

明 細 書

発明の名称：

設定方法、機器認証方法、機器認証システム、およびコントローラ

技術分野

[0001] 本発明は、スマートメータへの機器のIDおよび証明書の設定方法、およびスマートメータを含む機器認証方法等に関する。

背景技術

[0002] スマートグリッド（次世代送電線網）の導入に伴い、通信・制御機能を備えるスマートメータが普及してきている。

[0003] 一方、家庭内で用いられるエアコンなどの家電機器においても、通信機能を備えるものが増えている。これらの家電機器の通信機能を利用し、家庭内の家電機器をHEMS（Home Energy Management System）コントローラによって制御するHEMSが注目されている。

[0004] また、上記のような、スマートメータとHEMSコントローラおよび家電機器とを通信させることにより、スマートメータからDR（Demand Response）信号などの制御信号をHEMSコントローラおよび家電機器に送信するなどして、様々なサービスを提供することが検討されている。

先行技術文献

特許文献

[0005] 特許文献1：米国特許出願公開第2011／0047370号明細書

特許文献2：米国特許第7950044号明細書

特許文献3：米国特許出願公開第2011／0302635号明細書

発明の概要

発明が解決しようとする課題

[0006] スマートメータとHEMSコントローラおよび家電機器とを通信させるためには、HEMSコントローラおよび家電機器のそれぞれのIDおよび証明

書の情報を事前にスマートメータに設定（記憶）しておく必要がある。

[0007] そこで、本発明は、スマートメータに機器のＩＤおよび証明書の情報を簡単に設定することができる設定方法等を提供する。

課題を解決するための手段

[0008] 本発明の一態様に係る設定方法は、スマートメータと複数の機器とのネットワーク接続の認証に用いられる、前記機器のＩＤおよび証明書を前記スマートメータに設定するための設定方法であって、第１の通信ネットワークを介して接続されるスマートメータから、前記スマートメータのユーザ情報に対応づけられた前記スマートメータのＩＤを取得する第１取得ステップと、第２の通信ネットワークを介して接続される前記複数の機器のうちの１つであるコントローラから、前記コントローラのユーザ情報に対応づけられた、前記コントローラのＩＤおよび証明書と、前記コントローラが制御を行う前記複数の機器のうちの１つである家電機器のＩＤおよび証明書とを取得する第２取得ステップと、前記スマートメータのユーザ情報および前記コントローラのユーザ情報に基づいて、前記スマートメータのＩＤと、前記コントローラのＩＤおよび証明書、並びに前記家電機器のＩＤおよび証明書とを対応づけた管理情報を作成する管理ステップと、前記管理情報に基づいて、前記スマートメータのＩＤに対応づけられた前記コントローラのＩＤおよび証明書と、前記家電機器のＩＤおよび証明書とを当該スマートメータに送信する送信ステップとを含む。

[0009] なお、これらの包括的または具体的な態様は、装置、システム、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能なＣＤ－ＲＯＭなどの記録媒体で実現されてもよく、装置、システム、集積回路、コンピュータプログラムおよび記録媒体の任意な組み合わせで実現されてもよい。

発明の効果

[0010] 本発明によれば、スマートメータに機器のＩＤおよび証明書の情報を簡単に設定することができる。

図面の簡単な説明

[0011] [図1A]図1Aは、実施の形態1に係る機器認証システムのシステム構成図で

ある。

[図1B]図1Bは、実施の形態1に係る機器認証システムの動作を示すフロー

チャートである。

[図2]図2は、実施の形態1に係る、スマートメータ、HEMSコントローラ

、および、リモートサーバそれぞれの構成を示すブロック図である。

[図3]図3は、実施の形態1に係るリモートサーバが備えるデータベースに保

存される認証テーブルの構成例を示す図である。

[図4]図4は、実施の形態1に係る各機器間のデータのやり取りを示すシーケ

ンス図である。

[図5]図5は、実施の形態2に係る機器認証システムのシステム構成図である

。

[図6]図6は、実施の形態2において、初期状態(図5)からユーザリタイ

システムが接続された状態のシステム構成図である。

[図7]図7は、実施の形態3に係る機器認証システムのシステム構成図である

。

[図8]図8は、実施の形態3において、新たな家電機器がHEMSコントロー

ラに接続されることによって、リモートサーバが備えるデータベースのデー

タが更新されるとき例を示す図である。

発明を実施するための形態

[0012] 本発明の一態様に係る設定方法は、スマートメータと複数の機器とのネッ

トワーク接続の認証に用いられる、前記機器のIDおよび証明書を前記スマ

ートメータに設定するための設定方法であって、第1の通信ネットワークを

介して接続されるスマートメータから、前記スマートメータのユーザ情報に

対応づけられた前記スマートメータのIDを取得する第1取得ステップと、

第2の通信ネットワークを介して接続される前記複数の機器のうちの1つで

あるコントローラから、前記コントローラのユーザ情報に対応づけられた、

前記コントローラのIDおよび証明書と、前記コントローラが制御を行う前

記複数の機器のうちの1つである家電機器のIDおよび証明書とを取得する第2取得ステップと、前記スマートメータのユーザ情報および前記コントローラのユーザ情報に基づいて、前記スマートメータのIDと、前記コントローラのIDおよび証明書、並びに前記家電機器のIDおよび証明書とを対応づけた管理情報を作成する管理ステップと、前記管理情報に基づいて、前記スマートメータのIDに対応づけられた前記コントローラのIDおよび証明書と、前記家電機器のIDおよび証明書とを当該スマートメータに送信する送信ステップとを含む。

[0013] このように、機器（HEMSコントローラおよび家電機器）のIDおよび証明書を、より簡単にスマートメータに設定することができる。

[0014] また、例えば、前記第2の通信ネットワークを介して、前記管理情報に含まれない前記コントローラのIDおよび証明書または前記管理情報に含まれない前記家電機器のIDおよび証明書である、新規機器情報を取得した場合、前記管理ステップでは、前記新規機器情報を前記スマートメータのIDと対応づけて前記管理情報に追加することによって、前記管理情報を更新し、前記送信ステップでは、前記新規機器情報を、当該新規機器情報に対応づけられたIDを有する前記スマートメータに送信してもよい。

[0015] また、例えば、前記第1の通信ネットワークは、前記スマートメータとの通信専用のセキュアな通信ネットワークであってもよい。

[0016] また、例えば、前記コントローラは、前記機器を制御するHEMS（Home Energy Management System）コントローラであってもよい。

[0017] また、例えば、前記機器のIDは、当該機器のMAC（Media Access Control）アドレスであってもよい。

[0018] 本発明の一態様に係る機器認証方法は、スマートメータと複数の機器とのネットワーク接続を、サーバを用いて認証する機器認証方法であって、前記複数の機器のうちの1つである家電機器を制御する、前記複数の機器のうちの1つであるコントローラが、前記家電機器のIDおよび証明書を取得する

第1通信ステップと、前記コントローラが、前記第1通信ステップにおいて取得した前記家電機器のIDおよび証明書を前記サーバに送信する第2通信ステップと、前記サーバが、前記スマートメータのユーザ情報に対応づけられた前記スマートメータのIDを取得する第1取得ステップと、前記コントローラのユーザ情報に対応づけられた、前記コントローラのIDおよび証明書と、前記家電機器のIDおよび証明書とを取得する第2取得ステップと、前記サーバが、前記スマートメータのユーザ情報および前記コントローラのユーザ情報に基づいて、前記第1取得ステップにおいて取得した前記スマートメータのIDと、前記第2取得ステップにおいて取得した前記コントローラのIDおよび証明書、並びに前記家電機器のIDおよび証明書とを対応づけた管理情報を作成する管理ステップと、前記サーバが、前記管理情報に基づいて、前記スマートメータのIDに対応づけられた前記コントローラのIDおよび証明書と、前記家電機器のIDおよび証明書とを当該スマートメータに送信する送信ステップとを含む。

[0019] このように、機器のIDおよび証明書を、機器認証システムにより簡単にスマートメータに設定することができる。

[0020] また、例えば、前記スマートメータが、前記コントローラのIDおよび証明書と、前記家電機器のIDおよび証明書とを前記サーバから取得する第3取得ステップと、前記スマートメータが、前記コントローラまたは前記家電機器から前記認証を要求する情報である認証要求を受信したときに、前記認証要求に含まれるIDおよび証明書と、前記第3取得ステップにおいて取得したIDおよび証明書とが一致しているかどうかを判断し、一致している場合は、前記認証要求を送信した前記コントローラまたは前記家電機器と前記スマートメータとのネットワーク接続を許可する認証ステップを含んでもよい。

[0021] また、例えば、前記第1通信ステップにおいて、前記コントローラは、ZigBee（登録商標）規格に準拠した無線通信により前記家電機器と通信して前記家電機器のIDおよび証明書を取得してもよい。

[0022] 本発明の一態様に係る機器認証システムは、スマートメータと複数の機器とのネットワーク接続の認証に用いられる、前記機器のＩＤおよび証明書をサーバによって前記スマートメータに設定する機器認証システムであって、前記機器認証システムは、前記複数の機器のうちの１つである家電機器を制御する、前記複数の機器のうちの１つであるコントローラと、サーバとを備え、前記コントローラは、前記家電機器のＩＤおよび証明書を取得するための第１通信部と、前記第１通信部が取得した前記家電機器のＩＤおよび証明書を前記サーバに送信する第２通信部とを有し、前記サーバは、前記スマートメータのユーザ情報に対応づけられた前記スマートメータのＩＤを取得する第１取得部と、前記コントローラのユーザ情報に対応づけられた、前記コントローラのＩＤおよび証明書と、前記家電機器のＩＤおよび証明書とを取得する第２取得部と、前記スマートメータのユーザ情報および前記コントローラのユーザ情報に基づいて、前記第１取得部が取得した前記スマートメータのＩＤと、前記第２取得部が取得した前記コントローラのＩＤおよび証明書、並びに前記家電機器のＩＤおよび証明書とを対応づけた管理情報を作成する管理部と、前記管理情報に基づいて、前記スマートメータのＩＤに対応づけられた前記コントローラのＩＤおよび証明書と、前記家電機器のＩＤおよび証明書とを当該スマートメータに送信する送信部とを有する。

[0023] 本発明の一態様に係るコントローラは、サーバが機器の認証情報をスマートメータに送信した後に行われる、前記機器と前記スマートメータとの無線ネットワーク接続である第１ペアリングのための通信を行うコントローラであって、前記機器との無線ネットワーク接続である第２ペアリングを行って、前記機器の認証情報を取得する第１通信部と、前記第１通信部が取得した前記機器の認証情報を前記サーバに送信する第２通信部とを備える。

[0024] このように、コントローラは、スマートメータと機器とを無線ネットワークにより接続する最終的なペアリング（第１ペアリング）の前に予備的にコントローラと家電機器とを接続する第２のペアリングを行う。これにより、コントローラは、家電機器のＩＤおよび証明書をまとめて取得し、一括して

サーバに送信できるため、より簡単にＩＤおよび証明書をスマートメータに送信することができる。

[0025] また、例えば、サーバが機器の認証情報をスマートメータに送信した後に行われる、前記機器と前記スマートメータとの無線ネットワーク接続である第１ペアリングのための通信を行うコントローラであって、前記機器との無線ネットワーク接続である第２ペアリングを行って、前記機器の認証情報を取得する第１通信部と、前記第１通信部が取得した前記機器の認証情報を前記サーバに送信する第２通信部とを備えてもよい。

[0026] また、例えば、前記第１通信部は、前記機器の認証情報を取得した後、前記第１のペアリングが行われる前に前記第２のペアリングを解除してもよい。

[0027] なお、これらの包括的または具体的な態様は、装置、システム、方法、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能なＣＤ－ＲＯＭなどの記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラムまたは記録媒体の任意な組み合わせで実現されてもよい。

[0028] 以下、実施の形態について、図面を参照しながら具体的に説明する。

[0029] なお、以下で説明する実施の形態は、いずれも包括的または具体的な例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置位置および接続形態、ステップ、ステップの順序などは、一例であり、本発明を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素については、任意の構成要素として説明される。

[0030] （実施の形態１）

まず、本実施の形態に係る機器認証システムの概要について説明する。

[0031] 図１Ａは、実施の形態１に係る機器認証システムのシステム構成図である。

[0032] 図１Ａにおいて、機器認証システム１００は、スマートメータ（ＳＭ：Ｓ

mart Meter) 130と、HEMSコントローラ (HEMS-C : HEMS-Controller) 110と、リモートサーバ (Remote Server) 120とを備える。また、機器認証システム100は、さらに、家電機器 (Appliance) 141および142を備えてもよい。

[0033] 図1Aに示されるホームネットワーク (Home Network) 101は、ユーザ宅内のネットワークを意味する。また、ユーティリティネットワーク (Utility Network) 102は、例えば、電力会社、ガス会社、または水道会社などのインフラ事業者のネットワークを意味する。

[0034] ここで、スマートメータ130は、通信機能を有するメータであり、ユーザ宅内に設けられ、ユーザ宅の消費電力量、ガスの使用量、または水道の使用量などをそれぞれAMI (Advanced Metering Infrastructure) 104を通じてインフラ事業者に送信する。

[0035] スマートメータ130と、HEMSコントローラ110並びに家電機器141および142 (以下まとめて家電機器140と記載する) とを通信させることで、HEMSコントローラ110および家電機器140においてスマートメータ130の情報を利用した様々なサービスを提供することが考えられる。しかしながら、スマートメータ130と、HEMSコントローラ110および家電機器140とをセキュアに通信させるためには、HEMSコントローラ110および家電機器140のそれぞれの機器IDおよび証明書 (アカウントおよびパスワードなど通信のために用いられる認証情報) を予めスマートメータ130内に設定しておく必要がある。

[0036] しかしながら、HEMSコントローラ110および家電機器140を提供する事業者と、スマートメータ130をユーザ宅内に設置したインフラ事業者とは通常異なる。このため、上記機器IDおよび証明書をスマートメータ130内に記憶するためには、通常インフラ事業者へ作業員の派遣を依頼し、当該作業員がスマートメータ130内に上記機器IDおよび証明書を設定

する作業（工事）が必要である。つまり新たな家電機器 140 がユーザ宅内に追加されるごとに機器 ID および証明書のスマートメータ 130 への登録（設定）をインフラ事業者へ依頼する必要がある、利便性が低いことが課題である。

[0037] そこで、本実施の形態に係る機器認証システム 100 では、リモートサーバ 120 がユーザ宅の HEMS コントローラ 110、並びに家電機器 140 を、スマートメータ 130 の通信対象の機器として設定する。これにより、ユーザまたは家電機器 140 の事業者（メーカー）は、HEMS コントローラ 110 から機器 ID および証明書を、パケットネットワーク 103 を通じて送信する簡易な手続きにより、家電機器の機器 ID および証明書をスマートメータ 130 内に記憶させることができる。

[0038] この結果、スマートメータ 130 と、HEMS コントローラ 110 および家電機器 140 とが、同一のネットワークによって接続されるので、これらの機器が相互に通信することができる。すなわち、上述のようなスマートメータ 130 の情報を用いた様々なサービスが実現される。

[0039] 以下、図 1 A を用いて機器認証システム 100 の各構成について説明する。

[0040] 図 1 A において、スマートメータ 130 は、ユーザ宅（図示しない）に設置されているものとする。スマートメータ 130 は、AMI 104 として、ユーティリティネットワーク 102 に接続されている。スマートメータ 130 は、ユーティリティネットワーク 102 内のユーティリティヘッドエンド（Utility Head End）105 によりコントロールされている。なお、ユーティリティネットワーク 102 内には、データベース 170 が設けられている。

[0041] ユーティリティヘッドエンド 105 は、AMI を用いて、スマートメータ 130 からユーザ宅の消費電力量、ガスの使用量、または水道の使用量などを検針する。また、スマートメータ 130 は、通信対象の HEMS コントローラ 110 や各家電機器 140 に制御信号を送信することができる。

[0042] HEMSコントローラ110には、エアコン、冷蔵庫、洗濯機などの家電機器140が通信ネットワークを介して接続される。すなわち、HEMSコントローラ110は、HEMSコントローラ110に接続された各家電機器140を制御する。なお、ここでの家電機器140とは、家庭内で使用されるものに限定されず、コピー機などの事務用機器、医療用機器などの種々の電気機器を含む。すなわち、ここでの家電機器140とは、一般的な電気機器を意味する。

[0043] 図1Aにおいて、スタートメータ130、AM1104、およびユーティリティハットエント105は、ユーティリティネットワーク102を構成している。

[0044] また、HEMSコントローラ110および家電機器140は、ユーザ宅のホームネットワーク101構成している。

[0045] リモートサーバ120は、HEMSコントローラ110に接続されている各家電機器140のIDおよび証明書を収集（取得）し、各家電機器140のIDおよび証明書に基づいて設定対象のスタートメータ130に対して認証要求を行う。なお、リモートサーバ120は、ユーザ宅外（スタートメータ130、HEMSコントローラ110、および家電機器140が設けられる建物の外部）に設けられ、例えば、HEMSコントローラ110または家電機器140のメーカーによって管理される。また、リモートサーバ120は、データベース160を備える。

[0046] 次に、機器認証システム100の動作の概要について図1Aおよび図1Bを参照しながら説明する。

[0047] 図1Bは、機器認証システム100の動作を示すフローチャートである。まず、HEMSコントローラ110は、各家電機器140のIDおよび証明書を取得する（S101）。家電機器140のIDは、具体的には、家電機器のMAC（Media Access Control）アドレスであるが、家電機器を識別できる他の情報であってもよい。後述するHEMSコントローラ110のIDおよびスタートメータ130のIDについても同様

である。

[0049] なお、このとき、HEMSコントローラ110は、家電機器141および142と無線ネットワークにより接続される。この無線接続（第2ペアリンク）の詳細については後述する。

[0050] 次に、HEMSコントローラ110は、HEMSコントローラ110の1Dおよび証明書と、スラップS101において取得した家電機器140の1Dおよび証明書とをリモートサーバ120に送信する（S102）。HEMSコントローラ110とリモートサーバ120との通信には、パケットネットワーク103が用いられる。パケットネットワーク103は、具体的には、例えば、インターネット網である。

[0051] 次に、リモートサーバ120は、受信したHEMSコントローラ110の1Dおよび証明書と、家電機器140の1Dおよび証明書とをHEMS-C・家電の管理テーブルとしてデータベース160に保存する（S103）。次に、スマートメータ130は、スマートメータ130の1Dをリモートサーバ120に送信する（S104）。

[0053] リモートサーバ120は、受信したスマートメータ130の1Dをスマートメータ130の管理テーブルとして、データベース160に保存する（S105）。

[0054] さらに、リモートサーバ120は、スマートメータの1Dと、HEMSコントローラ110の1Dおよび証明書、並びに家電機器140の1Dおよび証明書とを対応づけた情報である認証テーブル（管理リスト、管理情報）を生成し、データベース160に保存する（S106）。

[0055] 最後に、リモートサーバ120は、スラップS106において生成した認証テーブルに基づいて、スマートメータ130の1Dに対応づけられたHEMSコントローラ110の1Dおよび証明書と、家電機器140の1Dおよび証明書とを当該スマートメータ130に送信する（S107）。リモートサーバ120とスマートメータ130との通信には、専用のセキュアな通信ネットワークが用いられる。セキュアなネットワークとは、スマートメータ

１３０を提供しているインフラ事業者と、リモートサーバ１２０の事業者とだけが接続可能な専用のネットワークを意味する。

[0056] 次に、スマートメータ１３０、ＨＥＭＳコントローラ１１０、およびリモートサーバ１２０それぞれの具体的な構成について説明する。

[0057] 図２は、スマートメータ１３０、ＨＥＭＳコントローラ１１０、およびリモートサーバ１２０それぞれの構成を示すブロック図である。

[0058] まず、スマートメータ１３０について説明する。

[0059] 図２に示されるように、スマートメータ１３０は、通信インターフェースとしてＡＭＩネットワークＩＦ１３４（第３取得部）とホームネットワークＩＦ１３５とを備える。

[0060] スマートメータ１３０は、また、指令部（Commissioning Manager）１３１と、認証部（Certification Manager）１３２と、メモリ１３６とを備える。

[0061] 指令部１３１は、ＡＭＩネットワークＩＦ１３４を用いてスマートメータ１３０のＩＤをリモートサーバ１２０に送信する。また、指令部１３１は、ＡＭＩネットワークＩＦ１３４を用いてリモートサーバ１２０からスマートメータ１３０に関連するＨＥＭＳコントローラ１１０の証明書および家電機器１４０の証明書を受信する。また、指令部１３１は、リモートサーバ１２０から受信したＨＥＭＳコントローラ１１０の証明書および家電機器１４０の証明書をメモリ１３６に保存する。

[0062] 認証部１３２は、スマートメータ１３０に接続されるＨＥＭＳコントローラ１１０や家電機器１４０を認証する。具体的には、認証部１３２は、スマートメータ１３０に認証要求をしてきたＨＥＭＳコントローラ１１０および家電機器１４０のＩＤおよび証明書と、メモリ１３６に記憶されたＩＤおよび証明書とを照合し、一致するか否かを判断する。一致している場合は、認証要求を送信したＨＥＭＳコントローラ１１０および家電機器１４０とのスマートメータ１３０とのネットワーク接続を許可する。

[0063] このネットワーク接続は、本実施の形態では、Ｚｉｇｂｅｅ（登録商標）

規格に準拠した無線通信ネットワーク接続である。しかしながら、上記ネットワーク接続は、その他の無線LAN接続(Wi-Fi (登録商標) など)であってもよいし、有線接続であってもよい。

[0064] メモリ136には、リモートサーバ120が送信した、HEMSコントローラ110のIDおよび証明書並びに家電機器140のIDおよび証明書が保存(記憶)される。メモリ136は、例えば、DRAM (Dynamic Random Access Memory)、または強誘電体メモリなどである。

[0065] 次に、HEMSコントローラ110について説明する。

[0066] HEMSコントローラ110は、通信インターフェースとしてホームネットワーク114 (第1通信部) とパケットネットワーク115 (第2通信部) とを備える。

[0067] また、HEMSコントローラ110は、収集部(Gathering Manager) 113と、指令部(Commissioning Manager) 111と、認証部(Certification Manager) 112と、メモリ116とを備える。

[0068] 収集部113は、家電機器140から家電機器140のIDおよび証明書を集める。家電機器140のIDおよび証明書は、収集部113によってネットワーク経由で集められてもよいし、HEMSコントローラ110の管理者の手動によってメモリ116内に登録されてもよい。

[0069] 本実施の形態では、収集部113は、ZigBee規格に準拠した無線通信ネットワークを用いて家電機器140のIDおよび証明書を集める。しかしながら、上記ネットワーク接続は、その他の無線LAN接続(Wi-Fi など)であってもよいし、有線接続であってもよい。

[0070] 指令部111は、指令部111自身のIDおよび証明書、並びに収集部113が集めた各家電機器140のIDおよび証明書をリモートサーバ120に送信する。このとき、指令部111は、HEMSコントローラ110のユーザを示すユーザ情報も合わせてリモートサーバ120に送信する。

- [0071] 認証部 112 は、スタートメータ 130 に認証要求を行う。
- [0072] メモリ 116 には、HEMS コントローラ 110 自身の ID および証明書、並びに HEMS コントローラ 110 に接続されている各家電機器 140 の ID および証明書が保存される。メモリ 116 は、例えば、DRAM、または強誘電体メモリなどである。
- [0073] 次に、リモートサーバ 120 について説明する。
- [0074] リモートサーバ 120 は、いわゆる情報処理装置であり、通信のインターフェースとしてパケットネットワーク 125 (第 2 取得部) と AMI ネットワーク 124 (第 1 取得部、送信部) とを備える。また、リモートサーバ 120 は、データベース 160 と、管理部 (System Manager) 121 とを備える。
- [0075] パケットネットワーク 125 は、ホームネットワーク 101 を介して接続される HEMS コントローラ 110 から、当該 HEMS コントローラ 110 の ID および証明書と、HEMS コントローラ 110 が制御を行う家電機器 140 の ID および証明書とを取得する。
- [0076] AMI ネットワーク 124 は、ユーティリティネットワーク 102 を介して接続されるスタートメータ 130 から、当該スタートメータ 130 の ID とを取得する。
- [0077] また、AMI ネットワーク 124 は、HEMS コントローラ 110 の ID および証明書と、家電機器 140 の ID および証明書とを当該スタートメータ 130 に送信する。HEMS コントローラ 110 の証明書および家電機器 140 の証明書は、管理部 121 が認証ツールに基づいて発行したものである。
- [0078] データベース 160 には、HEMS コントローラ 110 の証明書および家電の証明書とスタートメータの ID とが保存される。データベース 160 は、例えば、HDD (Hard Disc Drive)、DRAM、または強誘電体メモリなどで実現される。
- [0079] 管理部 121 は、ユーザ情報に基づいて、AMI ネットワーク 124

が取得したスタートメータ130のIDと、パケットネットワーク1F12
 が取得したHEMSコントローラ110のIDおよび証明書、並びに家電
 機器140のIDおよび証明書とを対応づけた認証テーブルを作成する。

[0080] なお、ユーザ情報は、ユーザを識別可能な情報である。ユーザ情報は、1
 DとともにHEMSコントローラ110およびスタートメータ130から送
 信されてもよいし、ID自体がユーザ情報を含むような情報であってもよい
 。また、リモートサーバ120内のデータベース160内において、取得し
 たIDに対応するユーザ情報が予め記憶されることで、IDとユーザ情報と
 が対応づけられていてもよい。

[0081] また、管理部121は、データベース160に登録されている認証テーブ
 ル（管理情報）に基づき、スタートメータ130に当該スタートメータ13
 0に対応づけられたHEMSコントローラ110の証明書および家電機器1
 40の証明書を発行する。

[0082] なお、上述のように、図1Aにおいてホームネットワーク101の通信プ
 ロトコルは、Zigbeeを用いることができる。すなわちスタートメータ
 130およびHEMSコントローラ110、HEMSコントローラ110お
 よび家電機器140、スタートメータ130および家電機器140のそれぞ
 れの間における通信プロトコルとしてZigbeeを用いることができる。
 [0083] 次に、リモートサーバ120のデータベース160に保存される認証テー
 ブルについて説明する。

[0084] 図3は、図2に示されるリモートサーバ120のデータベース160に保
 存される認証テーブルの構成例を示す図である。
 [0085] 図3に示されるように、リモートサーバ120は、スタートメータ130
 のID情報とHEMSコントローラ110および家電機器140のIDおよ
 び証明書とを紐付ける。
 [0086] まず、図3(a)に示されるように、リモートサーバ120のデータベー

ス160には、HEMSコントローラ110と各家電機器140とを対応づ
 けたHEMS-C・家電の管理テーブルが保存される。この管理テーブルで

は、各ユーザID (Individual ID、ユーザ情報) と、HEMSコントローラ110のIDおよび証明書と、各家電機器140のIDおよび証明書とが対応づけられて記憶される。

[0087] 例えば、図3(a)の場合、ユーザ「Aさん」のHEMSコントローラ110である、「Pana1」および証明書「AAA0」に対して、HEMSコントローラ110に接続されている各家電機器140のID「AOU1」、「AIU1」、および「AIU2」と、証明書「AAA1」、「AAA2」、および「AAA3」とが、それぞれ対応づけられている。

[0088] また、図3(b)に示されるように、リモートサーバ120のデータベース160には、スマートメータ130の管理テーブルとして、各ユーザID (Individual ID) とスマートメータ130のID (SM ID) とが対応づけられて記憶されている。

[0089] 例えば、図3(b)の場合、ユーザ「Aさん」、「Bさん」、および「Cさん」に対してそれぞれスマートメータ130である、「メータA」、「メータB」、および「メータC」が対応づけられている。

[0090] さらに、リモートサーバ120は、HEMS-C・家電の管理テーブルおよびスマートメータ130の管理テーブルから認証テーブルを作成する。

[0091] 図3(c)の認証テーブルは、例えば、ユーザ「Aさん」宅には、「メータA」のスマートメータ130が接続され、「Pana1」のHEMSコントローラ110、および、IDが「AOU1」、「AIU1」、「AIU2」の家電機器140が設置されていることを示している。また、図3(c)の認証テーブルは、「Aさん」宅のスマートメータ130である「メータA」に対応するHEMSコントローラ110「Pana1」の証明書は「AAA0」であり、家電「AOU1」、「AIU1」、および「AIU2」の証明書は、それぞれ、「AAA1」、「AAA2」、および「AAA3」であることを示している。

[0092] スマートメータ130は、リモートサーバ120の認証テーブルに基づいてHEMSコントローラ110の証明書および家電機器140の証明書を入

手し、証明書のある家電機器だけを認証する。これにより、家電機器のなりすましや不正接続を防ぐことができる。

[0093] また、スマートメータ 130 は、接続を許可した通信対象の HEMS コントローラ 110 および各家電機器 140 に接続することにより、これらの機器に制御信号を送信することができる。すなわち、HEMS コントローラ 110 および家電機器 140 と、スマートメータ 130 とを連携させた様々なサービスを提供することが可能となる。

[0094] 以下、以上のように構成された機器認証システム 100 の動作の詳細について説明する。

[0095] 図 4 は、実施の形態 1 に係る各機器間のデータのやり取りを示すシーケンス図である。

[0096] まず、スマートメータ 130 の指令部 131 は、自身の ID を AMI ネットワーク 1F134 を用いて、リモートサーバ 120 に送信する (S201)。

[0097] 次に、リモートサーバ 120 は、AMI ネットワーク 1F124 を用いてスマートメータ 130 において送信されたスマートメータ 130 の ID を受信した後、スマートメータ 130 の ID とユーザ ID とを関連付けてデータベース 160 に保存する (S202)。

[0098] 一方、HEMS コントローラ 110 は、まだ自身に接続されていない家電機器 140 から接続要求を受信すると (S203)、この家電機器 140 に接続応答を送信することによりこの家電機器 140 を自身に接続する (S204)。このとき、HEMS コントローラ 110 は、接続要求を送信してき

[0099] その後、HEMS コントローラ 110 の収集部 113 は、この新たに接続された家電機器 140 に対して、ホームネットワーク 1F114 を用いて証明書要求を送信する (S205)。

[0100] 証明書要求を受信した家電機器 140 は、自身の証明書を HEMS コントローラ 110 に送信する (S206)。HEMS コントローラ 110 の収集

部 113 は、ホームネットワーク I/F 114 を用いて証明書を受信し、メモリ 116 に保存する (S207)。

[0101] HEMSコントローラ 110 に複数の家電機器 140 が接続されている場合には、HEMSコントローラ 110 は、複数の家電機器 140 の証明書を同様の方法で入手する。

[0102] 次に、HEMSコントローラ 110 の指令部 111 は、パケットネットワーク I/F 115 を用いて自身の ID および証明書と、家電機器 140 の ID および証明書をリモートサーバ 120 に送信する (S208)。

[0103] リモートサーバ 120 は、パケットネットワーク I/F 125 を用いて受信した HEMSコントローラ 110 の ID および証明書と、家電機器 140 の ID および証明書を関連付けてデータベース 160 に保存する (S209)。データベース 160 には、スマートメータ 130 の ID と、HEMSコントローラ 110、および家電機器 140 のそれぞれの ID および証明書の情報が紐付けられて保存される。

[0104] リモートサーバ 120 の管理部 121 は、データベース 160 を参照し、スマートメータ 130 の ID に対応する HEMSコントローラ 110 の ID および証明書と、家電機器の ID および証明書を当該スマートメータ 130 に送信する (S210)。

[0105] スマートメータ 130 の指令部 131 は、AMI ネットワーク I/F 134 から HEMSコントローラ 110 の ID および証明書と、家電機器 140 の ID および証明書を受信する。スマートメータ 130 のメモリ 136 内には、これらの ID および証明書が保存される (S211)。

[0106] HEMSコントローラ 110 の認証部 112 は、ホームネットワーク I/F 114 を用いて、スマートメータ 130 へ認証要求を送信する (S212)。この認証要求を送信するタイミングについては特に限定されるものではない。例えば、リモートサーバ 120 から、HEMSコントローラの ID および証明書と、家電機器 140 の ID および証明書をスマートメータ 130 に送信したことを通知されることにより、HEMSコントローラ 110 は、

認証要求をスタートメータ 130 に送信してもよい。また、HEMS コントローラ 110 は、HEMS コントローラ 110 の ID および証明書と、家電機器 140 の ID および証明書とをリモートサーバ 120 に送信してから (S208)、所定の時間が経過した後にスタートメータ 130 に認証要求を送信してもよい。

[0107] 次に、スタートメータ 130 の認証部 132 は、ホームネットワーク 1F135 から認証要求を受信すると、スタートメータ 130 の認証部 132 は、メモリ 136 に保存されている、当該認証要求を送信してきた HEMS コントローラ 110 の ID に対応する証明書と、ホームネットワーク 1F135 から受信した証明書とを比較する (S213)。両者が同一である場合には、スタートメータ 130 は、HEMS コントローラ 110 の接続許可 (認証) を行う (S214)。

[0108] ここで、認証要求の際には、証明書をそのまま用いても構わないし、証明書を用いて生成された認証キーを用いても構わない。例えば、証明書からハッシュ関数を用いて認証キーを生成して使用する方法がある。

[0109] HEMS コントローラ 110 は、ホームネットワーク 1F114 を用いてスタートメータ 130 から受信した接続許可によって、スタートメータ 130 と通信することが可能になる。

[0110] なお、HEMS コントローラ 110 に接続されている各家電機器 140 について、HEMS コントローラ 110 の認証処理 (S212～S214) と同様の方法でスタートメータ 130 に認証され、スタートメータ 130 と通信することが可能になる (S215～S217)。

[0111] HEMS コントローラ 110 および家電機器 140 の証明書は、例えば、同一でも構わないし、また、同種類の家電機器 140 には、同一の証明書を設定しても構わない。また、HEMS コントローラ 110 および家電機器 140 の証明書は、全て異なっても構わない。

[0112] ユーザ ID は、任意の ID でも構わないし、ユーザ宅の住所や名前などの情報でも構わない。

- [0113] 以上、本実施の形態に係る機器認証システム１００では、リモートサーバ１２０を介して、ユーザ宅のＨＥＭＳコントローラ１１０およびこれに接続されている各家電機器１４０を、スマートメータ１３０の通信対象の機器として人手を介さずに設定することができる。設定後は、ＨＥＭＳコントローラ１１０およびこれに接続されている各家電機器１４０をスマートメータ１３０に接続することができ、ＨＥＭＳコントローラ１１０および家電機器１４０と、スマートメータ１３０とを連携させた様々なサービスを提供することが可能となる。
- [0114] また、スマートメータ１３０は、リモートサーバ１２０の認証テーブルに基づいてＨＥＭＳコントローラ１１０の証明書および家電機器１４０の証明書入手する。つまり、証明書のあるＨＥＭＳコントローラ１１０および家電機器１４０だけが接続許可を得られるので、通信対象の機器になりすました機器などの不正接続を防ぐことができる。
- [0115] なお、本実施の形態に係る機器認証システム１００では、特に、ＨＥＭＳコントローラ１１０の動作が特徴的である。
- [0116] ＨＥＭＳコントローラ１１０が行うステップＳ２０３およびステップＳ２０４の動作は、ＨＥＭＳコントローラ１１０と家電機器１４０とを無線ネットワークにより接続する、いわゆるペアリング動作（第２ペアリング）である。なお、この第２ペアリングは、例えば、ＨＥＭＳコントローラ１１０に設けられたボタンスイッチと家電機器１４０に設けられたボタンスイッチとを同時に押下することにより行われる。
- [0117] 第２ペアリングは、ＨＥＭＳコントローラ１１０が家電機器１４０のＩＤおよび証明書を取得するために行われるものである。すなわち、第２ペアリングは、スマートメータ１３０と、ＨＥＭＳコントローラ１１０および家電機器１４０とを無線ネットワークにより接続する最終的なペアリング（第１ペアリング）の前に予備的に行われる、いわば仮のペアリングである。よって、家電機器１４０の認証情報を取得した後、第１のペアリングが行われる前に第２のペアリングは、通常、解除される。

[0118] 第2ペアリングは、本来的には、H E M Sコントローラ110が家電機器140のIDおよび証明書を取得するために行われるが、H E M Sコントローラ110と家電機器とが無線ネットワークにより接続可能であることを事前に判断できるという効果もある。

[0119] 例えば、第2ペアリングにより、H E M Sコントローラ110および家電機器140の設置場所が、無線ネットワーク接続可能な範囲内であるかどうかを設置事業者（またはユーザ）は、事前に確認することができる。また、例えば、H E M Sコントローラ110および家電機器140の無線通信機能の故障の有無等も事前に確認可能である。

[0120] （実施の形態2）

図5は、実施の形態2に用いられる機器認証システムのシステム構成図を示す。図5に示される機器認証システム100aは、実施の形態1と異なり、スマートメータ130が存在していないシステム構成を示している。

[0121] 図5において、実施の形態1と同様にリモートサーバ120のデータベース160には、H E M Sコントローラ110のIDおよび証明書と、家電機器140のIDおよび証明書とが保存されている。例えば、図5の管理テーブルは、ユーザ「Cさん」には、IDが「P a n a 3」のH E M Sコントローラ110と、「A O U 2」、および「A I U 3」の家電機器とが設置されていることを示している。また、図5の管理テーブルは、H E M Sコントローラ110である、「P a n a 3」の証明書は、「C C C 0」であり、家電「A O U 2」および「A I U 3」の証明書は、それぞれ、「C C C 1」および「C C C 2」であることを示している。

[0122] 図6は、本実施の形態の初期状態（図5）に、スマートメータ130を含むユーティリティシステム（ユーティリティネットワーク102）が機器認証システム100aに接続された状態のシステム構成図を示している。図6では、初期状態（図5）では存在していないスマートメータ130がH E M Sコントローラ110に接続され、ユーティリティヘッドエンド105は、各ユーザに対してサービスを開始する。

[0123] 機器認証システム100aでは、図6に示されるようにユーザリタイネットワーク102が機器認証システム100aに接続された後、実施の形態1と同様にスタートメータ130のID情報がリモートサーバ120のデータベース160に登録される。スタートメータ130のID情報がデータベース160に登録されると、リモートサーバ120によって認証テーブルが作成される。

[0124] 認証テーブルが作成された後のスタートメータ130への認証処理は、実施の形態1と同様である。

[0125] 本態様によると、スタートメータ130がリモートサーバ120に接続される前に、予めHEMSコントローラ110が自身に接続される家電機器140の設定を行い、リモートサーバ120にHEMSコントローラ110のIDおよび証明書と各家電機器140のIDおよび証明書を送信する。

[0126] これにより、スタートメータ130がリモートサーバ120に接続されたときには、リモートサーバ120のデータベース160にHEMSコントローラ110のIDおよび証明書と各家電機器140のIDおよび証明書とがすでに保存されている。よって、スタートメータ130が接続されてからHEMSコントローラ110および家電機器140がスタートメータ130の認証を受けるまでの時間である認証時間を短縮することができる。

[0127] (実施の形態3)

図7は、実施の形態3に用いられる機器認証システムのシステム構成図を示す。実施の形態3では、実施の形態1のようにネットワークが構成された後で、機器認証システム100bにおいて新たな家電機器140がHEMSコントローラ110に接続されるときの実例を示す。

[0128] 図7は、家電機器143がユーザ宅内に新たに設置される例を示す図である。

[0129] 図8は、実施の形態3において、新たな家電機器143がHEMSコントローラ110に接続されることによって、リモートサーバ120が備えるデータベース160のデータが更新されるときの実例を示す図である。

[0130] 図8(a)は、家電機器143が設置される前のHEMS-C・家電の管理テーブルである。新たな家電機器143が登録されると、実施の形態1と同様の方法でHEMSコントローラ110は、リモートサーバ120に新たな家電機器143のIDおよび証明書(図8(b))を送信する。例として、図8では、新たに登録される家電機器143のIDが「A1U4」、証明書が「CCC3」であるとする。

[0131] HEMS-C・家電の管理テーブルが更新されると、図8(c)に示すように、認証テーブルも更新される。認証テーブルが更新されると、実施の形態1で示したように、リモートサーバ120は、スマートメータ130に新たな家電機器143の証明書を送信し、スマートメータ130は、新たな家電機器143の証明書によって、家電機器143の認証を行うことができる。

[0132] (変形例)

なお、本発明を上記実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されない。

[0133] 例えば、上記各実施の形態1～3のそれぞれにおいては、家電機器140の数は、2または3台であったが、4台以上であってもよい。すなわち、家電機器140の台数によらず、スマートメータ130への認証処理は、実現可能である。

[0134] また、上記各実施の形態では、1つの宅内に1つのスマートメータ130と1つのHEMSコントローラ110が設けられる例について説明したが、1つの宅内に複数のスマートメータ130が設けられてもよいし、1つの宅内に複数のHEMSコントローラ110が設けられてもよい。また、1つのスマートメータ130によって複数の世帯(ユーザ)が管理されていてもよいし、1つのHEMSコントローラ110によって複数の世帯(ユーザ)の家電機器が管理されていてもよい。また、1つのスマートメータ130に複数のHEMSコントローラ110が接続されてもよい。

[0135] また、上記各実施の形態では、HEMSコントローラ110および家電機

器 1 4 0 のそれぞれがスマートメータ 1 3 0 に認証要求をするものとして説明したが、H E M S コントローラ 1 1 0 が、当該 H E M S コントローラ 1 1 0 が制御する家電機器 1 4 0 の認証要求と自身の認証要求とを一括してスマートメータ 1 3 0 に送信してもよい。これにより、スマートメータ 1 3 0 への認証処理がより簡単となる。

[0136] なお、上記各実施の形態では、H E M S コントローラ 1 1 0 が各家電機器 1 4 0 を制御する例について説明したが、一の家電機器 1 4 0 が H E M S コントローラ 1 1 0 の機能を有し、他の家電機器 1 4 0 を制御するような構成であってもよい。すなわち、H E M S コントローラ 1 1 0 は、家電機器 1 4 0 の機能の一部として実現されてもよい。

[0137] また、上記各実施の形態では、リモートサーバ 1 2 0 とスマートメータ 1 3 0 との通信には、専用のセキュアな通信ネットワークが用いられるとしたが、リモートサーバ 1 2 0 とスマートメータ 1 3 0 との通信には、インターネット網などの汎用のネットワークが用いられてもよい。この場合、ID および証明書は、暗号化等が行われてセキュアに送受信されることが望ましい。

[0138] なお、リモートサーバ 1 2 0 とスマートメータ 1 3 0 との通信には、XML (E x t e n s i b l e M a r k u p L a n g u a g e) や、SOAP (S i m p l e O b j e c t A c c e s s P r t o c o l) が用いられてもよい。

[0139] また、上記各実施の形態では、H E M S コントローラ 1 1 0 は、家電機器 1 4 0 から ID および証明書を取得するとしたが、H E M S コントローラ 1 1 0 は、家電機器 1 4 0 から ID のみを取得してもよい。

[0140] この場合、H E M S コントローラ 1 1 0 は、上記 ID として、家電機器 1 4 0 の製造コード (M a n u f a c t u r e r I n s t a l l C o d e) やその他の家電機器 1 4 0 を識別可能な番号を家電機器 1 4 0 から取得し、リモートサーバ 1 2 0 に送信する。このような製造コードは、家電機器 1 4 0 のメーカーが独自に家電機器 1 4 0 を識別することができるものである。

。具体的には、例えば、家電機器 140 の MAC アドレスなどである。

[0141] また、例えば、家電機器 140 の ID として、ZigBee 固有の拡張メッセージ (Zigbee Manufacturer Specific Extension Code) を用いてもよい。この拡張メッセージは、HEMS コントローラ 110 と家電機器 140 とが ZigBee により無線接続される際に付与されるものである。

[0142] このように、HEMS コントローラ 110 が家電機器 140 から ID のみを取得する場合、家電機器 140 の ID とこれに対応する証明書とを当該家電機器 140 のメーカーにおいてデータベース化しておく。さらに、リモートサーバ 120 は、このデータベースにアクセスする、またはこのデータベースを予め記憶しておく。これにより、リモートサーバ 120 は、HEMS コントローラ 110 から ID のみを取得すれば、対応する証明書をスマートメータ 130 に送信することができる。

[0143] このような構成においては、HEMS コントローラ 110 とリモートサーバ 120 との間では、証明書の送受信が行われなため、より安全である。

[0144] また、HEMS コントローラ 110 が当該 HEMS コントローラ 110 に対応した正しいスマートメータ 130 を選択しているかどうかをリモートサーバ 120 に照会するような構成であってもよい。

[0145] HEMS コントローラ 110 は、無線接続可能なスマートメータ 130 が複数存在する場合、どのスマートメータ 130 が自身に対応した正しいスマートメータ 130 であるかを決定することができない場合がある。このような場合、HEMS コントローラ 110 は、リモートサーバ 120 にスマートメータ 130 の照会要求を送信してもよい。このとき、HEMS コントローラ 110 は、照会要求と合わせて、検出された近くのスマートメータ 130 の位置情報として、複数のスマートメータ 130 それぞれの、無線通信に用いられる信号の相対的な強度、スマートメータの GPS 座標、または無線環境の指紋などを送信してもよい。

[0146] HEMS コントローラ 110 からの照会要求を受信した場合、リモートサ

サーバ120は、さらに、H E M Sコントローラ110が設けられたユーザ宅の顧客宅内住所、顧客名や顧客の個人情報（例えば国民登録番号、運転免許証番号やパスポート番号など）などの関連情報を検索する。なお、これらの情報は、リモートサーバ120またはスマートメータ130を用いたサービスの顧客登録の際に取得済みであることもある。リモートサーバ120は、検索した情報に基づいて、H E M Sコントローラ110に、当該H E M Sコントローラ110に対応する正しいスマートメータ130を通知する。

[0147] また、このとき、リモートサーバ120がH E M Sコントローラ110に対応する正しいスマートメータ130がどのスマートメータ130であるのかをユーティリティネットワーク102（ユーティリティヘッドエンド105）に照会してもよい。

[0148] このとき、上記個人情報の一部は、ユーティリティネットワーク102が正しいスマートメータ130を判断するための条件として利用することができる。

[0149] また、以下のような場合も本発明に含まれる。

[0150] （1）上記の各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムで実現され得る。RAMまたはハードディスクユニットには、コンピュータプログラムが記憶されている。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わせられて構成されたものである。

[0151] （2）上記の各装置を構成する構成要素の一部または全部は、1個のシステムLSI（Large Scale Integration：大規模集積回路）から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュ

ータシステムである。ROMには、コンピュータプログラムが記憶されている。マイクロプロセッサが、ROMからRAMにコンピュータプログラムをロードし、ロードしたコンピュータプログラムにしたがって演算等の動作することにより、システムLSIは、その機能を達成する。

[0152] (3) 上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なICカードまたは単体のモジュールから構成されてもよい。ICカードまたはモジュールは、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。ICカードまたはモジュールには、上記の超多機能LSIが含まれてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、ICカードまたはモジュールは、その機能を達成する。このICカードまたはこのモジュールは、耐タンパ性を有してもよい。

[0153] (4) 本発明は、上記に示す方法で実現されてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムで実現してもよいし、コンピュータプログラムからなるデジタル信号で実現してもよい。

[0154] また、本発明は、コンピュータプログラムまたはデジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blue-ray Disc)、半導体メモリなどに記録したもので実現してもよい。また、これらの記録媒体に記録されているデジタル信号で実現してもよい。

[0155] また、本発明は、コンピュータプログラムまたはデジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送してもよい。

[0156] また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、メモリは、コンピュータプログラムを記憶しており、マイクロプロセッサは、コンピュータプログラムにしたがって動作してもよい。

[0157] また、プログラムまたはデジタル信号を記録媒体に記録して移送すること

により、またはプログラムまたはデジタル信号をネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

[0158] (5) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

[0159] 以上、一つまたは複数の態様に係る機器認証システムについて、実施の形態に基づいて説明したが、本発明は、この実施の形態に限定されるものではない。本発明の趣旨を逸脱しない限り、当業者が思いつく各種変形を本実施の形態に施したものや、異なる実施の形態における構成要素を組み合わせて構築される形態も、一つまたは複数の態様の範囲内に含まれてもよい。

産業上の利用可能性

[0160] 本発明は、H E M S等におけるスマートメータへの機器認証に用いられる、機器認証方法等として有用である。

符号の説明

[0161] 100、100a、100b 機器認証システム
101 ホームネットワーク
102 ユーティリティネットワーク
103 パケットネットワーク
104 A M I
105 ユーティリティヘッドエンド
110 H E M Sコントローラ
111、131 指令部
112、132 認証部
113 収集部
114、135 ホームネットワーク I F
115、125 パケットネットワーク I F
116、136 メモリ
120 リモートサーバ

1 2 1 管理部

1 2 4、1 3 4 AMI ネットワーク I F

1 3 0 スマートメータ

1 4 0、1 4 1、1 4 2、1 4 3 家電機器

1 6 0、1 7 0 データベース

請求の範囲

[請求項1]

スマートメータと複数の機器とのネットワーク接続の認証に用いられる、前記機器のＩＤおよび証明書を前記スマートメータに設定するための設定方法であって、

第１の通信ネットワークを介して接続されるスマートメータから、前記スマートメータのユーザ情報に対応づけられた前記スマートメータのＩＤを取得する第１取得ステップと、

第２の通信ネットワークを介して接続される前記複数の機器のうちの１つであるコントローラから、前記コントローラのユーザ情報に対応づけられた、前記コントローラのＩＤおよび証明書と、前記コントローラが制御を行う前記複数の機器のうちの１つである家電機器のＩＤおよび証明書とを取得する第２取得ステップと、

前記スマートメータのユーザ情報および前記コントローラのユーザ情報に基づいて、前記スマートメータのＩＤと、前記コントローラのＩＤおよび証明書、並びに前記家電機器のＩＤおよび証明書とを対応づけた管理情報を作成する管理ステップと、

前記管理情報に基づいて、前記スマートメータのＩＤに対応づけられた前記コントローラのＩＤおよび証明書と、前記家電機器のＩＤおよび証明書とを当該スマートメータに送信する送信ステップを含む設定方法。

[請求項2]

前記第２の通信ネットワークを介して、前記管理情報に含まれない前記コントローラのＩＤおよび証明書または前記管理情報に含まれない前記家電機器のＩＤおよび証明書である、新規機器情報を取得した場合、

前記管理ステップでは、前記新規機器情報を前記スマートメータのＩＤと対応づけて前記管理情報に追加することによって、前記管理情報を更新し、

前記送信ステップでは、前記新規機器情報を、当該新規機器情報に

対応づけられたIDを有する前記スマートメータに送信する
請求項1に記載の設定方法。

[請求項3] 前記第1の通信ネットワークは、前記スマートメータとの通信専用のセキュアな通信ネットワークである
請求項1または2に記載の設定方法。

[請求項4] 前記コントローラは、前記機器を制御するHEMS (Home Energy Management System) コントローラである
請求項1～3のいずれか1項に記載の設定方法。

[請求項5] 前記機器のIDは、当該機器のMAC (Media Access Control) アドレスである
請求項1～4のいずれか1項に記載の設定方法。

[請求項6] スマートメータと複数の機器とのネットワーク接続を、サーバを用いて認証する機器認証方法であって、

前記複数の機器のうちの1つである家電機器を制御する、前記複数の機器のうちの1つであるコントローラが、前記家電機器のIDおよび証明書を取得する第1通信ステップと、

前記コントローラが、前記第1通信ステップにおいて取得した前記家電機器のIDおよび証明書を前記サーバに送信する第2通信ステップと、

前記サーバが、前記スマートメータのユーザ情報に対応づけられた前記スマートメータのIDを取得する第1取得ステップと、

前記コントローラのユーザ情報に対応づけられた、前記コントローラのIDおよび証明書と、前記家電機器のIDおよび証明書とを取得する第2取得ステップと、

前記サーバが、前記スマートメータのユーザ情報および前記コントローラのユーザ情報に基づいて、前記第1取得ステップにおいて取得した前記スマートメータのIDと、前記第2取得ステップにおいて取

得した前記コントローラのＩＤおよび証明書、並びに前記家電機器の
ＩＤおよび証明書とを対応づけた管理情報を作成する管理ステップと
、

前記サーバが、前記管理情報に基づいて、前記スマートメータのＩ
Ｄに対応づけられた前記コントローラのＩＤおよび証明書と、前記家
電機器のＩＤおよび証明書とを当該スマートメータに送信する送信ス
テップとを含む

機器認証方法。

[請求項7] 前記スマートメータが、前記コントローラのＩＤおよび証明書と、
前記家電機器のＩＤおよび証明書とを前記サーバから取得する第３取
得ステップと、

前記スマートメータが、前記コントローラまたは前記家電機器から
前記認証を要求する情報である認証要求を受信したときに、前記認証
要求に含まれるＩＤおよび証明書と、前記第３取得ステップにおいて
取得したＩＤおよび証明書とが一致しているかどうかを判断し、一致
している場合は、前記認証要求を送信した前記コントローラまたは前
記家電機器と前記スマートメータとのネットワーク接続を許可する認
証ステップを含む

請求項６に記載の機器認証方法。

[請求項8] 前記第１通信ステップにおいて、前記コントローラは、Ｚｉｇｂ
ｅ規格に準拠した無線通信により前記家電機器と通信して前記家電機
器のＩＤおよび証明書を取得する

請求項６または７に記載の機器認証方法。

[請求項9] スマートメータと複数の機器とのネットワーク接続の認証に用いら
れる、前記機器のＩＤおよび証明書をサーバによって前記スマートメ
ータに設定する機器認証システムであって、

前記機器認証システムは、

前記複数の機器のうちの１つである家電機器を制御する、前記複数

の機器のうちの１つであるコントローラと、

サーバとを備え、

前記コントローラは、

前記家電機器のＩＤおよび証明書を取得するための第１通信部と、

前記第１通信部が取得した前記家電機器のＩＤおよび証明書を前記サーバに送信する第２通信部とを有し、

前記サーバは、

前記スマートメータのユーザ情報に対応づけられた前記スマートメータのＩＤを取得する第１取得部と、

前記コントローラのユーザ情報に対応づけられた、前記コントローラのＩＤおよび証明書と、前記家電機器のＩＤおよび証明書とを取得する第２取得部と、

前記スマートメータのユーザ情報および前記コントローラのユーザ情報に基づいて、前記第１取得部が取得した前記スマートメータのＩＤと、前記第２取得部が取得した前記コントローラのＩＤおよび証明書、並びに前記家電機器のＩＤおよび証明書とを対応づけた管理情報を作成する管理部と、

前記管理情報に基づいて、前記スマートメータのＩＤに対応づけられた前記コントローラのＩＤおよび証明書と、前記家電機器のＩＤおよび証明書とを当該スマートメータに送信する送信部とを有する

機器認証システム。

[請求項10]

サーバが機器の認証情報をスマートメータに送信した後に行われる、前記機器と前記スマートメータとの無線ネットワーク接続である第１ペアリングのための通信を行うコントローラであって、

前記機器との無線ネットワーク接続である第２ペアリングを行って、前記機器の認証情報を取得する第１通信部と、

前記第１通信部が取得した前記機器の認証情報を前記サーバに送信する第２通信部とを備える

コントローラ。

[請求項11] 前記第1通信部は、前記機器の認証情報を取得した後、前記第1のペアリングが行われる前に前記第2のペアリングを解除する

請求項10に記載のコントローラ。

[請求項12] 前記第1ペアリングおよび前記第2ペアリングは、Z i g b e e規格に準拠した無線ネットワーク接続である

請求項10または11に記載のコントローラ。