけられる。その結果、支払いベースのトークン204が異なるメータによって受信された場合、そのメータは、その計算されたHMACが完全性フィールド310と一致しないことを判定することによって、支払いベースのトークン204が自分用に意図されていないことを判定でき、その後、支払いベースのトークン204を廃棄することが可能となる。このようにして、支払いベースのトークン204が正しいメータ112で適用されることが保証され得る。

【0041】

さらなる実施例では、メータ112はまた、受信した支払いベースのトークン204のトランザクションIDが許容可能なウィンドウ内にあるかどうかを判定するように構成される。上記で簡単に説明したように、許容可能なウィンドウは、プロビジョニングデータ202に含まれるトークン受入パラメータに基づいて判定することができる。許容可能なウィンドウを判定し、支払いベースのトークン204が許容可能なウィンドウ内にあるかどうかを判定することの更なる詳細は、図9に関して以下に提供される。

【0042】

いくつかの実施例では、メータ112はまた、受信した支払いベースのトークン204が、以前に受信され処理された重複したトークンであるかどうかを判定するように構成されてもよい。これらの例では、メータ112は、メータ112が過去に受信し処理したトークンまたはTRNなどのトークン識別子(ID)220を格納するように構成されている。現在の支払いベースのトークン204が過去のトークンID220のいずれかと一致する場合、メータ112は、受信した支払いベースのトークン204が重複しており、有効なトークンではないことを判定することができる。

【0043】

メータ112が、受信した支払いベースのトークン204が有効なトークンであることを判定する場合、メータ112は、支払いベースのトークン204で指定されるサブタイプ304に従って、クレジット値306をメータ112に関連付けられる口座の残高に適用する。例えば、サブタイプ304が、トークンが負の調整(アジャストメント)のためのものであると指定する場合、メータ112は、口座の残高をクレジット値306によって減少させ、サブタイプ304が、トークンが正の調整(アジャストメント)のためのものであると指定する場合、メータ112は、口座の残高をクレジット値306によって増大させる。調整後の口座の残高に基づいて、メータ112は、建物構内132を資源供給130から接続又は切断することができる。言い換えれば、調整後、メータ112に関連付けられる残高が負から正に(又は、閾残高未満から閾残高以上に)変更された場合、メータ112は、例えば、スイッチ134を閉じることによって、資源供給130を建物構内132に接続させるであろう。メータ112に関連付けられる残高が正から負に(又は、閾残高以上から閾残高未満に)変更される場合、メータ112は、例えばスイッチ134を開くことによって、資源供給130を建物構内132から切断するであろう。調整後、メータ112に関連付けられる残高が正または閾残高の上(または負または閾残高の下)にある場合、メータ112は、建物構内132と資源供給130(すなわち資源分配ネットワーク)との間の接続(または切断)を維持することになる。

【0044】

建物構内132が資源供給130に接続されるときは常に、メータ112は、建物構内132における資源消費を測定し、資源消費に基づいてメータ112に関連付けられる残高を更新する。例えば、メータ112は、資源消費量を、資源が消費される時点のレートに基づいて貨幣価値に変換することができる。次いで、メータ112は、変換された貨幣量によってメータに関連付けられる残高を減少させる。メータ112は、残高が負または閾残高未満になると、建物構内132を資源供給130から切断し、正の残高または閾残高以上をもたらす新しいトークンが受信されると、再接続することになる。

【0045】

メータ112が支払いベースのトークン204を受信する場所に応じて、メータ112は、トークン適用応答218またはイベントメッセージ222を生成し、ヘッドエンドシステム104に送信することになる。支払いベースのトークン204がヘッドエンドシステム104から受信された場合、メータ112は、メータ112で受信された支払いベースのトークン204のステータスを報告するために、トークン適用応答218を生成する。いくつかの実装では、トークン適用応答218は、支払いベースのトークン204のステータスを含む。支払いベースのトークン204のステータスは、例えば、「トークンがメータで正常に適用された」、「トークンが許容可能なウィンドウの外にあるので拒否さ

10

20

30

40

50

れた」、「トークンが重複しているので拒否された」、「完全性チェックに失敗したので拒否された」など、含むことができる。

【0046】

トークン適用応答218は、メータ112に適用されたクレジット値、支払いベースのトークン204が適用された後のメータ112に関連付けられる残高、メータスイッチ134のステータス（例えば、開／切断または閉／接続）などの他の情報をさらに含むことができる。トークン適用応答218は、支払いベースのトークン204、またはTRNもしくはトランザクションIDなどの支払いベースのトークン204のシリアル番号も含んでもよい。トークン適用応答218は、収集されたメータデータなど、メータ112からヘッドエンドシステム104に送信される他のデータと共に送信されてもよく、または別々に送信されてもよい。

10

【0047】

支払いベースのトークン204がハンドヘルドデバイス106を介して受信された場合、メータ112は、支払いベースのトークン204を報告するために、支払いベースのトークン204を含むイベントメッセージ222を生成してヘッドエンドシステム104に送信する。イベントメッセージ222は、支払いベースのトークン204のステータス、メータスイッチ134のステータス、またはトークン適用応答218に含まれる任意の他のデータなどの他のデータを含むこともできる。トークン適用応答218と同様に、イベントメッセージ222は、収集されたメータデータなどの他のデータと共にヘッドエンドシステム104に送信することができ、又は別々に送信することができる。

20

【0048】

イベントメッセージ222を受信すると、ヘッドエンドシステム104は、イベントメッセージ222に含まれる支払いベースのトークン204が、ヘッドエンドシステム104によって生成された過去のトークンで検索するなどして、ヘッドエンドシステム104によって生成されたかどうかを判定するために、支払いベースのトークン204を分析する。そして、ヘッドエンドシステム104は、分析結果をメータ112に送信するように構成される。分析結果が、支払いベースのトークン204がヘッドエンドシステム104によって生成されていないことを示す場合、メータ112は、支払いベースのトークン204のクレジット値を除去するために、メータ112に関連付けられる残高を再調整することができる。また、メータ112は、分析結果及び分析結果に基づいてメータ112によって実行されたアクションを示すために、ハンドヘルドデバイス106に警告メッセージを表示させることができる。

30

【0049】

図4は、本開示の或る実施例に係る、メータ112をプリペイモードに切り替えるためのプロセス、および資源分配ネットワーク内のメータ112でセキュアトークンを適用できるようにメータ112をプロビジョニングするためのプロセスの一例を示している。特に、図4は、ヘッドエンドシステム104の態様を示すプロセス400A、およびメータ112の態様を示すプロセス400Bを含む。プロセス400Aおよび400Bは、以下で一緒に説明される。

【0050】

ブロック402において、プロセス400Aは、ヘッドエンドシステム104がプロビジョニングデータ202を生成することを含む。図2に関して上述したように、プロビジョニングデータ202は、メータ112で受信されたセキュアトークンを検証するためにメータ112によって使用される秘密鍵を含むことができる。プロビジョニングデータ202は、受信したセキュアトークンの有効性を判定するためにメータ112によって使用される他のパラメータをさらに含むことができる。例えば、プロビジョニングデータ202は、セキュアトークンの許容可能なウィンドウを判定するためのトークン受入パラメータを含むことができる。プロビジョニングデータ202は、許容可能なグローバルトークンをリストアップするグローバルトークンテーブルをさらに含んでもよい。いくつかの例では、プロビジョニングデータ202は、メータ112にプリペイモードに切り替えるよ

40

50

う求める明示的な命令も含んでもよい。ブロック 404 で、ヘッドエンドシステム 104 は、メッシュネットワーク 140 を介してプロビジョニングデータ 202 をメータ 112 に送信する。

【0051】

ブロック 412 で、プロセス 400 B は、メータ 112 がプロビジョニングデータ 202 を受信することを含む。ブロック 414 において、メータ 112 は、例えば、そのモードをプリペイモードに設定し、実行のためにプリペイモードに対応するファームウェアをロードすることによって、プリペイモードに切り替わる。ブロック 416 において、メータ 112 は、プロビジョニングデータ 202 をメモリまたはメータ 112 によってアクセス可能な他のストレージデバイスに格納する。ブロック 418 において、メータ 112 は、プロビジョニングデータ 202 の受信およびメータ 112 のモード切替を確認するために、ヘッドエンドシステム 104 にプロビジョニング応答を送信する。ブロック 406 で、ヘッドエンドシステム 104 は、プロビジョニング応答を受信し、プロビジョニングプロセスは終了する。

【0052】

上記の例では、メータ 112 がクレジットモードからプリペイモードに切り替わったときにプロビジョニングが実行されると説明したが、メータ 112 がプリペイモードに切り替わった後もプロビジョニングが実行されてもよいことを理解されたい。例えば、プロビジョニング処理は、ヘッドエンドシステム 104 が、セキュアトークンを検証するための秘密鍵、トークン受入パラメータ、またはグローバルトークンテーブルを更新することを決定するたびに実行されてもよい。それらの場合、ブロック 414 はスキップされてもよい。

【0053】

図 5 は、本開示の或る実施例に係る、資源分配ネットワーク内のメータ 112 で支払いベースのトークン 204 を生成し適用するためのプロセスの一例を示す。特に、図 5 は、プロセス 500 A、500 B、および 500 C を含む。プロセス 500 A は、ヘッドエンドシステム 104 の態様を例示する。プロセス 500 B は、メータ 112 の態様を示す。プロセス 500 C は、ハンドヘルドデバイス 106 の態様を示す。プロセス 500 A、500 B、および 500 C は、以下で一緒に説明される。

【0054】

プロセス 500 A は、ヘッドエンドシステム 104 がメータ 112 のための支払いベースのトークンの要求 216 を受信するブロック 502 で始まる。図 2 に関して上述したように、支払いベースのトークンの要求 216 は、メータ 112 のためにユーザ 120 によって行われた支払い 212 に応答して、支払い処理システム 206 によって生成され得る。支払いベースのトークンの要求 216 はまた、例えば、エラーの修正、払い戻しの発行、一時的な調整の取り消しなどのために、メータ 112 に関連付けられる残高を調整するべく支払い処理システム 206 によって生成され得る。このように、要求される支払いベースのトークン 204 は、正の調整（アジャストメント）または負の調整（アジャストメント）とすることができる。

【0055】

ブロック 504 において、プロセス 500 A は、メータ 112 のための支払いベースのトークン 204 を生成することを含む。支払いベースのトークン 204 をメータ 112 に固有のものにするために、支払いベースのトークン 204 は、メータ 112 のシリアル番号、メータ 112 のネットワーク ID、またはこれらの組み合わせなど、メータ 112 の識別子に基づいて生成される。さらに、生成された支払いベースのトークン 204 は、メッシュネットワーク 140 内の支払いベースのトークン 204 に固有のシリアル番号も含むか、またはこれに基づいている。また、支払いベースのトークン 204 は、トークンに関連付けられるクレジット値、及び負の調整（アジャストメント）や正の調整（アジャストメント）などの調整の種類を示す。一例では、支払いベースのトークン 204 は、図 3 に示す形式に従って生成され、トークンタイプ、サブタイプ、クレジット値、トークンの

トランザクションID、及び完全性フィールドを含む。いくつかの実装では、完全性フィールドは、支払いベースのトークン204の1つ以上のフィールド302～308、シリアル番号およびネットワークIDなどのメタ112の識別子、および支払いベースのトークン204のTRNに基づくHMACを生成するために秘密鍵を使用して生成される。

【0056】

ブロック506において、プロセス500Aは、生成された支払いベースのトークン204で支払いベースのトークンの要求216に対して応答することを含む。例えば、ヘッドエンドシステム104は、支払いベースのトークン204を、支払い処理システム206などの支払いベースのトークン204を要求したエンティティに送り、支払いベースのトークン204がユーザ120に転送され得るようにする。別の例では、ヘッドエンドシステム104は、プリペイド自動販売機208又はサービスシステム210など、ユーザ120が支払いを行ったシステムに支払いベースのトークン204を直接送信する。

【0057】

ユーザ120が、生成された支払いベースのトークン204をメタ112に自動的に適用することをヘッドエンドシステム104に認可した場合、ブロック506はさらに、支払いベースのトークン204をメタ112に送ることにより、支払いベースのトークン204を適用することを含む。支払いベースのトークン204のメタ112への適用は、支払いベースのトークン204を適用するための認可をヘッドエンドシステム104に提供する際にユーザ120によって行われる選択に応じて、直ちにまたは一定の遅延をもって実行され得る。

【0058】

ユーザ120がヘッドエンドシステム104に支払いベースのトークン204をメタ112に適用することを認可しない場合、ユーザ120は、ハンドヘルドデバイス106を使用して支払いベースのトークン204を手動で入力することができる。ブロック530において、プロセス500Cは、ユーザ入力によってハンドヘルドデバイス106で支払いベースのトークン204を受信することを含む。ブロック532において、プロセス500Cは、受け取った支払いベースのトークン204を、例えば、HANを通じてメタ112に送信することを含む。

【0059】

ブロック512において、プロセス500Bは、ヘッドエンドシステム104から、またはハンドヘルドデバイス106から、メタ112が支払いベースのトークン204を受信することを含む。ブロック514において、プロセス500Bは、受信した支払いベースのトークン204が有効なトークンであるかどうかを判定するために、支払いベースのトークン204を検証することを含む。検証プロセスは、例えば、支払いベースのトークン204の完全性を判定すること、支払いベースのトークン204がメタ112のために生成されたことを判定すること、トークンが許容可能なウィンドウ内にあることを判定すること、トークンが重複トークンでないことを判定すること、などを含む場合がある。支払いベースのトークン204を検証することに関する追加の詳細は、図9に関して以下に提供される。

【0060】

ブロック516で、プロセス500Bは、支払いベースのトークン204が有効なトークンであるかどうかを判定することを含む。そうでない場合、プロセス500Bは、ブロック520において、支払いベースのトークン204を拒否することを含む。支払いベースのトークン204が有効なトークンである場合、プロセス500Bは、ブロック518において、支払いベースのトークン204に基づいてメタ112に関連付けられる残高を更新し、残高に基づいて資源供給を接続または切断する（または接続または切断された状態を維持する）ことを、含む。支払いベースのトークン204が負の調整（アジャストメント）を示す場合、メタ112は、支払いベースのトークン204において指定されるクレジット値によってメタ112の残高を減少させる。支払いベースのトークン204が正の調整（アジャストメント）を示す場合、メタ112は、支払いベースのトークン

ン 2 0 4 において指定されるクレジット値だけメータ 1 1 2 の残高を増加させる。更新された残高が正である（又は、閾残高を上回る）場合、メータ 1 1 2 は、建物構内 1 3 2 と資源供給 1 3 0 との間の接続を接続又は維持する。更新された残高が負である（または閾残高以下である）場合、メータ 1 1 2 は、建物構内 1 3 2 と資源供給 1 3 0 との間の接続を解除するかまたは切断状態を維持する。

【 0 0 6 1 】

ブロック 5 2 2 において、プロセス 5 0 0 B は、支払いベースのトークン 2 0 4 がヘッドエンドシステム 1 0 4 から受信された場合、図 2 に関して上述したように、トークン適用応答 2 1 8 を送信することを含む。いくつかの実装では、トークン適用応答 2 1 8 は、（受け入れられた、または拒否された、などの）支払いベースのトークン 2 0 4 のステータス、メータ 1 1 2 に適用されたクレジット値、支払いベースのトークン 2 0 4 が適用された後のメータ 1 1 2 に関連付けられる残高、メータスイッチ 1 3 4 のステータス（例えば、開／切断または閉／接続）などの情報、またはそれらの任意の組合せを含んでいる。トークン適用応答 2 1 8 は、支払いベースのトークン 2 0 4、または TRN もしくはトランザクション ID などの支払いベースのトークン 2 0 4 のシリアル番号も含むことができる。

【 0 0 6 2 】

支払いベースのトークン 2 0 4 がハンドヘルドデバイス 1 0 6 から受信された場合、メータ 1 1 2 は、イベントメッセージ 2 2 2 を生成してヘッドエンドシステム 1 0 4 に送信し、受信した支払いベースのトークン 2 0 4 についてヘッドエンドシステム 1 0 4 に知らせ、ヘッドエンドシステム 1 0 4 に支払いベースのトークン 2 0 4 を検証するように要求する。イベントメッセージ 2 2 2 は、トークン適用応答 2 1 8 と同様の内容、例えば、（受け入れられたか拒否されたかなど）支払いベースのトークン 2 0 4 のステータス、メータ 1 1 2 に適用されたクレジット値、支払いベースのトークン 2 0 4 の適用後のメータ 1 1 2 に関連付けられる残高、メータスイッチ 1 3 4 のステータス（開／切断または閉／接続など）を含む場合がある。イベントメッセージ 2 2 2 はまた、支払いベースのトークン 2 0 4 の全体と、ヘッドエンドシステム 1 0 4 が支払いベースのトークン 2 0 4 の真正性を検証するための要求の表示とを含む。図 2 に関して上述したように、トークン適用応答 2 1 8 またはイベントメッセージ 2 2 2 は、メータ 1 1 2 で収集されたメータデータと共に送信されてもよいし、ヘッドエンドシステム 1 0 4 に別個に送信されてもよい。

【 0 0 6 3 】

ヘッドエンドシステム 1 0 4 は、ブロック 5 0 8 でトークン適用応答 2 1 8 またはイベントメッセージ 2 2 2 を受信し、受信したメッセージをそれに応じて処理する。例えば、ヘッドエンドシステム 1 0 4 がイベントメッセージ 2 2 2 を受信した場合、ヘッドエンドシステム 1 0 4 は、イベントメッセージ 2 2 2 に含まれる支払いベースのトークン 2 0 4 を検証し、支払いベースのトークン 2 0 4 が確かにヘッドエンドシステム 1 0 4 によって生成されたかどうかを判定する。ヘッドエンドシステム 1 0 4 は、例えば、メータ 1 1 2 に通知を送信することにより、検証結果をメータ 1 1 2 に通知する。メータ 1 1 2 は、支払いベースのトークン 2 0 4 がヘッドエンドシステム 1 0 4 によって生成されていない場合、メータ 1 1 2 で適用された支払いベースのトークン 2 0 4 をキャンセルするなど、検証結果に応じたアクションを取ることができる。

【 0 0 6 4 】

支払いベースのトークン 2 0 4 がハンドヘルドデバイス 1 0 6 から受信された場合、プロセス 5 0 0 B は、ブロック 5 2 4 において、メータ 1 1 2 がハンドヘルドデバイス 1 0 6 に確認メッセージを送信することをさらに含む。確認メッセージは、例えば、（例えば、受け入れられた、又は拒否された、などの）支払いベースのトークン 2 0 4 のステータス、メータ 1 1 2 に適用されたクレジット値、支払いベースのトークン 2 0 4 が適用された後のメータ 1 1 2 に関連付けられる残高、メータスイッチ 1 3 4 のステータス（例えば、開／切断又は閉／接続）等を含み得る。ハンドヘルドデバイス 1 0 6 は、ブロック 5 3 4 で確認メッセージを受信し、ユーザインターフェースでユーザ 1 2 0 に提示する。

【0065】

プリペイドモードにおいて、メータ112は、一般に、メータ112に関連付けられる残高がゼロ以下であるか又は閾値以下である場合、建物構内132を資源供給130から切断するように構成される。建物構内132のユーザ120は、資源供給130から切断されないために、適時に支払いを行い、支払いベースのトークンをメータ112で適用させる必要がある。いくつかのシナリオでは、ユーザ120の時間及び場所のために、ユーザ120が支払いを行うことは不可能であるか又は不便である。それらのシナリオでは、ユーザ120は、資源供給130との接続をある時間期間延長し、後の時間に支払いを行うために、時間ベースのトークンを要求することができる。

【0066】

図6は、本開示の或る実施例に係る、資源分配ネットワーク内のメータにおいて時間ベースのトークンを生成し適用するための例示的な動作環境600を示す図である。環境600は、図1および図2に関して上述したように、ユーティリティシステム102、ヘッドエンドシステム104、メータ112、およびサービスシステム210を含む。前に論じたように、サービスシステム210は、ユーザ120が支払い212を行うことを可能にするために、例えば、電力会社またはサードパーティによってホストされるコンピューティングシステムを含む。さらに、または代替的に、サービスシステム210は、ユーザ120が時間ベースのトークンを要求することを可能にするように構成されることも可能である。例えば、サービスシステム210は、ユーザ120が時間ベースのトークンを要求することができるウェブサイトまたは電話サービスを提供することができる。

【0067】

ユーザ120から要求を受け取ると、サービスシステム210は、時間ベースのトークンの要求616を生成し、ヘッドエンドシステム104に送信することができる。時間ベースのトークンの要求616は、時間ベースのトークンが生成されるべきメータ112の識別子、時間ベースのトークンに関連付けられる時間期間、期間の開始日などのデータを含むことができる。他の実施例では、支払い処理システム206は、ユーティリティシステム102と通信し得る。次いで、ユーティリティシステム102は、ヘッドエンドシステム104と通信して、時間ベースのトークンの要求616をヘッドエンドシステム104に送信するなどして、時間ベースのトークンを生成するよう要求することができる。

【0068】

時間ベースのトークンの要求616に基づき、ヘッドエンドシステム104は、時間ベースのトークン604を生成する。時間ベースのトークン604は、トークンのタイプ、トークンに関連付けられる時間期間、時間期間が開始する日付、デバイスのシリアル番号、トークンが生成されたメータなどの情報に基づいて生成される。これらのタイプの情報は、時間ベースのトークン604の1つまたは複数のフィールドに明示的に含まれてもよく、または時間ベースのトークン604に含まれる前に変換されてもよい。図7は、本開示の或る実施例に係るヘッドエンドシステム104によって生成される時間ベースのトークン604の一例を示す図である。

【0069】

図7に示す例では、時間ベースのトークン604は、20桁の10進数に相当する66ビットを含む。そのようなものとして、時間ベースのトークン604のサイズは、図3に示される支払いベースのトークン204のサイズと同じである。支払いベースのトークン204と同様に、時間ベースのトークン604の最初の2ビットは、トークンタイプ702を表すためにも使用される。いくつかの実施例では、トークンタイプ702の値が1である場合、そのトークンは時間ベースのトークンである。トークンタイプ702の他の値は、他のタイプのセキュアトークンを示すために使用することができる。図7に示す時間ベースのトークン604の次の15ビットは、時間ベースのトークン604に関連付けられる時間期間の開始日を示す。例えば、15ビットのうちの5ビットおよび4ビットは、それぞれ開始日の日704および月706を表すために使用することができる。15ビットのうちの6ビットは、開始日の年708の下位2桁を表すために使用することができる。

10

20

30

40

50

【0070】

図7に示す時間ベースのトークン604は、1～127日の間の任意の値であり得るトークン604に関連付けられる時間期間を定義する、7ビットで表されるトークン期間710をさらに含む。時間ベースのトークン604に関連付けられる時間期間は、時間ベースのトークン616の要求で指定され得る。他の実施例では、時間期間は、或る規則に基づいてヘッドエンドシステムによって判定または調整され得る。例えば、ルールは、時間ベースのトークン604を最初に要求するユーザに対して時間期間を7日以上とすることができず、時間ベースのトークン604を2回目に要求するユーザに対して5日以下とすることができることと指定し得る。ユーザが時間ベースのトークン604を要求することができる最大時間期間は、ユーザが時間ベースのトークン604を要求する回数が増加するにつれて減少する。他のタイプの規則も利用され得る。

10

【0071】

支払いベースのトークン204と同様に、図7に示す時間ベースのトークン604は、トランザクションID712の10ビットフィールドをさらに含む。いくつかの実施例では、トランザクションID712は、メータ112のための連続したトークン番号を一意に表す2進数である完全なTRNの最下位10ビットを表す。初期開始値の後、メータ112のために生成される各トークンは、それが支払いベースのトークンであろうと時間ベースのトークンであろうと、単調に増加するシーケンシャルTRNを有することになる。いくつかの実施例では、TRNは0から4294967295までの32ビット数であり、トランザクションID712は、この32ビット数の最下位10ビットを表す。

20

【0072】

図7に示す時間ベースのトークン604は、ハッシュベースのメッセージ認証コード（HMAC）などの暗号化ツールを用いて一意に計算される完全性フィールド714も含む。時間ベースのトークン604の完全性フィールド714は、時間ベースのトークン604のフィールド702～710の1つ以上、メータ112のシリアル番号、メータ112のネットワークID、およびトークンのTRNなどの資源分配ネットワーク内でトークンに固有の情報などのデータの暗号化に暗号化ツールを適用することによって生成することができる。いくつかの実施例では、ヘッドエンドシステム104は、プロビジョニングデータ202に含まれる秘密鍵に基づいて、セキュアハッシュアルゴリズムSHA-256などのハッシュ関数を使用してHMACを生成する。このようにして、メータ112は、時間ベースのトークン604を受信した後、同じ秘密鍵を使用してHMACを生成し、生成されたHMACを受信した時間ベースのトークン604の完全性フィールド714に含まれるものと比較して、トークンを検証し得る。検証は、例えば、支払いベースのトークン204の完全性及び真正性を判定することを含む。HMAC以外の暗号化ツールまたはSHA-256以外の暗号化ツールも、完全性フィールド714を生成するために使用できることが理解されるべきである。

30

【0073】

図6に戻ると、ヘッドエンドシステム104が時間ベースのトークン604を生成した後、ヘッドエンドシステム104は、サービスシステム210などの時間ベースのトークン604を要求したシステムに時間ベースのトークン604を送り返し、その結果、サービスシステム210は、時間ベースのトークン604を要求した。このようにして、ユーザ120は、生成された時間ベースのトークン604のコピーを取得することができる。時間ベースのトークン604のコピーを得ることにより、ユーザ120は、ヘッドエンドシステム104に依存することなく、ハンドヘルドデバイス106を使用してメータ112で時間ベースのトークン604を適用することができる。図2に関して上述したように、ハンドヘルドデバイス106は、ユーザ120が時間ベースのトークン604を入力し、時間ベースのトークン604をメータ112に送信することを可能にするユーザインターフェースを提示するように構成され得る。

40

【0074】

あるいは、ユーザ120は、時間ベースのトークン604をヘッドエンドシステム10

50

4によってメータ112に自動的に適用させるよう要求することができる。このような要求は、ヘッドエンドシステム104がそれに応じて行動できるように、時間ベースのトークン604の要求に含めることができる。ユーザ120が時間ベースのトークン604の自動適用を要求した場合、ヘッドエンドシステム104は、時間ベースのトークン604をメッシュネットワーク140を介してメータ112に送信する。ユーザ120が時間ベースのトークン604の自動適用を要求しない場合、ヘッドエンドシステム104は、時間ベースのトークン604をメータ112に送らない。いくつかの実施例では、ユーザ120は、ヘッドエンドシステム104が、ある量の遅延を伴って時間ベースのトークン604をメータ112に自動的に適用することを許可することを選択することができる。それらの例では、ヘッドエンドシステム104は、指定される量の遅延時間だけ待機し、その後、メッシュネットワーク140を介してメータ112に時間ベースのトークン604を送信する。

10

【0075】

ハンドヘルドデバイス106から、またはヘッドエンドシステム104から、時間ベースのトークン604を受信した後、メータ112は、時間ベースのトークン604を検証することができる。メータ112は、時間ベースのトークン604を解析して、時間ベースのトークン604に含まれる各フィールドを判定することができる。メータ112はさらに、プロビジョニングデータ202に含まれる秘密鍵を使用して、ヘッドエンドシステム104が完全性フィールド714を生成するために使用するものと同じ情報に基づいて、HMACなどの認証コードを生成する。この情報は、例えば、メータのシリアル番号、メータのネットワークID、TRN、及び時間ベースのトークン604の他のフィールド、例えばトークンタイプ702、開始日（フィールド704～708）、トークン期間710、及びトランザクションID712を含むことができる。生成された認証コードが時間ベースのトークン604の完全性フィールド714と一致する場合、メータ112は、時間ベースのトークン604がヘッドエンドシステム104によって生成され、時間ベースのトークン604のコンテンツが変更されていないことを判定することができる。

20

【0076】

時間ベースのトークン604の完全性フィールド714の生成において、メータ112のシリアル番号およびネットワークIDなどのメータ112の識別子を含む、支払いベースのトークン204と同様に、時間ベースのトークン604は、意図するメータ112に固有とされる。メータは、計算された認証コードが完全性フィールド714と一致するか否かを判定することにより、受信した時間ベースのトークン604が適切なトークンであるか否かを判定し、意図する時間ベースのトークン604のみを適用することが可能である。いくつかの実施例では、受信した時間ベースのトークン604を検証することは、時間ベースのトークン604が許容可能なウィンドウ内にあるかどうか、及び以前に受信して処理された重複するトークンであるかどうかを判定することも含む。許容可能なウィンドウを判定すること、および時間ベースのトークン604が許容可能なウィンドウ内にあるかどうかを判定することの更なる詳細は、図9に関して以下に提供される。

30

【0077】

メータ112が、受信した時間ベースのトークン604が有効なトークンではないことを判定した場合、メータ112は、時間ベースのトークン604を拒否または否定する。そうでなければ、メータ112は、メータ112の地理的位置の建物構内132を、開始日から開始して、時間ベースのトークン604で指定される時間期間、資源供給130に接続する。指定される時間期間が経過した後、メータ112は、メータ112に関連付けられる残高に基づいて、資源供給130を接続したままとし、または切断する。すなわち、残高が負であるか又は閾値残高値を下回る場合、メータ112は、建物構内132を資源供給130から切断し、そうでない場合、メータ112は、建物構内132を資源供給130と接続し続ける。

40

【0078】

支払いベースのトークン204と同様に、メータ112は、メータ112が時間ベース

50

のトークン604を受信した場所に応じて、トークン適用応答218またはイベントメッセージ222を生成し、ヘッドエンドシステム104に送信することになる。時間ベースのトークン604がヘッドエンドシステム104から受信された場合、メータ112は、メータ112で受信された時間ベースのトークン604のステータスを報告するために、トークン適用応答218を生成する。いくつかの実装では、トークン適用応答218は、「トークンがメータで正常に適用された」、「許容可能なウィンドウの外にあるのでトークンが拒否された」、「重複しているのでトークンが拒否された」、「完全性チェックに失敗したのでトークンが拒否された」などのような、時間ベースのトークン604のステータスを含んでいる。

【0079】

トークン適用応答218は、メータ112で適用された時間期間、またはメータスイッチ134のステータス（例えば、開／切断または閉／接続）など、他の情報をさらに含むことができる。トークン適用応答218は、時間ベースのトークン604、またはTRNもしくはトランザクションIDなどの時間ベースのトークン604のシリアル番号を含むこともできる。トークン適用応答218は、収集されたメータデータなど、メータ112からヘッドエンドシステム104に送信される他のデータとともに送信されてもよく、または別々に送信されてもよい。

【0080】

時間ベースのトークン604がハンドヘルドデバイス106を介して受信された場合、メータ112は、時間ベースのトークン604を報告するために、時間ベースのトークン604を含むイベントメッセージ222を生成してヘッドエンドシステム104に送信する。イベントメッセージ222は、時間ベースのトークン604のステータス、メータスイッチ134のステータス、またはトークン適用応答218に含まれる他のデータなどを含むこともできる。イベントメッセージ222はまた、収集されたメータデータなどの他のデータと共にヘッドエンドシステム104に送信され得るか、または別個に送信され得る。

【0081】

イベントメッセージ222を受信すると、ヘッドエンドシステム104は、ヘッドエンドシステム104によって生成された過去のトークンで検索するなどして、イベントメッセージ222に含まれる時間ベースのトークン604がヘッドエンドシステム104によって生成されたものかどうかを判定するために、時間ベースのトークンを分析する。そして、ヘッドエンドシステム104は、分析結果をメータ112に送信するように構成される。分析結果が、時間ベースのトークン604がヘッドエンドシステム104によって生成されなかったことを示す場合、メータ112は、資源供給130を切断し、接続中に発生した資源消費を反映するためにメータに関連付けられる残高を更新し得る。また、メータ112は、分析結果および分析結果に基づいてメータ112によって実行されたアクションを示すために、ハンドヘルドデバイス106に警告メッセージを表示させ得る。

【0082】

図8は、本開示の或る実施例に係る、資源分配ネットワーク内のメータ112で時間ベースのトークン604を生成し適用するためのプロセスの一例を示す。特に、図8は、プロセス800A、800B、および800Cを含む。プロセス800Aは、ヘッドエンドシステム104の態様を例示する。プロセス800Bは、メータ112の態様を示す。プロセス800Cは、ハンドヘルドデバイス106の態様を示す。プロセス800A、800B、および800Cは、以下で一緒に説明される。

【0083】

プロセス800Aは、ヘッドエンドシステム104がメータ112のための時間ベースのトークン616の要求を受信するブロック802で開始する。図6に関して上述したように、時間ベースのトークン616の要求は、ユーザ120による要求に応答してサービスシステム210によって生成される可能性がある。ブロック804において、プロセス800Aは、メータ112のための時間ベースのトークン604を生成することを含む。

時間ベースのトークン604をメータ112に固有にするために、ヘッドエンドシステム104は、メータ112のシリアル番号、メータ112のネットワークID、またはそれらの組み合わせなどのメータ112の識別子に基づいて、時間ベースのトークン604を生成する。さらに、生成された時間ベースのトークン604は、TRNなどのメッシュネットワーク140内の時間ベースのトークン604に固有のシリアル番号も含むか、またはこれに基づいている。時間ベースのトークン604はまた、メータ112が資源供給130を建物構内132に接続するための時間期間、ならびに時間期間の開始日を示す。

【0084】

一例では、時間ベースのトークン604は、図7に示す形式に従って生成され、この形式は、トークンタイプ702、開始日704~708、トークン期間710、トランザクションID712、および完全性フィールド714を含んでいる。いくつかの実装では、完全性フィールド714は、秘密鍵を使用して、時間ベースのトークン604のフィールド702~712、シリアル番号およびネットワークIDなどのメータ112の識別子、ならびに支払いベースのトークン204のTRNのうちの1つ以上に基づいてHMACを生成することにより生成される。

【0085】

ブロック806において、プロセス800Aは、生成された時間ベースのトークン604で時間ベースのトークン616の要求に対して応答することを含む。例えば、ヘッドエンドシステム104は、サービスシステム210などの時間ベースのトークン604を要求したエンティティに時間ベースのトークン604を送信する。ユーザ120が、生成された時間ベースのトークン604をメータ112に自動的に適用することをヘッドエンドシステム104に認可した場合、ブロック806はさらに、時間ベースのトークン604をメータ112に送信することにより、時間ベースのトークン604を適用することを含む。支払いベースのトークン204のメータ112への適用は、時間ベースのトークン604を適用するための認可をヘッドエンドシステム104に提供する際にユーザ120によって行われた選択に応じて、直ちにまたは一定の遅延をもって実行され得る。

【0086】

ユーザ120が、ヘッドエンドシステム104が時間ベースのトークン604をメータ112に適用することを認可しない場合、ユーザ120は、時間ベースのトークン604をハンドヘルドデバイス106で手動入力し得る。ブロック830において、プロセス800Cは、ユーザ入力によってハンドヘルドデバイス106で時間ベースのトークン604を受信することを含む。ブロック832において、プロセス800Cは、受信した時間ベースのトークン604を、例えば、HANを通じてメータ112に送信することを含む。

【0087】

ブロック812において、プロセス800Bは、メータ112が、ヘッドエンドシステム104から、またはハンドヘルドデバイス106から、時間ベースのトークン604を受信することを含む。ブロック814において、プロセス800Bは、受信した時間ベースのトークン604が有効なトークンであるかどうかを判定するために、時間ベースのトークン604を検証することを含む。検証プロセスは、例えば、時間ベースのトークン604の完全性を判定すること、時間ベースのトークン604がメータ112のために生成されたことを判定すること、トークンが許容可能なウィンドウ内にあることを判定すること、トークンが重複トークンでないことを判定することなどを、含み得る。時間ベースのトークン604を検証することに関する追加の詳細が、図9に関して以下に提供される。

【0088】

ブロック816において、プロセス800Bは、ブロック814で得られた検証結果に基づいて、時間ベースのトークン604が有効なトークンであるかどうかを判定することを含む。そうでない場合、プロセス800Bは、ブロック820において、時間ベースのトークン604を拒否することを含む。時間ベースのトークン604が有効なトークンである場合、プロセス800Bは、ブロック818において、時間ベースのトークン604において指定される開始日から開始して、トークン期間フィールド710において示され

10

20

30

40

50

た時間期間、資源供給 130 を接続することを含む。

【0089】

ブロック 822 において、プロセス 800B は、時間ベースのトークン 604 がヘッドエンドシステム 104 から受信された場合、図 6 に関して上述したように、トークン適用応答 218 を送信することを含む。いくつかの実装では、トークン適用応答 218 は、（受け入れられた、または拒否されたなどの）時間ベースのトークン 604 のステータス、時間ベースのトークン 604 で指定される時間期間、メタスイッチ 134 のステータス（例えば、開／切断または閉／接続）、または他の情報などの情報を含む。また、トークン適用応答 218 は、時間ベースのトークン 604、または TRN やトランザクション ID などの時間ベースのトークン 604 のシリアル番号を含んでもよい。

10

【0090】

時間ベースのトークン 604 がハンドヘルドデバイス 106 から受信された場合、メータ 112 は、イベントメッセージ 222 を生成してヘッドエンドシステム 104 に送信し、受信した時間ベースのトークン 604 についてヘッドエンドシステム 104 に通知し、ヘッドエンドシステム 104 に時間ベースのトークン 604 を検証するよう要求する。イベントメッセージ 222 は、支払いベースのトークン 204 のステータス、時間ベースのトークン 604 で指定される時間期間、メタスイッチ 134 のステータス（例えば、開／切断または閉／接続）等、トークン適用応答 218 と同様の内容を含んでもよい。イベントメッセージ 222 はまた、時間ベースのトークン 604 の全体と、ヘッドエンドシステム 104 が時間ベースのトークン 604 の真正性を確認するための要求とを含む。図 6 に関して上述したように、トークン適用応答 218 又はイベントメッセージ 222 は、メータ 112 で収集されたメータデータと共に送信されてもよいし、ヘッドエンドシステム 104 に別個に送信されてもよい。

20

【0091】

ヘッドエンドシステム 104 は、ブロック 808 でトークン適用応答 218 またはイベントメッセージ 222 を受信し、受信したメッセージをそれに応じて処理する。例えば、ヘッドエンドシステム 104 がイベントメッセージ 222 を受信した場合、ヘッドエンドシステム 104 は、イベントメッセージ 222 に含まれる支払いベースのトークン 204 を検証し、時間ベースのトークン 604 が本当にヘッドエンドシステム 104 によって生成されたかどうかを判定する。ヘッドエンドシステム 104 は、例えば、メータ 112 に通知を送信することにより、検証結果をメータ 112 に通知する。メータ 112 は、時間ベースのトークン 604 がヘッドエンドシステム 104 によって生成されていない場合、資源供給 130 を建物構内 132 から切断するなど、検証結果に応じたアクションをとることができる。

30

【0092】

時間ベースのトークン 604 がハンドヘルドデバイス 106 から受信される場合、プロセス 800B は、ブロック 824 において、メータ 112 がハンドヘルドデバイス 106 に確認メッセージを送信することをさらに含む。確認メッセージは、例えば、（例えば、受け入れられた又は拒否された、などの）時間ベースのトークン 604 のステータス、時間ベースのトークン 604 で指定される時間期間及び開始日、メタスイッチ 134 のステータス（例えば、開／切断又は閉／接続）等を含むことができる。ハンドヘルドデバイス 106 は、ブロック 834 で確認メッセージを受信し、ユーザインターフェースでユーザ 120 に提示する。

40

【0093】

図 9 は、本開示の或る実施例に係る、メータ 112 でセキュアトークンを検証するためのプロセス 900 の一例を示す。セキュアトークンは、支払いベースのトークン 204 または時間ベースのトークン 604 であり得る。プロセス 900 は、プロセス 500B のブロック 514 またはプロセス 800B のブロック 814 を実施するために使用され得る。メータ 112（例えば、環境 100、200 または 600 のメータ）は、適切なプログラムコードを実行することによって、図 9 に描かれたオペレーションを実施する。例示の目

50

的のために、プロセス 900 は、図に描かれた或る実施例を参照して説明される。しかしながら、他の実施例も可能である。

【0094】

ブロック 902 において、プロセス 900 は、図 2～5 に関して上述した支払いベースのトークン 204 または図 6～8 に関して上述した時間ベースのトークン 604 などの、セキュアトークンを取得することを伴う。プロセス 900 は、さらに、プロビジョニングデータ 202 から秘密鍵を取得することを含む。図 2 および図 4 に関して上述したように、ヘッドエンドシステム 104 は、プロビジョニングプロセス中にメータ 112 に送信されたプロビジョニングデータ 202 に秘密鍵を含む。秘密鍵は、ヘッドエンドシステム 104 によって、セキュアトークンの完全性フィールドを生成するために使用される。

10

【0095】

ブロック 904 において、プロセス 900 は、セキュアトークンに含まれる個々のフィールドを判定するために、セキュアトークンを復号化することを含む。例えば、セキュアトークンが図 3 または図 7 に示すようにフォーマットされている場合、メータ 112 は、トークンタイプを示すセキュアトークンの最初の 2 ビットを調べることによって、セキュアコードのタイプを判定することができる。トークンタイプが 0 である場合、メータ 112 は、セキュアトークンが支払いベースのトークン 204 であることを判定することができる。トークンタイプが 1 である場合、メータ 112 は、セキュアトークンが時間ベースのトークン 604 であることを判定することができる。セキュアトークンのタイプに基づいて、メータ 112 は、トークンの残りのフィールド、例えば、サブタイプ 304、クレジット値 306、支払いベースのトークン 204 のトランザクション ID 308、完全性フィールド 310、又は時間ベースのトークン 604 の開始日 704～708、トークン期間 710、トランザクション ID 712 及び完全性フィールド 714 を復号化することができる。

20

【0096】

ブロック 906 において、プロセス 900 は、秘密鍵を使用してセキュアトークンの認証コードを生成することと、認証コードに基づいてトークンの完全性を検証することとを含む。いくつかの実装では、メータ 112 は、ヘッドエンドシステム 104 が完全性フィールド 310 または 714 を生成するのと同じ方法で、かつ同じ秘密鍵を使用して認証コードを生成することができる。例えば、ヘッドエンドシステム 104 は、セキュアトークンの他のフィールド、メータ 112 のシリアル番号、メータ 112 のネットワーク ID、及びセキュアトークンの TRN に基づいて HMAC を生成し、SHA-256 アルゴリズムを使用することによってセキュアトークンの完全性フィールドを生成する。このような例では、メータ 112 は、同じフィールドの復号化されたバージョン、及びメータ 112 のシリアル番号、メータ 112 のネットワーク ID など、メータ 112 で利用できる他の対応する情報に対して、同じ秘密鍵を用いて同じ暗号アルゴリズムを適用することが可能である。生成された認証コードが、受信したセキュアトークンの完全性フィールドに含まれるデータと一致する場合、メータ 112 は、セキュアトークンがメータ 112 のためのものであり、改ざんされていないことを判定することができる。そうでなければ、セキュアトークンの完全性検証は失敗したことになる。

30

40

【0097】

ブロック 908 において、プロセス 900 は、ブロック 906 で得られた比較結果に基づいて、セキュアトークンの完全性が検証されたかどうかを判定することを含む。そうでない場合、メータ 112 は、セキュアトークンが無効であることを判定し得る。メータ 112 がセキュアトークンの完全性を首尾よく検証した場合、メータ 112 は、セキュアトークンの他の状態を引き続き調べて、その有効性を判定することができる。

【0098】

ブロック 910 において、プロセス 900 は、セキュアトークンの TRN またはトランザクション ID (TID) に対する現在の許容可能なウィンドウを判定することを含む。セキュアトークンの TRN またはトランザクション ID が許容可能なウィンドウ内に入る

50

場合、メータ112はセキュアトークンを受け入れることができ、そうでなければ、メータ112はセキュアトークンを拒否することになる。メータ112は、プロビジョニングデータ202内のトークン受入パラメータに基づいて、許容可能なウィンドウを判定することができる。いくつかの実施例では、トークン受入パラメータは、 TID_F 、 TID_{POS} 、および TID_{NEG} を含む。ここで、 TID_F は、許容可能なTIDのフロア値を表す。すなわち、メータ112で許容可能である最低のTIDは、 TID_F である。 TID_{POS} は、現在の許容可能なTID、 $TID_{current}$ と比較した許容可能なTIDの最大の正のオフセットを表す。 TID_{NEG} は、 $TID_{current}$ と比較して許容可能なTIDの最大の負のオフセットを表す。すなわち、 TID_{POS} と TID_{NEG} は、受信したセキュアトークンのTIDの許容可能なウィンドウ、すなわち $[TID_{current} - TID_{NEG}, TID_{current} + TID_{POS}]$ を定義している。ここで、 $TID_{current} - TID_{NEG}$ は許容可能なウィンドウの下限を定義し、 $TID_{current} + TID_{POS}$ は許容可能なウィンドウの上限を定義している。ただし、許容可能なTIDは TID_F より低くできないので、許容可能なウィンドウは以下のように再定式化できることに注意する。

【数1】

$$[\max(TID_F, TID_{current} - TID_{NEG}), TID_{current} + TID_{POS}]$$

【0099】

現在の許容可能なTID、 $TID_{current}$ は、受信したセキュアトークンに基づいて、メータ112によって更新される。一例では、 $TID_{current}$ は、支払いベースのトークン204および時間ベースのトークン604の両方を含む、メータ112で以前に受信されたセキュアトークンのうち最も高いTIDであるように設定される。現在受信されたセキュアトークンがこの許容可能なウィンドウの内側に入るTIDを有する場合、メータ112は、セキュアトークンが許容可能であることを判定し得、そうでなければ、セキュアトークンは許容不能であることを判定し得る。

【0100】

例えば、 $TID_{current}$ が10、 TID_{POS} が5、 TID_{NEG} が3、 TID_F が4の場合、許容可能なウィンドウは $[7, 15]$ となる。 TID が7より小さいか、15より大きいセキュアトークンは、この瞬間にメータ112で受入可能ではない。この仕組みにより、適用されるセキュアトークンの順番が、セキュアトークンのために生成されるTRNの順番と大きく乖離することを防ぐことができる。上記の例では、 $[7, 15]$ の許容可能なウィンドウは、許容可能なセキュアトークンのTIDが、メータ112で受け入れられたTIDである10に近いことを保証するものである。

【0101】

この例では、 TID は、セキュアトークンの許容可能なウィンドウを判定するために使用され、 TID は、TRNの最下位ビット10などのセキュアトークンの完全なTRNの切り捨て版であることに注意されたい。現在受信されたTIDがその最大数、例えば1023を超えると、 TID は0に戻り、1ずつ増加し始める。メータ112は、このシナリオを認識し、それに応じて許容ウィンドウを調整するように構成され得る。例えば、メータ112は、許容可能なウィンドウの下限を1021とし、許容可能なウィンドウの上限を3であると判定することができる。この例では、 $[1021, 1022, 1023, 0, 1, 2, 3]$ 内に入るTIDを有する任意のトークンが許容可能である。

【0102】

ブロック912において、プロセス900は、受信したセキュアトークンのTIDが許容可能なウィンドウの中に入るかどうかを判定することを含む。メータ112はさらに、セキュアトークンが、以前に受信され適用された重複トークンであるか否かを判定する。メータ112は、メータ112に格納されている過去のトークンID220にアクセスして、重複を検出することができる。メータ112が、セキュアトークンのTIDが許容可

10

20

30

40

50

能なウィンドウの外にある、またはセキュアトークンが以前に適用されたことがあることを判定する場合、ブロック 916 において、メータ 112 は、セキュアトークンが無効であることを判定する。そうでなければ、メータ 112 は、ブロック 914 において、セキュアトークンが有効なトークンであることを判定する。

【0103】

通常の状態では、ヘッドエンドシステム 104 は、支払いベースのトークンまたは時間ベースのトークンの生成、メータ 112 でセキュアトークンを適用するためのメータ 112 との通信などに利用可能である。しかし、他の状態では、メッシュネットワーク 140 が利用できなくなるか、または不安定になり、ヘッドエンドシステム 104 が、異常気象や自然災害などで利用できなくなる可能性がある。このような状態では、ユーザ 120 が、支払いベースのトークンを要求するための、または時間ベースのトークンを要求するための、支払いを行うことは、不可能であろう。これらの極端な状況においてユーザが資源を使用し続けることができるようにするために、ヘッドエンドシステム 104 は、グローバルトークンを発行するようにさらに構成される。

【0104】

簡単に上述したように、グローバルトークンは、任意のメータ 112 に固有でないタイプのセキュアトークンである。言い換えれば、同じグローバルトークンは、メッシュネットワーク 140 内の複数のメータ 112 において適用され得る。各グローバルトークンは、資源供給 130 をある時間期間の間継続したままにするようメータ 112 に指示する、それに関連付けられる時間期間を有する。グローバルトークンを使用することによって、ユーザ 120 は、ヘッドエンドシステム 104 がユーザ要求に基づいてトークンを生成するために利用できなくなった場合でも、資源供給へのアクセスを有することができる。

【0105】

図 10 は、本開示の或る実施例に係る、資源分配ネットワーク内のメータ 112 においてグローバルトークンを生成し適用するための例示的な動作環境 1000 を示す。環境 1000 は、ユーティリティシステム 102 と、ヘッドエンドシステム 104 と、図 1～9 に関して上述したようなメータ 112 およびそれらの関連付けられるハンドヘルドデバイス 106 とを含む。図 10 は、資源分配ネットワークにおけるメータ 112 のうちの 1 つを示す。

【0106】

いくつかの実施例では、電力会社は、天気予報が異常気象の到来を示すなど、特別な状況が生じたことを判定し、ヘッドエンドシステム 104 が一定期間利用不能になる可能性がある。電力会社は、ユーティリティシステム 102 を介してヘッドエンドシステム 104 にグローバルトークン要求 1002 を送信することにより、ネットワーク内のメータ 112 にグローバルトークンを発行することを決定することができる。グローバルトークン要求 1002 は、グローバルトークンに関連付けられる時間期間を指定することができる。

【0107】

グローバルトークン要求 1002 を受信すると、ヘッドエンドシステム 104 は、指定される時間期間に関連付けられるグローバルトークン 1004 を生成するか、または他の方法で取得することができる。いくつかの実装では、ヘッドエンドシステム 104 は、グローバルトークン要求 1002 に応答してグローバルトークン 1004 を生成する。他の実装では、グローバルトークン 1004 は、ヘッドエンドシステム 104 によってアクセスされる場所に格納されたグローバルトークンテーブル 1010 から取得される。一例では、グローバルトークンテーブル 1010 は、メータ 112 によって許容され得るグローバルトークンのリストを含む。グローバルトークンテーブル 1010 内のグローバルトークンの各々は、時間期間にマッピングされる。そのため、ヘッドエンドシステム 104 は、グローバルトークン要求 1002 において指定される時間期間に基づいて、対応するグローバルトークン 1004 を取得することができる。

【0108】

図 11 は、本開示の或る実施例に係る、グローバルトークンテーブル 1010 の一例を

示している。この例では、グローバルトークンテーブル 1010 は、グローバルトークン 1108A~1108K のリストを含む。このリスト内の各グローバルトークンについて、それに関連付けられる時間期間 1104 が存在する。例えば、図 11 に示す例におけるグローバルトークン 1 は 1 日の時間期間を有し、グローバルトークン 2 は 2 日の時間期間を有し、グローバルトークン N は M 個の日数の時間期間を有している。ここで、M は、127 のような任意の正の整数とすることができる。

【0109】

図 11 に示す例では、グローバルトークンテーブル 1010 は、テーブル内の各グローバルトークンに、対応するグローバルトークンが適用または使用されたか否かを示す適用フラグ 1106 も有する。例えば、前回ハリケーンが発生した際にグローバルトークン 2 が使用されていた場合、グローバルトークン 2 の適用フラグは、このグローバルトークンが使用されていることを示す YES に設定され得る。このように、ヘッドエンドシステム 104 がグローバルトークンを発行するたびに、ヘッドエンドシステム 104 は、グローバルトークンテーブル 1010 から、要求される時間期間に対応し、以前に使用されたことがないグローバルトークンを選択することになる。グローバルトークンを一度だけ使用できるようにすることの利点の 1 つは、トークンの不正使用や誤用を防止することである。例えば、グローバルトークンが繰り返し使用されることが許可される場合、資源供給へのアクセスを認可されていたが、もはや認可されていないユーザは、ヘッドエンドが特別な状況で利用可能である間、資源を取得するために過去のグローバルトークンを使用することが可能であろう。グローバルトークンを一度だけ使用することで、このような問題を防ぐことができる。

【0110】

図 11 に示すグローバルトークンテーブル 1010 の例は、説明のためだけのものであり、限定的に解釈されるべきではないことは理解されるべきである。グローバルトークンテーブル 1010 は、任意の他のフォーマットで構築されてもよい。例えば、グローバルトークンテーブル 1010 は、アプリケーションフラグなしで、グローバルトークン及び対応する時間期間のみを含んでもよい。このようなシナリオでは、グローバルトークンが使用されたか否かが、他のメカニズムを使用して示されてもよい。

【0111】

図 12 は、本開示の或る実施例に係る、資源分配ネットワーク内のメータ 112 で適用され得るグローバルトークン 1004 の例を示す。この例では、グローバルトークン 1004 は、20 個の 10 進数桁に相当する 66 ビットを含む。グローバルトークン 1004 のサイズは、図 7 に示される時間ベースのトークン 604 のサイズと同じであり、図 3 に示される支払いベースのトークン 204 のサイズと同じである。支払いベースのトークン 204 及び時間ベースのトークン 604 と同様に、グローバルトークン 1004 の最初の 2 ビットは、トークンタイプ 1202 を表すために使用される。いくつかの実施例では、トークンタイプ 1202 の値が 3 である場合、そのトークンはグローバルトークンである。トークンタイプの他の値は、他のタイプのセキュアトークンを示すために使用することができる。図 12 に示されるグローバルトークン 1004 の次の 64 ビットは、グローバルトークン 1004 を一意に識別する乱数を含む。

【0112】

図 10 に戻ると、いくつかの実施例では、グローバルトークン 1004 とその対応する時間期間を生成することによって、ヘッドエンドシステム 104 でグローバルトークンテーブル 1010 が生成される。他の実施例では、グローバルトークンテーブル 1010 は、ユーティリティシステム 102 または電力会社に関連付けられる別のシステムによって生成され、ヘッドエンドシステム 104 に送信される。いずれの場合も、ヘッドエンドシステム 104 はまた、グローバルトークンテーブル 1010 を、メッシュネットワーク 140 を介してメータ 112 に送信する。いくつかの実装では、グローバルトークンテーブル 1010 は、メータ 112 に送信される対応するプロビジョニングデータ 202 において、各メータ 112 に送信され得る。他の実装では、グローバルトークンテーブル 101

0 は、プロビジョニングデータ 202 とは別個にメータ 112 に送信される。

【0113】

グローバルトークンテーブル 1010 に基づいて、ヘッドエンドシステム 104 は、グローバルトークン要求 1002 で指定されるようにグローバルトークン 1004 を取得することができる。ヘッドエンドシステム 104 は、さらに、グローバルトークン 1004 をブロードキャストネットワーク 1008 を介してブロードキャストさせる。メッシュネットワーク 140 が既に利用不能又は不安定になっている可能性があるため、ブロードキャストネットワーク 1008 は、メッシュネットワーク 140 とは異なっている。ブロードキャストネットワーク 1008 は、ラジオネットワーク、テレビネットワーク、インターネット、セルラーネットワーク、などであってもよく、また、ユーザ 120 がグローバルトークン 1004 について通知され得るようにグローバルトークン 1004 をブロードキャストするために利用され得る任意の他のタイプのネットワークであってもよい。

【0114】

ブロードキャストネットワーク 1008 を通じてグローバルトークン 1004 を取得した後、ユーザ 120 は、ハンドヘルドデバイス 106 を通じてなど、グローバルトークン 1004 をメータ 112 に入力することができる。メータ 112 は、受信したグローバルトークン 1004 がグローバルトークンテーブル 1010 に含まれ、以前に使用されていないかどうかを判定することによって、受信したグローバルトークン 1004 を検証する。そうであれば、メータ 112 は、グローバルトークン 1004 が有効なトークンであることを判定することができる。そうでなければ、グローバルトークン 1004 は無効なトークンであり、メータ 112 によって拒否される。

【0115】

いくつかの実施例では、メータ 112 は、グローバルトークンテーブル 1010 内のグローバルトークン 1004 に関連付けられる適用フラグ 1106 をチェックすることによって、グローバルトークンが以前に使用されたことがあることを判定する。適用フラグ 1106 が、グローバルトークン 1004 が以前に使用されていないことを示す場合、メータ 112 は、グローバルトークン 1004 に関連付けられる時間期間の間、資源供給 130 を接続することによって、メータ 112 でグローバルトークン 1004 を適用する。また、メータ 112 は、グローバルトークンテーブル 1010 のグローバルトークン 1004 の適用フラグ 1106 を更新し、このグローバルトークン 1004 が現在使用されていることを表示する。

【0116】

特別な状況が終わり、メッシュネットワーク 140 及びヘッドエンドシステム 104 が回復した後、メータ 112 は、イベントメッセージ 1012 をヘッドエンドシステム 104 に送信し、メータ 112 によって処理されたグローバルトークン 1004 を報告することができる。イベントメッセージ 1012 は、メータ 112 によって受信されたグローバルトークン 1004 と、グローバルトークン 1004 のステータス（適用または拒否）、グローバルトークン 1004 で指定される時間期間、グローバルトークン 1004 が適用された時間、メータスイッチ 134 のステータスなどの他のデータとを含むことができる。イベントメッセージ 1012 は、ヘッドエンドシステム 104 に別々に送信することもできるし、メータ 112 から送信される他のデータ、例えば、メータ 112 が収集したメータデータとともに送信することもできる。

【0117】

イベントメッセージ 1012 を受信した後、ヘッドエンドシステム 104 は、イベントメッセージ 1012 に含まれるグローバルトークン 1004 を分析し、グローバルトークンテーブル 1010 を検索するなどして、グローバルトークン 1004 がヘッドエンドシステム 104 によって生成されたか、または発行されたか、を判定する。その後、ヘッドエンドシステム 104 は、分析結果をメータ 112 に送信するように構成される。分析結果が、グローバルトークン 1004 がヘッドエンドシステム 104 によって適切に発行されなかったことを示す場合、メータ 112 は、資源供給 130 を切断し、接続が確立され

10

20

30

40

50

た時間期間中に発生した資源消費を反映するためにメータ１１２に関連付けられる残高を更新し得る。また、メータ１１２は、分析結果および分析結果に基づいてメータ１１２によって実行されたアクションを示すために、ハンドヘルドデバイス１０６に警告メッセージを表示させ得る。

【０１１８】

上述したように、いくつかの実施例では、各グローバルトークン１００４は、１回だけ使用することが許可される。そのため、グローバルトークン１００４が発行された後、ヘッドエンドシステム１０４は、そのようなグローバルトークン１００４を使用済みとラベル付けし、したがって、それを再び使用することはないであろう。現在のグローバルトークンテーブル１０１０内のグローバルトークンの全て又は一部が使用された後、ヘッドエンドシステム１０４又はユーティリティシステム１０２又は電力会社に関連付けられる別のシステムは、異なるセットのグローバルトークンを含む新しいグローバルトークンテーブル１０１０を生成することができる。さらなる実施例では、グローバルトークンテーブル１０１０は、所定の期間に受け入れられ得るように構成され、グローバルトークンテーブル１０１０に含まれるグローバルトークンは、その期間の間のみ使用され得る。このように、現在の期間が満了した場合、新しいグローバルトークンテーブル１０１０を別の期間のために生成することもできる。

【０１１９】

ヘッドエンドシステム１０４は、新しいグローバルトークンテーブル１０１０を格納し、また、新しいグローバルトークンテーブル１０１０をメッシュネットワーク１４０内のメータ１１２に送信して、既存のグローバルトークンテーブル１０１０を置き換える。その後、次のグローバルトークン１００４は、グローバルトークン要求１００２で指定される時間期間に基づいて、新しいグローバルトークンテーブル１０１０から選択されることになる。

【０１２０】

図１３は、本開示の或る実施例に係る、メータでグローバルトークンを発行し適用するためのプロセスの例を示す図である。図１３に示す例は、グローバルトークンテーブル１０１０がヘッドエンドシステム１０４で生成されて格納され、メッシュネットワーク１４０内のメータ１１２に送信されたことを想定する。特に、図１３は、プロセス１３００Ａ、１３００Ｂ、および１３００Ｃを含む。プロセス１３００Ａは、ヘッドエンドシステム１０４の態様を例示する。プロセス１３００Ｂは、メータ１１２の態様を示す。プロセス１３００Ｃは、ハンドヘルドデバイス１０６の態様を示す。プロセス１３００Ａ、１３００Ｂ、および１３００Ｃは、以下で一緒に説明される。

【０１２１】

プロセス１３００Ａは、ブロック１３０２で始まり、ヘッドエンドシステム１０４は、グローバルトークン要求１００２に基づいて、グローバルトークン１００４を判定する。一例では、ヘッドエンドシステム１０４は、グローバルトークン要求１００２において指定されるような時間期間を有し、以前に使用されていないグローバルトークンテーブル１０１０からグローバルトークンを選択することによって、グローバルトークン１００４を判定する。ブロック１３０４において、プロセス１３００Ａは、グローバルトークン１００４を１つ以上のブロードキャストネットワーク１００８を介してブロードキャストさせることを含む。

【０１２２】

プロセス１３００Ｃは、ブロック１３１２で始まり、ハンドヘルドデバイス１０６は、例えばキーボードまたはイメージスキャンデバイスを使用するユーザ入力を通してグローバルトークン１００４を受信する。ブロック１３１４で、プロセス１３００Ｃは、グローバルトークン１００４をメータ１１２に送信することを含む。

【０１２３】

プロセス１３００Ｂは、ブロック１３２２で始まり、メータ１１２は、ハンドヘルドデバイス１０６からグローバルトークン１００４を受信する。ブロック１３２４において、

プロセス1300Bは、グローバルトークン1004を検証することを含み、さらに、グローバルトークン1004に関連付けられる時間期間を判定することを含む。いくつかの実施例では、メータ112は、グローバルトークン1004がグローバルトークンテーブル1010にリストされているかどうかを判定することによって、グローバルトークン1004を検証する。メータ112はさらに、例えば、グローバルトークンテーブル1010内のグローバルトークン1004に対する適用フラグ1106を調べることによって、グローバルトークン1004が以前に使用されたかどうかを判定する。グローバルトークン1004がグローバルトークンテーブル1010にリストされており、以前に使用されていないことをメータ112が判定する場合、メータ112はグローバルトークン1004が有効なトークンであることを判定し、そうでなければグローバルトークン1004を無効なトークンとして拒否する。

10

【0124】

ブロック1326において、プロセス1300Bは、グローバルトークン1004が有効なトークンであると判定した後、グローバルトークン1004に関連付けられる時間期間、建物構内132を資源供給130に接続することを含む。メータ112は、グローバルトークン1004に関連付けられる適用フラグをさらに更新して、グローバルトークン1004がメータ112で適用されたことを示す。ブロック1328において、プロセス1300Cは、グローバルトークン1004のステータス、例えば、適用された、または拒否されたことを示すために、ハンドヘルドデバイス106に確認メッセージを送信することを含む。ハンドヘルドデバイス106は、ブロック1316でその確認メッセージを受信し、ユーザインターフェースを通じてユーザ120に提示する。

20

【0125】

ブロック1330において、プロセス1300Bは、イベントメッセージ1012を生成し、ヘッドエンドシステム104に送信することを含む。これは、メッシュネットワーク140およびヘッドエンドシステム104が回復し、利用可能になった後に発生する。イベントメッセージ1012は、メータ112によって受信されたグローバルトークン1004、グローバルトークン1004のステータス（適用または拒否）、グローバルトークン1004で指定される時間期間、グローバルトークン1004が適用された時間、メータスイッチ134のステータス等を含むことができる。

【0126】

ブロック1306において、ヘッドエンドシステム104は、イベントメッセージ1012を受信し、イベントメッセージ1012を処理して、メッセージに含まれるグローバルトークン1004が本当にヘッドエンドシステム104によって発行されたかどうかを判定する。また、ヘッドエンドシステム104は、グローバルトークンテーブル1010が許容可能であった期間中にグローバルトークン1004が適用されたか否かを判定してもよい。図10に関して詳細に上述したように、グローバルトークン1004がヘッドエンドシステム104によって適切に発行されなかったとヘッドエンドシステム104が判定する場合、追加のアクションがメータ112で実行されることになる。

30

【0127】

上記の説明では、3種類のセキュアトークンが別々に議論されているが、これらはシステム内で共存できることを理解されたい。言い換えれば、ヘッドエンドシステム104は、受信した要求に応じて、支払いベースのトークン204、時間ベースのトークン604、またはグローバルトークン1004を生成または発行するように構成され得る。メッシュネットワーク140内の各メータ112も、これら3種類のセキュアトークンを認識し処理するように構成され得る。図14は、本開示の或る実施例に係る、メータでセキュアトークンを受信し処理するためのプロセス1400の一例を示す図である。メッシュネットワーク140の1つ以上のノードまたはメータ（例えば、メータ112またはルートノード114）は、適切なプログラムコードを実行することによって、図14に描かれたオペレーションを実装する。例示の目的のために、プロセス1400は、図に描かれた或る実施例を参照して説明される。しかしながら、他の実施例も可能である。

40

50

【0128】

ブロック1402において、プロセス1400は、セキュアトークンを受信することを含む。セキュアトークンは、支払いベースのトークン204、時間ベースのトークン604、またはグローバルトークン1004であってよい。セキュアトークンは、メッシュネットワーク140を介してヘッドエンドシステム104から、またはHANもしくは他の接続を介してハンドヘルドデバイス106から受信されてもよい。

【0129】

ブロック1404において、プロセス1400は、セキュアトークンを復号化して、セキュアトークンのタイプを判定することを含む。例えば、3種類のセキュアトークンのためのトークン形式が図3、図7および図12に示されるものに従う場合、メータ112は、受信したトークンの最初の2ビットを調べることによってセキュアトークンの種類を判定することができる。図3、7および12に示す例では、トークンの最初の2ビットの値が0であれば、トークンは支払いベースのトークン204であり、値が1であれば、トークンは時間ベースのトークン604であり、値が3であれば、トークンはグローバルトークン1004である。

【0130】

セキュアトークンのタイプに応じて、プロセス1400は異なるオペレーションを含む。セキュアトークンが支払いベースのトークン204である場合、プロセス1400は、ブロック1406において、図5に関して上述したプロセス500Bに従って、セキュアトークン进行处理することを含む。セキュアトークンが時間ベースのトークン604である場合、プロセス1400は、ブロック1408において、図8に関して前述したプロセス800Bに従ってセキュアトークン进行处理することを含む。セキュアトークンがグローバルトークン1004である場合、プロセス1400は、ブロック1410において、図13に関して前述したプロセス1300Bに従って、セキュアトークン进行处理することを含む。

【0131】

本開示は、水、ガス、電気、蒸気などの資源を建物構内に分配するために構成された資源分配ネットワークに焦点を当てているが、本明細書に提示された技術は、他のタイプの資源にも適用できることを理解されたい。例えば、本明細書に提示される技術は、セルラリソースへのアクセスを制御するために利用され得る。セルラリソースのユーザは、自分の口座に支払いを行うことによって支払いベースのトークンを要求するか、またはサービスシステムなどのサービスシステムを用いて時間ベースのトークンを要求するかのいずれかである。これら2種類のトークンは、例えば、携帯電話の国際移動体識別番号（IMEI）番号を用いて、彼の携帯電話に固有となるように生成される。このように、支払いベースのトークンまたは時間ベースのトークンは、ユーザの携帯電話でのみ適用することができる。同様に、セキュアトークンを生成するシステムが利用できなくなった場合、グローバルトークンが生成され、セルラリソースのユーザにブロードキャストされることがある。このような場合、ユーザは、携帯電話にグローバルトークンを入力することにより、セルラリソースの使用を継続することができる。ネットワークリソース、オンラインコンピューティングリソース、オンラインストレージリソースなどの他のリソースへのアクセスも、同様の方法で制御することができる。

【0132】

例示的なメータ

【0133】

図15は、メータ112またはルートノード114など、本明細書に記載のセキュアトークン処理機構を実装するために採用され得る例示的なメータ1500を示す。メータ1500は、ローカル又はシリアル接続1530を介して接続された通信モジュール1516及び計測モジュール1518を含む。これら2つのモジュールは、別々のボード上の同じユニットに収容されてもよく、したがって、ローカル接続1530は、オンボードソケットであってもよい。あるいは、モジュールは別々に収容され、したがって、ローカル接

10

20

30

40

50

続１５３０は、ＵＳＢケーブルなどの通信ケーブル、または他の導体であってもよい。これら２つの構成要素は物理的に別々であってもよいので、通信モジュール１５１６及び計測モジュール１５１８は、互いに独立して取り外し又は交換することができる。

【０１３４】

通信モジュール１５１６の機能は、メッシュネットワーク１４０を介して、セキュアトークンを含むメッセージを受信および送信することを含む。計測モジュール１５１８の機能は、リソースを管理するために必要な機能、特に、リソースへのアクセスを許可し、使用されるリソースを計測するために必要な機能を含む。通信モジュール１５１６は、アンテナ及び無線機などの通信装置１５１２を含んでもよい。あるいは、通信装置１５１２は、無線通信または有線通信を可能にする任意の装置であってもよい。また、通信モジュール１５１６は、プロセッサ１５１３、及びメモリ１５１４を含んでもよい。通信装置１５１２は、ネットワーク１４０を介してメッセージを受信及び送信するために使用される。プロセッサ１５１３は、通信モジュール１５１６によって実行される機能を制御する。メモリ１５１４は、プロセッサ１５１３がその機能を実行するために使用するデータを格納するために利用されてもよい。また、メモリ１５１４は、秘密鍵や受入パラメータなど、プロビジョニングデータ２０２に含まれるデータを格納してもよい。

【０１３５】

計測モジュール１５１８は、プロセッサ１５２１、メモリ１５２２、および測定回路１５２３を含んでもよい。計測モジュール１５１８のプロセッサ１５２１は、計測モジュール１５１８によって実行される機能を制御する。メモリ１５２２は、グローバルトークンを検証するために使用されるグローバルトークンテーブル１０１０など、プロセッサ１５２１がその機能を実行するために必要なデータを格納する。いくつかの実施例では、プロビジョニングデータ２０２の他のデータも、通信モジュール１５１６のメモリ１５１４ではなく、計測モジュール１５１８のメモリ１５０２に格納される。いずれの場合も、通信モジュール１５１６及び計測モジュール１５１８は、ローカル接続１５３０を介して互いに通信し、他のモジュールによって必要とされるデータを提供する。測定回路１５２３は、リソースの測定を処理し、また、測定された測定の記録を処理してもよい。通信モジュール１５１６及び計測モジュール１５１８の両方は、メモリ又は別のタイプのコンピュータ可読媒体に格納されたコンピュータ実行可能命令を含んでもよく、モジュール内の１つ又は複数のプロセッサが命令を実行して、本明細書に記載される機能を提供してもよい。

【０１３６】

或る実施形態を実装するためのヘッドエンドシステムの例

【０１３７】

本明細書に記載された動作を実行するために、任意の適切なコンピューティングシステムまたはコンピューティングシステム群を使用することができる。例えば、図１６は、コンピューティングシステム１６００の一例を示している。コンピューティングシステム１６００の実装は、ヘッドエンドシステム１０４のために使用され得る。

【０１３８】

コンピューティングシステム１６００の描かれた実施例は、１つ以上のメモリデバイス１６０４に通信可能に結合されたプロセッサ１６０２を含む。プロセッサ１６０２は、メモリデバイス１６０４に格納されたコンピュータ実行可能なプログラムコードを実行し、メモリデバイス１６０４に格納された情報にアクセスし、又はその両方を行う。プロセッサ１６０２の例は、マイクロプロセッサ、特定用途向け集積回路（「ASIC」）、フィールドプログラマブルゲートアレイ（「FPGA」）、または他の任意の適切な処理デバイスを含む。プロセッサ１６０２は、単一の処理デバイスを含む、任意の数の処理デバイスを含むことができる。

【０１３９】

メモリデバイス１６０４は、プログラムコード１６０５（たとえば、支払いベースのトークンまたは時間ベースのトークンの生成に使用されるコード）、プログラムデータ１６０７（たとえば、グローバルトークンテーブル）、または両方を記憶するための任意の適

10

20

30

40

50

切な非一時的コンピュータ読取可能媒体を含む。コンピュータ可読媒体は、コンピュータ可読命令または他のプログラムコードをプロセッサに提供することができる任意の電子、光学、磁気、または他のストレージデバイスを含むことができる。コンピュータ可読媒体の非限定的な例としては、磁気ディスク、メモリチップ、ROM、RAM、ASIC、光学ストレージ、磁気テープまたは他の磁気ストレージ、または処理装置が命令を読み出すことができる他の任意の媒体が挙げられる。命令は、例えば、C、C++、C#、Visual Basic、Java、Python、Perl、JavaScript、およびActionScriptを含む、任意の適切なコンピュータプログラミング言語で書かれたコードからコンパイラまたはインタープリタによって生成されたプロセッサ固有の命令を含んでもよい。

10

【0140】

コンピューティングシステム1600は、プロセッサ1602を構成して、本明細書に記載される動作のうちの1つ以上を実行するプログラムコード1605を実行する。プログラムコード1605の例は、さまざまな実施形態において、支払いベースのトークンを生成するために使用されるプログラムコード、時間ベースのトークンを生成するために使用されるプログラムコード、支払いベースのトークン、時間ベースのトークンまたはグローバルトークンを検証するために使用されるプログラムコード、または本明細書に記載の1以上の動作を実行する他の適切なアプリケーションを含む。プログラムコードは、メモリデバイス1604または任意の好適なコンピュータ可読媒体に常駐してもよく、プロセッサ1602または他の任意の好適なプロセッサによって実行されてもよい。

20

【0141】

いくつかの実施形態では、1つ以上のメモリデバイス1604は、本明細書に記載された1つ以上のデータセットを含むプログラムデータ1607を格納する。これらのデータセットの例には、過去のセキュアトークン、グローバルトークンテーブルなどが含まれる。いくつかの実施形態では、データセット、モデル、及び関数のうちの1つ以上が、同じメモリデバイス（例えば、メモリデバイス1604のうちの1つ）に格納される。追加または代替の実施形態では、本明細書に記載されたプログラム、データセット、モデル、および機能の1つ以上は、データネットワークを介してアクセス可能な異なるメモリデバイス1604に格納される。また、1つ以上のバス1606がコンピューティングシステム1600に含まれる。バス1606は、コンピューティングシステム1600のそれぞれの1つまたは複数のコンポーネントを通信可能に結合している。

30

【0142】

いくつかの実施形態では、コンピューティングシステム1600はまた、ネットワークインターフェースデバイス1610を含む。ネットワークインターフェースデバイス1610は、1つまたは複数のデータネットワークへの有線または無線データ接続を確立するのに適した任意のデバイスまたはデバイス群を含む。ネットワークインターフェースデバイス1610の非限定的な例としては、イーサネットネットワークアダプタ、モデム、及び／又はそのようなものが挙げられる。コンピューティングシステム1600は、ネットワークインターフェースデバイス1610を使用して、データネットワークを介して1つまたは複数の他のコンピューティングデバイス（例えば、ルートノード114）と通信することが可能である。

40

【0143】

コンピューティングシステム1600はまた、多数の外部または内部デバイス、入力デバイス1620、プレゼンテーションデバイス1618、または他の入力または出力デバイスを含むことができる。例えば、コンピューティングシステム1600は、1つ以上の入力／出力（「I/O」）インターフェース1608を備えて示されている。I/Oインターフェース1608は、入力デバイスから入力を受け取り、または出力デバイスに出力を提供することができる。入力デバイス1620は、プロセッサ1602の動作を制御または影響する視覚、聴覚、または他の適切な入力を受信するのに適した任意のデバイスまたはデバイス群を含むことができる。入力デバイス1620の非限定的な例としては、タ

50

タッチスクリーン、マウス、キーボード、マイクロフォン、別個のモバイルコンピューティングデバイスなどがある。プレゼンテーションデバイス1618は、視覚、聴覚、または他の適切な感覚出力を提供するのに適した任意の装置または装置群を含むことができる。プレゼンテーションデバイス1618の非限定的な例としては、タッチスクリーン、モニタ、スピーカ、別個のモバイルコンピューティング装置等が挙げられる。

【0144】

図16は、入力デバイス1620及びプレゼンテーションデバイス1618を、ヘッドエンドシステム104を実行するコンピューティング装置にローカルであるように描いているが、他の実施態様も可能である。例えば、いくつかの実施形態では、入力デバイス1620およびプレゼンテーションデバイス1618のうちの1つまたは複数は、本明細書に記載される1つまたは複数のデータネットワークを使用して、ネットワークインターフェースデバイス1610を介してコンピューティングシステム1600と通信するリモートクライアントコンピューティングデバイスを含むことが可能である。

【0145】

一般的な考慮事項

【0146】

請求された主題の徹底的な理解を提供するために、多数の具体的な詳細が本明細書に記載されている。しかし、当業者は、請求された主題がこれらの具体的な詳細なしに実施され得ることを理解するであろう。他の実施例では、当業者に知られているであろう方法、装置、又はシステムは、クレームされた主題を不明瞭にしないように、詳細には記載されていない。

【0147】

本明細書で論じた特徴は、特定のハードウェア・アーキテクチャまたは構成に限定されるものではない。コンピューティングデバイスは、1つ以上の入力を条件とする結果を提供するコンポーネントの任意の好適な配置を含むことができる。好適なコンピューティング装置は、コンピューティングシステムを汎用コンピューティング装置から本主題の1つ以上の態様を実装する特殊コンピューティング装置へとプログラムまたは構成する格納ソフトウェア（すなわち、コンピュータシステムのメモリ上に格納されたコンピュータ可読命令）にアクセスする多目的マイクロプロセッサベースのコンピュータシステムを含む。任意の適切なプログラミング、スクリプト、または他のタイプの言語または言語の組み合わせが、コンピューティング装置をプログラミングまたは構成する際に使用されるソフトウェアにおいて、本明細書に含まれる教示を実装するために使用され得る。

【0148】

本明細書に開示される方法の態様は、そのようなコンピューティングデバイスの動作において実行されてもよい。上記の例で提示されたブロックの順序は、変化させることができる。例えば、ブロックは、再順序付けされ、結合され、および／またはサブブロックに分割されることができる。或るブロックまたはプロセスは、並行して実行することができる。

【0149】

本明細書における「に適合された」または「に構成された」の使用は、追加のタスクまたはステップを実行するように適合または構成されたデバイスを妨げない、オープンかつ包括的な言語として意図されている。さらに、「に基づく」の使用は、プロセス、ステップ、計算、または他の動作が、1つまたは複数の言及された条件または値に「基づく」場合、実際には、言及されたものを超える追加の条件または値に基づくことができるという意味で、開放的かつ包括的であることが意図されている。本明細書に含まれる見出し、リスト、および番号付けは、説明を容易にするためだけのものであり、限定することを意図していない。

【0150】

本主題は、その特定の態様に関して詳細に説明されてきたが、当業者は、前述の理解に達した時点で、そのような態様に対する変更、変形、および同等物を容易に作り出すこと

10

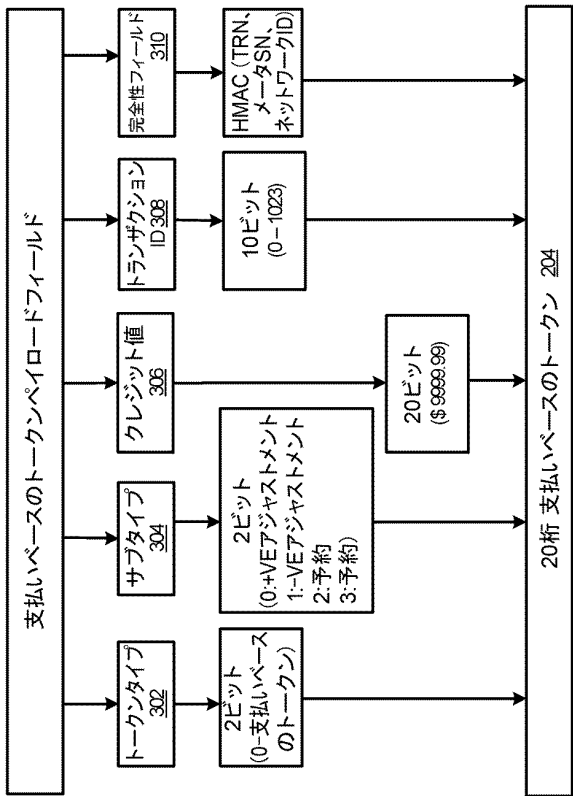
20

30

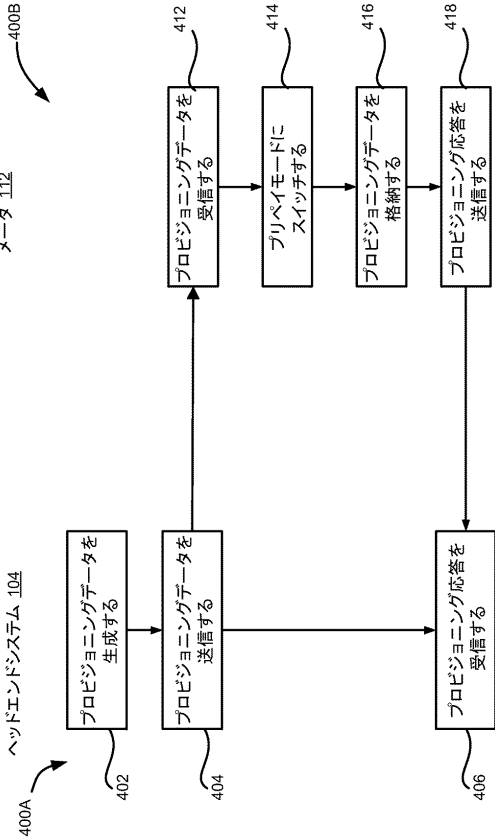
40

50

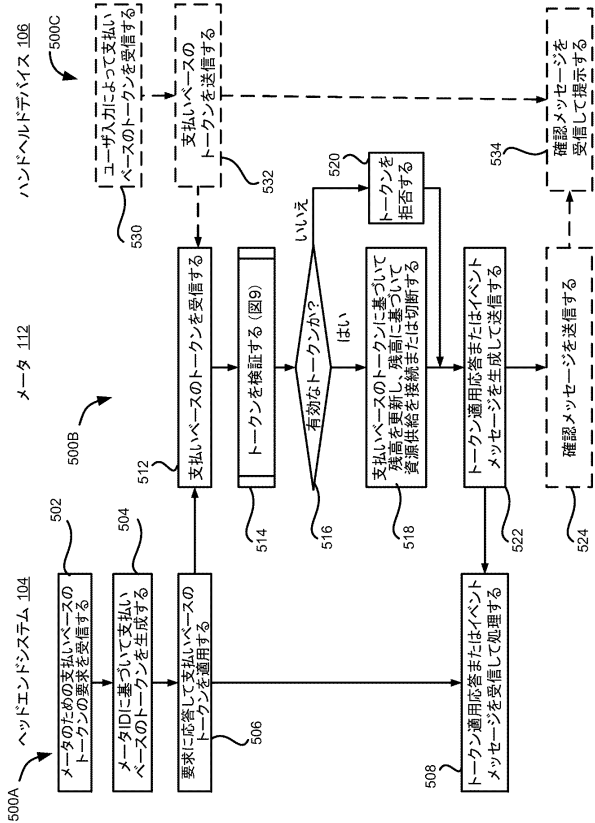
【図 3】



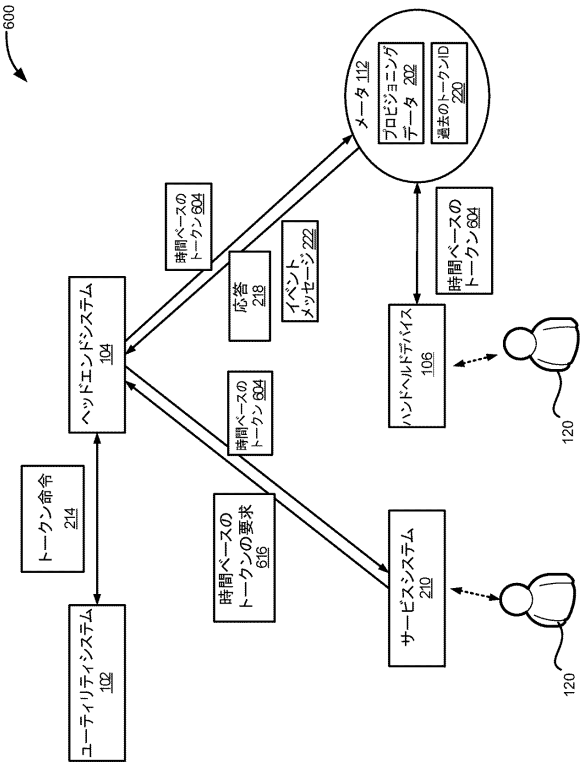
【図 4】



【図 5】



【図 6】



10

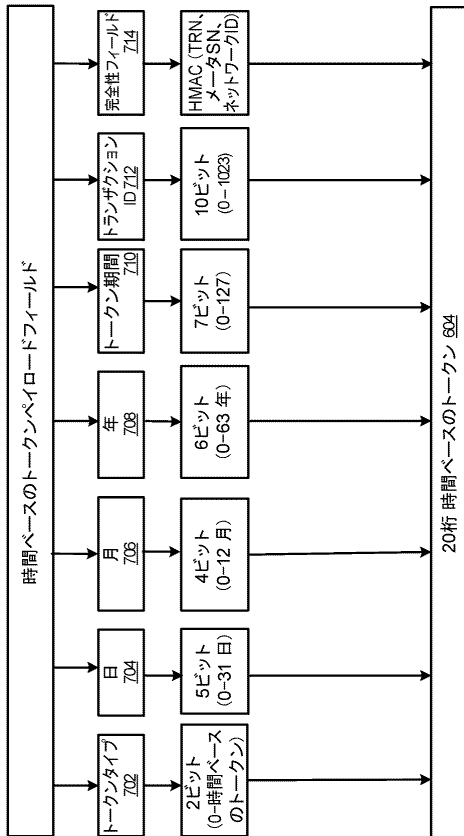
20

30

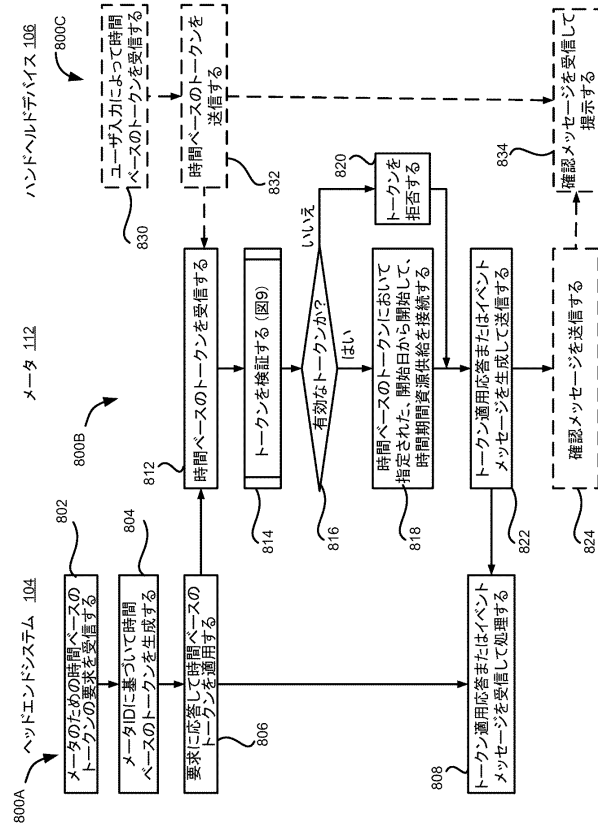
40

50

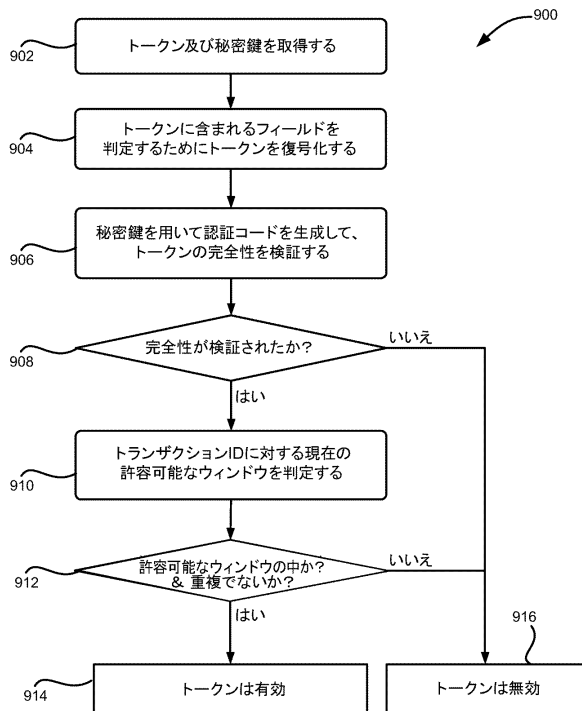
【図 7】



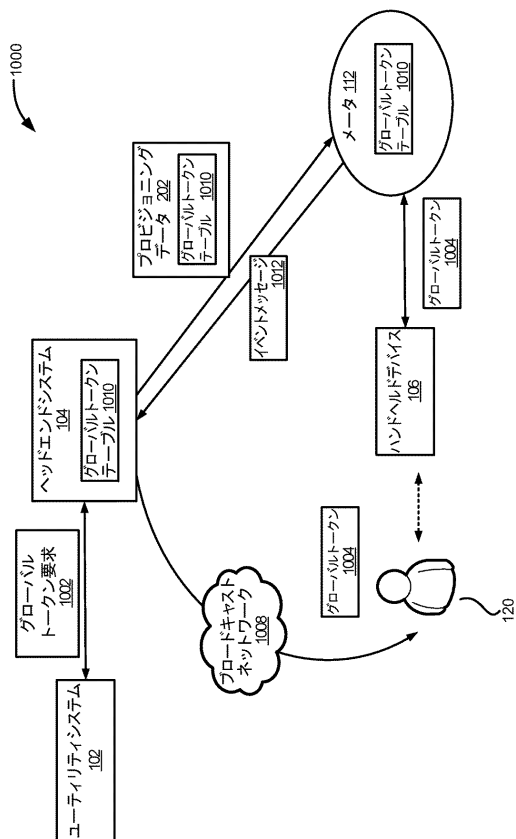
【図 8】



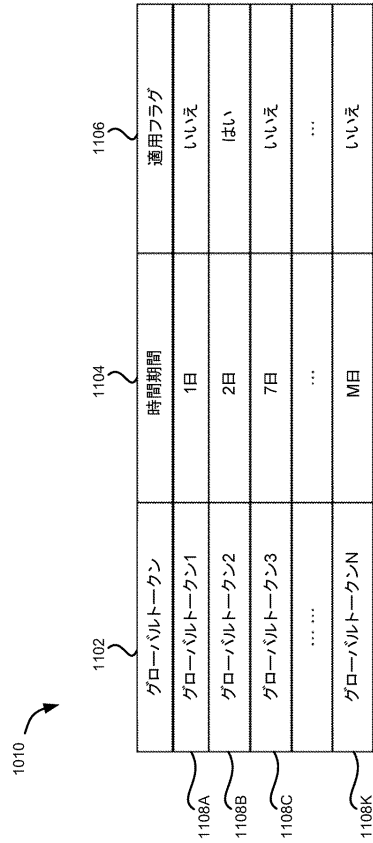
【図 9】



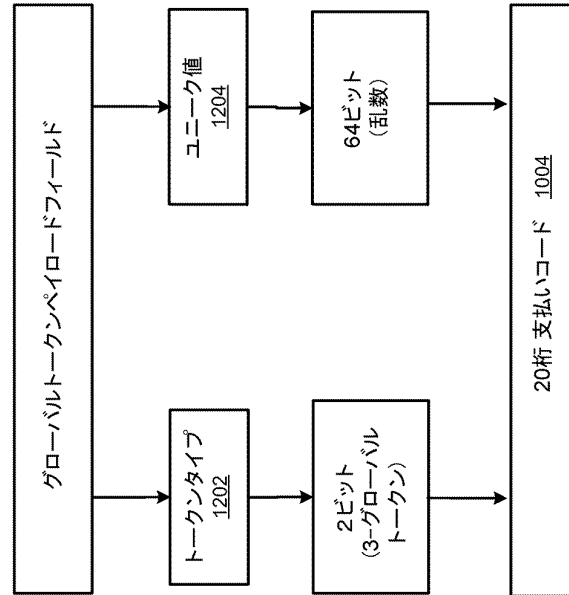
【図 10】



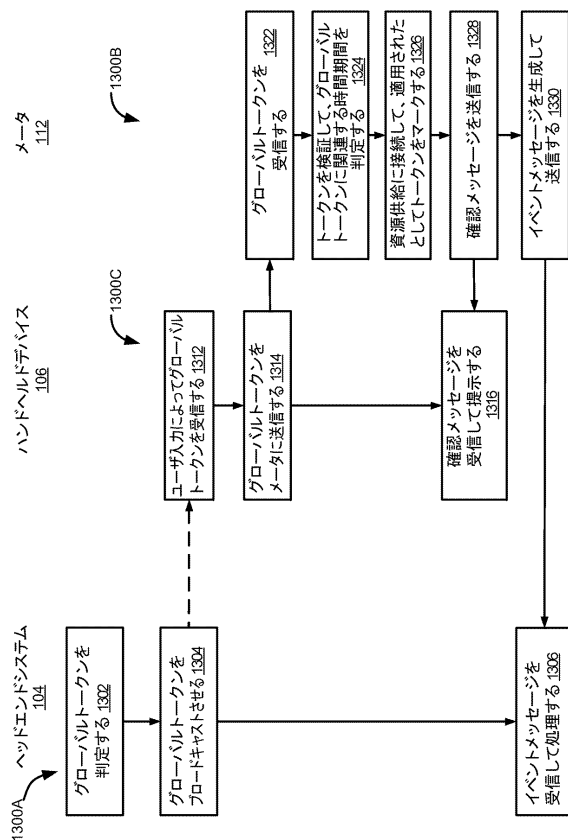
【図 1 1】



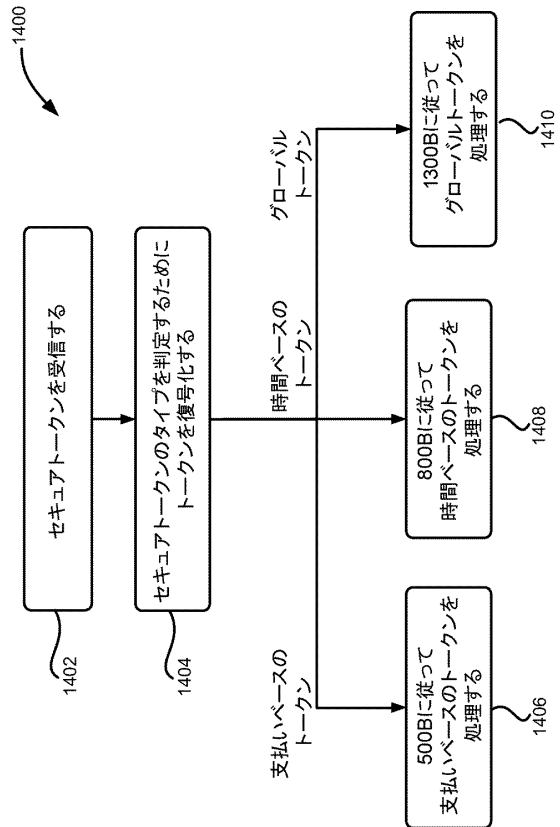
【図 12】



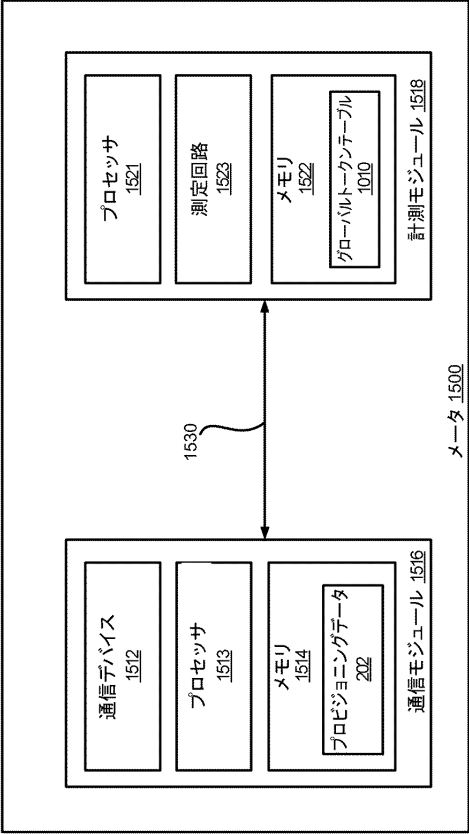
【図 13】



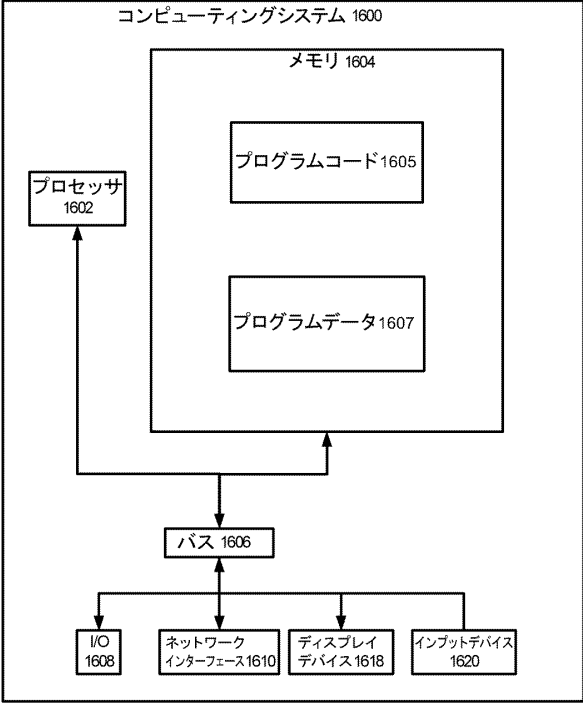
【図 14】



【図 1 5】



【図 1 6】



10

20

30

40

50

フロントページの続き

(51)国際特許分類

F I
G 0 6 Q 50/06
G 0 6 F 21/62 3 1 8

アメリカ合衆国 3 0 0 2 2 ジョージア州アルファレッタ、ミル・クリーク・アベニュー 3 0 0 0 0
、スウィート 1 0 0

審査官 上島 拓也

(56)参考文献

特開 2 0 1 3 - 1 9 8 1 2 3 (J P , A)
特表 2 0 1 8 - 5 0 6 7 7 0 (J P , A)
特開 2 0 0 2 - 0 7 4 2 1 7 (J P , A)
特開平 0 8 - 0 0 5 3 9 8 (J P , A)
特開 2 0 1 6 - 1 2 6 6 2 7 (J P , A)
Archelle B. Batiller et al., Prepaid metering system for isolated microgrids, 2016 IEEE Innovative Smart Grid Technologies - Asia (ISGT-Asia), IEEE, 2016年12月26日, P529-534,
<https://ieeexplore.ieee.org/document/7796440>, DOI: 10.1109/ISGT-Asia.2016.7796440

(58)調査した分野 (Int.Cl., D B 名)

H 0 4 L 9 / 3 2
G 0 6 F 2 1 / 6 2
H 0 4 L 9 / 0 8
G 0 6 Q 2 0 / 3 8
G 0 6 Q 5 0 / 0 6