(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6825296号
(P6825296)
(45)発行日　令和3年2月3日(2021.2.3)　(24)登録日　令和3年1月18日(2021.1.18)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675B
H04L	9/08	(2006.01)	H04L	9/00	601F
G09C	1/00	(2006.01)	H04L	9/00	601B
G06F	21/33	(2013.01)	G09C	1/00	640E
			G06F	21/33	

請求項の数 7　(全 30 頁)

(21)出願番号　特願2016-199945(P2016-199945)
(22)出願日　平成28年10月11日(2016.10.11)
(65)公開番号　特開2018-64142(P2018-64142A)
(43)公開日　平成30年4月19日(2018.4.19)
審査請求日　令和1年7月9日(2019.7.9)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100113608
弁理士　平川　明
(74)代理人　100105407
弁理士　高田　大輔
(72)発明者　今井　悟史
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　関屋　元義
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】エッジサーバ，及びその暗号化通信制御方法

(57)【特許請求の範囲】
【請求項１】
クラウドと前記クラウドにサービスを要求する端末との間に配置されるエッジサーバにおいて、
前記エッジサーバへの接続を要求する端末について前記要求より前に生成された暗号鍵情報が前記クラウド及び少なくとも１つの他のエッジサーバと共有される共有情報に含まれている場合に、前記暗号鍵情報を用いて前記端末との暗号化通信を開始する制御部を含み、
前記制御部は前記エッジサーバへの接続を要求する端末との間で新たな暗号鍵情報を生成した場合に、前記新たな暗号鍵情報を前記共有情報に含める処理を行い、
前記制御部は、前記共有情報がブロックチェーン形式で保管される場合に、前記新たな暗号鍵情報を含むトランザクション情報を生成し、
前記制御部は、サービスプロバイダの公開鍵と前記サービスプロバイダによって提供されるサービスの公開鍵と前記エッジサーバの公開鍵とが前記エッジサーバと前記サービスプロバイダとの間で共有されている場合に、前記サービスプロバイダが前記共有されている前記エッジサーバの公開鍵を用いて暗号化された前記サービスの秘密鍵及び前記サービスの証明書を受け取る、
エッジサーバ。
【請求項２】
前記端末の公開鍵と前記サービスの公開鍵とが前記端末，前記エッジサーバ及び前記ク

ラウドとの間で共有されている場合に、前記制御部は、送信元に前記端末が指定され、宛先に前記サービスが指定され、ハッシュ値と前記ハッシュ値を前記端末の秘密鍵を用いて暗号化した前記端末の署名とを含むサービス申込メッセージを前記端末から受信して前記共有情報に含める処理と、前記共有情報に含められた前記サービス申込メッセージが承認された場合に、送信元に前記サービスが指定され、宛先に前記端末が指定され、ハッシュとしての前記サービス申込メッセージの情報と、前記サービス申込メッセージの情報を前記サービスの秘密鍵を用いて暗号化した前記サービスの署名とを含むサービス認可メッセージを前記端末に送信する処理とを行う、
請求項１に記載のエッジサーバ。
【請求項３】
前記制御部は、送信元に前記端末が指定され、宛先に前記サービスが指定され、ハッシュとしての前記サービス認可メッセージの情報と、前記サービス認可メッセージの情報を前記端末の秘密鍵を用いて暗号化した前記端末の署名と、前記サービスの公開鍵で暗号化された前記サービスでの処理対象のデータを含むサービス要求メッセージを前記端末から受信して前記共有情報に含める処理と、前記端末の署名が正当な場合に、送信元に前記サービスが指定され、宛先に前記端末が指定され、ハッシュとしての前記サービス要求メッセージの情報と前記サービス要求メッセージの情報を前記サービスの秘密鍵を用いて暗号化した前記サービスの署名と、前記端末の公開鍵と前記サービスの公開鍵とでそれぞれ暗号化された前記サービスの処理結果を含むサービス処理メッセージを前記共有情報に含めるとともに前記端末へ送信する処理とを行う
請求項２に記載のエッジサーバ。
【請求項４】
前記制御部は、前記サービス要求メッセージ中の前記端末の署名を前記端末の公開鍵を用いて検証する
請求項３に記載のエッジサーバ。
【請求項５】
前記制御部は、前記サービス要求メッセージに含まれる前記端末の位置情報に基づいて前記サービス要求メッセージに対応する処理を行う前記エッジサーバ以外の前記端末の接続先を特定した場合に、前記接続先の変更指示と前記接続先の場所を示す情報を前記端末に送信する
請求項３又は４に記載のエッジサーバ。
【請求項６】
前記端末の位置が前記端末に係るトランザクション情報を前記エッジサーバが管理するカバレッジ外である場合に前記制御部は前記端末に係るトランザクション情報を破棄する
請求項３から５のいずれか１項に記載のエッジサーバ。
【請求項７】
クラウドと前記クラウドにサービスを要求する端末との間に配置されるエッジサーバが、
前記エッジサーバへの接続を要求する端末について前記要求より前に生成された暗号鍵情報が前記クラウド及び少なくとも１つの他のエッジサーバと共有される共有情報に含まれている場合に、前記暗号鍵情報を用いて前記端末との暗号化通信を開始することと、
前記エッジサーバへの接続を要求する端末との間で新たな暗号鍵情報を生成した場合に、前記新たな暗号鍵情報を前記共有情報に含めることと、
前記共有情報がブロックチェーン形式で保管される場合に、前記新たな暗号鍵情報を含むトランザクション情報を生成することと、
サービスプロバイダの公開鍵と前記サービスプロバイダによって提供されるサービスの公開鍵と前記エッジサーバの公開鍵とが前記エッジサーバと前記サービスプロバイダとの間で共有されている場合に、前記サービスプロバイダが前記共有されている前記エッジサーバの公開鍵を用いて暗号化された前記サービスの秘密鍵及び前記サービスの証明書を受け取ることと、

を実行するエッジサーバの暗号化通信制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、エッジサーバ，その暗号化通信制御方法，及び端末に関する。
【背景技術】
【０００２】
クラウドコンピューティングでは、端末にサービスを提供するためのデータ蓄積及び情報処理機能を有する単数又は複数のサーバがクラウド（ネットワーク）に配置される。
【０００３】
分散コンピューティング環境の一種にエッジコンピューティングがある。エッジコンピューティングでは、クラウドサービスを提供するサーバと端末との間（ネットワークのエッジ）に複数のコンピュータが用意される。コンピュータは「エッジノード」,「エッジサーバ」,「エッジゲートウェイ」などと呼ばれる。
【０００４】
エッジコンピューティングでは、上記のデータ蓄積及び情報処理機能が複数のエッジサーバに分散配置される。エッジサーバはサーバよりも端末に近い位置に配置されるためネットワークの伝送遅延が短縮化される。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００５－６５００４号公報
【特許文献２】特許第５８５８５０６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
クラウドサービスの利用時に通信の暗号化が行われる場合がある。暗号化のプロトコルとして例えばSecure Sockets Layer（ＳＳＬ）/Transport Layer Security（ＴＬＳ）などが適用される。ＳＳＬ／ＴＬＳでは、通信開始に先立ち端末とクラウドサーバ（サービスプロバイダ）との間で証明書の検証及び鍵交換が行われ、鍵を用いて暗号化されたデータが送受信される。エッジコンピューティングでも、端末とエッジサーバとの間で暗号化通信が行われると考えられる。
【０００７】
エッジコンピューティングの環境下で、端末が移動性又は可搬性を有し、端末の位置に応じて接続先のエッジサーバが変更される場合があり得る。この場合、端末が新たなエッジサーバの間で暗号化の手順（証明書の検証及び鍵交換）をやり直すのは時間がかかる。暗号化の手順に時間を要すると、クラウドサーバよりも端末に近い位置にエッジサーバを置いた意義が損なわれる可能性がある。
【０００８】
本発明は、エッジサーバが接続を要求する端末と暗号化通信を開始するまでの時間を短縮できる技術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】
【０００９】
一つの態様は、　クラウドと前記クラウドにサービスを要求する端末との間に配置されるエッジサーバにおいて、
前記エッジサーバへの接続を要求する端末について前記要求より前に生成された暗号鍵情報が前記クラウド及び少なくとも１つの他のエッジサーバと共有される共有情報に含まれている場合に、前記暗号鍵情報を用いて前記端末との暗号化通信を開始する制御部
を含むエッジサーバである。
【発明の効果】

【００１０】
一側面では、エッジサーバが接続を要求する端末と暗号化通信を開始するまでの時間を短縮できる。
【図面の簡単な説明】
【００１１】
【図１】図１はブロックチェーン（ＢＣ）を模式的に示す。
【図２】図２はＳＳＬ／ＴＬＳの基本シーケンス例である。
【図３】図３は実施形態に係るネットワーク構成例を示す。
【図４】図４は図３に示したネットワークシステムによって構築されるサービス提供システムの例を示す。
【図５】図５はエッジサーバ３のハードウェア構成例を示す図である。
【図６】図５はクラウド上のサーバ４（クラウドサーバ）のハードウェア構成例を示す図である。
【図７】図７は端末２（デバイス）のハードウェア構成例を示す図である。
【図８】図８は端末２，エッジサーバ３，サーバ４が有する機能を模式的に示す。
【図９】図９は第１の分散ストレージの説明図である。
【図１０】図１０は第２の分散ストレージの説明図である。
【図１１】図１１はサービスの運用が開始される前（事前）のサービス設定時におけるエッジサーバ３及びサーバ４の動作例の説明図である。
【図１２】図１２はサービス事前設定トランザクションのデータ構造例を示す。
【図１３】図１３はサービス運用時に発行されるトランザクションの説明図である。
【図１４】図１４はサービス申込トランザクション（サービス申込Ｔｘ）のデータ構造例を示す。
【図１５】図１５はサービス認可トランザクション（サービス認可Ｔｘ）のデータ構造例を示す。
【図１６】図１６はサービス要求トランザクション（サービス要求Ｔｘ）のデータ構造例を示す。
【図１７】図１７はサービス処理トランザクション（サービス処理Ｔｘ）のデータ構造例を示す。
【図１８】図１８はサービス申込トランザクション，サービス認可トランザクション，サービス要求トランザクション及びサービス処理トランザクションとＢＣとの関係を模式的に示す図である。
【図１９】図１９は端末２（デバイス）の登録手続を示すシーケンス図である。
【図２０】図２０は、登録手続に係る端末２及びサーバ４の処理例を示すフローチャートである。
【図２１】図２１はサービス要求トランザクション及びサービス処理トランザクションに係る動作例を示すシーケンス図である。
【図２２】図２２はサービス要求トランザクション及びサービス処理トランザクションに係る処理例を示すフローチャートである。
【図２３】図２３はサービス要求トランザクション及びサービス処理トランザクションに係る動作例を示すシーケンス図である。
【図２４】図２４はサービス要求トランザクション及びサービス処理トランザクションに係る処理例を示すフローチャートである。
【図２５】図２５は動作例２に係るシーケンス図である。
【図２６】図２６は動作例２に係るシーケンス図である。
【図２７】図２７は動作例２に係るＣＰＵの処理例を示すフローチャートである。
【図２８】図２８は、トランザクションデータの保持範囲（カバレッジ）を模式的に示す図である。
【図２９】図２９は、エッジサーバ（ＧＷ）のＣＰＵによって実行される処理例を示すフローチャートである。

【図３０】図３０はエッジサーバの入出口にレイヤ７のファイヤウォールを配備する場合を模式的に示す。
【発明を実施するための形態】
【００１２】
以下、図面を参照して実施形態について説明する。但し、実施形態の構成は例示であり、本発明は実施形態の構成に限定されない。
【００１３】
実施形態では、複数のエッジサーバによって形成される計算機インフラを用い、端末（デバイス）のエッジサーバへの接続や端末に提供されるサービス実行を管理及び制御するエッジコンピューティングシステムについて説明する。
【００１４】
実施形態では、端末のエッジサーバに対する初回接続時に生成された暗号化通信の情報（ＳＳＬ／ＴＬＳセッション情報）をエッジサーバとクラウド（サービスプロバイダ）が分散ストレージ上で共有する。分散ストレージは、例えばエッジサーバやクラウドにある複数のストレージに情報を分散配置することによって形成される。端末の２回目以降の接続時に分散ストレージに記憶された暗号化通信の情報が利用される。これによって、端末の接続先のエッジサーバの変更に要する時間を短縮化できる。
【００１５】
実施形態の説明に先立ち、実施形態にて使用されている「ブロックチェーン（ＢＣ）」及び「ＳＳＬ／ＴＬＳ」の概要を説明する。
【００１６】
〔ブロックチェーン（ＢＣ）〕
ブロックチェーンは、仮想通貨（ビットコイン等）などで使用されている分散型台帳技術又は分散ネットワークであり、複数のノードに同一の記録を同期させる仕組みである。ＢＣでは、契約又は取引(トランザクション)が記録された台帳が公開され、ユーザが取引の正当性をチェックする。
【００１７】
ＢＣを利用するサービスの開始時に、ユーザの秘密鍵から生成される公開鍵と、公開鍵から生成されるユーザＩＤ（ビットコインアドレス等）とが発行される。公開鍵及びユーザＩＤはＢＣ上で保管・公開される。各ユーザは、トランザクション（トランザクション情報）を生成し、ＢＣネットワークにブロードキャストされる。
【００１８】
トランザクション情報は、送信元情報と、宛先情報と、トランザクション本体と、前のトランザクションのハッシュ値と、トランザクション本体の電子署名とを含む。トランザクション本体は、例えば、支払先のユーザＩＤ（アドレス）と支払元から支払先への支払額とを含む。電子署名は支払元の秘密鍵を用いて暗号化された前のトランザクション情報のハッシュ値である。
【００１９】
トランザクション情報を受信したユーザ（「マイナー」と呼ばれる検証を実行するユーザ）は、ユーザＩＤに対応するユーザの公開鍵を用いて電子署名を復号する。復号によって得られたハッシュ値と、トランザクション情報中のハッシュ値（平文）とを対比して両者が同じであれば、トランザクション情報が正当と判断（承認）される。なお、ユーザＩＤの代わりに公開鍵を用いる場合や、支払先の公開鍵をトランザクション情報に含める場合もある。
【００２０】
図１は、ブロックチェーン（ＢＣ）を模式的に示す。ＢＣでは、“ブロック”と呼ばれるデータの塊がチェーン状に連結され、分散ストレージ上で保管される。ブロックは、ブロックヘッダとトランザクションデータとを含む。トランザクションデータは、或る期間内に行われたトランザクションのトランザクション情報がまとめられたもの（トランザクションのリスト）である。なお、図１における“ＢＴＣ”はビットコインを例にした仮想

通貨単位を示す。

【００２１】

ブロックヘッダは、直前のブロックヘッダのハッシュ値（そのブロックの一つ前のブロックに関する情報）と、マークルルートのハッシュ値と、Nonce（Number used once：ナンス）とを含む。マークルルートのハッシュ値は、リスト中のトランザクションに係るマークルツリーを形成したときのルートのハッシュ値である。ナンスは、所定条件を満たすハッシュ値の探索（マイニング）に使用される使い捨ての値である。

【００２２】

ブロックは「マイナー」と呼ばれるブロックの生成者によって生成される。ブロックの生成処理は（proof-of work（ＰｏＷ））と呼ばれる。マイナーは、直前のブロックのハッシュ値、マークルルートのハッシュ値及びナンスから求められるハッシュ値が所定条件（先頭からｎ個が０）を満たすまで、ナンスを変更してハッシュ計算を繰り返す。この所定条件を満たすハッシュ値が得られるナンスを探しだす行為は「マイニング（採掘）」と呼ばれる。

【００２３】

所定条件を満たすハッシュ値を最初に算出できたマイナーがブロックを生成する権利を得る。所定条件を満たすハッシュが得られる場合のナンスは、ブロックに含められ、他のユーザは、ブロック中のナンスを用いて計算したハッシュ値が所定条件を満たすことを確認することで、ブロックが正当と判断（ブロックを承認）できる。

【００２４】

このように、ＢＣではトランザクションが改竄困難な状態で分散ストレージに記録され各ユーザが各トランザクションを監視することができる。ブロック内の情報を改竄しようとすると、マークルルートのハッシュ値やナンスに矛盾が生じ、その影響がＢＣ全体に及ぶので、実質改ざん不能なデータベースが構築される。

【００２５】

〔ＳＳＬ／ＴＬＳ〕

ＳＳＬ／ＴＬＳは、コンピュータネットワークにおいてセキュリティを要求される通信を行うためのプロトコルである。主な機能として、通信相手の認証、通信内容の暗号化、改竄の検出を提供する。多くの場合、コネクション型のトランスポート層プロトコル（例えば、Transmission Control Protocol（ＴＣＰ））とアプリケーション層の間で使われ、ＯＳＩ参照モデルのセッション層のプロトコルを担う。

【００２６】

図２はＳＳＬ／ＴＬＳの基本シーケンス（暗号化通信手続）の例を示す。図２（Ａ）は、クライアント（Ｃ）のサーバ（Ｓ）への初回アクセスの手順を示し、図２（Ｂ）は、クライアント（Ｃ）のサーバ（Ｓ）への２回目以降のアクセス（セッション再利用）の手順を示す。

【００２７】

[1. Client Hello]

図２（Ａ）において、クライアントとサーバとの間でＴＣＰに基づくハンドシェイクの手続が完了すると、クライアントが、通信の開始を示す“Client Hello”をサーバに通知する。メッセージ“Client Hello”は次の内容を含む。

・ＳＳＬ／ＴＬＳのプロトコルバージョン
・乱数（以降の共通鍵の算出に使用）
・セッションＩＤ（直前にアクセスしていれば、このＩＤを指定することでセッションを再開してネゴシエーションを省略することが可能）
・クライアントが利用可能な暗号化方式やデータの圧縮方法の一覧

【００２８】

[2. Server Hello]

サーバ（Ｓ）は“Client Hello”を受けて、これから使う暗号とハッシュ関数のアルゴリズムを決定し、メッセージ“Server Hello”をクライアントに通知する。サーバは暗号

化方式やデータの圧縮方式をクライアントから送信された一覧の中から選択する。メッセージ“Server Hello”は次の内容を含む。
・ＳＳＬ／ＴＬＳのプロトコルバージョン
・乱数（以降の共通鍵の算出に使用）
・セッションＩＤ（再接続してネゴシエーションを省略する場合に使用）
・サーバが決定した暗号化方式やデータの圧縮方式
【００２９】
[3. Server Certificate（省略可）]
サーバはクライアントに向けて、ＳＳＬ／ＴＬＳ通信に用いるサーバ証明書を送信する。このメッセージの送信は省略可能である。
【００３０】
[4. Server Key Exchange（省略可）]
サーバがサーバ証明書を送信しない場合、或いはServer Certificateによって送信したサーバ証明書に公開鍵が含まれない場合に、サーバは“Server Key Exchange”を用いて共通鍵を交換するための公開鍵を送信する。サーバは一時的な公開鍵を生成し、サーバの署名と共に送信する。
【００３１】
[5. Certificate Request（省略可）]
Certificate Requestは、クライアントを認証する必要がある場合に、サーバがクライアントに対してクライアント認証用の証明書を送るように要求するメッセージである。Certificate Requestはサーバが信頼するルート証明書のリストを含む。
【００３２】
[6. Server Hello Done]
Server Hello Doneは、クライアントに“Server Hello”から始まる一連のメッセージが完了したことを通知するために使用される。
【００３３】
[7. Client Certificate（省略可）]
クライアントはサーバからCertificate Requestを受信した場合にクライアント証明書をサーバに送る。サーバからCertificate Request が受信されない場合には省略される。
【００３４】
[8. Client Key Exchange]
ここまでの手順によって、クライアントはServer Certificate中のサーバ証明書に含まれている公開鍵を得る。クライアントはサーバとクライアントだけが知り得る共通鍵を作り出すために、「プリマスタシークレット」と呼ばれる乱数情報を生成し、生成したプリマスタシークレットをサーバの公開鍵を使って暗号化してサーバに送信する。暗号化されたプリマスタシークレットは、サーバが有する秘密鍵で解読（復号）され、クライアントとサーバがプリマスタシークレットを共有する。
【００３５】
[9. Certificate Verify（ 省略可）]
Certificate Verifyは、Client Certificate が送信された場合に送信される、クライアント証明書に対する署名データである。クライアントは署名 (Certificate Verify) を生成し、サーバに送信する。Certificate Verifyを受け取ったサーバは、クライアントから受け取ったクライアント証明書 (Client Certificate) を使って署名を検証する。ただし、サーバからCertificate Request が送信されない場合、Client Certificateも送信されない。
【００３６】
[10. Change Cipher Spec]
ここまでの手順によって、クライアントとサーバがプリマスタシークレットを共有する。クライアントとサーバとのそれぞれは、Client HelloとServer Helloに含まれていた乱数とプリマスタシークレットとを用いて「マスタシークレット」を生成する。このとき、

クライアントとサーバは同じ方法でマスタシークレットを生成する。さらに、クライアント及びサーバは、マスタシークレットから、以降の暗号化通信に用いるための共通鍵を生成する。共通鍵を用いた暗号化通信を行うことを通知するために、クライアントはサーバに対してChange Cipher Spec を送信する。

【００３７】

[11. Finished]

クライアントがサーバ認証に成功し、共通鍵を共有できたことをサーバに通知する。その後、共通鍵を用いてメッセージを暗号化して送信する。

【００３８】

[12. Change Cipher Spec、13. Finished]

サーバは共通鍵を用いた暗号化通信を行うことを通知するためにクライアントにChange Cipher Spec を送信する。また、サーバはFinishedをクライアントに送信して認証成功及び共通鍵共有をクライアントに通知する。

【００３９】

なお、ＳＳＬ／ＴＬＳ通信において、クライアントはセッション切断時に通信鍵や証明書を含むセッション情報を一時的に保存（キャッシュ）することができる。クライアントは、サーバに再接続を要求するClient Helloの送信時にセッションＩＤを指定する（セッションＩＤをClient Helloに含める）ことによって、上述した３～９のプロセスを省略することができる（図２（Ｂ）参照）。このリジューム機能は、“SSL/TLS Resumption”と呼ばれる。

【００４０】

“SSL/TLS Resumption”は一度確立された ＳＳＬ／ＴＬＳセッションの情報をそのセッションによって定義されたＩＤと関連づけて保存（キャッシュ）し、再接続時にキャッシュされた情報を利用して前回の接続を回復する機能である。

【００４１】

TLS Session resumption を利用したときのプロトコルの動作は TLS 1.2 の RFC5246 に記述されている。セッション確立時に交換されるClient Hello とServer Hello とは“セッションid”と呼ばれるデータを含む。

【００４２】

クライアントが新規セッションを確立する場合では、以下が行われる。クライアントはサーバに送るClient Helloのセッションidは空で送る。空のセッションidを受け取ったサーバは新規のセッションidを生成し、Server Helloに載せてクライアントに返す。これにより、セッション再開時、クライアントは証明書の検証を行わず、また Server/Clientにおける鍵共有も行わず、セッション確立のハンドシェイクの手続きを一部省略する事が可能になる。

【００４３】

クライアントが再開したいセッションid を持つ場合には、クライアントは再開を所望するセッションidの値を含むClient Helloをサーバに送る。なお，サーバとクライアントは交換したセッションidをキーに、確立したセッションの情報をキャッシュに格納する。

【００４４】

＜ネットワーク構成＞

図３は実施形態に係るネットワーク構成例を示す。図１にはエッジコンピューティングに係るネットワークの一例が図示されている。図１では、クラウド（ネットワーク）に接続された複数のデータセンター１と端末（デバイス）２との間に複数のエッジサーバ３が分散配置されている。各データセンター１は、単数又は複数のサーバ４によって形成される。サーバ４は、端末２にサービスを提供するためのデータ蓄積や情報処理を行うサービスプロバイダとして機能する。サービスプロバイダとして機能するサーバ４の数は単数でも複数でも良い。以下の説明において、サーバ４をエッジサーバ３との区別のためにクラウドサーバと称する場合もある。サーバ４は「クラウド」の一例である。

【００４５】

端末２は、移動端末（無線端末）であってもよく、固定端末であっても良い。実施形態３では、端末２が移動端末である場合について説明する。移動端末は車載端末を含む。

【００４６】

エッジサーバ３は、クラウド（ネットワーク）のエッジに配置されている。エッジサーバ３は、端末２から要求されたサービスをサーバ４の代わりに提供することができる。エッジサーバ３から端末２へ提供されるサービスは、サーバ４から提供できるものであってもなくても良い。複数のサーバ４と複数のエッジサーバ３とは相互に接続され、ピアツーピア（Ｐ２Ｐ）ネットワークを形成している。

【００４７】

図４は、図３に示したネットワークシステムによって構築されるサービス提供システムの例を示す。例えば、以下を仮定する。データセンター１Ａにある複数のサーバ４がサービスプロバイダＸとして機能する。データセンター１Ｂにある複数のサーバ４がサービスプロバイダＡとして機能する。データセンター１Ｃにある複数のサーバ４がサービスプロバイダＢとして機能する。

【００４８】

エッジサーバ３（ＧＷ＃１）は、サービスプロバイダＡ及びサービスプロバイダＢから、各プロバイダのユーザ向けの情報を得る。また、サービスプロバイダＸからは、サービスプロバイダＡのユーザとサービスプロバイダＢのユーザ間で共通な情報を得る。ＧＷ＃１は、サービスプロバイダＡのユーザ向けのマッシュアップを行う。ＧＷ＃１は、サービスプロバイダＢのユーザ向けのマッシュアップを行う。

【００４９】

サービスプロバイダＡのユーザの端末２は、パブリッシャとしてサブスクライバに供給する情報（Ａユーザ向けにマッシュアップされたコンテンツ）を指定する。端末２はサブスクライバとしてＧＷ＃１から受信できる。サービスプロバイダＢのユーザの端末２は、パブリッシャにより指定された情報（Ｂユーザ向けにマッシュアップされたコンテンツ）をサブスクライバとして受信することができる。但し、上記のサービス提供の態様は一例である。例えば、エッジサーバ３は、各サービスプロバイダが提供する情報をサービスプロバイダ（サーバ４）に変わって提供しても良い。

【００５０】

＜ハードウェア構成＞

図５はエッジサーバ３のハードウェア構成例を示す図である。図６はクラウド上のサーバ４のハードウェア構成例を示す図である。図７は端末２（デバイス）のハードウェア構成例を示す図である。

【００５１】

図５において、エッジサーバ３は、バスを介して相互に接続された、Central Processing Unit（ＣＰＵ）１１，メモリ１２，無線インタフェース（無線ＩＦ）１３，伝送路インタフェース（伝送路ＩＦ）１４,及びユーザインタフェース（ＵＩ）１６を含む。無線ＩＦ１３には、アンテナ１５が接続されている。

【００５２】

メモリ１２は、主記憶装置と補助記憶装置とを含む。主記憶装置は、プログラムの展開領域，ＣＰＵ１１の作業領域，データやプログラムの記憶領域又はバッファ領域として使用される。主記憶装置は、例えばRandom Access Memory（ＲＡＭ），或いはＲＡＭとRead Only Memory（ＲＯＭ）との組み合わせで形成される。

【００５３】

補助記憶装置は、データやプログラムの記憶領域として使用される。補助記憶装置は、例えば、ハードディスクドライブ（ＨＤＤ），Solid State Drive（ＳＳＤ），フラッシュメモリ，Electrically Erasable Programmable Read-Only Memory（ＥＥＰＲＯＭ）などの不揮発性記憶媒体で形成される。補助記憶装置には、ディスク型記憶媒体や、ＵＳＢメモリなど、可搬性を有する記録媒体を含むことができる。メモリ１２（主記憶装置及び補助記憶装置のそれぞれ）は、「記憶装置」，「記憶媒体」，「メモリ」，「記憶部」の

一例である。

【００５４】

無線ＩＦ１３は、ベースバンド回路（ＢＢ回路）と、Radio Frequency（ＲＦ）回路とを含む。ＢＢ回路は、データ（ディジタル）信号とベースバンド信号（ＢＢ信号）との間の変換処理を行う。ＲＦ回路は、ＢＢ信号と無線信号との間の変換処理を行う。無線信号はアンテナ１５によって送受信される。

【００５５】

伝送路ＩＦ１４は、伝送路（例えば有線ＬＡＮ）を介して外部ネットワークに接続される。伝送路ＩＦ１４として、例えば、ＬＡＮカード（ネットワークインタフェースカード）を適用し得る。

【００５６】

ＵＩ１６は、入力装置と出力装置とを含む。入力装置はデータや情報の入力に使用される。入力装置は、例えば、キー，ボタン，ポインティングデバイス（マウスなど），タッチパネル，マイクロフォンなどである。出力装置は、情報の出力に使用される。出力装置は、ディスプレイ，スピーカ，ランプなどである。

【００５７】

ＣＰＵ１１は、メモリ１２に記憶されたプログラムをロードして実行する。ＣＰＵ１１がプログラムを実行することによって、エッジサーバ３としての様々な処理及び動作が行われる。ＣＰＵ１１は、「制御装置」，「制御部」，「コントローラ」，「プロセッサ」の一例である。

【００５８】

ＣＰＵは、ＭＰＵ（Microprocessor）、プロセッサとも呼ばれる。ＣＰＵは、単一のプロセッサに限定される訳ではなく、マルチプロセッサ構成であってもよい。また、単一のソケットで接続される単一のＣＰＵがマルチコア構成を有していても良い。ＣＰＵで行われる処理の少なくとも一部は、ＣＰＵ以外のプロセッサ、例えば、Digital Signal Processor(DSP)、Graphics Processing Unit（GPU）、数値演算プロセッサ、ベクトルプロセッサ、画像処理プロセッサ等の専用プロセッサで行われても良い。

【００５９】

また、ＣＰＵで行われる処理の少なくとも一部は、集積回路（ＩＣ）、その他のディジタル回路で行われても良い。また、集積回路やディジタル回路はアナログ回路を含んでいても良い。集積回路は、ＬＳＩ，Application Specific Integrated Circuit（ASIC），プログラマブルロジックデバイス（ＰＬＤ）を含む。ＰＬＤは、例えば、Field-Programmable Gate Array(FPGA)を含む。ＣＰＵ１１で行われる処理の少なくとも一部は、プロセッサと集積回路との組み合わせにより実行されても良い。組み合わせは、例えば、マイクロコントローラ（ＭＣＵ），ＳｏＣ（System-on-a-chip），システムＬＳＩ，チップセットなどと呼ばれる。

【００６０】

図６に示すように、クラウド上のサーバ４は、エッジサーバ３の構成から無線ＩＦ及びアンテナを除いたものになっている点を除きエッジサーバ３と同じであるので重ねての説明は省略する。図７に例示する端末２は、エッジサーバ３の構成から伝送路ＩＦが除かれた構成を有している。但し、端末２が伝送路ＩＦを有し、伝送路（有線ＬＡＮなど）と接続されても良い。また、端末２は、端末２の測定に用いるＧＰＳ（Global Positioning System）受信機１７を含んでいる。

【００６１】

図８は、端末２，エッジサーバ３，サーバ４が有する機能を模式的に示す。図８において、端末８は、ストレージ２１を有し、トランザクション発行２２，端末２の位置情報通知２３，暗号化通信処理２４，データ送受信２５を行う装置として動作する。図７に示したメモリ１２はストレージ２１として機能する。ＣＰＵ１１はプログラム実行によってトランザクション発行２２，位置情報通知２３，暗号化通信処理２４の各処理を行う。データ送受信２５は無線ＩＦ１３及びアンテナ１５を用いて行われる。

【００６２】
また、図８において、エッジサーバ３／サーバ４は、メモリ１２を用いて形成されるストレージ３１及びカバレッジ定義データベース（ＤＢ）３２を含む。また、エッジサーバ３／サーバ４は、無線ＩＦ１３及びアンテナ１５、或いは伝送路ＩＦ１４を用いてデータ送受信３３を行う。また、エッジサーバ３／サーバ４は、ＣＰＵ１１のプログラム実行によって、暗号化通信処理３４，サービス処理３５，通信切替処理３６，場所分析３７，トランザクション発行３８を行う。さらに、エッジサーバ３／サーバ４は、ＣＰＵ１１のプログラム実行によって、分散ストレージ同期３９，トランザクション確定処理４０，及びデータ保有制御４１を行う。
【００６３】
図３に示した端末２（デバイス）は、移動性又は可搬性を有し、移動によって端末２の位置が変化する。端末２の移動に伴い、端末２とエッジサーバ３（ＧＷ）との間の通信接続の切り替え（接続先のエッジサーバ３の変更）が発生する。端末２の移動距離が長い場合、通信接続の切り替えが頻繁に起こる可能性がある。このとき、接続先の切替の度に暗号鍵（例えば共通鍵）の生成が行われると、エッジサーバ３の切替に要する時間が長くなり、好適なサービス提供に影響を与える可能性がある。実施形態では、接続を要求した端末２との暗号化通信開始までの時間を短縮し得るエッジコンピューティングシステムについて説明する。
【００６４】
実施形態では、過去における端末２とエッジサーバ３又はサーバ４との接続により生成されたＳＳＬ／ＴＬＳの通信鍵の情報（暗号鍵情報）が分散ストレージの一例であるブロックチェーン（ＢＣ）上で共有される。暗号化鍵情報は、端末２（デバイス），エッジサーバ３（ＧＷ），サーバ４（サービスプロバイダ）間で共有し得る。
【００６５】
ＢＣ上で共有されるセッション情報を用いて、端末２が移動に伴い異なるエッジサーバ３に接続する（接続先を変更する）場合の鍵交換手続き（暗号鍵の生成）が省略される。鍵交換手続の省略によって、切り替え（変更）に要する時間の短縮が図られ、迅速かつ好適なサービス提供がなされる。
【００６６】
なお、実施形態では、共有される情報の管理形式としてＢＣが用いられる例について説明する。もっとも、共有される情報の保管形式はＢＣに制限されない。例えば、複数のストレージを用いて情報を分散して記憶する分散ストレージ機構により共有される情報が保管されても良い。実施形態では、一例として、クラウド上に分散ストレージが構築され、分散ストレージで記憶される共有情報の一部又は全部のコピーが端末２，エッジサーバ３，サーバ４に記憶される例について説明する。もっとも、端末２，エッジサーバ３，サーバ４が有するメモリ１２が分散ストレージを形成するストレージの一部であっても良い。
【００６７】
実施形態では、端末２（デバイス），エッジサーバ３（ＧＷ）、サーバ４（クラウド）のそれぞれが発行するトランザクション（メッセージ）の情報が分散ストレージに保持される。或いは、トランザクション情報がブロードキャストされ、分散ストレージに記憶されるとともに、端末２，エッジサーバ３，及びサーバ４のメモリ１２に記憶されるようにしても良い。端末２（デバイス），エッジサーバ３（ＧＷ）、サーバ４（クラウド）のそれぞれが発行する「トランザクション」はメッセージの一例である。
【００６８】
端末２，エッジサーバ３，及びサーバ４のメモリ１２に、これらに関係するトランザクション情報が予め記憶されるか、必要に応じて分散ストレージからダウンロード出来るようになっていれば良い。
【００６９】
実施形態では、第１の分散ストレージと、第２の分散ストレージとが構築される。第１の分散ストレージは、エッジサーバ３（ＧＷ）とサーバ４（クラウドサーバ：サービスプ

ロバイダ）間でトランザクション情報を共有するために構築される。第１の分散ストレージに記憶されるトランザクション情報は、端末２（デバイス：ユーザ）へのサービス提供開始前に設定される情報を含む。

【００７０】

第２の分散ストレージは、端末２（デバイス），エッジサーバ３（ＧＷ），及びサーバ４（サービスプロバイダ）間でトランザクション情報を共有するために構築される。第２の分散ストレージに記憶される情報は、サービス運用時の通信手続に係る情報や、サービス利用の履歴の把握に使用される情報を含む。通信手続に係る情報は、上述したＳＳＬ／ＴＬＳのセッション情報（暗号鍵情報など）を含む。

【００７１】

図９は第１の分散ストレージの説明図である。図９において、第１の分散ストレージ５１は、サービスの事前設定時に利用されるエッジサーバ３の公開鍵（Ｇ公開鍵）、サービスプロバイダの公開鍵（Ｐ公開鍵）、サービスの公開鍵（Ｓ公開鍵）を公開及び管理するために構築される。

【００７２】

第１の分散ストレージ５１に記憶される情報のコピーは、エッジサーバ３及びサーバ４（クラウドサーバ）のメモリ１２（ストレージ３１）に記憶される。なお、エッジサーバ３はＧ秘密鍵及びＧ公開鍵を発行し、サービスプロバイダ（サーバ４）は、Ｐ秘密鍵及びＰ公開鍵と、各サービスのＳ秘密鍵及びＳ公開鍵とを発行する。

【００７３】

エッジサーバ３は各エッジサーバ３のＧ秘密鍵をメモリ１２に記憶しており、サーバ４（クラウドサーバ）は、各サービスプロバイダのＰ秘密鍵をメモリ１２に記憶している。各サービスのＳ秘密鍵及びサービス証明書は暗号化されてサーバ４から各エッジサーバ３に配布される。

【００７４】

図１０は第２の分散ストレージの説明図である。図１０において、第２の分散ストレージ５２はサービス運用時に使用される。第２の分散ストレージ５２はサービスの公開鍵（Ｓ公開鍵）と端末２（デバイス）の公開鍵（Ｄ公開鍵）を公開及び管理する。第２の分散ストレージの記憶内容のコピーは、端末２（デバイス），エッジサーバ３及びサーバ４（クラウドサーバ）のメモリ１２に記憶され、端末２（デバイス），エッジサーバ３及びサーバ４（クラウドサーバ）で閲覧できる。

【００７５】

＜事前のサービス設定時における動作例＞

図１１はサービスの運用が開始される前（事前）のサービス設定時におけるエッジサーバ３及びサーバ４の動作例の説明図である。

【００７６】

実施形態に係るエッジサーバ３及びサーバ４のそれぞれとして動作する情報処理装置（コンピュータ）のメモリ１２には、専用のアプリケーションプログラムがインストールされる。

【００７７】

（１０１の処理）

図１１の１０１において、エッジサーバ３及びサーバ４のＣＰＵ１１は、専用のアプリケーションの実行によって公開鍵及び秘密鍵を生成する。このとき、エッジサーバ３ではＧ秘密鍵及びＧ公開鍵が生成され、サーバ４ではＰ秘密鍵及びＰ公開鍵が生成される。Ｇ秘密鍵はエッジサーバ３で秘匿及び管理され、Ｐ秘密鍵はサーバ４で秘匿及び管理される。

【００７８】

エッジサーバ３（ＧＷ）は、Ｇ公開鍵の公開に係るトランザクション（メッセージ、送信元：ＧＷ、宛先：サービスプロバイダ）を発行し、Ｇ公開鍵を第１の分散ストレージ５１上で公開可能とする。サーバ４（サービスプロバイダ）は、Ｐ公開鍵の公開に係るトラ

ンザクション（メッセージ、送信元：サービスプロバイダ、宛先：ＧＷ）を発行し、Ｐ公開鍵を第１の分散ストレージ５１上で公開する。なお、Ｇ秘密鍵及びＧ公開鍵はエッジサーバ３毎に固有の通信鍵であっても良く、複数のエッジサーバ３間で共通の通信鍵であっても良い。

【００７９】

（１０２の処理）

図１１の１０２において、サーバ４のＣＰＵ１１は、サーバ４がサービスプロバイダとして提供する各サービスの秘密鍵及び公開鍵（Ｓ秘密鍵及びＳ公開鍵）を生成するとともに、サービス証明書を生成する。サーバ４は、各サービスのＳ公開鍵を第１の分散ストレージ５１上で公開する。サーバ４のＣＰＵ１１（サービスプロバイダ）は、認証局(ＣＡ：Certification Authority)の証明書を事前にメモリ１２に保持し、認証局の署名付きのサービス証明書をサービス毎に生成、管理する。

【００８０】

（１０３の処理）

Ｓ秘密鍵は、ＳＳＬ／ＴＬＳ通信時と各エッジサーバ３におけるサービス処理トランザクション（サービス処理メッセージの一例）発行時の署名に活用される。１０２で生成されたサービス証明書は、ＳＳＬ／ＴＬＳ通信時のサービス認証に利用される。

【００８１】

１０３において、サーバ４（サービスプロバイダ）は、サーバ４が有するＳ秘密鍵とサービス証明書とを、配布及び共有先のエッジサーバのＧ公開鍵（第１の分散ストレージ５１から入手）を用いて暗号化する。サーバ４は、Ｐ公開鍵で指定された送信元情報と、Ｐ秘密鍵を用いた署名情報と、各エッジサーバ３のＧ公開鍵で指定された宛先情報とを含むサービス事前設定トランザクション（サービス事前設定のメッセージ）に埋め込んで、第１の分散ストレージ５１に登録する。これにより、エッジサーバ３にＳ秘密鍵及びサービス証明書が配布される（図９参照）。これにより、エッジサーバ３がサーバ４に代わってＳ秘密鍵を用いた署名を含むトランザクションを発行可能となる。

【００８２】

図１２はサービス事前設定トランザクションのデータ構造例を示す。トランザクションは、例えば、サーバ４（サービスプロバイダ＃１）からエッジサーバ３（ＧＷ＃２）への登録、及び０．１ＢＴＣの送金である。

【００８３】

この場合、前のトランザクションのハッシュはＮＵＬＬに設定される。入力（送信元）情報としては、サービスプロバイダ＃１の署名とサービスプロバイダ＃１の公開鍵（Ｇ公開鍵）が設定される。

【００８４】

また、出力（宛先）情報としては、送金額０．１（ＢＴＣ）と、ＧＷ＃２の公開鍵（Ｇ公開鍵）と、ＧＷ＃２の公開鍵で暗号化されたＳ秘密鍵及びサービス証明書である。ＧＷ＃２の公開鍵で暗号化されたＳ秘密鍵及びサービス証明書（認証局署名付き）は、トランザクションのフォーマット内（たとえばオプション領域）に記載される。

【００８５】

サービス事前設定トランザクションは、未承認のトランザクションとして扱われ、図１１に示すように、マイナーによるマイニング（新規のブロック生成処理）においてトランザクションデータの一部となる。マイニングはサーバ４やエッジサーバ３で実行されても良い。或いは、第１の分散ストレージ５１に登録される情報の管理者がマイニングを実行しても良い。

【００８６】

なお、図１２に示す例では、仮想通貨（ビットコイン等）の送金もトランザクション情報に含まれているが、仮想通貨の送金に係る情報は必ずしもサービス事前設定トランザクションに含まれていることを要しない。

【００８７】

図１１に示した処理によって、エッジサーバ３は、エッジサーバ３に対応するＧ秘密鍵を用いて、各サービスのＳ秘密鍵とサービス証明書とをセキュアに保有することが可能になる。

【００８８】

＜サービス運用時の動作例＞

図１３はサービス運用時に発行されるトランザクションの説明図である。第２の分散ストレージ５２は、図１３に示すような４種類のトランザクション（メッセージ。具体的にはサービス申込トランザクション，サービス認可トランザクション，サービス要求トランザクション，及びサービス処理トランザクション）を記憶および管理する。サービス申込トランザクションはサービス申込メッセージの一例であり、サービス認可トランザクションはサービス認可メッセージの一例であり、サービス要求トランザクションはサービス要求メッセージの一例であり、サービス処理トランザクションはサービス処理メッセージの一例である。

【００８９】

図１４はサービス申込トランザクション（サービス申込Ｔｘ）のデータ構造例を示す。サービス申込トランザクションは、サービス提供を所望する端末２（デバイス）によって発行される。

【００９０】

図１４には、或る端末２（デバイスＡ）から或るサービス（サービス＃１）へのサービス申込トランザクションが例示されている。サービス申込トランザクションの送信元は端末２の公開鍵（Ｄ公開鍵）であり、宛先はＳ公開鍵である。すなわち、送信元に端末２が指定され、宛先にサービスが指定されている。

【００９１】

前のトランザクションのハッシュ値（前の入力Ｔｘハッシュ）はＮＵＬＬである。入力（送信元）として、デバイスＡの電子署名とデバイスＡの公開鍵（Ｄ公開鍵）とが設定される。デバイスＡの電子署名は、デバイスＡの公開鍵でＮＵＬＬのハッシュ値を暗号化することで生成される。出力（宛先）として、送金額０．１ＢＴＣ（サービス利用料）と、サービス＃１の公開鍵（Ｓ公開鍵）が設定される。また、フォーマット内の記載情報にはＮＵＬＬが設定される。

【００９２】

図１５はサービス認可トランザクション（サービス認可Ｔｘ：サービス認可のメッセージ）のデータ構造例を示す。サービス認可トランザクションは、端末２（デバイス）からの申込を認可するエッジサーバ３又はサービスプロバイダ（サーバ４）によって発行される。

【００９３】

図１５には、或るサービス（サービス＃２）から或る端末２（デバイスＣ）へのサービス認可トランザクションが例示されている。サービス認可トランザクションの送信元はサービス＃２であり、宛先は端末２（デバイスＣ）である。

【００９４】

サービス認可トランザクションにおける前のトランザクションのハッシュ値（前の入力Ｔｘハッシュ）として、対応するサービス申込トランザクションの情報“ＸＸＸＸ”が使用される。入力（送信元）として、Ｓ秘密鍵を用いたサービス＃２の署名とサービス＃１の公開鍵（Ｓ公開鍵）とが設定される。出力（宛先）として、送金額０とデバイスＡの公開鍵（Ｄ公開鍵）とが設定される。また、フォーマット内の記載情報にはＮＵＬＬが設定される。

【００９５】

図１６はサービス要求トランザクション（サービス要求Ｔｘ）のデータ構造例を示す。サービス要求トランザクションはサービスに係る処理を要求する端末２（デバイス）によって発行される。

【００９６】

図１６には、或る端末２（デバイスＢ）から或るサービス（サービス＃２）へのサービス要求トランザクションが例示されている。サービス要求トランザクションの送信元は端末２（デバイス）であり、宛先はサービスである。

【００９７】

前のトランザクションのハッシュ値（前の入力Ｔｘハッシュ）として、対応する確定済みのサービス認可トランザクション情報“ＹＹＹＹ”が使用される。入力（送信元）として、デバイスＢの署名とデバイスＢの公開鍵（Ｄ公開鍵）とが設定される。出力（宛先）として、送金額０と、サービス＃２の公開鍵（Ｓ公開鍵）が設定される。また、フォーマット内の記載情報には、Ｓ公開鍵で暗号化された端末２（デバイス）の位置情報及びセンサデータが設定される。

【００９８】

位置情報は、例えば端末２が有するＧＰＳ受信機１７を用いて取得される。但し、端末２以外で検出又は測定された位置情報であっても良い。センサデータは端末２が備えるセンサのセンシングデータである。センサデータは、サービス処理に使用されるデータ（クラウドでのデータの蓄積や演算処理等の対象のデータ（アプリデータと称する））の一例である。アプリデータはセンサデータに制限されない。アプリデータは「サービスでの処理対象のデータ」の一例である。

【００９９】

図１７はサービス処理トランザクション（サービス処理Ｔｘ）のデータ構造例を示す。サービス処理トランザクションはサービスに係る処理を実行するサービスプロバイダ（サーバ４）によって発行される。

【０１００】

図１７には、或るサービス（サービス＃５）から或る端末２（デバイスＸ）へのサービス処理トランザクションが例示されている。サービス処理トランザクションの送信元はサービスであり、宛先は端末２（デバイス）である。

【０１０１】

前のトランザクションのハッシュ値（前の入力Ｔｘハッシュ）として、対応する確定済みのサービス申込トランザクション情報、又はサービス処理要求トランザクション情報が使用される。入力（送信元）として、サービス＃５の署名とサービス＃５の公開鍵（Ｓ公開鍵）とが設定される。出力（宛先）として、送金額０と、デバイスＸの公開鍵（Ｄ公開鍵）が設定される。また、フォーマット内の記載情報には、サービス＃５の公開鍵で暗号化されたセッションＩＤ，処理内容区分（サービス処理，接続切替処理），接続先（例えば切替先ＧＷ）の場所（処理の実行場所），並びに処理結果を含む。また、フォーマット内の記載情報には、デバイスＸの公開鍵で暗号化されたセッションＩＤ，処理内容区分及び処理場所，及び処理結果が含まれる。フォーマット内の記載情報には、さらに、サービス＃５の公開鍵で暗号化されたデバイス位置情報と、サービス＃５の公開鍵で暗号化されたセッション情報とが含まれる。

【０１０２】

図１８に示すように、所定期間内に発行されたサービス申込トランザクション，サービス認可トランザクション，サービス要求トランザクション，サービス処理トランザクションは、マイナーによりＢＣをなす一つのブロックにまとめられる。マイニングは、エッジサーバ３又はサーバ４で実行されてもよく、第２の分散ストレージの管理者によって実行されても良い。

【０１０３】

＜デバイスのサービス申込（サービス登録）手続＞

図１９は端末２（デバイス）の登録手続を示すシーケンス図であり、図２０は、登録手続に係る端末２及びサーバ４の処理例を示すフローチャートである。

【０１０４】

＜＜図１９（１）の処理＞＞

端末２（デバイス）のメモリ１２には、専用のアプリケーションプログラムがインスト

ールされる。端末２のＣＰＵ１１は、インストールされたアプリケーションプログラムの実行によってデバイスの秘密鍵及び公開鍵（Ｄ秘密鍵／Ｄ公開鍵）を生成する。Ｄ秘密鍵は端末２（デバイス）で秘匿管理される。端末２はＤ公開鍵をトランザクションの送信元／宛先の情報として第２の分散ストレージ５２上で公開する。端末２（デバイス）は、提供乃至利用を所望する各サービスの公開鍵（Ｓ公開鍵）を第２の分散ストレージ５２から取得する。さらに、端末２（デバイス）は、認証局（ＣＡ）の電子証明書を事前にメモリ１２に保持し、認証局の署名つきのデバイス証明書を生成する（図２０の１１１）。

【０１０５】

＜＜図１９（２）の処理＞＞

端末２（デバイス）のＣＰＵ１１は、利用を所望するサービスのサービス申込トランザクション（図１４）を生成し、クラウド（サーバ４）又はエッジサーバ３（ＧＷ）宛てに送信する（図２０の１１２）。図１９及び図２０の例では、サービス申込トランザクションはクラウド（サーバ４）に送信される。

【０１０６】

＜＜図１９（３）の処理＞＞

サーバ４のＣＰＵ１１は、サービス申込トランザクションを第２の分散ストレージ５２（ＢＣ）に登録する（図２０の１１３）。サービス申込トランザクションは、マイニング（ブロックの確定処理）によって確定される。この契機で、サービス処理トランザクションの対象サービスに対応するサービスプロバイダがデバイスのユーザ向けに課金を決定するようにしてもよい。

【０１０７】

＜＜図１９（４），（５）の処理＞＞

サービス申込トランザクションの確定処理が終了すると（図２０の１１４のＹｅｓ）、サーバ４のＣＰＵ１１は、サービス認可トランザクションを発行して第２の分散ストレージ５２に登録する。また、ＣＰＵ１１は端末２（デバイス）に送信する（図１９＜４＞、図２０の１１５）。

【０１０８】

サービス認可トランザクションには、対応するサービス申込トランザクションの情報（前のトランザクション（入力Ｔｘ）のハッシュ値）が含まれる。端末２（デバイス）はサービス認可トランザクションを受信し、保持する（図２０の１１６）。

【０１０９】

＜動作例１：サービス要求及びサービス処理手続き（アプリケーション側でデバイスを認証するケース）＞

図２１及び図２３は、サービス要求トランザクション及びサービス処理トランザクションに係る動作例を示すシーケンス図である。図２２及び図２４はサービス要求トランザクション及びサービス処理トランザクションに係る処理例を示すフローチャートである。図２２及び図２３の処理は、端末２及びエッジサーバ３の各ＣＰＵ１１によって実行される。

【０１１０】

＜＜図２１（１）の処理：暗号化通信手続＞＞

図２１の（１）では、通信を所望する端末２（デバイス）が、初回接続用に設定された接続先ＧＷ（エッジサーバ３）やクラウド（サーバ４）について、クライアント認証無しの暗号化通信手続き（ＳＳＬ／ＴＬＳに基づくネゴシエーション）を実行する（図２２の１２１）。図２１（１）の暗号化通信手続きは、図２（Ａ）に示した初回アクセス時の手順と同じであるので説明を省略する。

【０１１１】

＜＜図２１（２）の処理：サービス要求トランザクション＞＞

端末２（デバイス）は、利用を所望するサービスに係るサービス要求トランザクション（図１６）を発行する。サービス要求トランザクション中の、前のトランザクションのハッシュ値（前の入力Ｔｘハッシュ）には、対応するサービス認可トランザクションの情報

が設定される。また、サービス要求トランザクションのフォーマット内の記載情報には、対応するサービスの公開鍵（Ｓ公開鍵）で暗号化した端末２自身の位置情報やセンサデータが設定される。

【０１１２】

サービス要求トランザクションは、初回接続ＧＷ（エッジサーバ３）又はクラウド（サーバ４）へ送信される（図２２の１２２）。図２１の例では、サービス要求トランザクションは初回接続ＧＷに当たるエッジサーバ３へ送信される。エッジサーバ３は、サービス要求トランザクションを第２の分散ストレージに登録する（図２２の１２３）。

【０１１３】

＜＜図２１（３）の処理：デバイス署名検証、サービス処理＞＞

エッジサーバ３は、サービス要求トランザクション（図１６参照）に含まれるデバイスの電子署名が正当であるかを検証する（図２２の１２４）。すなわち、エッジサーバ３は、サービス要求トランザクション中の入力に設定されたデバイスの署名を同じく入力に設定されたデバイスの公開鍵で復号し、復号結果がデバイス署名記載前のトランザクションのハッシュ値と同じであれば、デバイスの署名が正当と判定する。

【０１１４】

デバイスの署名が正当と判定される場合には、エッジサーバ３は、サービス要求トランザクション中のフォーマット内の記載情報の暗号化データをサービス要求トランザクション中のＳ秘密鍵で復号し、位置情報及びセンサデータを得る。エッジサーバ３は端末２（デバイス）の位置情報に基づき、サービス要求に対応する処理をエッジサーバ３自身で実行するかを判定する（図２２の１２５）。

【０１１５】

例えば、端末２との距離がより近い他のエッジサーバ３がない場合には、エッジサーバ３はサービス処理を自身で実行すると判定する。これに対し、端末２との距離がより近い他のエッジサーバ３がある場合には、エッジサーバ３はサービス処理を他のエッジサーバ３で行うべきと判定し、端末２の接続先をその他のエッジサーバ３へ変更する（切り替える）ことを決定する。

【０１１６】

１２５の処理において、エッジサーバ自身がサービス処理を実行すると判定される場合、エッジサーバ３は、例えばセンサデータを用いてサービス処理を実行する（図２２の１２６）。エッジサーバ３はサービス処理の結果に応じたサービス処理トランザクション（図１７）を発行し、第２の分散ストレージ５２に登録する（図２２の１２７）。

【０１１７】

エッジサーバ３は、さらに、サービス処理トランザクションをサービス要求トランザクションの発行元のデバイス（端末２）に送信する（図２２の１２８）。サービス処理トランザクションは端末２に受信される（図２２の１２９）。

【０１１８】

ところで、１２５の処理で、サービス処理を他のエッジサーバ３で実行すると判定される場合には、エッジサーバ３は接続先切替の情報（サービス接続先変更指示：他のエッジサーバ３の情報を含む）をデバイス（端末２）に通知する（図２２の１３０）。さらに、エッジサーバ３は、Ｓ秘密鍵で暗号化された接続切替情報（処理内容区分：接続切替）及びセッション情報を含むサービス処理トランザクションを発行し、第２の分散ストレージ５２に登録するとともに端末２（デバイス）へ送信する（図２２の１３１）。

【０１１９】

セッション情報は、例えば、プロトコルのバージョン（ＳＳＬ／ＴＬＳのバージョン），暗号化に必要な乱数情報（例えば、プリマスタシークレット及び乱数），セッションＩＤ，暗号化方式やデータの圧縮形式を含む。或いは、セッション情報は通信用の共通鍵情報そのものを含んでも良い。

【０１２０】

なお、サービス処理トランザクションには、サービスプロバイダ用にＳ公開鍵で暗号化

されたサービス処理結果のデータと、デバイス参照のためにＤ公開鍵で暗号化されたサービス処理結果のデータとが含まれる。

【０１２１】

これにより、エッジサーバ３（ＧＷ）やクラウド（サーバ４）は、暗号化のセッション情報を共有することができる。また、分散ストレージの情報の管理者が、登録されたトランザクションに含まれる署名情報を検証し、それらのトランザクションを束ねて、改ざん不能な情報に纏め、定期的に確定処理（マイニング）を実行する。この契機で、該当サービスを持つサービスプロバイダがデバイスユーザに対する課金を決定してもよい。

【０１２２】

＜＜図２３の（４）の処理：暗号化通信手続き＞＞

図２３に示すように、２回目以降の接続に関して、端末２（デバイス）は初回接続時に生成されたセッションＩＤを保持し、セッションＩＤを含む暗号化通信要求（ＳＳＬ／ＴＬＳのClientHello）の送信することで、セッションＩＤを指定する。接続先のエッジサーバ３が変更される場合、端末２は、サーバ接続先変更指示で指定されたエッジサーバ３宛てにセッションＩＤを含むClientHelloを送信する。セッションＩＤは指定情報の一例である。

【０１２３】

セッションＩＤの指定を含むClientHelloを受けたエッジサーバ３（ＧＷ）は、ローカルストレージ（メモリ１２）に記憶された分散ストレージのコピーを参照し、対応するサービス処理トランザクション中のセッション情報を取得する。エッジサーバ３はセッション情報を利用することで、再度鍵交換のネゴシエーションすることなく、端末２との暗号化通信を開始することができる。

【０１２４】

端末２がセッションＩＤを指定しない場合、或いは、セッションＩＤに対応するセッション情報が無い場合は、図２１の（１）に示した初回接続と同じプロセスが実行される。端末２（デバイス）がセッション情報を新規に更新したい場合は、セッションＩＤを指定しなければよい。

【０１２５】

＜＜図２３（５）及び（６）の処理＞＞

図２３（５）及び（６）の処理は、図２１における（２）及び（３）と同じ処理であるため説明を省略する。

【０１２６】

図２４は、２回目以降の接続時における端末２（デバイス）及びエッジサーバ３（ＧＷ）の処理例を示すフローチャートである。図２４の処理は、端末２及びエッジサーバ３のそれぞれにおけるＣＰＵ１１によって実行される。

【０１２７】

１４１の処理では、端末２はセッションＩＤを指定した暗号化通信要求（ClientHello）を送信する。１４２では、エッジサーバ３が暗号化通信要求を受信する。１４３では、エッジサーバ３は、分散ストレージにセッションＩＤに対応するセッション情報が記憶されているか否かを判定する。セッション情報が記憶されていないと判定される場合には、図２４の処理が終了する。この場合、図２２の１２１から処理が再開される。

【０１２８】

１４３にてセッションＩＤに対応するセッション情報が記憶されていると判定される場合には、エッジサーバ３は、セッション情報を用いた暗号化通信手続を実行する。これにより、通信鍵交換が少なくとも省略されるので、暗号化通信手続が短縮化される。

【０１２９】

１４５において、端末２はエッジサーバ３との暗号化通信手続が終了した後に、サービス要求トランザクションを発行（生成）し、エッジサーバ３へ送信する。その後は、図２２に示した１２３以降の処理と同じ処理が実行されるので、処理の説明は省略する。

【０１３０】

＜動作例２：サービス要求及びサービス処理手続き（ＳＳＬ／ＴＬＳプロトコル内でデバイス認証を行うケース）＞

動作例２では、アプリケーション側でのデバイス認証は行われず、暗号化通信プロトコル内で認証が実行される。図２５及び図２６は動作例２に係るシーケンス図であり、図２７は動作例２に係るＣＰＵの処理例を示すフローチャートである。

【０１３１】

図２５において、通信を所望する端末２（デバイス）が、初回接続用に設定された接続先ＧＷ（エッジサーバ３）やクラウド（サーバ４）に対して、クライアント認証付の暗号鍵生成手続き（ＳＳＬ／ＴＬＳのネゴシエーション）を実行する。動作例１（図２１）との違いは、以下である。

【０１３２】

１．エッジサーバ３から端末２へデバイス認証用の証明書を要求するCertificateRequestが送信されている。

２．端末２からエッジサーバ３へデバイス証明書を含むClientCertificateが送信されるとともに、デバイス証明書に対する署名（CertificateVerify）がエッジサーバ３へ送信される。

３．CertificateVerifyを受信したエッジサーバ３はデバイス証明書を用いて署名を検証し、署名（デバイス証明書）が正当か否かを判定する。

【０１３３】

上記１～３を除き、動作例２に係る図２５の処理は図２１の処理と同じであるので説明を省略する。また、動作例２に係る図２６における処理は、動作例１（図２３）における（６）デバイス署名検証処理が行われない点を除き、動作例１と同じであるので説明を省略する。

【０１３４】

図２７は動作例２に係るＣＰＵ１１の処理例を示すフローチャートである。動作例２では、図２２における１２１の処理（クライアント認証無しの暗号化通信手続）の代わりに、１２１Ａの処理（クライアント認証付きの暗号化通信手続）が行われる。また、動作例２では、動作例１における１２４の処理（電子署名の検証）が行われない。これらの点を除き、動作例２における処理は動作例１と同じであるので説明を省略する。

【０１３５】

＜動作例３＞

動作例３として、暗号化に必要なセッション情報を含むトランザクションデータの保持範囲の制御について図２８及び図２９を用いて説明する。図２８は、トランザクションデータの保持範囲（カバレッジ）を模式的に示す図であり、図２９は、エッジサーバ３（ＧＷ）のＣＰＵ１１によって実行される処理例を示すフローチャートである。

【０１３６】

動作例３では、端末２（デバイス）からのサービス要求トランザクションに記載された端末２（デバイス）の位置情報に従って、該当の端末２（デバイス）の暗号化に必要な乱数情報（例えば、プリマスタシークレット及び乱数）を含むトランザクションの保有範囲を周辺のエッジサーバ３（ＧＷ）に制限する。これによって、エッジサーバ３（ＧＷ）での不必要なトランザクション情報の保持を回避する。

【０１３７】

図２９における１５１の処理において、各エッジサーバ３（ＧＷ）のメモリ１２に、セッション情報を保有するデバイスの管理範囲（カバレッジ）の情報が記憶されるカバレッジ定義ＤＢ３２が記憶される。図２８に示すように、カバレッジは、エッジサーバ３の位置から所定距離内にある地理的なエリアである。カバレッジの大きさ、形状は適宜設定可能である。カバレッジ同士が重複エリアを有しても良い。エッジサーバ３（ＧＷ）やクラウド（サーバ４）では、トランザクション情報が第２の分散ストレージ５２に登録されるたびに、トランザクション情報のコピーがエッジサーバ３やサーバ４のメモリ１２（ストレージ２１、ストレージ３１）に反映される。

【０１３８】
例えば、エッジサーバ３は、Ｋ個の位置情報を含むトランザクション情報を得たと仮定する（図２９の１５２）。この場合、エッジサーバ３は、カウンタ値ｉの値を初期値“１”に設定し（１５３）、トランザクション情報を１つ抽出して、位置情報がカバレッジの範囲内か否かを判定する（１５４）。位置情報がカバレッジの範囲外と判定される場合には、トランザクション情報が破棄される（１５５）。これに対し、位置情報がカバレッジの範囲内と判定される場合には、トランザクション情報が維持される（１５６）。
【０１３９】
１５５又は１５６の処理が行われた場合には、カウンタ値ｉがインクリメントされる（１５７）。その後、カウンタ値ｉがＫより大きいかが判定され（１５８）、ｉがＫより大きくなければ処理が１５４に戻される。これによって、Ｋ個のトランザクション情報のうち、カバレッジ範囲内のトランザクション情報がメモリ１２に残り、範囲外のトランザクション情報は破棄される。
【０１４０】
ブロックチェーンを利用する場合は、一部のトランザクションデータのみ保有することが可能になる、ＳＰＶ（Simple Payment Verification）の仕組みで前記方法で判断された不必要なトランザクション情報は削除することが可能になる。
【０１４１】
＜他サービスとの連携＞
実施形態に係るトランザクション（メッセージ）情報の分散ストレージ上での共有は、ＳＳＬ／ＴＬＳの鍵情報（暗号化通信のセッション情報）に限定されない。例えばＩＰｓｅｃなどＳＳＬ／ＴＬＳ以外のプロトコルに基づき生成された鍵情報を分散ストレージで共有するのに使用することができる。
【０１４２】
また、暗号鍵情報を特定のサービスに開示することによって、端末２（デバイス）－エッジサーバ３間の暗号化通信データが経由する経路上のパケットキャプチャ装置において暗号化データの復号及び解析が可能となる。
【０１４３】
また、サービスプロバイダは、サービスプロバイダ自身が提供するサービスの処理履歴を参照することで、課金処理などを実行できる。
【０１４４】
さらに、図３０に示すように、エッジサーバ３の入出口にレイヤ７（Ｌ７）のファイヤウォールを配備する場合がある。ファイヤウォール（プログラム実行によりファイヤウォールとしての処理を行うＣＰＵ）は、パケットのペイロード部が不正情報を含むかの検査を実行する。しかしながら、ＳＳＬ／ＴＬＳに基づく暗号化通信ではパケットのペイロード部は暗号化される。このため、ペイロート部にある不正な情報の検査が困難になる。
【０１４５】
上記問題に鑑み、ファイヤウォールが分散ストレージ５２で管理されるセッション情報から暗号鍵(ＳＳＬ／ＴＬＳで生成される共通鍵)を取得することにより、暗号化されたペイロード部を暗号鍵の情報を用いて復号化することができ、ペイロード内の不正な情報を検査することも可能になる。
【０１４６】
＜実施形態の効果＞
実施形態に係るエッジサーバ３は、クラウド（サーバ４）と前記クラウド（サーバ４）にサービスを要求する端末２との間に他のエッジサーバ３とともに配置される。エッジサーバ３は端末２について前記要求より前に生成された暗号鍵情報がクラウド（サーバ４）及び少なくとも１つの他のエッジサーバ３と共有される共有情報に含まれている場合に暗号鍵情報を用いて端末２との暗号化通信を開始する制御部（ＣＰＵ１１）を含む。これによって、暗号鍵情報を用いることで、暗号鍵の生成に係る処理を省略できるので、通信が開始されるまでの時間を短縮することができる。

【０１４７】
実施形態に係るエッジサーバ３のＣＰＵ１１（制御部の一例）は、エッジサーバ３への接続を要求する端末２との間で新たな暗号鍵情報を生成した場合に、新たな暗号鍵情報を共有情報（ＢＣ）に含める処理を行う。これによって、クラウド及びエッジサーバ３間で暗号鍵情報が共有されるので、その後に端末２からの接続が要求されたエッジサーバ３又はクラウド（サーバ４）が暗号鍵情報を用いることが可能となる。
【０１４８】
実施形態に係るエッジサーバ３のＣＰＵ１１は、共有情報がブロックチェーン形式で保管される場合に、新たな暗号鍵情報を含むトランザクション情報を生成する。ＢＣを用いたトランザクション情報をＢＣにより管理することで、ユーザ全員で監視可能で且つ改竄が困難な記録を保持することができる。
【０１４９】
実施形態に係るエッジサーバ３のＣＰＵ１１は、Ｐ公開鍵とＳ公開鍵とＧ公開鍵とがエッジサーバ３とサービスプロバイダとの間で共有されている場合に、サービスプロバイダがＧ公開鍵を用いて暗号化されたサービスの秘密鍵及びサービスの証明書を受け取る。これによって、エッジサーバ３がセキュアなＳ秘密鍵及びサービス証明書を受け取ることができる。エッジサーバ３は、Ｓ秘密鍵をサービス認可トランザクションやサービス処理トランザクションの生成に使用できる。また、サービス証明書はＳＳＬ／ＴＬＳの手順に使用される。すなわち、エッジサーバ３がクラウドの代わりに振る舞うための情報の授受を秘密状態の確保された状態で行うことが可能となる。
【０１５０】
実施形態に係るエッジサーバ３のＣＰＵ１１は、Ｄ公開鍵とＳ公開鍵とが端末２，エッジサーバ３及びクラウドとの間で共有されている場合に、サービス申込トランザクションを端末２から受信して共有情報に含める。サービス申込トランザクションは、送信元に端末２が指定され、宛先にサービスが指定され、ハッシュ値と前記ハッシュ値を端末２の秘密鍵を用いて暗号化した端末の署名とを含む。ＣＰＵ１１は、共有情報に含められたサービス申込トランザクションが承認された場合に、サービス認可トランザクションを前記端末に送信する。サービス認可トランザクションは、送信元にサービスが指定され、宛先に端末２が指定され、ハッシュとしてのサービス申込トランザクションの情報と、サービス申込トランザクションの情報をＳ秘密鍵で暗号化したサービスの署名とを含む。このようにすれば、端末２からのサービス申込の履歴とサービス認可の履歴とをトランザクションとしてＢＣにて管理可能となる。
【０１５１】
実施形態に係るエッジサーバ３のＣＰＵ１１は、サービス要求トランザクションを前記端末から受信して前記共有情報に含める。サービス要求トランザクションは、送信元に端末２が指定され、宛先にサービスが指定され、ハッシュとしてのサービス認可トランザクションの情報と、サービス認可トランザクションの情報をＤ秘密鍵で暗号化した端末の署名とを含む。サービス要求トランザクションは、さらにＳ公開鍵で暗号化されたサービスでの処理対象のデータ（アプリデータ）を含む。ＣＰＵ１１は、端末２の署名が正当な場合に、サービス処理トランザクションを前記共有情報に含めるとともに前記端末へ送信する。サービス処理トランザクションは、送信元にサービスが指定され、宛先に端末２が指定され、ハッシュとしてのサービス要求トランザクションの情報とサービス要求トランザクションの情報をＳ秘密鍵で暗号化したサービスの署名とを含む。さらに、サービス要求トランザクションは、端末２の公開鍵とサービスの公開鍵とでそれぞれ暗号化された前記サービスの処理結果を含む。このようにすれば、端末２からのサービス要求の履歴とサービス処理の履歴とをトランザクションとしてＢＣにて管理可能となる。
【０１５２】
エッジサーバ３のＣＰＵ１１は、サービス要求トランザクション中の端末２の署名を端末２の公開鍵を用いて検証することができる。
【０１５３】

エッジサーバ３のＣＰＵ１１は、サービス要求トランザクションに含まれる端末２の位置情報に基づいてサービス要求トランザクションに対応する処理を行うエッジサーバ３以外の端末２の接続先（他のエッジサーバ、クラウド）を特定できる。この場合、ＣＰＵ１１は前記接続先の変更指示と前記接続先の場所を示す情報を端末２に送信する。これにより、端末２の位置から好適な接続先でサービスを受けることができる。

【０１５４】

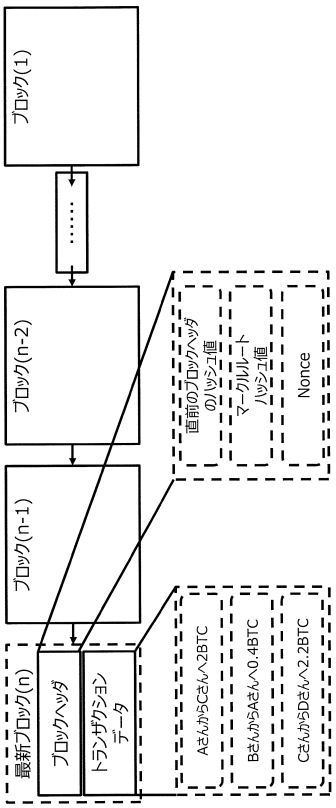
エッジサーバ３のＣＰＵ１１は、端末２の位置が端末２に係るトランザクション情報をエッジサーバ３が管理するカバレッジ外である場合に端末２に係るトランザクション情報を破棄する。これによって、無用のトランザクション情報を保持するのを回避できる。実施形態で説明した構成は、適宜組み合わせることができる。

【符号の説明】

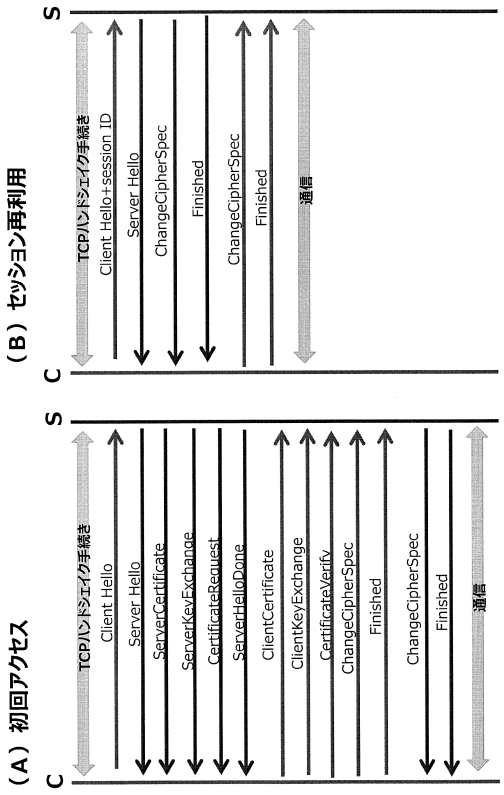
【０１５５】

２・・・端末
３・・・エッジサーバ
４・・・サーバ
１１・・・ＣＰＵ

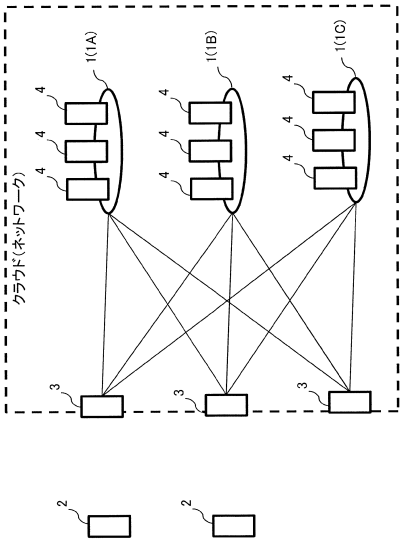
【図１】



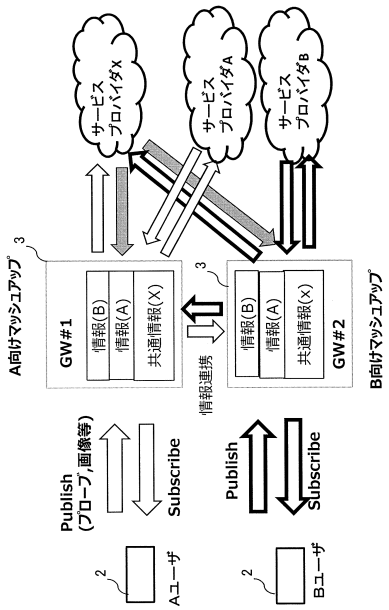
【図２】



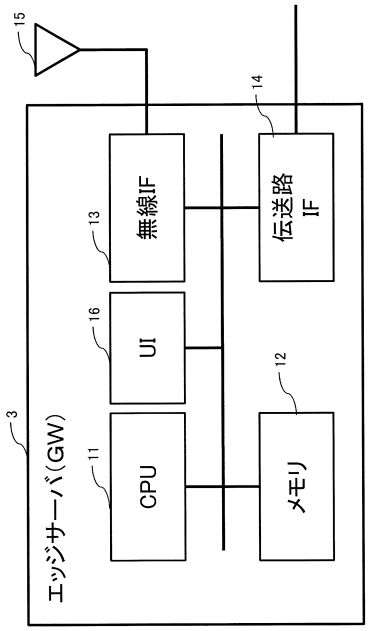
【図３】


クラウド(ネットワーク)
1(1A)
1(1B)
1(1C)
4
3
2

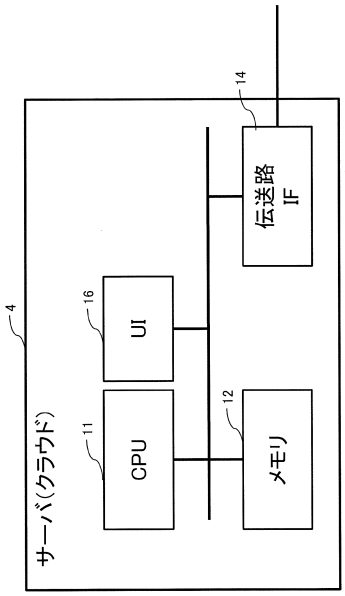
【図４】


サービス プロバイダX
サービス プロバイダA
サービス プロバイダB
A向けマッシュアップ
GW#1
情報(B)
情報(A)
共通情報(X)
情報連携
GW#2
B向けマッシュアップ
Publish (プローブ,画像等)
Subscribe
Publish
Subscribe
Aユーザ
Bユーザ
2
3

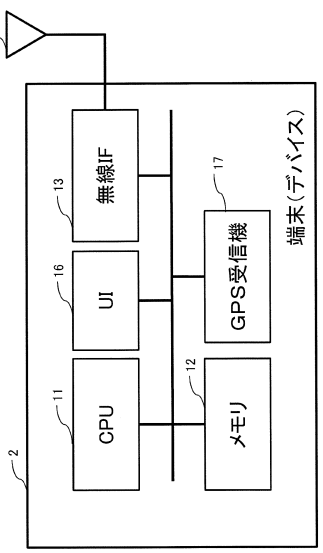
【図５】


エッジサーバ(GW)
CPU
UI
無線IF
メモリ
伝送路 IF
11
12
13
14
15
16
3

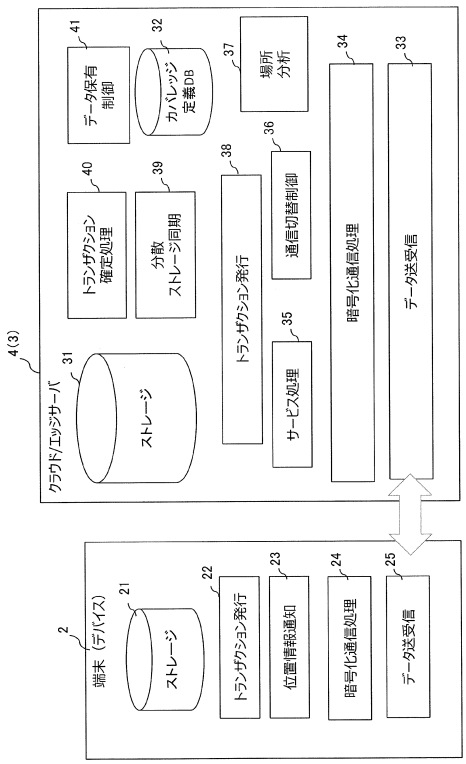
【図６】


サーバ(クラウド)
CPU
UI
メモリ
伝送路 IF
11
12
14
16
4

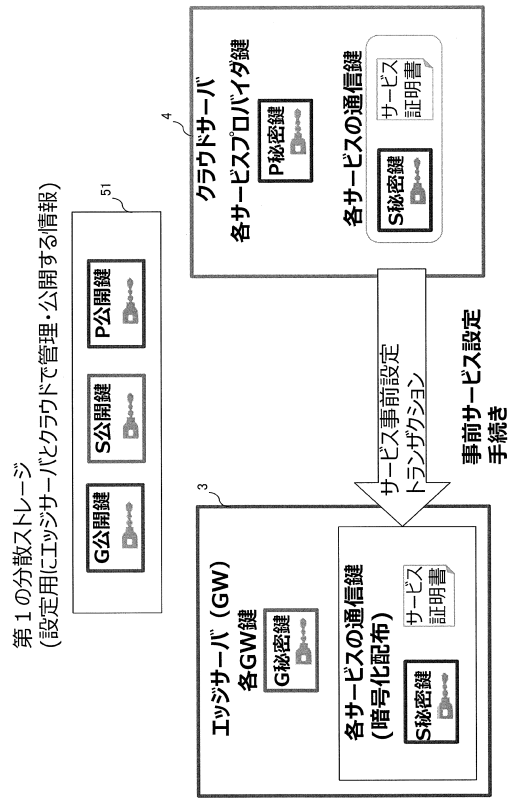
【図７】


15
2
CPU
11
メモリ
12
UI
16
無線IF
13
GPS受信機
17
端末（デバイス）

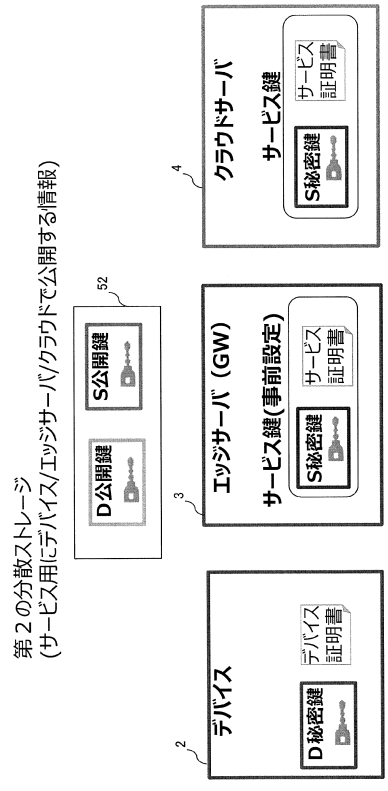
【図８】


4(3)
クラウド/エッジサーバ
ストレージ
31
トランザクション確定処理
40
分散ストレージ同期
39
データ保有制御
41
カバレッジ定義DB
32
トランザクション発行
38
サービス処理
35
通信切替制御
36
場所分析
37
暗号化通信処理
34
データ送受信
33
2
端末（デバイス）
ストレージ
21
トランザクション発行
22
位置情報通知
23
暗号化通信処理
24
データ送受信
25

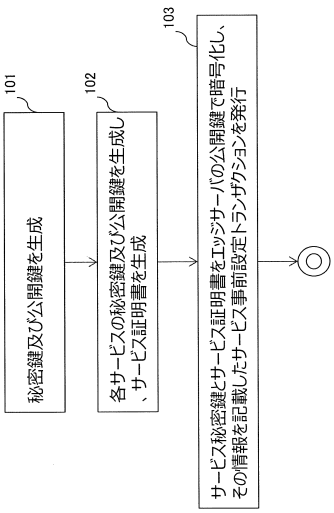
【図９】


第１の分散ストレージ
(設定用にエッジサーバとクラウドで管理・公開する情報)
G公開鍵
S公開鍵
P公開鍵
51
エッジサーバ（GW）
各GW鍵
G秘密鍵
各サービスの通信鍵
(暗号化配布)
S秘密鍵
サービス証明書
3
クラウドサーバ
各サービスプロバイダ鍵
P秘密鍵
各サービスの通信鍵
S秘密鍵
サービス証明書
4
サービス事前設定
トランザクション
事前サービス設定
手続き

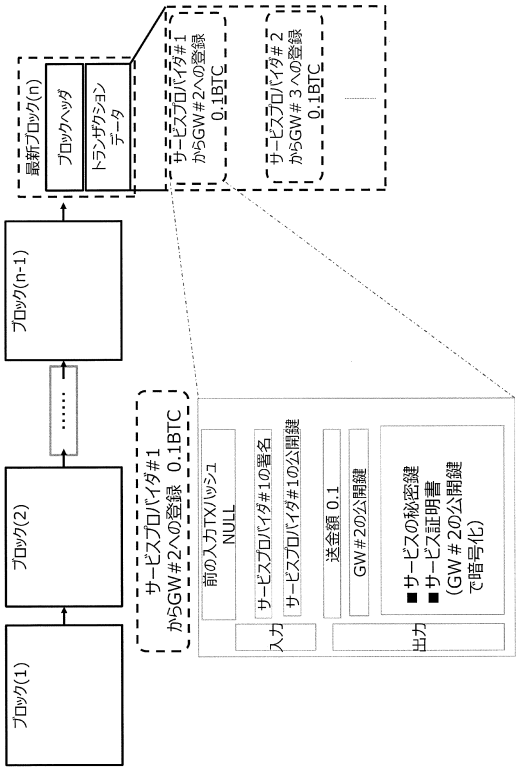
【図１０】


第２の分散ストレージ
(サービス用にデバイス/エッジサーバ/クラウドで公開する情報)
D公開鍵
S公開鍵
52
デバイス
D秘密鍵
デバイス証明書
2
エッジサーバ（GW）
サービス鍵(事前設定)
S秘密鍵
サービス証明書
3
クラウドサーバ
サービス鍵
S秘密鍵
サービス証明書
4

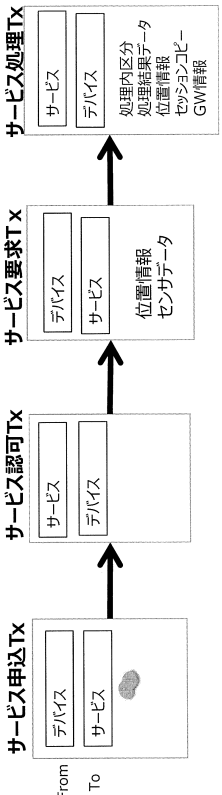
【図１１】



【図１２】

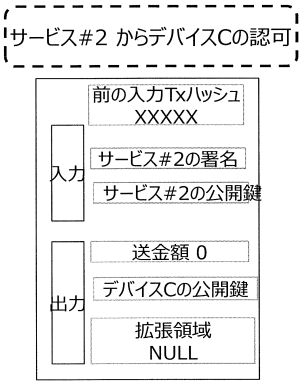


【図１３】

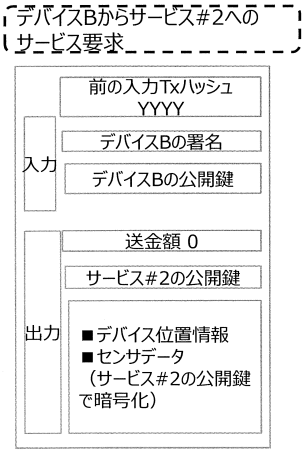


【図１４】

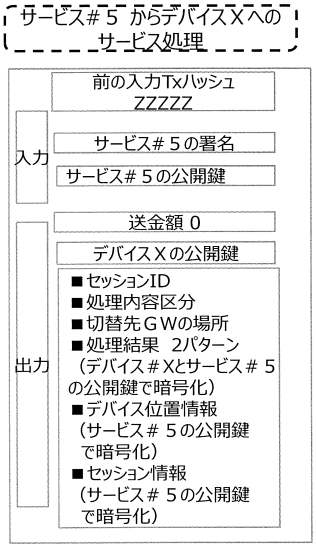
【図１５】



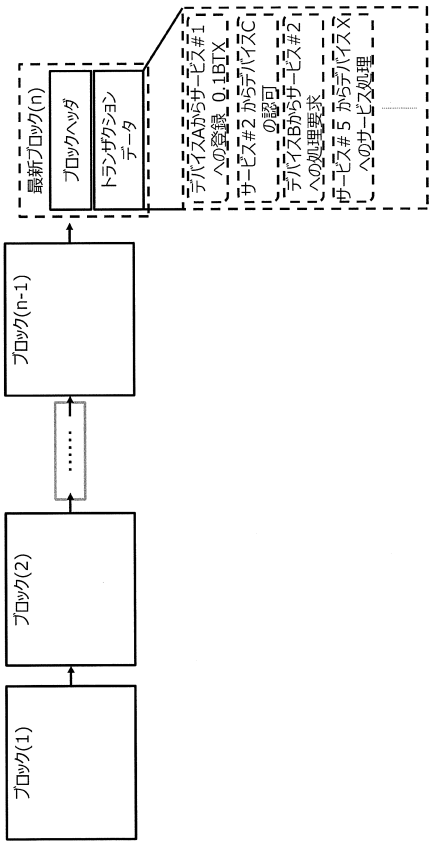
【図１６】



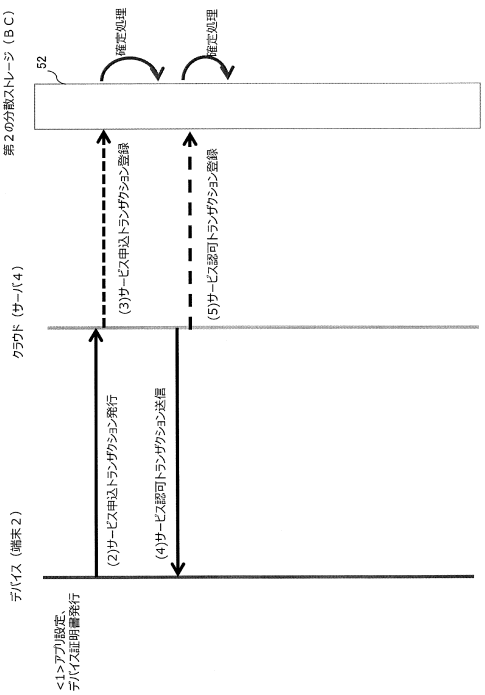
【図１７】



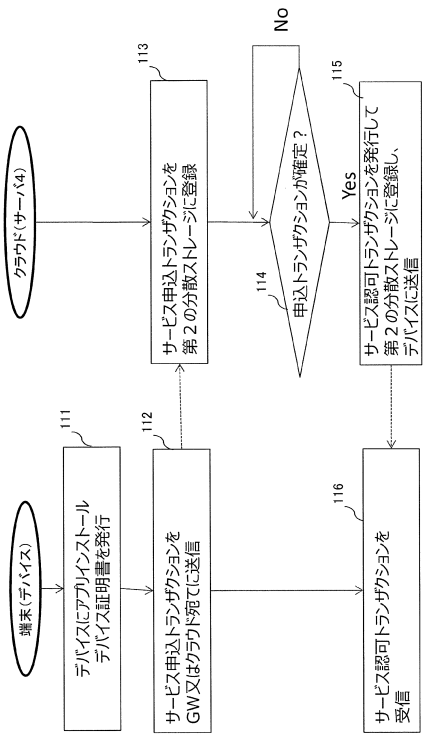
【図１８】



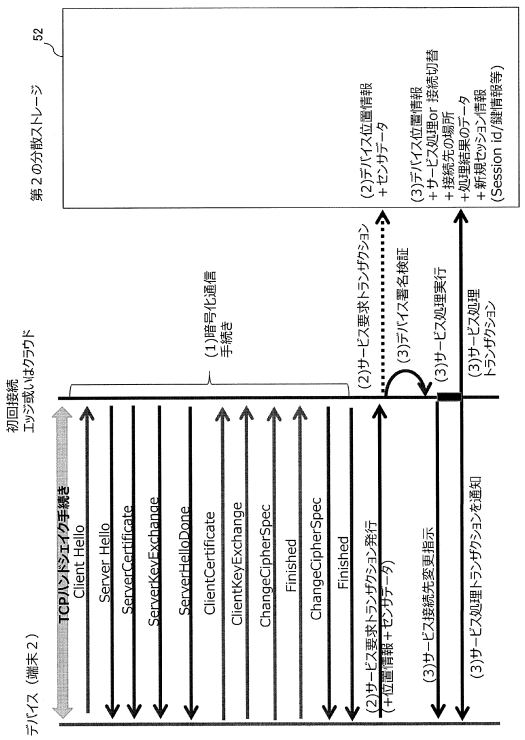
【図１９】



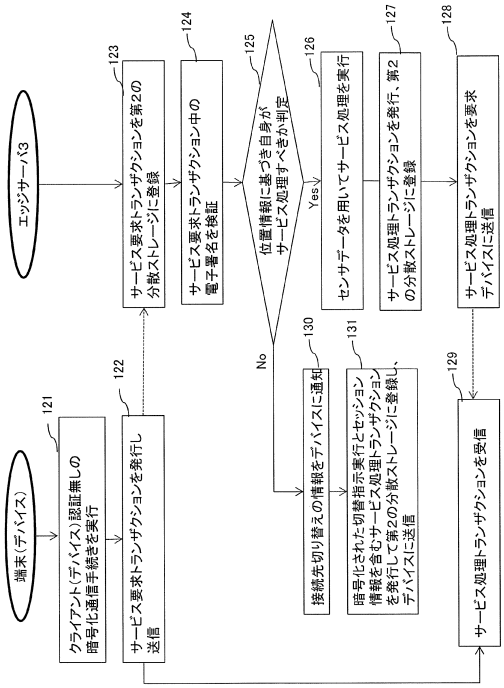
【図２０】



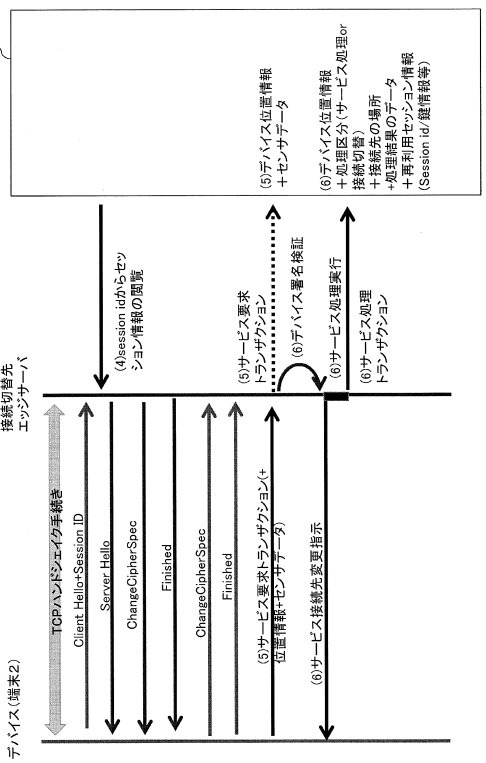
【図２１】



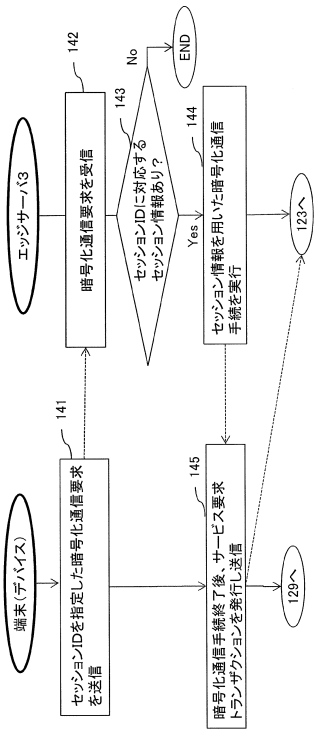
【図２２】



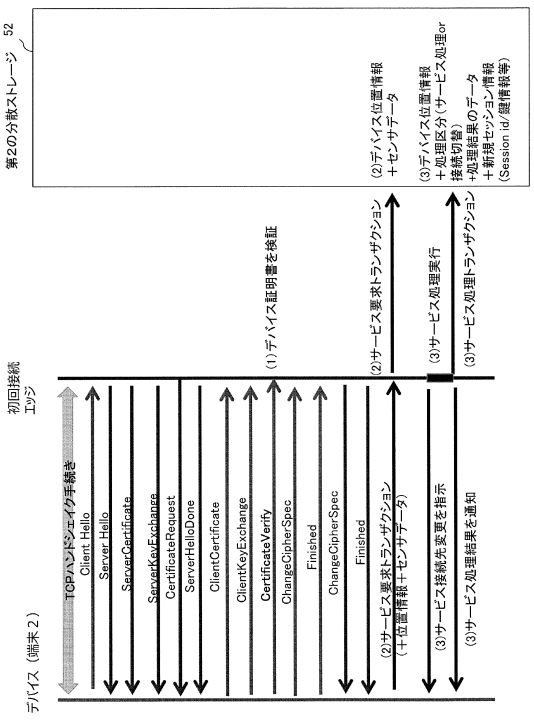
【図２３】



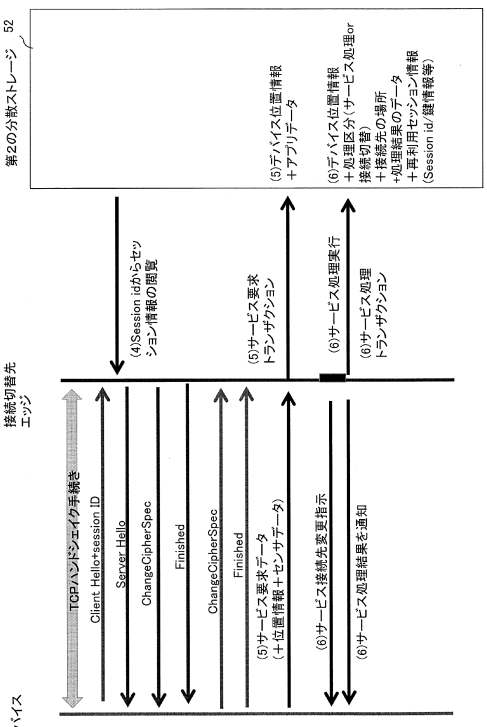
【図２４】



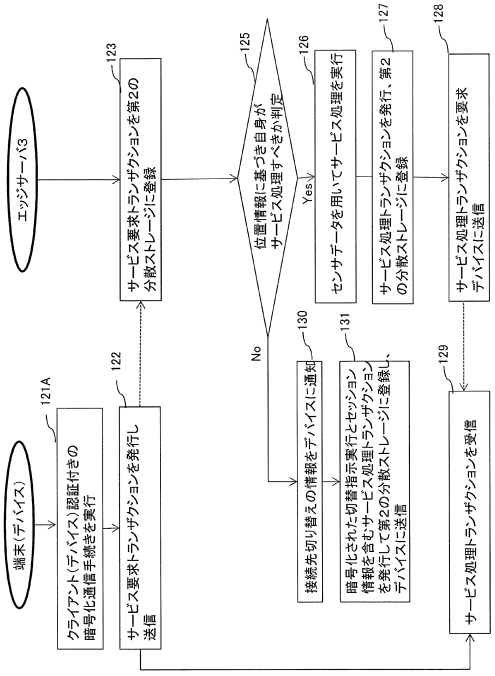
【図２５】



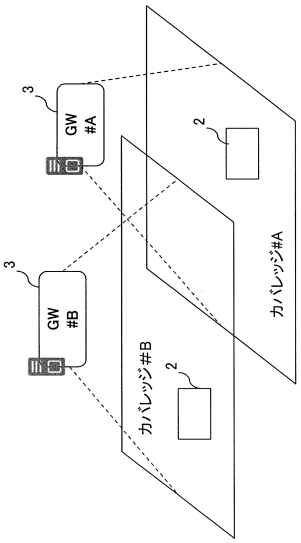
【図２６】



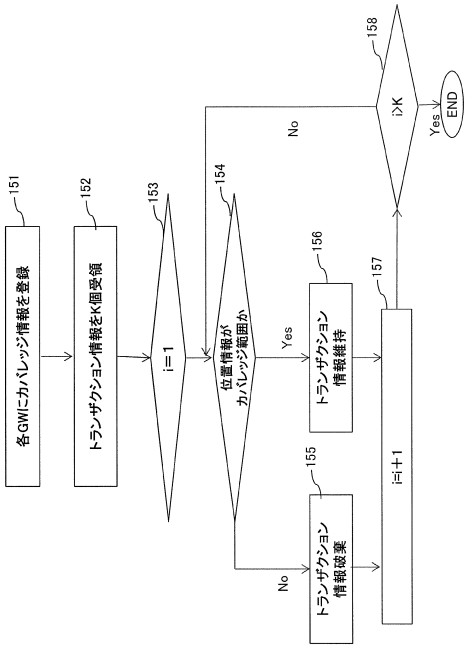
【図２７】



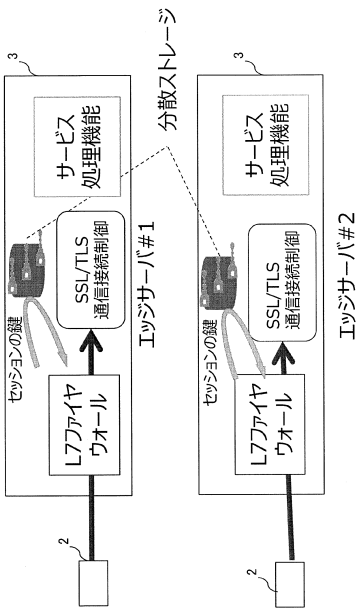
【図２８】



【図２９】



【図３０】



フロントページの続き

(72)発明者　片桐　徹
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　山田　徹哉
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　松平　英

(56)参考文献　特開２００８－１３６１７０（ＪＰ，Ａ）
特開２０１５－１２２７６４（ＪＰ，Ａ）
国際公開第２００６／００９１７２（WO，Ａ１）
特開２００７－２０１５２２（ＪＰ，Ａ）
米国特許出願公開第２００４／００９３４１９（ＵＳ，Ａ１）
次世代仮想通貨研究会，これから買う人の仮想通貨入門，株式会社ＬＵＦＴメディアコミュニケーション，２０１６年　9月１０日，初版，ｐ．８４～８５，ISBN: 978-4-906784-42-4

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ１２／１４
１９／００
２１／００－２１／８８
Ｇ０６Ｑ１０／００－５０／２０
５０／２６－９９／００
Ｇ０９Ｃ　１／００－５／００
Ｈ０４Ｋ　１／００－３／００
Ｈ０４Ｌ　９／００－９／３８