(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-175227
(P2017-175227A)
(43)公開日　平成29年9月28日(2017.9.28)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675D	5J104
H04L 9/08	(2006.01)	H04L	9/00	601F	
G06F 21/44	(2013.01)	G06F	21/44		
G06F 21/31	(2013.01)	G06F	21/31		

審査請求 未請求　請求項の数 8　ＯＬ　（全 29 頁）

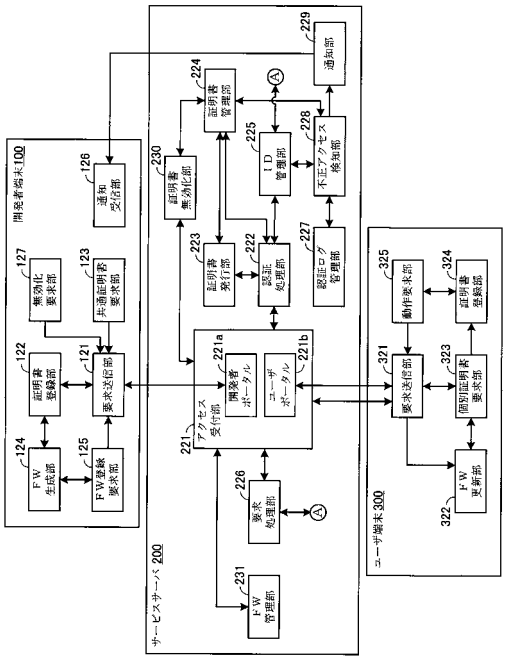
(21)出願番号　特願2016-56165(P2016-56165)
(22)出願日　平成28年3月18日(2016.3.18)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100123881
弁理士　大澤　豊
(74)代理人　100080931
弁理士　大澤　敬
(72)発明者　中島　正登
東京都大田区中馬込１丁目３番６号　株式会社リコー内

Ｆターム(参考)　5J104 AA07 AA16 AA32 EA05 EA08 EA19 JA21 KA02 KA05 NA02 NA36 NA37 NA38 PA07

(54)【発明の名称】証明書管理システム、証明書管理方法及びプログラム

(57)【要約】
【課題】　共通証明書を用いて認証した装置に個別証明書を発行する場合において、共通証明書が流出した場合にその流出がセキュリティやシステムの運用に与える影響を低減する。
【解決手段】　証明書発行部２２３が、複数の装置が共通して使用する共通証明書を発行紙、また、上記共通証明書を用いて認証した装置に対して、その装置に固有の、上記共通証明書と対応する個別証明書を発行する。証明書管理部２２４は、発行済みの共通証明書と上記個別証明書との対応関係を登録する。認証処理部２２２は、上記個別証明書を用いてアクセス元装置を認証する。不正アクセス検知部２２８が、上記個別証明書を用いた所定の条件を満たすアクセスを発見した場合に、通知部２２９により、そのアクセスに用いられた個別証明書と対応する共通証明書の発行先に、その旨を通知する。
【選択図】　図３



【特許請求の範囲】
【請求項１】
複数の装置が共通して使用する電子証明書である第１証明書を発行する第１発行手段と、
前記第１証明書を用いて認証した装置に対して、該装置に固有の、前記第１証明書と対応する電子証明書である第２証明書を発行する第２発行手段と、
発行済みの前記第１証明書と前記第２証明書との対応関係を登録する第１登録手段と、
前記第２証明書を用いてアクセス元装置を認証する認証手段と、
前記第２証明書を用いた所定の条件を満たすアクセスを発見した場合に、該アクセスに用いられた第２証明書と対応する第１証明書の発行先にその旨を通知する通知手段とを備えることを特徴とする証明書管理システム。
【請求項２】
請求項１に記載の証明書管理システムであって、
前記第１証明書の発行先からの要求に従い、該第１証明書と対応する発行済みの第２証明書を無効にする無効化手段とを備えることを特徴とする証明書管理システム。
【請求項３】
請求項２に記載の証明書管理システムであって、
発行済みの第１証明書を格納したファームウェアの情報を登録する第２登録手段と、
前記無効化手段が発行済みの第２証明書を無効にした場合に、該無効にした第２証明書の発行先に、該無効にした第２証明書と対応する第１証明書を格納したファームウェアを更新すべきことを通知する通知手段を備えることを特徴とする証明書管理システム。
【請求項４】
請求項１乃至３のいずれか一項に記載の証明書管理システムであって、
前記第１証明書の発行先と対応付けられた所定の管理者からの要求に従い、一時的に有効な一時認証情報を生成する認証情報生成手段と、
前記第２発行手段は、前記一時認証情報を用いて認証した装置に対して、該装置に固有の前記第２証明書であって、前記所定の管理者と対応する発行先の前記第１証明書と対応する第２証明書を発行することを特徴とする証明書管理システム。
【請求項５】
請求項１乃至４のいずれか一項に記載の証明書管理システムであって、
ユーザのアカウントを登録する第３登録手段と、
登録済みのアカウントを持つユーザからの、管理者を特定した発行要求に応じて、該ユーザに対して、該管理者と対応する有効化情報を発行する第３発行手段と、
前記第２証明書を用いて認証したアクセス元装置から前記有効化情報を受信した場合に、該アクセス元装置を、受信した有効化情報と対応する管理者が管理する装置として登録する登録手段とを備えることを特徴とする証明書管理システム。
【請求項６】
請求項５に記載の証明書管理システムであって、
前記発行要求は、前記第２証明書の発行先装置の位置を示す情報を含み、
前記有効化情報は、前記発行要求に含まれる発行先装置の位置の情報を含むこと特徴とする証明書管理システム。
【請求項７】
複数の装置が共通して使用する電子証明書である第１証明書を発行する第１発行手順と、
前記第１証明書を用いて認証した装置に対して、該装置に固有の、前記第１証明書と対応する電子証明書である第２証明書を発行する第２発行手順と、
発行済みの前記第１証明書と前記第２証明書との対応関係を登録する第１登録手順と、
前記第２証明書を用いてアクセス元装置を認証する認証手順と、
前記第２証明書を用いた所定の条件を満たすアクセスを発見した場合に、該アクセスに用いられた第２証明書と対応する第１証明書の発行先にその旨を通知する通知手順とを備

えることを特徴とする証明書管理方法。
【請求項８】
コンピュータに、請求項７に記載の証明書管理方法の各手順を実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、証明書管理システム、証明書管理方法及びプログラムに関する。
【背景技術】
【０００２】
近年、インターネットなどのネットワーク上で提供されているソフトウェアを利用してサービスを提供する提供形態が普及しつつある。このようなサービスの提供形態として、クラウドサービスが知られている。
【０００３】
情報処理装置がユーザの操作に従い又は自動的にクラウドサービスを提供するサーバに接続してクラウドサービスを利用しようとする場合、情報処理装置自体が、サーバに認証（デバイス認証）を受ける必要があるシステムも知られている。また、この認証を、ＳＳＬ（Secure Sockets Layer）／ＴＬＳ（Transport Layer Security）を利用したクライアント証明書を用いる手法で行うことも知られている。
このようなシステムに関連する技術としては、例えば特許文献１に記載のものが知られている。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
ところで、上記のクライアント証明書を用いたデバイス認証を行う場合、クライアントとなる情報処理装置に予め装置に固有の電子証明書（以下「個別証明書」という）（及びこれと対になる秘密鍵）を記憶させておく必要がある。しかし、多数製造される装置の中でクラウドサービスを利用する装置を特定してその全ての装置に予め個別証明書を記憶させることは困難である。
【０００５】
特許文献１には、このような問題に対応するため、複数の装置に共通の証明書（以下「共通証明書」という）（及びこれと対になる秘密鍵）を一律に記憶させておき、上位装置がその共通証明書を用いて下位装置を認証した場合に、その下位装置のための個別証明書を証明書管理装置から取得して設定することが記載されている。この技術によれば、上位装置は、共通証明書を用いて相手装置の素性をある程度確認した上で、個別証明書を設定することができる。
しかし、特許文献１に記載の技術では、共通証明書は多数の装置が共通に用いるため、外部に流出してしまうとセキュリティに与える影響が大きい。しかし、特許文献１には、この流出が発生した場合の効果的な対処法は開示されていない。
【０００６】
この発明は、このような点に鑑みてなされたものであり、共通証明書を用いて認証した装置に個別証明書を発行する場合において、共通証明書が流出した場合にその流出がセキュリティやシステムの運用に与える影響を低減することを目的とする。
【課題を解決するための手段】
【０００７】
この発明の証明書管理システムは、上記の目的を達成するため、複数の装置が共通して使用する電子証明書である第１証明書を発行する第１発行手段と、上記第１証明書を用いて認証した装置に対して、その装置に固有の、上記第１証明書と対応する電子証明書である第２証明書を発行する第２発行手段と、発行済みの上記第１証明書と上記第２証明書との対応関係を登録する第１登録手段と、上記第２証明書を用いてアクセス元装置を認証す

る認証手段と、上記第２証明書を用いた所定の条件を満たすアクセスを発見した場合に、そのアクセスに用いられた第２証明書と対応する第１証明書の発行先にその旨を通知する通知手段とを設けたものである。

【発明の効果】

【０００８】

上記構成によれば、共通証明書を用いて認証した装置に個別証明書を発行する場合において、共通証明書が流出した場合にその流出がセキュリティやシステムの運用に与える影響を低減することができる。

【図面の簡単な説明】

【０００９】

【図１】この発明の一実施形態である証明書管理システムを構成する装置を含む、各種の装置の配置例を示す図である。

【図２】図１に示したサービスサーバのハードウェア構成を示す図である。

【図３】図１に示した開発者端末、サービスサーバ、およびユーザ端末が備える機能のうち、共通証明書及び個別証明書の取扱に関連する機能の構成を示す図である。

【図４】証明書の信頼の連鎖について説明するための図である。

【図５】開発フェーズにおける図３に示した各部の動作シーケンスを示す図である。

【図６】設置フェーズの、個別証明書を発行する動作における図３に示した各部の動作シーケンスを示す図である。

【図７】図６の続きの図である。

【図８】設置フェーズの、個別証明書をアクティベートする動作における図３に示した各部の動作シーケンスを示す図である。

【図９】図８の続きの図である。

【図１０】設置フェーズの、サービスサーバがサービスを提供する動作における図３に示した各部の動作シーケンスを示す図である。

【図１１】運用フェーズにおける、個別証明書の不正利用を検出した場合の図３に示した各部の動作シーケンスを示す図である。

【図１２】不正アクセスの疑いありと判断する場合の一例を示す図である。

【図１３】運用フェーズにおける、個別証明書を無効化する場合の図３に示した各部の動作シーケンスを示す図である。

【図１４】運用フェーズにおける、共通証明書が無効化された状態でユーザ端末がサービスを利用しようとした場合の図３に示した各部の動作シーケンスを示す図である。

【図１５】サービスサーバが一次認証情報を発行する動作における図３に示した各部の動作シーケンスを示す図である。

【図１６】図１５の続きの図である。

【図１７】ユーザ端末が一時ＵＲＬにアクセスして個別証明書を取得する動作における図３に示した各部の動作シーケンスを示す図である。

【発明を実施するための形態】

【００１０】

以下、この発明の実施形態について、図面を参照しつつ説明する。

図１に、この発明の一実施形態である証明書管理システムを構成する装置を含む、各種装置の配置例を示す。

図１の例において、サービスサーバ２００が、この発明の一実施形態の証明書管理システムである。このサービスサーバ２００は、複数のサーバが協働あるいは連携してその機能を実現するものであってもよいが、ここでは説明を簡単にするため１台の情報処理装置により構成されるシステムであるとして説明する。また、このサービスサーバ２００は、インターネットＮに接続される装置に対して広くサービスを提供するため、クラウド環境２０に配置されている（ただし、インターネットＮ以外の、ローカルネットワーク等のネットワークを用いることも妨げられない）。

【００１１】

また、ユーザ端末３００－１～ｎ（以下、個体を区別する必要がない場合には「－」以降の数字がない符号を用いる。他の符号についても同様である）は、サービスサーバ２００が提供するサービスを利用するユーザが使用する端末装置である。具体的には、ユーザ端末３００は、ＰＣ（パーソナルコンピュータ）、タブレット型コンピュータ、スマートフォン等の汎用性の高い機器であっても、ＭＦＰ（デジタル複合機）、プリンタ、ファクシミリ通信装置、プロジェクタ、電子会議システム等の特定用途向けの機器であってもよい。いずれにせよ、インターネットＮを介してサービスサーバ２００にアクセスして認証を受け、サービスサーバ２００が提供するサービスを利用する機能を備えていればよい。

【００１２】

各ユーザ端末３００は、装置に固有の第２証明書である個別証明書（アクティベートされたもの）を用いてサービスサーバ２００に認証を受けた場合に、サービスサーバ２００が提供するサービスを利用可能である。この点については後述する。

また、ユーザは、ユーザ端末３００にサービスサーバ２００が提供するサービスを利用する機能を追加するため、あるいはその他の用途でも、サービスサーバ２００からファームウェア（ＦＷ）をダウンロードしてユーザ端末３００に記憶させ、実行させることができる。

【００１３】

また、ユーザ端末３００は、単にサービスを利用するだけの一般ユーザではなく、一般ユーザにサービスの利用権を与える等、サービスに関する管理を行う権限を有する管理者も利用することができる。

ユーザ端末３００が配置されるユーザ環境３０は、自宅、会社、学校、公共ネットワークなど、ユーザがユーザ端末３００を使用する任意のネットワーク環境である。なお、図１では各ユーザ環境３０にユーザ端末３００を１台配置しているが、複数台配置されていてよいことはもちろんである。また、ユーザ環境３０にユーザ端末３００以外の装置があってもよいことはもちろんである（このような装置については後に具体例を示す）。

【００１４】

次に、開発者端末１００－１～ｍは、サービスサーバ２００が提供するサービスの機能を実現するためのアプリケーションを開発する開発者が使用する端末装置である。ハードウェアとしては、適宜公知のコンピュータを用いることができる。

開発者端末１００は、サービスサーバ２００から複数のユーザ端末３００が共通して使用する第１証明書である共通証明書の発行を受け、ユーザ端末３００のファームウェアにその共通証明書を埋め込んでサービスサーバ２００に登録することができる。ユーザ端末３００は、このファームウェアをダウンロードして実行することにより、そこに埋め込まれた共通証明書を利用可能となる。

【００１５】

なお、開発者端末１００は、開発者個人というよりは、サービスサーバ２００の運営者と、アプリケーションの開発や提供等について合意した開発企業等が使用する端末装置である。上記共通証明書も、開発者端末１００自体に対してというよりは、サービスサーバ２００の運営者から上記開発企業等に対して発行されるものである。

【００１６】

開発者端末１００が配置される開発者環境１０は、上記開発企業等のネットワーク環境である。なお、１つの開発者環境１０に開発者端末１００が複数あることも妨げられないが、少なくとも発行された共通証明書の管理は開発者環境１０（共通証明書の発行先）内で一元化して行うことが望ましい。開発者環境１０に開発者端末１００以外の装置があってもよいことはもちろんである。

【００１７】

次に、図２に、図１に示したサービスサーバ２００のハードウェア構成を示す。

図２に示すように、サービスサーバ２００は、ＣＰＵ２０１、ＲＯＭ２０２、ＲＡＭ２０３、ＨＤＤ（ハードディスクドライブ）２０４、通信Ｉ／Ｆ（インタフェース）２０５、操作部２０６、表示部２０７を備え、これらをシステムバス２０８により接続した構成

としている。
【００１８】
そして、ＣＰＵ２０１が、ＲＡＭ２０３をワークエリアとしてＲＯＭ２０２あるいはＨＤＤ２０４に記憶されたプログラムを実行することにより、サービスサーバ２００全体を制御し、図３を用いて後述するものをはじめとする種々の機能を実現する。
ＲＯＭ２０２及びＨＤＤ２０４は、不揮発性記憶媒体（記憶手段）であり、ＣＰＵ２０１が実行する各種プログラムや後述する各種データを格納している。
通信Ｉ／Ｆ２０５は、インターネットＮを介して開発者端末１００やユーザ端末３００等の他の装置と通信するためのインタフェースである。
【００１９】
操作部２０６は、ユーザからの操作を受け付けるための操作手段であり、各種のキー、ボタン、タッチパネル等により構成することができる。
表示部２０７は、サービスサーバ２００の動作状態や設定内容、メッセージ等をユーザに提示するための提示手段であり、液晶ディスプレイやランプ等を備える。
【００２０】
なお、操作部２０６及び表示部２０７は外付けであってもよい。また、サービスサーバ２００がユーザからの操作を直接受ける必要がない（通信Ｉ／Ｆ２０５を介して接続された外部装置により操作を受け付けたり情報の提示を行ったりすればよい）場合には、操作部２０６や表示部２０７を設けなくてよい。
【００２１】
開発者端末１００及びユーザ端末３００も、図２に示した範囲のハードウェア構成は基本的に共通である。ただし、機種や性能が同じである必要はないし、ＨＤＤ２０４に代えて他の記憶手段を用いることもできる。
以上説明してきた各装置の機能において特徴的な点の一つは、共通証明書を利用した、各ユーザ端末への個別証明書の設定及び管理に関する機能であり、特に、個別証明書の不正利用が疑われる事態に対する対処に関する機能である。以下、この点について、個別証明書の発行、利用、廃棄のライフサイクルを踏まえつつ説明する。
【００２２】
図３に、開発者端末１００、サービスサーバ２００、およびユーザ端末３００が備える機能のうち、共通証明書及び個別証明書の取扱に関連する機能の構成を示す。図３に示す各部の機能は、各装置のＣＰＵが、所要のプログラムを実行して所要のハードウェアを制御することにより実現されるものである。
【００２３】
図３に示すように、開発者端末１００は、要求送信部１２１、証明書登録部１２２、共通証明書要求部１２３、ＦＷ生成部１２４、ＦＷ登録要求部１２５、通知受信部１２６、無効化要求部１２７を備える。
このうち要求送信部１２１は、他の各部からの要求に基づき、サービスサーバ２００に対して、何からの動作の実行を求める要求を送信する機能を備える。要求送信部１２１による要求の送信は、基本的にオペレータの指示に従って、オペレータからの要求を伝えるものである。オペレータは、まずサービスサーバ２００の開発者ポータル２２１ａのアドレスにアクセスし、開発者認証情報（ここでは開発者ＩＤ及びパスワード）を用いてユーザ認証を受けた上で、開発者端末１００に対してサービスサーバ２００への要求の送信を指示する。
【００２４】
証明書登録部１２２は、サービスサーバ２００から発行された共通証明書を登録する機能を備える。
共通証明書要求部１２３は、オペレータの指示に従い、サービスサーバ２００に対して共通証明書の発行を要求する機能を備える。この要求は、要求送信部１２１からサービスサーバ２００に送信される。
ＦＷ生成部１２４は、オペレータの指示に従い、証明書登録部１２２に登録された共通

証明書（及び対応する秘密鍵）を埋め込んだファームウェアを生成する機能を備える。この埋め込みは、開発済みのファームウェアに共通証明書を付加する形で行うことができる。

【００２５】

ＦＷ登録要求部１２５は、ＦＷ生成部１２４が生成した、共通証明書の埋め込まれたファームウェアを、ユーザ端末３００がダウンロードできるように登録することを、オペレータの指示に従いサービスサーバ２００に対して要求する機能を備える。この要求は、要求送信部１２１からサービスサーバ２００に送信される。

【００２６】

通知受信部１２６は、サービスサーバ２００からの通知を受信する機能を備える。この通知は、例えば電子メールのように、サービスサーバ２００側から任意のタイミングで開発者端末１００に送信できることが望ましい。サービスサーバ２００には、開発者端末１００宛の通知の送信先とするアドレス等を予め登録しておく。

無効化要求部１２７は、オペレータの指示に従い、サービスサーバ２００に対し、開発者端末１００に対して発行された共通証明書（のうち指定したもの）を無効化するよう要求する機能を備える。この要求は、要求送信部１２１からサービスサーバ２００に送信される。

【００２７】

次に、サービスサーバ２００は、アクセス受付部２２１、認証処理部２２２、証明書発行部２２３、証明書管理部２２４、ＩＤ管理部２２５、要求処理部２２６、認証ログ管理部２２７、不正アクセス検知部２２８、通知部２２９、証明書無効化部２３０、ＦＷ管理部２３１を備える。

これらのうちアクセス受付部２２１は、開発者ポータル２２１ａとユーザポータル２２１ｂを備える。

【００２８】

開発者ポータル２２１ａは、オペレータの指示に従った開発者端末１００からのアクセスを受け付ける機能を備える。開発者端末１００のオペレータを未認証であれば開発者端末１００から受信した認証情報を用いて認証処理部２２２にユーザ認証を行わせ、認証済みであれば、開発者端末１００から受信した要求を、その要求を処理する処理部に渡して処理させる。

【００２９】

ユーザポータル２２１ｂは、オペレータ（一般ユーザ又は管理者）の指示に従ったユーザ端末３００からのアクセスを受け付ける機能を備える。ユーザ端末３００のオペレータを未認証であればユーザ端末３００から受信した認証情報を用いて認証処理部２２２にユーザ認証を行わせ、認証済みであれば、ユーザ端末３００から受信した要求を、その要求を処理する処理部に渡して処理させる。

【００３０】

また、アクセス受付部２２１は、ユーザ端末３００からの、共通証明書又は個別証明書を用いた認証の要求を受け付け、認証処理部２２２にそれらを用いたデバイス認証を行わせる機能を備える。また、アクセス受付部２２１は、認証済みのユーザ端末３００から受信した受信した要求を、その要求を処理する処理部に渡して処理させる。

他の各部の機能及び動作については、図５以降のシーケンス図を用いて詳細に説明するため、ここでは簡潔に説明する。

【００３１】

認証処理部２２２は、認証情報を用いたユーザ認証、証明書を用いたデバイス認証、後述するアクティベーショントークンの発行及び検証、一時ＵＲＬの発行など、認証に関する種々の機能を備える。

証明書発行部２２３は、共通証明書及び個別証明書の発行など、証明書の発行に関する種々の機能を備える。

証明書管理部２２４は、発行済みの証明書の管理に関する種々の機能を備える。また、

共通証明書に署名するためのルートＣＡ（Certification Authority）証明書（及び対応する秘密鍵）も記憶する。

【００３２】

ＩＤ管理部２２５は、開発者、管理者、一般ユーザ等の情報を管理する機能を備える。ＩＤ管理部２２５が管理する情報は、ＩＤ、パスワード、通知送信先等である。

要求処理部２２６は、アクセス受付部２２１が受け付けた要求に従った処理を行う機能を備える。この要求に従った処理は、基本的には、サービスサーバ２００が要求元にサービスを提供するための処理である。

【００３３】

認証ログ管理部２２７は、認証処理部２２２が実行した認証処理のログを記録しまた他の各部に提供する機能を備える。

不正アクセス検知部２２８は、認証ログ管理部２２７が記録したログを参照し、サービスサーバ２００に対する個別証明書を用いた不正アクセスを、所定のアルゴリズムに従って監視する機能を備える。

通知部２２９は、不正アクセス検知部２２８が不正アクセスを検知した場合に、その旨を、不正アクセスに用いられた個別証明書と対応する共通証明書の発行先である開発者端末１００に通知する機能を備える。

【００３４】

証明書無効化部２３０は、開発者端末１００からの要求に従い、その開発者端末１００に発行した共通証明書のうち指定されたものを無効化する機能を備える。さらに、共通証明書を無効化した場合に、その共通証明書と対応する（その共通証明書を用いた認証が成功したことに応じて発行した）個別証明書も、全て無効化する機能も備える。

ＦＷ管理部２３１は、開発者端末１００からの要求に従い、ファームウェアを、ユーザ端末３００からダウンロード可能なように記録し、また、ユーザ端末３００からの要求に応じてダウンロードさせる機能を備える。

【００３５】

次に、ユーザ端末３００は、要求送信部３２１、ＦＷ更新部３２２、個別証明書要求部３２３、証明書登録部３２４、動作要求部３２５を備える。

このうち要求送信部３２１は、他の各部からの要求に基づき、サービスサーバ２００に対して、何からの動作の実行を求める要求を送信する機能を備える。要求送信部３２１による要求の送信には、オペレータの指示に従って、オペレータからの要求を伝えるものと、ユーザ端末３００自身からの要求を伝えるものとがある。

【００３６】

オペレータの指示に従った要求の場合、オペレータは、まずサービスサーバ２００のユーザポータル２２１ｂのアドレスにアクセスし、ユーザ認証情報又は管理者認証情報（ここではＩＤ及びパスワード）を用いてユーザ認証を受けた上で、ユーザ端末３００に対してサービスサーバ２００への要求の送信を指示する。

【００３７】

ユーザ端末３００自身からの要求の場合、要求送信部３２１は、サービスサーバ２００のアクセス受付部２２１に対し、個別証明書あるいは共通証明書を用いたデバイス認証の要求を行う。そして、その認証が成功した後、アクセス受付部２２１に対して動作の要求を送信する。なお、認証に用いる証明書は基本的には個別証明書であり、共通証明書を用いるのは特殊な場合である。

【００３８】

ＦＷ更新部３２２は、ユーザ端末３００のファームウェアをＦＷ管理部２３１から取得して更新する機能を備える。取得の要求は、要求送信部３２１からサービスサーバ２００に送信させる。

個別証明書要求部３２３は、ユーザ端末３００に個別証明書が記憶されていない場合に、サービスサーバ２００に対し、個別証明書の発行を要求する機能を有する。発行の要求は、要求送信部３２１からサービスサーバ２００に送信させる。また、この要求に際し、

要求送信部３２１は、アクセス受付部２２１に対し、実行中のファームウェアに埋め込まれている共通証明書を用いた認証を要求する。

【００３９】

証明書登録部３２４は、ユーザ端末３００の個別証明書を登録する機能を備える。共通証明書についても、ファームウェアから取り出して記憶してもよい。

動作要求部３２５は、サービスサーバ２００に対し、サービスの提供に係る種々の動作を要求する機能を備える。この要求は、要求送信部３２１からサービスサーバ２００に送信させる。

【００４０】

ところで、以上説明してきたサービスサーバ２００は、開発者端末１００に対して共通証明書を発行し、ユーザ端末３００に対して個別証明書を発行する。そして、これらの証明書（いずれも電子証明書である）が改ざん等されていないこと、および、証明書を用いた認証を要求してきた要求元装置が確かに個別証明書の発行先装置であることは、図４に示す信頼の連鎖に基づき確認する。

【００４１】

まず、サービスサーバ２００は、図４に示すように、共通証明書を発行する際に、その共通証明書に、ルートＣＡ証明書５００を用いて署名を付す。

ここで、本明細書でいう「証明書」は、公開鍵証明書であり、書誌事項と公開鍵暗号の公開鍵とを含むものである。そして、署名は、その証明書のデータのハッシュ値を署名に用いる証明書の公開鍵と対応する秘密鍵で暗号化した署名データを、証明書に添付して行うことができる。署名済みの公開鍵証明書が転々流通した後でも、署名データを、署名に用いた証明書の公開鍵で復号化し、これを証明書のデータのハッシュ値と比較して一致すれば、証明書が改ざん等されていない（発行時と同内容である）ことを確認できる。

【００４２】

以上から、共通証明書を取得したサービスサーバ２００は、ルートＣＡ証明書５００を用いれば、共通証明書５１０，５２０，５３０が改ざん等されていないことを確認できる。

また、サービスサーバ２００は、個別証明書を発行する際に、共通証明書を用いて署名を付す。従って、例えば共通証明書５１０を用いれば、その共通証明書５１０を用いて署名された個別証明書５１１，５１２が改ざん等されていないことを確認できる。同様に、共通証明書５２０を用いて個別証明書５２１，５２２の、共通証明書５３０を用いて個別証明書５３１，５３２の正当性を確認できる。

【００４３】

従って、ルートＣＡ証明書５００と対応する秘密鍵が流出しない限り、各個別証明書が改ざん等されていないことは、その署名に用いた共通証明書と、ルートＣＡ証明書５００とを用いて確認することができる。このように、ある証明書の正当性を、署名に用いた証明書を順次辿って確認できることを、信頼の連鎖と呼ぶ。ただし、この信頼の連鎖は、途中の証明書と対応する秘密鍵が、正当な所持者以外に流出すると、途切れてしまい、その箇所よりも下流の証明書の正当性を、ルートＣＡ証明書５００を用いて確認できなくなる。

【００４４】

この実施形態では、上述のように、ファームウェアに共通証明書を埋め込んでいることから、同じファームウェアを使用するデバイス（ユーザ端末３００）には、同じ共通証明書を用いて署名した個別証明書を記憶させる。図４の例で、共通証明書５２０が、バージョン「０１」から「０Ａ」のファームウェアに使用されているように、複数のファームウェアに同じ共通証明書を埋め込むことは妨げられない。機種が異なるデバイスのファームウェアに同じ共通証明書を埋め込んでもよい。しかし、共通証明書は特定の開発者端末１００に対して発行するため、ファームウェアの開発者が異なれば埋め込まれる共通証明書も異なることが通常である。

【００４５】

また、証明書の正当な所持者は、証明書と、対応する秘密鍵とをセットで所持している。共通証明書については、ファームウェアをダウンロードした装置は、正当な所持者であると考える。そして、証明書を用いてサービスサーバ２００にデバイス認証を受けたい装置は、何らかのデータを、自身が持つ証明書の公開鍵と対応する秘密鍵で暗号化して、元のデータ及び証明書と共にサービスサーバ２００へ送信する。サービスサーバ２００は、受信した暗号化データを、証明書に含まれる公開鍵で復号化し、元のデータと比較して、一致すれば、送信元の装置は、受信した証明書の正当な持ち主であると判断することができる。また、上記のように、その証明書への署名に用いた各種証明書を順次用いて、証明書が改ざん等されていないことを確認できる。そしてその後、証明書の書誌事項に基づき、その持ち主を認証してよい（サービスサーバ２００の機能を利用させてよい）か否かを判断して、認証の成否を決定することができる。

【００４６】

なお、書誌事項は、例えばＸ．５０９　ｖ３の形式で記述することができる。また、書誌事項としては、発行先デバイスの製造者、種別、用途等を記載することが考えられる。また、個別証明書の場合、発行先デバイスのデバイスＩＤも記載するとよい。また、発行先デバイスが使用するファームウェアのバージョン（共通証明書であれば、埋め込み先のファームウェアのバージョン）が特定できる場合、そのバージョンを記載してもよい。

また、図４に示した各証明書を用いた認証の要求及びそれに対する認証結果の通知は、ＳＳＬ／ＴＬＳ等の、公知のプロトコルを適宜利用して構成することができる。

【００４７】

ところで、サービスサーバ２００が発行する個別証明書のライフサイクルは、概ね以下のフェーズに分かれる。

（１）開発フェーズ：開発者が共通証明書の発行を受けて個別証明書の利用環境を整備する。共通証明書を埋め込んだファームウェアをサービスサーバ２００に登録することを含む。

（２）設置フェーズ：ユーザが納品されたユーザ端末をセッティングし、サービスサーバ２００が提供するクラウドサービスを利用できるようにする。ユーザ端末３００に対して個別証明書を発行し、ユーザからの要求に基づきその個別証明書をアクティベートする。アクティベートした個別証明書を持つユーザ端末３００に対し、サービスサーバ２００がサービスを提供する。

（３）運用フェーズ：セキュリティインシデントを検出し、リカバリする。個別証明書の不正利用（又はそれが疑われる事態）を検出した場合に、不正利用された個別証明書だけでなく、その個別証明書の発行に用いた共通証明書と、同じ共通証明書を用いて発行された他の全ての個別証明書を無効化する。無効化した個別証明書を持つユーザ端末３００に、個別証明書を再発行する。

以下、これらの各フェーズにおける各装置の動作について、図５以降のシーケンス図を用いつつ、順を追って説明する。

【００４８】

まず図５に、開発フェーズにおける各部の動作シーケンスを示す。

図５の動作においてはまず、開発者が開発者端末１００に対し、共通証明書取得指示を行うと共に、開発者認証情報を入力する（Ｓ１１）。この指示は、共通証明書要求部１２３が受け付ける。またこの指示は、まず開発者端末１００を用いて開発者ポータル２２１ａにアクセスし、開発者ポータル２２１ａにより提供される画面から入力する形でもよい。

【００４９】

なお、サービスサーバ２００のＩＤ管理部２２５には、表１に示すように開発者のアカウントを開発者情報として予め登録しておく。すなわち、サービスサーバ２００の運用者は、共通証明書の発行要求等を行うことができる開発者を予め登録しておき、そのＩＤ及びパスワードを開発者認証情報として用いて、開発者を認証する。また、各開発者へ通知を行う際の送信先アドレスとして、ここでは電子メールアドレスを登録している。その他

、開発者の社名、権限、証明書発行許可数等を登録することが考えられる。

【００５０】

【表１】

開発者情報

開発者ＩＤ	パスワード	送信先アドレス	・・・
DevA	******	DevA@aaaa.com	・・・
DevB	******	DevB@bbbb.com	・・・
⋮	⋮	⋮	⋮

【００５１】

ステップＳ１１の指示を受けた開発者端末１００は、まず入力された開発者認証情報を含む認証要求を開発者ポータル２２１ａに対して送信する（Ｓ１２）。開発者ポータル２２１ａは、この要求を認証処理部２２２に渡して認証を実行させる（Ｓ１３）。認証処理部２２２は、開発者認証情報をＩＤ管理部２２５に登録されている開発者情報と照合して認証処理を行い（Ｓ１４）、一体したものがあれば開発者ポータル２２１ａに認証成功の認証結果を返す（Ｓ１５）。開発者ポータル２２１ａは開発者端末１００に認証成功の認証結果を返す（Ｓ１６）。認証失敗であれば同様に認証失敗の応答を返す。

【００５２】

開発者端末１００は、認証成功の認証結果を受けると、開発者ポータル２２１ａに対し、共通証明書発行要求を送信する（Ｓ１７）。このとき、有効期限や暗号強度、証明書と紐付ける属性等の証明条件を指定してもよい。

開発者ポータル２２１ａは、この要求を受けると、その要求が先に認証した開発者からのものであると判断し、先に認証した開発者の開発者ＩＤを添付して共通証明書発行要求を証明書発行部２２３へ送信する（Ｓ１８）。証明書発行部２２３は、この要求に応じて共通証明書を発行する（Ｓ１９）。この動作が第１発行手順の動作であり、第１発行手段の機能に係る動作である。発行要求に証明条件が指定されている場合、その証明条件に合った証明書を発行する。また、この共通証明書には、図４を用いて説明したようにルートＣＡ証明書を用いた署名を付す。

【００５３】

次に、証明書発行部２２３は発行した共通証明書の登録を証明書管理部２２４に対して要求し（Ｓ２０）、証明書管理部２２４はその共通証明書（及び対応する私有鍵）を、発行先開発者の開発者ＩＤと対応付けて登録する（Ｓ２１）。

また、証明書発行部２２３は、発行した共通証明書を共通証明書発行要求に対する応答として開発者ポータル２２１ａに返す（Ｓ２２）。開発者ポータル２２１ａは開発者端末１００に共通証明書を返す（Ｓ２３）。

共通証明書を受け取った開発者端末１００は、証明書登録部１２２にその共通証明書を登録する（Ｓ２４）。

【００５４】

その後、開発者は、ファームウェア（ＦＷ）を開発し、あるいは開発済みのファームウェアを指定し、そのファームウェアをサービスサーバ２００に登録することを指示する（Ｓ３１）。この指示は、ＦＷ登録要求部１２５が受け付ける。またこの指示は、開発者ポータル２２１ａにより提供される画面から入力する形でもよい。

ステップＳ３１の指示を受けた開発者端末１００は、ＦＷ生成部１２４の機能により、指示に係るファームウェアに、証明書登録部１２２に登録されている共通証明書を埋め込む（Ｓ３２）。複数の共通証明書が登録されていれば、そのいずれかを選択して埋め込む。この選択は開発者の指示に従っても、自動で最新のものを選択する等でもよい。

【００５５】

次に、開発者端末１００は、開発者認証情報の入力を受け付けてステップＳ１２～Ｓ１６の場合と同様に認証処理を行う（Ｓ３３）。その後、開発者端末１００は開発者ポータル２２１ａにＦＷ登録要求と共にステップＳ３２で共通証明書を埋め込んだＦＷを送信する（Ｓ３４）。開発者ポータル２２１ａは、この要求に応じてＦＷ管理部２３１にＦＷ登録要求を送信し（Ｓ３５）、ＦＷ管理部２３１がＦＷの登録を行う（Ｓ３６）。この登録の機能は、第２登録手段としての機能である。

【００５６】

以上の動作により、開発者は、共通証明書の発行を受けた上で、その共通証明書を埋め込んだファームウェアを、ユーザ端末３００がダウンロードして実行できる状態とすることができる。

【００５７】

次に、図６及び図７に、設置フェーズにおける、ユーザ端末３００に対して個別証明書を発行する動作における各部の動作シーケンスを示す。

ここでは、共通証明書が埋め込まれたファームウェアをユーザ端末３００にインストールした後、その共通証明書を用いて個別証明書を取得する例について説明する。ユーザ端末３００が持つデバイスＩＤがグローバルユニークであり、共通証明書を外部から取り出せない形でユーザ端末３００に記憶させることができる場合には、この方式が有用である。

【００５８】

図６の動作において、ユーザ端末３００には、個別証明書の取得に先立ち、共通証明書が埋め込まれたファームウェアをインストールする必要がある。ユーザ端末３００のユーザは、まずこのファームウェアをダウンロードするために、サービスサーバ２００にログインすべく、ユーザ端末３００に対し、ログイン指示を行うと共にユーザ認証情報を入力する（Ｓ４１）。この指示は、まずユーザ端末３００を用いてユーザポータル２２１ｂにアクセスし、ユーザポータル２２１ｂにより提供される画面から入力する形でもよい。

【００５９】

なお、サービスサーバ２００のＩＤ管理部２２５には、表２に示すようにユーザのアカウントをユーザ情報として予め登録しておく。すなわち、サービスサーバ２００の運用者は、サービスサーバ２００が提供するサービスを利用するユーザを予め登録しておき、そのＩＤ及びパスワードをユーザ認証情報として用いて、ユーザを認証する。また、各ユーザへ通知を行う際の送信先アドレスとして、ここでは電子メールアドレスを登録している。さらに、そのユーザに提供するサービスを管理する管理者も、ユーザの情報として登録する。この管理者は、開発者と一致している必要はなく、開発者が開発したアプリをサービスサーバ２００を利用して運用し、実際にユーザにサービスを提供する企業等である。複数の管理者が、同じアプリを運用してユーザにサービスを提供する場合もある。その他、ユーザの情報として、ユーザの氏名、住所、サービス利用権限（利用契約の内容）等を登録することが考えられる。以上の登録の機能は、第３登録手段としての機能である。

【００６０】

【表２】

ユーザ情報

ユーザＩＤ	パスワード	管理者	送信先アドレス	・・・
UsrA	******	AdmB	UsrA@efgh.com	・・・
UsrB	******	AdmB	UsrB@efgh.com	・・・
⋮	⋮	⋮	⋮	⋮

【００６１】

ステップＳ４１の指示を受けたユーザ端末３００は、まず入力されたユーザ認証情報を

含む認証要求をユーザポータル２２１ｂに対して送信する（Ｓ４２）。ユーザポータル２２１ｂは、この要求を認証処理部２２２に渡して認証を実行させる（Ｓ４３）。認証処理部２２２は、開発者認証情報をＩＤ管理部２２５に登録されている開発者情報と照合して認証処理を行い（Ｓ４４）、一体したものがあればユーザポータル２２１ｂに認証成功の認証結果を返す（Ｓ４５）。ユーザポータル２２１ｂはユーザ端末３００に認証成功の認証結果を返す（Ｓ４６）。認証失敗であれば同様に認証失敗の応答を返す。

【００６２】

ユーザ端末３００は、認証成功の認証結果を受けると、ユーザから次の指示を受け付ける。これに応じてユーザは、ファームウェアをダウンロードすべく、ユーザ端末３００に対してＦＷ取得指示を行う（Ｓ５１）。この指示には、ユーザ端末３００の機種や、ユーザが利用しようとするサービスの種類など、ファームウェアを特定するために必要な情報を含むものとする。またこの指示は、ＦＷ更新部３２２が受け付ける。

【００６３】

ステップＳ５１の指示を受けたユーザ端末３００は、指示に従ったＦＷ取得要求をユーザポータル２２１ｂに送信する（Ｓ５２）。ユーザポータル２２１ｂは、その要求をＦＷ管理部２３１に伝える（Ｓ５３）。ＦＷ管理部２３１は、この要求に応じて、要求に応じて指定された機種等の条件に従ったファームウェアのうち最新のバージョンを、ユーザポータル２２１ｂに返す（Ｓ５４）。ユーザポータル２２１ｂは、受け取ったファームウェアをユーザ端末３００に返す（Ｓ５５）。

【００６４】

ユーザ端末３００は受け取ったファームウェアを、セキュア領域にインストールする（Ｓ５６）。このことにより、ユーザ端末３００に、ファームウェアに埋め込まれた共通証明書（及び対応する秘密鍵）が登録され、ユーザ端末３００がこの共通証明書を用いたデバイス認証をサービスサーバ２００に受けられる状態となる。

【００６５】

次に、動作は図７に示す部分に進む。なお、初めからファームウェアがインストールされた状態でユーザ端末３００がユーザの手元に届く場合、ユーザは図７の部分から動作を開始することができる。

ユーザは、ファームウェアがインストールされたユーザ端末３００に対し、サービスサーバ２００へのアクセスを指示する（Ｓ６１）。ユーザ端末３００では、動作要求部３２５がこの指示を受けつける。この指示の受付は、ユーザポータル２２１ｂとは関係なく行うことができる。

【００６６】

ステップＳ５１の指示を受け付けたユーザ端末３００は、証明書登録部３２４に個別証明書が登録されていないことを検出すると（Ｓ６２）、サービスサーバ２００のアクセス受付部２２１にアクセスして、共通証明書を用いたデバイス認証を要求すると共に、発行を受けたい個別証明書の証明条件を送信する（Ｓ６３）。この証明条件には、有効期限、暗号強度、要求元であるユーザ端末３００のデバイスＩＤ、個別証明書の用途等が含まれる。

【００６７】

なお、ユーザ端末３００は、ステップＳ６２で個別証明書が登録されていれば、後述する図１０の動作を行う。また、ステップＳ６２の動作は、ファームウェアのインストール完了に応じて自動で行ってもよい。ステップＳ６２でのアクセス先（ＵＲＬ（Uniform Resource Locator）など）は、ファームウェアに登録しておくか、ユーザ端末３００が利用するサービスの情報としてユーザ端末３００に予め登録しておくとよい。

【００６８】

ステップＳ６３の要求を受けたアクセス受付部２２１は、認証処理部２２２に対して共通証明書を用いた認証を要求する（Ｓ６４）。認証処理部２２２はこの要求に応じて、図４を用いて説明した手法により、共通証明書の正当性をルートＣＡ証明書５００を用いて確認しつつ、要求元のユーザ端末３００が、共通証明書（及び対応する秘密鍵）を所持す

る装置であることを確認する。さらに、表４を用いて後述するように、証明書管理部２２４においてその共通証明書が有効状態とされていることを確認する。認証処理部２２２は、これらの確認ができると、認証成功の応答をアクセス受付部２２１へ返す（Ｓ６５）。以上の認証の機能は、認証手段としての機能である。また、この認証の動作が、認証手順の動作である。

【００６９】

アクセス受付部２２１は、ステップＳ６５の応答により、共通証明書を用いた認証が成功したことを確認すると、認証要求元に対し個別証明書を発行すべく、ステップＳ６３で受信した証明条件に従った個別証明書の発行を、証明書発行部２２３に対して要求する（Ｓ６６）。この要求を受けた証明書発行部２２３は、ステップＳ６３で受信した共通証明書により署名した、上記証明条件に従った個別証明書を発行する（Ｓ６７）。証明書管理部２２４には、発行済みの共通証明書と対応する秘密鍵も登録されているため、証明書発行部２２３は、その秘密鍵を用いて、任意の共通証明書を用いた署名を個別証明書に付すことができる。このステップＳ６７の動作が、第２発行手順の動作であり、第２発行手段の機能に係る動作である。

【００７０】

次に、証明書発行部２２３は発行した個別証明書の登録を証明書管理部２２４に対して要求し（Ｓ６８）、証明書管理部２２４はその個別証明書（及び対応する私有鍵）を、署名に用いた共通証明書と対応付けて登録する（Ｓ６９）。発行先ユーザ端末３００のデバイスＩＤとも対応付けてもよい。この登録の機能は、第１登録手順の動作であり、第１登録手段としての機能である。

【００７１】

また、証明書発行部２２３は、発行した個別証明書を個別証明書発行要求に対する応答としてアクセス受付部２２１に返す（Ｓ７０）。アクセス受付部２２１はユーザ端末３００に個別証明書を返す（Ｓ７１）。個別証明書を受け取ったユーザ端末３００は、証明書登録部３２４にその個別証明書を登録する（Ｓ７２）。

なお、ステップＳ６５で認証失敗の場合、アクセス受付部２２１は、その旨をユーザ端末３００に通知する。この場合、個別証明書の発行は行わない。ただし、認証失敗の理由が、共通証明書が無効化されていたことにある場合は、後述する図１４の場合と同様、ファームウェアの更新を推奨してもよい。

【００７２】

以上の動作により、ユーザ端末３００は、共通証明書をクレデンシャルとして用いて装置に固有の個別証明書の発行を受け、以後サービスサーバ２００に認証を受ける際に使用できるように登録することができる。

【００７３】

次に、図８及び図９に、設置フェーズにおける、ユーザからの要求に基づき個別証明書（を登録したユーザ端末３００）をアクティベートする動作における各部の動作シーケンスを示す。アクティベートとは、当該個別証明書を持つ装置を、サービスの提供対象としてサービスサーバ２００に登録し、実際にサービスの提供を受けられるようにする（サービスを有効化する）処理である。

【００７４】

ここでは、共通証明書が埋め込まれたファームウェアをユーザ端末３００にインストールした後、その共通証明書を用いて個別証明書を取得する例について説明する。ユーザ端末３００が持つデバイスＩＤがグローバルユニークであり、共通証明書を外部から取り出せない形でユーザ端末３００に記憶させることができる場合には、この方式が有用である。

【００７５】

図８の動作において、個別証明書が登録されたユーザ端末３００のユーザは、第２ユーザ端末４００を用いて、ユーザポータル２２１ｂにアクセスし、図６のステップＳ４１乃至Ｓ４６の場合と同様に、サービスサーバ２００にユーザ認証情報を用いたユーザ認証を

受ける（Ｓ８１，Ｓ８２）。ここで第２ユーザ端末４００を用いているのは、第１ユーザ端末３００は必ずしもユーザにとって操作性がよい装置であるとは限らないので、別の装置も利用できるようにしたことによるものである。しかし、第１ユーザ端末３００を用いることも妨げられない。また、第２ユーザ端末４００は、ユーザ端末３００と通信できれば、ユーザ端末３００と同じユーザ環境にあるものでもよいし、違うユーザ環境にあるものでもよい。前者の例としては、ＭＦＰと同じ社内ＬＡＮにつながったＰＣが考えられる。後者の例としては、社内ＬＡＮにつながっていないスマートフォン等が考えられる。後者の場合、第２ユーザ端末４００とユーザ端末３００との間の通信には、ＢＬＥ（Bluetooth（登録商標） Low Energy）やＮＦＣ（Near Field Communication）、Ｗｉｆｉ－ｄｉｒｅｃｔ等を用いることが考えられる。

【００７６】

ステップ８２で認証を受けたユーザは、第２ユーザ端末４００に対し、第２ユーザ端末４００から見た、アクティベート対象のユーザ端末３００の接続先を指定したアクティベーション指示を行う（Ｓ８３）。ユーザ端末３００のデバイスＩＤも合わせて指定してもよい。この指示を受けた第２ユーザ端末４００は、ユーザポータル２２１ｂに対し、有効化情報であるアクティベーショントークンの送信を要求するトークン要求を送信する（Ｓ８４）。このトークン要求には、ステップＳ８３の指示において指定されたユーザ端末３００の情報が含まれる。接続先等、第２ユーザ端末４００から見たユーザ端末３００の位置の情報を含むとよい。接続先は、ポートやローカルアドレス等により特定することができる。

【００７７】

ステップＳ８４の要求を受けたユーザポータル２２１ｂは、認証処理部２２２にこの要求を渡す（Ｓ８５）。これに応じて認証処理部２２２は、ＩＤ管理部２２５から、ステップＳ８２で認証したユーザ（トークンを要求したユーザ）と対応する管理者ＩＤを取得する（Ｓ８６）。この管理者ＩＤは、表２のユーザ情報にユーザのユーザＩＤと対応付けて登録されているものである。

【００７８】

次に、認証処理部２２２は、ステップＳ８６で取得した管理者ＩＤと、トークン要求に含まれるユーザ端末３００の接続先等の情報を含むアクティベーショントークンを生成する（Ｓ８７）。この生成の機能が、第３発行手段としての機能である。また、アクティベーショントークンは、ユーザ認証で認証したユーザのユーザＩＤに基づき、ユーザに対して発行するものである。

【００７９】

次に、認証処理部２２２は、発行したアクティベーショントークンを、ステップＳ８５の要求に対する応答としてユーザポータル２２１ｂに返す（Ｓ８８）。ユーザポータル２２１ｂは、そのアクティベーショントークンを第２ユーザ端末４００に返す（Ｓ８９）。

これを受け取った第２ユーザ端末４００は、そのアクティベーショントークンにて指定された接続先にあるユーザ端末３００に対し、そのアクティベーショントークンを送信してアクティベーション要求を行う（Ｓ９０）。

【００８０】

この要求を受け取ったユーザ端末３００は、受け取ったトークンの正当性（改ざん等されていないこと）を、チェックサム、署名等により確認する（Ｓ９１）。また、自身の証明書登録部３２４に自身の個別証明書が登録されていることを確認する（Ｓ９２）。ここで登録されていれば図９の動作に進むが、登録されていなければ、図７のステップＳ６３以降の動作を行ってサービスサーバ２００から個別証明書の発行を受けるか、あるいは第２ユーザ端末４００に対してエラーを返す。

【００８１】

図９の動作では、ユーザ端末３００は、サービスサーバ２００のアクセス受付部２２１にアクセスして、個別証明書を用いたデバイス認証を要求する（Ｓ９３）。この要求を受けたアクセス受付部２２１は、認証処理部２２２に対して個別証明書を用いた認証を要求

する（Ｓ９４）。認証処理部２２２はこの要求に応じて、図４を用いて説明した手法により、個別証明書の正当性をルートＣＡ証明書５００及び個別証明書の署名に用いた共通証明書を用いて確認しつつ、要求元のユーザ端末３００が、個別証明書（及び対応する秘密鍵）を所持する装置であることを確認する。さらに、表５を用いて後述するように、証明書管理部２２４においてその個別証明書及び個別証明書の署名に用いた共通証明書が有効状態とされていることを確認する。

【００８２】

認証処理部２２２は、この確認ができると、認証成功の応答をアクセス受付部２２１へ返す（Ｓ９７）。また、それに先立ち、認証ログ管理部２２７に要求して認証の結果をログとして登録させる（Ｓ９５，Ｓ９６）。この登録は認証の成否に関わらず行うものである。また、図１１の動作において不正アクセス検知部２２８が不正アクセスの検知を行うために必要な情報を登録する。例えば認証の日時、要求元装置のＩＰアドレス、およびデバイスＩＤ等を登録することが考えられる。

【００８３】

一方、ステップＳ９７で認証成功の応答を受けたアクセス受付部２２１は、ユーザ端末３００に対し認証成功の応答を返す（Ｓ９８）。

ステップＳ９８の応答を受けたユーザ端末３００は、サービスサーバ２００に動作を要求できる状態になったと判断する。そして、自身が登録している個別証明書をアクティベートすべく、自身のデバイスＩＤと、図８のステップＳ９０で受け取ったアクティベーショントークンとを含む登録要求を生成し、自身の個別証明書を用いて署名する（Ｓ９９）。そして、その登録要求をアクセス受付部２２１に送信する（Ｓ１００）。

【００８４】

この登録要求を受けたアクセス受付部２２１は、これを認証処理部２２２に渡す（Ｓ１０１）。認証処理部２２２は登録要求になされた署名を、認証の場合と同様に検証し（Ｓ１０２）、登録要求に改ざん等されていないことを確認する。また、登録要求に含まれるアクティベーショントークンの内容と、登録要求を送信してきたユーザ端末３００の情報とが矛盾しないことを確認する。この確認ができると、認証処理部２２２は、登録要求中のデバイスＩＤと、登録要求に含まれるアクティベーショントークン中の管理者ＩＤとを取得する（Ｓ１０３）。そして、それらのＩＤを含む登録要求をＩＤ管理部２２５に渡す（Ｓ１０４）。ＩＤ管理部２２５は、この要求を受けると、要求に係るデバイスＩＤと管理者ＩＤとを対応付け、サービス提供対象として登録する（Ｓ１０５）。

【００８５】

この登録は、表３に示すようなデバイス情報として行う。デバイス情報は、サービスサーバ２００によるサービスの提供対象となるユーザ端末を登録するものであり、該当ユーザ端末のデバイスＩＤと、サービスを提供する管理者の管理者ＩＤとを登録する。また、これに加え、ユーザ端末を使用するユーザの情報を登録してもよい。ユーザの情報については、一旦デバイスＩＤを登録した後で、ユーザに提供を求めて登録するとよい。またアクティベーショントークンにユーザの情報を含めたり、図８のステップＳ９０のアクティベーション要求の際にユーザに入力させたりすることも考えられる。

ＩＤ管理部２２５は、ステップＳ１０５の登録が成功すると認証処理部２２２に登録成功の応答を返し（Ｓ１０６）、認証処理部２２２及びアクセス受付部２２１は、これに応じて順次登録成功の応答を要求元へ返す（Ｓ１０７，Ｓ１０８）。

【００８６】

【表３】

デバイス情報

デバイスＩＤ	管理者ＩＤ	・・・
DevA	AdmB	・・・
DevB	AdmB	・・・
⋮	⋮	⋮

【００８７】

以上により、ユーザは、第２ユーザ端末４００を操作して、個別証明書を発行済みのユーザ端末３００を、サービスサーバ２００に、サービスの提供対象として登録することができる。

なお、アクティベーショントークンは、ユーザ端末３００の情報を特定せずに発行できるようにしてもよい。このようにすると、登録するユーザ端末３００を制約することはできなくなるが、ユーザがアクティベーショントークンを流出させないと信頼できる場合には特に問題はない。また、アクティベーショントークンの有効期間を絞る等すれば、流出した場合にユーザと無関係なユーザ端末３００が登録されてしまうリスクを軽減できる。

また、ステップＳ９７で認証失敗の場合、アクセス受付部２２１は、その旨をユーザ端末３００に通知する。この場合、アクティベーションは行わない。ステップＳ１０２での検証失敗の場合も同様である。

【００８８】

次に、図１０に、設置フェーズにおける、アクティベートした個別証明書を持つユーザ端末３００に対し、サービスサーバ２００がサービスを提供する動作における各部の動作シーケンスを示す。

アクティベートした個別証明書を持つユーザ端末３００は、ユーザからの指示（Ｓ１２１）に応じて、あるいは自動的に、サービスサーバ２００が提供するサービスを利用しようとする場合、図１０の動作を行う。サービスの利用指示受け付けあるいは利用する事の決定は、動作要求部３２５が行う。

【００８９】

図１０の動作においてユーザ端末３００は、まず個別証明書が証明書登録部３２４に登録されていることを確認する（Ｓ１２２）。そして、図９のステップＳ９３乃至Ｓ９８の場合と同様、サービスサーバ２００に個別証明書を用いた認証を受ける（Ｓ１２３乃至Ｓ１２９）。このとき、サービスサーバ２００は、一定時間以内に同じユーザ端末３００を認証していた場合、認証処理の一部を省略してもよい。また、認証したユーザ端末３００のデバイスＩＤを保持する（Ｓ１２８）。

【００９０】

ユーザ端末３００は、認証成功の応答を受けると、アクセス受付部２２１に対し、サービスサーバ２００が提供するサービスの利用を要求する動作要求を送信する（Ｓ１３０）。ここで要求する動作は、サービスサーバ２００からの具体的なアウトプットを求めるものの他、データの通知や登録である場合もある。

【００９１】

アクセス受付部２２１は、ステップＳ１３０で送信された動作要求に、ステップＳ１２８で保持したデバイスＩＤを付して要求処理部２２６に渡す（Ｓ１３１）。要求処理部２２６は、ＩＤ管理部２２５に問い合わせ、その要求に含まれるデバイスＩＤが、デバイス情報にサービス提供対象として登録された装置のものであることを確認する（Ｓ１３２）。登録されていれば、要求に応じた動作を実行し（Ｓ１３３）、認証処理部２２２を介して要求元のユーザ端末３００にその結果を応答として返す（Ｓ１３４，Ｓ１３５）。ステップＳ１３３で実行する動作は、データの登録やイベント処理等である。

以上により、ユーザ端末３００あるいはそのユーザは、サービスサーバ２００が提供するサービスを利用することができる。

【００９２】

次に、図１１に、運用フェーズにおける、個別証明書の不正利用（又はそれが疑われる事態）を検出した場合の各部の動作シーケンスを示す。

サービスサーバ２００において、不正アクセス検知部２２８は、随時認証ログ管理部２２７から認証ログを取得して分析し、不正アクセスの有無を判定する（Ｓ１５１，Ｓ１５２）。判定のアルゴリズムは、サービスサーバ２００の運用者が、ユーザ端末３００の特性や、提供するサービスの特性等により適宜定めればよい。例えば、図１２に示すように、ほぼ同じ時間域において、異なるＩＰアドレスを持つユーザ端末３００，３００′から同一のデバイスＩＤの個別証明書を用いて複数回アクセスされたといった所定の条件を満たしたアクセスを発見した場合に、不正アクセスの疑いありと判断することができる。

【００９３】

なおここでは、不正アクセス検知部２２８は、個別証明書を用いた不正アクセスの検知を行う（これに加えて他の手段での不正アクセスの検知を行うことも妨げられない）。個別証明書自体に問題がなければ、認証処理部２２２では不正を見抜けないため、別途このケースの不正を検出するための不正アクセス検知部２２８を設けたものである。不正アクセス検知部２２８が検出する不正としては、個別証明書（及び対応する秘密鍵）が流出し、本来の発行先以外の装置に利用されたケースが考えられる。また、共通証明書（及び対応する秘密鍵）が流出した結果、本来共通証明書を保持しているべきでない装置からの不正な要求に基づき、図６の動作により個別証明書が取得されてしまったケースも考えられる。

【００９４】

いずれにせよ、不正アクセス検知部２２８は、不正アクセス又はそれが疑われる事態を検知しなければ（Ｓ１５３のＮＯ）、図１１の動作を終了するが、検知した場合（Ｓ１５３のＹｅｓ）、証明書管理部２２４に問い合わせ、不正アクセスに使用された個別証明書と対応する共通証明書の発行先開発者の開発者ＩＤを特定する（Ｓ１５４）。個別証明書には共通証明書を用いた署名が付されているはずであるので、その署名に基づき発行済み共通証明書のデータを参照することにより特定が可能である。

【００９５】

その後、不正アクセス検知部２２８は、ステップＳ１５４で特定した開発者ＩＤと対応する通知先を、ＩＤ管理部２２５の開発者情報を参照して取得し（Ｓ１５５）、その通知先に対する不正アクセス検出通知の送信を、通知部２２９に対して要求する（Ｓ１５６）。通知部２２９は、この要求に応じて、指定された通知先である開発者端末１００に対して、不正アクセスを検出した旨の通知を、例えば電子メールにより送信する（Ｓ１５７）。このとき、検出した不正アクセスに係るログを合わせて提供してもよい。以上の各部の動作が、通知手順の動作であり、通知手段の機能による動作である。

【００９６】

以上の動作により、サービスサーバ２００は、個別証明書を用いた、不正なあるいは不正が疑われるアクセスを検出した場合に、その個別証明書の発行に用いられた共通証明書の発行先に、その旨を通知することができる。

【００９７】

この通知を受けた開発者は、ログ等を参照し、詳細を確認する。その結果、個別証明書（及び対応する秘密鍵）が流出したと考えられる場合は、その個別証明書のみを無効化すれば、以後の不正は防止できると考えられる。しかし、共通証明書（及び対応する秘密鍵）が流出していると考えられる場合は、共通証明書を無効化することになる。そして、共通証明書を無効化すると、以後、当該共通証明書が埋め込まれたファームウェアを用いては、個別証明書の取得が行えなくなる。また、図４の信頼の連鎖を考慮すると、発行済みの個別証明書についても、その個別証明書を用いた認証が行えなくなる。

【００９８】

次に、図１３に、運用フェーズにおける、不正利用された個別証明書の発行に用いた共通証明書と、同じ共通証明書を用いて発行された他の全ての個別証明書を無効化する場合の各部の動作シーケンスを示す。

開発者は、図１１の動作による通知を受け、共通証明書を無効化すべきと判断すると、開発者認証情報を用いて開発ポータル２２１ａにログインする（Ｓ１７１～Ｓ１７６）。この動作は、ステップＳ１７１の指示がログイン指示である他は、図５のステップＳ１１～ステップＳ１６の動作と同様である。

【００９９】

ログインが成功すると、開発者は、開発者端末１００に、共通証明書の検索及びその検索条件を指示する（Ｓ１８１）。ここで指示する検索条件は、デバイスＩＤ、証明書のシリアルＩＤ、発行日時などが考えられる。開発者端末１００は、この指示に応じて開発者ポータル２２１ａに検索要求を送信し（Ｓ１８２）、開発者ポータル２２１ａが認証処理部２２２を介して証明書管理部２２４にその検索要求を伝える（Ｓ１８３）。証明書管理部２２４は、ステップＳ１７５で認証した開発者に対して発行済みの共通証明書のうち、検索条件に合うものを抽出する（Ｓ１８４）。そして、その結果を認証処理部２２２及び開発者ポータル２２１ａを介して、検索要求に対する応答として開発者端末１００へ返す（Ｓ１８５，Ｓ１８６）。開発者端末１００は、受信した検索結果を表示し（Ｓ１８７）、開発者からの指示を受け付ける。

【０１００】

開発者は、表示された検索結果の中から無効にすべき証明書を指定し、無効化指示を行う（Ｓ１８８）。開発者端末１００では無効化要求部１２７がこの指示を受け付ける。ここでは、共通証明書を無効にする指示がなされたとする。

開発者端末１００は、この指示に応じて開発者ポータル２２１ａに無効化要求を送信し（Ｓ１８９）、開発者ポータル２２１ａが認証処理部２２２を介して証明書管理部２２４にその無効化要求を伝える（Ｓ１９０）。証明書管理部２２４は、その要求に応じて、指定された共通証明書を無効化する（Ｓ１９１）と共に、その共通証明書と対応付けられている、その共通証明書を用いて署名した個別証明書を全て無効化する（Ｓ１９２）。そして、その結果を認証処理部２２２及び開発者ポータル２２１ａを介して、無効化要求に対する応答として開発者端末１００へ返す（Ｓ１９３，Ｓ１９４）。

【０１０１】

以上の動作により、共通証明書の発行先である開発者からの要求に従い、その共通証明書と対応する発行済みの個別証明書を全て無効化することができる。この無効化を行うステップＳ１９２の動作が、無効化手段の機能と対応する動作である。なお、ステップＳ１８２の要求が共通証明書の発行先からの要求であることは、ステップＳ１７５の認証により担保しているが、ステップＳ１８９の要求を受け付ける際に再度認証を行ってもよい。

【０１０２】

ここで、証明書管理部２２４は、表４に示すように、発行済みの共通証明書及び個別証明書と、それらの各証明書が有効か無効かの「状態」の情報を管理している。また、個別証明書は、その個別証明書の署名に用いた共通証明書と対応付けて管理している。証明書管理部２２４は、ステップＳ１９１及びＳ１９２で、この証明書情報中の「状態」の情報を「無効」に変更する。この状態では、図７のステップＳ６５や図９のステップＳ９７等における証明書を用いた認証は、証明書が失効していることにより失敗することになる。個別証明書の「管理者」の情報については、図１７の説明で述べる。

【０１０３】

【表４】

証明書情報

共通証明書	状態	個別証明書	状態	管理者
ComA	有効	IndA	有効	－
		IndB	無効	AdmB
		⋮	⋮	⋮
ComB	有効	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮

【０１０４】

また、共通証明書を無効化した場合にその共通証明書と対応する個別証明書を全て失効させるのは、共通証明書が流出した場合、その共通証明書をクレデンシャルとして取得された個別証明書はいずれも、不正に取得されたものである可能性があり、また、正当に取得されたものと不正に取得されたものとを認証処理で見分けることができないためである。ただし、本実施形態のように共通証明書の署名によって個別証明書が生成されている場合は、各個別証明書を失効させる必要がない場合もある。

【０１０５】

なお、開発者は、共通証明書を無効化する前に、サービスサーバ２００から新しい共通証明書の発行を受け、その新しい共通証明書を埋め込んだ新しいバージョンのファームウェアを、サービスサーバ２００に登録しておくことが望ましい。このようにすれば、個別証明書が失効したユーザ端末３００にも、図１４に示す動作により新しい共通証明書を用いて速やかに新しい個別証明書を登録できるためである。

また、開発者は、個別証明書を無効にしたい場合も、ステップＳ１８８で無効にしたい個別証明書を指定することにより、同様に無効化することができる。この場合、証明書管理部２２４はステップＳ１９１で指定された共通証明書を無効化し、ステップＳ１９２はスキップする。

【０１０６】

次に、図１４に、運用フェーズにおける、共通証明書が無効化された状態でユーザ端末３００がサービスサーバ２００のサービスを利用しようとした場合の各部の動作シーケンスを示す。

この場合も、ステップＳ２０１～Ｓ２０４は、共通証明書が有効な場合の図１０のステップＳ１２１乃至Ｓ１２４と同じである。しかし、認証処理部２２２では、認証に用いた個別証明書への署名に用いた共通証明書が失効していることにより、信頼の連鎖が形成されなくなっているため、認証が失敗する。なお、図１３で説明したようにこの場合には個別証明書自体も失効しているため、これも認証失敗の理由となる。

【０１０７】

図１４の場合もログの記録は行うが（Ｓ２０５，Ｓ２０６）、認証結果は、共通証明書が失効していることにより失敗となる。認証処理部２２２はこれをアクセス受付部２２１に通知する（Ｓ２０７）。アクセス受付部２２１は、この通知により共通証明書が失効していることを把握すると、ユーザ端末３００に対して認証結果を通知すると共に、ファームウェアを更新することを推奨する通知を行う（Ｓ２０８）。ユーザ端末３００は、この通知を受けると、ユーザに対し、認証失敗の旨と、ファームウェアを更新することを推奨するメッセージを表示する（Ｓ２０９）。ユーザ端末３００自体への表示以外にも、ユーザへのメールによる通知等でもよい。また、ユーザ端末３００が、共通証明書の失効を通知された場合にステップＳ２０９の通知を行う機能を備えているのであれば、アクセス受

付部２２１は、単にユーザ端末３００に共通証明書の失効を理由とする認証失敗を通知するのみ、ファームウェアの更新を推奨することができる。

【０１０８】

また、ステップＳ２０９のメッセージを見たユーザがユーザ端末３００にファームウェアの更新を指示すると（Ｓ２１０）、ユーザ端末３００は、図６のステップＳ４２～Ｓ５６と同様な手順でファームウェアを更新する。

また、ユーザ端末３００はその後、ユーザの指示に従い、更新語のファームウェアに埋め込まれた新しい共通証明書をクレデンシャルとして用い、図７乃至図９と同様な手順で新たな個別証明書の発行を受けてアクティベーションを行うことができる。

【０１０９】

以上の動作により、共通証明書の無効化によりサービスサーバ２００のサービスを利用できなくなったユーザ端末を、サービスサーバ２００のサービスを利用できる状態に復帰させることができる。

なお、ファームウェアの更新は、サービスサーバ２００ユーザ認証情報を用いてユーザを認証した場合に行うため、共通証明書を不正に取得した人は、ファームウェアの更新ができず、新たな個別証明書を取得することはできないと考えられる。

また、個別証明書のみが無効化された場合も、図１４の場合と同様にステップＳ２０７での認証は失敗するが、この場合には、アクセス受付部２２１からユーザ端末３００に対して何らかの動作を推奨する必要はない。

【０１１０】

次に、ユーザ端末３００に個別証明書を発行するための別の手順について説明する。この手順では、共通証明書は用いず、サービスの管理者からの要求に従って一時認証情報を発行し、その一時認証情報を用いて認証したユーザ端末３００に対して個別証明書を発行する。この手順は、ユーザ端末３００がデバイスＩＤを持っていなかったり、ユーザ端末３００のデバイスＩＤがユニークでなかったりする場合に有用である。また、ユーザ端末３００がＰＣやスマートフォン、タブレットコンピュータなど、比較的解析が容易な汎用デバイスであり、共通証明書を登録した場合に解析により共通証明書を取り出されてしまう危険性が高い場合にも有用である。

【０１１１】

まず、図１５及び図１６に、管理者からの指示に従ってサービスサーバ２００が一時認証情報を発行する動作における各部の動作シーケンスを示す。

図１５の動作においてはまず、管理者が管理者端末４１０に対し、サービスサーバ２００にログインすべくログイン指示を行うと共に管理者認証情報を入力する（Ｓ２３１）。この指示は、まず管理者端末４１０を用いてユーザポータル２２１ｂにアクセスし、ユーザポータル２２１ｂにより提供される画面から入力する形でもよい。管理者端末４１０は、任意の環境に配置されていてよい。

【０１１２】

なお、サービスサーバ２００のＩＤ管理部２２５には、表５に示すように管理者のアカウントを管理者情報として予め登録しておく。すなわち、サービスサーバ２００の運用者は、サービスサーバ２００が提供するサービスの管理者を予め登録しておき、そのＩＤ及びパスワードを管理者認証情報として用いて、管理者を認証する。また、各管理者へ通知を行う際の送信先アドレスとして、ここでは電子メールアドレスを登録している。さらに、その管理者が、どの開発者が開発したサービスを管理するかを示す開発者ＩＤも、管理者と対応する情報として登録する。その他、開発者の情報として、開発者の社名、住所、証明書発行可能数等を登録することが考えられる。

【０１１３】

【表５】

管理者情報

管理者ＩＤ	パスワード	利用開発者	送信先アドレス	・・・
AdmA	******	DevA	AdmA@abcd.com	・・・
AdmB	******	DevA	AdmB@efgh.com	・・・
⋮	⋮	⋮	⋮	⋮

【０１１４】

ステップＳ２３１の指示を行った管理者は、使用する装置が管理者端末４１０であり使用する認証情報が管理者認証情報である点以外は図６のステップＳ４１乃至Ｓ４６の場合と同様に、サービスサーバ２００の認証を受けることができる。

この認証を受けた管理者は、管理者端末４１０に対してユーザリスト表示指示を行う（Ｓ２４１）。この指示を受けた管理者端末４１０は、ユーザポータル２２１ｂに対してユーザリストを要求し（Ｓ２４２）、ユーザポータル２２１ｂがこの要求を認証処理部２２２に伝える（Ｓ２４３）。

【０１１５】

認証処理部２２２は、この要求に応じてＩＤ管理部２２５から、ステップＳ２３５で認証した管理者が管理するユーザのリストを取得する（Ｓ２４４）。このリストは、表２のユーザ情報に基づき生成できる。そして、認証処理部２２２は、取得したユーザリストをユーザポータル２２１ｂを介して管理者端末４１０へ返す（Ｓ２４５，Ｓ２４６）。管理者端末４１０は、取得したユーザリストを表示する（Ｓ２４７）。

【０１１６】

管理者は、表示されたユーザリストから、一時認証情報である一時ＵＲＬの発行先のユーザを指定し、管理者端末４１０に一時ＵＲＬの発行を指示する（Ｓ２５１）。この指示を受けた管理者端末４１０は、ユーザポータル２２１ｂに対して、指定されたユーザのユーザＩＤを含む一時ＵＲＬの発行要求を送信し（Ｓ２５２）、ユーザポータル２２１ｂがこの要求を認証処理部２２２に伝える（Ｓ２５３）。

【０１１７】

認証処理部２２２は、この要求に応じてＩＤ管理部２２５から、指定されたユーザＩＤと対応する送信先アドレスを取得する（Ｓ２５４）。送信先アドレスは、表２のユーザ情報にから取得できる。次に、認証処理部２２２は、一定時間だけ有効な一時ＵＲＬを生成する（Ｓ２５５）。また、画像処理部２２２ａの機能により、その一時ＵＲＬをコードするコード記号の画像を作成させ、これを取得する（Ｓ２５６，Ｓ２５７）。一時ＵＲＬは、乱数によるアドレスで、アドレスを知らなければアクセスするのが困難であるので、アドレスの通知相手を認証するための一時認証情報として用いることができる。これを発行するステップＳ２５５の動作は、認証情報生成手段の機能と対応する動作である。

【０１１８】

また、処理は図１６に示す部分に進み、認証処理部２２２は、生成した一時ＵＲＬと対応する個別証明書送信実行用の一時コードを生成して記憶する（Ｓ２５８）。この一時コードは、一時ＵＲＬにアクセスされた場合に実行するコードであり、個別証明書を発行してアクセス元に送信するためのコードである。また、発行する個別証明書に記載する情報や、個別証明書と共に証明書管理部２２４に登録する情報として、発行要求元の管理者ＩＤ、発行先のユーザＩＤ、および証明書の証明条件等をコードに含めておく。

【０１１９】

次に、認証処理部２２２は、通知部２２９の機能により、生成した一時ＵＲＬとコード記号を含む電子メールを、ステップＳ２５４で取得した送信先アドレスに送信する（Ｓ２５９）。その後、ユーザポータル２２１ｂを介して管理者端末４１０に、一時ＵＲＬ発行

完了の応答を返す（Ｓ２６０，Ｓ２６１）。
なお、ステップＳ２５９での電子メールの送信先は、必ずしもユーザ端末３００とは限らないが、ここではユーザ端末３００であるとする。
【０１２０】
以上の動作により、管理者からの指示に従い、個別証明書を取得するための一時ＵＲＬをユーザに対して発行することができる。この発行に共通証明書は不要であり、開発者は発行に関与しないため、開発者は別途何らかの手段により管理者を管理することが望ましい。
【０１２１】
次に、図１７に、ユーザ端末３００が一時ＵＲＬにアクセスして個別証明書を取得する動作における各部の動作シーケンスを示す。
図１７の動作においてはまず、ユーザ端末３００が、受信した電子メールから一時ＵＲＬを取得し（Ｓ２７１）、その一時ＵＲＬへアクセスする（Ｓ２７２）。一時ＵＲＬは、ユーザ端末３００自身が電子メールを受信していれば、その電子メールのデータから取得できる。ユーザが電子メールの文面を画面に表示させ、その中の一時ＵＲＬをクリックしたことに応じてそのＵＲＬにアクセスできる。また、他の装置が電子メールを受信していた場合でも、ユーザがその装置の画面に電子メールの文面を表示させ、その中のコード記号の画像を、ユーザ端末３００に搭載されたカメラ等の読取手段により読み取ることによっても、ユーザ端末３００に一時ＵＲＬを取得させることができる。
【０１２２】
また、ステップＳ２７２のアクセスは、ユーザ端末３００において、サービスサーバ２００が提供するサービスを利用するためのアプリを起動し、そのアプリの機能を利用して行う。例えば、サービスサーバ２００が提供するサービスがウェブブラウザを用いて利用するサービスであれば、起動するアプリはウェブブラウザである。専用アプリを用いて利用する場合、ユーザ端末３００が一時ＵＲＬを取得した場合にその専用アプリを起動して一時ＵＲＬを渡す処理が必要となる。
【０１２３】
いずれの場合も、ステップＳ２７２のアクセスは、サービスサーバ２００の認証処理部２２２が受ける。そして、認証処理部２２２は、アクセスされた一時ＵＲＬを取得対応付けて記憶している一時コードを読み出して検証する（Ｓ２７３）。特に問題なければ、アクセス元ユーザ端末に付与するデバイスＩＤを生成する（Ｓ２７４）。そして、一時コードを実行することにより、ステップＳ２７４で生成したデバイスＩＤの装置用の個別証明書であって、一時コードに含まれる管理者ＩＤと対応する共通証明書で署名した個別証明書を生成する（Ｓ２７５）。管理者ＩＤと対応する共通証明書は、表５の管理者情報において管理者ＩＤと対応付けられた開発者ＩＤを持つ開発者に対して発行されている共通証明書である。また、有効期限等、その他の事項は一時コードに含まれる証明条件に従う。
【０１２４】
認証処理部２２２は、ここで生成した個別証明書を、図７のステップＳ６８及びＳ６９の場合と同様に署名に用いた共通証明書と対応付けて証明書管理部２２４に表４の証明書情報として登録させる（Ｓ２７６，Ｓ２７７）。また、ここではさらに、一時コードに含まれる管理者ＩＤ（一時ＵＲＬの発行を指示した管理者の管理者ＩＤ）も、個別証明書と対応付けて登録する。このことにより、個別証明書の発行に関与して管理者を明確にし、開発者やサービスサーバ２００の運営者が管理者の統制を取りやすくすることができる。
【０１２５】
また、認証処理部２２２は、生成した個別証明書をステップＳ２７２のアクセス元へ送信する（Ｓ２７８）。個別証明書を受け取ったユーザ端末３００は、図７のステップＳ７２の場合と同様、証明書登録部３２４にその個別証明書を登録する（Ｓ２７９）。
【０１２６】
以上の動作により、ユーザ端末３００は、一時ＵＲＬをクレデンシャルとして、共通証明書を用いずに装置に固有の個別証明書の発行を受け、以後サービスサーバ２００に認証

を受ける際に使用できるように登録することができる。なお、図１７の動作により個別証明書の発行を受けた場合、サービスサーバ２００へアクセスする際には、ユーザ端末３００は、個別証明書に記載されたデバイスＩＤを持つ装置としてアクセスする。また、アクティベートは、図８及び図９の場合と同様に可能である。

【０１２７】

以上説明してきたシステムによれば、共通証明書が保証する範囲をファームウェアレベルで限定することができる。従って、共通証明書が流出した場合の被害を狭い範囲に抑えることができる。また、共通証明書が流出した際にはこれを自動検出すると共に、開発者主導で共通証明書を（当該共通証明書と対応する個別証明書も含めて）無効化し、その後速やかに再発行することができるので、被害からの回復も容易である。また、共通証明書の無効化と再発行を開発者手動でおこなうことができるので、セキュリティインシデント対策を柔軟かつ容易に行うことができる。このような態勢は、サービスサーバ２００の運営者が、別の開発者を呼び込んでサービスサーバ２００をプラットフォームとするサービスの開発、運営を行ってもらおうとする場合に、有用である。

【０１２８】

また、モバイル端末やＰＣのような汎用端末を想定し、共通証明書ベースではない手法（管理者によるクレデンシャルの一時発行）を行う事で、それを担保として共通証明書なしでも個別証明書を取得可能である。従って、解析が容易な端末に共通証明書を記憶させることによる流出の危険を低減することができる。

【０１２９】

以上で実施形態の説明を終了するが、この発明において、装置の具体的な構成、具体的な処理の手順、データの形式、通信に用いるプロトコル、ネットワークの構成等は、実施形態で説明したものに限るものではない。

例えば、共通証明書を用いて個別証明書に署名することは必須ではない。共通証明書と個別証明書の対応関係が把握できてれば、署名自体は、例えばルートＣＡ証明書５００を用いて行ってもよい。

【０１３０】

また、上述した実施形態において各装置が備えていた機能は、複数の装置に分散して設け、それらの装置を協働させて特定の機能を実現させたり、逆に、複数の装置に分散して設けられていた機能を１つの装置に統合して設けたりしてもよい。例えば、開発者端末１００のいずれかがサービスサーバ２００と一体であってもよい。サービスサーバ２００が、複数の装置が連携してその機能を実現するものであってもよい。

【０１３１】

また、この発明のプログラムの実施形態は、コンピュータに所要のハードウェアを制御させて上述した実施形態における開発者端末１００、サービスサーバ２００、ユーザ端末３００あるいはその他の装置の機能を実現させるためのプログラムである。

このようなプログラムは、はじめからコンピュータに備えるＲＯＭや他の不揮発性記憶媒体（フラッシュメモリ，ＥＥＰＲＯＭ等）などに格納しておいてもよい。しかし、メモリカード、ＣＤ、ＤＶＤ、ブルーレイディスク等の任意の不揮発性記録媒体に記録して提供することもできる。それらの記録媒体に記録されたプログラムをコンピュータにインストールして実行させることにより、上述した各機能を実現させることができる。

【０１３２】

さらに、ネットワークに接続され、プログラムを記録した記録媒体を備える外部装置あるいはプログラムを記憶手段に記憶した外部装置からダウンロードし、コンピュータにインストールして実行させることも可能である。

また、以上説明してきた各実施形態及び変形例の構成は、相互に矛盾しない限り任意に組み合わせて実施可能であることは勿論である。

【符号の説明】

【０１３３】

１０：開発者環境、２０：クラウド環境、３０：ユーザ環境、１００：開発者端末、１２

１：要求送信部、１２２：証明書登録部、１２３：共通証明書要求部、１２４：ＦＷ生成部、１２５：ＦＷ登録要求部、１２６：通知受信部、１２７：無効化要求部、２００：サービスサーバ、２０１：ＣＰＵ、２０２：ＲＯＭ、２０３：ＲＡＭ、２０４：ＨＤＤ、２０５：通信Ｉ／Ｆ、２０６：操作部、２０７：表示部、２０８：システムバス、２２１：アクセス受付部、２２１ａ：開発者ポータル、２２１ｂ：ユーザポータル、２２２：認証処理部、２２２ａ：画像処理部、２２３：証明書発行部、２２４：証明書管理部、２２５：ＩＤ管理部、２２６：要求処理部、２２７：認証ログ管理部、２２８：不正アクセス検知部、２２９：通知部、２３０：証明書無効化部、２３１：ＦＷ管理部、３００：ユーザ端末、３２１：要求送信部、３２２：ＦＷ更新部、３２３：個別証明書要求部、３２４：証明書登録部、３２５：動作要求部、４００：第２ユーザ端末、４１０：管理者端末、Ｎ：インターネット

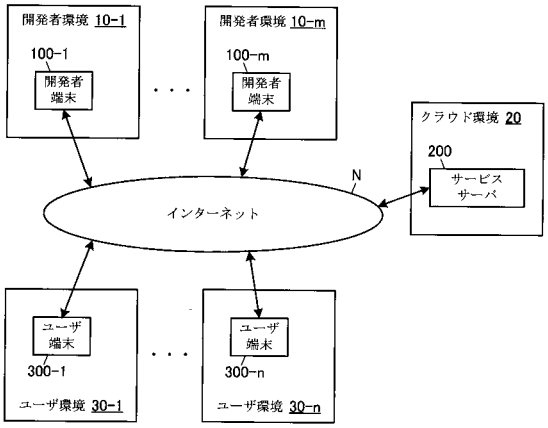
【先行技術文献】

【特許文献】

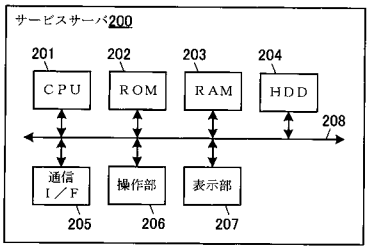
【０１３４】

【特許文献１】特開２００５－１３０４５８号公報

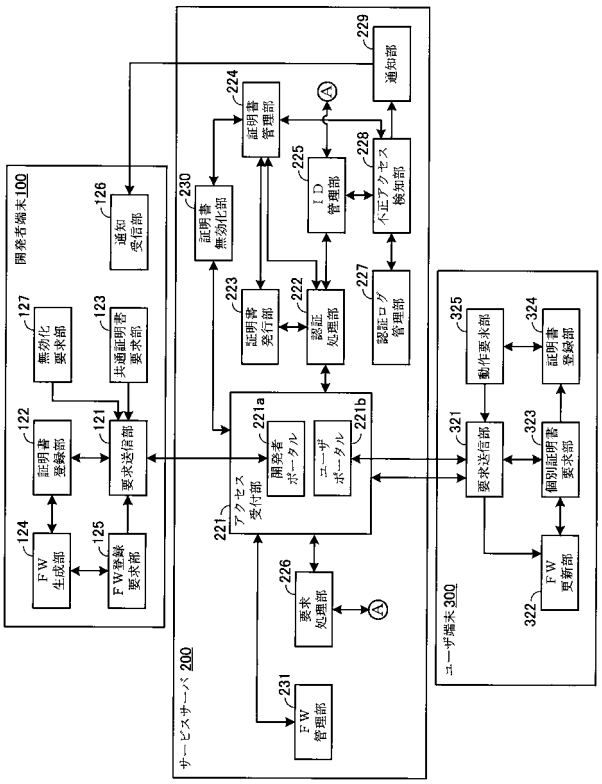
【図１】



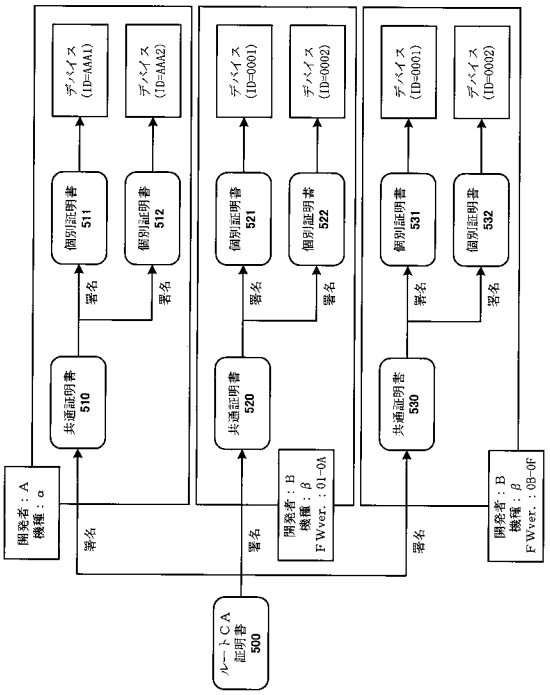
【図２】



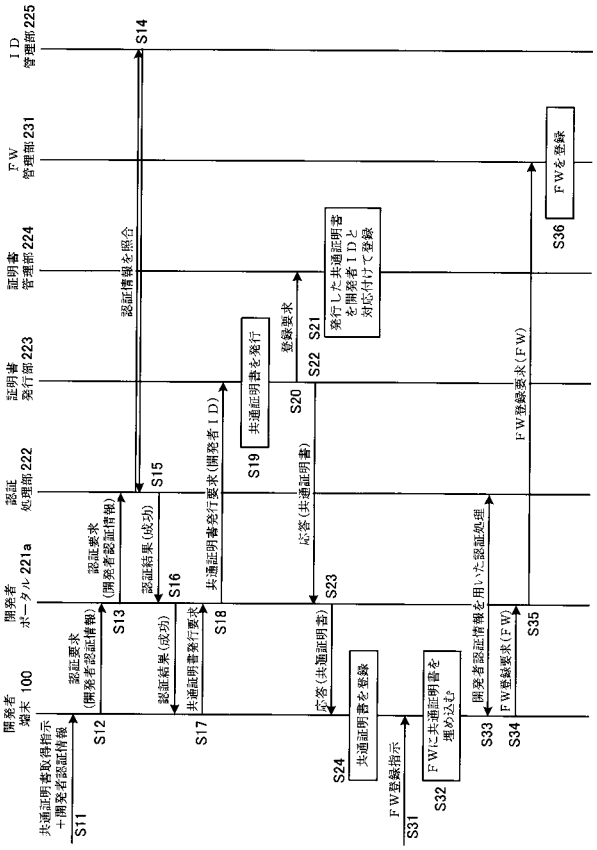
【図３】



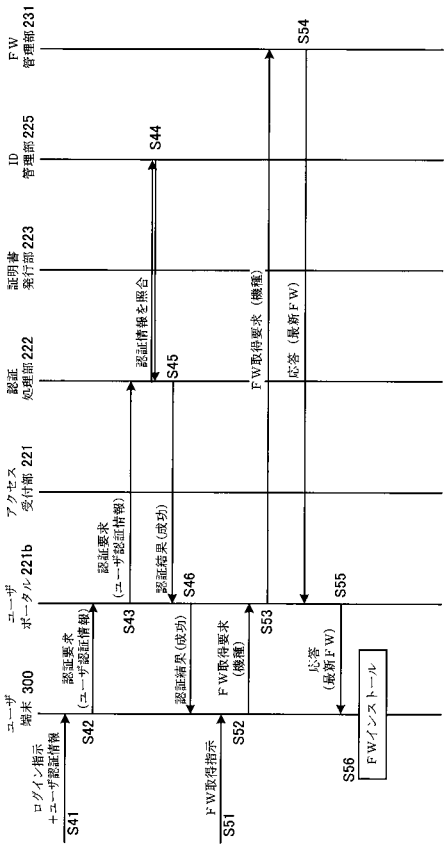
【図４】


ルートCA
証明書
500
開発者：A
機種：α
署名
共通証明書
510
個別証明書
511
デバイス
(ID=AAA1)
デバイス
(ID=AAA2)
個別証明書
512
開発者：B
機種：β
FWver.：01-0A
共通証明書
520
個別証明書
521
デバイス
(ID=0001)
個別証明書
522
デバイス
(ID=0002)
開発者：B
機種：β
FWver.：0B-0F
共通証明書
530
個別証明書
531
デバイス
(ID=0001)
個別証明書
532
デバイス
(ID=0002)

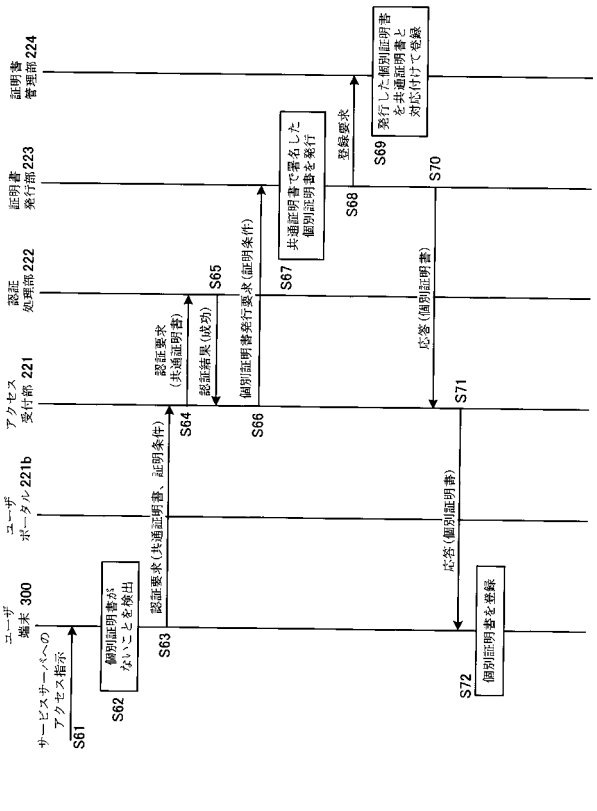
【図５】


開発者
端末 100
開発者
ポータル 221a
認証
処理部 222
証明書
発行部 223
証明書
管理部 224
FW
管理部 231
ID
管理部 225
共通証明書取得指示
＋開発者認証情報
S11
認証要求
(開発者認証情報)
S12
S13
認証結果(成功)
S16
S15
認証情報を照合
S14
共通証明書発行要求(開発者ID)
S17
S18
共通証明書を発行
S19
応答(共通証明書)
S20
登録要求
S22
発行した共通証明書
を開発者ID と
対応付けて登録
S21
応答(共通証明書)
S23
FW登録要求(FW)
S35
FWを登録
S36
開発者認証情報を用いた認証処理
S34
開発者認証情報を
送り返す
S33
FWに共通証明書を
送り返す
S32
FW登録指示
S31
共通証明書を登録
S24

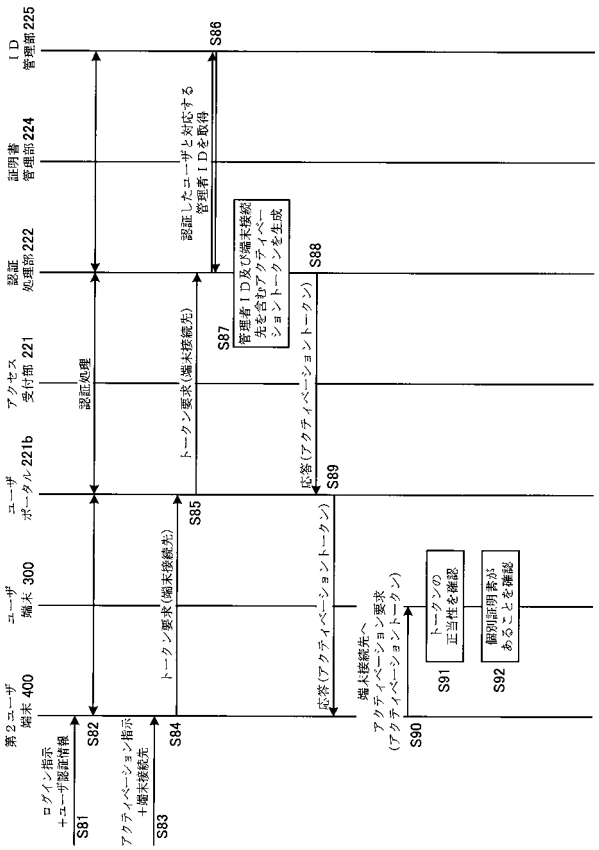
【図６】


ユーザ
端末 300
ユーザ
ポータル 221b
アクセス
受付部 221
認証
処理部 222
証明書
発行部 223
ID
管理部 225
FW
管理部 231
ログイン指示
＋ユーザ認証情報
S41
認証要求
(ユーザ認証情報)
S42
S43
認証情報を照合
S44
認証結果(成功)
S45
S46
FW取得要求
(機種)
S51
S52
S53
FW取得要求（機種）
応答（最新FW）
S54
応答
(最新FW)
S55
S56
FWインストール

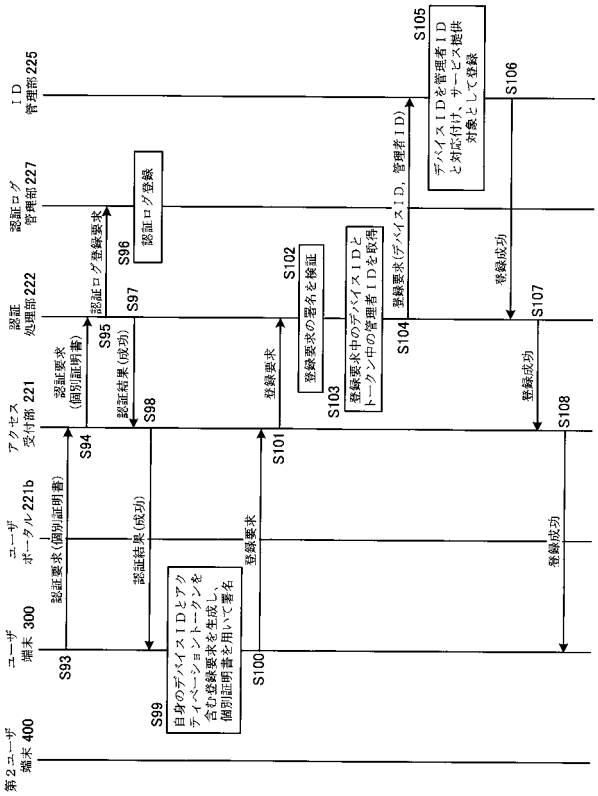
【図７】


ユーザ
端末 300
ユーザ
ポータル 221b
アクセス
受付部 221
認証
処理部 222
証明書
発行部 223
証明書
管理部 224
サービスサーバへの
アクセス指示
S61
個別証明書が
ないことを検出
S62
認証要求(共通証明書、証明条件)
S63
認証要求
(共通証明書)
S64
認証結果(成功)
S65
個別証明書発行要求(証明条件)
S66
共通証明書で署名した
個別証明書を発行
S67
S68
登録要求
S69
発行した個別証明書
を共通証明書と
対応付けて登録
S70
応答(個別証明書)
S71
応答(個別証明書)
S72
個別証明書を登録

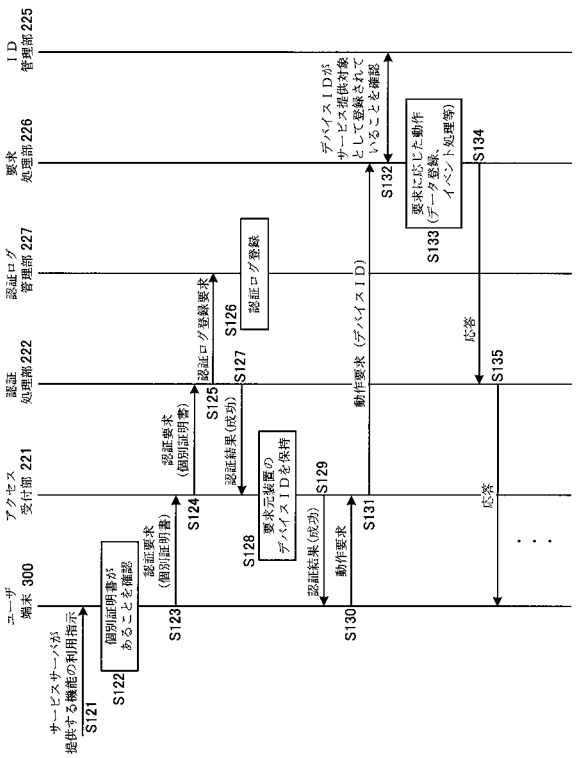
【図８】



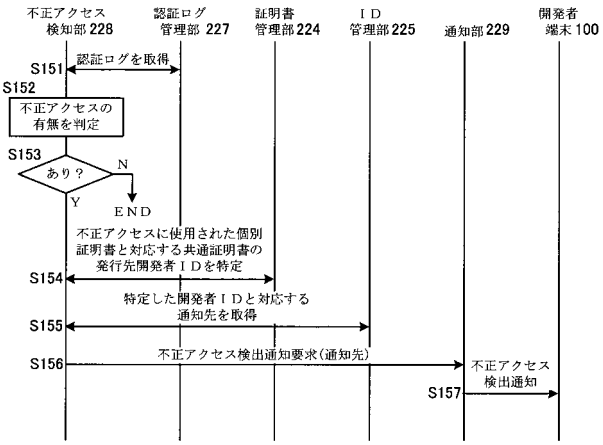
【図９】



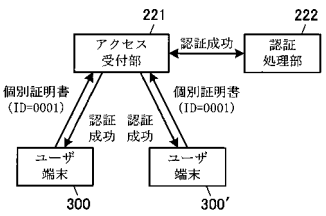
【図１０】



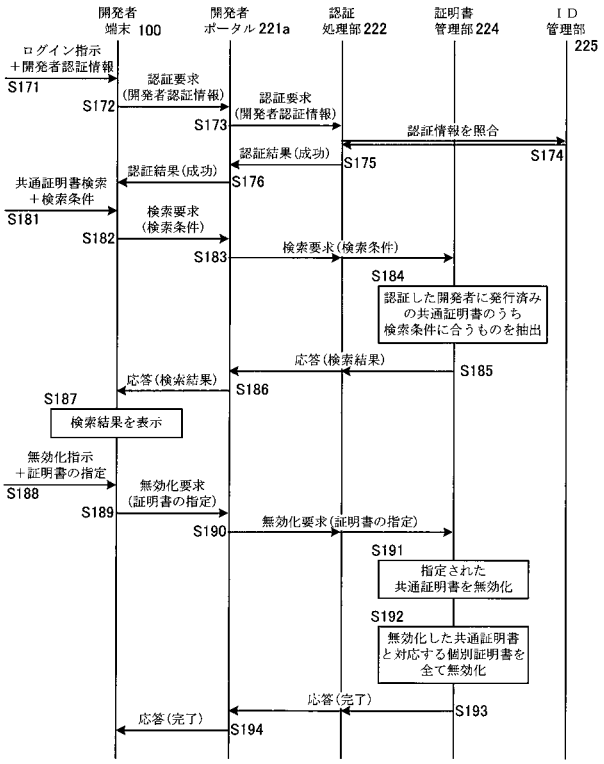
【図１１】



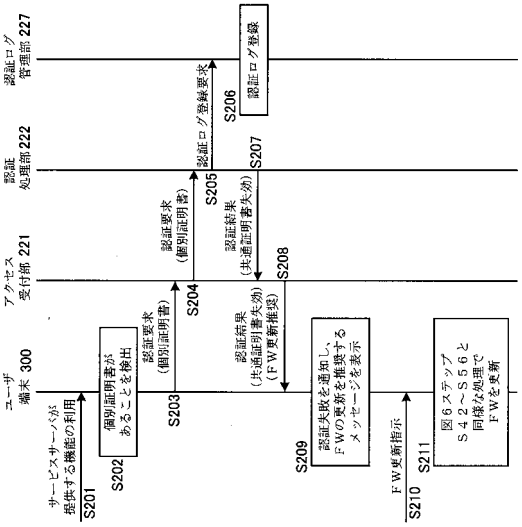
【図１２】



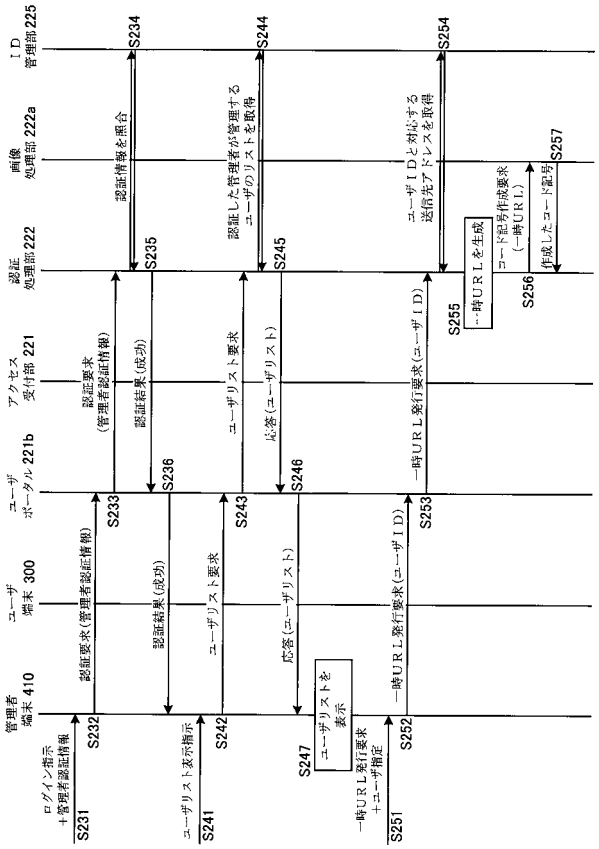
【図１３】



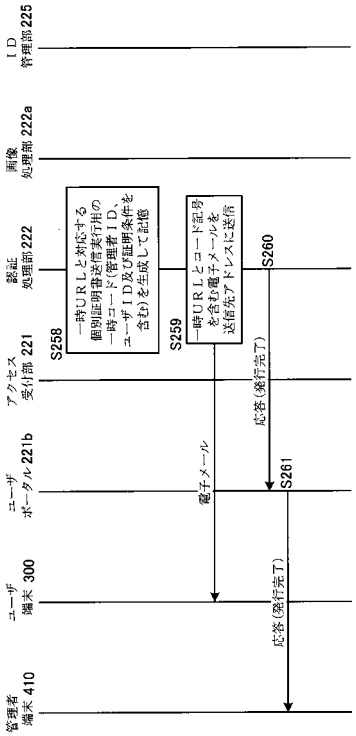
【図１４】



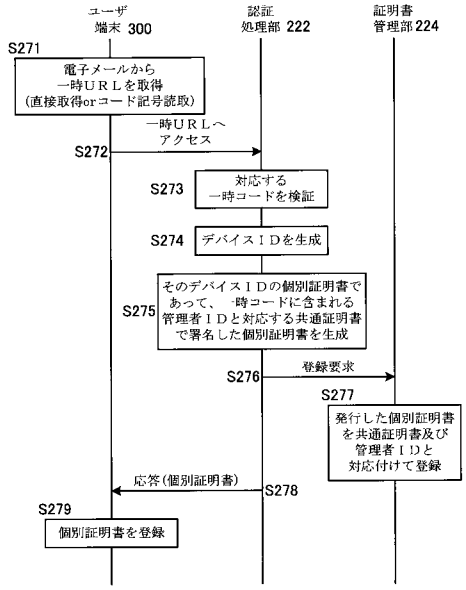
【図１５】



【図１６】



【図１７】


ユーザ
端末 300
認証
処理部 222
証明書
管理部 224
S271
電子メールから
一時ＵＲＬを取得
(直接取得orコード記号読取)
一時ＵＲＬへ
アクセス
S272
S273
対応する
一時コードを検証
S274
デバイスＩＤを生成
S275
そのデバイスＩＤの個別証明書で
あって、一時コードに含まれる
管理者ＩＤと対応する共通証明書
で署名した個別証明書を生成
登録要求
S276
S277
発行した個別証明書
を共通証明書及び
管理者ＩＤと
対応付けて登録
応答(個別証明書)
S278
S279
個別証明書を登録