

(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
2016年3月24日(24.03.2016)



(10) 国際公開番号

WO 2016/042664 A1

(51) 国際特許分類:

H04L 9/08 (2006.01) H04L 9/32 (2006.01)

(21) 国際出願番号:

PCT/JP2014/074872

(22) 国際出願日:

2014年9月19日(19.09.2014)

(25) 国際出願の言語:

日本語

(26) 国際公開の言語:

日本語

(71) 出願人: 株式会社東芝 (KABUSHIKI KAISHA TOSHIBA) [JP/JP]; 〒1058001 東京都港区芝浦一丁目1番1号 Tokyo (JP).

(72) 発明者: 小椋 直樹(OGURA, Naoki); 〒1058001 東京都港区芝浦一丁目1番1号 株式会社東芝 知的財産室内 Tokyo (JP). 上林 達(KAMBAYASHI, Toru); 〒1058001 東京都港区芝浦一丁目1番1号 株式会社東芝 知的財産室内 Tokyo (JP). 花谷 嘉一(HANATANI, Yoshikazu); 〒1058001 東京都港区芝浦一丁目1番1号 株式会社東芝 知的財産室内 Tokyo (JP). 山田 孝裕(YAMADA, Takahiro); 〒1058001 東京都港区芝浦一丁目1番1号 株式会社東芝 知的財産室内

Tokyo (JP). 斎藤 健(SAITO, Takeshi); 〒1058001 東京都港区芝浦一丁目1番1号 株式会社東芝 知的財産室内 Tokyo (JP).

(74) 代理人: 特許業務法人酒井国際特許事務所 (SAKAI INTERNATIONAL PATENT OFFICE); 〒1000013 東京都千代田区霞が関3丁目8番1号 虎の門三井ビルディング Tokyo (JP).

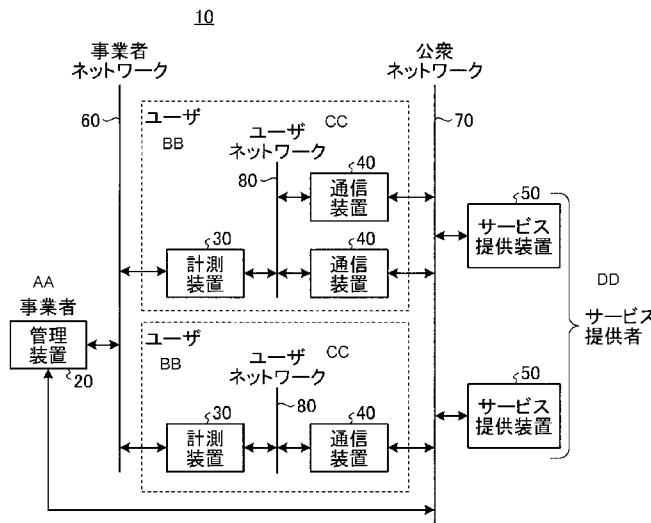
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG,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

(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, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユー

[続葉有]

(54) Title: MANAGING DEVICE, MEASURING DEVICE, SERVICE PROVIDING DEVICE, PROGRAM, TRANSMITTING SYSTEM AND TRANSMITTING METHOD

(54) 発明の名称: 管理装置、計測装置、サービス提供装置、プログラム、伝送システムおよび伝送方法



(57) Abstract: A managing device according to an embodiment is connected via a first network to a measuring device installed for each user. The managing device is also connected via a second network to a service providing device managed by a service provider. The managing device includes a class creating unit, a first key creating unit, a class transmitting unit, and user secret information transmitting unit. The class creating unit uses a service-providing-device identifier, which is stored therein and shared with the service providing device, to create class information. The first key creating unit uses the class information and a measuring device individual key, which is stored therein and shared with the measuring device, to create a user key. The class transmitting unit transmits the created class information to the measuring device via the first network. The user secret information transmitting unit transmits the created user key to the service providing device via the second network.

(57) 要約:

[続葉有]

- 20 Managing device
- 30 Measuring device
- 40 Communication device
- 50 Service providing device
- 60 Business operator network
- 70 Public network
- AA Business operator
- BB User
- CC User network
- DD Service provider



ラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨー 添付公開書類:

ロッパ (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, KM, ML, MR, NE, SN, TD, TG). — 国際調査報告（条約第 21 条(3)）

実施形態に係る管理装置は、ユーザ毎に設置される計測装置と第 1 ネットワークを介して接続される。管理装置は、サービス提供者により管理されるサービス提供装置と第 2 ネットワークを介して接続される。管理装置は、種生成部と、第 1 鍵生成部と、種送信部と、ユーザ秘密情報送信部とを備える。種生成部は、サービス提供装置と共有して記憶するサービス提供装置識別子を用いて、種情報を生成する。第 1 鍵生成部は、計測装置と共有して記憶する計測装置個別鍵および種情報を用いて、ユーザ鍵を生成する。種送信部は、生成された種情報を第 1 ネットワークを介して計測装置へと送信する。ユーザ秘密情報送信部は、生成されたユーザ鍵を第 2 ネットワークを介してサービス提供装置へと送信する。

明細書

発明の名称：

管理装置、計測装置、サービス提供装置、プログラム、伝送システムおよび伝送方法

技術分野

[0001] 本発明の実施形態は、管理装置、計測装置、サービス提供装置、プログラム、伝送システムおよび伝送方法に関する。

背景技術

[0002] 計測装置が計測した計測情報は、計測情報に関する情報処理サービスをユーザに提供する情報処理装置（サービス提供装置）に送信される。サービス提供装置は、受信した計測情報に基づき、情報処理を実行する。

先行技術文献

特許文献

[0003] 特許文献1：特開2012-213009号公報

発明の概要

発明が解決しようとする課題

[0004] 本発明が解決しようとする課題は、計測装置が計測した計測情報を、安全かつ簡易な処理でサービス提供装置に送信することにある。

課題を解決するための手段

[0005] 実施形態に係る管理装置は、ユーザ毎に設置される計測装置と第1ネットワークを介して接続される。前記管理装置は、サービス提供者により管理されるサービス提供装置と第2ネットワークを介して接続される。管理装置は、種生成部と、第1鍵生成部と、種送信部と、ユーザ秘密情報送信部とを備える。種生成部は、前記サービス提供装置と共有して記憶するサービス提供装置識別子を用いて、種情報を生成する。第1鍵生成部は、前記計測装置と共有して記憶する計測装置個別鍵および前記種情報を用いて、ユーザ鍵を生

成する。種送信部は、生成された前記種情報を前記第1ネットワークを介して前記計測装置へと送信する。ユーザ秘密情報送信部は、生成された前記ユーザ鍵を前記第2ネットワークを介して前記サービス提供装置へと送信する。

図面の簡単な説明

[0006] [図1]第1実施形態に係る伝送システムを示す図。

[図2]伝送システムの各部が記憶している情報を示す図。

[図3]第1実施形態に係る伝送システムの処理の流れを示す図。

[図4]第1実施形態に係る管理装置の構成図。

[図5]第1実施形態に係る計測装置の構成図。

[図6]第1実施形態に係るサービス提供装置の構成図。

[図7]種情報の生成のフロー図。

[図8]ユーザ鍵の生成のフロー図。

[図9]ユーザ鍵識別子の生成のフロー図。

[図10]証明情報の生成のフロー図。

[図11]検証処理のフロー図。

[図12]鍵無効化処理のフロー図。

[図13]第1実施形態の変形例に係る管理装置の構成図。

[図14]第2実施形態に係る伝送システムの処理の流れを示す図。

[図15]第2実施形態に係る管理装置の構成図。

[図16]第2実施形態に係る計測装置の構成図。

[図17]第2実施形態の鍵無効化処理のフロー図。

[図18]第3実施形態の更新処理のフロー図。

[図19]第3実施形態に係る計測装置の構成図。

[図20]第3実施形態に係るサービス提供装置の構成図。

[図21]第2の方法でのユーザ鍵の生成のフロー図。

[図22]第2の方法でのユーザ鍵識別子の生成のフロー図。

[図23]管理装置およびサービス提供装置のハードウェア構成図。

[図24]計測装置のハードウェア構成図。

発明を実施するための形態

[0007] 以下、図面を参照しながら実施形態に係る伝送システムについて詳細に説明する。本実施形態に係る伝送システムは、計測装置が計測した計測情報を、安全かつ簡易な処理でサービス提供装置に送信することができる。なお、以下、複数の実施形態および変形例を説明するが、先に説明した実施形態等の構成要素と略同一の機能の構成要素には図面中に同一の符号を付けて、重複した説明を省略する。

[0008] (第1実施形態)

図1は、第1実施形態に係る伝送システム10を示す図である。伝送システム10は、管理装置20と、1以上の計測装置30と、1以上の通信装置40と、1以上のサービス提供装置50とを備える。

[0009] 管理装置20およびそれぞれの計測装置30は、事業者ネットワーク60を介して接続される。サービス提供装置50およびそれぞれの通信装置40は、公衆ネットワーク70を介して接続される。計測装置30は、対応する通信装置40とユーザネットワーク80を介して接続される。サービス提供装置50および管理装置20は、公衆ネットワーク70を介して接続される。なお、サービス提供装置50および管理装置20は、公衆ネットワーク70とは異なるネットワーク（例えば専用のネットワーク）を介して接続されてもよい。また、サービス提供装置50および管理装置20は、一つの装置内に形成されていてもよい。

[0010] なお、図1では、伝送システム10が、2つの計測装置30、3つの通信装置40および2つのサービス提供装置50を備える例を示しているが、伝送システム10が備えるこれらの装置の数は限定されない。

[0011] 管理装置20は、事業者により管理される情報処理装置である。事業者は、電力の供給、ガスの供給、熱の供給、水の供給、または、汚水の排出等のサービスを、ユーザに対して提供する。ユーザは、事業者が電気の供給等のサービスを提供する対象であり、例えば家庭、会社、ビル等の建物、地域、

店舗または工場等である。ユーザは、例えば、代表者の氏名、電話番号、顧客番号またはサービス提供場所の住所等のユーザ情報により特定される。

- [0012] 計測装置30は、ユーザ毎に設置される情報処理装置である。計測装置30は、事業者からユーザに提供されるサービスの対象の物理量を表す計測情報を取得する。本実施形態においては、計測装置30は、ユーザが使用する機器毎の単位時間毎の電力使用量を計測する。なお、計測装置30は、ガスの使用量、熱使用量、水の使用量、または、汚水の排出量等を計測する装置であってもよい。計測装置30は、ユーザが事業者からのサービスの提供を受ける場所（家、会社、ビル等の建物、地域、店舗または工場等）に設置され、ユーザと一対一で対応付けられている。
- [0013] 事業者ネットワーク60は、事業者により管理されるネットワークである。事業者ネットワーク60は、一例として、複数の計測装置30を無線マルチホップ方式により接続した通信網、または、携帯電話通信網等であってよい。また、事業者ネットワーク60は、集線装置（コンセントレータ）を用いたPLC（電力線搬送通信）と広域通信網とにより形成される通信網であってもよい。事業者ネットワーク60は、事業者により管理されるので、管理装置20とそれぞれの計測装置30は、通信に必要な情報を共有することができ、相互認証処理、暗号化通信および完全性検証等を安全に実行することができる。
- [0014] 通信装置40は、それぞれのユーザ毎に設置される。通信装置40は、計測装置30により計測された計測情報をユーザネットワーク80を介して取得する。通信装置40は、一例として、計測装置30とユーザネットワーク80を介して接続されたホームゲートウェイである。また、通信装置40は、一例として、ブロードバンドルータ、スマートフォン等の携帯端末であってもよい。また、通信装置40は、計測装置30の終端器であるコンセントレータ、または、計測装置30に内蔵した装置であってもよい。なお、通信装置40は、コンセントレータまたは計測装置30に内蔵した装置の場合、ユーザネットワーク80を介さずに計測装置30に接続される。

- [0015] また、通信装置40は、ユーザが使用するデバイス（例えば、エアーコンディショナーおよびその他の電化製品等）とユーザネットワーク80を介して接続され、それぞれのデバイスによる、事業者から提供される対象の使用量（例えば、電力使用量）を計測情報として取得する。そして、通信装置40は、これらの情報に基づき、計測情報に示された情報の内訳を算出してユーザに提供してもよい。
- [0016] ユザネットワーク80は、計測装置30とそれぞれの通信装置40とをユーザ内で接続するためのネットワークであり、例えば家庭内に形成されたネットワークである。ユーザネットワーク80は、LAN (Local Area Network)、インターネットおよびイーサネット（登録商標）等である。ユーザネットワーク80は、ユーザにより管理されており、基本的には事業者およびサービス提供者等が直接管理しない。
- [0017] サービス提供装置50は、サービス提供者により管理される情報処理装置である。サービス提供者は、事業者が提供するサービスに関連する情報処理サービスを、サービス提供装置50を用いてユーザに提供する。サービス提供装置50は、例えば、事業者が供給したサービス対象に対する課金（例えば、電力使用量に対する課金）を情報処理により実行する。また、サービス提供装置50は、電力使用の抑制要求をユーザに発行し、その抑制要求に対する報酬の支払い（デマンドレスポンス処理）等の情報処理を実行する。
- [0018] それぞれのサービス提供装置50は、複数のユーザのグループ（例えば、ユーザの地域または契約の内容毎のグループ）毎に、同一の情報処理サービスを提供する。伝送システム10は、情報処理サービスの種類毎に異なるサービス提供装置50を備えてもよい。
- [0019] 公衆ネットワーク70は、不特定の者が利用できるネットワークである。例えば、公衆ネットワーク70は、インターネットまたはVPN (Virtual Private Network) 等である。公衆ネットワーク70は、事業者ネットワーク60と比較して、大量のデータを高速に低コストで伝送することが可能である。ただし、公衆ネットワーク70は、不特定の者が利用できるので、二

者間で秘密に通信をする場合には、相互認証処理および完全性検証等をしなければならない。サービス提供装置50は、公衆ネットワーク70を介して、管理装置20との間で相互認証処理および完全性検証等をすることが可能である。

[0020] 図2は、第1実施形態に係る伝送システム10の各部が記憶している情報を示す図である。

[0021] それぞれの計測装置30には、固有の識別情報である計測装置識別子SM-IDが割り当てられている。それぞれの計測装置30は、自己に割り当てられた計測装置識別子SM-IDを記憶する。計測装置識別子SM-IDの付加方法は、事業者が設定したポリシに依存する。なお、異なる計測装置30には、異なる計測装置識別子SM-IDが設定される。

[0022] また、それぞれの計測装置30は、管理装置20との間で、暗号化通信および相互認証等を行うための秘密鍵である計測装置個別鍵kSMを記憶する。それぞれの計測装置30は、計測装置個別鍵kSMを、回路の難読化または物理解析対策が施された耐タンパ性を有する記憶装置に記憶する。従って、悪意の第三者が計測装置30を解析して計測装置個別鍵kSMを取得することは困難である。また、計測装置個別鍵kSMは、例えば管理装置20により更新される。計測装置個別鍵kSMの更新頻度は、事業者が設定したポリシに依存し、例えば半年または数年等であってもよい。

[0023] それぞれのサービス提供装置50には、固有の識別情報であるサービス提供装置識別子AGGIDが割り当てられている。それぞれのサービス提供装置50は、自己に割り当てられたサービス提供装置識別子AGGIDを記憶する。

[0024] 管理装置20は、ユーザ毎に、ユーザ情報を記憶する。また、管理装置20は、ユーザ毎に、設置されている計測装置30の計測装置識別子SM-IDおよび計測装置個別鍵kSMを記憶する。なお、管理装置20は、計測装置識別子SM-IDおよび計測装置個別鍵kSMを悪意の第三者が入手できないように、秘匿して安全に管理する。また、管理装置20は、サービス提供装

置 50 毎に、割り当てられているサービス提供装置識別子 AGGID を記憶する。

[0025] すなわち、管理装置 20 およびそれぞれの計測装置 30 は、計測装置識別子 SMID および計測装置個別鍵 kSM を共有して記憶する。また、管理装置 20 およびそれぞれのサービス提供装置 50 は、サービス提供装置識別子 AGGID を共有して記憶する。

[0026] 図 3 は、第 1 実施形態に係る伝送システム 10 の情報処理の流れを示す図である。

[0027] まず、管理装置 20 は、情報処理サービスを提供するサービス提供装置 50 のサービス提供装置識別子 AGGID（第 1 の識別情報）を取得する（ステップ S11）。続いて、管理装置 20 は、サービス提供装置 50 が情報処理サービスを提供する対象であるユーザのユーザ情報を取得する（ステップ S12）。続いて、管理装置 20 は、取得したユーザ情報に対応付けて記憶している計測装置個別鍵 kSM（第 1 の鍵）および計測装置識別子 SMID（第 2 の識別情報）を読み出す（ステップ S13）。

[0028] 続いて、管理装置 20 は、取得したサービス提供装置識別子 AGGID および乱数 r から、種情報 s（第 1 の生成値）を生成する（ステップ S14）。なお、種情報 s の生成方法の具体例については詳細を後述する。

[0029] 続いて、管理装置 20 は、計測装置個別鍵 kSM および種情報 s から、ユーザ鍵 k u（第 2 の生成値）を生成する（ステップ S15）。なお、ユーザ鍵 k u の生成方法の具体例については詳細を後述する。

[0030] 続いて、管理装置 20 は、計測装置識別子 SMID および種情報 s から、ユーザ鍵識別子 UKID（第 3 の生成値）を生成する（ステップ S16）。なお、ユーザ鍵識別子 UKID の生成方法の具体例については詳細を後述する。

[0031] 続いて、管理装置 20 は、種情報 s を、事業者ネットワーク 60 を介して対応する計測装置 30 へと送信する（ステップ S17）。なお、管理装置 20 は、複数の計測装置 30 について並行に本処理を実行する場合には、複数

の計測装置30に対して同一の種情報sを、例えばマルチキャストにより一括して送信してもよい。

- [0032] 続いて、管理装置20は、ユーザ鍵ku、ユーザ鍵識別子UKIDおよびユーザ情報を、公衆ネットワーク70を介して対応するサービス提供装置50へと送信する（ステップS18）。この場合において、管理装置20は、ユーザ鍵ku、ユーザ鍵識別子UKIDおよびユーザ情報を暗号化通信等を用い、第三者に対して秘匿化してサービス提供装置50へと送信する。
- [0033] 続いて、計測装置30は、自身が記憶している計測装置個別鍵kSM、および、管理装置20から受信した種情報sから、ユーザ鍵kuを生成する（ステップS19）。ユーザ鍵kuの生成方法は、管理装置20のステップS15と同一である。
- [0034] 続いて、計測装置30は、自身が記憶している計測装置識別子SMID、および、管理装置20から受信した種情報sから、ユーザ鍵識別子UKIDを生成する（ステップS20）。ユーザ鍵識別子UKIDの生成方法は、管理装置20のステップS16と同一である。
- [0035] 続いて、計測装置30は、計測情報mを取得する（ステップS21）。計測装置30は、一例として、ユーザが使用する機器毎の単位時間毎の電力使用量を計測情報mとして取得する。
- [0036] 続いて、計測装置30は、シーケンス番号jを取得する（ステップS22）。なお、シーケンス番号jは、証明情報MACを生成する毎に、予め定められた初期値から予め定められた値ずつ（例えば1ずつ）増加または減少する値である。
- [0037] 続いて、計測装置30は、計測情報m、ユーザ鍵kuおよびシーケンス番号jに基づき、計測情報mの正当性を証明する証明情報MACを生成する（ステップS23）。計測装置30は、計測情報mが計測装置30により正当に生成され、計測情報mが改ざんされていないことを証明する情報である。なお、証明情報MACの生成方法の具体例については詳細を後述する。
- [0038] 続いて、計測装置30は、計測情報m、証明情報MAC、シーケンス番号

j およびユーザ鍵識別子UKIDを、通信装置40および公衆ネットワーク70を介して対応するサービス提供装置50へと送信する（ステップS24）。

[0039] 続いて、サービス提供装置50は、管理装置20から受信したユーザ鍵kuと、計測装置30から受信した計測情報m、シーケンス番号jおよび証明情報MACに基づき、計測情報mの正当性を検証する（ステップS25）。より具体的には、サービス提供装置50は、管理装置20から受信したユーザ鍵ku、計測装置30から受信した計測情報mおよびシーケンス番号jに基づき、検証用証明情報MAC'を生成する。そして、サービス提供装置50は、検証用証明情報MAC'と、計測装置30から受信した証明情報MACとが一致すれば、計測装置30から受信した計測情報mが正当であると判断する。

[0040] そして、サービス提供装置50は、正当であると判断された計測情報mを用いて、情報処理サービスを実行する（ステップS26）。サービス提供装置50は、単位時間毎の電力使用量に基づき、使用電力量の課金、または、例えばデマンドレスポンスのための情報処理を実行する。

[0041] このような伝送システム10において、計測装置30は、第三者に対して秘匿されたユーザ鍵kuにより、計測情報mの証明情報MACを生成する。これにより、計測装置30は、計測情報mの改ざんを防止することができる。また、サービス提供装置50は、ユーザ鍵kuを管理装置20から取得するので、計測装置30との間で相互認証処理等をしなくても、計測装置30と秘密鍵を共有でき、計測情報mの正当性を検証することができる。これにより、伝送システム10によれば、簡易に、計測情報mの改ざんを防止することができる。

[0042] また、計測装置30は、計測情報mを公衆ネットワーク70を介してサービス提供装置50へと送信する。これにより、伝送システム10によれば、通信路による制限を少なくて、大量の計測情報mを高速に計測装置30からサービス提供装置50へと伝送することができる。

- [0043] また、管理装置20は、複数の計測装置30へ、サービス提供装置50毎に生成された種情報sを送信する。従って、管理装置20は、計測装置30に依存しない1つのデータを複数の計測装置30に送信すればよいので、事業者ネットワーク60での通信負荷を軽減することができる。
- [0044] このように本実施形態に係る伝送システム10によれば、計測装置30が取得した計測情報mを、安全で簡易にサービス提供装置50へと送信することができる。
- [0045] 図4は、第1実施形態に係る管理装置20の構成を示す図である。管理装置20は、サービス情報記憶部210と、サービス情報取得部211と、ユーザ情報取得部212と、種生成部213と、第1計測情報記憶部214と、検索部215と、第1鍵生成部216と、第1鍵識別子生成部217と、種送信部218と、ユーザ秘密情報送信部219と、第1更新制御部220と、第1更新部221とを備える。
- [0046] サービス情報記憶部210は、それぞれのサービス提供装置50毎に、サービス提供装置識別子AGGIDを記憶する。これにより、サービス情報記憶部210は、サービス提供装置識別子AGGIDをサービス提供装置50と共有して記憶することができる。サービス情報取得部211は、サービスを提供するサービス提供装置50のサービス提供装置識別子AGGIDをサービス情報記憶部210から取得する。サービス情報取得部211は、サービス提供装置50から暗号化通信から取得したり、オペレータが入力したりすることにより、対応するサービス提供装置50の情報を取得してサービス提供装置識別子AGGIDを検索してもよい。あるいは、サービス情報取得部211は、オペレータまたは外部の装置からサービス提供装置識別子AGGIDを直接取得してもよい。また、サービス提供装置50毎に異なるサービス提供装置識別子AGGIDを管理装置20が生成してサービス情報記憶部210に記憶させてもよい。
- [0047] ユーザ情報取得部212は、サービス情報取得部211により取得されたサービス提供装置識別子AGGIDに対応するサービス提供装置50が、サ

ービスを提供する対象となるユーザのユーザ情報を取得する。ユーザ情報取得部212は、対応するサービス提供装置50から暗号化通信によりユーザ情報を取得してもよいし、オペレータがユーザ情報を入力してもよいし、対象のユーザ情報を予め記憶していてもよい。

- [0048] 種生成部213は、サービス情報取得部211により取得されたサービス提供装置識別子AGGIDおよび乱数rを用いて、種情報sを生成する。種生成部213は、一例として、下記の式(1)に示す演算により種情報sを生成する。

$$s = H1(AGGID, r) \quad \dots (1)$$

- [0049] 関数H1(x, y)は、xとyとを入力として、1つの値を生成する関数である。関数H1(x, y)は、xとyとを入力値とする一方向性関数であってよい。一方向性関数は、一例として、sha-1、md5、sha256またはsha3-256等である。また、関数H1(x, y)は、xを鍵、yをメッセージとして入力する鍵付きハッシュ関数であってよい。鍵付きハッシュ関数は、一例として、hmacまたはomac等である。また、関数H1(x, y)は、xとyとを連結したビット列を入力とする擬似乱数生成器であってよい。擬似乱数生成器は、一例として、Hash_DRBG、HMAC_DRBGまたはCTR-DRBG等である。

- [0050] 亂数rは、第三者が推測することが困難な値であればどのような値であってよい。乱数rは、一例として、接続された装置の物理的な振る舞いを計測する等して得られる物理乱数であってよい。また、乱数rは、一例として、「2012年1月1日」、「14:35:46, 1/1/2012」、または、UNIX(登録商標)時刻(1970年1月1日0時0分0秒(GMT))等から経過した秒数等の時刻情報であってよい。また、乱数rは、更新前に使用した種情報s、ユーザ鍵ku、ユーザ鍵識別子UKID、および、これらから得たビット列を連結して擬似乱数生成器に入力した出力結果であってよい。

- [0051] 種生成部213は、管理装置20が接続されている装置または通信I/F

を介して接続される装置から受信した情報を元に乱数 r を生成してもよい。本実施形態においては、種生成部 213 は、システム開始時点において外部から取得した時刻情報を擬似乱数生成器に入力して出力された値を、乱数 r として用いる。

- [0052] なお、種生成部 213 は、上述した方法によらず、種情報 s を乱数 r のみから生成してもよい。ただし、その場合には、種生成部 213 は、種情報 s を、サービス提供装置 50 毎に異なるように生成する必要がある。種生成部 213 は、例えば、種情報 s を生成する度に、異なるサービス提供装置 50 用の種情報 s と比較し、同じであることを検知した場合には、乱数を生成し直してもよい。
- [0053] 第 1 計測情報記憶部 214 は、ユーザ毎に、ユーザ情報、計測装置個別鍵 k_{SM} および計測装置識別子 $SMID$ の組を記憶する。これにより、第 1 計測情報記憶部 214 は、計測装置個別鍵 k_{SM} および計測装置識別子 $SMID$ を、計測装置 30 と共有して記憶することができる。
- [0054] 検索部 215 は、ユーザ情報取得部 212 により取得されたユーザ情報を受け取る。そして、検索部 215 は、第 1 計測情報記憶部 214 から、受け取ったユーザ情報と組みにされた計測装置個別鍵 k_{SM} および計測装置識別子 $SMID$ を読み出す。検索部 215 は、一例として、受け取ったユーザ情報の代表者の氏名および住所と、第 1 計測情報記憶部 214 に記憶されたユーザ情報の代表者の氏名および住所とを比較して、一致したユーザ情報に対応付けられた計測装置個別鍵 k_{SM} および計測装置識別子 $SMID$ を読み出す。
- [0055] 第 1 鍵生成部 216 は、検索部 215 により読み出された計測装置個別鍵 k_{SM} 、および、種生成部 213 により生成された種情報 s を用いて、ユーザ鍵 k_u を生成する。第 1 鍵生成部 216 は、一例として、下記の式（2）に示す演算によりユーザ鍵 k_u を生成する。

$$k_u = H2(k_{SM}, s) \quad \dots (2)$$

- [0056] 関数 $H2(x, y)$ は、 x と y とを入力として、1 つの値を生成する関数

である。関数H2(x, y)は、xとyとを入力値とする一方向性関数であつてよい。一方向性関数は、一例として、sha-1、md5、sha256またはsha3-256等である。また、関数H2(x, y)は、xを鍵、yをメッセージとして入力する鍵付きハッシュ関数であつてもよい。鍵付きハッシュ関数は、一例として、hmacまたはomac等である。

[0057] 第1鍵識別子生成部217は、検索部215により読み出された計測装置識別子SMID、および、種生成部213により生成された種情報sを用いて、ユーザ鍵識別子UKIDを生成する。第1鍵識別子生成部217は、一例として、下記の式(3)に示す演算によりユーザ鍵識別子UKIDを生成する。

$$\text{UKID} = \text{H3}(\text{SMID}, s) \quad \cdots (3)$$

[0058] 関数H3(x, y)は、xとyとを入力として、1つの値を生成する関数である。関数H3(x, y)は、xとyとを入力値とする一方向性関数であつてよい。一方向性関数は、一例として、sha-1、md5、sha256またはsha3-256等である。また、関数H3(x, y)は、xを鍵、yをメッセージとして入力する鍵付きハッシュ関数であつてもよい。鍵付きハッシュ関数は、一例として、hmacまたはomac等である。

[0059] 第1鍵識別子生成部217は、第1鍵生成部216がユーザ鍵kuを生成する毎に、対応するユーザ鍵識別子UKIDを生成する。すなわち、ユーザ鍵識別子UKIDは、ユーザ鍵ku毎に異なる値であり、ユーザ鍵kuを識別する情報として機能する。

[0060] なお、第1鍵識別子生成部217は、異なるユーザ鍵識別子UKIDを生成する場合に、同一の種情報sを用いてもよい。ただし、第1鍵識別子生成部217は、計測装置識別子SMID毎に、異なるユーザ鍵識別子UKIDを生成しなければならない。従って、関数H3(x, y)は、xを計測装置識別子SMIDの定義域に制限した場合に単射性を満たさなければならない。また、ユーザ鍵kuを生成する際に用いる種情報sとユーザ鍵識別子UKIDを生成する際に用いる種情報sは異なっていてもよい。その場合、種送

信部 218 では、ユーザ鍵用の種情報 s とユーザ鍵識別子用の種情報 s' を区別して計測装置 30 に送信する。

- [0061] もし、関数 $H_3(x, y)$ が単射性を満たさない場合には、管理装置 20 と計測装置 30との間で共有する予め定められたアルゴリズムで、計測装置識別子 $SIMID$ 每に異なるユーザ鍵識別子 $UKID$ を生成させてもよい。第 1 鍵識別子生成部 217 は、一例として、 $H_3(SIMID_1, s) = H_3(SIMID_2, s')$ を満たす $SIMID_1$ および $SIMID_2$ が存在した場合、種生成部 213 を呼び出す。そして、第 1 鍵識別子生成部 217 は、種生成部 213 に $H_3(SIMID_1, s') \neq H_3(SIMID_2, s')$ となる新たな種情報 s'' を生成させ、新たな種情報 s'' を用いてユーザ鍵識別子 $UKID$ を生成する。
- [0062] 種送信部 218 は、種生成部 213 により生成された種情報 s を事業者ネットワーク 60 を介して計測装置 30 へと送信する。この場合において、種送信部 218 は、複数の計測装置 30 に対して同一の種情報 s を、例えばマルチキャストにより一括して送信してもよい。これにより、種送信部 218 は、比較的に少ない通信負荷で種情報 s をそれぞれの計測装置 30 に送信することができる。また、種送信部 218 は、必要に応じて、他の情報を事業者ネットワーク 60 を介して計測装置 30 へと送信してもよい。種送信部 218 は、一例として、更新処理を指示するコマンドを計測装置 30 へと送信してもよい。
- [0063] ユーザ秘密情報送信部 219 は、第 1 鍵生成部 216 が生成したユーザ鍵 k_u 、第 1 鍵識別子生成部 217 が生成したユーザ鍵識別子 $UKID$ 、および、対応するユーザ情報を、公衆ネットワーク 70 を介して、対応するサービス提供装置 50 へと送信する。この場合において、ユーザ秘密情報送信部 219 は、ユーザ鍵 k_u 、ユーザ鍵識別子 $UKID$ およびユーザ情報を暗号化通信等を用いて、第三者に対して秘匿化してサービス提供装置 50 へと送信する。
- [0064] なお、ユーザ秘密情報送信部 219 は、サービス提供装置 50 によりユー

ザが特定可能であれば、ユーザ情報の一部のみを送信してもよいし、ユーザ情報以外の識別情報を送信してもよい。ユーザ情報以外の識別情報を送信する場合、ユーザ情報取得部212が、サービス提供装置50から予め識別情報とユーザとの対応関係を示す情報を受信していてもよいし、ユーザ情報取得部212が、識別情報とユーザとの対応関係を示す情報を生成して、予めサービス提供装置50に送信しておいてもよい。

- [0065] また、ユーザ秘密情報送信部219は、複数のユーザに対して並行に処理を実行する場合には、ユーザ鍵k_u、ユーザ鍵識別子UKIDおよびユーザ情報の組を格納した表データをサービス提供装置50に送信してもよい。また、ユーザ秘密情報送信部219は、送信された情報からサービス提供装置50がユーザを特定できる形式であれば、ユーザ情報または識別情報を送信しなくてもよい。例えば、ユーザ秘密情報送信部219は、ユーザ鍵k_uおよびユーザ鍵識別子UKIDの組を、ユーザ情報のうちの代表者の氏名等を辞書式に並べ替た順序で格納した表データを送信してもよい。
- [0066] また、ユーザ秘密情報送信部219は、必要に応じて、他の情報を公衆ネットワーク70を介してサービス提供装置50に送信してもよい。ユーザ秘密情報送信部219は、一例として、更新処理を指示するコマンドをサービス提供装置50に送信してもよい。
- [0067] 第1更新制御部220は、ユーザ鍵k_uを更新する必要が生じたか否かを判断する。第1更新制御部220は、一例として、最後に更新してから一定の時間が経過した場合、または、予め定められたイベントが発生した場合等にユーザ鍵k_uを更新する必要が生じたと判断する。さらに、具体的には、例えば、第1更新制御部220は、計測装置30の証明情報MACの生成で用いられるシーケンス番号jのオーバーフローが発生した場合、ユーザ鍵k_uについて事前に設定された有効期限が終了した場合、ユーザ鍵k_uの鍵無効化の要求を受けた場合、または、計測装置個別鍵k_{SM}が更新された場合等に、ユーザ鍵k_uを更新する必要が生じたと判断する。
- [0068] 第1更新制御部220は、ユーザ鍵k_uを更新する必要が生じた場合には

、第1更新部221に通知する。本実施形態においては、第1更新制御部220は、ユーザ鍵k_uを更新する必要が生じていない場合には、第1更新部221に対して、値が0の更新通知フラグを出力し、それ以外の場合には、第1更新部221に対して、値が1の更新通知フラグを出力する。さらに、第1更新制御部220は、第1更新部221が複数の方法でユーザ鍵k_uを更新することができる場合には、更新方法を決定し、第1更新部221に更新方法を通知してもよい。

[0069] 第1更新部221は、第1更新制御部220からユーザ鍵k_uの更新の通知を受けた場合（例えば、値が1の更新通知フラグを受け取った場合）、種生成部213、第1鍵生成部216および第1鍵識別子生成部217を呼び出す。そして、第1更新部221は、種生成部213に種情報sを更新させ、第1鍵生成部216にユーザ鍵k_uを更新させ、第1鍵識別子生成部217にユーザ鍵識別子UKIDを更新させる。

[0070] 更新する場合、種生成部213は、サービス提供装置識別子AGGIDを用いて新たな種情報sを生成する。また、第1鍵生成部216は、計測装置個別鍵kSMおよび新たな種情報sを用いて、新たなユーザ鍵k_uを生成する。また、第1鍵識別子生成部217は、計測装置識別子SMIDおよび新たな種情報sを用いて、新たなユーザ鍵識別子UKIDを生成する。

[0071] そして、種送信部218は、新たな種情報sを事業者ネットワーク60を介して計測装置30へと送信する。この場合、種送信部218は、更新を指示するコマンドを計測装置30へと送信してもよい。

[0072] また、ユーザ秘密情報送信部219は、新たなユーザ鍵k_u、新たなユーザ鍵識別子UKID、および、対応するユーザ情報を、公衆ネットワーク70を介して、対応するサービス提供装置50へと送信する。この場合、ユーザ秘密情報送信部219は、更新を指示するコマンドをサービス提供装置50へと送信してもよい。

[0073] 図5は、第1実施形態に係る計測装置30の構成を示す図である。計測装置30は、種受信部311と、第2計測情報記憶部312と、第2鍵生成部

313と、第2鍵識別子生成部314と、第1ユーザ情報記憶部315と、初期値生成部316と、第1シーケンス番号記憶部317と、計測部318と、証明部319と、計測情報送信部320と、第2更新制御部321と、第2更新部322とを備える。

- [0074] 種受信部311は、種情報sを事業者ネットワーク60を介して管理装置20から受信する。第2計測情報記憶部312は、当該計測装置30の計測装置個別鍵kSMおよび計測装置識別子SMIDを記憶する。
- [0075] 第2鍵生成部313は、第2計測情報記憶部312に記憶された計測装置個別鍵kSM、および、種受信部311により受信された種情報sを用いて、ユーザ鍵kuを生成する。第2鍵生成部313は、管理装置20の第1鍵生成部216が出力する結果と同一の結果が得られる方法によりユーザ鍵kuを生成する。第2鍵生成部313は、第1鍵生成部216と同一の処理を実行してもよいし、高速化処理を実行してもよい。
- [0076] 第2鍵識別子生成部314は、第2計測情報記憶部312に記憶された計測装置識別子SMID、および、種受信部311により受信された種情報sを用いて、ユーザ鍵識別子UKIDを生成する。第2鍵識別子生成部314は、管理装置20の第1鍵識別子生成部217が出力する結果と同一の結果が得られる方法によりユーザ鍵識別子UKIDを生成する。第2鍵識別子生成部314は、第1鍵識別子生成部217と同一の処理を実行してもよいし、高速化処理を実行してもよい。
- [0077] 第1ユーザ情報記憶部315は、第2鍵生成部313が生成したユーザ鍵kuおよび第2鍵識別子生成部314が生成したユーザ鍵識別子UKIDを記憶する。
- [0078] 初期値生成部316は、ユーザ鍵kuが更新された場合、証明情報MACを生成するために用いられるシーケンス番号jの初期値を生成する。初期値生成部316は、一例として、j=0またはj=1とした初期値を生成してもよい。また、初期値生成部316は、取扱い可能な値の最大値を初期値としてもよいし、乱数を初期値としてもよい。

[0079] 第1シーケンス番号記憶部317は、証明情報MACを生成するために用いられるシーケンス番号jの現在の値を記憶する。

[0080] 計測部318は、事業者からユーザに提供されるサービスの対象の物理量を表す計測情報mを取得する。本実施形態においては、計測部318は、ユーザが使用する機器毎の電力使用量を計測情報mとして取得する。計測部318は、一定の単位時間毎の電力使用量を収集してもよいし、通信装置40から収集の要求を受けた時に電力使用量を収集してもよいし、管理装置20から計測指示のコマンドを受け取った場合に電力使用量を収集してもよい。また、計測部318は、管理装置20からのコマンドに応じて、電力使用量の収集の開始および終了をしてよい。

[0081] 証明部319は、計測部318により取得された計測情報m、第1ユーザ情報記憶部315に記憶されたユーザ鍵ku、および、第1シーケンス番号記憶部317に記憶されたシーケンス番号jを用いて、計測情報mの正当性を証明する証明情報MACを生成する。証明部319は、一例として、下記の式(4)に示す演算により証明情報MACを生成する。

$$MAC = H4(ku, m, j) \dots (4)$$

[0082] 関数H4(x, y, z)は、xとyとzを入力として、1つの値を生成する関数である。関数H4(x, y, z)は、xとyとzを入力値とする一方向性関数であってよい。一方向性関数は、一例として、sha-1、md5、sha256またはsha3-256等である。また、関数H4(x, y, z)は、xを鍵、yとzとを連結したメッセージとして入力する鍵付きハッシュ関数であってもよい。鍵付きハッシュ関数は、一例として、hmacまたはomac等である。

[0083] また、証明部319は、証明情報MACを生成する毎に、第1シーケンス番号記憶部317に記憶されているシーケンス番号jを更新する。シーケンス番号jは、証明情報MACを生成する毎に値が増加（または減少する）番号であり、例えば、証明情報MACを生成する毎に1ずつ増加する値であっても、1ずつ減少する値であってもよい。また、第1シーケンス番号記憶部

317が過去に使用したシーケンス番号jを全て記憶しておき、証明部319が、過去に使用したシーケンス番号jとは異なる任意の値をシーケンス番号jとして生成してもよい。また、証明部319は、今回の更新により、次回あるいは回数を決定するアルゴリズムによって決定された一定回数以降でシーケンス番号jが更新できない場合（例えば、オーバーフローすることを検知した場合）、更新できることを示すフラグを管理装置20に送信してもよい。

- [0084] なお、証明部319は、証明情報MACを生成する場合に、第2鍵生成部313および第2鍵識別子生成部314を呼び出して、ユーザ鍵kuおよびユーザ鍵識別子UKIDを生成させてもよい。この場合、計測装置30は、第1ユーザ情報記憶部315を備えない構成であってよい。
- [0085] 計測情報送信部320は、計測情報m、証明情報MAC、シーケンス番号jおよびユーザ鍵識別子UKIDを、通信装置40に渡す。通信装置40は、計測装置30から受け取った計測情報m、証明情報MAC、シーケンス番号jおよびユーザ鍵識別子UKIDを、公衆ネットワーク70を介してサービス提供装置50へと送信する。
- [0086] なお、計測情報送信部320は、必要に応じて、他の情報を通信装置40および公衆ネットワーク70を介して、サービス提供装置50へと送信してもよい。例えば、計測情報送信部320は、ユーザ鍵kuが更新された直後において、計測情報m等とともに更新直後を示すコマンドをサービス提供装置50へと送信してもよい。
- [0087] 第2更新制御部321は、ユーザ鍵kuを更新する必要が生じたか否かを判断する。本実施形態においては、第2更新制御部321は、種受信部311が種情報sを受信した場合、ユーザ鍵kuを更新する必要が生じたと判断する。また、第2更新制御部321は、計測装置30が保存している情報を用いて更新の必要性を判断してもよい。例えば、第1シーケンス番号記憶部317に記憶されている現在のシーケンス番号jが、次回または予め決められたアルゴリズムにより決定された一定回数を越えるとオーバーフローする

ことが判明した場合のみ、第2更新制御部321は、更新する必要が生じたと判断してもよい。あるいは、第2更新制御部321は、計測装置30が接続されている装置または通信I/Fを介して接続される装置から受信した任意の情報を用いて更新の必要性を判断してもよい。

- [0088] 第2更新制御部321は、ユーザ鍵k_uを更新する必要が生じた場合には、第2更新部322に通知する。本実施形態においては、第2更新制御部321は、ユーザ鍵k_uを更新する必要が生じていない場合には、第2更新部322に対して、値が0の更新通知フラグを出力し、それ以外の場合には、第2更新部322に対して、値が1の更新通知フラグを出力する。さらに、第2更新制御部321は、第2更新部322が複数の方法でユーザ鍵k_uを更新することができる場合には、更新方法を決定し、第2更新部322に更新方法を通知してもよい。
- [0089] 第2更新部322は、第2更新制御部321からユーザ鍵k_uの更新の通知を受けた場合（例えば、値が1の更新通知フラグを受け取った場合）、第2鍵生成部313および第2鍵識別子生成部314を呼び出す。そして、第2更新部322は、第2鍵生成部313にユーザ鍵k_uを更新させ、第2鍵識別子生成部314にユーザ鍵識別子UKIDを更新させる。
- [0090] 更新する場合、第2鍵生成部313は、計測装置個別鍵kSM、および、受信した新たな種情報sを用いて、新たなユーザ鍵k_uを生成する。また、第2鍵識別子生成部314は、計測装置識別子SMID、および、受信した新たな種情報sを用いて、新たなユーザ鍵識別子UKIDを生成する。
- [0091] さらに、第2更新部322は、第1シーケンス番号記憶部317に記憶されている現在のシーケンス番号jを破棄して、初期値生成部316を呼び出してシーケンス番号jの初期値を生成させる。そして、この場合、初期値生成部316は、生成した初期値を第1シーケンス番号記憶部317に記憶させる。
- [0092] 図6は、第1実施形態に係るサービス提供装置50の構成を示す図である。サービス提供装置50は、ユーザ秘密情報受信部511と、第2ユーザ情

報記憶部512と、鍵有効化制御部513と、鍵有効化部514と、更新情報付加部515と、計測情報受信部516と、第2シーケンス番号記憶部517と、検証部518と、計測情報記憶部519と、サービス実行部520と、鍵無効化制御部521と、鍵無効化部522とを備える。

- [0093] ユーザ秘密情報受信部511は、ユーザ鍵k_u、ユーザ鍵識別子UKIDおよびユーザ情報を、管理装置20から公衆ネットワーク70を介して受信する。この場合において、ユーザ秘密情報受信部511は、ユーザ鍵k_u、ユーザ鍵識別子UKIDおよびユーザ情報を暗号化通信等により、第三者に対して秘匿化して受信する。
- [0094] 第2ユーザ情報記憶部512は、当該サービス提供装置50が情報処理サービスを提供するユーザ毎に、ユーザ秘密情報受信部511により受信され、更新情報付加部515により順序情報および使用フラグを付加された、ユーザ鍵k_uおよびユーザ鍵識別子UKIDを対応付けて記憶する。ここで、第2ユーザ情報記憶部512は、更新情報付加部515が新たなユーザ鍵k_uおよび新たなユーザ鍵識別子UKIDの組を記憶させる場合、既に記憶されているユーザ鍵k_uおよびユーザ鍵識別子UKIDの組を削除せずに残す。従って、第2ユーザ情報記憶部512は、1単位のユーザに対して、ユーザ鍵k_uとユーザ鍵識別子UKIDとの組を複数記憶している場合がある。
- [0095] 鍵有効化制御部513は、第2ユーザ情報記憶部512に記憶されたユーザ鍵k_uを更新する必要が生じたか否かを判断する。本実施形態においては、鍵有効化制御部513は、ユーザ秘密情報受信部511が、新たなユーザ鍵k_uを管理装置20から受信した場合、ユーザ鍵k_uを更新する必要が生じたと判断する。
- [0096] 鍵有効化制御部513は、ユーザ鍵k_uを更新する必要が生じた場合には、鍵有効化部514に通知する。本実施形態においては、鍵有効化制御部513は、ユーザ鍵k_uを更新する必要が生じていない場合には、鍵有効化部514に対して、値が0の更新通知フラグを出力し、それ以外の場合には、鍵有効化部514に対して、値が1の更新通知フラグを出力する。さらに、

鍵有効化制御部 513 は、鍵有効化部 514 が複数の方法でユーザ鍵 k_u を更新することができる場合には、更新方法を決定し、鍵有効化部 514 に更新方法を通知してもよい。

- [0097] 鍵有効化部 514 は、鍵有効化制御部 513 からユーザ鍵 k_u の更新の通知を受けた場合（例えば、値が 1 の更新通知フラグを受け取った場合）、更新情報付加部 515 を呼び出す。
- [0098] 更新情報付加部 515 は、鍵有効化部 514 により呼び出されると、更新に関する情報を付加した上で、第 2 ユーザ情報記憶部 512 に新たなユーザ鍵 k_u と新たなユーザ鍵識別子 UKID を書き込む。
- [0099] 更新情報付加部 515 は、ユーザ秘密情報受信部 511 が受信したユーザ鍵 k_u 、ユーザ鍵識別子 UKID およびユーザ情報を受け取る。ユーザ秘密情報受信部 511 がユーザ情報に代えて、ユーザを特定するための他の情報等が送信されてきた場合には、他の情報に基づきユーザを特定する。
- [0100] さらに、更新情報付加部 515 は、ユーザ秘密情報受信部 511 が受信した新たなユーザ鍵 k_u に対して、更新順序を識別可能な順序情報を付加する。順序情報は、一例として、そのユーザ鍵 k_u を管理装置 20 から受信した時刻を表す情報であってよい。順序情報は、一例として、受信した順序を表す数値であってよい。
- [0101] さらに、更新情報付加部 515 は、ユーザ秘密情報受信部 511 が受信した新たなユーザ鍵 k_u に、未使用であることを示す情報を付加する。本実施形態においては、受信した新たなユーザ鍵 k_u に、値が 0 の使用フラグを付加する。
- [0102] さらに、更新情報付加部 515 は、特定したユーザに対応させて、順序情報および使用フラグを付加したユーザ鍵 k_u およびユーザ鍵識別子 UKID を第 2 ユーザ情報記憶部 512 に書き込む。
- [0103] 計測情報受信部 516 は、計測情報 m 、証明情報 MAC、シーケンス番号 j およびユーザ鍵識別子 UKID を、通信装置 40 および公衆ネットワーク 70 を介して計測装置 30 から受信する。

- [0104] 第2シーケンス番号記憶部517は、ユーザ鍵識別子UKID毎に、計測情報受信部516が受信したシーケンス番号jを記憶する。なお、第2シーケンス番号記憶部517は、検証部518により計測情報mが正当であると判定された場合にシーケンス番号jを記憶し、正当でないと判定された場合にはシーケンス番号jを記憶しない。
- [0105] 検証部518は、計測情報受信部516が計測装置30から受信した計測情報mが正当であるかを検証する。すなわち、検証部518は、計測情報受信部516が計測装置30から受信した計測情報mが改ざんされていないかを検証する。
- [0106] 具体的には、検証部518は、第2ユーザ情報記憶部512に記憶されたユーザ鍵ku、計測情報受信部516が受信した計測情報m、および、計測情報受信部516が受信したシーケンス番号jを用いて、計測装置30の証明部319と同一の処理により、検証用証明情報MAC'を生成する。そして、検証部518は、生成した検証用証明情報MAC'と、計測装置30から受信した証明情報MACとを比較し、一致しなければ、計測情報mが正当ではないと判定する。
- [0107] 一致した場合、さらに、検証部518は、計測情報受信部516が受信したシーケンス番号jが、計測情報受信部516が受信したユーザ鍵識別子UKIDに対応付けて、第2シーケンス番号記憶部517に記憶されているかを判断する。受信したシーケンス番号jが、受信したユーザ鍵識別子UKIDに対応付けて記憶されている場合には、検証部518は、計測情報mが正当ではないと判定する。
- [0108] 検証用証明情報MAC'が受信した証明情報MACとが一致し、且つ、受信したシーケンス番号jが、受信したユーザ鍵識別子UKIDに対応付けて記憶されていない場合、検証部518は、受信した計測情報mが正当であると判断する。すなわち、この場合、検証部518は、受信した計測情報mが改ざんされていないと判断する。
- [0109] さらに、検証部518は、受信した計測情報mが正当であると判断した場

合、受信したシーケンス番号 j を、受信したユーザ鍵識別子 UKID に対応付けて第 2 シーケンス番号記憶部 517 に記憶させる。

- [0110] また、検証部 518 は、受信した計測情報 m が正当であると判断した場合、受信したユーザ鍵識別子 UKID に対応付けられたユーザ情報を、第 2 ユーザ情報記憶部 512 から検索する。そして、検証部 518 は、受信した計測情報 m を、検索して得られたユーザ情報に対応付けて計測情報記憶部 519 に記憶させる。
- [0111] また、検証部 518 は、受信した計測情報 m が正当であると判断した場合、受信したユーザ鍵識別子 UKID に対応付けられて第 2 ユーザ情報記憶部 512 に記憶されているユーザ鍵 k_u に、使用済みであることを示す情報を付加する。本実施形態においては、検証部 518 は、ユーザ鍵 k_u に対応付けられている使用フラグの値が 0 の場合には、使用フラグの値を 1 に書き換える。また、検証部 518 は、今回の更新により、次回あるいは回数を決定するアルゴリズムによって決定された一定回数以降で計測装置 30 がシーケンス番号が更新できない場合（例えば、オーバーフローすることを検知した場合）、更新できないことを示すフラグを管理装置 20 に送信してもよい。
- [0112] サービス実行部 520 は、計測情報記憶部 519 に記憶された正当であることが検証された計測情報 m を用いて、その計測情報 m を送信した計測装置 30 が設置されるユーザに対するサービス提供処理を実行する。サービス実行部 520 は、一例として、サービス提供装置 50 は、単位時間毎の電力使用量に基づき、使用電力量の課金、または、例えばデマンドレスポンスのための情報処理を実行する。
- [0113] 鍵無効化制御部 521 は、使用がされないユーザ鍵 k_u を削除する必要が生じたか否かを判断する。鍵無効化制御部 521 は、一例として、最後に削除してから一定の時間が経過した場合、または、予め定められたイベントが発生した場合等にユーザ鍵 k_u を削除する必要が生じたと判断する。さらに、具体的には、鍵無効化制御部 521 は、例えば、検証部 518 の検証処理において、計測装置 30 側のユーザ鍵 k_u の更新が確定した場合（例えば、

使用フラグの値が0から1に書き換えられた場合)、管理装置20から古いユーザ鍵k_uの削除を行う旨の信号を受信した場合、古いユーザ鍵が漏洩して不正に利用される恐れがある場合等に、ユーザ鍵k_uを削除する必要が生じたと判断する。また、鍵無効化制御部521は、使用フラグなどの情報を用いて計測装置30の更新失敗を検知する仕組みを備えててもよい。例えば、鍵無効化制御部521は、あるユーザ鍵k_uの使用フラグの値に0が付された後、一定時間経過した場合、計測装置30のユーザ鍵の更新が失敗したとみなし、管理装置20に更新が失敗した旨を通知してよい。

- [0114] 鍵無効化部522は、第2ユーザ情報記憶部512から、使用がされないユーザ鍵k_uおよびユーザ鍵識別子UKIDの組を削除する。さらに、鍵無効化部522は、第2シーケンス番号記憶部517から、使用がされないシーケンス番号jを削除する。
- [0115] 具体的には、鍵無効化部522は、ユーザ毎に、使用済みである情報が附加されているユーザ鍵k_u(本実施形態においては、使用フラグの値が1となっているユーザ鍵k_u)を取得し、取得したユーザ鍵k_uのうち順序情報(例えば時刻情報)が最新のユーザ鍵k_uを特定する。そして、鍵無効化部522は、特定された最新のユーザ鍵k_uを除いた、使用フラグの値が1となっているユーザ鍵k_uおよびユーザ鍵識別子UKIDの組を削除する。さらに、鍵無効化部522は、第2シーケンス番号記憶部517から、削除了ユーザ鍵識別子UKIDに対応付けて記憶されているシーケンス番号jを削除する。
- [0116] 図7は、種情報sの生成のフロー図である。管理装置20は、種情報sを生成する場合、図7のステップS101からステップS103の処理を実行する。
- [0117] まず、サービス情報取得部211は、サービス情報記憶部210からサービス提供装置識別子AGGIDを取得する(ステップS101)。続いて、種生成部213は、乱数rを取得する(ステップS102)。続いて、種生成部213は、サービス提供装置識別子AGGIDおよび乱数rを用いて、

H1 (AGGID, r) を演算して、種情報 s を生成する（ステップS103）。

[0118] 図8は、ユーザ鍵k_uの生成のフロー図である。管理装置20および計測装置30は、ユーザ鍵k_uを生成する場合、図8のステップS201からステップS203の処理を実行する。

[0119] まず、管理装置20のユーザ鍵k_uの生成処理について説明する。検索部215は、第1計測情報記憶部214から計測装置個別鍵k_{SM}を取得する（ステップS201）。続いて、第1鍵生成部216は、種生成部213で生成された種情報sを取得する（ステップS202）。続いて、第1鍵生成部216は、計測装置個別鍵k_{SM}および種情報sを用いて、H2 (k_{SM}, s) を演算して、ユーザ鍵k_uを生成する（ステップS203）。そして、ユーザ秘密情報送信部219は、生成したユーザ鍵k_uをサービス提供装置50へと送信する。

[0120] つぎに、計測装置30のユーザ鍵k_uの生成処理について説明する。第2鍵生成部313は、第2計測情報記憶部312から計測装置個別鍵k_{SM}を取得する（ステップS201）。続いて、第2鍵生成部313は、種受信部311が受信した種情報sを取得する（ステップS202）。続いて、第2鍵生成部313は、計測装置個別鍵k_{SM}および種情報sを用いて、H2 (k_{SM}, s) を演算して、ユーザ鍵k_uを生成する（ステップS203）。そして、第2鍵生成部313は、生成したユーザ鍵k_uを第1ユーザ情報記憶部315に記憶させる。

[0121] 図9は、ユーザ鍵識別子UKIDの生成のフロー図である。管理装置20および計測装置30は、ユーザ鍵識別子UKIDを生成する場合、図9のステップS301からステップS303の処理を実行する。

[0122] まず、管理装置20のユーザ鍵識別子UKIDの生成処理について説明する。検索部215は、第1計測情報記憶部214から計測装置識別子SMIDを取得する（ステップS301）。続いて、第1鍵識別子生成部217は、種生成部213で生成された種情報sを取得する（ステップS302）。

続いて、第1鍵識別子生成部217は、計測装置識別子SMIDおよび種情報sを用いて、H3(SMID, s)を演算して、ユーザ鍵識別子UKIDを生成する(ステップS303)。そして、ユーザ秘密情報送信部219は、生成したユーザ鍵識別子UKIDをサービス提供装置50へと送信する。

[0123] つぎに、計測装置30のユーザ鍵識別子UKIDの生成処理について説明する。第2鍵識別子生成部314は、第2計測情報記憶部312から計測装置識別子SMIDを取得する(ステップS301)。続いて、第2鍵識別子生成部314は、種受信部311が受信した種情報sを取得する(ステップS302)。続いて、第2鍵識別子生成部314は、計測装置識別子SMIDおよび種情報sを用いて、H3(SMID, s)を演算して、ユーザ鍵識別子UKIDを生成する(ステップS303)。そして、第2鍵識別子生成部314は、生成したユーザ鍵識別子UKIDを第1ユーザ情報記憶部315に記憶させる。

[0124] 図10は、証明情報MACの生成のフロー図である。計測装置30は、証明情報MACを生成する場合、図10のステップS401からステップS406の処理を実行する。

[0125] まず、証明部319は、第1ユーザ情報記憶部315からユーザ鍵kuを取得する(ステップS401)。続いて、証明部319は、計測部318から計測情報mを取得する(ステップS402)。続いて、証明部319は、第1シーケンス番号記憶部317からシーケンス番号jを取得する(ステップS403)。続いて、証明部319は、シーケンス番号jを更新する。本実施形態においては、証明部319は、シーケンス番号jに1を加算して新たなシーケンス番号jを生成する(ステップS404)。

[0126] 続いて、証明部319は、ユーザ鍵ku、計測情報mおよび新たなシーケンス番号jを用いて、H4(ku, m, j)を演算して、証明情報MACを生成する(ステップS405)。続いて、証明部319は、新たなシーケンス番号jを第1シーケンス番号記憶部317に記憶させる(ステップS406)。

- [0127] 図11は、検証処理のフロー図である。サービス提供装置50は、計測装置30から受信した計測情報mを検証する場合、図11のステップS501からステップS513の処理を実行する。
- [0128] まず、検証部518は、計測情報受信部516からユーザ鍵識別子UKIDを取得する（ステップS501）。続いて、検証部518は、第2ユーザ情報記憶部512から、取得したユーザ鍵識別子UKIDに対応付けられているユーザ鍵kuを取得する（ステップS502）。
- [0129] 続いて、検証部518は、計測情報受信部516から計測情報mを取得する（ステップS503）。続いて、検証部518は、計測情報受信部516からシーケンス番号jを取得する（ステップS504）。続いて、検証部518は、計測情報受信部516から証明情報MACを取得する（ステップS505）。
- [0130] 続いて、検証部518は、ユーザ鍵ku、計測情報mおよびシーケンス番号jを用いて、 $H4(ku, m, j)$ を演算して、検証用証明情報MAC'を生成する（ステップS506）。続いて、検証部518は、受信した証明情報MACと、生成した検証用証明情報MAC'が一致するか否かを判断する（ステップS507）。一致しない場合（ステップS507のNo）、検証部518は、検証は不合格（NG）であることを表す結果を出力して処理を終了する（ステップS513）。
- [0131] 一致する場合（ステップS507のYes）、検証部518は、第2シーケンス番号記憶部517から、受信したユーザ鍵識別子UKIDに対応して記憶された受信済みシーケンス番号j'を取得する（ステップS508）。続いて、検証部518は、受信したシーケンス番号jと、何れかの受信済みシーケンス番号j'が一致するか否かを判断する（ステップS509）。一致する場合（ステップS509のYes）、検証部518は、検証は不合格（NG）であることを表す結果を出力して処理を終了する（ステップS513）。
- [0132] 一致しない場合（ステップS509のNo）、検証部518は、検証は合

格（OK）であることを表す結果を出力する（ステップS510）。続いて、検証部518は、受信したシーケンス番号jを、受信済みシーケンス番号として第2シーケンス番号記憶部517に記憶させる（ステップS511）。そして、検証部518は、第2ユーザ情報記憶部512のユーザ鍵kuに対応して記憶された使用フラグの値を1とする（ステップS512）。

[0133] 図12は、第1実施形態に係るサービス提供装置50における鍵無効化処理のフロー図である。サービス提供装置50は、更新前に用いていたユーザ鍵ku等を鍵無効化する場合、図12のステップS601からステップS608の処理を実行する。

[0134] まず、鍵無効化部522は、第2ユーザ情報記憶部512に記憶されている、同一のユーザ情報に対応付いているユーザ鍵識別子UKIDのうち、使用フラグの値が1となっているユーザ鍵識別子UKID_1, …, UKID_nを全て取得する（ステップS601）。続いて、鍵無効化部522は、取得したユーザ鍵識別子UKID_1, …, UKID_nのそれぞれについて、更新時刻tID_1, …, tID_nを取得する（ステップS602）。続いて、鍵無効化部522は、取得した更新時刻tID_1, …, tID_nの中で、最新の更新時刻tを計算する（ステップS603）。

[0135] 続いて、鍵無効化部522は、変数iを1から1ずつ増やし、iがnに等しくなるまで、ステップS605からステップS607までの処理を繰り返す（ステップS604とステップS608との間のループ）。ループ内のステップS605においては、鍵無効化部522は、最新の更新時刻tと更新時刻tID_iとが一致するか否かを判断する。一致する場合（ステップS605のYes）、鍵無効化部522は、ステップS606およびステップS607の処理を行わず、iを次の値にする。一致しない場合（ステップS605のNo）、ステップS606において、鍵無効化部522は、第2ユーザ情報記憶部512から、ユーザ鍵ku_iおよびユーザ鍵識別子UKID_iを削除する。続いて、ステップS607において、鍵無効化部522は、第2シーケンス番号記憶部517から、ユーザ鍵識別子UKID_iに

対応する全ての受信済みシーケンス番号を削除する。

- [0136] 以上のように本実施形態に係る伝送システム10では、管理装置20がサービス提供装置50毎に種情報sを生成する。また、管理装置20が、計測装置30毎に、計測装置個別鍵kSMおよび種情報sを用いてユーザ鍵kuを生成し、計測装置識別子SMIDおよび種情報sを用いてユーザ鍵識別子UKIDを生成する。そして、管理装置20が、種情報sをそれぞれの計測装置30に送信し、ユーザ鍵kuおよびユーザ鍵識別子UKIDをサービス提供装置50に送信する。
- [0137] 一方、それぞれの計測装置30は、自身の計測装置個別鍵kSMおよび受信した種情報sを用いてユーザ鍵kuを生成し、自身の計測装置識別子SMIDおよび受信した種情報sを用いてユーザ鍵識別子UKIDを生成する。そして、それぞれの計測装置30は、ユーザ鍵kuにより計測情報mの証明情報MACを生成し、計測情報mと証明情報MACとユーザ鍵識別子UKIDとをサービス提供装置50に送信する。
- [0138] サービス提供装置50は、管理装置20からユーザ鍵kuおよびユーザ鍵識別子UKIDを受信する。サービス提供装置50は、計測装置30から計測情報mと証明情報MACとユーザ鍵識別子UKIDとを受信すると、管理装置20から受信したユーザ鍵識別子UKIDが同一のユーザ鍵kuを用いて、計測情報mの検証を行う。そして、サービス提供装置50は、検証の結果、計測情報mが正当であれば（改ざんされていなければ）、その計測情報mを用いて情報処理サービスを提供する。
- [0139] このように、伝送システム10によれば、サービス提供装置50と計測装置30との間で相互認証処理等をしなくても、秘密鍵を共有でき、計測情報mの正当性を検証することができる。これにより、伝送システム10によれば、簡易に、計測情報mの改ざんを防止することができる。
- [0140] また、伝送システム10では、計測情報mを公衆ネットワーク70を介してサービス提供装置50へと送信する。これにより、伝送システム10によれば、通信路による制限を少なくして、大量の計測情報mを高速に計測装置

30からサービス提供装置50へと伝送することができる。

[0141] また、伝送システム10では、管理装置20が複数の計測装置30へ種情報sを送信する。従って、管理装置20は、計測装置30に依存しない1つのデータを複数の計測装置30に送信することができるので、事業者ネットワーク60での通信負荷を軽減することができる。

[0142] 以上のように本実施形態に係る伝送システム10によれば、計測装置30が取得した計測情報mを、安全で簡易にサービス提供装置50へと送信することができる。

[0143] (変形例)

つぎに、第1実施形態の変形例について説明する。第1実施形態の変形例は、図1から図12を参照して説明した伝送システム10と略同一の機能および構成を有するので、略同一の構成要素に同一の符号を付けて、相違点を除き詳細な説明を省略する。

[0144] 図13は、第1実施形態の変形例に係る管理装置20の構成を示す図である。第1実施形態の変形例に係る管理装置20は、図4に示す管理装置20に加えて、更新タイミング情報生成部610をさらに備える。

[0145] 第1更新制御部220は、ユーザ鍵kuを更新する必要が生じた場合、例えば更新通知フラグの値を1にして、更新タイミング情報生成部610に通知する。更新タイミング情報生成部610は、第1更新制御部220から通知を受け取った場合（更新通知フラグの値が1とされた場合）、種情報sおよびユーザ鍵kuの更新タイミングを示す更新タイミング情報を生成する。

[0146] 更新タイミング情報には、一例として、更新を開始するタイミングを指定する開始情報、および、更新を完了するタイミングを指定する完了情報が含まれる。本例においては、開始情報は、更新を開始する時刻が示され、完了情報は、更新を完了する時刻が示される。これに代えて、開始情報および完了情報は、計測装置30およびサービス提供装置50との間で行われる特定の情報の送受信回数が示されてもよいし、計測装置30およびサービス提供装置50が接続可能な外部の機器から受信する値が示されてもよい。

- [0147] また、開始情報および完了情報の、一方または両方について、計測装置30およびサービス提供装置50が同一の値を共有できる方法で、計測装置30、サービス提供装置50それぞれが生成してもよい。その場合、管理装置20は、更新タイミング情報として、各装置が開始情報および完了情報の生成に必要な情報を生成する。例えば、計測装置30およびサービス提供装置50が事前に完了情報の生成に必要な開始情報からの差分の時間を固定値として保存しておき、第1更新制御部220が更新タイミング情報として開始情報のみを生成してもよい。
- [0148] 開始情報は、現在より未来のタイミングを指定する情報である。例えば、開始情報は、現在時刻より未来の時刻が示される。また、完了情報は、開始情報より未来のタイミングを指定する情報である。開始情報が時刻で示されている場合には、完了情報は、開始情報より未来の時刻が示される。また、完了情報は、開始情報からの差分の時間であってもよい。
- [0149] 更新タイミング情報生成部610は、更新タイミング情報を例えばサービス提供装置50または他の外部の機器から取得してもよい。また、更新タイミング情報生成部610は、更新タイミング情報を予め記憶した値を用いて生成してもよい。
- [0150] 更新タイミング情報生成部610は、生成した更新タイミング情報を種送信部218およびユーザ秘密情報送信部219に渡す。種送信部218は、更新後の種情報sとともに、更新タイミング情報を計測装置30へと送信する。また、ユーザ秘密情報送信部219は、更新後のユーザ鍵kuおよびユーザ鍵識別子UKIDとともに、更新タイミング情報をサービス提供装置50へと送信する。
- [0151] 一方、計測装置30の種受信部311は、管理装置20から、種情報sとともに更新タイミング情報を受信する。第2更新制御部321は、種受信部311が受信した更新タイミング情報に含まれる開始情報を参照して、ユーザ鍵kuを更新する必要が生じたか否かを判断する。例えば、第2更新制御部321は、現在時刻と、開始情報に示されている開始時刻とを比較し、現

在時刻が開始時刻以後であれば、ユーザ鍵 k_u を更新する必要が生じたと判断して、更新通知フラグの値を 1 とする。

[0152] 第 2 更新部 322 は、第 2 更新制御部 321 がユーザ鍵 k_u を更新する必要が生じたと判断した場合（更新通知フラグの値が 1 とされた場合）、第 2 鍵生成部 313 および第 2 鍵識別子生成部 314 を呼び出して、ユーザ鍵 k_u およびユーザ鍵識別子 UKID を更新させる。また、第 2 更新部 322 は、必要に応じて、種受信部 311 が受信した更新タイミング情報に含まれる完了情報を参照して、現在のタイミングが更新を完了する期限以内か否かを確認してもよい。例えば、第 2 更新部 322 は、現在時刻が、完了情報に示された完了時刻より前であるか否かを確認してもよい。そして、第 2 更新部 322 は、現在のタイミングが更新を完了する期限以内でない場合には、更新処理を中止し、ユーザ鍵 k_u の更新に失敗した旨を管理装置 20 に通知してもよい。あるいは、計測装置 30 は、完了確認や失敗通知を一切せず、サービス提供装置 50 に計測装置 30 における更新失敗を検出させるようにしてもよい。

[0153] また、サービス提供装置 50 のユーザ秘密情報受信部 511 は、管理装置 20 から、ユーザ鍵 k_u およびユーザ鍵識別子 UKID とともに、更新タイミング情報を受信する。鍵有効化制御部 513 は、ユーザ秘密情報受信部 511 が受信した更新タイミング情報に含まれる開始情報を参照して、ユーザ鍵 k_u を更新する必要が生じたか否かを判断する。例えば、鍵有効化制御部 513 は、現在時刻と、開始情報に示されている開始時刻とを比較し、現在時刻が開始時刻以後であれば、ユーザ鍵 k_u を更新する必要が生じたと判断して、更新通知フラグの値を 1 とする。

[0154] 鍵有効化部 514 は、鍵有効化制御部 513 がユーザ鍵 k_u を更新する必要が生じたと判断した場合（更新通知フラグの値が 1 とされた場合）、更新情報付加部 515 を呼び出して、更新に関するフラグを付加したユーザ鍵 k_u およびユーザ鍵識別子 UKID を更新させる。また、ユーザ秘密情報受信部 511 が受信した更新タイミング情報に含まれる完了情報を参照して、現

在のタイミングが更新を完了する期限以内か否かを確認する。例えば、鍵有効化部514は、現在時刻が、完了情報に示された完了時刻より前であるか否かを確認する。そして、鍵有効化部514は、現在のタイミングが更新を完了する期限以内でない場合には、更新処理を中止し、ユーザ鍵k_uの更新に失敗した旨を管理装置20に通知する。

- [0155] 鍵無効化制御部521は、ユーザ秘密情報受信部511が受信した更新タイミング情報に含まれる完了情報を参照して、使用がされないユーザ鍵k_uを削除する必要が生じたか否かを判断する。例えば、鍵無効化制御部521は、現在時刻と、完了情報に示されている完了時刻とを比較し、現在時刻が完了時刻以後であれば、使用がされないユーザ鍵k_uを削除する必要が生じたと判断する。
- [0156] また、鍵無効化制御部521は、更新タイミング情報を用いて計測装置30の更新失敗を検知する仕組みを備えてもよい。例えば、検証部518が使用フラグをユーザ鍵k_uに付すようにし、鍵無効化制御部521は、あるユーザ鍵k_uについて、使用フラグ=0かつ現在のタイミングが更新を完了する期限より後である場合、計測装置30のユーザ鍵の更新が失敗したとみなし、管理装置20に更新が失敗した旨を通知してよい。
- [0157] 鍵無効化部522は、ユーザ鍵k_uおよびユーザ鍵識別子UKIDの削除処理、および、使用済みのシーケンス番号jの削除処理をする場合、ユーザ秘密情報受信部511が受信した更新タイミング情報に含まれる完了情報を参照して、現在のタイミングが更新を完了する期限以内か否かを確認する。そして、鍵無効化部522は、現在のタイミングが更新を完了する期限より後である場合に、削除処理を実行する。
- [0158] また、鍵無効化部522は、使用フラグ=1を判定する代わりに、現在のタイミングが更新を完了する期限より後であるか否かを判定してもよい。さらに、鍵無効化部522は、順序情報の代わりに、更新タイミングを用いてもよい。鍵無効化部522が使用フラグや順序情報を用いない場合には、更新情報付加部515は、これらの情報の付加を省略してもよい。

[0159] 以上のような、第1実施形態の変形例に係る伝送システム10によれば、種情報s、ユーザ鍵k_uおよびユーザ鍵識別子UKIDの転送タイミングとは異なるタイミングで、計測装置30およびサービス提供装置50にユーザ鍵k_u等を更新させることができる。これにより、伝送システム10によれば、計測装置30の更新タイミングとサービス提供装置50の更新タイミングとを一致させることができる。

[0160] (第2実施形態)

つぎに、第2実施形態について説明する。第2実施形態は、図1から図13を参照して説明した第1実施形態に係る伝送システム10と略同一の機能および構成を有するので、略同一の構成要素に同一の符号を付けて、相違点を除き詳細な説明を省略する。

[0161] 第1実施形態においては、ユーザ鍵k_uを更新する毎に、ユーザ鍵k_uを識別する新たなユーザ鍵識別子UKIDを生成していた。第2実施形態においては、ユーザ鍵識別子UKIDに代えて、ユーザ鍵k_uが更新されても値が変わらないユーザ識別情報UIDを用いる。ユーザ識別情報UIDは、それぞれのユーザ毎に異なる値が割り当てられる。サービス提供装置50は、ユーザ識別情報UIDを記憶する。

[0162] 図14は、第2実施形態に係る伝送システム10の情報伝送の流れを示す図である。

[0163] まず、管理装置20は、情報処理サービスを提供するサービス提供装置50のサービス提供装置識別子AGGIDを取得する(ステップS31)。続いて、管理装置20は、サービス提供装置50が情報処理サービスを提供する対象のユーザのユーザ情報、および、ユーザ識別情報UIDを取得する(ステップS32)。続いて、管理装置20は、取得したユーザ情報に対応付けられている計測装置個別鍵kSMを読み出す(ステップS33)。

[0164] 続いて、管理装置20は、取得したサービス提供装置識別子AGGIDおよび乱数rから、種情報sを生成する(ステップS34)。続いて、管理装置20は、計測装置個別鍵kSMおよび種情報sから、ユーザ鍵k_uを生成

する（ステップS35）。なお、本実施形態においては、管理装置20は、ユーザ鍵識別子UKIDを生成しない。

[0165] 続いて、管理装置20は、種情報s、および、ユーザ識別情報UIDを、事業者ネットワーク60を介して対応する計測装置30へと送信する（ステップS36）。なお、管理装置20は、複数の計測装置30について並行に本処理を実行する場合には、複数の計測装置30に対して同一の種情報sおよびユーザ識別情報UIDを、例えばマルチキャストにより一括して送信してもよい。

[0166] 続いて、管理装置20は、ユーザ鍵ku、ユーザ識別情報UID、およびユーザ情報を、通信装置40および公衆ネットワーク70を介して、対応するサービス提供装置50へと送信する（ステップS37）。この場合において、管理装置20は、ユーザ鍵kuおよびユーザ情報を暗号化通信等を用いて第三者に対して秘匿化してサービス提供装置50へと送信する。

[0167] 続いて、計測装置30は、自身が記憶している計測装置個別鍵kSM、および、管理装置20から受信した種情報sから、ユーザ鍵kuを生成する（ステップS38）。なお、本実施形態においては、計測装置30は、ユーザ鍵識別子UKIDを生成しない。

[0168] 続いて、計測装置30は、種情報sとともに受信したユーザ識別情報UIDを取得する（ステップS39）。続いて、計測装置30は、ユーザ鍵kuの更新番号NIDを生成する（ステップS40）。更新番号NIDは、ユーザ識別情報UID毎のユーザ鍵kuの更新回数を識別する値である。例えば、更新番号NIDは、ユーザ鍵kuが更新される毎に、予め定められた初期値から予め定められた値ずつ（例えば1ずつ）増加または減少する値である。

[0169] 続いて、計測装置30は、計測情報mを取得する（ステップS41）。続いて、計測装置30は、シーケンス番号jを取得する（ステップS42）。続いて、計測装置30は、計測情報m、ユーザ鍵kuおよびシーケンス番号jに基づき、計測情報mの正当性を証明する証明情報MACを生成する（ス

ステップS43)。

- [0170] 続いて、計測装置30は、計測情報m、証明情報MAC、シーケンス番号j、ユーザ識別情報UIDおよび更新番号NIDを、通信装置40および公衆ネットワーク70を介して対応するサービス提供装置50へと送信する(ステップS44)。
- [0171] 続いて、サービス提供装置50は、管理装置20から受信したユーザ鍵kuと、計測装置30から受信した計測情報m、シーケンス番号jおよび証明情報MACに基づき、計測情報mの正当性を検証する(ステップS45)。そして、サービス提供装置50は、正当であると判断された計測情報mを用いて、情報処理サービスを実行する(ステップS46)。
- [0172] 図15は、第2実施形態に係る管理装置20の構成を示す図である。第2実施形態に係る管理装置20は、図4に示した第1実施形態に係る管理装置20と比較して、第1鍵識別子生成部217を備えない構成である。
- [0173] ユーザ情報取得部212は、サービスを提供する対象となるユーザのユーザ情報、および、ユーザ識別情報UIDを取得する。そして、ユーザ情報取得部212は、取得したユーザ識別情報UIDを種送信部218に渡す。また、ユーザ情報取得部212は、ユーザ識別情報UIDを受信する代わりに、管理装置20が生成してもよい。
- [0174] 検索部215は、第1計測情報記憶部214から、受け取ったユーザ情報と組みにされた計測装置個別鍵kSMを読み出す。なお、検索部215は、第1計測情報記憶部214から、計測装置識別子SMIDを読み出さない。
- [0175] 種送信部218は、種生成部213により生成された種情報s、および、ユーザ情報取得部212が取得したユーザ識別情報UIDを、事業者ネットワーク60を介して計測装置30へと送信する。ユーザ秘密情報送信部219は、第1鍵生成部216が生成したユーザ鍵ku、ユーザ情報取得部212が取得したユーザ識別情報UID、および、対応するユーザ情報を、公衆ネットワーク70を介して、対応するサービス提供装置50へと送信する。ただし、ユーザ秘密情報送信部219は、サービス提供装置50がユーザ情

報を用いてユーザ識別情報U I Dを取得できる場合は、ユーザ識別情報U I Dを送信しなくてもよい。なお、ユーザ秘密情報送信部219は、ユーザ鍵識別子U K I Dを送信しない。

[0176] 図16は、第2実施形態に係る計測装置30の構成を示す図である。第2実施形態に係る計測装置30は、図5に示した第1実施形態に係る計測装置30と比較して、第2鍵識別子生成部314を備えない構成である。

[0177] 種受信部311は、種情報sおよびユーザ識別情報U I Dを事業者ネットワーク60を介して管理装置20から受信する。第2更新部322は、第2鍵生成部313を呼び出してユーザ鍵k uを更新する場合、更新後のユーザ鍵k uの更新回数を表す更新番号N I Dを生成する。第1ユーザ情報記憶部315は、種受信部311が受信したユーザ識別情報U I Dに対応させて、第2鍵生成部313が生成したユーザ鍵k u、および、そのユーザ鍵k uの更新番号N I Dを記憶する。なお、本実施形態において、第1ユーザ情報記憶部315は、ユーザ鍵識別子U K I Dを記憶しない。

[0178] 証明部319は、計測部318により取得された計測情報m、第1ユーザ情報記憶部315に記憶されたユーザ鍵k uおよび第1シーケンス番号記憶部317に記憶されたシーケンス番号jを用いて、計測情報mの正当性を証明する証明情報M A Cを生成する。計測情報送信部320は、計測情報m、証明情報M A C、シーケンス番号j、ユーザ識別情報U I Dおよび更新番号N I Dを、通信装置40に渡す。通信装置40は、計測装置30から受け取った計測情報m、証明情報M A C、シーケンス番号j、ユーザ識別情報U I Dおよび更新番号N I Dを、公衆ネットワーク70を介してサービス提供装置50へと送信する。証明部319は、ユーザ鍵k uの更新状況に応じて、更新番号N I Dを送信するかどうかを判断してもよい。例えば、証明部319は、ユーザ鍵k uの更新後、初めて処理を実行する場合に、更新番号N I Dを送信し、それ以外の場合に、更新番号N I Dを送信しないようにしてもよい。

[0179] 第2実施形態に係るサービス提供装置50は、図6に示した第1実施形態

に係るサービス提供装置50と同一の構成となる。

- [0180] ユーザ秘密情報受信部511は、ユーザ情報およびユーザ鍵k_uに加え、ユーザ鍵識別子UKIDに代えて、ユーザ識別情報UIDを受信する。ただし、ユーザ秘密情報受信部511は、ユーザ識別情報UIDを受信する代わりに、ユーザ情報からユーザ識別情報UIDを検索してもよい。そして、更新情報付加部515は、ユーザに対応させて、ユーザ鍵k_uおよびユーザ識別情報UIDを第2ユーザ情報記憶部512に書き込む。第2ユーザ情報記憶部512は、ユーザ毎に、ユーザ情報と、ユーザ鍵k_uおよびユーザ識別情報UIDを対応付けて記憶する。なお、第2実施形態において、第2ユーザ情報記憶部512は、順序情報（時刻情報）を記憶しない。
- [0181] 計測情報受信部516は、計測情報m、証明情報MAC、シーケンス番号j、ユーザ識別情報UIDおよび更新番号NIDを、通信装置40および公衆ネットワーク70を介して計測装置30から受信する。第2シーケンス番号記憶部517は、ユーザ識別情報UIDおよび更新番号NID毎に、計測情報受信部516が受信したシーケンス番号jを全て記憶する。
- [0182] 検証部518は、第2ユーザ情報記憶部512から、受信したユーザ識別情報UIDおよび更新番号NIDが一致するユーザ鍵k_uを取得する。検証部518は、更新番号NIDが一致するユーザ鍵k_uを取得できなかつた場合、更新番号NIDが付加されていないユーザ鍵k_uを順次取得し、あるユーザ鍵k_uで受信した計測情報mが正当であると判断されるか、あるいは、全てのユーザ鍵k_uで受信した計測情報mが正当でないと判断されるまで検証処理を繰り返す。そして、検証部518は、取得したユーザ鍵k_u、計測情報受信部516が受信した計測情報m、および、計測情報受信部516が受信したシーケンス番号jを用いて、計測装置30の証明部319と同一の処理により、検証用証明情報MAC'を生成する。そして、検証部518は、生成した検証用証明情報MAC'と、計測装置30から受信した証明情報MACとを比較し、一致しなければ、計測情報mが正当ではないと判定する。

- [0183] 一致した場合、さらに、検証部518は、計測情報受信部516が受信したシーケンス番号jが、計測情報受信部516が受信したユーザ識別情報UIDおよび更新番号NIDに対応付けて、第2シーケンス番号記憶部517に記憶されているかを判断する。受信したシーケンス番号jが、受信したユーザ識別情報UIDおよび更新番号NIDに対応付けて記憶されている場合には、検証部518は、計測情報mが正当ではないと判定する。
- [0184] 検証用証明情報MAC'が受信した証明情報MACとが一致し、且つ、受信したシーケンス番号jが、受信したユーザ識別情報UIDおよび更新番号NIDに対応付けて記憶されていない場合、検証部518は、受信した計測情報mが正当であると判断する。
- [0185] さらに、検証部518は、受信した計測情報mが正当であると判断した場合、受信したシーケンス番号jを、受信したユーザ識別情報UIDおよび更新番号NIDに対応付けて第2シーケンス番号記憶部517に記憶させる。また、検証部518は、受信した計測情報mが正当であると判断し、検証に用いたユーザ鍵kuに更新番号が付加されていない場合、計測情報受信部516で受信した更新番号NIDをユーザ鍵kuに付加する。
- [0186] 図17は、第2実施形態に係るサービス提供装置50における鍵無効化処理のフロー図である。第2実施形態に係るサービス提供装置50は、更新前に用いていたユーザ鍵ku等を鍵無効化する場合、図17のステップS701からステップS708の処理を実行する。
- [0187] まず、鍵無効化部522は、第2ユーザ情報記憶部512に記憶されているユーザ識別情報UID毎に、更新番号NIDが付加されているユーザ鍵ku_1, ..., ku_nを全て取得する（ステップS701）。続いて、鍵無効化部522は、取得したユーザ鍵ku_1, ..., ku_nのそれぞれについて、更新番号NID_1, ..., NID_nを取得する（ステップS702）。続いて、鍵無効化部522は、取得した更新番号NID_1, ..., NID_nの中で、最新の更新番号NIDを計算する（ステップS703）。
- [0188] 続いて、鍵無効化部522は、iを1から1ずつ増やし、iがnに等しく

なるまで、ステップS705からステップS707までの処理を繰り返す（ステップS704とステップS708との間のループ）。ループ内のステップS705においては、鍵無効化部522は、最新更新番号NIDと更新番号NID_iとが一致するか否かを判断する。一致する場合（ステップS705のYes）、鍵無効化部522は、ステップS706およびステップS707の処理を行わず、iを次の値にする。一致しない場合（ステップS705のNo）、ステップS706において、鍵無効化部522は、第2ユーザ情報記憶部512から、ユーザ鍵ku_iを削除する。続いて、ステップS707において、鍵無効化部522は、第2シーケンス番号記憶部517から、更新番号NIDに対応する全ての受信済みシーケンス番号を削除する。

[0189] 以上のように第2実施形態に係る伝送システム10によれば、第1実施形態と同様に、計測装置30が取得した計測情報mを、安全で簡易にサービス提供装置50へと送信することができる。さらに、第2実施形態に係る伝送システム10は、ユーザ鍵識別子UKIDの更新をしなくてよいので、更新処理のコストを低くすることができる。

[0190] なお、第2実施形態に係る伝送システム10でも、第1実施形態の変形例と同様に、更新タイミング情報を生成して、計測装置30およびサービス提供装置50に指定されたタイミングでユーザ鍵kuを更新させてもよい。

[0191] また、本実施形態においては、更新番号NIDを計測装置30が送信して、サービス提供装置50が更新番号に応じて更新処理を実行する。これに代えて、計測装置30が更新を示すフラグをサービス提供装置50に送信し、サービス提供装置50が受信した更新を示すフラグを用いて、サービス提供装置50が記憶している更新番号NIDを修正し、修正を行った更新番号NIDに応じて更新処理を行うようにしてもよい。

[0192] (第3実施形態)

つぎに、第3実施形態について説明する。第3実施形態は、図1から図3を参照して説明した第1実施形態に係る伝送システム10と略同一の機能

および構成を有するので、略同一の構成要素に同一の符号を付けて、相違点を除き詳細な説明を省略する。

- [0193] 第3実施形態においては、ユーザ鍵 k_u およびユーザ鍵識別子UKIDの更新を、第1の方法または第2の方法の2つの何れかで実行する。第1の方法は、第1実施形態において実行した方法と同様である。第2の方法は、更新する直前のユーザ鍵 k_u （現在のユーザ鍵 k_u ）を用いて、更新後のユーザ鍵 k_u を生成する方法である。ユーザ鍵識別子UKIDについても同様である。
- [0194] また、第2の方法で更新する場合には、管理装置20は、更新後のユーザ鍵 k_u および更新後のユーザ鍵識別子UKIDをサービス提供装置50に送信するのではなく、更新後の種情報sをサービス提供装置50に送信する。これにより、管理装置20は、それぞれの計測装置30のユーザ鍵 k_u およびユーザ鍵識別子UKIDをサービス提供装置50に送信しなくてよいので、更新時における通信負担を軽減することができる。
- [0195] 図18は、第3実施形態に係る管理装置20における更新処理のフロー図である。第3実施形態に係る管理装置20は、ユーザ鍵 k_u の更新時において、図18のステップS901からステップS910の処理を実行する。
- [0196] まず、ステップS901において、第1更新制御部220は、ユーザ鍵 k_u の更新タイミングであるか否かを判断する。第1更新制御部220は、ユーザ鍵 k_u の更新タイミングではない場合には（S901のNo）、第1更新部221に更新タイミングではない旨の通知をし（例えば、値が0の更新通知フラグを出力し）、処理をステップS901で待機する。第1更新制御部220は、更新タイミングである場合には（S901のYes）、処理をステップS902に進める。
- [0197] ステップS902において、第1更新制御部220は、第1の方法での更新タイミングであるか、第2の方法での更新タイミングであるかを判断する。例えば、第1更新制御部220は、ユーザ鍵の漏洩が疑われる場合（例えば、ユーザ鍵 k_u の無効化要求時、計測装置個別鍵 k_{SM} の更新時など）は、更

新前のユーザ鍵 k_u (旧鍵)を用いないで更新を行うことが適切であるため、第1の方法での更新タイミングであると判断する。また、第1更新制御部220は、これら第1の方法での更新タイミングではない場合には、第2の方法での更新タイミングであると判断する。第1更新制御部220は、例えば、計測装置30において証明情報MACを生成するためのシーケンス番号 j がオーバーフローする場合、または、事前に設定されたユーザ鍵 k_u の有効期間の終了直前の場合等に、第2の方法での更新タイミングであると判断してもよい。

- [0198] 第1の方法での更新タイミングである場合（ステップS902のY_es）、第1更新制御部220は、第1更新部221に第1の方法での更新タイミングである旨の通知をし（例えば、値が1の更新通知フラグを出力し）、処理をステップS903に進める。第2の方法での更新タイミングである場合（ステップS902のN_o）、第1更新制御部220は、第1更新部221に第2の方法での更新タイミングである旨の通知をし（例えば、値が2の更新通知フラグを出力し）、処理をステップS908に進める。
- [0199] 第1の方法での更新タイミングであるとの通知を受けた場合、ステップS903において、第1更新部221は、種生成部213を呼び出して新たな種情報 s を生成させる。具体的には、第1更新部221は、サービス提供装置識別子AGGIDと新たな乱数 r とを用いて、 $H_1(AGGID, r)$ を演算して、新たな種情報 s を生成する。
- [0200] 続いて、ステップS904において、第1更新部221は、第1鍵生成部216を呼び出し、第1の方法で新たなユーザ鍵 k_u を生成させる。具体的には、第1鍵生成部216は、計測装置個別鍵 k_{SM} と新たな種情報 s とを用いて、 $H_2(k_{SM}, s)$ を演算して、新たなユーザ鍵 k_u を生成する。
- [0201] 続いて、ステップS905において、第1更新部221は、第1鍵識別子生成部217を呼び出し、第1の方法で新たなユーザ鍵識別子UKIDを生成させる。具体的には、第1鍵生成部216は、計測装置識別子SMIDと新たな種情報 s とを用いて、 $H_3(SMID, s)$ を演算して、新たなユー

ザ鍵識別子UKIDを生成する。

- [0202] 続いて、ステップS906において、種送信部218は、更新後の新たな種情報sと第1の方法で更新したことを示す更新方法情報を計測装置30へと送信する。続いて、ステップS907において、ユーザ秘密情報送信部219は、更新後の新たなユーザ鍵kuと新たなユーザ鍵識別子UKIDと更新方法情報を、サービス提供装置50へと送信する。
- [0203] 一方、第2の方法での更新タイミングであるとの通知を受けた場合、ステップS908において、第1更新部221は、種生成部213を呼び出して新たな種情報sを生成させる。具体的には、第1更新部221は、サービス提供装置識別子AGGIDと新たな乱数rとを用いて、H1(AGGID, r)を演算して、新たな種情報sを生成する。
- [0204] 続いて、ステップS909において、種送信部218は、更新後の新たな種情報sと第2の方法で更新したことを示す更新方法情報を計測装置30へと送信する。
- [0205] 続いて、ステップS910において、ユーザ秘密情報送信部219は、更新後の新たな種情報sと更新方法情報をサービス提供装置50へと送信する。なお、ユーザ秘密情報送信部219は、複数の計測装置30のユーザ鍵kuを更新する場合には、複数の計測装置30について1回で同一の種情報sを送信すればよい。
- [0206] 図19は、第3実施形態に係る計測装置30の構成を示す図である。第3実施形態に係る計測装置30は、図5に示す第1実施形態に係る計測装置30の構成に加えて、第3鍵生成部701と、第3鍵識別子生成部702とをさらに備える。
- [0207] 種受信部311は、管理装置20から、更新方法情報をさらに受信する。第2更新制御部321は、更新方法情報を参照して、第1の方法で更新するか、第2の方法で更新するか、更新をしないか、のいずれであるかを判断する。第2更新部322は、第2更新制御部321の判断に従い、第1の方法で更新する場合には、第2鍵生成部313および第2鍵識別子生成部314

を呼び出して、第1実施形態と同様の方法でユーザ鍵 k_u およびユーザ鍵識別子UKIDを更新する。第2更新部322は、第2の方法で更新する場合には、第3鍵生成部701および第3鍵識別子生成部702を呼び出す。

- [0208] 第3鍵生成部701は、第2更新部322が第2の方法で更新する際に呼び出される。第3鍵生成部701は、第2更新部322から呼び出された場合、第2の方法で新たなユーザ鍵 k_u を生成する。具体的には、第3鍵生成部701は、第1ユーザ情報記憶部315に記憶されている現在のユーザ鍵 k_u' と新たな種情報 s とを用いて、下記の式(5)に示す演算により、新たなユーザ鍵 k_u を生成する。

$$k_u = H5(k_u', s) \quad \dots (5)$$

- [0209] 関数 $H5(x, y)$ は、 x と y とを入力として、1つの値を生成する関数である。関数 $H5(x, y)$ は、 x と y とを入力値とする一方向性関数であってよい。一方向性関数は、一例として、sha-1、md5、sha256またはsha3-256等である。また、関数 $H5(x, y)$ は、 x を鍵、 y をメッセージとして入力する鍵付きハッシュ関数であってもよい。鍵付きハッシュ関数は、一例として、hmacまたはomac等である。

- [0210] 第3鍵識別子生成部702は、第2更新部322が第2の方法で更新する際に呼び出される。第3鍵識別子生成部702は、第2更新部322から呼び出された場合、第2の方法で新たなユーザ鍵識別子UKIDを生成する。具体的には、第3鍵識別子生成部702は、第1ユーザ情報記憶部315に記憶されている現在のユーザ鍵識別子UKID' と新たな種情報 s とを用いて、下記の式(6)に示す演算により、新たなユーザ鍵識別子UKIDを生成する。

$$UKID = H6(UKID', s) \quad \dots (6)$$

- [0211] 関数 $H6(x, y)$ は、 x と y とを入力として、1つの値を生成する関数である。関数 $H6(x, y)$ は、 x と y とを入力値とする一方向性関数であってよい。一方向性関数は、一例として、sha-1、md5、sha256またはsha3-256等である。また、関数 $H6(x, y)$ は、 x を鍵

、 y をメッセージとして入力する鍵付きハッシュ関数であってもよい。鍵付きハッシュ関数は、一例として、 $hmac$ または $omac$ 等である。

[0212] 図20は、第3実施形態に係るサービス提供装置50の構成を示す図である。第3実施形態に係るサービス提供装置50は、図6に示す第1実施形態に係るサービス提供装置50の構成に加えて、第4鍵生成部711と、第4鍵識別子生成部712とをさらに備える。

[0213] ユーザ秘密情報受信部511は、管理装置20から、種情報sおよび更新方法情報をさらに受信する。鍵有効化部514は、更新方法情報を参照して、更新方法を判断する。鍵有効化部514は、第1の方法で更新する場合には、第1実施形態と同様の方法でユーザ鍵 k_u およびユーザ鍵識別子UKIDを更新する。鍵有効化部514は、第2の方法で更新する場合には、第4鍵生成部711および第4鍵識別子生成部712を呼び出す。

[0214] 第4鍵生成部711は、第2ユーザ情報記憶部512に記憶された現在のユーザ鍵 k_u' と、ユーザ秘密情報受信部511により受信された種情報sを用いて、新たなユーザ鍵 k_u を生成する。第4鍵生成部711は、計測装置30の第3鍵生成部701が出力する結果と同一の結果が得られる方法によりユーザ鍵 k_u を生成する。

[0215] 第4鍵識別子生成部712は、第2ユーザ情報記憶部512に記憶された現在のユーザ鍵識別子UKID'、および、ユーザ秘密情報受信部511により受信された種情報sを用いて、新たなユーザ鍵識別子UKIDを生成する。第4鍵識別子生成部712は、計測装置30の第3鍵識別子生成部702が出力する結果と同一の結果が得られる方法によりユーザ鍵識別子UKIDを生成する。

[0216] 図21は、第3実施形態における、第2の方法でのユーザ鍵 k_u の生成のフロー図である。第3実施形態に係る計測装置30およびサービス提供装置50は、管理装置20から送信された更新方法情報に基づき、第1の方法で更新するか第2の方法で更新するかを判断する。第1の方法でユーザ鍵 k_u を更新する場合には、図8に示した処理と同様の処理を実行する。第2の方

法でユーザ鍵 k_u を更新する場合には、図 21 に示す処理を実行する。

- [0217] まず、計測装置 30 のユーザ鍵 k_u の生成処理について説明する。第 3 鍵生成部 701 は、第 1 ユーザ情報記憶部 315 から現在のユーザ鍵 k_u' を取得する（ステップ S1001）。続いて、第 3 鍵生成部 701 は、種受信部 311 が受信した新たな種情報 s を取得する（ステップ S1002）。続いて、第 3 鍵生成部 701 は、現在のユーザ鍵 k_u' および種情報 s を用いて、 $H_5(k_u', s)$ を演算して、新たなユーザ鍵 k_u を生成する（ステップ S1003）。そして、第 3 鍵生成部 701 は、生成した新たなユーザ鍵 k_u を第 1 ユーザ情報記憶部 315 に記憶させる。
- [0218] また、サービス提供装置 50 のユーザ鍵 k_u の生成処理について説明する。第 4 鍵生成部 711 は、第 2 ユーザ情報記憶部 512 から現在のユーザ鍵 k_u' を取得する（ステップ S1001）。続いて、第 4 鍵生成部 711 は、ユーザ秘密情報受信部 511 が受信した新たな種情報 s を取得する（ステップ S1002）。続いて、第 4 鍵生成部 711 は、現在のユーザ鍵 k_u' および種情報 s を用いて、 $H_5(k_u', s)$ を演算して、新たなユーザ鍵 k_u を生成する（ステップ S1003）。そして、第 4 鍵生成部 711 は、生成した新たなユーザ鍵 k_u を第 2 ユーザ情報記憶部 512 に記憶させる。
- [0219] 図 22 は、第 3 実施形態における、第 2 の方法でのユーザ鍵識別子 UKID の生成のフロー図である。第 3 実施形態に係る計測装置 30 およびサービス提供装置 50 は、管理装置 20 から送信された更新方法情報に基づき、第 1 の方法で更新するか第 2 の方法で更新するかを判断する。第 1 の方法でユーザ鍵識別子 UKID を更新する場合には、図 9 に示した処理と同様の処理を実行する。第 2 の方法でユーザ鍵識別子 UKID を更新する場合には、図 22 に示す処理を実行する。
- [0220] まず、計測装置 30 のユーザ鍵識別子 UKID の生成処理について説明する。第 3 鍵識別子生成部 702 は、第 1 ユーザ情報記憶部 315 から現在のユーザ鍵識別子 UKID' を取得する（ステップ S1101）。続いて、第 3 鍵識別子生成部 702 は、種受信部 311 が受信した新たな種情報 s を取

得する（ステップS1102）。続いて、第3鍵識別子生成部702は、現在のユーザ鍵識別子UKID'および種情報sを用いて、H6(UKID', s)を演算して、新たなユーザ鍵識別子UKIDを生成する（ステップS1103）。そして、第3鍵識別子生成部702は、生成した新たなユーザ鍵識別子UKIDを第1ユーザ情報記憶部315に記憶させる。

[0221] また、サービス提供装置50のユーザ鍵識別子UKIDの生成処理について説明する。第4鍵識別子生成部712は、第2ユーザ情報記憶部512から現在のユーザ鍵識別子UKID'を取得する（ステップS1101）。続いて、第4鍵識別子生成部712は、ユーザ秘密情報受信部511が受信した新たな種情報sを取得する（ステップS1102）。続いて、第4鍵識別子生成部712は、現在のユーザ鍵識別子UKID'および種情報sを用いて、H6(UKID', s)を演算して、新たなユーザ鍵識別子UKIDを生成する（ステップS1103）。そして、第4鍵識別子生成部712は、生成した新たなユーザ鍵識別子UKIDを第2ユーザ情報記憶部512に記憶させる。

[0222] 以上のように第3実施形態に係る伝送システム10によれば、第1実施形態と同様に、計測装置30が取得した計測情報mを、安全で簡易にサービス提供装置50へと送信することができる。さらに、第3実施形態に係る伝送システム10は、状況に応じて更新方法を変えることができ、さらに、第2の方法で更新する場合には、管理装置20からサービス提供装置50へ種情報sを送信すればよいので通信負担を軽減することができる。

[0223] なお、第3実施形態に係る伝送システム10でも、第1実施形態の変形例と同様に、更新タイミング情報を生成して、計測装置30およびサービス提供装置50に指定されたタイミングでユーザ鍵kuおよびユーザ鍵識別子UKIDを更新させてもよい。

[0224] また、第3実施形態に係る伝送システム10でも、第2実施形態と同様に、ユーザ鍵識別子UKIDに代えて固定のユーザ識別情報UIDを用いてもよい。そして、この場合、計測装置30とサービス提供装置50とは、計測

装置30が生成した更新番号NIDにより更新の同期を取ってよい。

[0225] (ハードウェア構成)

図23は、管理装置20およびサービス提供装置50のハードウェア構成を示す図である。各実施形態に係る管理装置20およびサービス提供装置50は、例えば図23に示すようなハードウェア構成の情報処理装置により実現される。なお、図23の例では、管理装置20およびサービス提供装置50が1つ情報処理装置により実現されているが、複数の情報処理装置が連携して実現されていてよい。

[0226] 情報処理装置は、CPU (Central Processing Unit) 1001と、RAM (Random Access Memory) 1002と、ROM (Read Only Memory) 1003と、記憶装置1004と、第1の通信装置1006と、第2の通信装置1007とを備える。そして、これらの各部は、バスにより接続される。

[0227] なお、サービス提供装置50を実現する情報処理装置は、第1の通信装置1006を備えない。

[0228] CPU1001は、プログラムに従って演算処理および制御処理等を実行するプロセッサである。CPU1001は、RAM1002の所定領域を作業領域として、ROM1003および記憶装置1004等に記憶されたプログラムとの協働により各種処理を実行する。

[0229] RAM1002は、SDRAM (Synchronous Dynamic Random Access Memory) 等のメモリである。RAM1002は、CPU1001の作業領域として機能する。ROM1003は、プログラムおよび各種情報を書き換え不可能に記憶するメモリである。

[0230] 記憶装置1004は、フラッシュメモリ等の半導体による記憶媒体、または、磁気的若しくは光学的に記録可能な記憶媒体等にデータを書き込みおよび読み出しをする装置である。記憶装置1004は、CPU1001からの制御に応じて、記憶媒体にデータの書き込みおよび読み出しをする。

[0231] 第1の通信装置1006は、CPU1001からの制御に応じて、事業者

ネットワーク 60 を介して外部の機器と通信する。第 2 の通信装置 1007 は、CPU 1001 からの制御に応じて、公衆ネットワーク 70 を介して外部の機器と通信する。

[0232] 各実施形態の管理装置 20 で実行されるプログラムは、サービス情報取得モジュール、ユーザ情報取得モジュール、種生成モジュール、検索モジュール、第 1 鍵生成モジュール、第 1 鍵識別子生成モジュール、種送信モジュール、ユーザ秘密情報送信モジュール、第 1 更新制御モジュールおよび第 1 更新モジュールを含むモジュール構成となっている。このプログラムは、CPU 1001 (プロセッサ) により RAM 1002 上に展開して実行されることにより、情報処理装置を、サービス情報取得部 211、ユーザ情報取得部 212、種生成部 213、検索部 215、第 1 鍵生成部 216、第 1 鍵識別子生成部 217、種送信部 218、ユーザ秘密情報送信部 219、第 1 更新制御部 220、および、第 1 更新部 221 として機能させる。また、このプログラムは、記憶装置 1004 を第 1 計測情報記憶部 214 として機能させる。

[0233] なお、管理装置 20 は、このような構成に限らず、サービス情報取得部 211、ユーザ情報取得部 212、種生成部 213、検索部 215、第 1 鍵生成部 216、第 1 鍵識別子生成部 217、種送信部 218、ユーザ秘密情報送信部 219、第 1 更新制御部 220、および、第 1 更新部 221 の少なくとも一部をハードウェア回路 (例えば半導体集積回路) により実現した構成であってもよい。

[0234] また、各実施形態のサービス提供装置 50 で実行されるプログラムは、ユーザ秘密情報受信モジュール、鍵有効化制御モジュール、鍵有効化モジュール、更新情報付加モジュール、計測情報受信モジュール、検証モジュール、サービス実行モジュール、鍵無効化制御モジュール、および、鍵無効化モジュールを含むモジュール構成となっている。このプログラムは、CPU 1001 (プロセッサ) により RAM 1002 上に展開して実行されることにより、情報処理装置を、ユーザ秘密情報受信部 511、鍵有効化制御部 513

、鍵有効化部514、更新情報付加部515、計測情報受信部516、検証部518、サービス実行部520、鍵無効化制御部521、および、鍵無効化部522として機能させる。また、このプログラムは、記憶装置1004を、第2ユーザ情報記憶部512、第2シーケンス番号記憶部517、および、計測情報記憶部519として機能させる。

[0235] なお、サービス提供装置50は、このような構成に限らず、ユーザ秘密情報受信部511と、第2ユーザ情報記憶部512と、鍵有効化制御部513、鍵有効化部514、計測情報受信部516、検証部518、サービス実行部520、および、鍵無効化部522の少なくとも一部をハードウェア回路（例えば半導体集積回路）により実現した構成であってもよい。

[0236] 図24は、計測装置30のハードウェア構成を示す図である。各実施形態に係る計測装置30は、例えば図24に示すようなハードウェア構成の情報処理装置により実現される。この情報処理装置は、CPU1011と、RAM1012と、ROM1013と、記憶装置1014と、計測機器1016と、第3の通信装置1017と、第4の通信装置1018とを備える。そして、これらの各部は、バスにより接続される。

[0237] CPU1011は、プログラムに従って演算処理および制御処理等を実行するプロセッサである。CPU1011は、RAM1012の所定領域を作業領域として、ROM1013および記憶装置1014等に記憶されたプログラムとの協働により各種処理を実行する。

[0238] RAM1012は、SDRAM等のメモリである。RAM1012は、CPU1011の作業領域として機能する。ROM1013は、プログラムおよび各種情報を書き換え不可能に記憶するメモリである。

[0239] 記憶装置1014は、フラッシュメモリ等の半導体による記憶媒体、または、磁気的若しくは光学的に記録可能な記憶媒体等にデータを書き込みおよび読み出しをする装置である。記憶装置1014は、CPU1011からの制御に応じて、記憶媒体にデータの書き込みおよび読み出しをする。

[0240] 計測機器1016は、電力量、ガスの流量、水道水または排水等の流量等

を測定する計測機器である。第3の通信装置1017は、CPU1011からの制御に応じて、事業者ネットワーク60を介して外部の機器と通信する。第4の通信装置1018は、CPU1011からの制御に応じて、ユーザネットワーク80を介して外部の機器と通信する。

- [0241] なお、計測機器1016は、計測装置30の外部に設けられ、計測装置30内に一体として設けられていなくてもよい。また、証明情報MACの生成処理が計測機器1016以外の機器により実行されてもよい。例えば、計測装置30の集約機器であるコンセントレータ、または、電力使用量を一時的に蓄積するヘッドエンドシステム等で実行されてもよい。
- [0242] また、各実施形態の計測装置30で実行されるプログラムは、種受信モジュール、第2鍵生成モジュール、第2鍵識別子生成モジュール、初期値生成モジュール、計測モジュール、証明モジュール、計測情報送信モジュール、第2更新制御モジュール、および、第2更新モジュールを含むモジュール構成となっている。このプログラムは、CPU1011（プロセッサ）によりRAM1012上に展開して実行されることにより、情報処理装置を、種受信部311、第2鍵生成部313、第2鍵識別子生成部314、初期値生成部316、計測部318、証明部319、計測情報送信部320、第2更新制御部321および第2更新部322として機能させる。また、このプログラムは、記憶装置1014を、第2計測情報記憶部312、第1ユーザ情報記憶部315および第1シーケンス番号記憶部317として機能させる。
- [0243] なお、計測装置30は、このような構成に限らず、種受信部311、第2鍵生成部313、第2鍵識別子生成部314、初期値生成部316、計測部318、証明部319、計測情報送信部320、第2更新制御部321および第2更新部322の少なくとも一部をハードウェア回路（例えば半導体集積回路）により実現した構成であってもよい。
- [0244] また、上述の各実施形態に係る発明の利用される場面例については、以下に記載する。
- [0245] スマートグリッドと呼ばれる次世代電力網システムでは、ユーザ毎に電力

使用量を計測する計測装置が設置される。この計測装置は、スマートメータ（S M）とも呼ばれる。計測装置が計測した計測情報は、電力使用に関する情報処理サービスをユーザに提供する情報処理装置（サービス提供装置）に送信される。サービス提供装置は、受信した計測情報に基づき、例えば、使用電力量の課金処理、および、例えばデマンドレスポンス（D R）と呼ばれる電力抑制要求およびその報酬の支払処理等の情報処理を実行する。

[0246] サービス提供装置が計測装置から計測情報を取得する経路は2つある。計測装置は、電力の送配電を行う事業者（送配電事業者と称する。）により管理される。それぞれの計測装置は、送配電事業者により管理される、ヘッドエンドシステムと呼ばれる管理装置にネットワークで接続されている。管理装置は、計測装置からの計測情報を収集して、メータデータ管理システム（M D M S）に保存する。このような管理装置が計測装置から計測情報を収集する経路は、スマートグリッドの分野では、A ルートと呼ばれる。サービス提供装置が計測装置から計測情報を取得する経路のうちの1つは、サービス提供装置がメータデータ管理システムを介して計測情報を取得する経路（A ルートを介して取得する経路）である。

[0247] ユーザは、計測装置、電気機器、蓄電池等と接続され、電力等のエネルギーの管理および制御を行うホームゲートウェイ（H G W）を設置することができる。ホームゲートウェイを用いてエネルギーの管理および制御を行うシステムは、スマートグリッドの分野では、ホームエネルギー・マネージメントシステム（H E M S）と呼ばれる。ホームゲートウェイは、計測装置から、ユーザが設置したユーザネットワークを介して電力使用量を直接取得することができる。ホームゲートウェイが計測情報を収集する経路は、スマートグリッドの分野では、B ルートと呼ばれる。サービス提供装置が計測装置から計測情報を取得する経路のうちの他の1つは、サービス提供装置が、ホームゲートウェイ、または、ホームゲートウェイに接続された公衆通信網接続用の通信装置（例えば、ブロードバンドルータ）を介して計測情報を取得する経路（B ルートを介して取得する経路）である。

- [0248] ところで、Aルートは、一例として、複数の計測装置を経由した無線マルチホップ方式による通信網、または、携帯電話通信網等により実現される。また、Aルートは、集線装置（コンセントレータ）を用いたPLC（電力線搬送通信）と、広域通信網とにより形成される通信網により実現される場合もある。このようなAルートは、送配電事業者によって管理されている。従って、Aルートは、信頼性が高い。しかし、Aルートは、様々な通信路を経由し、また、多数の計測装置が接続されているので、伝達できる情報量に一定の制約が生じる。このため、サービス提供装置は、Aルートを介して計測情報を取得した場合には、情報量が制限されてしまう。
- [0249] Bルートは、Aルートと比較して、豊富な帯域を利用することができ、より多くの情報を伝達できる。しかし、Bルートは、ユーザにより管理される通信機器を経由する。従って、不正なユーザが通信機器を改造し、計測情報を改ざんしてサービス提供装置に送信する可能性がある。計測情報が改ざんされると、電力料金の不正不払いおよびデマンドレスポンスにおける報酬の不正取得が可能となり、サービス事業者の損失につながってしまう。
- [0250] このため、Bルートを経由して計測情報を取得する場合には、計測装置とサービス提供装置の間で秘密鍵を共有した上で、計測装置が、秘密鍵を用いて計測情報の証明情報を生成しなければならない。しかしながら、計測装置とサービス提供装置との間で秘密鍵を共有するには、計測装置とサービス提供装置との間で双方向の鍵共有プロトコルによる秘匿通信が必要となってしまい、通信負担が大きくなってしまう。
- [0251] このような場合などで、上述した各実施形態に係る発明は利用され、計測装置が計測した計測情報を、安全かつ簡易な処理でサービス提供装置に送信することができる。
- [0252] また、各実施形態の管理装置20、計測装置30およびサービス提供装置50で実行されるプログラムは、コンピュータにインストール可能な形式または実行可能な形式のファイルで、CD-ROM、フレキシブルディスク、CD-R、DVD（Digital Versatile Disk）等のコンピュータで読み取

り可能な記録媒体に記録されて提供される。

- [0253] また、これらのプログラムを、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成してもよい。また、これらのプログラムをインターネット等のネットワーク経由で提供または配布するように構成してもよい。また、これらのプログラムを、ROM等に予め組み込んで提供するように構成してもよい。
- [0254] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、請求の範囲に記載された発明とその均等の範囲に含まれる。

請求の範囲

- [請求項1] ユーザ毎に設置される計測装置と第1ネットワークを介して接続され、サービス提供者により管理されるサービス提供装置と第2ネットワークを介して接続された管理装置であって、
前記サービス提供装置と共有して記憶するサービス提供装置識別子を用いて、種情報を生成する種生成部と、
前記計測装置と共有して記憶する計測装置個別鍵および前記種情報を用いて、ユーザ鍵を生成する第1鍵生成部と、
生成された前記種情報を前記第1ネットワークを介して前記計測装置へと送信する種送信部と、
生成された前記ユーザ鍵を前記第2ネットワークを介して前記サービス提供装置へと送信するユーザ秘密情報送信部と、
を備える管理装置。
- [請求項2] 前記ユーザ秘密情報送信部は、前記計測装置が設置される前記ユーザを特定する情報を前記サービス提供装置へと送信する
請求項1に記載の管理装置。
- [請求項3] 前記種送信部は、複数の前記計測装置に対して同一の前記種情報を送信する
請求項1または2に記載の管理装置。
- [請求項4] 前記計測装置を識別する計測装置識別子および前記種情報を用いて、ユーザ鍵識別子を生成する第1鍵生成部をさらに備え、
前記ユーザ秘密情報送信部は、前記ユーザ鍵識別子を前記サービス提供装置へと送信する
請求項1から3の何れか1項に記載の管理装置。
- [請求項5] 前記種送信部は、前記計測装置が設置された前記ユーザを識別するユーザ識別情報を前記種情報とともに前記計測装置へと送信する
請求項1から3の何れか1項に記載の管理装置。
- [請求項6] 前記ユーザ鍵を更新する必要が生じた場合に、前記種生成部に前記

種情報を更新させ、前記第1鍵生成部に前記ユーザ鍵を更新させる第1更新部をさらに備える

請求項1から5の何れか1項に記載の管理装置。

[請求項7] 前記種情報をおよび前記ユーザ鍵の更新タイミングを示す更新タイミング情報を生成する更新タイミング情報生成部をさらに備え、前記種情報をおよび前記ユーザ鍵が更新された場合、前記種送信部は、前記更新タイミング情報を前記計測装置へと送信し、前記ユーザ秘密情報送信部は、前記更新タイミング情報を前記サービス提供装置へと送信する

請求項6に記載の管理装置。

[請求項8] 更新する場合、前記種生成部は、前記サービス提供装置識別子を用いて新たな前記種情報を生成し、前記第1鍵生成部は、前記計測装置個別鍵および新たな前記種情報を用いて、新たな前記ユーザ鍵を生成し、前記種送信部は、新たな前記種情報を前記計測装置へと送信し、前記ユーザ秘密情報送信部は、新たな前記ユーザ鍵を前記サービス提供装置へと送信する

請求項6または7に記載の管理装置。

[請求項9] 前記種情報を更新する場合、前記種生成部は、前記サービス提供装置識別子を用いて新たな前記種情報を生成し、前記ユーザ鍵を更新する場合、前記第1鍵生成部は、現在の前記ユーザ鍵と更新された前記種情報を用いて、新たな前記ユーザ鍵を生成し、前記種送信部は、更新された前記種情報を前記計測装置へと送信し、前記ユーザ秘密情報送信部は、更新された前記種情報を前記サービス提供装置へと送信する

請求項 6 または 7 に記載の管理装置。

- [請求項10] 事業者により管理される管理装置と第 1 ネットワークを介して接続され、サービス提供者により管理されるサービス提供装置と第 2 ネットワークを介して接続された計測装置であって、
前記管理装置と前記サービス提供装置とが共有して記憶するサービス提供装置識別子を用いて生成された種情報を、前記第 1 ネットワークを介して前記管理装置から受信する種受信部と、
前記管理装置と共有して記憶する計測装置個別鍵および前記種情報を用いて、ユーザ鍵を生成する第 2 鍵生成部と、
前記事業者からユーザに提供されるサービスの対象の物理量を表す計測情報を取得する計測部と、
前記計測情報および前記ユーザ鍵を用いて、前記計測情報の正当性を証明する証明情報を生成する証明部と、
前記計測情報および前記証明情報を、前記第 2 ネットワークを介して前記サービス提供装置へと送信する計測情報送信部と、
を備える計測装置。

- [請求項11] 前記証明情報を生成するために用いられるシーケンス番号を保存する第 1 シーケンス番号記憶部と、
前記ユーザ鍵の更新をシーケンス番号の状態を用いて判断する第 2 更新制御部とをさらに備え、
前記証明部は、前記シーケンス番号を用いて前記証明情報を生成する
- 請求項 10 に記載の計測装置。

- [請求項12] 請求項 10 に記載の計測装置と前記第 2 ネットワークを介して接続され、前記管理装置と前記第 2 ネットワークと接続されたサービス提供装置であって、
前記ユーザ鍵を、前記管理装置から前記第 2 ネットワークを介して受信するユーザ秘密情報受信部と、

前記計測情報および前記証明情報を、前記第2ネットワークを介して前記計測装置から受信する計測情報受信部と、
前記ユーザ鍵および前記証明情報を用いて、前記計測装置から受信した前記計測情報が正当であるかを検証する検証部と、
正当であることが検証された前記計測情報を用いて、前記計測情報を送信した前記計測装置が設置されるユーザに対するサービス提供処理を実行するサービス実行部と、
を備えるサービス提供装置。

[請求項13] 前記ユーザ鍵の優先順位を表す順序情報を付加する更新情報付加部をさらに備え、

前記検証部は、前記計測装置の前記ユーザ鍵の更新完了を示す使用情報を付加し、

前記ユーザ鍵の更新タイミングを、前記順序情報と前記使用情報を用いて、特定の前記ユーザ鍵を削除する鍵無効化部をさらに備える請求項12に記載のサービス提供装置。

[請求項14] 前記鍵無効化部は、前記計測装置の前記ユーザ鍵の更新失敗を、前記順序情報と前記使用情報を用いて判定する

請求項13に記載のサービス提供装置。

[請求項15] コンピュータを請求項1から9の何れか1項に記載の管理装置として機能させるためのプログラム。

[請求項16] コンピュータを請求項10または11に記載の計測装置として機能させるためのプログラム。

[請求項17] コンピュータを請求項12から14の何れか1項に記載のサービス提供装置として機能させるためのプログラム。

[請求項18] ユーザ毎に設置される計測装置と、事業者により管理される管理装置とを備える伝送システムであって、

前記管理装置は、前記計測装置と第1ネットワークを介して接続され、

前記計測装置は、サービス提供者により管理されるサービス提供装置と第2ネットワークを介して接続され、

前記サービス提供装置は、前記管理装置と第3ネットワークを介して接続され、

前記管理装置は、

前記サービス提供装置と共有して記憶するサービス提供装置識別子を用いて、種情報を生成する種生成部と、

前記計測装置と共有して記憶する計測装置個別鍵および前記種情報を用いて、ユーザ鍵を生成する第1鍵生成部と、

生成された前記種情報を前記第1ネットワークを介して前記計測装置へと送信する種送信部と、

生成された前記ユーザ鍵を前記第3ネットワークを介して前記サービス提供装置へと送信するユーザ秘密情報送信部と、

を有し、

前記計測装置は、

前記管理装置と前記サービス提供装置とが共有して記憶するサービス提供装置識別子を用いて生成された前記種情報を、前記第1ネットワークを介して前記管理装置から受信する種受信部と、

前記管理装置と共有して記憶する計測装置個別鍵および前記種情報を用いて、前記ユーザ鍵を生成する第2鍵生成部と、

前記事業者からユーザに提供されるサービスの対象の物理量を表す計測情報を取得する計測部と、

前記計測情報および前記ユーザ鍵を用いて、前記計測情報の正当性を証明する証明情報を生成する証明部と、

前記計測情報および前記証明情報を、前記第2ネットワークを介して前記サービス提供装置へと送信する計測情報送信部と、

を有する

伝送システム。

[請求項19]

前記サービス提供装置をさらに備え、
前記サービス提供装置は、
前記ユーザ鍵を、前記管理装置から前記第3ネットワークを介して受信するユーザ秘密情報受信部と、
前記計測情報および前記証明情報を、前記第2ネットワークを介して前記計測装置から受信する計測情報受信部と、
前記ユーザ鍵および前記証明情報を用いて、前記計測装置から受信した前記計測情報が正当であるかを検証する検証部と、
正当であることが検証された前記計測情報を用いて、前記計測情報を送信した前記計測装置が設置されるユーザに対するサービス提供処理を実行するサービス実行部と、
を有する
請求項18に記載の伝送システム。

[請求項20]

ユーザ毎に設置される計測装置と、事業者により管理される管理装置と、サービス提供者により管理されるサービス提供装置とを備える伝送システムで実行される伝送方法であって、
前記管理装置は、前記計測装置と第1ネットワークを介して接続され、
前記計測装置は、前記サービス提供装置と第2ネットワークを介して接続され、
前記サービス提供装置は、前記管理装置と第3ネットワークを介して接続され、
前記管理装置が、前記サービス提供装置と共有して記憶するサービス提供装置識別子を用いて、種情報を生成し、
前記管理装置が、前記計測装置と共有して記憶する計測装置個別鍵および前記種情報を用いて、ユーザ鍵を生成し、
前記管理装置が、生成された前記種情報を前記第1ネットワークを介して前記計測装置へと送信し、

前記管理装置が、生成された前記ユーザ鍵を前記第3ネットワークを介して前記サービス提供装置へと送信し、

前記計測装置が、前記管理装置と前記サービス提供装置とが共有して記憶するサービス提供装置識別子を用いて生成された前記種情報を、前記第1ネットワークを介して前記管理装置から受信し、

前記計測装置が、前記管理装置と共有して記憶する計測装置個別鍵および前記種情報を用いて、前記ユーザ鍵を生成し、

前記計測装置が、前記事業者からユーザに提供されるサービスの対象の物理量を表す計測情報を取得し、

前記計測装置が、前記計測情報および前記ユーザ鍵を用いて、前記計測情報の正当性を証明する証明情報を生成し、

前記計測装置が、前記計測情報および前記証明情報を、前記第2ネットワークを介して前記サービス提供装置へと送信する
伝送方法。

[請求項21]

前記サービス提供装置が、前記ユーザ鍵を、前記管理装置から前記第3ネットワークを介して受信し、

前記サービス提供装置が、前記計測情報および前記証明情報を、前記第2ネットワークを介して前記計測装置から受信し、

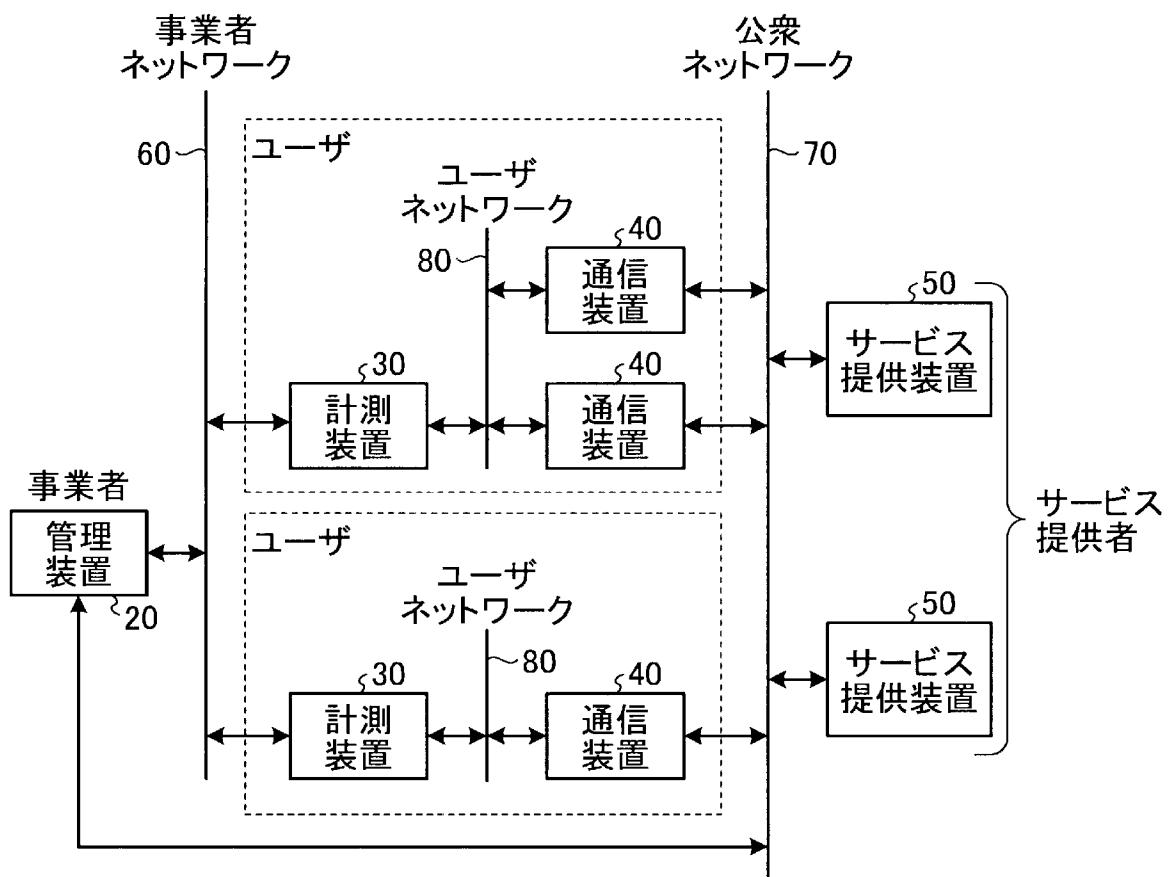
前記サービス提供装置が、前記ユーザ鍵および前記証明情報を用いて、前記計測装置から受信した前記計測情報が正当であるかを検証し、

前記サービス提供装置が、正当であることが検証された前記計測情報を用いて、前記計測情報を送信した前記計測装置が設置されるユーザに対するサービス提供処理を実行する

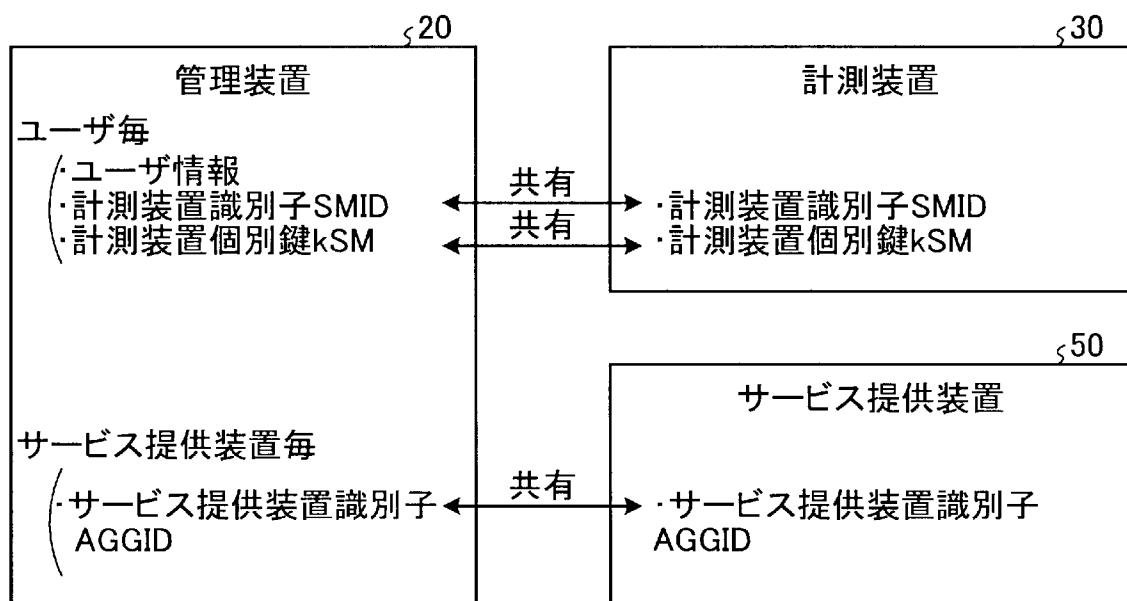
請求項20に記載の伝送方法。

[図1]

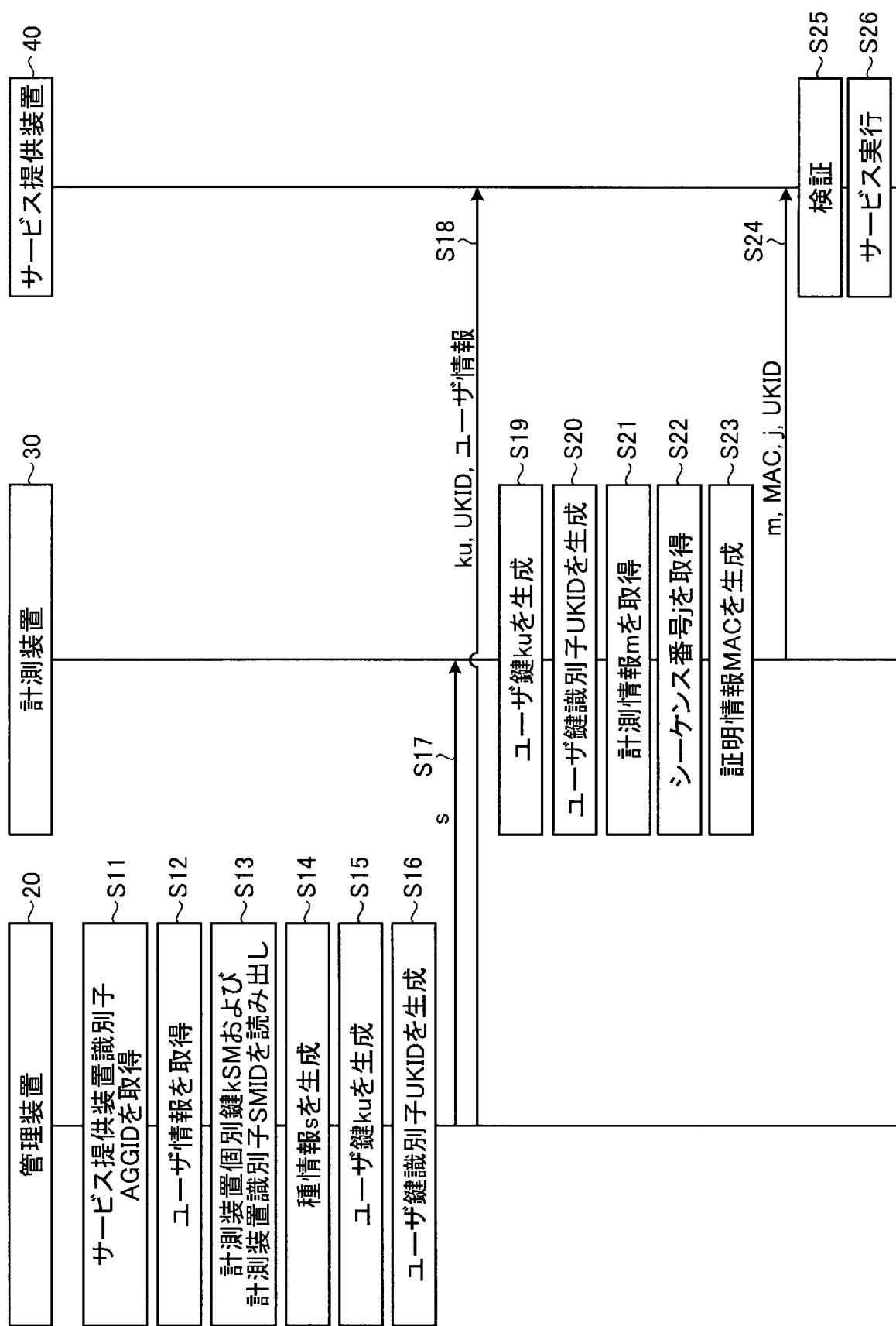
10



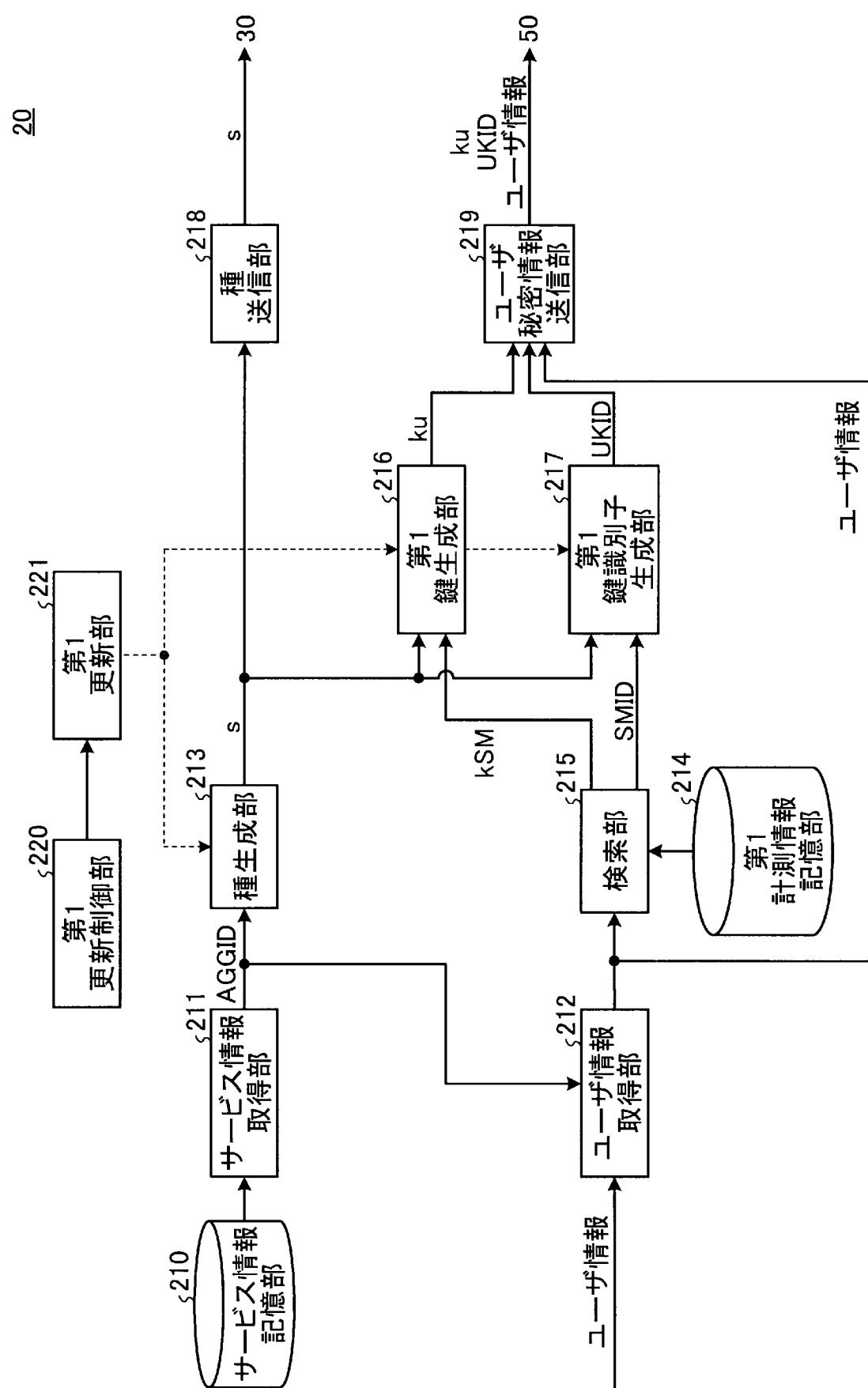
[図2]



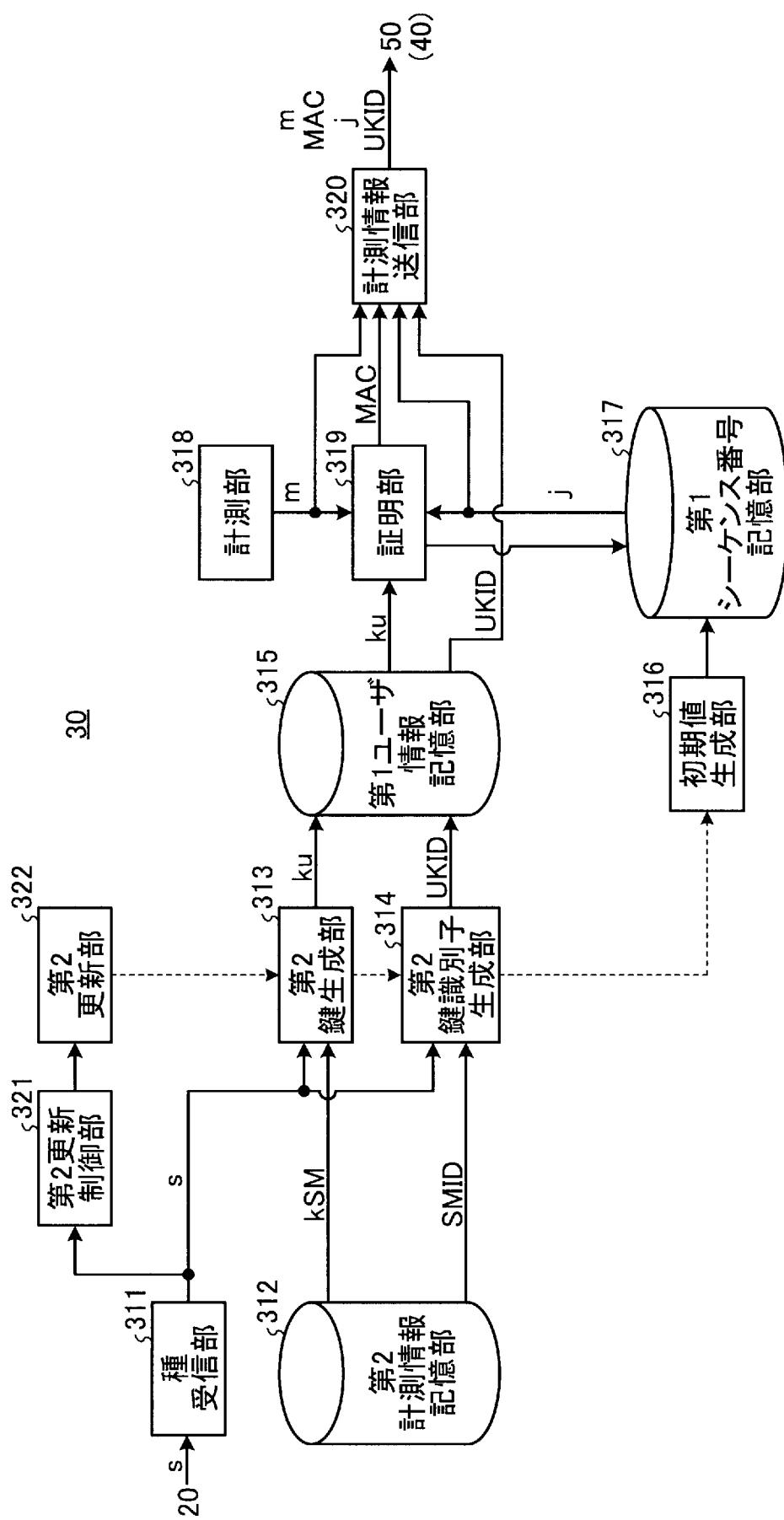
[図3]



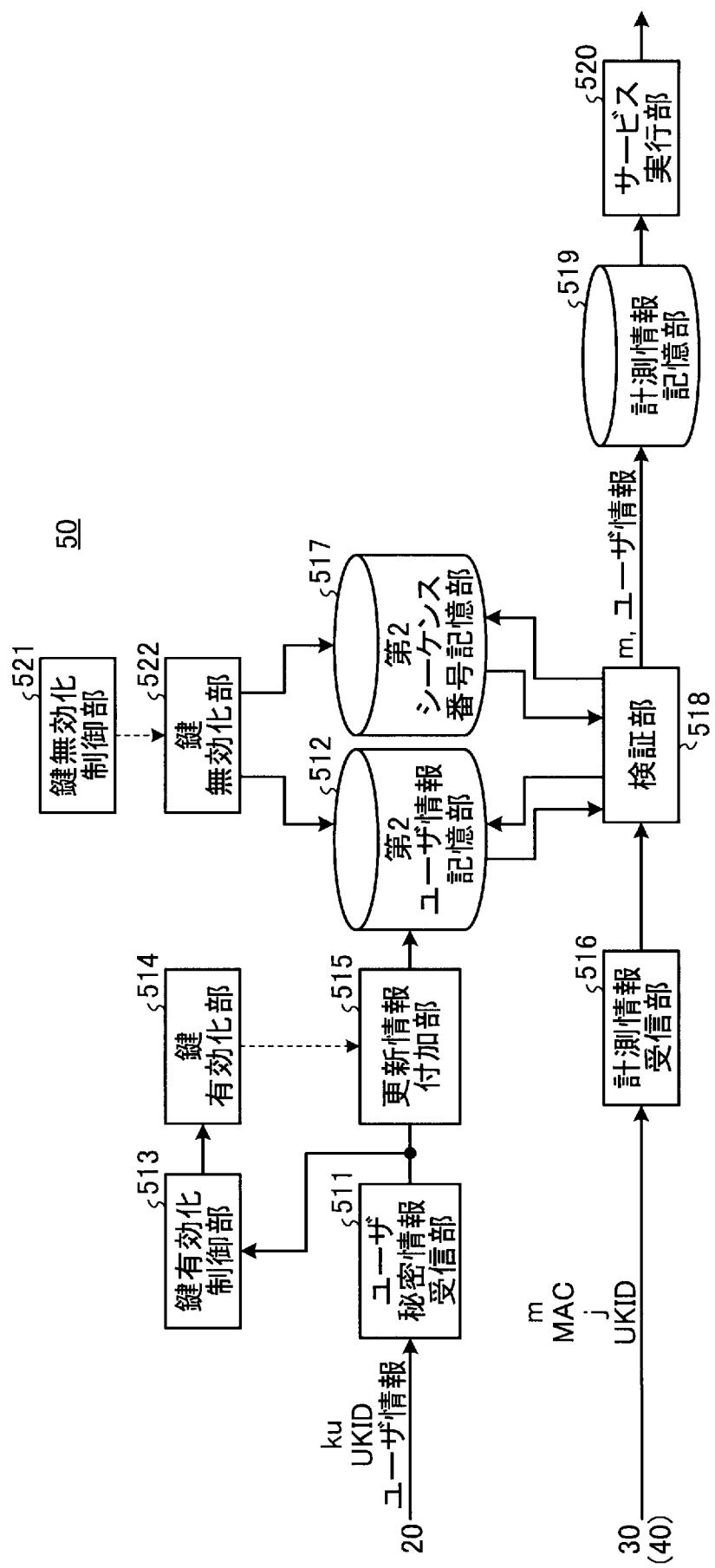
[図4]



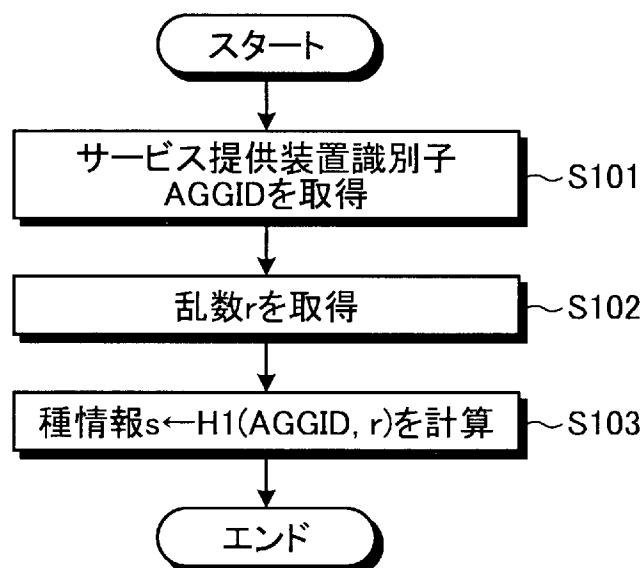
[図5]



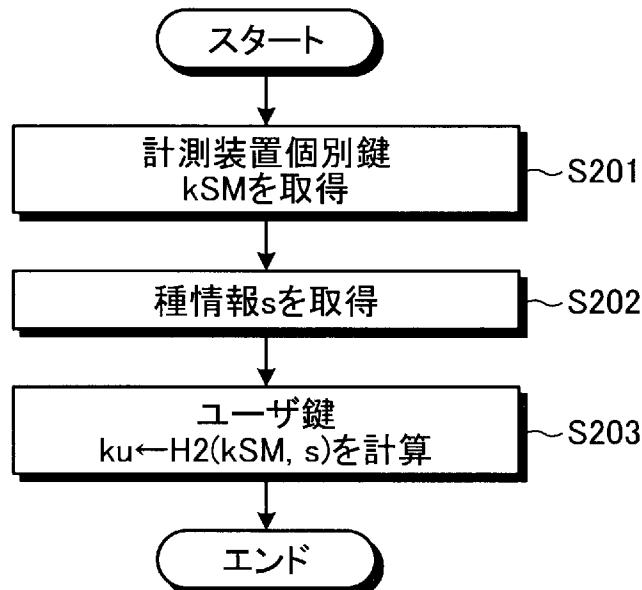
[図6]



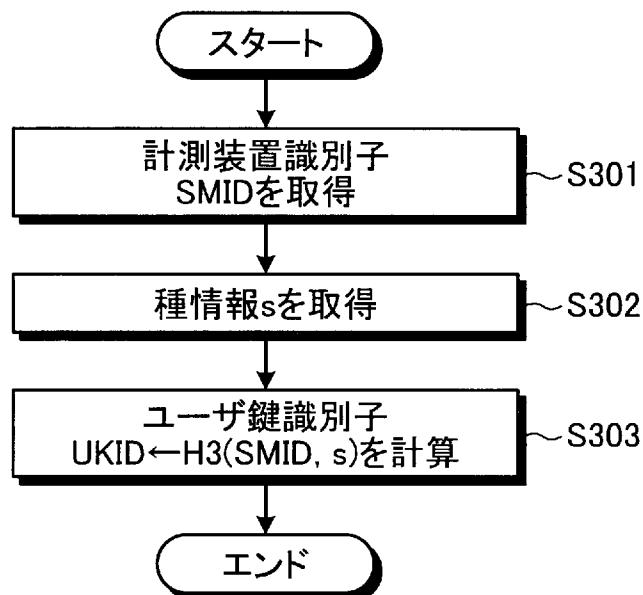
[図7]



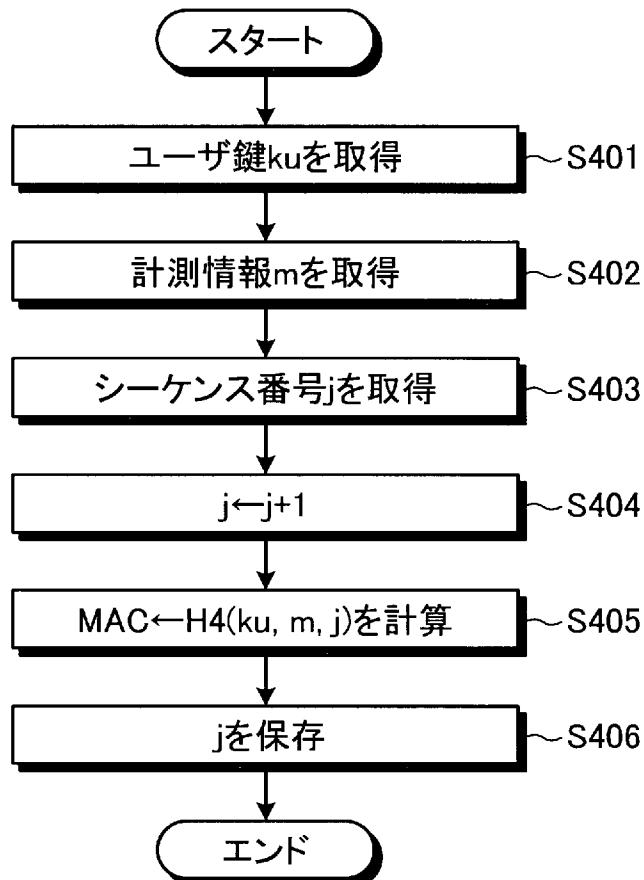
[図8]



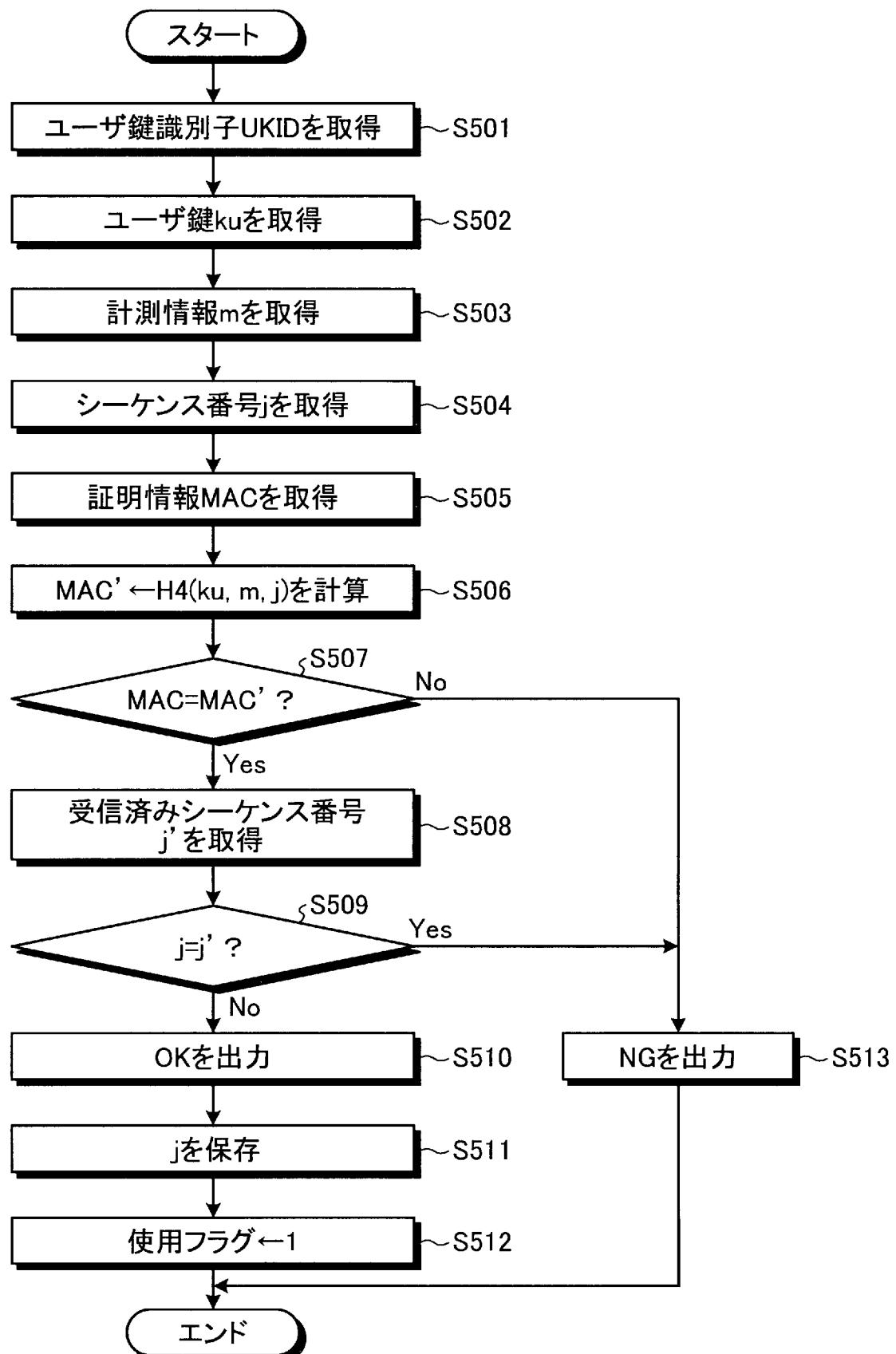
[図9]



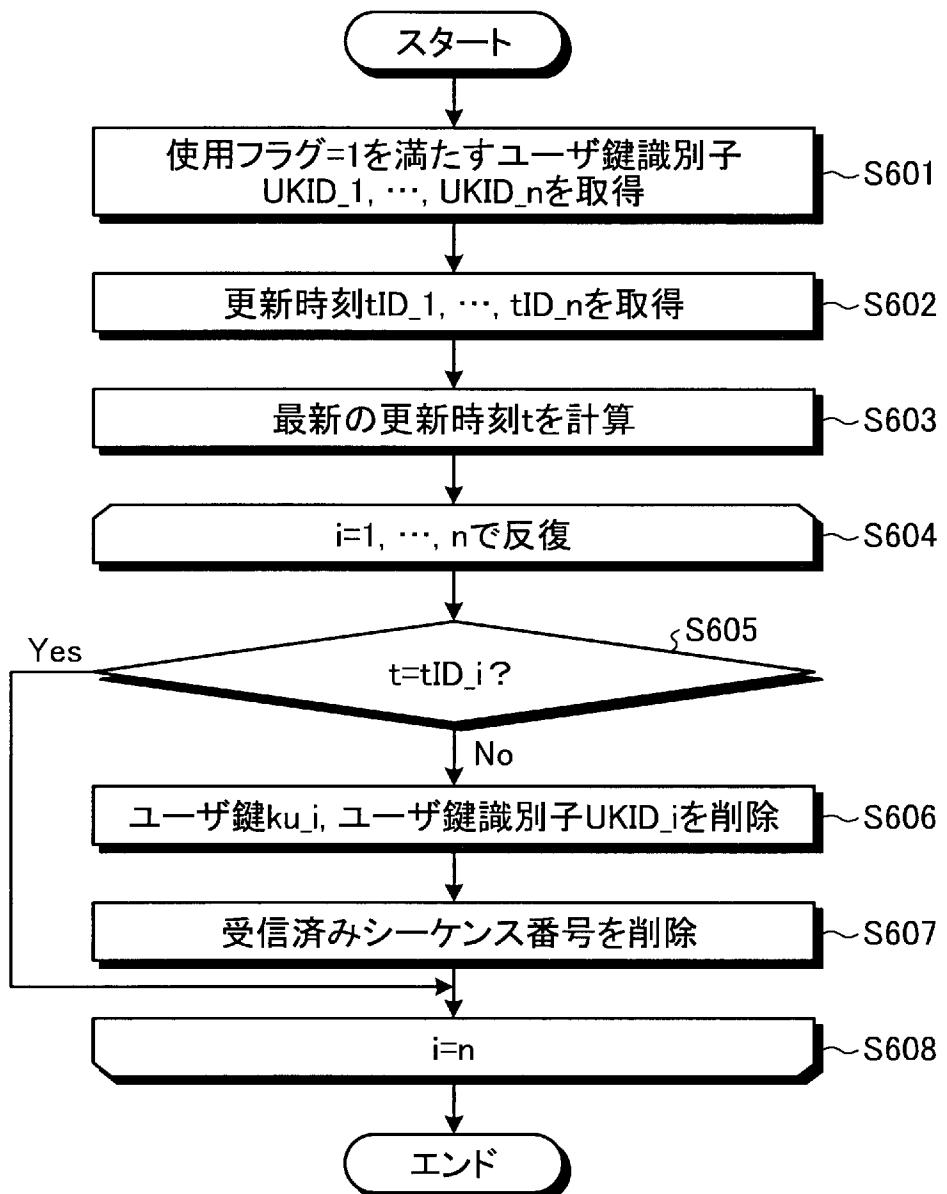
[図10]



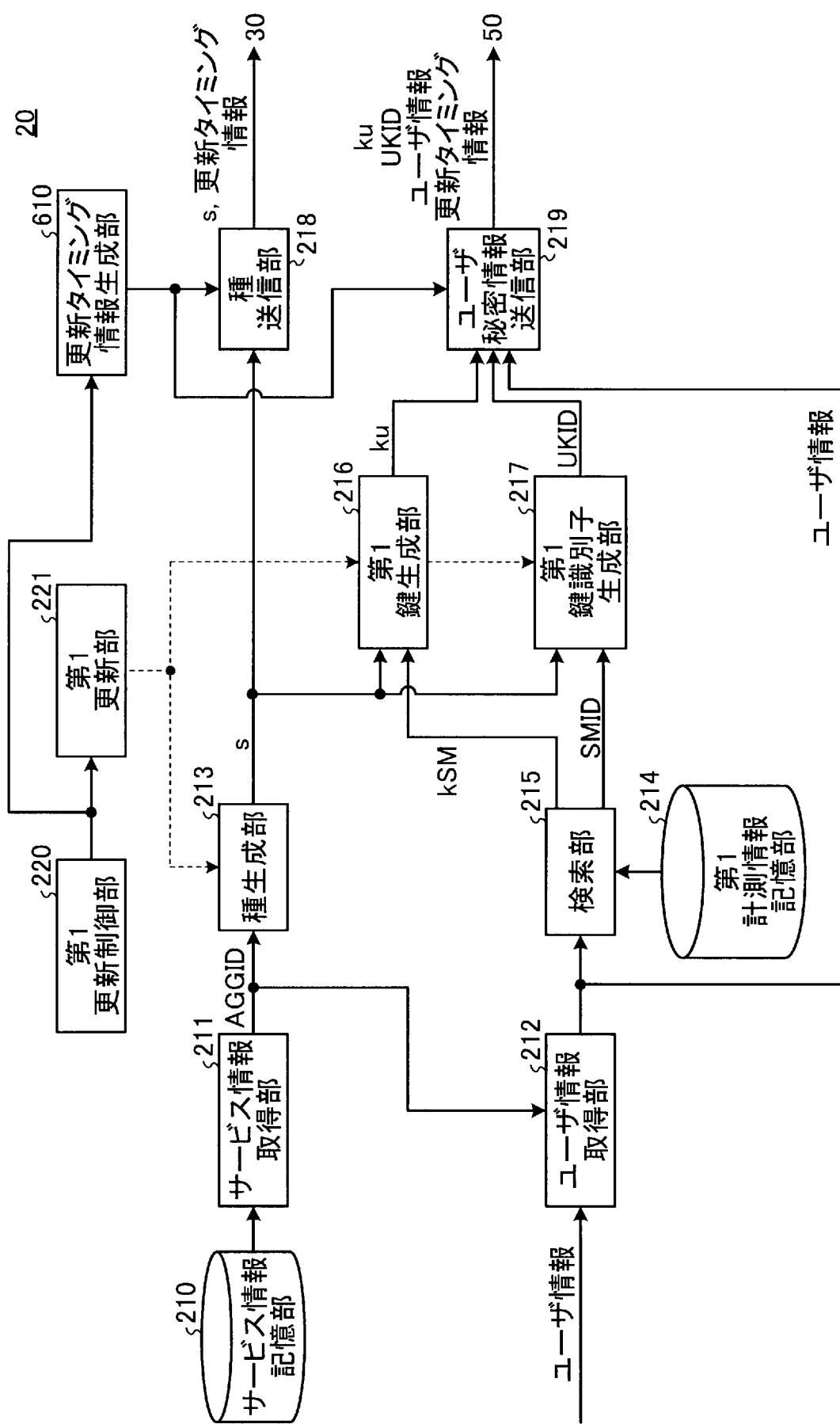
[図11]



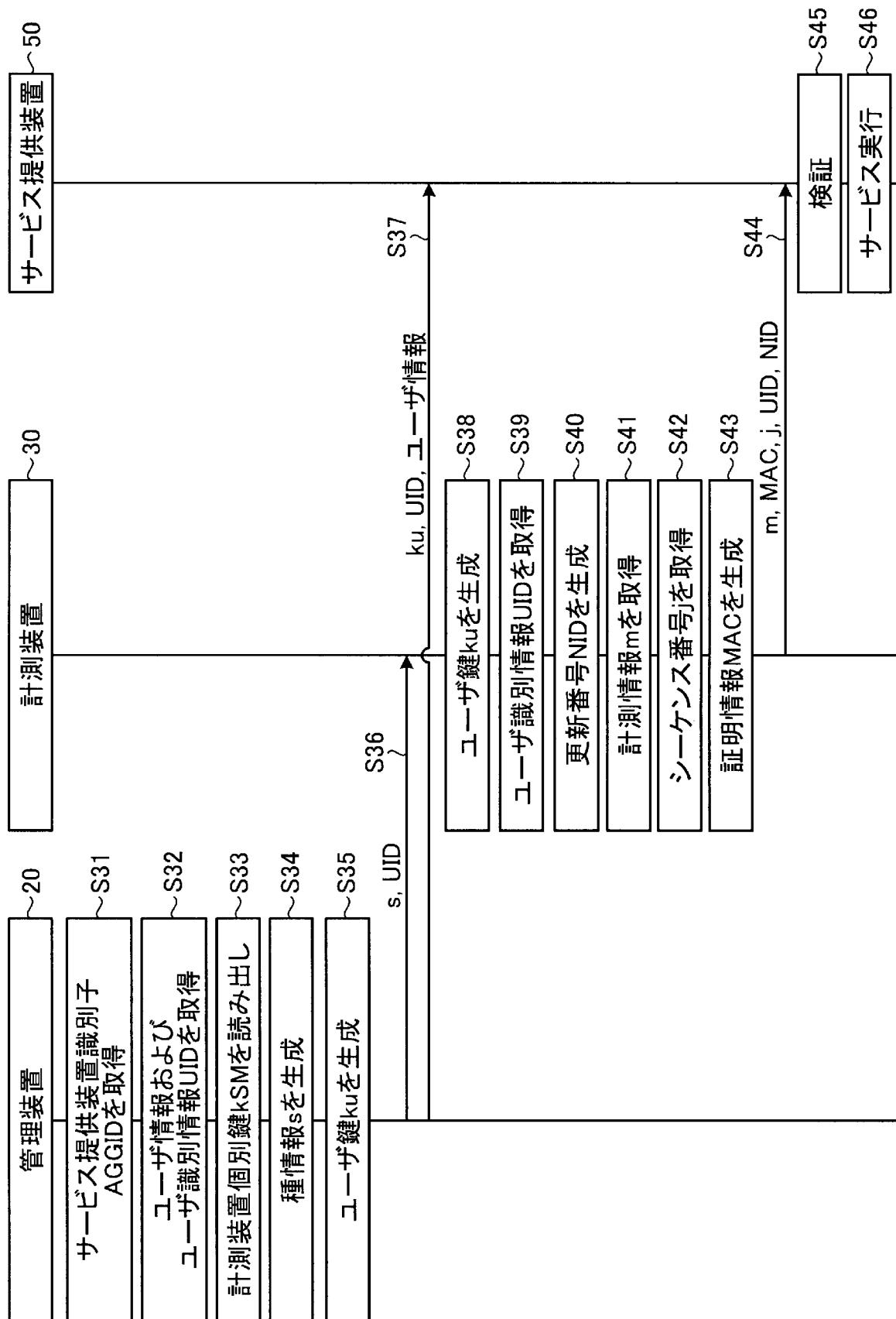
[図12]



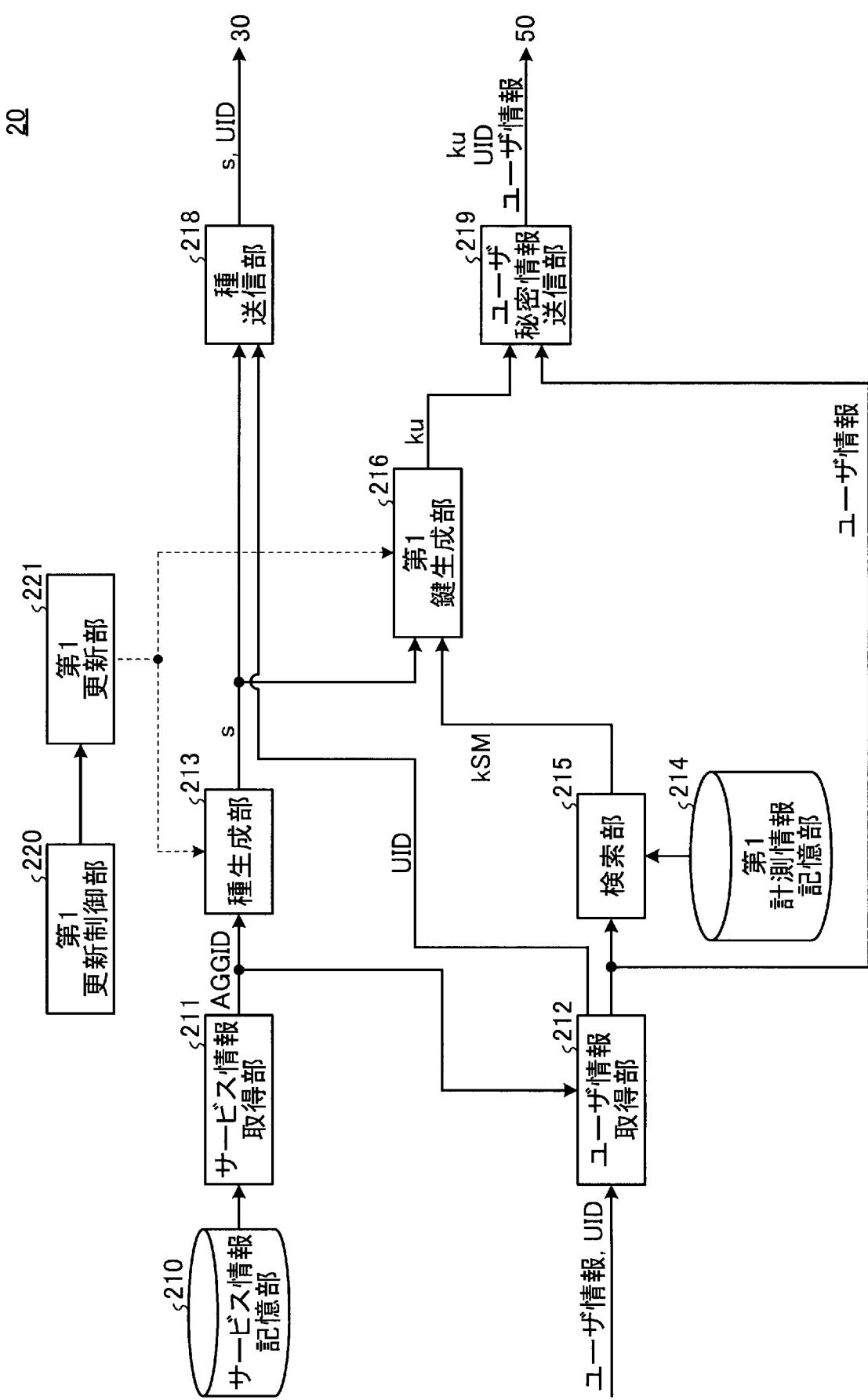
[図13]



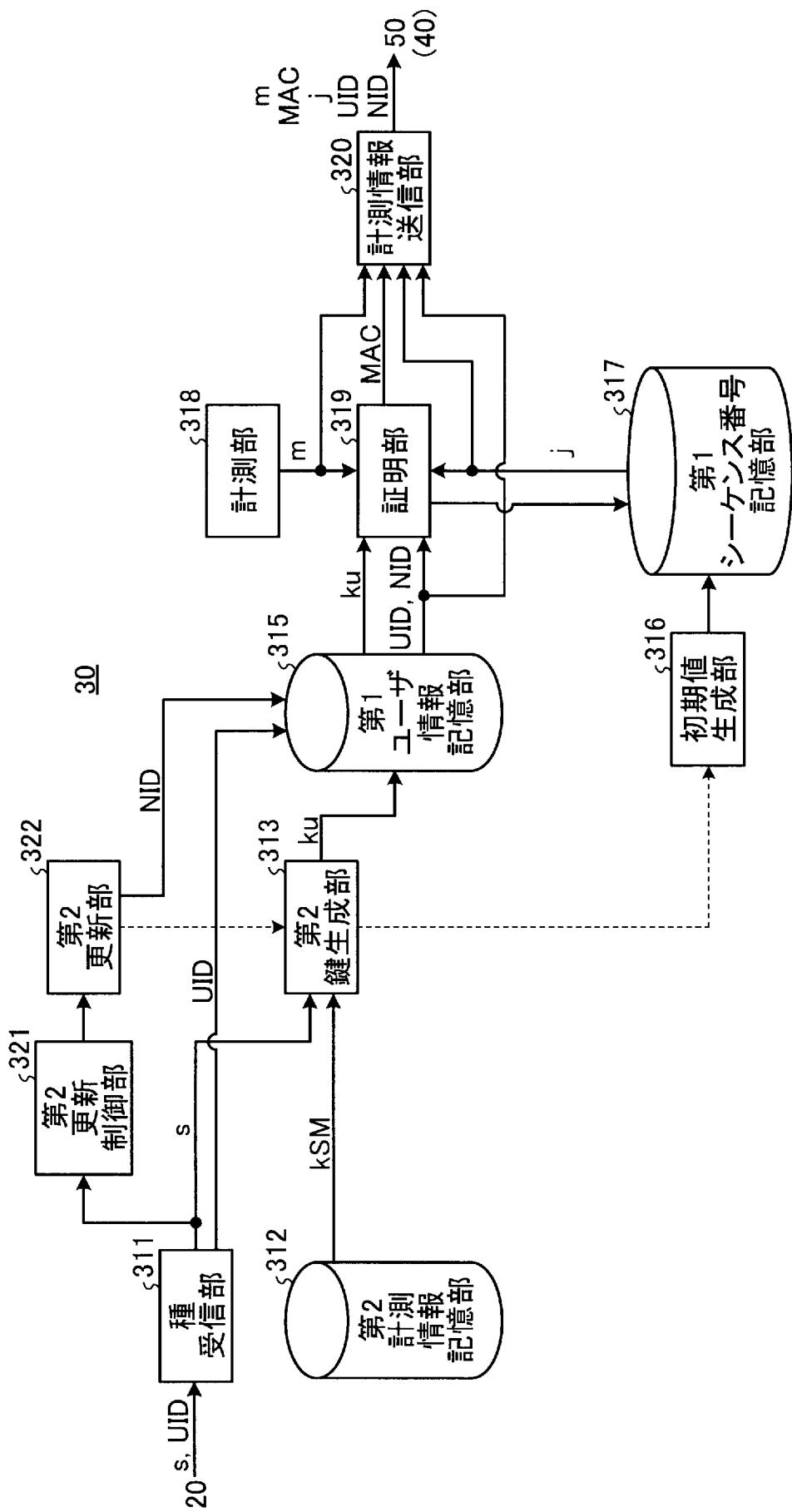
[図14]



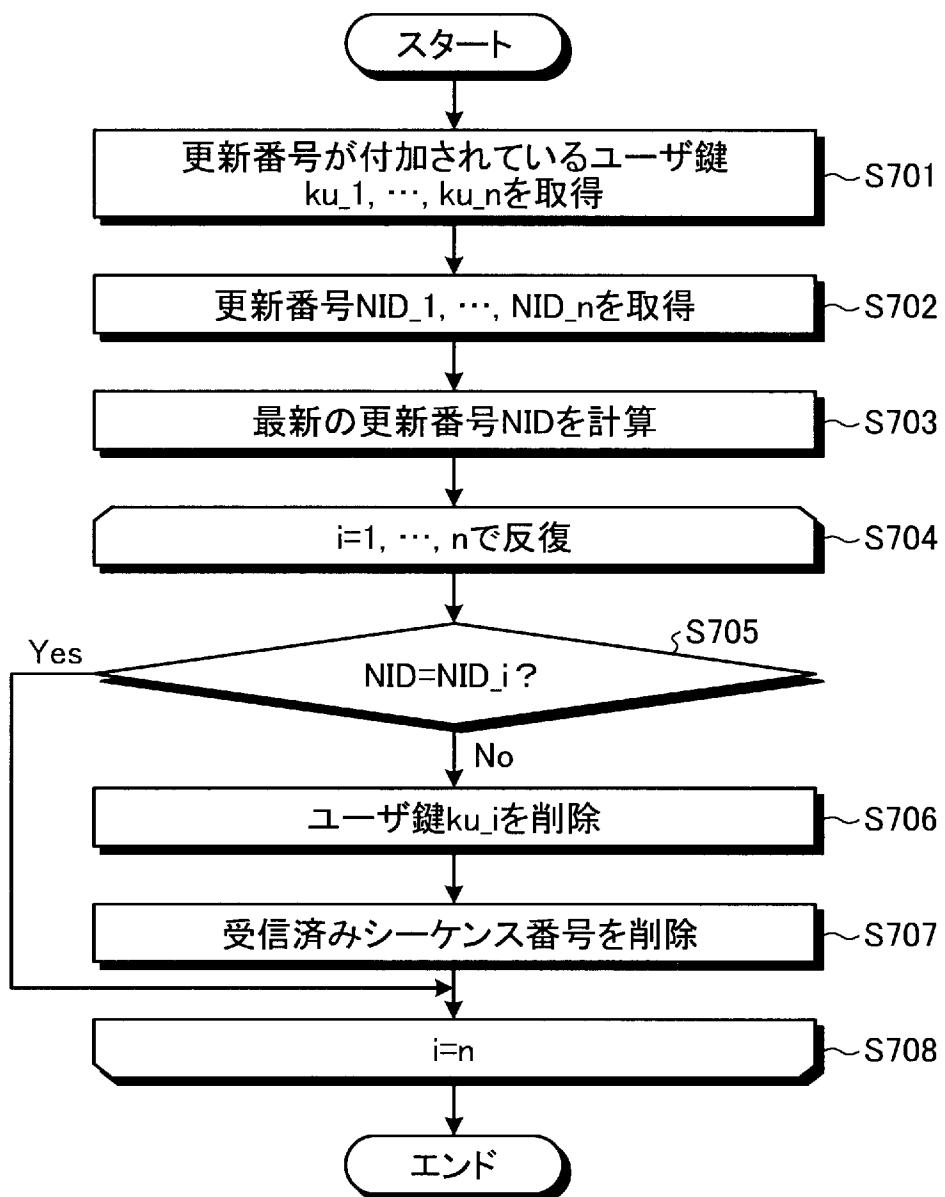
[図15]



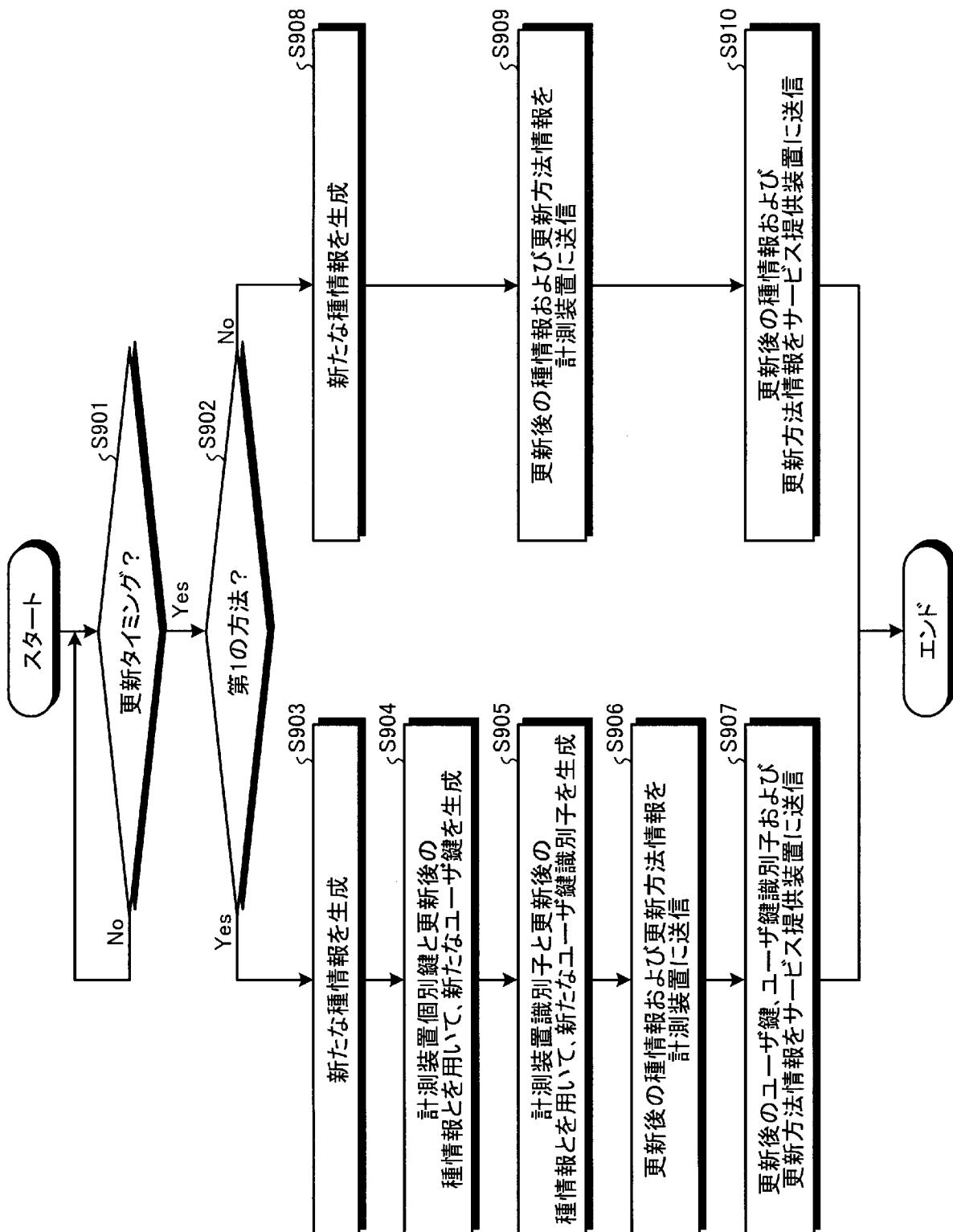
[図16]



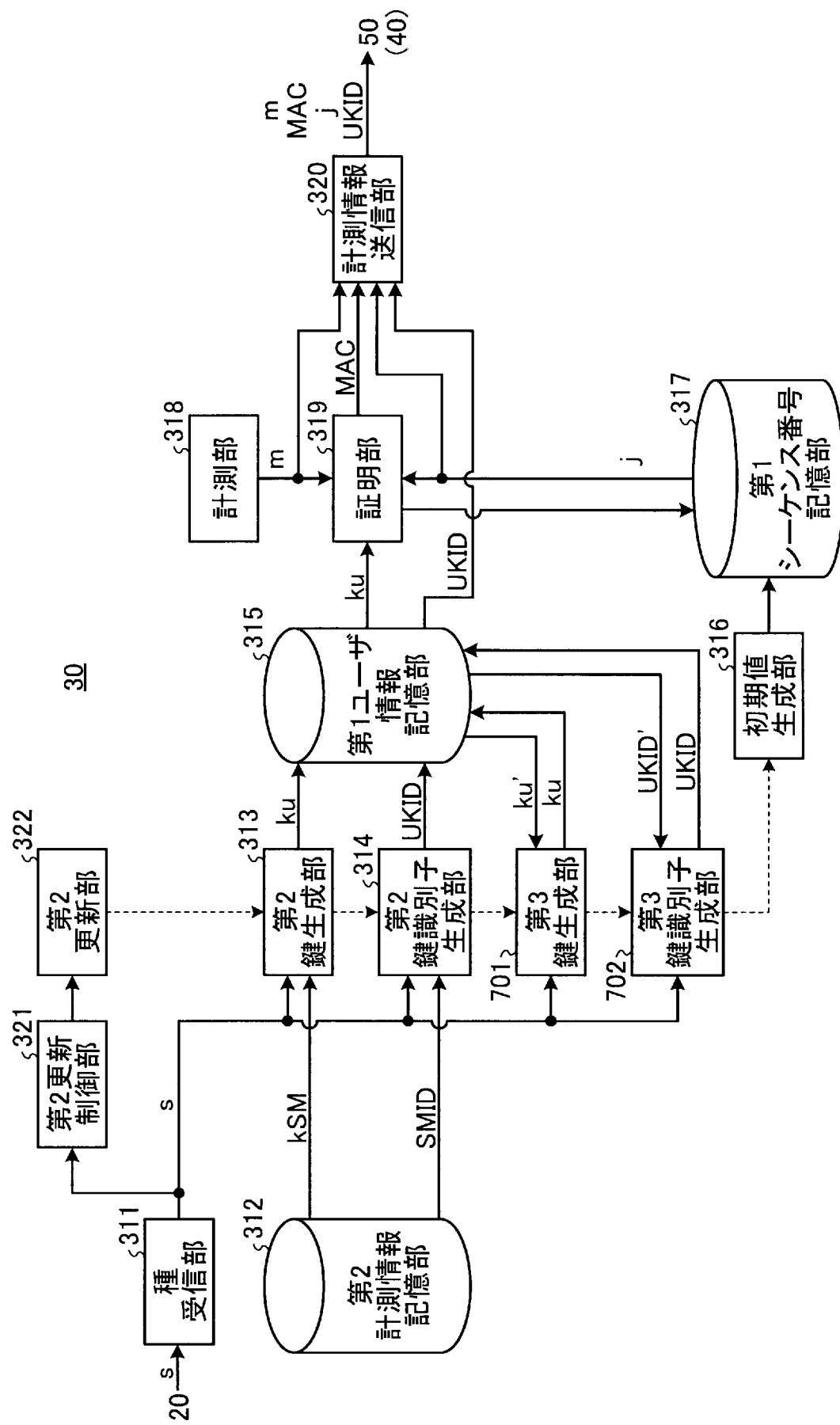
[図17]



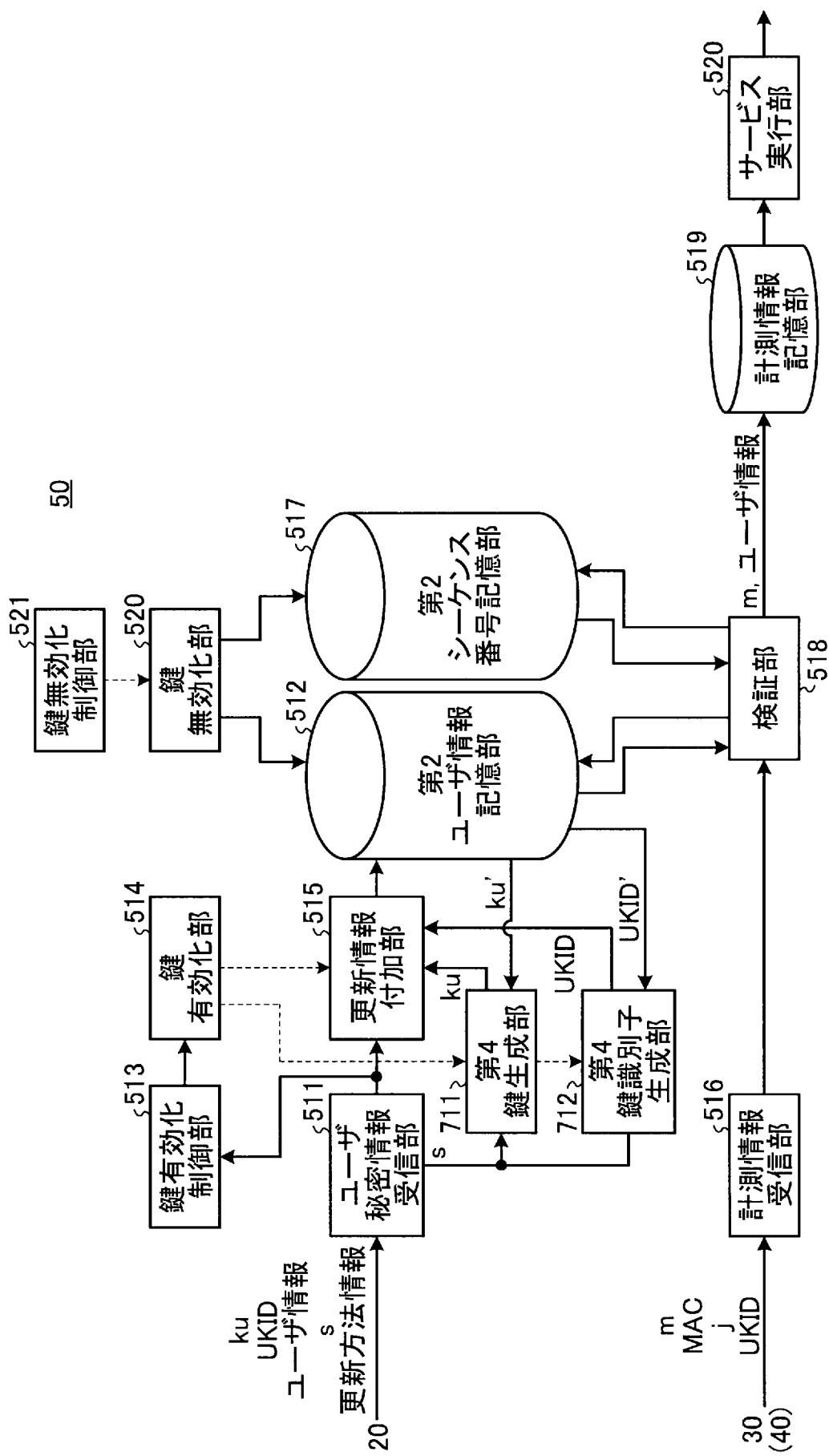
[図18]



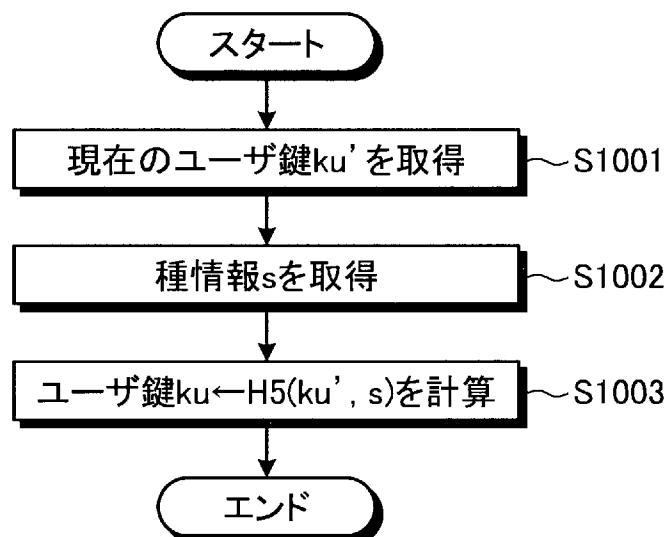
[図19]



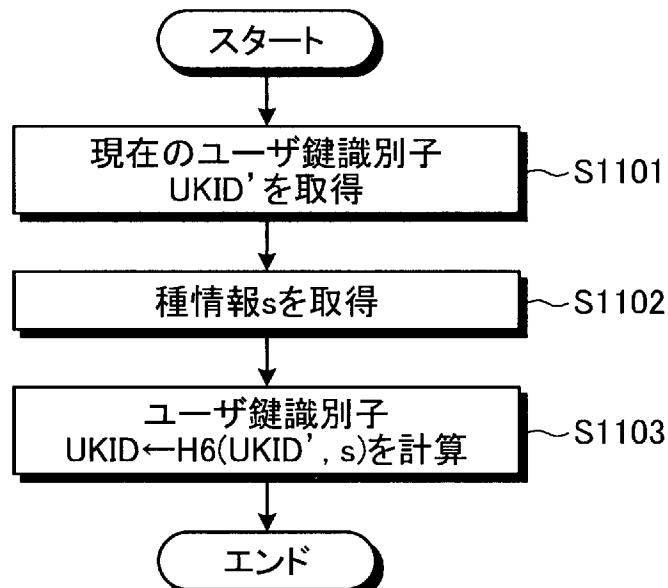
[図20]



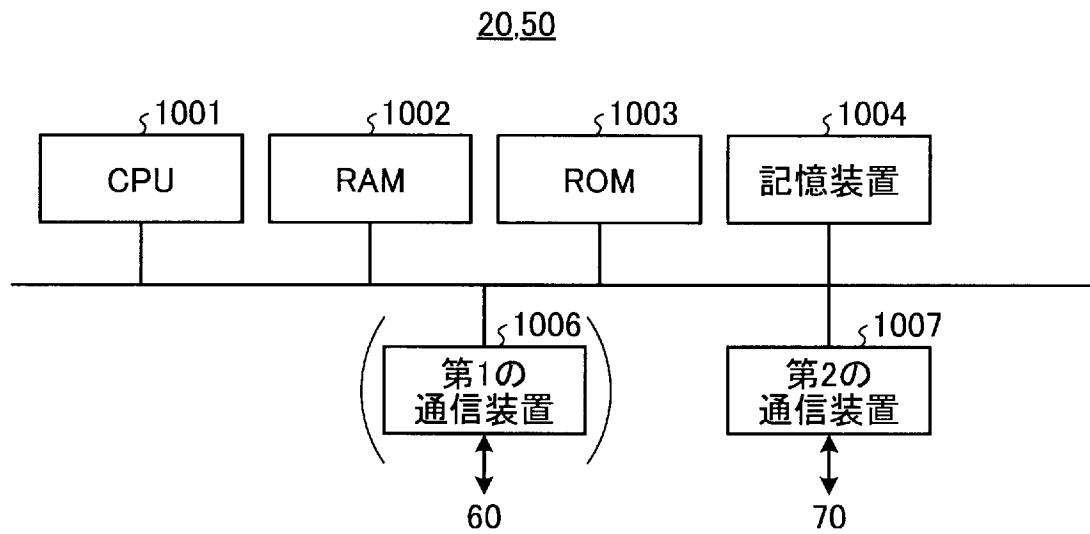
[図21]



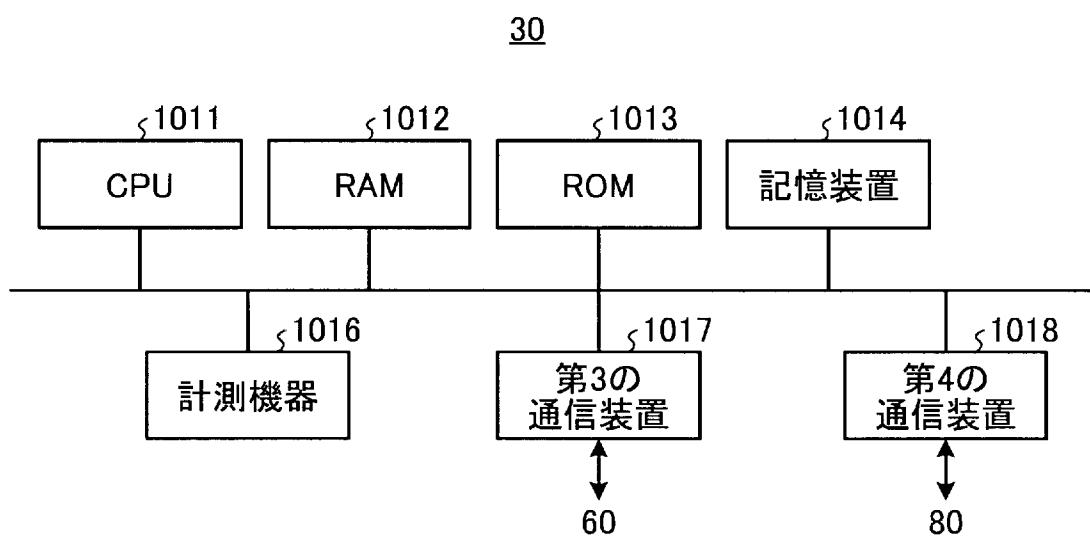
[図22]



[図23]



[図24]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/074872

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08 (2006.01) i, H04L9/32 (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)
H04L9/08, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2014
Kokai Jitsuyo Shinan Koho 1971-2014 Toroku Jitsuyo Shinan Koho 1994-2014

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580 (JDreamIII), smart meter, smart grid,
key distribution, authentication, integrity

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 2007-215103 A (Seiko Instruments Inc.), 23 August 2007 (23.08.2007), paragraphs [0010] to [0020], [0054] to [0060], [0080] to [0087], [0139] to [0142]	12, 17 1-11, 13-16, 18-21
A	WO 2010/096923 A1 (CERTICOM CORP.), 02 September 2010 (02.09.2010), paragraphs [0025] to [0030], [0180], [0192] to [0202]	1-21
A	Xia, J. and Wang, Y., Secure Key Distribution for the Smart Grid, IEEE Transactions on Smart Grid, 2012.09, Volume:3 Issue:3, p.1437-1443, especially III. OUR PROPOSED SECURE KEY DISTRIBUTION SCHEME FOR THE SMART GRID	1-21

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	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"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
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
07 November, 2014 (07.11.14)

Date of mailing of the international search report
18 November, 2014 (18.11.14)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/074872

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Nicanfar, H. et al., Efficient Authentication and Key Management Mechanisms for Smart Grid Communications, IEEE Systems Journal, 2014.06, Volume:8 Issue:2, p.629-640, especially III. SGMA, IV.SGKM PROTOCOL	1-21

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2014/074872

JP 2007-215103 A	2007.08.23	(Family: none)
WO 2010/096923 A1	2010.09.02	US 2010/0241848 A1 2010.09.23
		EP 2401835 A1 2012.01.04
		CA 2752752 A 2010.09.02
		AU 2010217154 A 2011.09.15

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04L9/08(2006.01)i, H04L9/32(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. H04L9/08, H04L9/32

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	1971-2014年
日本国実用新案登録公報	1996-2014年
日本国登録実用新案公報	1994-2014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）

JSTPlus/JMEDPlus/JST7580(JDreamIII) smart meter, smart grid, key distribution, authentication, integrity

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
X	JP 2007-215103 A (セイコーアイテクノロジーズ株式会社) 2007.08.23,	12, 17
A	10-20, 54-60, 80-87, 139-142段落	1-11, 13-16, 18-21
A	WO 2010/096923 A1 (CERTICOM CORP.) 2010.09.02, 25-30, 180, 192-202段落	1-21

 C欄の続きにも文献が挙げられている。 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」国際出願目前で、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

07. 11. 2014

国際調査報告の発送日

18. 11. 2014

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）

中里 裕正

5S

9364

電話番号 03-3581-1101 内線 3546

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	Xia, J. and Wang, Y., Secure Key Distribution for the Smart Grid, IEEE Transactions on Smart Grid, 2012.09, Volume:3 Issue:3, p. 1437-1443, especially III. OUR PROPOSED SECURE KEY DISTRIBUTION SCHEME FOR THE SMART GRID	1-21
A	Nicanfar, H. et al., Efficient Authentication and Key Management Mechanisms for Smart Grid Communications, IEEE Systems Journal, 2014.06, Volume:8 Issue:2, p. 629-640, especially III. SGMA, IV. SGKM PROTOCOL	1-21

JP 2007-215103 A	2007.08.23	ファミリーなし	
WO 2010/096923 A1	2010.09.02	US 2010/0241848 A1	2010.09.23
		EP 2401835 A1	2012.01.04
		CA 2752752 A	2010.09.02
		AU 2010217154 A	2011.09.15