

(19) 日本国特許庁(JP)

再公表特許(A1)

(11) 国際公開番号

W02018/021535

発行日 令和1年5月23日(2019.5.23)

(43) 国際公開日 平成30年2月1日(2018.2.1)

(51) Int.Cl.	F I	テーマコード (参考)
G09C 1/00 (2006.01)	G09C 1/00 640D	5J104
H04L 9/32 (2006.01)	H04L 9/00 675D	

審査請求 未請求 予備審査請求 未請求 (全 35 頁)

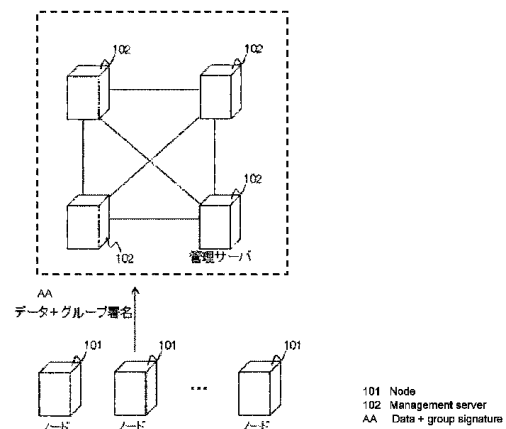
出願番号	特願2018-530424 (P2018-530424)	(71) 出願人	000004237
(21) 国際出願番号	PCT/JP2017/027461		日本電気株式会社
(22) 国際出願日	平成29年7月28日 (2017.7.28)		東京都港区芝五丁目7番1号
(31) 優先権主張番号	特願2016-150100 (P2016-150100)	(74) 代理人	100080816
(32) 優先日	平成28年7月29日 (2016.7.29)		弁理士 加藤 朝道
(33) 優先権主張国	日本国 (JP)	(74) 代理人	100098648
			弁理士 内田 深人
		(72) 発明者	佐古 和恵
			東京都港区芝五丁目7番1号 日本電気株式会社内
		(72) 発明者	寺西 勇
			東京都港区芝五丁目7番1号 日本電気株式会社内
		Fターム(参考)	5J104 AA08 LA06 MA01 NA02 NA37 PA07

最終頁に続く

(54) 【発明の名称】 システム、データ管理方法及びプログラム

(57) 【要約】

データの正当性を検証可能としつつ、当該データから得られる情報を適切に制限するシステムを提供する。システムは、グループ署名が付与されたデータを送信する、複数のノードと、相互に直接接続されている、複数の管理サーバと、を含む。複数の管理サーバのそれぞれは、ノードから受信したデータを管理するための台帳を有する。複数の管理サーバのうち少なくとも1つの管理サーバによる台帳へのデータの追記は他の管理サーバの台帳に反映される。



【特許請求の範囲】**【請求項 1】**

グループ署名が付与されたデータを送信する、複数のノードと、
相互に直接接続されている、複数の管理サーバと、
を含み、

前記複数の管理サーバのそれぞれは、前記ノードから受信したデータを管理するための
台帳を有し、

前記複数の管理サーバのうち少なくとも 1 つの管理サーバによる前記台帳へのデータの
追記は他の管理サーバの台帳に反映される、システム。

【請求項 2】

前記複数のノードは、複数のグループのいずれかに属しており、

前記複数のグループそれぞれに属するノードを管理する、複数のノード管理サーバをさ
らに含み、

前記ノード管理サーバのそれぞれは、自グループに属する前記ノードに対し、グループ
署名を生成する際に用いるメンバ証明書を発行する、請求項 1 のシステム。

【請求項 3】

前記複数のノードは、複数のグループのいずれかに属しており、

前記複数のグループそれぞれに属するノードを管理する、複数のノード管理サーバと、

前記複数のノードそれぞれに対し、グループ署名を生成する際に用いるメンバ証明書を
発行する、証明書管理サーバと、をさらに含み、

前記複数のノード管理サーバのそれぞれは、特権者公開鍵を公開し、

前記証明書管理サーバは、管理者公開鍵を公開する、請求項 1 のシステム。

【請求項 4】

前記ノードは、前記管理者公開鍵と、前記複数のノード管理サーバそれぞれが公開する
特権者公開鍵と、を用いてグループ署名を生成する、請求項 3 のシステム。

【請求項 5】

前記生成されたグループ署名は、前記証明書管理サーバが公開する管理者公開鍵と前記
複数のノード管理サーバのそれぞれが公開した特権者公開鍵により、検証可能である請求
項 4 のシステム。

【請求項 6】

前記ノード管理サーバは、自身が管理するグループに属するノードが生成したグループ
署名に含まれるデータを、前記特権者公開鍵とペアとなる特権者秘密鍵により取り出し、
自身が管理するグループに属するノードを特定する、請求項 3 乃至 5 のいずれか一項に記
載のシステム。

【請求項 7】

それぞれがグループに属する、複数のノードと、

それぞれのグループに属するノードを管理する、複数のノード管理サーバと、

前記複数のノードそれぞれに対し、グループ署名を生成する際に用いるメンバ証明書を
発行すると共に、管理者公開鍵を公開する証明書管理サーバと、を含み、

前記複数のノード管理サーバのそれぞれは、特権者公開鍵を公開し、

前記ノードは、データに付与するグループ署名の生成を、少なくとも前記管理者公開鍵
と前記複数のノード管理サーバのそれぞれが公開する特権者公開鍵を用いて行う、システ
ム。

【請求項 8】

前記ノードが生成するグループ署名は、前記グループ署名を生成したノード自身の公開
鍵を、前記複数のノード管理サーバが公開するいずれかの特権者公開鍵で暗号化し、前記
自身の公開鍵にメンバ証明書が存在すること、且つ、暗号化した主体が前記自身の公開鍵
に対応する秘密鍵を有すること、を証明するデータを含む、請求項 7 のシステム。

【請求項 9】

前記複数のノード管理サーバが公開する特権者公開鍵は、一部の要素が共通するように

10

20

30

40

50

生成された公開鍵である、請求項 7 及び 8 のシステム。

【請求項 10】

前記共通する一部の要素は、前記特権者公開鍵に対応する特権者秘密鍵に依存して生成される要素である、請求項 9 のシステム。

【請求項 11】

前記ノードの公開鍵は、前記共通する一部の要素に基づき生成される、請求項 10 のシステム。

【請求項 12】

前記ノードは、自身が属するグループとは異なるグループのチャレンジ値をランダムに選択し、前記ランダムに選択されたチャレンジ値を用いて前記グループ署名を生成する、請求項 7 乃至 11 のいずれか一項に記載のシステム。

10

【請求項 13】

前記ノードが生成したグループ署名の検証には、前記計算されたハッシュ値と、前記ランダムに選択されたチャレンジ値と、グループ署名を生成したノードが属するグループのチャレンジ値と、を用いる検証が少なくとも含まれる、請求項 12 のシステム。

【請求項 14】

複数のノードと、

相互に直接接続され、前記ノードから受信したデータを管理するための台帳を有する、複数の管理サーバと、

を含むシステムにおいて、

20

前記ノードが、グループ署名が付与されたデータを送信するステップと、

前記管理サーバが、前記グループ署名が付与されたデータを受信するステップと、

前記管理サーバが、前記受信したデータを前記台帳に追記するステップと、

前記複数の管理サーバのうち少なくとも 1 つの管理サーバによる前記台帳へのデータの追記を、他の管理サーバの台帳に反映するステップと、

を含む、データ管理方法。

【請求項 15】

他の管理サーバと相互に直接接続され、ノードから受信したデータを管理するための台帳を有する管理サーバに搭載されたコンピュータに実行させるプログラムであって、

前記ノードが送信する、グループ署名が付与されたデータを受信する処理と、

30

前記受信したデータを前記台帳に追記する処理と、

前記他の管理サーバの台帳へのデータの追記を、自装置の台帳に反映する処理と、

を実行させるプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

(関連出願についての記載)

本発明は、日本国特許出願：特願 2016-150100 号（2016 年 7 月 29 日出願）の優先権主張に基づくものであり、同出願の全記載内容は引用をもって本書に組み込み記載されているものとする。

40

本発明は、システム、データ管理方法及びプログラムに関する。特に、複数のノードが含まれ、各ノードのそれぞれがデータを送信するシステム、データ管理方法及びプログラムに関する。

【背景技術】

【0002】

ネットワーク技術、情報処理技術の向上により、競合関係にあるような複数の企業が連携し、利便性の高いサービスの提供を行うことがある。上記サービスの一例として、スマートフォン等の端末を用いたタクシー配車システムが挙げられる。タクシー配車システムには複数のタクシー会社が参加し、各タクシー会社のタクシーは、専用のタクシーメータ等を用いて自車の現在位置等を含むデータ（運用管理データ）を管理システム（配車サー

50

バ)に送信するように構成されている。

【0003】

管理システムは、運用管理データにより各タクシーの現在位置を把握する。また、各タクシー会社も運用管理データにアクセスし、自社のタクシーの運行状況等の把握に利用する。上記システム構成において、顧客が自身の端末を操作してタクシーの配車を依頼すると、管理システムは、サービス提供エリア内の顧客に近いタクシーを選択し、上記顧客の迎車を指示する。

【0004】

上記タクシー配車システムでは、スマートフォン等に接続したタクシーメータを使用することが想定され、既存のモバイル回線等を介して運用管理データを送受信することが求められる。その際、運用管理データを送信する主体の正当性の保証（即ち、各タクシーの認証）が必要となる。このような正当性の保証に関し、デジタル署名を使用することが考えられる。

【0005】

特許文献1には、委託者がアウトソーシング業者に会員情報を渡さずに、会員向けサービスをアウトソーシング業者に委託できるサービス提供システムが開示されている。特許文献1には、グループ署名方式を用いることによって、利用者装置が委託者装置の会員であるか否かを、委託者装置の公開情報のみで検証する、と記載されている。

【0006】

特許文献2には、ユーザ装置のグループへの登録やグループからの脱退の際における情報処理の計算量を低減したグループ署名システム、および情報処理方法を提供する、と記載されている。

【0007】

非特許文献1には、Camenisch-Grothの方式と称されるグループ署名の一方式が開示されている。また、非特許文献2には、非特許文献1にて開示されたCamenisch-Grothの方式の概要が説明されている。

【先行技術文献】

【特許文献】

【0008】

【特許文献1】特開2007-004461号公報

【特許文献2】特許第5099003号公報

【非特許文献】

【0009】

【非特許文献1】Jan Camenisch. Jens Groth. Group Signatures, "Better Efficiency and New Theoretical Aspects" SCN 2004, vol. 3352 of LNCS, pp. 120-133, 2004

【非特許文献2】佐古和恵、米沢祥子、古川潤、"セキュリティとプライバシーを両立させる匿名認証技術について"、情報処理学会誌、Vol. 47, No.4, pp.410-416, 2006.4

【発明の概要】

【発明が解決しようとする課題】

【0010】

なお、上記先行技術文献の各開示を、本書に引用をもって繰り込むものとする。以下の分析は、本発明者らによってなされたものである。

【0011】

上述のように、運用管理データを送信する主体の正当性の保証に関し、タクシーメータが運用管理データを送信する際、公開鍵基盤（PKI；Public Key Infrastructure）によるデジタル署名を添付することが考えられる。管理システムは、当該デジタル署名を検証することで、各タクシーの正当性を確認することができる。つまり、運用管理データを受け入れる管理システムは、当該運用管理データに付されたデジタル署名を検証することで、各タクシーの正当性を検証する。

【0012】

一方で、デジタル署名を用いると、自社のタクシーに関する情報が他社に知られてしまうという問題が生じ得る。各タクシー（タクシーメータ）が付与したデジタル署名の検証には、当該タクシーの公開鍵が必要となる。また、公開鍵の所有者（タクシー）がタクシー配車システムへの参加資格を有するタクシーであることが確認可能であることが求められ、上記公開鍵の電子証明書（公開鍵証明書）には少なくともタクシーの所属会社等に関する情報が含まれている必要がある。

【0013】

公開鍵が同じであればその所有者たるタクシーも同一であるので、公開鍵証明書からタクシーの所属会社が判明すると、各タクシー会社に所属するタクシーの数や運行履歴が特定され得る。例えば、デジタル署名が付与された複数の運用管理データからA社に所属すると判明した運用管理データを抽出し、且つ、抽出された運用管理データに適用された公開鍵の数を計数することで、タクシー配車システムに参加しているA社のタクシーの台数が判明する。このように、運用管理データの正当性保証にデジタル署名を用いると、運用管理データや公開鍵証明書を利用することで、競合他社が所有するタクシーの台数等が把握され得る。タクシー配車システムに参加している各タクシー会社は、本来、競合関係にあり、上記のような情報が他社に知られることは望ましくない。競合関係にあるような複数の会社、企業が連携してサービスを提供するようなシステムの場合、取得するデータの正当性検証と把握可能な情報の制限が望まれる。

【0014】

本発明は、データの正当性を検証可能としつつ、当該データから得られる情報を適切に制限する、システム、データ管理方法及びプログラムを、提供することを目的とする。

【課題を解決するための手段】

【0015】

本発明の第1の視点によれば、グループ署名が付与されたデータを送信する、複数のノードと、相互に直接接続されている、複数の管理サーバと、を含み、前記複数の管理サーバのそれぞれは、前記ノードから受信したデータを管理するための台帳を有し、前記複数の管理サーバのうち少なくとも1つの管理サーバによる前記台帳へのデータの追記は他の管理サーバの台帳に反映される、システムが提供される。

【0016】

本発明の第2の視点によれば、それぞれがグループに属する、複数のノードと、それぞれのグループに属するノードを管理する、複数のノード管理サーバと、前記複数のノードそれぞれに対し、グループ署名を生成する際に用いるメンバ証明書を発行すると共に、管理者公開鍵を公開する証明書管理サーバと、を含み、前記複数のノード管理サーバのそれぞれは、特権者公開鍵を公開し、前記ノードは、データに付与するグループ署名の生成を、少なくとも前記管理者公開鍵と前記複数のノード管理サーバのそれぞれが公開する特権者公開鍵を用いて行う、システムが提供される。

【0017】

本発明の第3の視点によれば、複数のノードと、相互に直接接続され、前記ノードから受信したデータを管理するための台帳を有する、複数の管理サーバと、を含むシステムにおいて、前記ノードが、グループ署名が付与されたデータを送信するステップと、前記管理サーバが、前記グループ署名が付与されたデータを受信するステップと、前記管理サーバが、前記受信したデータを前記台帳に追記するステップと、前記複数の管理サーバのうち少なくとも1つの管理サーバによる前記台帳へのデータの追記を、他の管理サーバの台帳に反映するステップと、を含む、データ管理方法が提供される。

【0018】

本発明の第4の視点によれば、他の管理サーバと相互に直接接続され、ノードから受信したデータを管理するための台帳を有する管理サーバに搭載されたコンピュータに実行させるプログラムであって、前記ノードが送信する、グループ署名が付与されたデータを受信する処理と、前記受信したデータを前記台帳に追記する処理と、前記他の管理サーバの台帳へのデータの追記を、自装置の台帳に反映する処理と、を実行させるプログラムが提

10

20

30

40

50

供される。

なお、このプログラムは、コンピュータが読み取り可能な記憶媒体に記録することができる。記憶媒体は、半導体メモリ、ハードディスク、磁気記録媒体、光記録媒体等の非トランジェント（non-transient）なものとすることができる。本発明は、コンピュータプログラム製品として具現することも可能である。

【発明の効果】

【0019】

本発明の各視点によれば、データの正当性を検証可能としつつ、当該データから得られる情報を適切に制限することに寄与する、システム、データ管理方法及びプログラムが、提供される。

10

【図面の簡単な説明】

【0020】

【図1】一実施形態の概要を説明するための図である。

【図2】第1の実施形態に係るタクシー配車システムのシステム構成の一例を示す図である。

【図3】第1の実施形態に係る配車サーバのハードウェア構成の一例を示すブロック図である。

【図4】第1の実施形態に係るタクシーの概略構成の一例を示す図である。

【図5】第1の実施形態に係る配車サーバの処理構成の一例を示すブロック図である。

【図6】第1の実施形態に係る運用管理サーバの処理構成の一例を示すブロック図である。

20

【図7】第1の実施形態に係るタクシーメータの処理構成の一例を示すブロック図である。

【図8】運用管理データの一例を示す図である。

【図9】グループ署名の生成を説明するための図である。

【図10】グループ署名の生成を説明するための図である。

【図11】第1の実施形態に係る管理サーバの処理構成の一例を示すブロック図である。

【図12】管理サーバが生成するブロックの一例を示す図である。

【図13】第1の実施形態に係る管理サーバの動作の一例を示すシーケンス図である。

【図14】第1の実施形態に係るタクシー配車システムにおけるセットアップ動作の一例を示すシーケンス図である。

30

【図15】第1の実施形態に係るタクシー配車システムの運用時に係る動作の一例を示すシーケンス図である。

【図16】第2の実施形態に係るタクシー配車システムのシステム構成の一例を示す図である。

【図17】第2の実施形態に係る証明書管理サーバの処理構成の一例を示す図である。

【図18】第2の実施形態に係る運用管理サーバの処理構成の一例を示す図である。

【図19】第2の実施形態に係るグループ署名の生成を説明するための図である。

【図20】第2の実施形態に係るグループ署名の生成を説明するための図である。

40

【発明を実施するための形態】

【0021】

初めに、一実施形態の概要について説明する。なお、この概要に付記した図面参照符号は、理解を助けるための一例として各要素に便宜上付記したものであり、この概要の記載はなんらの限定を意図するものではない。

【0022】

一実施形態に係るシステムは、グループ署名が付与されたデータを送信する、複数のノード101と、相互に直接接続されている、複数の管理サーバ102と、を含む（図1参照）。複数の管理サーバ102のそれぞれは、ノード101から受信したデータを管理するための台帳を有する。複数の管理サーバ102のうち少なくとも1つの管理サーバ102による台帳へのデータの追記は他の管理サーバ102の台帳に反映される。

50

【0023】

上記一実施形態に係るシステムでは、データに付与されたグループ署名により当該データを生成した主体の正当性を検証可能としている。また、グループ署名から得られる情報は、当該グループ署名を生成した主体が属するグループ（企業、団体）に限られ、当該生成主体を一意に特定することはできない。従って、データ及びその署名から得られる情報が適切に制限される。

【0024】

以下に具体的な実施の形態について、図面を参照してさらに詳しく説明する。なお、各実施形態において同一構成要素には同一の符号を付し、その説明を省略する。

【0025】

〔第1の実施形態〕

第1の実施形態に係るシステムについて、図面を用いてより詳細に説明する。第1の実施形態では、タクシー配車システムを例に取り説明する。しかし、本願開示が適用可能なシステムをタクシー配車システムに限定する趣旨ではない。管理するデータの正当性を検証可能としつつ、当該データから得られる情報を適切に制限する必要のあるシステムであれば、どのようなシステムであってもよい。

【0026】

例えば、タクシーの配車に係るシステム以外にも、タクシーメータから取り出すことのできる走行データを活用したタクシー料金事前予測システム、タクシー料金決定システム又は所要時間予測システム等が、上記要件に該当する。

【0027】

あるいは、上記システムとして、複数の自動車メーカーが提供する、電気自動車の充電システムが挙げられる。当該充電システムでは、充電システムを利用しようとしている自動車の資格（充電システムに参加している自動車メーカーの自動車であるか否か）を検証する必要があるが、実際に充電システムを利用した自動車を特定する必要はなく、上記要件に適合する。

【0028】

〔システム構成概略〕

図2は、第1の実施形態に係るタクシー配車システムのシステム構成の一例を示す図である。図2を参照すると、タクシー配車システムは、配車サーバ10と、運用管理サーバ20-1～20- α （ α は正の整数、以下同じ）と、各タクシー会社に所属するタクシー30-1～30- β （ β は正の整数、以下同じ）と、データ管理システム40と、を含んで構成される。なお、以降の説明において、運用管理サーバ20-1～20- α のそれぞれを区別する特段の必要がない場合には、単に「運用管理サーバ20」と表記する。同様に、タクシー30-1～30- β のそれぞれを区別する特段の理由がない場合には、単に「タクシー30」と表記する。

【0029】

配車サーバ10、運用管理サーバ20及びデータ管理システム40のそれぞれは、インターネット等のネットワークを介して相互に接続されている。また、タクシー30は、モバイル回線等を利用してネットワークに接続可能に構成されている。

【0030】

配車サーバ10は、タクシー協会等に設置されるサーバである。配車サーバ10は、タクシー配車システムの主たる機能の実現を担う装置である。具体的には、配車サーバ10は、データ管理システム40により管理される運用管理データを参照し、配車の依頼を行った顧客（より正確には顧客が使用する端末）に近いタクシー30を選択する。その後、配車サーバ10は、選択したタクシーに対し、顧客の位置を指定しつつ迎車指示を行う。

【0031】

運用管理サーバ20は、複数のタクシー会社が参加するタクシー配車システムにおいて自社のタクシー30を管理するための装置である。運用管理サーバ20は、タクシー30をシステムに含まれるノードとした場合の「ノード管理サーバ」に相当する。運用管理サ

10

20

30

40

50

サーバ20は、自社のタクシー30がタクシー配車システムに参加するのに（システムのメンバーとなるのに）必要な手続、準備を行う。具体的には、運用管理サーバ20は、自社のタクシー30が運用管理データをデータ管理システムに送信する際に付与するグループ署名に必要な情報の生成等を行う。また、運用管理サーバ20は、データ管理システム40が提供する電子掲示板に格納されている運用管理データを参照し、自社のタクシーに関する運用状況を管理する機能も有する。

【0032】

タクシー30は、上記ノード101に相当する。タクシー30は、タクシー配車システムに参加している複数のタクシー会社（グループ）のうち、いずれかのタクシー会社に属している。

10

【0033】

タクシー30には、スマートフォン等の端末を利用するタクシーメータが搭載されている。当該タクシーメータは、運用管理データを生成し、当該生成したデータをデータ管理システム40に向けて送信する。その際、タクシーメータは、当該送信する運用管理データにグループ署名を付与してデータ管理システム40に送信する。また、タクシーメータは、配車サーバ10から自車向けの迎車指示を取得すると、当該迎車指示をディスプレイに表示し、運転手に通知する。

【0034】

データ管理システム40は、タクシー協会や各タクシー会社から独立した立場の機関等が運営するシステムである。データ管理システム40は、外部（第3者）に対し追記及び読み出しの可能な電子掲示板を提供するシステムである。データ管理システム40は、所謂、ブロックチェーンにより運用管理データを初めとした各種情報を管理する。

20

【0035】

データ管理システム40は、所定の手数料を支払うことで、どのような主体でも情報を追記できると共に、書き込まれた情報を読み出すことができ、且つ、一度書き込まれた情報は消去されたり改ざんされたりすることのない電子掲示板を提供する。より正確には、データ管理システム40は、外部装置からは電子掲示板のように扱うことのできるデータ入出力に係るインターフェイスを提供するシステムである。

【0036】

図2に示すタクシー配車システムでは、タクシーの配車に必要な情報（即ち、運用管理データ）の授受を、データ管理システム40が提供する電子掲示板を介して行う。なお、上述のように、データ管理システム40は、第3者に電子掲示板を提供するシステムであるため、当該電子掲示板には上記運用管理データとは無関係なデータ（例えば、タクシーの配車とは無関係な商品売上データ等）が混在することとなる。

30

【0037】

データ管理システム40は、複数の管理サーバ50-1～50-4から構成されている。なお、図2の例示は、データ管理システム40を構成する管理サーバの台数を4台に限定する趣旨ではない。データ管理システム40は2台以上の管理サーバを含んで構成されていればよい。また、運用管理サーバ20等と同様に、管理サーバ50-1～50-4を区別する特段の理由がない場合には、単に「管理サーバ50」と表記する。

40

【0038】

データ管理システム40をなす複数の管理サーバ50は、図2に示すように、相互に直接接続されている。即ち、データ管理システム40は、P2P（Peer to Peer）接続された複数の管理サーバ50を含んで構成される。

【0039】

データ管理システム40では、P2P接続された複数の管理サーバ50それぞれが、外部から受信したデータ（運用管理データや売上データ等）を管理するための台帳（以下、データ管理台帳と表記する）を有する。データ管理システム40は、当該データ管理台帳を複数の管理サーバ50に分散し共有し、管理する。

【0040】

50

以降の説明において、データ管理システム４０とその外部とのデータの授受は、データ管理システム４０と、配車サーバ１０、運用管理サーバ２０及びタクシー３０の間に限って説明する。但し、実際には、データ管理システム４０は、汎用的な電子掲示板を広く第三者に提供するものであるため、配車サーバ１０等以外との間でもデータの授受が行われる。

【００４１】

[ハードウェア構成]

次に、第１の実施形態に係るタクシー配車システムを構成する各種装置のハードウェア構成を説明する。図３は、第１の実施形態に係る配車サーバ１０のハードウェア構成の一例を示すブロック図である。

10

【００４２】

配車サーバ１０は、情報処理装置（コンピュータ）により構成可能であり、図３に例示する構成を備える。例えば、配車サーバ１０は、内部バスにより相互に接続される、ＣＰＵ（Central Processing Unit）１１、メモリ１２、入出力インターフェイス１３及び通信手段であるＮＩＣ（Network Interface Card）１４等を備える。

【００４３】

但し、図３に示す構成は、配車サーバ１０のハードウェア構成を限定する趣旨ではない。配車サーバ１０は、図示しないハードウェアを含んでもよいし、必要に応じて入出力インターフェイス１３を備えていなくともよい。また、配車サーバ１０に含まれるＣＰＵ等の数も図３の例示に限定する趣旨ではなく、例えば、複数のＣＰＵが配車サーバ１０に含まれていてもよい。

20

【００４４】

メモリ１２は、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）、補助記憶装置（ハードディスク等）である。

【００４５】

入出力インターフェイス１３は、図示しない表示装置や入力装置のインターフェイスとなる手段である。表示装置は、例えば、液晶ディスプレイ等である。入力装置は、例えば、キーボードやマウス等のユーザ操作を受け付ける装置である。

【００４６】

配車サーバ１０の機能は、後述する各種処理モジュールにより実現される。当該処理モジュールは、例えば、メモリ１２に格納されたプログラムをＣＰＵ１１が実行することで実現される。また、そのプログラムは、ネットワークを介してダウンロードするか、あるいは、プログラムを記憶した記憶媒体を用いて、更新することができる。さらに、上記処理モジュールは、半導体チップにより実現されてもよい。即ち、上記処理モジュールが行う機能を何らかのハードウェア、及び／又は、ソフトウェアで実行する手段があればよい。

30

【００４７】

なお、運用管理サーバ２０や管理サーバ５０も配車サーバ１０と同様に情報処理装置により構成可能であり、その基本的なハードウェア構成は配車サーバ１０と相違する点はないので説明を省略する。

40

【００４８】

図４は、タクシー３０の概略構成の一例を示す図である。図４に示すように、タクシー３０には、スマートフォン３２を利用したタクシーメータ３１が含まれる。タクシーメータ３１とスマートフォン３２は、Bluetooth（登録商標）等の近距離無線通信やケーブルを利用した有線接続により相互に通信可能に構成されている。タクシーメータ３１は、スマートフォン３２と通信することにより、そのハードウェア（例えば、モバイル回線へのアクセス手段やＧＰＳ（Global Positioning System）機能）を利用する。

【００４９】

なお、図４には、タクシーメータ３１やスマートフォン３２を図示しているが、タクシー（車両）としての機能を実現するハードウェアの図示は省略している。また、タクシー

50

メータ 3 1 やスマートフォン 3 2 のハードウェアは実質的に情報処理装置（コンピュータ）と同様とすることができ、当業者にとって明らかでもあるのでその説明を省略する。

【0050】

[配車サーバ]

次に、配車サーバ 1 0 の詳細について説明する。

【0051】

図 5 は、第 1 の実施形態に係る配車サーバ 1 0 の処理構成の一例を示すブロック図である。図 5 を参照すると、配車サーバ 1 0 は、通信制御部 2 0 1 と、記憶部 2 0 2 と、配車処理部 2 0 3 と、を含んで構成される。

【0052】

通信制御部 2 0 1 は、他の装置との間の通信を実現する手段である。通信制御部 2 0 1 は、他の装置から受信したメッセージ（パケット）を各処理モジュール部に振り分ける、又は、各処理モジュール部から取得したメッセージを他の装置に送信する手段でもある。

【0053】

記憶部 2 0 2 は、例えば、配車処理部 2 0 3 の処理等に必要データを記憶する。

【0054】

配車処理部 2 0 3 は、顧客からの配車依頼を処理する手段である。配車処理部 2 0 3 は、顧客からの配車依頼を受信すると、データ管理システム 4 0 から運用管理データを取得する。例えば、配車処理部 2 0 3 は、過去の所定時刻から現在までの所定期間の間に電子掲示板に格納された運用管理データの読み出し依頼をデータ管理システム 4 0 に行い、運用管理データを取得する。あるいは、配車処理部 2 0 3 は、取得するデータ量を指定して運用管理データの読み出し依頼をデータ管理システム 4 0 に行ってもよい。配車処理部 2 0 3 は、取得した運用管理データに基づいて、顧客の元に向かわせるタクシー 3 0 を決定し、当該タクシー 3 0 に対して迎車指示を行う。

【0055】

配車処理部 2 0 3 は、署名検証部 2 1 1 と迎車決定部 2 1 2 の 2 つのサブモジュールを備える。

【0056】

署名検証部 2 1 1 は、データ管理システム 4 0 から取得する運用管理データに付与されているグループ署名の検証を行う手段である。後述するように、各タクシー会社の運用管理サーバ 2 0 は、管理者公開鍵及び特権者公開鍵を公開するので、署名検証部 2 1 1 は、各タクシー会社の公開鍵（管理者公開鍵、特権者公開鍵）を用いて運用管理データに付与されているグループ署名の検証を行う。なお、グループ署名の検証は、非特許文献 2 の図 7 に示される「グループ署名検証アルゴリズム」に従って行うことができる。

【0057】

検証の結果、運用管理データの正当性が確認できた場合には、署名検証部 2 1 1 は、当該データを迎車決定部 2 1 2 に引き渡す。検証の結果、運用管理データの正当性が確認できない場合には、署名検証部 2 1 1 は、当該データを破棄する。署名検証部 2 1 1 は、上記の様な検証処理を取得した運用管理データに対して実施し、正当性が確認できたデータを迎車決定部 2 1 2 に引き渡す。

【0058】

迎車決定部 2 1 2 は、正当性が確認できた運用管理データを用いて、迎車指示を出すタクシー 3 0 を決定する手段である。例えば、迎車決定部 2 1 2 は、配車依頼を行った顧客の現在位置と、運用管理データに含まれるタクシー 3 0 の現在位置と、を比較し、顧客に最も近い現在地を含む運用管理データを特定する。後述するように、運用管理データには各タクシー 3 0 のメッセージ通知先（例えば、メールアドレス）が含まれるため、迎車決定部 2 1 2 は、特定した運用管理データから得られる通知先に対して迎車指示を行う。その際、迎車決定部 2 1 2 は、上記迎車指示に顧客の現在位置を含ませる。

【0059】

[運用管理サーバ]

次に、運用管理サーバ２０の詳細について説明する。

【００６０】

第１の実施形態に係る運用管理サーバ２０は、グループのメンバ（タクシー３０）に配布するメンバ証明書を発行する機能と、運用管理データを生成したタクシー３０を特定する機能と、を備える。つまり、第１の実施形態に係る運用管理サーバ２０は、非特許文献２に記載された「管理者」として役割と「特権者」としての役割を備える。

【００６１】

図６は、第１の実施形態に係る運用管理サーバ２０の処理構成の一例を示すブロック図である。図６を参照すると、運用管理サーバ２０は、通信制御部３０１と、記憶部３０２と、証明書管理部３０３と、を含んで構成される。なお、図６において、自グループに属するタクシー３０の運行状況を確認するための機能モジュールは図示を省略している。

10

【００６２】

通信制御部３０１は、他の装置との間の通信を実現する手段である。通信制御部３０１は、他の装置から受信したメッセージ（パケット）を各処理モジュール部に振り分ける、又は、各処理モジュールから取得したメッセージを他の装置に送信する手段でもある。

【００６３】

記憶部３０２は、証明書管理部３０３による鍵生成やメンバ証明書の生成に必要な情報を記憶する。

【００６４】

証明書管理部３０３は、自社のタクシー３０が運用管理データに付与するグループ署名を生成するために必要な情報の生成、管理を行う手段である。証明書管理部３０３は、鍵生成部３１１と証明書生成部３１２の２つのサブモジュールを備える。

20

【００６５】

鍵生成部３１１は、グループ署名に用いる、管理者公開鍵と管理者秘密鍵によるペアと、特権者公開鍵と特権者秘密鍵によるペアを生成する。鍵生成部３１１は、管理者公開鍵と特権者公開鍵を公開する。公開された管理者公開鍵は、少なくとも配車サーバ１０により取得される。また、特権者公開鍵は、少なくとも自社の各タクシー３０及び配車サーバ１０により取得される。

【００６６】

証明書生成部３１２は、自社のタクシー３０がグループ署名を生成する際に必要となる「メンバ証明書」を生成し、発行する手段である。証明書生成部３１２は、後述するタクシーメータ３１の証明書取得部４０３と協働してメンバ証明を生成し、生成したメンバ署名書をタクシー３０に配布する。具体的には、非特許文献２の図５に示される「ユーザ登録プロトコル」に従うことにより、各タクシー３０は、自身の公開鍵、秘密鍵、さらにその公開鍵の正当性を管理者秘密鍵によって保証するメンバ証明書を入手する。

30

【００６７】

[タクシー]

次に、タクシー３０の詳細について説明する。

【００６８】

上述のように、タクシー３０がタクシー配車システムに参加するための機能は、タクシーメータ３１により実現される。そのため、以下、タクシーメータ３１の処理構成について説明する。

40

【００６９】

図７は、第１の実施形態に係るタクシーメータ３１の処理構成の一例を示すブロック図である。図７を参照すると、タクシーメータ３１は、通信制御部４０１と、記憶部４０２と、証明書取得部４０３と、運用管理データ処理部４０４と、を含んで構成される。

【００７０】

通信制御部４０１は、スマートフォン３２との間の通信を制御し、他の装置との間の通信を実現する手段である。通信制御部４０１は、他の装置から受信したメッセージ（パケット）を各処理モジュール部に振り分ける、又は、各処理モジュールから取得したメッセ

50

ージを他の装置に送信する手段でもある。

【0071】

記憶部402は、グループ署名の生成等に必要データを記憶する。

【0072】

証明書取得部403は、運用管理サーバ20の証明書生成部312と協働してメンバ証明書を作成し、運用管理サーバ20からメンバ証明書を取得する手段である。なお、運用管理サーバ20から取得したメンバ証明書は記憶部402に格納される。証明書取得部403は、メンバ証明書を生成する際に必要となる鍵（秘密鍵）を生成する。

【0073】

運用管理データ処理部404は、運用管理データを生成し、当該生成した運用管理データをデータ管理システム40に送信する手段である。

【0074】

運用管理データ処理部404は、運用管理データ生成部411とグループ署名生成部412の2つのサブモジュールを備える。

【0075】

運用管理データ生成部411は、運用管理データを生成する手段である。運用管理データには、少なくとも自車の現在位置と、メッセージ通知先（例えば、メールアドレス）が把握可能な情報が含まれる。例えば、図8に示すように、顧客を乗せた場所に関する情報（乗車位置）、顧客を降ろした場所に関する情報（降車位置）、自車の現在位置に関する情報、迎車指示を送信するメッセージ通知先に関する情報等が、運用管理データに含まれる。なお、運用管理データから当該データの生成主体が特定されることを困難とするため、メッセージ通知先には所定期間に限り使える使い捨てのメールアドレス等を用いるのが好ましい。

【0076】

なお、図8において、運用管理データに「降車位置」と「現在位置」が含まれるのは、降車位置と現在位置が一致しない場合を考慮した結果である。また、図8に示す運用管理データは例示であって、運用管理データの内容を制限する趣旨ではない。例えば、乗車位置や降車位置に関する情報が運用管理データに含まれていなくてもよいし、他の情報（例えば、顧客の乗車、降車に関する時刻や走行距離等）が含まれていてもよい。

【0077】

運用管理データ生成部411は、運用管理データに記載する「位置」に関する情報を、例えば、スマートフォン32に内蔵されたGPSにより取得する。運用管理データ生成部411は、例えば、運転手が顧客を乗せた旨の操作をタッチパネル等に行うと、スマートフォン32のGPSにより得られる位置情報を乗車位置に設定する。

【0078】

なお、運用管理データを生成するタイミングは種々のものが考えられる。例えば、運用管理データ生成部411は、所定時刻や所定の間隔にて、運用管理データを生成してもよいし、顧客を降ろしたタイミングにて運用管理データを生成してもよい。つまり、運用管理データが定期的に生成されるようにしてもよいし、顧客を降ろす等のイベントを契機として運用管理データが生成されるようにしてもよい。運用管理データ生成部411は、生成した運用管理データをグループ署名生成部412に引き渡す。

【0079】

グループ署名生成部412は、送信するメッセージ（運用管理データ）に付与するグループ署名を生成する手段である。グループ署名生成部412は、証明書取得部403が生成した秘密鍵、自社の運用管理サーバ20から取得したメンバ証明書及び特権者公開鍵によりグループ署名を生成する。なお、グループ署名の生成は、非特許文献2の図6に示される「グループ署名作成アルゴリズム」に従って行うことができる。

【0080】

グループ署名の生成が終了すると、運用管理データ処理部404は、生成された運用管理データにグループ署名を付与して、データ管理システム40に送信する（電子掲示板へ

10

20

30

40

50

の追記を依頼する)。なお、その際、運用管理データ処理部404は、運用管理データに、当該データがタクシー配車システムにて用いられることを識別する識別子を付与する。

【0081】

上述のように、メンバ証明書の発行、グループ署名の作成及びグループ署名の検証等は、非特許文献2に開示されたアルゴリズム、プロトコルを使用することができ、また、これらのアルゴリズム等の更なる詳細は非特許文献1の開示を参考にすることができる。ここでは、図面を参照しつつ、非特許文献2の記載に準拠してタクシー配車システムにグループ署名を導入する際の概略動作を説明する。

【0082】

なお、本願開示の数式に用いられる記号を下記のとおりとする。

10

N：2素数の積

A、a、b：剰余環の現

g、u：素数体の元

H：ハッシュ関数

c：ハッシュ値

P、p、q：素数

r、s、x、v、ρ、τ：乱数

k：整数

【0083】

図9を参照すると、タクシー会社それぞれが1つのグループとして扱われる。1つのグループ（タクシー会社）には、複数のメンバ（タクシー）が所属している。各タクシー会社の運用管理サーバ20は、タクシー配車システムに参加する際に、管理者公開鍵と管理者秘密鍵によるペアと、特権者公開鍵と特権者秘密鍵のペアを生成する。

20

【0084】

ここでは、管理者公開鍵、特権者公開鍵、管理者秘密鍵及び特権者秘密鍵を以下の式(1)～(4)のように定める。

管理者公開鍵： $gpk_1 = (N, a_0, a_1, a_2, k_e, H) \dots (1)$

特権者公開鍵： $gpk_2 = (g_1, g_2, g_3, P, q) \dots (2)$

管理者秘密鍵： $(p_1, p_2) \text{ s.t. } N = p_1 p_2 \dots (3)$

特権者秘密鍵： $y \text{ s.t. } g_2 = g_1^y \text{ mod } P \dots (4)$

30

【0085】

各タクシー会社（運用管理サーバ20）は、管理者公開鍵と特権者公開鍵を公開する。また、各タクシー会社に属するタクシー30それぞれには、識別子（ID；Identification）が割り振られている。

【0086】

上述のように、各タクシー会社（運用管理サーバ20）とタクシー30との間でメンバ登録（ユーザ登録）に係る処理が実行される。

【0087】

ここでは、ユーザ公開鍵と秘密鍵を以下の式(5)、(6)のように定める。

ユーザ公開鍵： $h = g_2^x \text{ mod } P \dots (5)$

40

ユーザ秘密鍵： $(x, r) \text{ s.t. } a_0 a_1^x a_2^r = A^e \text{ mod } N \dots (6)$

【0088】

各タクシー30の証明書取得部403は、上記(6)式に示すような秘密鍵を生成し、当該生成した秘密鍵から変換した情報を生成する。具体的には、証明書取得部403は、非特許文献2に記載されたように、x、r'をランダムに選択し、下記の式(7)に示す情報を生成する。

$A' \leftarrow a_1^x a_2^{r'} \text{ mod } N \dots (7)$

証明書取得部403は、上記(7)に示す情報（秘密鍵を変換した情報）と、上記(5)に示す公開鍵を運用管理サーバ20に送信する。運用管理サーバ20の証明書生成部31

50

2は、非特許文献2の図5に記載されたプロトコルに従い、下記の式(8)に示すメンバ証明書を生成する。

メンバ証明書：(A、e)・・・(8)

【0089】

各タクシー30は、グループ署名生成のために、運用管理サーバ20から発行されたメンバ証明書と上記生成した秘密鍵を準備する。例えば、ID=i(iは正の整数、以下同じ)のタクシー30は、メンバ証明書(Ai、ei)と秘密鍵sk(i)を準備する。各タクシーに送信されたメンバ証明書(Ai、ei)と秘密鍵sk(i)が、各タクシー30に関するグループ署名生成用秘密鍵sk(gs)となる。なお、以降の説明において、ID=iのタクシーをタクシー(i)と表記する。

10

【0090】

タクシー(i)のグループ署名生成部412は、グループ署名を生成する。例えば、図10を参照すると、上記メンバ証明書(Ai、ei)を有するタクシー(i)は、グループ署名生成の際に、運用管理データであるメッセージMに対しグループ署名生成用秘密鍵sk(gs)及び特権者公開鍵を適用しグループ署名sig(i、M)を生成する。

【0091】

より具体的には、グループ署名生成部412は、s、vをランダムに選択した上で、下記の式(9)及び(10)に示す情報を計算する。

$$b \leftarrow a_2^{s \cdot A} \bmod N \quad \dots (9)$$

$$(u_1, u_2, u_3) \leftarrow (g_1^v, h g_2^v, g_3^{v+e'}) \bmod P \quad \dots (10)$$

20

【0092】

次に、グループ署名生成部412は、 ρ_x 、 ρ_r 、 ρ'_e 、 ρ_v をランダムに選択した上で、下記の式(11)～(16)によりグループ署名を得る。

$$\bar{b} \leftarrow b^{\rho'_e} a_1^{-\rho_x} a_2^{-\rho_r} \bmod N \quad \dots (11)$$

$$(\bar{u}_1, \bar{u}_2, \bar{u}_3) \leftarrow (g_1^{\rho_v}, g_2^{\rho_v + \rho_x}, g_3^{\rho_v + \rho'_e}) \bmod P \quad \dots (12)$$

30

$$c = H(gpk_1, gpk_2, b, u_1, u_2, u_3, \bar{b}, \bar{u}_1, \bar{u}_2, \bar{u}_3, M) \quad \dots (13)$$

$$\tau_x = \rho_x + c x, \tau_r = \rho_r + c(r + se) \quad \dots (14)$$

$$\tau'_e = \rho'_e + c e', \tau_v = \rho_v + c v \bmod q \quad \dots (15)$$

$$Sig = (b, u_1, u_2, u_3, c, \tau_x, \tau_r, \tau'_e, \tau_v) \quad \dots (16)$$

【0093】

このグループ署名は、タクシー(i)がタクシー会社の管理者公開鍵に対応する正しい管理者秘密鍵を持つ主体が発行するメンバ証明書を所有しており、さらに、特権者公開鍵に対応する正しい特権者秘密鍵を持つ主体により、正しくメンバ証明書を特定できることを保証するゼロ知識証明機能を持つものになっている。

40

【0094】

続いて、グループ署名を用いた検証及び追跡の概略について説明する。上述のように、配車サーバ10の署名検証部211は、運用管理データに付与されているグループ署名の検証を行う。具体的には、署名検証部211は、各タクシー会社により公開された管理者公開鍵と特権者公開鍵を用いて、グループ署名を検証する。より具体的には、署名検証部211は、下記の式(17)～(19)が成立するか否かによりグループ署名の検証を行う。

$$\bar{b} \leftarrow b^c a_0^{2^{k+e+r'e}} a_1^{-e} a_2^{-\tau_x} \bmod N \quad \dots (17)$$

50

$$(\overline{u}_1, \overline{u}_2, \overline{u}_3) \leftarrow (u_1^{-c} g_1^{\tau_v}, u_2^{-c} g_2^{\tau_v + \tau_x}, u_3^{-c} g_3^{\tau_v + \tau_e}) \bmod P \quad \cdots (18)$$

$$c = H(gpk_1, gpk_2, b, u_1, u_2, u_3, \overline{b}, \overline{u}_1, \overline{u}_2, \overline{u}_3, M) \quad \cdots (19)$$

【0095】

例えば、A社の管理者公開鍵と特権者公開鍵により、グループ署名の正当性が保証されれば、当該グループ署名が付された運用管理データは、タクシー配車システムに参加しているA社の正当な一員であることが判明する。さらに、A社は、グループ署名から自社に所属するいずれのタクシーが生成した運用管理データか特定できる（自社のタクシーを特定できる）。

10

【0096】

このように、管理者公開鍵と特権者公開鍵によるグループ署名の検証により、運用管理データを電子掲示板に書き込んだタクシー30が、システム上の正当な資格を有するタクシー会社の一員であるか否か判明する。しかし、上記検証だけでは、配車サーバ10等は、運用管理データを電子掲示板に書き込んだタクシー30を特定することができない。つまり、グループ署名を使用することで、配車サーバ10等が把握可能な情報は、運用管理データを電子掲示板に書き込んだタクシー30の正当性に関する情報に制限される。また、このように情報が制限されたとしても、配車サーバ10は、運用管理データの正当性が確認でき（システムへの正当な参加資格を有するタクシー会社の一員であることが保証され）、且つ、タクシー30の現在位置とメッセージ通知先が把握できれば、システムの運用には支障がない。

20

【0097】

対して、グループの管理者たるタクシー会社では、特権者秘密鍵を用いることで、当該グループ署名を付与したタクシー30を一意に特定できる。具体的には、タクシー会社の運用管理サーバ20は、下記の式(20)を計算することで、グループ署名を生成したタクシー30を特定できる。

$$h = u_2 / u_1^y \quad \cdots (20)$$

【0098】

タクシー会社（運用管理サーバ20）は、グループ署名に含まれるデータを、特権者秘密鍵を用いて変換すると、各タクシー30のメンバ証明書を取り出すことができる。タクシー会社は、この取り出したメンバ証明書から、タクシー30のIDを特定することができる。つまり、タクシー会社は、データ管理システム40から運用管理データを取得し、グループ署名から当該運用管理データを送信したタクシー30を一意に特定できる（メンバの追跡ができる）。その結果、タクシー会社は、自社のタクシー30それぞれについて、運行状況、稼働状況等の詳細を知ることができる。

30

【0099】

[管理サーバ]

次に、データ管理システム40をなす管理サーバ50の詳細について説明する。

【0100】

図11は、第1の実施形態に係る管理サーバ50の処理構成の一例を示すブロック図である。図11を参照すると、管理サーバ50は、通信制御部501と、記憶部502と、台帳管理部503と、を含んで構成される。

40

【0101】

通信制御部501は、他の装置との間の通信を実現する手段である。通信制御部501は、他の装置から受信したメッセージ（パケット）を各処理モジュール部に振り分ける、又は、各処理モジュール部から取得したメッセージを他の装置に送信する手段でもある。

【0102】

記憶部502は、各処理モジュールの処理に必要な情報を記憶する手段である。記憶部502には、データを一時的に記憶する一時記憶領域とデータ管理台帳を記憶する領域が

50

含まれる。

【0103】

台帳管理部503は、電子掲示板への配車サーバ10やタクシー30からのアクセス要求を処理する手段である。具体的には、例えば、タクシー30から電子掲示板への運用管理データの書き込み要求を受け付けると、記憶部502に格納されているデータ管理台帳に運用管理データを追記する。また、台帳管理部503は、外部装置から電子掲示板の読み出しに係る要求を受け付けると、当該要求に付随する識別子（タクシー配車システム用のデータを示す識別子）をキーとしてデータ管理台帳を検索し、当該識別子が付されたデータ（即ち、運用管理データ）を抽出する。その際、台帳管理部503は、運用管理データの読み出し範囲が指定されている場合には、当該読み出し範囲に適合する運用管理データを抽出する。台帳管理部503は、抽出した運用管理データを配車サーバ10等へ送信する。

10

【0104】

台帳管理部503は、ブロック生成部511とブロック検証部512の2つのサブモジュールを有する。

【0105】

ブロック生成部511は、データ管理台帳を他の管理サーバ50にて共有し、管理するためのブロックを生成する。

【0106】

台帳管理部503は、タクシー30等から運用管理データを取得すると、当該取得した運用管理データを記憶部502の一時記憶領域に保存する。その後、ブロック生成部511は、直前に生成されたブロックのヘッダと、当該一時記憶領域に保存されたデータ（例えば、運用管理データや売上データ；データ管理台帳への追記データ）から、「正当性保証データ」を生成する。例えば、ブロック生成部511は、追記データ、前ブロックのヘッダ及び正当性保証データのハッシュ値を計算すると、当該計算されたハッシュ値を所定の規則に適合するものにする値（所謂、ノンス値又はナンス値）を正当性保証データとして生成する。また、正当性保証データには、ブロックを生成した管理サーバ50の電子署名が含まれる。

20

【0107】

ブロック生成部511は、直前に生成されたブロックのヘッダと上記の正当性保証データからなるヘッダを有するブロックを生成する。具体的には、図12に示すようなブロックが生成される。

30

【0108】

ブロック生成部511によるブロック生成が終了すると、当該ブロックはデータ管理台帳に追記される。また、ブロック生成部511は、生成したブロックを、通信制御部501を介して他の管理サーバ50に配布（送信）する。

【0109】

他の管理サーバ50から上記ブロックを受信した管理サーバ50の通信制御部501は、取得したブロックをブロック検証部512に引き渡す。

【0110】

ブロック検証部512は、自装置の記憶部502に格納されているデータ管理台帳（ブロック）に基づき、他の管理サーバ50が送信するブロックの正当性を検証する手段である。具体的には、ブロックを受信した管理サーバ50のブロック検証部512は、当該受信したブロックの正当性を、ブロックを送信した管理サーバ50が生成したブロックと自装置（ブロックを受信した管理サーバ50）が管理している直前に生成されたブロックのヘッダを用いて検証する。

40

【0111】

初めに、ブロック検証部512は、受信したブロックに含まれる正当性保証データに送信元となる管理サーバ50の電子署名が付与されていることを確認し、受信したブロックに記載された「前ブロックのヘッダ」を自身が管理するデータ管理台帳に基づき特定する

50

。その後、ブロック検証部 5 1 2 は、受信したブロック内の追記データと前ブロックのヘッダを入力として、ヘッダ内の正当性保証データの整合がとれているか否か（正当性保証データが所定の規則に適合するか否か）を確認する。

【0 1 1 2】

ブロック検証部 5 1 2 は、正当性保証データの整合性が確認できれば、他の管理サーバ 5 0 が送信するブロックは正当であると判定する。一方、正当性保証データの整合性が確認できなければ、ブロック検証部 5 1 2 は、他の管理サーバ 5 0 が送信するブロックは不当であると判定する。

【0 1 1 3】

ブロック検証部 5 1 2 が、他の管理サーバ 5 0 が送信するブロックが正当であると判定した場合には、台帳管理部 5 0 3 は、記憶部 5 0 2 のデータ管理台帳を更新する（追記データを含むブロックを追記する）。つまり、ブロック検証部 5 1 2 は、他の管理サーバ 5 0 の台帳へのデータの追記を、自装置の台帳に反映する処理を行う。なお、ブロック検証部 5 1 2 は、他の管理サーバ 5 0 が送信するブロックが不当であると判定した場合には、当該ブロックを破棄する。

【0 1 1 4】

また、ブロック検証部 5 1 2 は、検証結果（受信したブロックは正当、不当）に関する情報を、ブロックを送信してきた管理サーバ 5 0 に通知する。

【0 1 1 5】

管理サーバ 5 0 の動作をまとめると図 1 3 に示すシーケンス図のとおりとなる。なお、図 1 3 には、管理サーバ 5 0 - 1 がタクシー 3 0 から運用管理データを取得し、当該データをデータ管理台帳に追記する場合を示す。

【0 1 1 6】

管理サーバ 5 0 - 1 は、タクシー 3 0 から運用管理データを取得すると（ステップ S 1 0 1）、当該データを自装置の記憶部 5 0 2 の一部記憶領域に複製する（ステップ S 1 0 2）。

【0 1 1 7】

その後、一部記憶領域に複製されたデータが所定量蓄積される等の条件により、管理サーバ 5 0 - 1 は、一時記憶領域に記憶された運用管理データに基づき、上述のブロックを生成する（ステップ S 1 0 3）。その後、管理サーバ 5 0 - 1 は、生成したブロックを他の管理サーバ 5 0 - 2 ～ 5 0 - 4 に向けて送信する（ステップ S 1 0 4）。

【0 1 1 8】

ブロックを受信した管理サーバ 5 0 - 2 ～ 5 0 - 4 のそれぞれは、管理サーバ 5 0 - 1 が生成したブロックを個別に検証する（ステップ S 1 0 5）。管理サーバ 5 0 - 2 ～ 5 0 - 4 のそれぞれは、ブロックの正当性が確認できた場合に自装置のデータ管理台帳を更新する（ステップ S 1 0 6）。このように、データ管理システム 4 0 をなす複数の管理サーバ 5 0 のうちの少なくとも 1 つの管理サーバ 5 0 によるデータ管理台帳へのデータの追記は、他の管理サーバ 5 0 のデータ管理台帳に反映される。

【0 1 1 9】

なお、他の管理サーバ 5 0 から送信されたブロックの正当性が確認できない場合には、当該ブロックを破棄すると共に、管理サーバ 5 0 はその旨を、ブロックを送信する管理サーバ 5 0 に通知する。当該通知を受けた管理サーバ 5 0 の台帳管理部 5 0 3 は、ブロック送信前のデータ管理台帳の状態を取り戻す。

【0 1 2 0】

次に、タクシー配車システムの動作について説明する。

【0 1 2 1】

図 1 4 は、タクシー配車システムにおけるセットアップ動作の一例を示すシーケンス図である。

【0 1 2 2】

タクシー配車システムの運用開始にあたり、各タクシー会社は、上記 2 つの公開鍵秘密

10

20

30

40

50

鍵ペアを生成する（ステップS01）。その後、タクシー会社は、管理者公開鍵と特権者公開鍵を公開する。

【0123】

各タクシー30は、グループ署名の生成に必要な秘密鍵を生成する（ステップS02）。その後、各タクシー30は、生成した秘密鍵を変換した情報等をタクシー会社（運用管理サーバ20）に送信する。

【0124】

タクシー会社（運用管理サーバ20）は、取得した秘密鍵を変換した情報に対して特権者秘密鍵による署名を生成し、メンバ証明書を生成する（ステップS03）。生成したメンバ証明書は、各タクシー30に送信される。

10

【0125】

タクシー配車システムに参加するタクシー会社ごとに図14に示すセットアップ処理が実行され、システム稼働の準備が完了する。また、新たなタクシー会社がシステムに参加する際にも、当該タクシー会社に関して図14に示すセットアップ処理が実行される。

【0126】

続いて、タクシー配車システムにおける通常動作（タクシーの配車処理）について説明する。

【0127】

図15は、タクシー配車システムの運用時に係る動作の一例を示すシーケンス図である。

20

【0128】

タクシー配車システムのサービス提供エリアにあるタクシー30は、所定の条件が満たされることにより、運用管理データを生成する（ステップS11）。次に、タクシー30は、当該生成した運用管理データのグループ署名を生成する（ステップS12）。その後、タクシー30は、運用管理データにグループ署名を付与してデータ管理システム40に、当該データを送信する（ステップS13）。データ管理システム40の管理サーバ50は、当該受信した運用管理データをデータ管理台帳に追記する（ステップS14）。

【0129】

ステップS11～S14の処理が繰り返されることにより、データ管理システム40の電子掲示板には各タクシー30の現在位置を含む情報が蓄積される。

30

【0130】

配車サーバ10は、顧客の現在位置を含む配車依頼を受信すると、データ管理システム40から所定範囲の運用管理データを取得する（ステップS15）。その後、配車サーバ10は、取得した運用管理データのそれぞれについてグループ署名を検証（ステップS16）し、システムに参加しているタクシー会社に属するタクシー30が生成した運用管理データか否かを確認する。配車サーバ10は、正当性が確認できた運用管理データのなかから、配車依頼を行った顧客に近いタクシー30の現在位置を特定し、当該タクシー30に対して迎車指示を行う（ステップS17）。

【0131】

以上のように、第1の実施形態では、運用管理データの生成主体に関する正当性の判定に、グループ署名を用いている。グループ署名を用いることで、運用管理データの生成主体が、タクシー配車システムに参加する正当な資格を有するタクシー会社の一員であるか否か判定できる。また、グループ署名による検証だけでは、運用管理データを生成したタクシー30を一意に特定することはできない。このような特定が可能であるのは、グループ管理者であるタクシー会社に限られる。即ち、運用管理データの正当性を検証可能としつつ、当該データから得られる情報が適切に制限される。

40

【0132】

〔第2の実施形態〕

続いて、第2の実施形態について図面を参照して詳細に説明する。

【0133】

50

第1の実施形態では、グループ署名を使用することで、運用管理データを生成した主体が、各タクシー会社の一員であることを保証している。その際、配車サーバ10は、各タクシー会社が公開している管理者公開鍵及び特権者公開鍵を用いてグループ署名の検証を行う。

【0134】

ここで、各タクシー会社が公開している管理者公開鍵及び特権者公開鍵は、他のタクシー会社も知ることができるので、他社も運用管理データに付されたグループ署名の検証が可能である。例えば、図9を参照すると、A社の管理者公開鍵及び特権者公開鍵はB社も知ることが出来るので、A社に属するタクシー30が付与したグループ署名の検証が、A社の管理者公開鍵及び特権者公開鍵により成功すれば、B社は、当該グループ署名が付された運用管理データはA社のタクシー30により生成された事実を知ることができる。B社が、データ管理システム40に格納されている運用管理データ及びそのグループ署名に関し、上記のような検証を繰り返すことで、A社のタクシー30の運用状況が把握され得る。

10

【0135】

A社のタクシー30の運用状況が把握できれば、当該情報を分析することで、A社の営業方針等が判明する可能性がある。例えば、A社に関する、時間帯別やエリア別のタクシー稼働状況等の情報が作成できる可能性がある。

【0136】

タクシー配車システムに参加しているタクシー会社は、本来、競合関係にあるため、上記のような情報が作成できることは望ましくない。つまり、第1の実施形態では、グループ署名を使用することで、運用管理データ及びその署名から得られる情報を各タクシーの所属会社に制限したが、当該制限でも不十分である可能性がある。即ち、運用管理データの生成主体が、タクシー配車システムに参加する資格があるか否かが検証可能であれば十分であり、当該生成主体の帰属するグループ（タクシー会社）はグループ署名から把握できないことが望ましい。

20

【0137】

上記問題に対し、第2の実施形態では、グループ署名におけるメンバ登録機能（メンバ証明書発行機能）と追跡機能（自社のタクシーの識別機能）を分離することで、上記問題を解決する。具体的には、第2の実施形態では、タクシー協会がメンバ登録を行う。なお、第2の実施形態においても、第1の実施形態と同様に、各タクシー会社がグループ署名から自社のタクシーを特定できる。

30

【0138】

第2の実施形態では、図2に示すシステム構成に対し、タクシー協会等に設置される証明書管理サーバ60が追加される（図16参照）。

【0139】

図17は、第2の実施形態に係る証明書管理サーバ60の処理構成の一例を示す図である。証明書管理サーバ60は、他の装置と同様な通信制御部601と記憶部602を備える。さらに、証明書管理サーバ60は、証明書管理部603を含む。

【0140】

証明書管理部603は、鍵生成部611と証明書生成部612の2つのサブモジュールを備える。上記サブモジュールを含む証明書管理サーバ60の動作は後述する。

40

【0141】

第1の実施形態では、運用管理サーバ20にてメンバ証明書を生成していたが、当該機能は証明書管理サーバ60が担うため、第2の実施形態に係る運用管理サーバ20には証明書生成部が存在しない（図18参照）。但し、後述するように、運用管理サーバ20は、特権者公開鍵を生成し、公開する機能を有するので、第2の実施形態に係る運用管理サーバ20には、特権者公開鍵及び特権者秘密鍵を生成する鍵生成部311aが含まれる。

【0142】

次に、図面を参照しつつ、第2の実施形態に係るグループ署名の生成について説明する

50

。

【0143】

図19は、第2の実施形態に係るグループ署名の生成を説明するための図である。図19を参照すると、証明書管理サーバ60の鍵生成部611は、管理者公開鍵と管理者秘密鍵のペアを生成し、管理者公開鍵を公開する。また、各タクシー会社の運用管理サーバ20（鍵生成部311a）は、特権者公開鍵と特権者秘密鍵のペアを生成し、特権者公開鍵を公開する。

【0144】

各タクシー会社とそのタクシー30は、第1の実施形態と同様の方法により、メンバ証明書の生成及び取得を行う。

10

【0145】

タクシー30は、運用管理データに付するグループ署名を生成するが、当該グループ署名の生成方法が、第1と第2の実施形態では異なる。第1の実施形態では、運用管理データ（メッセージM）のグループ署名 $sig(i, M)$ を生成する際、メンバ証明書と自社の特権者公開鍵を用いて作成している（図10参照）。対して、第2の実施形態では、各タクシー30は、どの特権者公開鍵を使ったかを秘匿するために、すべてのタクシー会社の特権者公開鍵を入力する（図20参照）。

【0146】

グループ署名は、非特許文献2に記載されたように、「公開鍵について漏らす知識をゼロにして、正しく登録された公開鍵が暗号化されていることと、ユーザがこの公開鍵の持ち主であること」を示す技術である。そして当該技術の実現には「自分の公開鍵を暗号化し、その公開鍵にメンバ証明書が存在すること、なおかつ暗号化した人がこの公開鍵に対応する秘密鍵を持つことを証明するゼロ知識証明データ」を付与することが必要になる。しかしながら、この場合、どの特権者公開鍵を使って自分の公開鍵を暗号化したかを、検証者に伝えることが必要となる。しかし、当該事実（使用した特権者公開鍵）を伝えることによって、各タクシー30の所属先が判明してしまう。

20

【0147】

このような不都合、問題点を解消するため、第2の実施形態に係るグループ署名生成部412は、全てのタクシー会社の特権者公開鍵（図19の例では、 gpk_{2A} 、 gpk_{2B} 、・・・）を入力とし、グループ署名の生成に利用する。つまり、「自分の公開鍵を、いずれかの特権者公開鍵で暗号化し、その公開鍵にメンバ証明書が存在すること、なおかつ暗号化した人（主体）がこの公開鍵に対応する秘密鍵を持つことを証明するゼロ知識証明データ」を付与することにする。

30

【0148】

当該変更を加えることにより、どのタクシー会社に所属しているかを秘匿しつつ、タクシー協会から発行されたメンバ証明書であり、なおかつ、各タクシーの所属は該当するタクシー会社のみが特定できるグループ署名を発行することができる。

【0149】

ここで、「データがいずれかの公開鍵で暗号化したもの」であることのゼロ知識証明は、いわゆる $OR\ proof$ と呼ばれるものであり、以下のようにその構成を得ることができる。

40

【0150】

たとえば、上記第1の実施形態にて説明した式(1)～(20)に基づいてゼロ知識証明を構成すると、下記のようなになる。なお、下記の説明では、タクシー会社Aに属するタクシー30がグループ署名を生成する場合を例示する。さらに下記例示では、タクシー配車システムに参加しているタクシー会社は3社（A社、B社、C社）としている。但し、システムに含まれるタクシー会社（グループ）の数を限定する趣旨ではないことは勿論である。

【0151】

上記の式(1)～(4)に示した管理者公開鍵、特権者公開鍵、管理者秘密鍵、特権者

50

秘密鍵に関し、第2の実施形態では、特権者公開鍵及び特権者秘密鍵が第1の実施形態とは異なる。具体的には、式(2)に示す特権者公開鍵をタクシー会社の数だけ用意する。その際、式(2)に示す特権者公開鍵のうち、 (g_1, g_3, P, q) はパラメータに関する情報であり、全てのタクシー会社に共通して設定される。タクシー会社ごとに異なるのは、特権者秘密鍵に依存して生成される要素 g_2 となる。例えば、A社の特権者公開鍵を式(21)、B社の特権者公開鍵を式(22)のようにする。

A社の特権者公開鍵： $gpk_{2A} = (g_1, g_{2A}, g_3, P, q) \cdots (21)$

B社の特権者公開鍵： $gpk_{2B} = (g_1, g_{2B}, g_3, P, q) \cdots (22)$

なお、以下の説明では、式(21)に対応するタクシー会社Aの特権者秘密鍵を y_A 、式(22)に対応するタクシー会社Bの特権者秘密鍵を y_B とする。

10

【0152】

上記の式(5)に示したユーザ公開鍵(各タクシー30の公開鍵)は自社の特権者公開鍵に応じて生成される。例えば、A社のタクシー30に関するユーザ公開鍵は式(23)、B社のタクシー30に関するユーザ公開鍵は式(24)のとおりとなる。

A社タクシーの公開鍵： $h = g_{2A}^x \bmod P \cdots (23)$

B社タクシーの公開鍵： $h = g_{2B}^x \bmod P \cdots (24)$

このように、ユーザ公開鍵は、自身が属するタクシー会社の特権者公開鍵に含まれる要素 g_2 (A社；要素 g_{2A} 、B社；要素 g_{2B})を x 乗することで得られる値により生成される。

20

【0153】

なお、メンバ証明書の発行に関しては、上述のとおり第1の実施形態と同様である。但し、各タクシー30のユーザ公開鍵 h は、自身が属するタクシー会社の特権者公開鍵に含まれる要素 g_2 を x 乗することで得られる情報を含む。

【0154】

次に、上記の式(9)～(16)に示したグループ署名の生成に関し、第1及び第2の実施形態での相違点を以下のように示す。

【0155】

第1の実施形態にて説明した式(10)に関し、第2の実施形態では、 u_2 の生成に用いられる要素が第1の実施形態とは異なる。例えば、A社のタクシー30では、下記の式(25)を用いる。

30

$(u_1, u_2, u_3) \leftarrow (g_1^v, hg_{2A}^v, g_3^{v+c'}) \bmod P \cdots (25)$

なお、B社のタクシー30がグループ署名を生成する際に、上記の式(25)が計算される場合には、式(25)の g_{2A} が g_{2B} となる。

【0156】

また、第2の実施形態では、式(13)～(16)の計算において、 $\rho_x, \rho_r, \rho_e, \rho_v$ をランダムに選択することに加え、 c_B, c_C もランダムに選択し、グループ署名の計算に利用する。なお、 c_B, c_C は、下記の式(27)により計算されるハッシュ値 c をA社用のチャレンジ値 c_A 、B社用のチャレンジ値 c_B 、C社用のチャレンジ値 c_C に分割することを想定し、ランダムに選択されるものである。ここで、ゼロ知識証明は、コミット、チャレンジ、レスポンスの3つのプロセスで成り立ち、通常は、チャレンジにひとつのハッシュ値を用いる。ORproofでは、A or B or Cを証明するため、チャレンジをA用、B用、C用に分解し、どれかひとつに正しく答えられれば成立するゼロ知識証明を構成する。このために、第2の実施形態では、通常のチャレンジ値(ハッシュ値 c)を、それぞれ、タクシー会社用に分割する。第2の実施形態では、ゼロ知識証明の模倣可能という性質から、自分が証明できないチャレンジはランダムに生成し、(上記例示では、 c_B と c_C)、自分が証明できるチャレンジ(上記例示では、 c_A)はハッシュ値 c に依存して $(c - c_B - c_C)$ と計算する。さらに、ORproofを実現するために、管理者公開鍵の証明に必要なアップパー u_2 の要素を、各タクシー会社の数分重複させる。すなわち、第2の実施形態では、上記の式(12)は、下記の式(26)のと

40

50

おりとなる。

$$(\overline{u}_1, \overline{u}_{2A}, \overline{u}_{2B}, \overline{u}_{2C}, \overline{u}_3)$$

$$\leftarrow (g_1^{\rho_v}, g_{2A}^{\rho_v + \rho_x}, u_2^{-c_B} g_{2B}^{\rho_x + c_{B^X}}, u_2^{-c_C} g_{2C}^{\rho_x + c_{C^X}}, g_3^{\rho_v + \rho'_e}) \bmod P \cdots (26)$$

【0157】

上記の式(26)により得られる値は、下記の式(27)に示すようにハッシュ関数Hの入力パラメータの一部となる。

$$c = H(gpk_1, gpk_{2A}, gpk_{2B}, gpk_{2C}, b, u_1, u_2, u_3, \overline{b}, \overline{u}_1, \overline{u}_{2A}, \overline{u}_{2B}, \overline{u}_{2C}, \overline{u}_3, M) \cdots (27)$$

10

なお、上述のように、第2の実施形態では、全てのタクシー会社の特権者公開鍵がグループ署名の生成に用いられる。そのため、第1の実施形態にて説明した式(13)の特権者公開鍵 gpk_2 に替えて、各タクシー会社の特権者公開鍵 gpk_{2A} 、 gpk_{2B} 、 gpk_{2C} が上記の式(27)における入力パラメータとなる。

【0158】

また、第1の実施形態にて説明した式(14)及び式(15)から得られる τ_x 、 τ_v に替えて、第2の実施形態では、以下の式(28)、(29)から τ_{xA} 、 τ_{xB} 、 τ_{xC} 、 τ_{vA} 、 τ_{vB} 、 τ_{vC} が計算される。

20

$$\tau_{xA} = \rho_x + c_A x, \tau_{xB} = \rho_x + c_B x, \tau_{xC} = \rho_x + c_C x \cdots (28)$$

$$\tau_{vA} = \rho_v + c_A v, \tau_{vB} = \rho_v + c_B v, \tau_{vC} = \rho_v + c_C v \cdots (29)$$

なお、式(28)、(29)を含む下記の式において、 c_A は、 $c_A = c - c_B - c_C$ により求まる値である。その結果、 c_B 、 c_C など、他のタクシー会社に関する成分は知らなくても、自社の c_A に対する秘密鍵を知っていることで、各タクシーがどのタクシー会社に所属しているかを秘匿する、ORproofを構成することができる。

【0159】

上記の式(28)、(29)により算出された値を用いて、下記の式(30)により署名が生成される。

30

$$Sig = (b, u_1, u_2, u_3, c_A, c_B, c_C, \tau_{xA}, \tau_{xB}, \tau_{xC}, \tau_r, \tau'_e, \tau_{vA}, \tau_{vB}, \tau_{vC}) \cdots (30)$$

上記の式(30)と第1の実施形態にて説明した式(16)を比較すると、署名の生成に用いるパラメータ c が c_A 、 c_B 、 c_C に、 τ_x が τ_{xA} 、 τ_{xB} 、 τ_{xC} に、 τ_v が τ_{vA} 、 τ_{vB} 、 τ_{vC} に、それぞれ変更となっている。

【0160】

第2の実施形態に係る署名の検証は、以下の式(31)～(33)により行われる。

$$\overline{b} \leftarrow b^c \cdot 2^{k_e + r'_e} a_0^{-e} a_1^{-\tau_x} a_2^{-\tau_r} \bmod N \cdots (31)$$

40

$$(\overline{u}_1, \overline{u}_{2A}, \overline{u}_{2B}, \overline{u}_{2C}, \overline{u}_3) \leftarrow$$

$$(u_1^{-c_C} g_1^{\tau_v}, u_{2A}^{-c_A} g_{2A}^{\tau_{xA} + \tau_{vA}}, u_{2B}^{-c_B} g_{2B}^{\tau_{xB} + \tau_{vB}}, u_{2C}^{-c_C} g_{2C}^{\tau_{xC} + \tau_{vC}}, u_3^{-c_C} g_3^{\tau_v + \tau'_e}) \bmod P \cdots (32)$$

$$c = H(gpk_1, gpk_{2A}, gpk_{2B}, gpk_{2C}, b, u_1, u_2, u_3, \overline{b}, \overline{u}_1, \overline{u}_{2A}, \overline{u}_{2B}, \overline{u}_{2C}, \overline{u}_3, M) \cdots (33)$$

【0161】

50

第2の実施形態では、上記の式(31)～(33)の成立検証に加え、下記の式(34)が成立することを検証する。

$$c = c_A + c_B + c_C \quad \dots (34)$$

【0162】

タクシー会社Aに所属するタクシー30が生成したグループ署名に対して、当該タクシー30の特定は、下記の式(35)により行われる。

$$h = u_2 / u_1^{y_A} \quad \dots (35)$$

式(35)における y_A はタクシー会社Aの特権者秘密鍵である。

【0163】

なお、上記のようにして生成されたグループ署名の検証には、証明書管理サーバ60から公開された管理者公開鍵と、各タクシー会社が公開した特権者公開鍵を用いて検証が行える。例えば、A社のタクシー30が生成したグループ署名は、管理者公開鍵 gpk_1 とA社の特権者公開鍵 gpk_{2A} とB社の特権者公開鍵 gpk_{2B} とC社の特権者公開鍵 gpk_{2C} によって検証可能である。このように、第2の実施形態におけるグループ署名の検証には、管理者公開鍵に加えて、全てのグループの特権者が公開する特権者公開鍵が必要となるので、どの特権者公開鍵に対応するメンバ証明書を持っているのかが、秘匿される。つまり、上記グループ署名により、運用管理データを生成したタクシー30がタクシー協会に加盟しているタクシー会社に所属しているか否かに限り確認可能となる。換言するならば、上記グループ署名の検証では、当該署名を作成したタクシーの所属会社まで把握することはできない。

【0164】

また、運用管理データを生成したタクシー30を特定できるのは、グループ署名の生成に使用された特権者公開鍵とペアになる特権者秘密鍵を持つタクシー会社に限られる。つまり、各タクシー会社は、自社のタクシーにより生成されたグループ署名から、当該グループ署名及び運用管理データを生成したタクシーを一意に特定することができる。

【0165】

以上のように、第2の実施形態では、タクシー配車システムに参加するタクシー会社に属する、複数のタクシー30を1つのグループと捉え、タクシー会社の上位組織であるタクシー協会が、各タクシー30のメンバ証明書を発行する。当該メンバ証明書とタクシー配車システムに参加する全てのタクシー会社が公開する特権者公開鍵を用いて生成されたグループ署名は、タクシー協会が公開する管理者公開鍵と上記複数の特権者公開鍵より検証可能である。また、当該グループ署名により正当性が検証されたグループ署名の生成主体は、タクシー配車システムに参加する資格があるか否か(タクシー協会がメンバとして認めたか否か)という事実がグループ署名の検証により判明するに留まる。また、グループ署名を生成したタクシー30を一意に特定するためのメンバ追跡機能は、各タクシー会社が備える。具体的には、各タクシー30がグループ署名生成の際に使用する特権者公開鍵の生成、管理はタクシー会社(運用管理サーバ20)に委ねられる。その結果、グループ署名からデータを取り出して各タクシーを特定することができるのは、各タクシー30の所属会社に限られる。このように、第2の実施形態では、グループ署名におけるメンバ登録機能とメンバ追跡機能を適切に分離することで、データの正当性の検証と開示する情報の制限を両立させている。

【0166】

なお、第1及び第2の実施形態にて説明したシステムの構成は例示であって、システムの構成を限定する趣旨ではない。例えば、必要に応じて、メンバの失効を管理するサーバ装置がシステムに含まれていても良い。あるいは、図2では、データ管理システム40には複数の管理サーバ50が含まれ、当該管理サーバ50が、所謂ブロックチェーン技術を用いて、運用管理データを管理することを説明した。しかし、実質的に1台のサーバ等が集中的に運用管理データを管理するものであってもよい。

【0167】

また、第1の実施形態では、データ管理システム40は、タクシー協会等から独立した

機関であることを前提としたが、データ管理システム 40 はタクシー協会の管理下で運用されるものであっても良いことは勿論である。

【0168】

また、第 1 及び第 2 の実施形態では、非特許文献 1 及び 2 に記載されたグループ署名の方式 (Camenisch-Groth 方式) を例にとり説明したが、他のグループ署名の方式を用いることができるのは勿論である。とりわけ、第 2 の実施形態に関し、既存のグループ署名の方式におけるチャレンジを分割することによって「どれかひとつの特権者公開鍵に対する正しいグループ署名である」という $OR\ proof$ を構成することにより、非特許文献 1 及び 2 の方式 (Camenisch-Groth 方式) とは異なる他のグループ署名の方式に基づいても実現可能であることは明らかである。

10

【0169】

上記の実施形態の一部又は全部は、以下のようにも記載され得るが、以下には限られない。

[形態 1]

上述の第 1 の視点に係るシステムのとおりである。

[形態 2]

前記複数のノードは、複数のグループのいずれかに属しており、

前記複数のグループそれぞれに属するノードを管理する、複数のノード管理サーバをさらに含み、

前記ノード管理サーバのそれぞれは、自グループに属する前記ノードに対し、グループ署名を生成する際に用いるメンバ証明書を発行する、好ましくは形態 1 のシステム。

20

[形態 3]

前記複数のノードは、複数のグループのいずれかに属しており、

前記複数のグループそれぞれに属するノードを管理する、複数のノード管理サーバと、

前記複数のノードそれぞれに対し、グループ署名を生成する際に用いるメンバ証明書を発行する、証明書管理サーバと、をさらに含み、

前記複数のノード管理サーバのそれぞれは、特権者公開鍵を公開し、

前記証明書管理サーバは、管理者公開鍵を公開する、好ましくは形態 1 のシステム。

[形態 4]

前記ノードは、前記管理者公開鍵と、前記複数のノード管理サーバそれぞれが公開する特権者公開鍵と、を用いてグループ署名を生成する、好ましくは形態 3 のシステム。

30

[形態 5]

前記生成されたグループ署名は、前記証明書管理サーバが公開する管理者公開鍵と前記複数のノード管理サーバのそれぞれが公開した特権者公開鍵により、検証可能である、好ましくは形態 4 のシステム。

[形態 6]

前記ノード管理サーバは、自身が管理するグループに属するノードが生成したグループ署名に含まれるデータを、前記特権者公開鍵とペアとなる特権者秘密鍵により取り出し、自身が管理するグループに属するノードを特定する、好ましくは形態 3 乃至 5 のいずれかに記載のシステム。

40

[形態 7]

上述の第 2 の視点に係るシステムのとおりである。

[形態 8]

前記ノードが生成するグループ署名は、前記グループ署名を生成したノード自身の公開鍵を、前記複数のノード管理サーバが公開するいずれかの特権者公開鍵で暗号化し、前記自身の公開鍵にメンバ証明書が存在すること、且つ、暗号化した主体が前記自身の公開鍵に対応する秘密鍵を有すること、を証明するデータを含む、好ましくは形態 7 のシステム。

[形態 9]

前記複数のノード管理サーバが公開する特権者公開鍵は、一部の要素が共通するように

50

生成された公開鍵である、好ましくは形態 7 及び 8 のシステム。

〔形態 1 0〕

前記共通する一部の要素は、前記特権者公開鍵に対応する特権者秘密鍵に依存して生成される要素である、好ましくは形態 9 のシステム。

〔形態 1 1〕

前記ノードの公開鍵は、前記共通する一部の要素に基づき生成される、好ましくは形態 1 0 のシステム。

〔形態 1 2〕

前記ノードは、自身が属するグループとは異なるグループのチャレンジ値をランダムに選択し、前記ランダムに選択されたチャレンジ値を用いて前記グループ署名を生成する、好ましくは形態 7 乃至 1 1 のいずれかに記載のシステム。

10

〔形態 1 3〕

前記ノードが生成したグループ署名の検証には、前記計算されたハッシュ値と、前記ランダムに選択されたチャレンジ値と、グループ署名を生成したノードが属するグループのチャレンジ値と、を用いる検証が少なくとも含まれる、好ましくは形態 1 2 のシステム。

〔形態 1 4〕

上述の第 3 の視点に係るデータ管理方法のとおりである。

〔形態 1 5〕

上述の第 4 の視点に係るプログラムのとおりである。

なお、形態 1 4 及び形態 1 5 は、形態 1 と同様に、形態 2 ～形態 6 のように展開することが可能である。

20

【0 1 7 0】

なお、引用した上記の特許文献等の各開示は、本書に引用をもって繰り込むものとする。本発明の全開示（請求の範囲を含む）の枠内において、さらにその基本的技術思想に基づいて、実施形態ないし実施例の変更・調整が可能である。また、本発明の全開示の枠内において種々の開示要素（各請求項の各要素、各実施形態ないし実施例の各要素、各図面の各要素等を含む）の多様な組み合わせ、ないし、選択が可能である。すなわち、本発明は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし得るであろう各種変形、修正を含むことは勿論である。特に、本書に記載した数値範囲については、当該範囲内に含まれる任意の数値ないし小範囲が、別段の記載のない場合でも具体的に記載

30

【符号の説明】

【0 1 7 1】

- 1 0 配車サーバ
- 1 1 C P U (Central Processing Unit)
- 1 2 メモリ
- 1 3 入出力インターフェイス
- 1 4 N I C (Network Interface Card)
- 2 0、2 0 - 1 ~ 2 0 - α 運用管理サーバ
- 3 0、3 0 - 1 ~ 3 0 - β タクシー
- 3 1 タクシーメータ
- 3 2 スマートフォン
- 4 0 データ管理システム
- 5 0、5 0 - 1 ~ 5 0 - 4、1 0 2 管理サーバ
- 6 0 証明書管理サーバ
- 1 0 1 ノード
- 2 0 1、3 0 1、4 0 1、5 0 1、6 0 1 通信制御部
- 2 0 2、3 0 2、4 0 2、5 0 2、6 0 2 記憶部
- 2 0 3 配車処理部
- 2 1 1 署名検証部

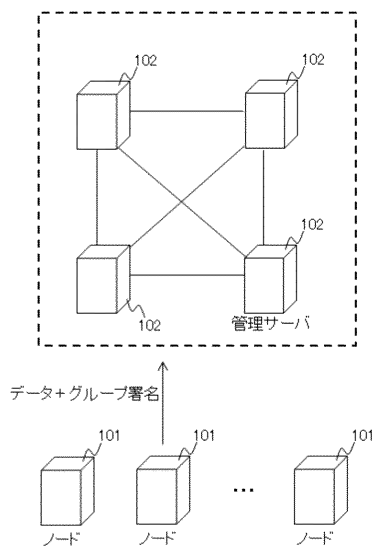
40

50

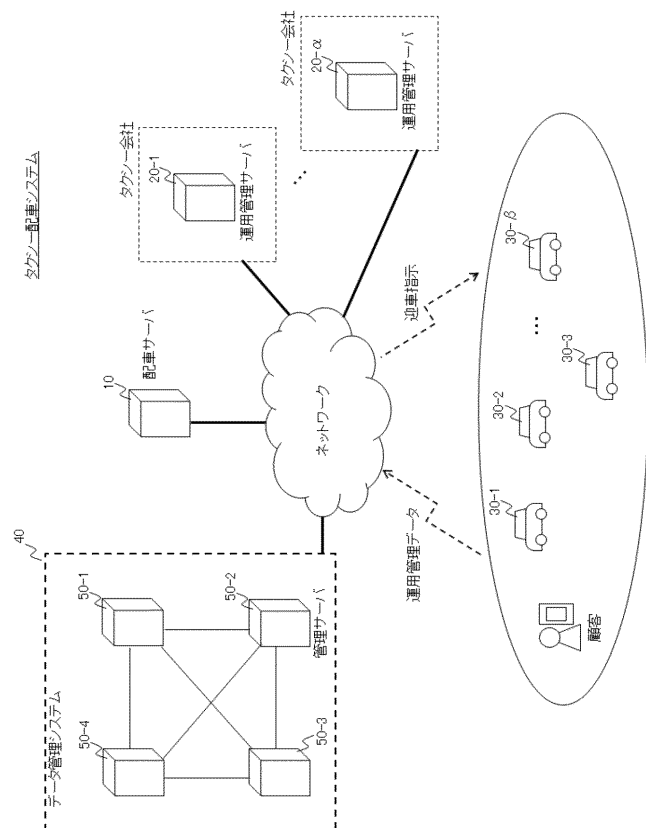
- 2 1 2 迎車決定部
- 3 0 3、6 0 3 証明書管理部
- 3 1 1、3 1 1 a、6 1 1 鍵生成部
- 3 1 2、6 1 2 証明書生成部
- 4 0 3 証明書取得部
- 4 0 4 運用管理データ処理部
- 4 1 1 運用管理データ生成部
- 4 1 2 グループ署名生成部
- 4 2 1 リンググループ署名生成部
- 5 0 3 台帳管理部
- 5 1 1 ブロック生成部
- 5 1 2 ブロック検証部

10

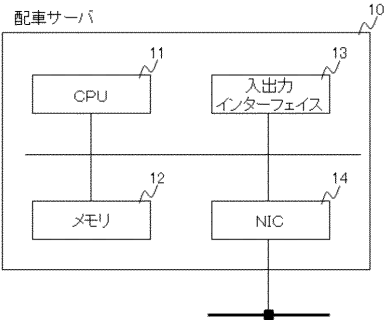
【図 1】



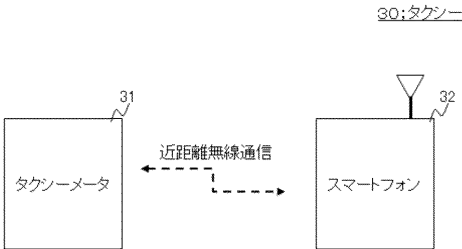
【図 2】



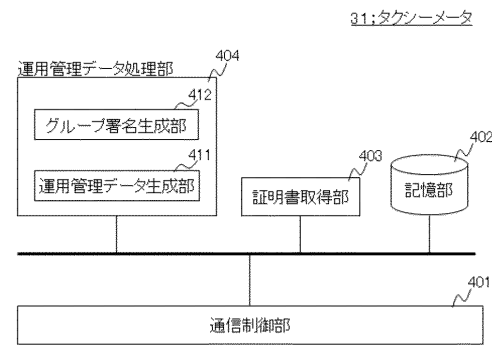
【図 3】



【図 4】



【図 7】

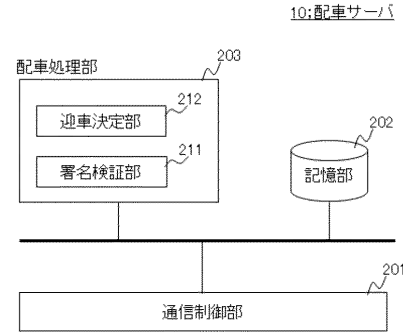


【図 8】

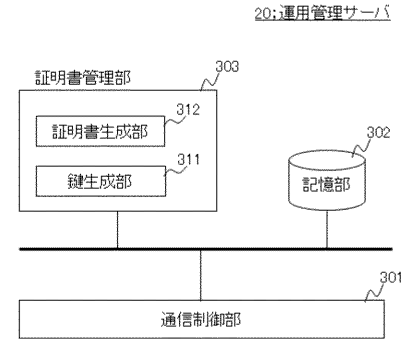
運用管理データ

乗車位置	降車位置	現在位置	通知先
X地点	Y1地点	Y2地点	xxx@yyy zzz

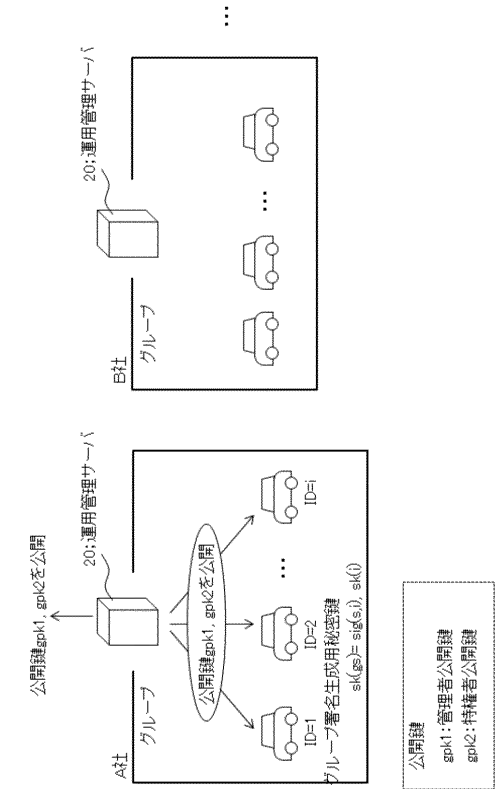
【図 5】



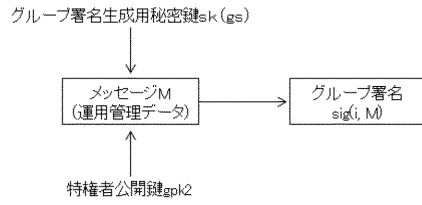
【図 6】



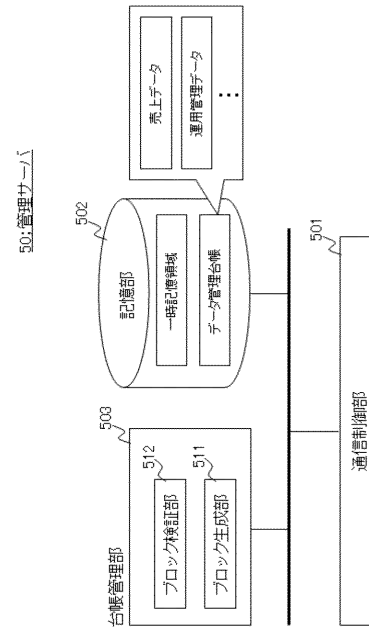
【図 9】



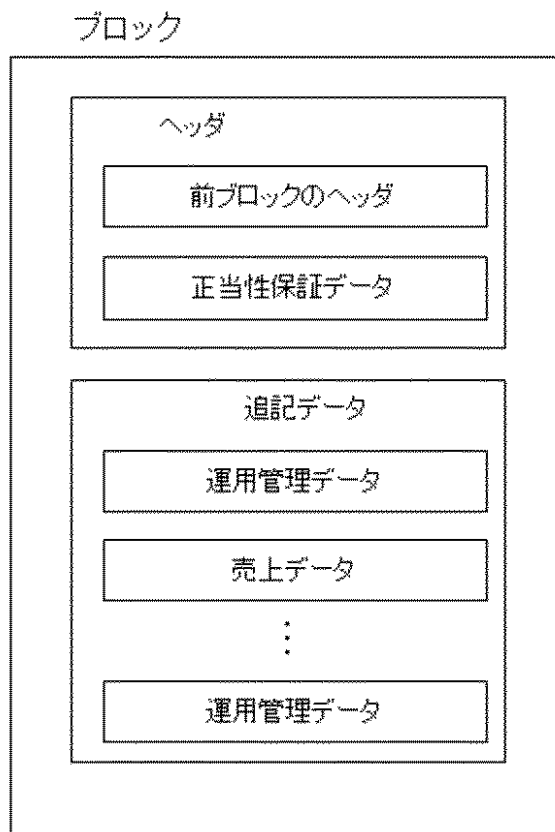
【図 10】



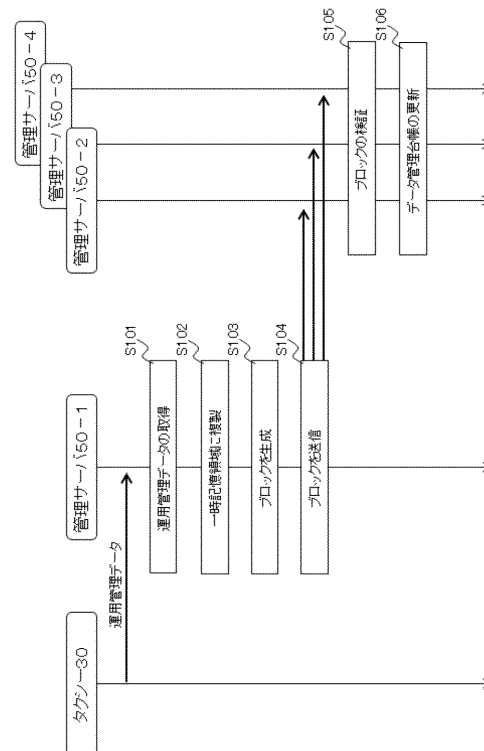
【図 11】



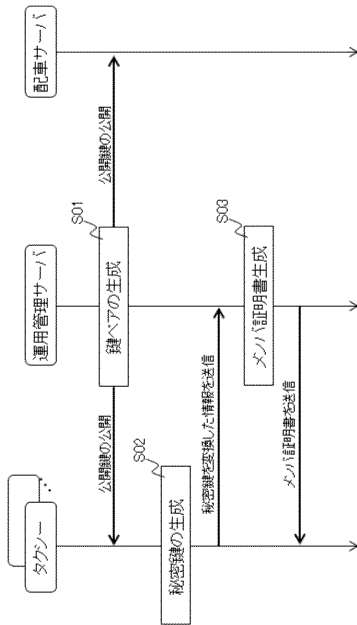
【図 12】



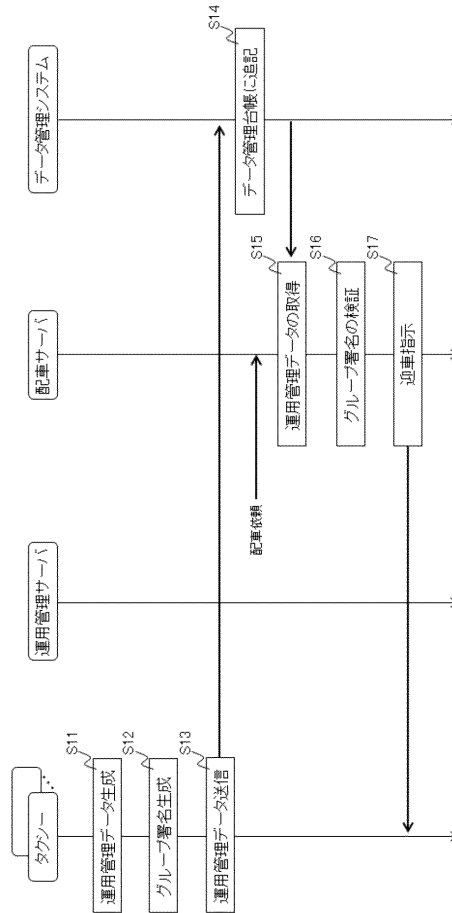
【図 13】



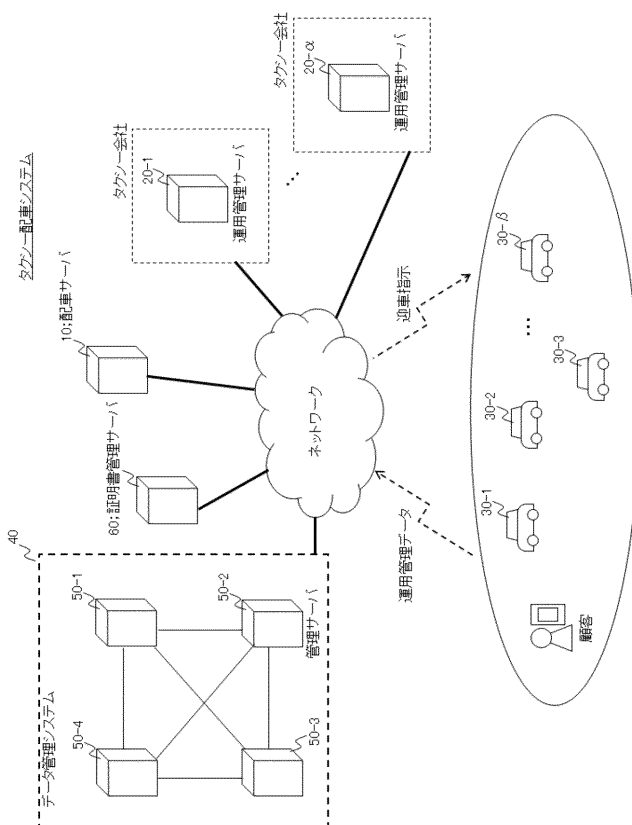
【図 14】



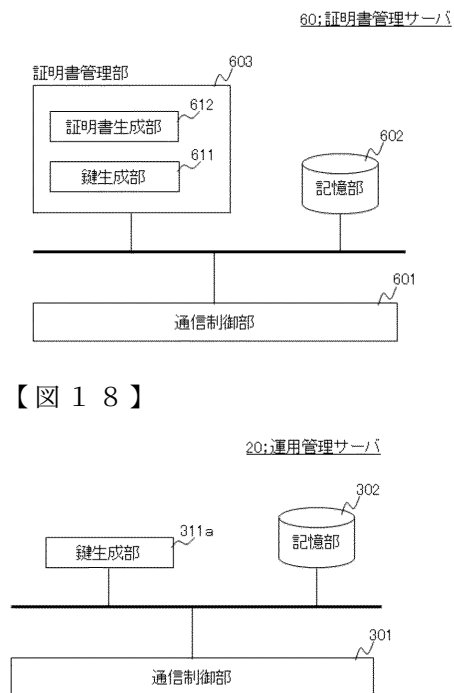
【 図 1 5 】



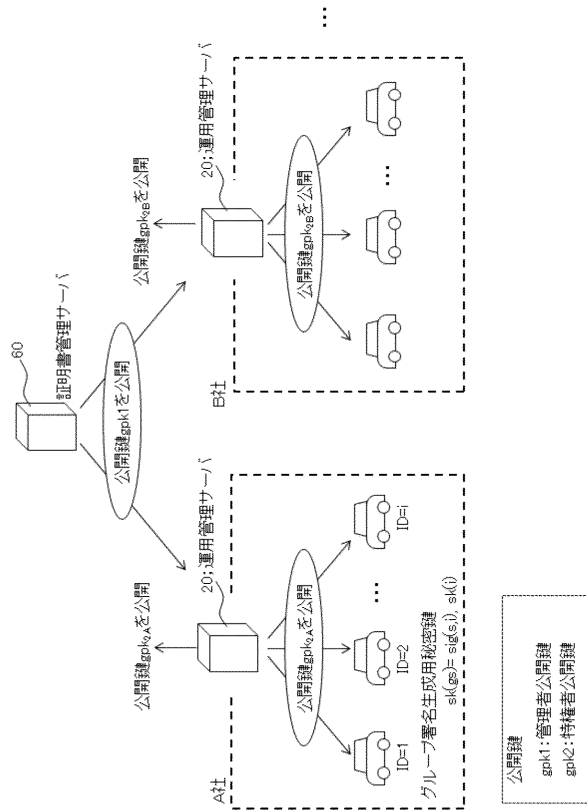
【图 1 6】



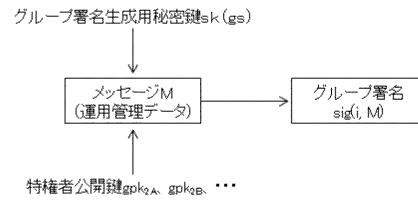
【图 17】



【図 19】



【図 20】



【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP2017/027461
A. CLASSIFICATION OF SUBJECT MATTER G09C1/00(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) G09C1/00, 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 1996-2017 Kokai Jitsuyo Shinan Koho 1971-2017 Toroku Jitsuyo Shinan Koho 1994-2017 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.
Y A	Yasuyuki FUCHITA, "Block Chain to Kin'yu Torihiki no Kakushin", Nomura Capital Markets Quarterly, 01 November 2015 (01.11.2015), vol.19, no.2, pages 11 to 35	1, 2, 14, 15 3-6
Y A	WO 2006/137250 A1 (NEC Corp.), 28 December 2006 (28.12.2006), paragraphs [0037] to [0059], [0237] to [0241]; fig. 7 & US 2009/0089575 A1 paragraphs [0078] to [0101], [0291] to [0295]; fig. 7 & EP 1895709 A1 & KR 10-2008-0021801 A & CN 101194462 A	1, 2, 7-11, 14, 15 3-6, 12, 13
☒ 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 12 October 2017 (12.10.17)		Date of mailing of the international search report 24 October 2017 (24.10.17)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2017/027461

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2011-24011 A (NEC Corp.), 03 February 2011 (03.02.2011), paragraphs [0021] to [0053] (Family: none)	7-11 1-6, 12-15
Y	JP 2002-215026 A (Nippon Telegraph and Telephone Corp.), 31 July 2002 (31.07.2002), claim 1 (Family: none)	9-11

国際調査報告		国際出願番号 PCT/J P 2 0 1 7 / 0 2 7 4 6 1	
A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. G09C1/00(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. G09C1/00, 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 1971-2017年 日本国実用新案登録公報 1996-2017年 日本国登録実用新案公報 1994-2017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	
Y A	淵田 康之, ブロックチェーンと金融取引の革新, 野村資本市場ク ォータリー, 2015.11.01, Vol.19 No.2, pp.11-35	1, 2, 14, 15 3-6	
Y A	WO 2006/137250 A1 (日本電気株式会社) 2006.12.28, 段落 [0037] - [0059], [0237] - [0241], 図7 & US 2009/0089575 A1, 段落 [0078] - [0101], [0291] - [0295], 図7 & EP 1895709 A1 & KR 10-2008-0021801 A & CN 101194462 A	1, 2, 7-11, 14, 15 3-6, 12, 13	
❶ C欄の続きにも文献が列挙されている。 ❷ 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 12.10.2017		国際調査報告の発送日 24.10.2017	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 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) 行田 悦資 電話番号 03-3581-1101 内線 3546	

国際調査報告		国際出願番号 PCT/J P 2 0 1 7 / 0 2 7 4 6 1
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
Y A	JP 2011-24011 A (日本電気株式会社) 2011.02.03, 段落 [0021] - [0053] (ファミリーなし)	7-11 1-6, 12-15
Y	JP 2002-215026 A (日本電信電話株式会社) 2002.07.31, 請求項 1 (ファミリーなし)	9-11

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT

(注) この公表は、国際事務局(WIPO)により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願(日本語実用新案登録出願)の国際公開の効果は、特許法第184条の10第1項(実用新案法第48条の13第2項)により生ずるものであり、本掲載とは関係ありません。