

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局

(43) 国際公開日  
2011年9月29日(29.09.2011)



(10) 国際公開番号

WO 2011/118432 A1

(51) 国際特許分類:

H04L 9/32 (2006.01) G06F 21/24 (2006.01)  
G06F 21/20 (2006.01) G09C 1/00 (2006.01)

中央区海岸通8番 慧通信技術工業 株式会社内 Hyogo (JP).

(21) 国際出願番号:

PCT/JP2011/055917

(74) 代理人: 是枝 洋介, 外(KOREEDA Yosuke et al.);  
〒6500024 兵庫県神戸市中央区海岸通8番 神港ビルディング Hyogo (JP).

(22) 国際出願日:

2011年3月14日(14.03.2011)

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(25) 国際出願の言語:

日本語

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア

(26) 国際公開の言語:

日本語

(30) 優先権データ:

特願 2010-069500 2010年3月25日(25.03.2010) JP

(71) 出願人(米国を除く全ての指定国について): 慧通信技術工業 株式会社 (Kei Communication Technology Inc.) [JP/JP]; 〒6500024 兵庫県神戸市中央区海岸通8番 Hyogo (JP).

(72) 発明者; および

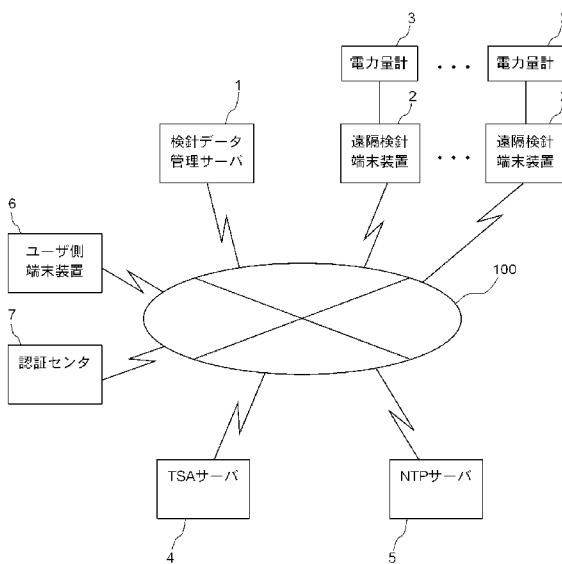
(75) 発明者/出願人(米国についてのみ): 粟田 隆央 (AWATA Takao) [JP/JP]; 〒6500024 兵庫県神戸市

[続葉有]

(54) Title: MEASUREMENT DATA MANAGEMENT METHOD AND MEASUREMENT DATA MANAGEMENT SYSTEM

(54) 発明の名称: 計測データ管理方法及び計測データ管理システム

[図1]



- 1... METER-READING DATA MANAGEMENT SERVER  
2... REMOTE METER-READING TERMINAL DEVICE  
3... ELECTRICITY METER  
4... TSA SERVER  
5... NTP SERVER  
6... USER-SIDE TERMINAL DEVICE  
7... AUTHENTICATION CENTER

(57) Abstract: On the basis of meter-reading information including measurement values, measurement dates and times, and electricity meter IDs, obtained from electricity meters (3), remote meter-reading terminal devices (2, 2, ...) create electronic signature data and send the generated electronic signature data and the aforementioned meter-reading information to a meter-reading data management server (1). If the meter-reading data management server (1) is successful in validating the electronic signature data received from a remote meter-reading terminal device (2), the meter-reading data management server generates a hash value from that meter-reading information and sends said hash value to a TSA server (4). Also, the meter-reading data management server (1) acquires a timestamp generated by the TSA server (4) and stores meter-reading data, which includes the timestamp, the meter-reading information, the electronic signature data, and the hash value.

(57) 要約:

[続葉有]



(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ 添付公開書類:

(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI  
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— 国際調査報告（条約第 21 条(3)）

---

各遠隔検針端末装置 2, 2, …は、電力量計 3 により得られた計測値、計測日時、及び電力量計 ID を含む検針情報に基づいて電子署名データを生成し、生成した電子署名データ及び前記検針情報を検針データ管理サーバ 1 へ送信する。検針データ管理サーバ 1 は、遠隔検針端末装置 2 から受信した電子署名データの検証に成功した場合、前記検針情報のハッシュ値を生成し、そのハッシュ値を TSA サーバ 4 に対して送信する。また、検針データ管理サーバ 1 は、TSA サーバ 4 によって生成されたタイムスタンプを取得し、そのタイムスタンプと、前記検針情報、前記電子署名データ及び前記ハッシュ値とを含む検針データを記憶する。

## 明細書

### 発明の名称：計測データ管理方法及び計測データ管理システム 技術分野

[0001] 本発明は、電力量計及びガスマータ等の計測値に関する計測データを管理する計測データ管理方法及びその方法を実施するための計測データ管理システムに関する。

### 背景技術

[0002] 近年では、通信ネットワーク技術の進展に伴って、遠隔地に設置された電力量計及びガスマータ等の様々な計測器とセンタ装置との間で通信ネットワークを介して種々のデータを送受信することにより、計測器によって得られた計測値に関する計測データをセンタ装置にて集中的に管理することができるコンピュータシステムが提案されている。

[0003] 例えば、特許文献1には、複数のグループに分けられた複数の端末装置とセンタ装置とを備え、各グループにおける特定の端末装置が同一のグループに属する他の端末装置の検針データを纏めて一括してセンタ装置に送信する遠隔管理システムが開示されている。この遠隔管理システムによれば、各端末装置が個別にセンタ装置に対して検針データを送信する場合と比べて、センタ装置側の負荷を軽減することができるため、検針データを効率的に収集することが可能になる。

### 先行技術文献

#### 特許文献

[0004] 特許文献1：特開2008-90544号公報

### 発明の概要

### 発明が解決しようとする課題

[0005] ところで、通信ネットワークを用いた遠隔管理の場合、何者かによって通信中にデータの改ざんが行われる危険性がある。そのため、そのようなデータの改ざんが起きた場合に、そのことを検出することができる仕組みが必要

になる。改ざんの危険性が高いインターネットを用いる場合は、その要求がより一層高くなるものと考えられる。

[0006] しかしながら、上記の遠隔管理システムの場合、センタ装置と端末装置との間の通信中又は各端末装置間の通信中等にデータが改ざんされた場合であっても、そのことを検出する手段が用意されていないため、収集されたデータが正しいものであることを担保することができなかった。

[0007] 本発明は斯かる事情に鑑みてなされたものであり、その主たる目的は、時刻データを用いることによって、上記課題を解決することができる計測データ管理方法及びその方法を実施するための計測データ管理システムを提供することにある。

### 課題を解決するための手段

[0008] 上述した課題を解決するために、本発明の一の態様の計測データ管理方法は、計測器に接続された端末装置と、前記端末装置と通信可能に接続され、前記計測器による計測処理により得られた計測値を含む計測データを管理する計測データ管理装置と、前記計測データ管理装置にて管理される計測データの認証を行うための認証装置と、時刻の認証を行うための時刻認証局とを用いて、前記計測データを管理する計測データ管理方法であって、前記端末装置が、前記計測器による計測処理により得られた計測値、当該計測処理を実行した計測日時、及び当該計測器を識別するための識別子を含む計測情報に基づいて電子署名データを生成する電子署名工程と、前記電子署名工程により生成された電子署名データ及び前記計測情報を前記計測データ管理装置へ送信する送信工程とを実行し、前記計測データ管理装置が、前記端末装置から受信した電子署名データを検証する電子署名データ検証工程と、前記電子署名データ検証工程において前記電子署名データの検証に成功した場合、前記端末装置から受信した計測情報のハッシュ値を生成するハッシュ値生成工程と、前記ハッシュ値生成工程により生成されたハッシュ値を前記時刻認証局に対して送信するハッシュ値送信工程と、前記ハッシュ値に基づいて前記時刻認証局によって生成されたタイムスタンプと前記ハッシュ値とを含む

タイムスタンプトークンを、当該時刻認証局から取得するタイムスタンプ取得工程と、前記計測情報、前記電子署名データ、及び前記タイムスタンプ取得工程により取得されたタイムスタンプトークンを含む計測データを記憶する計測データ記憶工程とを実行し、前記認証装置が、前記計測データ管理装置から前記計測データを取得する計測データ取得工程と、前記計測データ取得工程により取得された計測データに含まれるタイムスタンプトークンを前記時刻認証局に送信することにより、当該タイムスタンプトークンに含まれるタイムスタンプの検証を当該時刻認証局に対して要求するタイムスタンプ検証要求工程とを実行し、前記時刻認証局が、前記ハッシュ値送信工程の結果取得した前記ハッシュ値に基づいて生成した前記タイムスタンプトークンを記憶するタイムスタンプトークン記憶工程と、前記タイムスタンプトークン記憶工程により記憶されたタイムスタンプトークンに含まれるハッシュ値に基づいて、前記タイムスタンプ検証要求工程の結果前記認証装置から取得したタイムスタンプトークンに含まれるタイムスタンプの検証を実行するタイムスタンプ検証工程と、前記タイムスタンプ検証工程による検証の結果を前記認証装置に対して送信する検証結果送信工程とを実行する。

- [0009] この態様の計測データ管理方法において、前記計測データ管理装置が、前記計測データ記憶工程により記憶された計測データを外部の装置に対して送信する計測データ送信工程をさらに実行し、前記計測データ管理装置から計測データを受信した前記外部の装置及び前記時刻認証局によって当該計測データに含まれるタイムスタンプの検証が実行されるようにしてもよい。
- [0010] また、前記態様の前記電子署名工程において、前記端末装置が、外部のNTPサーバから前記計測日時を取得するようにしてもよい。
- [0011] また、前記態様の計測データ管理方法において、前記端末装置が、前記計測器から前記計測値を複数回取得し、これにより得られた複数の前記計測値が一致するか否かを判定する判定工程をさらに実行し、前記判定工程により複数の前記計測値が一致すると判定された場合に、前記電子署名工程を実行するようにしてもよい。

[0012] 本発明の一の態様の計測データ管理システムは、計測器に接続された端末装置と、前記端末装置と通信可能に接続され、前記計測器による計測処理により得られた計測値を含む計測データを管理する計測データ管理装置と、前記計測データ管理装置にて管理される計測データの認証を行うための認証装置と、時刻の認証を行うための時刻認証局とを備える計測データ管理システムであって、前記端末装置が、前記計測器による計測処理により得られた計測値、当該計測処理を実行した計測日時、及び当該計測器を識別するための識別子を含む計測情報に基づいて電子署名データを生成する電子署名手段と、前記電子署名手段により生成された電子署名データ及び前記計測情報を前記計測データ管理装置へ送信する送信手段とを具備し、前記計測データ管理装置が、前記端末装置から受信した電子署名データを検証する電子署名データ検証手段と、前記電子署名データ検証手段により前記電子署名データの検証に成功した場合、前記端末装置から受信した計測情報のハッシュ値を生成するハッシュ値生成手段と、前記ハッシュ値生成手段により生成されたハッシュ値を前記時刻認証局に対して送信するハッシュ値送信手段と、前記ハッシュ値に基づいて前記時刻認証局によって生成されたタイムスタンプと前記ハッシュ値とを含むタイムスタンプトークンを、当該時刻認証局から取得するタイムスタンプ取得手段と、前記計測情報、前記電子署名データ、及び前記タイムスタンプ取得手段により取得されたタイムスタンプトークンを含む計測データを記憶する計測データ記憶手段とを具備し、前記認証装置が、前記計測データ管理装置から前記計測データを取得する計測データ取得手段と、前記計測データ取得手段により取得された計測データに含まれるタイムスタンプトークンを前記時刻認証局に送信することにより、当該タイムスタンプトークンに含まれるタイムスタンプの検証を当該時刻認証局に対して要求するタイムスタンプ検証要求手段とを更に具備し、前記時刻認証局が、前記計測データ管理装置から取得した前記ハッシュ値に基づいて生成した前記タイムスタンプトークンを記憶するタイムスタンプトークン記憶手段と、前記タイムスタンプトークン記憶手段により記憶されたタイムスタンプトークン

に含まれるハッシュ値に基づいて、前記認証装置から取得したタイムスタンプトークンに含まれるタイムスタンプの検証を実行するタイムスタンプ検証手段と、前記タイムスタンプ検証手段による検証の結果を前記認証装置に対して送信する検証結果送信手段とを具備する。

[0013] この態様の計測データ管理システムにおいて、前記計測データ管理装置が、時刻認証局と共に計測データに含まれるタイムスタンプの検証を実行する外部の装置に対して、前記計測データ記憶手段により記憶された計測データを送信する計測データ送信手段をさらに具備するようにしてもよい。

[0014] また、前記態様の計測データ管理システムにおいて、前記電子署名手段が、外部のNTPサーバから前記計測日時を取得するように構成されていてもよい。

[0015] また、前記態様の計測データ管理システムにおいて、前記端末装置が、前記計測器から前記計測値を複数回取得し、これにより得られた複数の前記計測値が一致するか否かを判定する判定手段をさらに具備し、前記電子署名手段が、前記判定手段により複数の前記計測値が一致すると判定された場合に、前記電子署名データを生成するように構成されていてもよい。

## 発明の効果

[0016] 本発明に係る計測データ管理方法及び計測データ管理システムによれば、各機器間の通信の過程で計測データの改ざんが行われたか否かを確認することができる。

## 図面の簡単な説明

[0017] [図1]本発明の実施の形態に係る計測データ管理システムの構成を示すブロック図。

[図2]本発明の実施の形態に係る検針データ管理サーバの構成を示すブロック図。

[図3]本発明の実施の形態に係る検針データ管理サーバの検針データDBに格納される検針データのデータ構造を示す図。

[図4]本発明の実施の形態に係る遠隔検針端末装置が実行する遠隔検針端末装

置起動処理の手順を示すフローチャート。

[図5]本発明の実施の形態に係る遠隔検針端末装置が実行する遠隔検針端末装置ライブチェック処理の手順を示すフローチャート。

[図6]本発明の実施の形態に係る計測データ管理システムが実行する検針処理の手順を示すフローチャート。

[図7]認証センタ及びTSAサーバによって実行されるタイムスタンプ検証処理の手順を示すフローチャート。

## 発明を実施するための形態

[0018] 以下、本発明の好ましい実施の形態を、図面を参照しながら説明する。なお、以下に示す実施の形態は、本発明の技術的思想を具体化するための方法及び装置を例示するものであって、本発明の技術的思想は下記のものに限定されるわけではない。本発明の技術的思想は、特許請求の範囲に記載された技術的範囲内において種々の変更を加えることができる。

[0019] 本発明は、電力量計及びガスマータ等、各種の計測対象の計測を行う計測器により得られたデータを取り扱うことが可能である。このうち、本実施の形態では、電力量計により得られたデータを取り扱う場合について例示する。

[0020] [計測データ管理システムの構成]

図1は、本発明の実施の形態に係る計測データ管理システムの構成を示すブロック図である。図1に示すとおり、本実施の形態の計測データ管理システムは、検針データ管理サーバ1と、複数の遠隔検針端末装置2, 2, …とを備えている。これらの検針データ管理サーバ1及び遠隔検針端末装置2, 2, …は、インターネット100を介して通信可能に接続されている。なお、検針データ管理サーバ1及び遠隔検針端末装置2, 2, …間の通信は、仮想プライベートネットワーク(VPN:Virtual Private Network)で行われるため、高いセキュリティが保たれる。

[0021] 遠隔検針端末装置2, 2, …はそれぞれ、太陽光発電等の発電設備が設けられた建物等に設置されており、当該発電設備の発電量を計測する電力量計

3, 3, …と接続されている。各電力量計3, 3, …から各遠隔検針端末装置2, 2, …に対しては検針値を含む所定形式の電文がそれぞれ出力される。各遠隔検針端末装置2, 2, …はそれぞれ、各電力量計3, 3, …から受け取った電文を用いて後述するようにして検針情報を生成し、その検針情報を検針データ管理サーバ1に対して送信する。なお、検針データ管理サーバ1の構成の詳細については後述する。

[0022] また、遠隔検針端末装置2, 2, …は、液晶ディスプレイ等で構成された表示部（図示せず）を備えており、この表示部には電力量計3, 3, …の検針値等の各種の情報が表示される。さらに、遠隔検針端末装置2, 2, …は、不揮発性メモリ等で構成された記憶部（図示せず）を備えており、電力量計3, 3, …から取得した電文に基づいて生成した検針情報等の各種の情報がこの記憶部に記憶される。

[0023] また、インターネット100には、いわゆるアーカイビング方式の時刻認証を行う時刻認証局であるTSA（Time Stamping Authority）サーバ4、インターネット100に接続されている他の機器に対して時刻情報を送信するNTP（Network Time Protocol）サーバ5、本実施の形態の計測データ管理システムを利用するユーザが操作するユーザ側端末装置6、及び本実施の形態の計測データ管理システムで管理される計測データの認証を行う認証センタ7が接続されている。

#### [検針データ管理サーバの構成]

次に、本実施の形態の検針データ管理サーバ1の構成の詳細について説明する。

図2は、本発明の実施の形態に係る検針データ管理サーバ1の構成を示すブロック図である。図2に示すとおり、検針データ管理サーバ1は、CPU11と、そのCPU11に接続された主記憶装置12、補助記憶装置13及び通信インターフェース（I/F）14とを備えている。なお、これらのCPU11、主記憶装置12、補助記憶装置13及び通信I/F14はバスによって接続されている。

- [0025] C P U 1 1は、補助記憶装置13に記憶されているコンピュータプログラムを実行する。これにより、検針データ管理サーバ1は、各種のデバイスの動作を制御しながら、後述する各種の処理を実行することが可能になる。
- [0026] 主記憶装置12は、S R A MまたはD R A M等によって構成されており、補助記憶装置13に記憶されているコンピュータプログラムの読み出しに用いられる。また、主記憶装置12は、C P U 1 1がコンピュータプログラムを実行するときに、C P U 1 1の作業領域としても利用される。
- [0027] 補助記憶装置13は、フラッシュメモリ又はハードディスクなどの不揮発性記憶装置によって構成されており、C P U 1 1に実行させるための種々のコンピュータプログラム及び当該コンピュータプログラムの実行に用いられるデータ等を記憶している。また、補助記憶装置13には、後述する検針データD B 1 3 Aが設けられている。
- [0028] 通信I／F 1 4は、インターネット100を介して各種の装置と通信をするためのインターフェース装置である。上述したように、検針データ管理サーバ1と遠隔検針端末装置2, 2, …との間の通信はV P Nで行われるため、通信I／F 1 4はV P Nルータとしての機能を有している。
- [0029] 図3は、本発明の実施の形態に係る検針データ管理サーバ1の検針データD B 1 3 Aに格納される検針データのデータ構造を示す図である。図3に示すとおり、検針データは、電力量計3の検針値を含む検針情報101と、遠隔検針端末装置2によって生成される署名データ102と、検針情報101に基づいて検針データ管理サーバ1が生成するハッシュ値103と、T S Aサーバ4によって生成されるタイムスタンプ104とで構成されている。
- [0030] また、上記の検針情報101は、図3に示すとおり、電力量計3を識別するための電力量計I D（例えば製造番号等）111と、電力量計3による検針が実行された日時である検針日時112と、電力量計3の検針値である積算電力量113とで構成されている。後述するように、これらの電力量計I D 1 1 1、検針日時112及び積算電力量113は、遠隔検針端末装置2から検針データ管理サーバ1へ送信される。

[0031] [計測データ管理システムの動作]

次に、以上のように構成されている本実施の形態の計測データ管理システムの動作について、フローチャートを参照しながら説明する。なお、本実施の形態の計測データ管理システムが実行する主な処理には、（1）各遠隔検針端末装置2，2，…が起動時に実行する遠隔検針端末装置起動処理、（2）各遠隔検針端末装置2，2，…が正常に動作していることを検針データ管理サーバ1に対して通知するための遠隔検針端末装置ライブチェック処理、及び（3）検針データ管理サーバ1及び各遠隔検針端末装置2，2，…によって実行される検針処理がある。以下、これらの各処理の詳細についてそれぞれ説明する。

[0032] （1）遠隔検針端末装置起動処理

図4は、本発明の実施の形態に係る遠隔検針端末装置が実行する遠隔検針端末装置起動処理の手順を示すフローチャートである。

S N M P (Simple Network Management Protocol) エージェントである遠隔検針端末装置2は、起動時に、S N M Pマネージャである検針データ管理サーバ1に対してコールドスタートトラップを送信する（S101）。

[0033] 次に、遠隔検針端末装置2は、自身に接続されている電力量計3から、当該電力計3に固有の情報である電力量計ID及び計器乗率を取得する（S102）。そして、遠隔検針端末装置2は、インターネット100を介して、N T Pサーバ5から現在時刻を取得する（S103）。これにより、遠隔検針端末装置起動処理が終了する。

[0034] （2）遠隔検針端末装置ライブチェック処理

上述したようにして遠隔検針端末装置起動処理が実行された後、検針日時になるまで、遠隔検針端末装置2は検針データ管理サーバ1に対してアクセスを行わない。そのため、検針間隔が1ヶ月乃至1年程度等のように比較的長い場合、遠隔検針端末装置2が正常に動作しているか否かを確認する必要が生じる。以下の遠隔検針端末装置ライブチェック処理はそのための処理である。

[0035] 図5は、本発明の実施の形態に係る遠隔検針端末装置が実行する遠隔検針端末装置ライブチェック処理の手順を示すフローチャートである。

遠隔検針端末装置2は、稼働中、所定時間（例えば5分間）が経過したか否かを繰り返し判定する（S111）。ここで、所定時間が経過したと判定した場合（S111でYES）、SNMPエージェントである遠隔検針端末装置2は、SNMPマネージャである検針データ管理サーバ1に対してライブチェックトラップを送信する（S112）。このライブチェックトラップを受信した検針データ管理サーバ1は、送信元である遠隔検針端末装置2が正常に動作していることを確認することができる。

[0036] なお、検針データ管理サーバ1は、ライブチェックトラップが連続して所定回数欠損した場合等、異常を検出した場合は、その旨を示す警告情報を出力し、管理者に対して警告を行う。この場合、管理者は、ネットワーク障害が生じていないか、遠隔検針端末装置2の動作が停止していないか等を調査することになる。

### [0037] (3) 検針処理

図6は、本発明の実施の形態に係る計測データ管理システムが実行する検針処理の手順を示すフローチャートである。この検針処理は、検針データ管理サーバ1がユーザ側端末装置6から検針データの取得要求を受けたとき等のタイミングで実行される。なお、このようにユーザ側端末装置6が検針データ管理サーバ1に対して検針データの取得要求を送信する場合、その取得要求には電力量計3（又はその電力量計3と接続されている遠隔検針端末装置2）の識別子が含まれている。この取得要求を受けた検針データ管理サーバ1は、その識別子で特定される電力量計3に接続されている遠隔検針端末装置2（又はその識別子で特定される遠隔検針端末装置2）に対して、後述する処理を実行する。これにより、各ユーザは、所望の電力量計3に係る検針データを取得することができる。

[0038] 検針データ管理サーバ1はまず、検針情報の送信を要求するための検針情報送信要求を遠隔検針端末装置2に対して送信する（S121）。なお、検

針データ管理サーバ1は、この検針情報送信要求に応じて遠隔検針端末装置2から検針情報が送信されてくるのを所定時間（例えば1分程度）待つ（S122）。そして、所定時間経過しても遠隔検針端末装置2から検針情報を受信しなかった場合（S122でYES）、検針情報送信要求を遠隔検針端末装置2に対して再送信する（S121）。この再送信を例えば3回繰り返しても遠隔検針端末装置2から検針情報を受信しなかった場合、検針処理は失敗となる。

- [0039] 遠隔検針端末装置2は、検針データ管理サーバ1から送信された検針情報送信要求を受信した場合（S131）、電力量計3から積算電力量を含む電文を取得する（S132）。遠隔検針端末装置2はさらに、電力量計3から積算電力量を含む電文を取得し（S133）、ステップS132で取得した1回目の電文に示される積算電力量と、ステップS133で取得した2回目の電文に示される積算電力量とを比較してそれらの値が一致するか否かを判定する（S134）。
- [0040] ステップS134において両電文における積算電力量の値が一致しないと判定した場合（S134でNO）、遠隔検針端末装置2は、ステップS132に戻り再度電力量計3から電文を連続して2回取得し、両電文における積算電力量が一致するか否かを判定する。これを例えば3回繰り返しても積算電力量の値が一致しなかった場合、検針処理は失敗となる。このような処理を行うことにより、電力量計3の検針値の正確性を確保することができる。
- [0041] ステップS134において両電文における積算電力量の値が一致すると判定した場合（S134でYES）、遠隔検針端末装置2は、インターネット100を介してNTPサーバ5から現在時刻を取得する（S135）。このようにしてNTPサーバ5から取得した現在時刻が電力量計3の検針日時となる。これにより、電力量計3の検針日時の正確性を確保することができる。
- [0042] 次に、遠隔検針端末装置2は、起動処理の際に電力量計3から取得した電力量計IDと、ステップS135にて取得した電力量計3の検針日時と、電

力量計3から取得した電文に示される積算電力量とから構成される検針情報を用いて電子署名を実行し、署名データを生成する（S136）。具体的には、例えばRSA暗号方式を採用し、検針情報を所定長の秘密鍵で暗号化することにより署名データを生成する。遠隔検針端末装置2は、このようにして生成された署名データを検針情報と共に検針データ管理サーバ1に対して送信する（S137）。

[0043] 検針データ管理サーバ1は、遠隔検針端末装置2から検針情報及び署名データを受信した場合（S123）、公開鍵を用いてその署名データを復号することにより検証処理を実行する（S124）。そして、この検証が成功したか否かを判定する（S125）。ここで、復号ができなかった場合又は復号した結果得られた値と検針情報とが一致しなかった場合、検針データ管理サーバ1は署名データの検証に失敗したと判定し（S125でNO）、ステップS121に戻ってそれ以降の処理を繰り返す（再検針）。この再検針は例えば1回のみとし、再度署名データの検証に失敗した場合、検針データ管理サーバ1はその旨を示す警告情報を出力し、管理者に対して警告を行う。

[0044] 他方、復号した結果得られた値と検針情報とが一致した場合、この検針情報が遠隔検針端末装置2から受信したものであることが確認できたと判断できるため、検針データ管理サーバ1は署名データの検証に成功したと判定する（S125でYES）。この場合、検針データ管理サーバ1は、所定のハッシュ関数を用いて、検針情報のハッシュ値を生成する（S126）。そして、検針データ管理サーバ1は、生成したハッシュ値を、インターネット100を介してTSAサーバ4に対して送信する（S127）。

[0045] TSAサーバ4は、検針データ管理サーバ1からハッシュ値を受信すると、そのハッシュ値と現在時刻とを結合してタイムスタンプトークンを生成し、そのタイムスタンプトークンを検針データ管理サーバ1に対して送信する。ここで、TSAサーバ4は、タイムスタンプトークンに電子署名を施してもよい。この場合、そのタイムスタンプトークンを生成したのがTSAサーバ4であることを証明することが可能になる。

[0046] T S A サーバ 4 は、後に実行するタイムスタンプの検証処理の際に用いるために、上述したようにして生成したタイムスタンプトークンを保存しておく。これにより、検針データ管理サーバ 1 及び T S A サーバ 4 の両者が同一内容のタイムスタンプトークンを保存することになる。以下では、このように T S A サーバ 4 に保存されるタイムスタンプトークンを検証用タイムスタンプトークンと称する。

[0047] 検針データ管理サーバ 1 は、インターネット 100 を介して T S A サーバ 4 からタイムスタンプトークンを受信すると (S 128) 、そのタイムスタンプトークン (ハッシュ値及びタイムスタンプ) と、遠隔検針端末装置 2 から受信した上記の検針情報及び署名データとから構成される検針データを、検針データ DB 13A に保存する (S 129) 。

以上の検針処理を繰り返すことにより、検針データ管理サーバ 1 に検針データが蓄積されることになる。

[0048] なお、ユーザ側端末装置 6 からの要求に応じて上記の検針処理が実行された場合、検針データ管理サーバ 1 は、ステップ S 129 において保存した検針データを、当該ユーザ側端末装置 6 及び認証センタ 7 に対して送信する。その後、この検針データに含まれるタイムスタンプの検証処理が、認証センタ 7 及び T S A サーバ 4 によって行われることになる。以下、この (4) タイムスタンプ検証処理について説明する。

#### [0049] (4) タイムスタンプ検証処理

図 7 は、認証センタ 7 及び T S A サーバ 4 によって実行されるタイムスタンプ検証処理の手順を示すフローチャートである。

ユーザ側端末装置 6 からタイムスタンプ検証処理の実行指示を受け付けた認証センタ 7 は、検針データ管理サーバ 1 から受信した検針データに含まれる検針情報のハッシュ値を所定のハッシュ関数（上記のステップ S 126 において検針データ管理サーバ 1 が用いたハッシュ関数と同じもの）を用いて生成する (S 201) 。そして、認証センタ 7 は、生成したハッシュ値と、検針データに含まれているハッシュ値との照合を行い (S 202) 、両ハッ

シユ値が一致したことが確認された場合に、タイムスタンプトークンを含む検証要求情報をTSAサーバ4に対して送信する(S203)。

- [0050] TSAサーバ4は、認証センタ7から送信された検証要求情報を受信した場合(S211)、受信した検証要求情報に含まれるタイムスタンプトークンと、先に保存した検証用タイムスタンプトークンとの照合を行うことによってタイムスタンプの検証処理を実行する(S212)。ここで、両タイムスタンプトークンに含まれるハッシュ値が一致した場合は検証が成功したこととなり、不一致の場合は検証が失敗したことになる。TSAサーバ4は、その検証が成功したか否かを示す検証結果情報を認証センタ7に対して送信する(S213)。
- [0051] 認証センタ7は、TSAサーバ4から送信された検証結果情報を受信する(S204)。ここで、その検証結果情報がタイムスタンプの検証に成功したことを見示す情報である場合、タイムスタンプが生成された時刻に検針情報が存在しており、しかもそのタイムスタンプが生成された時刻から現在までの間に当該検針情報が改ざんされていないことになる。この場合、認証センタ7は、ユーザ側端末装置6に対して検針データの認証がなされたことを示す情報を送信する。これにより、ユーザは、検針情報が改ざんされていないことを確認することができる。
- [0052] なお、本実施の形態においては計測器として電力量計を例示しているが、本発明はこれに限定されるわけではなく、例えばガスマータ又は水道メータ等の他の計測器を用いる場合にも適用することが可能である。これらの他の計測器を用いる場合でも、上述した本実施の形態の場合と同様に、通信の過程で計測データの改ざんが行われていないかどうか等を確認することができる。
- [0053] また、上述したとおり、本実施の形態では、検針データ管理サーバ1と遠隔検針端末装置2との間の通信がSNMPを用いて行われているが、これは例示にすぎず、他の通信プロトコルを用いることも可能である。

## 産業上の利用可能性

[0054] 本発明の計測データ管理方法及び計測データ管理システムは、発電量等に関する計測データの計測データ管理方法及び計測データ管理システムなどとして有用である。

### 符号の説明

[0055] 1 検針データ管理サーバ

2 遠隔検針端末装置

3 電力量計

4 T S A サーバ

5 N T P サーバ

6 ユーザ側端末装置

7 認証センタ

11 C P U

12 主記憶装置

13 補助記憶装置

13A 検針データ D B

14 通信インターフェース

100 インターネット

101 検針情報

102 署名データ

103 ハッシュ値

104 タイムスタンプ

111 電力量計 I D

112 検針日時

113 積算電力量

## 請求の範囲

- [請求項1] 計測器に接続された端末装置と、前記端末装置と通信可能に接続され、前記計測器による計測処理により得られた計測値を含む計測データを管理する計測データ管理装置と、前記計測データ管理装置にて管理される計測データの認証を行うための認証装置と、時刻の認証を行うための時刻認証局とを用いて、前記計測データを管理する計測データ管理方法であって、  
前記端末装置が、  
前記計測器による計測処理により得られた計測値、当該計測処理を実行した計測日時、及び当該計測器を識別するための識別子を含む計測情報に基づいて電子署名データを生成する電子署名工程と、  
前記電子署名工程により生成された電子署名データ及び前記計測情報を前記計測データ管理装置へ送信する送信工程と  
を実行し、  
前記計測データ管理装置が、  
前記端末装置から受信した電子署名データを検証する電子署名データ検証工程と、  
前記電子署名データ検証工程において前記電子署名データの検証に成功した場合、前記端末装置から受信した計測情報のハッシュ値を生成するハッシュ値生成工程と、  
前記ハッシュ値生成工程により生成されたハッシュ値を前記時刻認証局に対して送信するハッシュ値送信工程と、  
前記ハッシュ値に基づいて前記時刻認証局によって生成されたタイムスタンプと前記ハッシュ値とを含むタイムスタンプトークンを、当該時刻認証局から取得するタイムスタンプ取得工程と、  
前記計測情報、前記電子署名データ、及び前記タイムスタンプ取得工程により取得されたタイムスタンプトークンを含む計測データを記憶する計測データ記憶工程と

を実行し、

前記認証装置が、

前記計測データ管理装置から前記計測データを取得する計測データ取得工程と、

前記計測データ取得工程により取得された計測データに含まれるタイムスタンプトークンを前記時刻認証局に送信することにより、当該タイムスタンプトークンに含まれるタイムスタンプの検証を当該時刻認証局に対して要求するタイムスタンプ検証要求工程と

を実行し、

前記時刻認証局が、

前記ハッシュ値送信工程の結果取得した前記ハッシュ値に基づいて生成した前記タイムスタンプトークンを記憶するタイムスタンプトークン記憶工程と、

前記タイムスタンプトークン記憶工程により記憶されたタイムスタンプトークンに含まれるハッシュ値に基づいて、前記タイムスタンプ検証要求工程の結果前記認証装置から取得したタイムスタンプトークンに含まれるタイムスタンプの検証を実行するタイムスタンプ検証工程と、

前記タイムスタンプ検証工程による検証の結果を前記認証装置に対して送信する検証結果送信工程と

を実行する、計測データ管理方法。

## [請求項2]

前記計測データ管理装置が、

前記計測データ記憶工程により記憶された計測データを外部の装置に対して送信する計測データ送信工程をさらに実行し、

前記計測データ管理装置から計測データを受信した前記外部の装置及び前記時刻認証局によって当該計測データに含まれるタイムスタンプの検証が実行される、請求項1に記載の計測データ管理方法。

## [請求項3]

前記電子署名工程において、前記端末装置が、外部のNTPサーバ

から前記計測日時を取得する、請求項 1 又は 2 に記載の計測データ管理方法。

[請求項4] 前記端末装置が、

前記計測器から前記計測値を複数回取得し、これにより得られた複数の前記計測値が一致するか否かを判定する判定工程をさらに実行し、前記判定工程により複数の前記計測値が一致すると判定された場合に、前記電子署名工程を実行する、請求項 1 乃至 3 の何れかに記載の計測データ管理方法。

[請求項5] 計測器に接続された端末装置と、前記端末装置と通信可能に接続され、前記計測器による計測処理により得られた計測値を含む計測データを管理する計測データ管理装置と、前記計測データ管理装置にて管理される計測データの認証を行うための認証装置と、時刻の認証を行うための時刻認証局とを備える計測データ管理システムであって、

前記端末装置が、

前記計測器による計測処理により得られた計測値、当該計測処理を実行した計測日時、及び当該計測器を識別するための識別子を含む計測情報に基づいて電子署名データを生成する電子署名手段と、

前記電子署名手段により生成された電子署名データ及び前記計測情報を前記計測データ管理装置へ送信する送信手段とを具備し、

前記計測データ管理装置が、

前記端末装置から受信した電子署名データを検証する電子署名データ検証手段と、

前記電子署名データ検証手段により前記電子署名データの検証に成功した場合、前記端末装置から受信した計測情報のハッシュ値を生成するハッシュ値生成手段と、

前記ハッシュ値生成手段により生成されたハッシュ値を前記時刻認証局に対して送信するハッシュ値送信手段と、

前記ハッシュ値に基づいて前記時刻認証局によって生成されたタイムスタンプと前記ハッシュ値とを含むタイムスタンプトークンを、当該時刻認証局から取得するタイムスタンプ取得手段と、

前記計測情報、前記電子署名データ、及び前記タイムスタンプ取得手段により取得されたタイムスタンプトークンを含む計測データを記憶する計測データ記憶手段と

を具備し、

前記認証装置が、

前記計測データ管理装置から前記計測データを取得する計測データ取得手段と、

前記計測データ取得手段により取得された計測データに含まれるタイムスタンプトークンを前記時刻認証局に送信することにより、当該タイムスタンプトークンに含まれるタイムスタンプの検証を当該時刻認証局に対して要求するタイムスタンプ検証要求手段と

を更に具備し、

前記時刻認証局が、

前記計測データ管理装置から取得した前記ハッシュ値に基づいて生成した前記タイムスタンプトークンを記憶するタイムスタンプトークン記憶手段と、

前記タイムスタンプトークン記憶手段により記憶されたタイムスタンプトークンに含まれるハッシュ値に基づいて、前記認証装置から取得したタイムスタンプトークンに含まれるタイムスタンプの検証を実行するタイムスタンプ検証手段と、

前記タイムスタンプ検証手段による検証の結果を前記認証装置に対して送信する検証結果送信手段と

を具備する、計測データ管理システム。

[請求項6]

前記計測データ管理装置が、

時刻認証局と共に計測データに含まれるタイムスタンプの検証を実

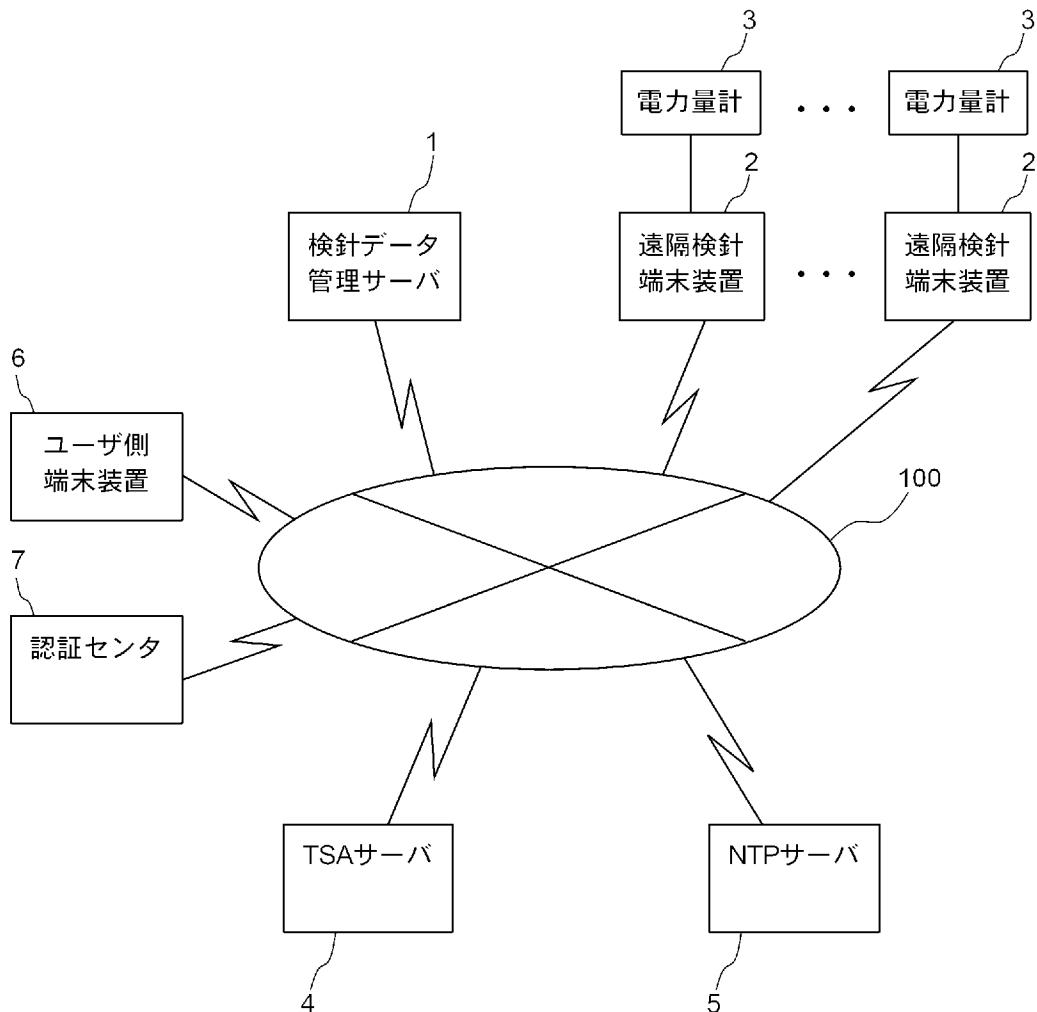
行する外部の装置に対して、前記計測データ記憶手段により記憶された計測データを送信する計測データ送信手段をさらに具備する、請求項 5 に記載の計測データ管理システム。

[請求項7] 前記電子署名手段が、外部の NTP サーバから前記計測日時を取得するように構成されている、請求項 5 又は 6 に記載の計測データ管理システム。

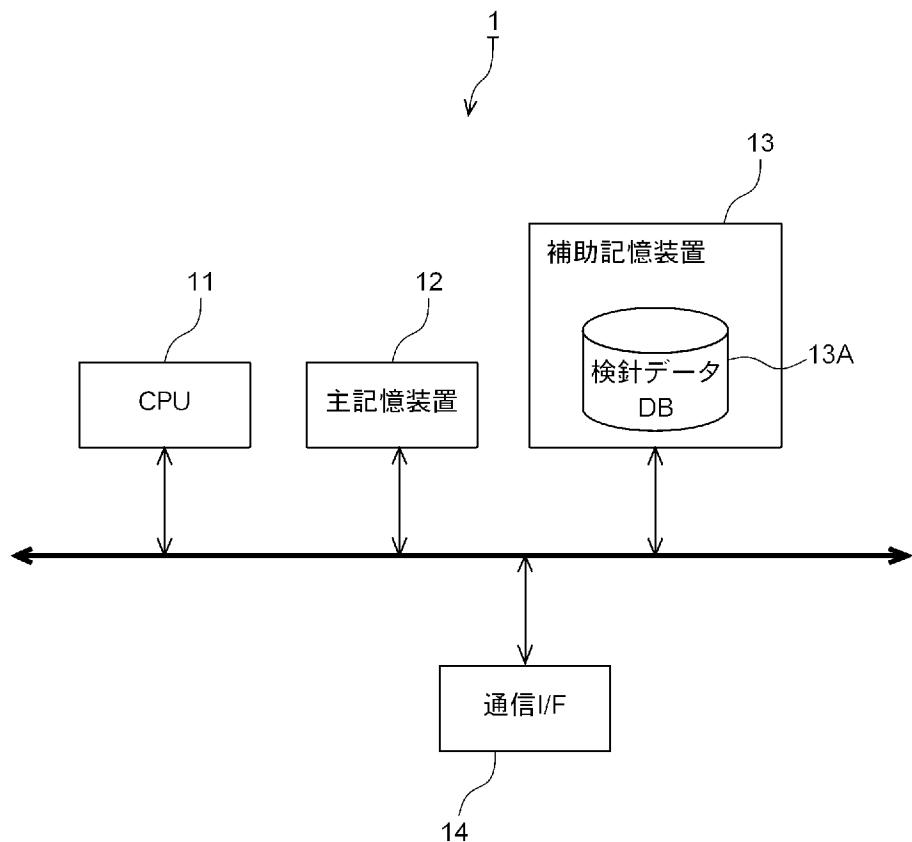
[請求項8] 前記端末装置が、  
前記計測器から前記計測値を複数回取得し、これにより得られた複数の前記計測値が一致するか否かを判定する判定手段をさらに具備し、

前記電子署名手段が、前記判定手段により複数の前記計測値が一致すると判定された場合に、前記電子署名データを生成するように構成されている、請求項 5 乃至 7 の何れかに記載の計測データ管理システム。

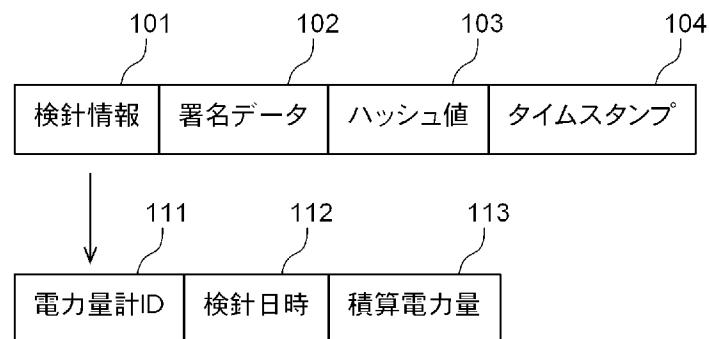
[図1]



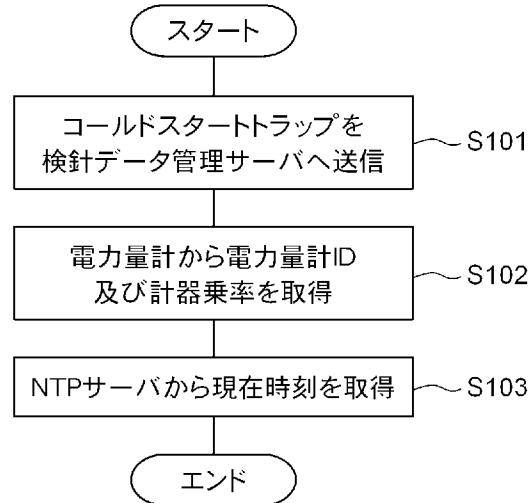
[図2]



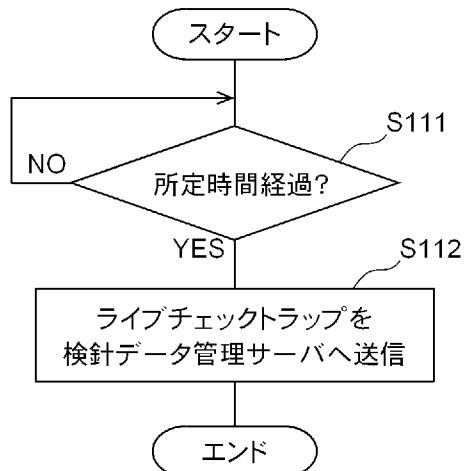
[図3]



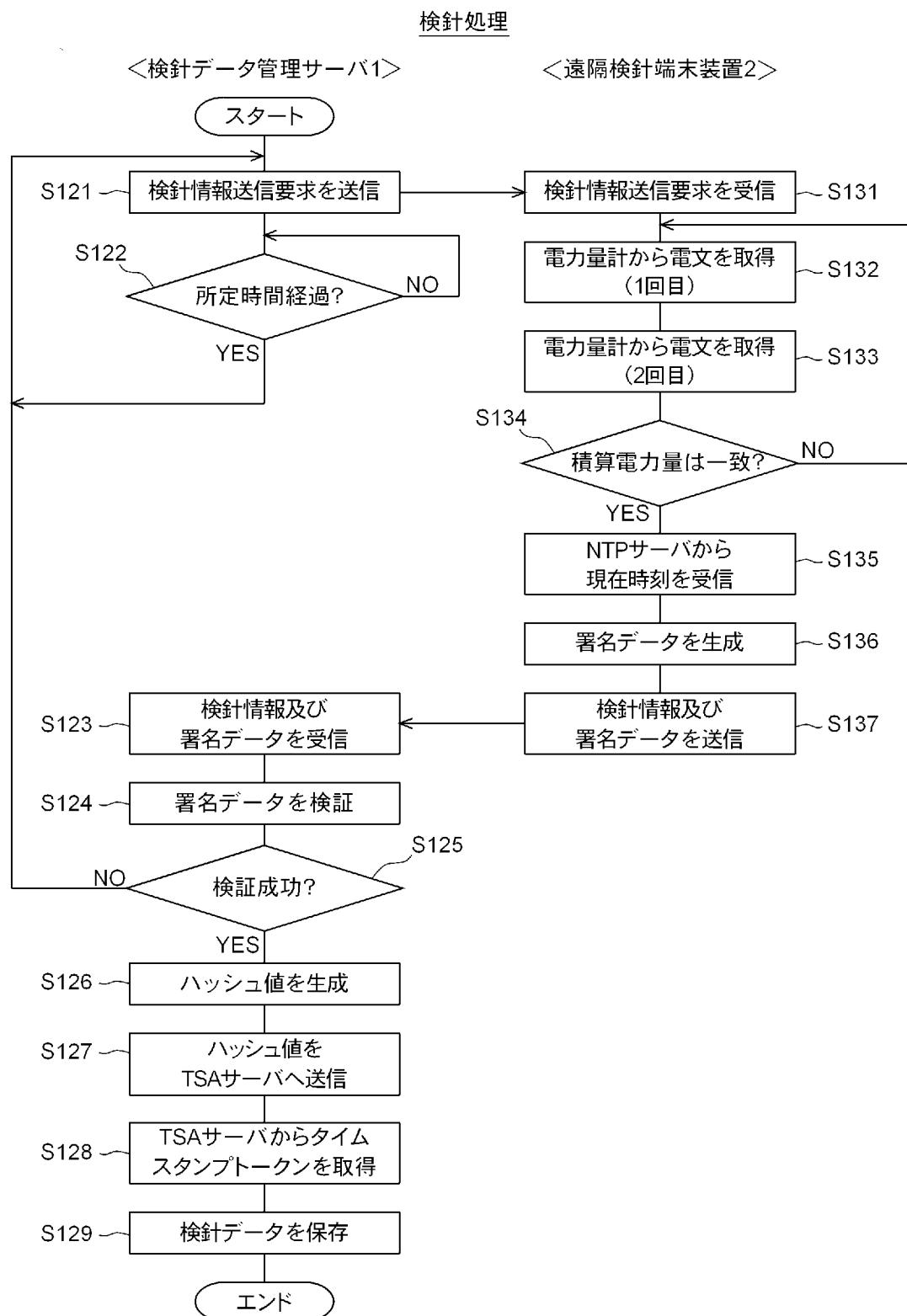
[図4]

遠隔検針端末装置起動処理

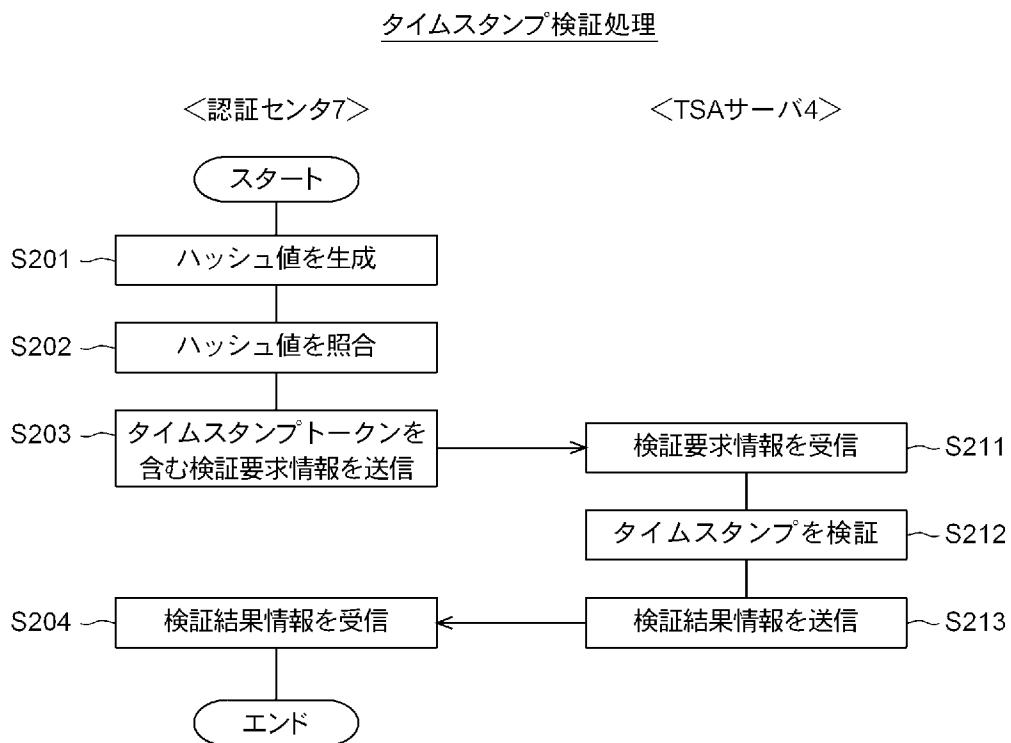
[図5]

遠隔検針端末装置ライブチェック処理

[図6]



[図7]



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/055917

### A. CLASSIFICATION OF SUBJECT MATTER

*H04L9/32(2006.01)i, G06F21/20(2006.01)i, G06F21/24(2006.01)i, G09C1/00(2006.01)i*

According to International Patent Classification (IPC) or to both national classification and IPC

### B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

*H04L9/32, G06F21/24*

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

<i>Jitsuyo Shinan Koho</i>	1922-1996	<i>Jitsuyo Shinan Toroku Koho</i>	1996-2011
<i>Kokai Jitsuyo Shinan Koho</i>	1971-2011	<i>Toroku Jitsuyo Shinan Koho</i>	1994-2011

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

### C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007-215104 A (Seiko Instruments Inc.), 23 August 2007 (23.08.2007), paragraphs [0139] to [0142], [0180] to [0186]; fig. 12, 15 to 17, 22 (Family: none)	1-8
A	JP 2007-306352 A (Seiko Instruments Inc.), 22 November 2007 (22.11.2007), paragraphs [0080] to [0084], [0093] to [0096]; fig. 12, 14 (Family: none)	1-8
A	JP 2003-323357 A (Hitachi, Ltd.), 14 November 2003 (14.11.2003), paragraphs [0045] to [0048], [0082] to [0084]; fig. 7, 12 & US 2003/0212828 A1 & EP 1361695 A2	2-4, 6-8

Further documents are listed in the continuation of Box C.

See patent family annex.

\* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
10 May, 2011 (10.05.11)

Date of mailing of the international search report  
17 May, 2011 (17.05.11)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2011/055917

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007-249559 A (Fujitsu Ltd.), 27 September 2007 (27.09.2007), paragraph [0032] (Family: none)	4, 8

## A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04L9/32(2006.01)i, G06F21/20(2006.01)i, G06F21/24(2006.01)i, G09C1/00(2006.01)i

## B. 調査を行った分野

## 調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. H04L9/32, G06F21/24

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2011年
日本国実用新案登録公報	1996-2011年
日本国登録実用新案公報	1994-2011年

## 国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2007-215104 A (セイコーインスツル株式会社) 2007.08.23, 段落[0139]-[0142], [0180]-[0186], 図12, 15-17, 22 (ファミリーなし)	1-8
A	JP 2007-306352 A (セイコーインスツル株式会社) 2007.11.22, 段落[0080]-[0084], [0093]-[0096], 図12, 14 (ファミリーなし)	1-8

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの  
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）  
 「O」口頭による開示、使用、展示等に言及する文献  
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

## の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
 「&」同一パテントファミリー文献

国際調査を完了した日  10.05.2011	国際調査報告の発送日  17.05.2011
国際調査機関の名称及びあて先 日本国特許庁（ISA/JP） 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 石田 信行 電話番号 03-3581-1101 内線 3546 5S 9469

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2003-323357 A (株式会社日立製作所) 2003.11.14, 段落[0045]-[0048], [0082]-[0084], 図7, 12 & US 2003/0212828 A1 & EP 1361695 A2	2-4, 6-8
A	JP 2007-249559 A (富士通株式会社) 2007.09.27, 段落[0032] (ファミリーなし)	4, 8