

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6786830号
(P6786830)

(45) 発行日 令和2年11月18日 (2020. 11. 18)

(24) 登録日 令和2年11月2日 (2020. 11. 2)

(51) Int. Cl.		F I			
H04L	9/32	(2006.01)	H04L	9/00	675D
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	

請求項の数 8 (全 30 頁)

(21) 出願番号	特願2016-56165 (P2016-56165)	(73) 特許権者	000006747
(22) 出願日	平成28年3月18日 (2016. 3. 18)		株式会社リコー
(65) 公開番号	特開2017-175227 (P2017-175227A)		東京都大田区中馬込 1 丁目 3 番 6 号
(43) 公開日	平成29年9月28日 (2017. 9. 28)	(72) 発明者	中島 正登
審査請求日	平成31年1月30日 (2019. 1. 30)		東京都大田区中馬込 1 丁目 3 番 6 号 株式 会社リコー内
		審査官	寺谷 大亮

最終頁に続く

(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) 【特許請求の範囲】

【請求項 1】

証明書管理システムであって、

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

、
 当該証明書管理システムが前記第 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 証明書を用いて正当性を確認でき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、不正アクセス又は不正が疑われるアクセスを発見した場合に、
前記第 1 登録手段に登録された対応関係に基づき、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、前記第 1 登録手段に登録された対応関係に基づき該第 1 証明書と対応する発行済みの第 2 証明書を失効させる失効手段とを備える
 ことを特徴とする証明書管理システム。

【請求項 3】

10

20

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であって、当該証明書管理システムからダウンロードされて、そのダウンロード先の装置で実行されるファームウェアを登録する第 2 登録手段と、

前記失効手段が、発行済みの第 2 証明書を失効させた場合に、該失効させた第 2 証明書の発行先に、該失効させた第 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、

発行済の前記第 1 証明書とその発行先との対応関係を登録する発行先登録手段と、

いずれかの前記発行先と対応付けられた所定の管理者が操作する端末装置からの要求に従い、一時的に有効な一時認証情報を生成して記憶する認証情報生成手段と、

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 証明書を用いて正当性を確認できる第 2 証明書を、前記発行先登録手段が登録する対応関係に基づき発行する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 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が操作する端末装置からの、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第 1 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第 1 情報を受信した場合に、該アクセス元装置を、受信した第 1 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、

前記第 1 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】

証明書管理システムが、

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、

前記証明書管理システムが前記第 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 証明書を用いて正当性を確認でき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、不正アクセス又は不正が疑われるアクセスを発見した場合に、前記第 1 登録手順で登録された対応関係に基づき、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実行す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。

10

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。

20

【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の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。

30

【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、証明書管理システムにおいて、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、上記証明書管理システムが上記第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証明書を用いて正当性を確認でき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、不正アクセス又は不正が疑われるアクセスを発見した場合に、上記第1登録手段に登録された対応関係に基づき、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。

40

【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

50

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「一」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

10

20

30

40

50

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、CPU 201、ROM 202、RAM 203、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、CPU 201 が、RAM 203 をワークエリアとして ROM 202 あるいは HDD 204 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。

ROM 202 及び HDD 204 は、不揮発性記憶媒体（記憶手段）であり、CPU 201 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。

10

20

30

40

50

通信 I / F 2 0 5 は、インターネット N を介して開発者端末 1 0 0 やユーザ端末 3 0 0 等の他の装置と通信するためのインタフェースである。

【0 0 1 9】

操作部 2 0 6 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 2 0 7 は、サービスサーバ 2 0 0 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。

【0 0 2 0】

なお、操作部 2 0 6 及び表示部 2 0 7 は外付けであってもよい。また、サービスサーバ 2 0 0 がユーザからの操作を直接受ける必要がない（通信 I / F 2 0 5 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 2 0 6 や表示部 2 0 7 を設けなくてよい。

【0 0 2 1】

開発者端末 1 0 0 及びユーザ端末 3 0 0 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、HDD 2 0 4 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。

【0 0 2 2】

図 3 に、開発者端末 1 0 0、サービスサーバ 2 0 0、およびユーザ端末 3 0 0 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。

【0 0 2 3】

図 3 に示すように、開発者端末 1 0 0 は、要求送信部 1 2 1、証明書登録部 1 2 2、共通証明書要求部 1 2 3、FW 生成部 1 2 4、FW 登録要求部 1 2 5、通知受信部 1 2 6、無効化要求部 1 2 7 を備える。

このうち要求送信部 1 2 1 は、他の各部からの要求に基づき、サービスサーバ 2 0 0 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 1 2 1 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 2 0 0 の開発者ポータル 2 2 1 a 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 1 0 0 に対してサービスサーバ 2 0 0 への要求の送信を指示する。

【0 0 2 4】

証明書登録部 1 2 2 は、サービスサーバ 2 0 0 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 1 2 3 は、オペレータの指示に従い、サービスサーバ 2 0 0 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 1 2 1 からサービスサーバ 2 0 0 に送信される。

FW 生成部 1 2 4 は、オペレータの指示に従い、証明書登録部 1 2 2 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。

【0 0 2 5】

FW 登録要求部 1 2 5 は、FW 生成部 1 2 4 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 3 0 0 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 2 0 0 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）を無効化するように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。

10

【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。

20

【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】

30

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。

40

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

50

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。

10

【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。

20

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。

30

【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。

40

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

50

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。

10

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。

20

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。

30

【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。

40

【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。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

50

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の機能を利用してよい）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。

10

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。

20

（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。

30

【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。

40

【0050】

【表 1】

開発者情報

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

10

【0051】

ステップ S 1 1 の指示を受けた開発者端末 1 0 0 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 2 2 1 a に対して送信する (S 1 2)。開発者ポータル 2 2 1 a は、この要求を認証処理部 2 2 2 に渡して認証を実行させる (S 1 3)。認証処理部 2 2 2 は、開発者認証情報を I D 管理部 2 2 5 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 (S 1 4)、一体したものがあれば開発者ポータル 2 2 1 a に認証成功の認証結果を返す (S 1 5)。開発者ポータル 2 2 1 a は開発者端末 1 0 0 に認証成功の認証結果を返す (S 1 6)。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 1 0 0 は、認証成功の認証結果を受けると、開発者ポータル 2 2 1 a に対し、共通証明書発行要求を送信する (S 1 7)。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。

20

開発者ポータル 2 2 1 a 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 I D を添付して共通証明書発行要求を証明書発行部 2 2 3 へ送信する (S 1 8)。証明書発行部 2 2 3 は、この要求に応じて共通証明書を発行する (S 1 9)。この動作が第 1 発行手順の動作であり、第 1 発行手順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 C A 証明書を付した署名を付す。

【0053】

30

次に、証明書発行部 2 2 3 は発行した共通証明書の登録を証明書管理部 2 2 4 に対して要求し (S 2 0)、証明書管理部 2 2 4 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 I D と対応付けて登録する (S 2 1)。

また、証明書発行部 2 2 3 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 2 2 1 a に返す (S 2 2)。開発者ポータル 2 2 1 a は開発者端末 1 0 0 に共通証明書を返す (S 2 3)。

共通証明書を受け取った開発者端末 1 0 0 は、証明書登録部 1 2 2 にその共通証明書を登録する (S 2 4)。

【0054】

40

その後、開発者は、ファームウェア (F W) 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 2 0 0 に登録することを指示する (S 3 1)。この指示は、F W 登録要求部 1 2 5 が受け付ける。またこの指示は、開発者ポータル 2 2 1 a 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 S 3 1 の指示を受けた開発者端末 1 0 0 は、F W 生成部 1 2 4 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 1 2 2 に登録されている共通証明書を埋め込む (S 3 2)。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 1 0 0 は、開発者認証情報の入力を受け付けてステップ S 1 2 ~ S 1 6 の場合と同様に認証処理を行う (S 3 3)。その後、開発者端末 1 0 0 は開発者ポータル

50

ル 2 2 1 a に F W 登録要求と共にステップ S 3 2 で共通証明書を埋め込んだ F W を送信する (S 3 4) 。開発者ポータル 2 2 1 a は、この要求に応じて F W 管理部 2 3 1 に F W 登録要求を送信し (S 3 5) 、 F W 管理部 2 3 1 が F W の登録を行う (S 3 6) 。この登録の機能は、第 2 登録手段としての機能である。

【 0 0 5 6 】

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 3 0 0 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。

【 0 0 5 7 】

次に、図 6 及び図 7 に、設置フェーズにおける、ユーザ端末 3 0 0 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 3 0 0 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 3 0 0 が持つデバイス I D 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 3 0 0 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。

【 0 0 5 8 】

図 6 の動作において、ユーザ端末 3 0 0 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 3 0 0 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 2 0 0 にログインすべく、ユーザ端末 3 0 0 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 (S 4 1) 。この指示は、まずユーザ端末 3 0 0 を用いてユーザポータル 2 2 1 b にアクセスし、ユーザポータル 2 2 1 b により提供される画面から入力する形でもよい。

【 0 0 5 9 】

なお、サービスサーバ 2 0 0 の I D 管理部 2 2 5 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 2 0 0 の運用者は、サービスサーバ 2 0 0 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 I D 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 2 0 0 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。

【 0 0 6 0 】

【表 2】

ユーザ情報

ユーザ I D	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	...
⋮	⋮	⋮	⋮	⋮

【 0 0 6 1 】

ステップ S 4 1 の指示を受けたユーザ端末 3 0 0 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 2 2 1 b に対して送信する (S 4 2) 。ユーザポータル 2 2 1 b は、この要求を認証処理部 2 2 2 に渡して認証を実行させる (S 4 3) 。認証処理

部 2 2 2 は、開発者認証情報を I D 管理部 2 2 5 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 (S 4 4)、一体したものがあればユーザポータル 2 2 1 b に認証成功の認証結果を返す (S 4 5)。ユーザポータル 2 2 1 b はユーザ端末 3 0 0 に認証成功の認証結果を返す (S 4 6)。認証失敗であれば同様に認証失敗の応答を返す。

【 0 0 6 2 】

ユーザ端末 3 0 0 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 3 0 0 に対して F W 取得指示を行う (S 5 1)。この指示には、ユーザ端末 3 0 0 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、F W 更新部 3 2 2 が受け付ける。

10

【 0 0 6 3 】

ステップ S 5 1 の指示を受けたユーザ端末 3 0 0 は、指示に従った F W 取得要求をユーザポータル 2 2 1 b に送信する (S 5 2)。ユーザポータル 2 2 1 b は、その要求を F W 管理部 2 3 1 に伝える (S 5 3)。F W 管理部 2 3 1 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 2 2 1 b に返す (S 5 4)。ユーザポータル 2 2 1 b は、受け取ったファームウェアをユーザ端末 3 0 0 に返す (S 5 5)。

【 0 0 6 4 】

ユーザ端末 3 0 0 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 (S 5 6)。このことにより、ユーザ端末 3 0 0 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 3 0 0 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 2 0 0 に受けられる状態となる。

20

【 0 0 6 5 】

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 3 0 0 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 3 0 0 に対し、サービスサーバ 2 0 0 へのアクセスを指示する (S 6 1)。ユーザ端末 3 0 0 では、動作要求部 3 2 5 がこの指示を受け付ける。この指示の受付は、ユーザポータル 2 2 1 b とは関係なく行うことができる。

30

【 0 0 6 6 】

ステップ S 5 1 の指示を受け付けたユーザ端末 3 0 0 は、証明書登録部 3 2 4 に個別証明書が登録されていないことを検出すると (S 6 2)、サービスサーバ 2 0 0 のアクセス受付部 2 2 1 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 (S 6 3)。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 3 0 0 のデバイス I D、個別証明書の用途等が含まれる。

【 0 0 6 7 】

なお、ユーザ端末 3 0 0 は、ステップ S 6 2 で個別証明書が登録されていれば、後述する図 1 0 の動作を行う。また、ステップ S 6 2 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 S 6 2 でのアクセス先 (U R L (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 3 0 0 が利用するサービスの情報としてユーザ端末 3 0 0 に予め登録しておくもよい。

40

【 0 0 6 8 】

ステップ S 6 3 の要求を受けたアクセス受付部 2 2 1 は、認証処理部 2 2 2 に対して共通証明書を用いた認証を要求する (S 6 4)。認証処理部 2 2 2 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 C A 証明書 5 0 0 を用いて確認しつつ、要求元のユーザ端末 3 0 0 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 2 2 4 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 2 2 2 は

50

、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。

10

【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】

20

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。

30

【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。

40

【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

50

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S82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

10

20

30

40

50

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。

10

【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】

20

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】

30

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）。

40

【0086】

【表 3】

デバイス情報

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

10

【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。

20

【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。

30

【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に個別証明書を用了認証を受ける(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。

40

【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。

50

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。

10

【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。

20

【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。

30

【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。

40

【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】

50

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】

10

20

30

40

【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	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮

10

【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。

20

【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

30

【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。

40

【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

50

付部 2 2 1 は、単にユーザ端末 3 0 0 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。

【0 1 0 8】

また、ステップ S 2 0 9 のメッセージを見たユーザがユーザ端末 3 0 0 にファームウェアの更新を指示すると（S 2 1 0）、ユーザ端末 3 0 0 は、図 6 のステップ S 4 2 ～ S 5 6 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 3 0 0 はその後、ユーザの指示に従い、更新後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。

【0 1 0 9】

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 2 0 0 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 2 0 0 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 2 0 0 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 1 4 の場合と同様にステップ S 2 0 7 での認証は失敗するが、この場合には、アクセス受付部 2 2 1 からユーザ端末 3 0 0 に対して何らかの動作を推奨する必要はない。

【0 1 1 0】

次に、ユーザ端末 3 0 0 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 3 0 0 に対して個別証明書を発行する。この手順は、ユーザ端末 3 0 0 がデバイス ID を持っていなかったり、ユーザ端末 3 0 0 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 3 0 0 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。

【0 1 1 1】

まず、図 1 5 及び図 1 6 に、管理者からの指示に従ってサービスサーバ 2 0 0 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 1 5 の動作においてはまず、管理者が管理者端末 4 1 0 に対し、サービスサーバ 2 0 0 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（S 2 3 1）。この指示は、まず管理者端末 4 1 0 を用いてユーザポータル 2 2 1 b にアクセスし、ユーザポータル 2 2 1 b 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 4 1 0 は、任意の環境に配置されていてよい。

【0 1 1 2】

なお、サービスサーバ 2 0 0 の ID 管理部 2 2 5 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 2 0 0 の運用者は、サービスサーバ 2 0 0 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。

【0 1 1 3】

10

20

30

40

【表 5】

管理者情報

管理者 I D	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	．．．
⋮	⋮	⋮	⋮	⋮

10

【0114】

ステップ S 2 3 1 の指示を行った管理者は、使用する装置が管理者端末 4 1 0 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 S 4 1 乃至 S 4 6 の場合と同様に、サービスサーバ 2 0 0 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 4 1 0 に対してユーザリスト表示指示を行う（S 2 4 1）。この指示を受けた管理者端末 4 1 0 は、ユーザポータル 2 2 1 b に対してユーザリストを要求し（S 2 4 2）、ユーザポータル 2 2 1 b がこの要求を認証処理部 2 2 2 に伝える（S 2 4 3）。

【0115】

認証処理部 2 2 2 は、この要求に応じて I D 管理部 2 2 5 から、ステップ S 2 3 5 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（S 2 4 4）。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 2 2 2 は、取得したユーザリストをユーザポータル 2 2 1 b を介して管理者端末 4 1 0 へ返す（S 2 4 5、S 2 4 6）。管理者端末 4 1 0 は、取得したユーザリストを表示する（S 2 4 7）。

20

【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 4 1 0 に一時 URL の発行を指示する（S 2 5 1）。この指示を受けた管理者端末 4 1 0 は、ユーザポータル 2 2 1 b に対して、指定されたユーザのユーザ I D を含む一時 URL の発行要求を送信し（S 2 5 2）、ユーザポータル 2 2 1 b がこの要求を認証処理部 2 2 2 に伝える（S 2 5 3）。

30

【0117】

認証処理部 2 2 2 は、この要求に応じて I D 管理部 2 2 5 から、指定されたユーザ I D と対応する送信先アドレスを取得する（S 2 5 4）。送信先アドレスは、表 2 のユーザ情報から取得できる。次に、認証処理部 2 2 2 は、一定時間だけ有効な一時 URL を生成する（S 2 5 5）。また、画像処理部 2 2 2 a 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（S 2 5 6、S 2 5 7）。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 S 2 5 5 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 1 6 に示す部分に進み、認証処理部 2 2 2 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（S 2 5 8）。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 2 2 4 に登録する情報として、発行要求元の管理者 I D、発行先のユーザ I D、および証明書の証明条件等をコードに含めておく。

40

【0119】

次に、認証処理部 2 2 2 は、通知部 2 2 9 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 S 2 5 4 で取得した送信先アドレスに送信する（S 2 5 9）。その後、ユーザポータル 2 2 1 b を介して管理者端末 4 1 0 に、一時 URL 発行

50

完了の応答を返す（S 2 6 0，S 2 6 1）。

なお、ステップ S 2 5 9 での電子メールの送信先は、必ずしもユーザ端末 3 0 0 とは限らないが、ここではユーザ端末 3 0 0 であるとする。

【0 1 2 0】

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。

【0 1 2 1】

次に、図 1 7 に、ユーザ端末 3 0 0 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。

10

図 1 7 の動作においてはまず、ユーザ端末 3 0 0 が、受信した電子メールから一時 URL を取得し（S 2 7 1）、その一時 URL へアクセスする（S 2 7 2）。一時 URL は、ユーザ端末 3 0 0 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 3 0 0 に搭載されたカメラ等の読取手段により読み取ることも、ユーザ端末 3 0 0 に一時 URL を取得させることができる。

【0 1 2 2】

20

また、ステップ S 2 7 2 のアクセスは、ユーザ端末 3 0 0 において、サービスサーバ 2 0 0 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する。例えば、サービスサーバ 2 0 0 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 3 0 0 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。

【0 1 2 3】

いずれの場合も、ステップ S 2 7 2 のアクセスは、サービスサーバ 2 0 0 の認証処理部 2 2 2 が受ける。そして、認証処理部 2 2 2 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（S 2 7 3）。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（S 2 7 4）。そして、一時コードを実行することにより、ステップ S 2 7 4 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（S 2 7 5）。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。

30

【0 1 2 4】

認証処理部 2 2 2 は、ここで生成した個別証明書を、図 7 のステップ S 6 8 及び S 6 9 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 2 2 4 に表 4 の証明書情報として登録させる（S 2 7 6，S 2 7 7）。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 2 0 0 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。

40

【0 1 2 5】

また、認証処理部 2 2 2 は、生成した個別証明書をステップ S 2 7 2 のアクセス元へ送信する（S 2 7 8）。個別証明書を受け取ったユーザ端末 3 0 0 は、図 7 のステップ S 7 2 の場合と同様、証明書登録部 3 2 4 にその個別証明書を登録する（S 2 7 9）。

【0 1 2 6】

以上の動作により、ユーザ端末 3 0 0 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 2 0 0 に認証

50

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主導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、運営を行ってもらうとする場合に、有用である。

10

【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。

20

【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。

30

【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리카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。

40

【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】

50

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、121：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】

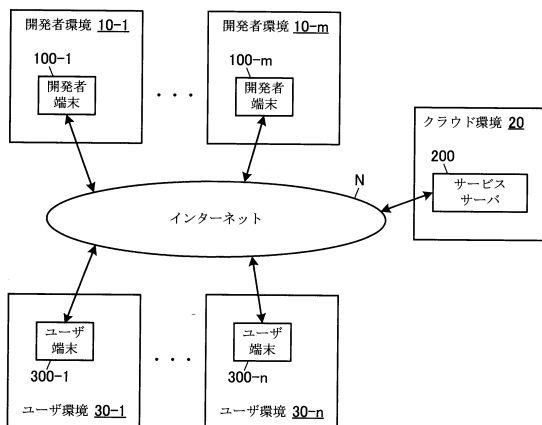
【特許文献】

【0134】

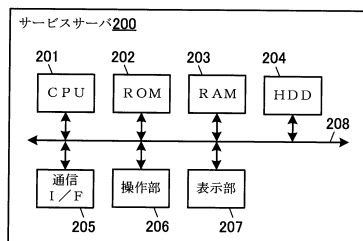
【特許文献1】特開2005-130458号公報

10

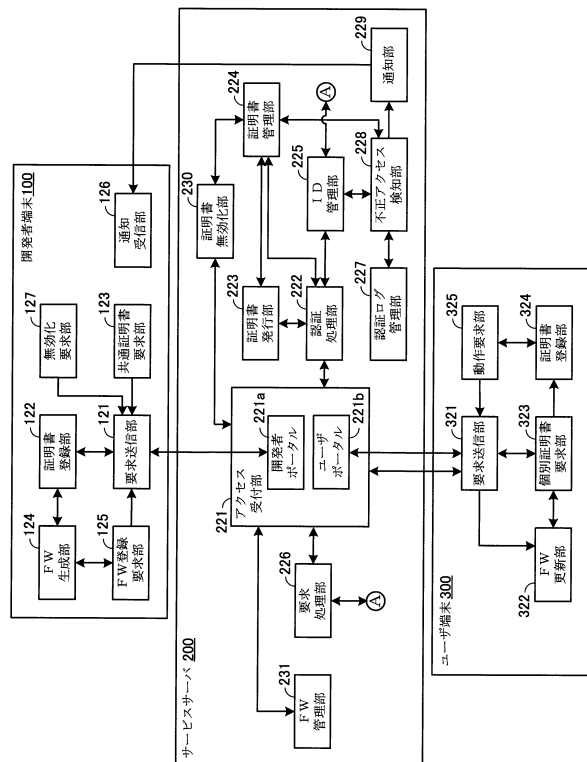
【図1】



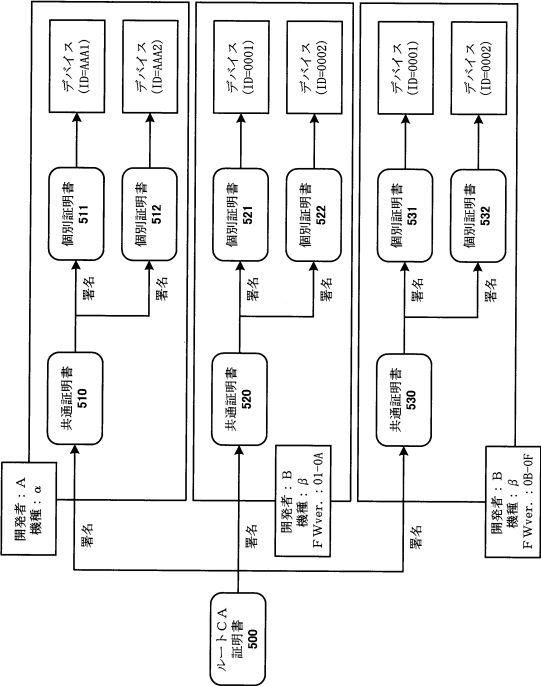
【図2】



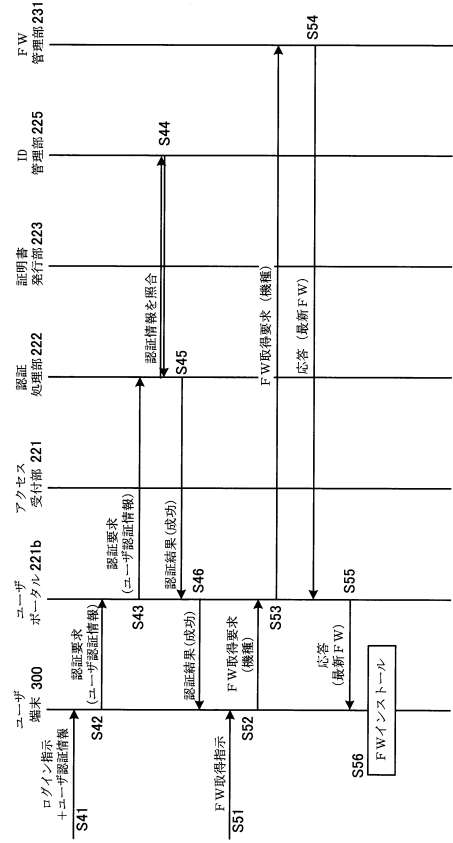
【図3】



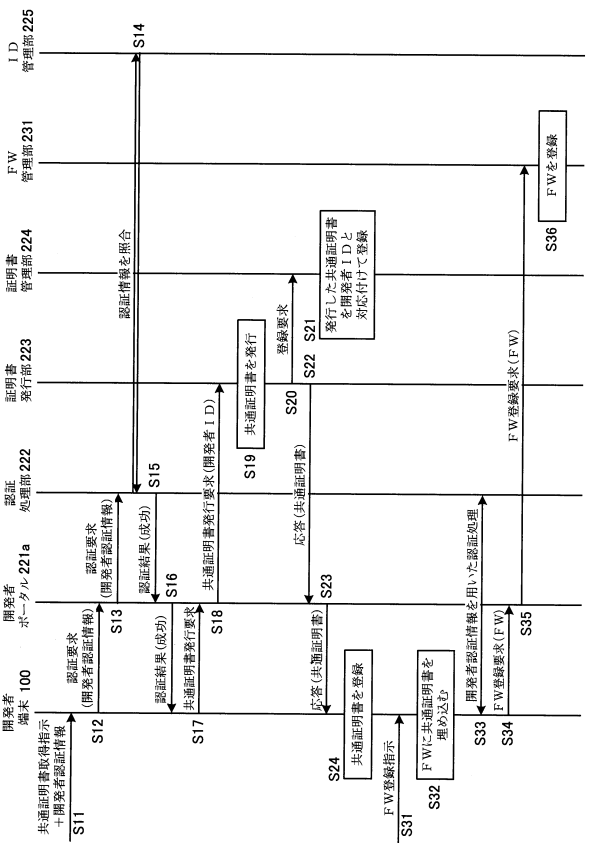
【図 4】



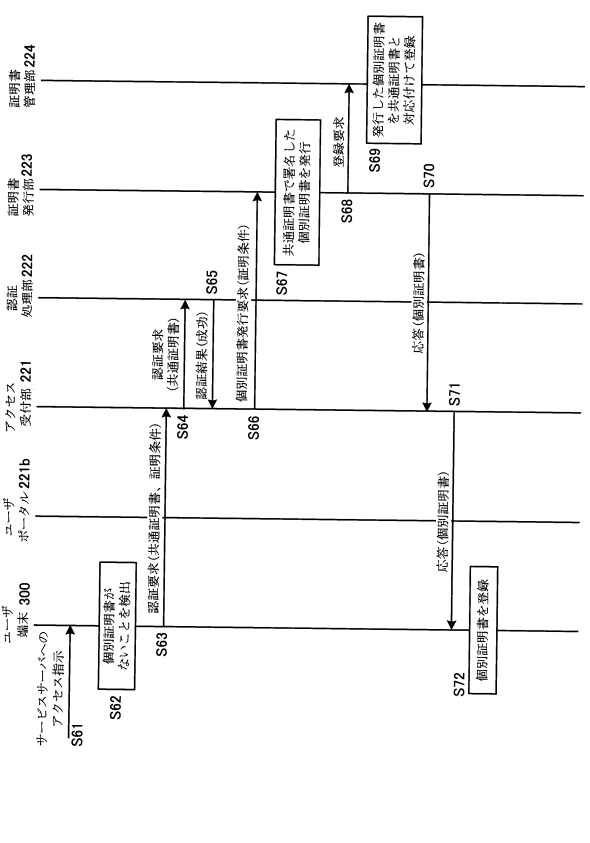
【図 6】



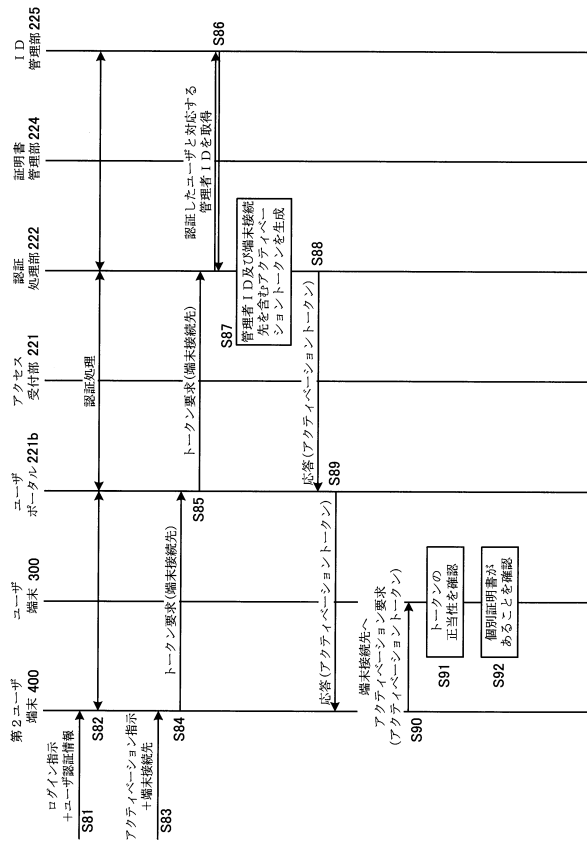
【図 5】



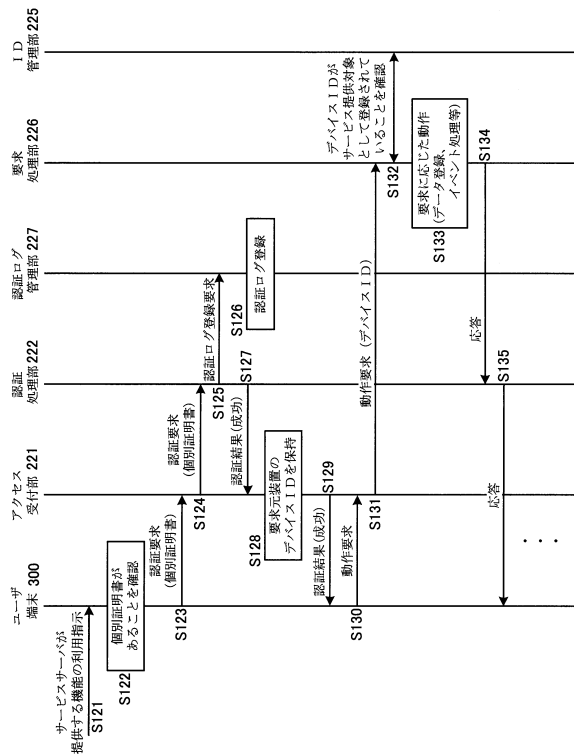
【図 7】



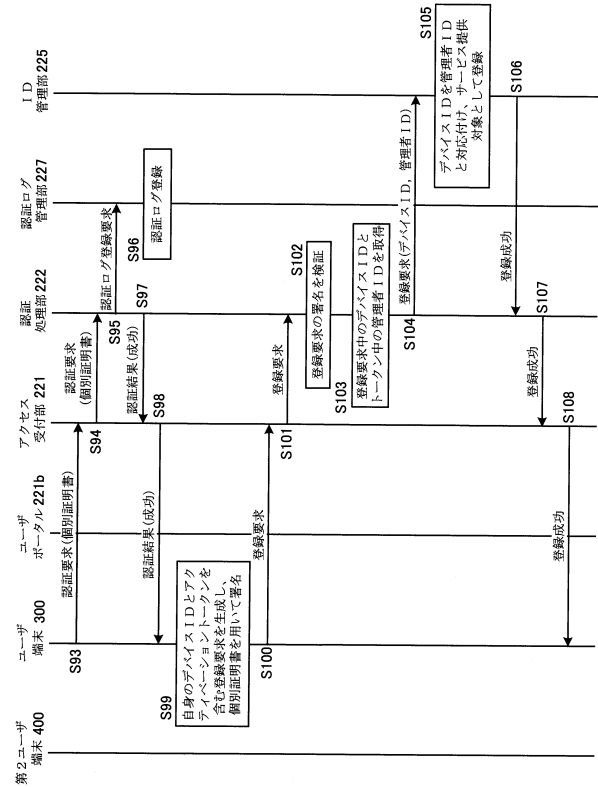
【図 8】



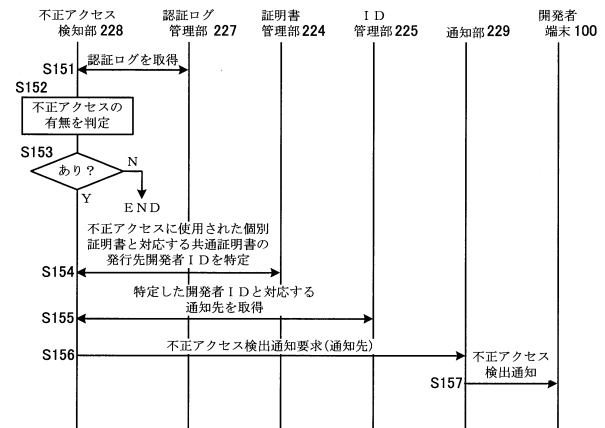
【図 10】



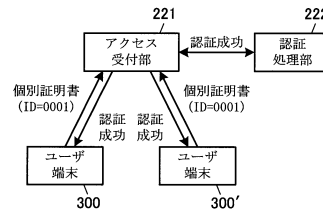
【図 9】



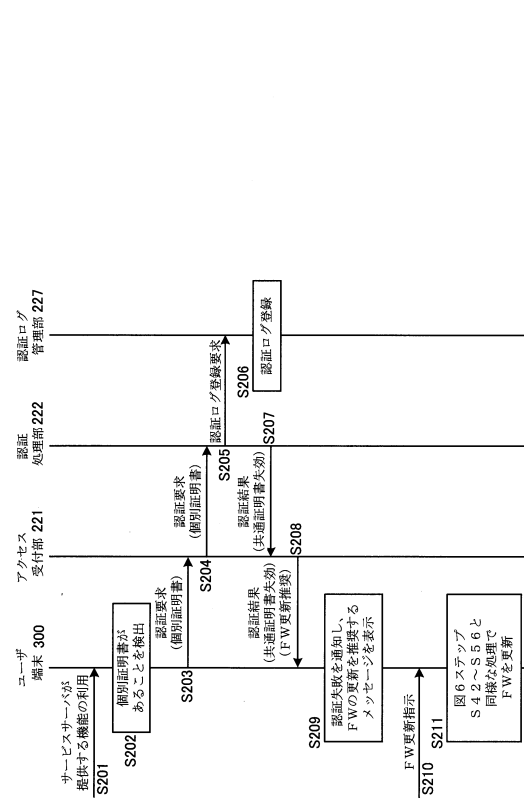
【図 1 1】



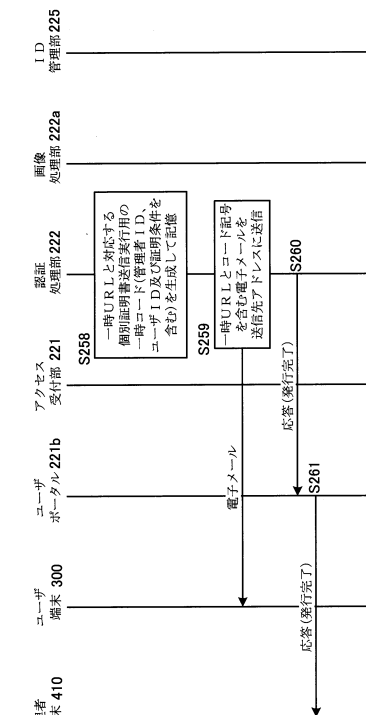
【図 1 2】



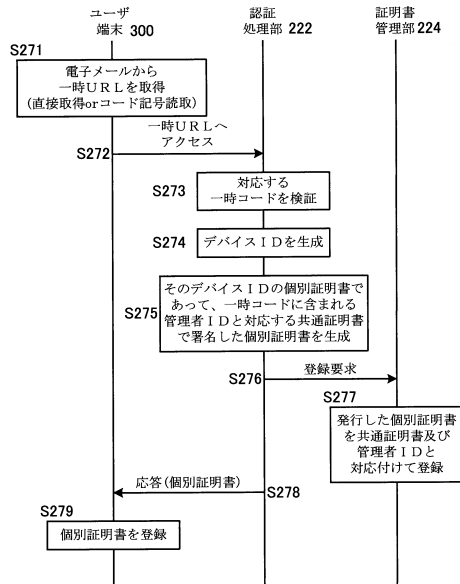
【図 14】



【図 1 6】



【図 17】



フロントページの続き

- (56)参考文献 特開2004-297333 (JP, A)
特開2005-065236 (JP, A)
特開2005-204283 (JP, A)
特開2005-318572 (JP, A)
国際公開第2007/096858 (WO, A2)
特開2011-160475 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F21/00
21/30-21/46
G09C 1/00-5/00
H04K 1/00-3/00
H04L 9/00-9/38