(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2017-228145
(P2017-228145A)
(43)公開日　平成29年12月28日(2017.12.28)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/44	(2013.01)	G06F	21/44		5J104
H04W 12/06	(2009.01)	H04W	12/06		5K067
G06F 21/62	(2013.01)	G06F	21/62		
H04L 9/32	(2006.01)	H04L	9/00	675D	

審査請求 未請求　請求項の数 10　ＯＬ　（全 13 頁）

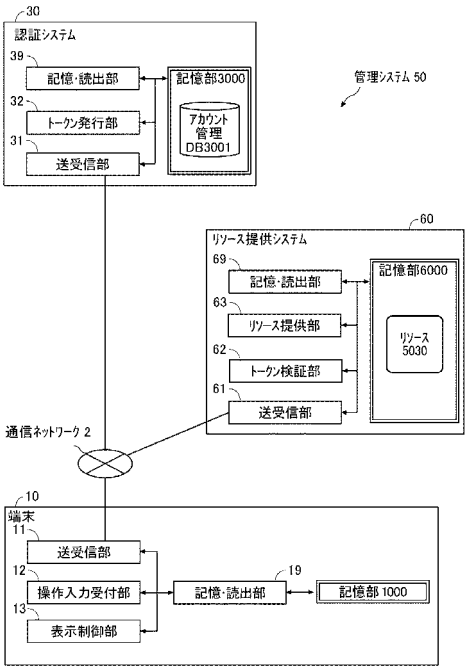
(21)出願番号　特願2016-124755 (P2016-124755)
(22)出願日　平成28年6月23日 (2016.6.23)

(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
(72)発明者　堀内　岳志
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　梅原　直樹
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　日野原　寛
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　宮本　篤
東京都大田区中馬込１丁目３番６号　株式会社リコー内

最終頁に続く

(54)【発明の名称】認証システム、通信システム、認証認可方法、及びプログラム

(57)【要約】　（修正有）
【課題】サービス側の機能が複数のシステムに分散された通信システムにおいて、リソース提供システムとは異なるコネクションに接続する認証システムによる認証情報を、リソース提供システムと認証システムとの間で共有可能とする。
【解決手段】認証システム３０の送受信部３１は、端末１０によって送信されるクライアント証明書で認証してから、端末との間の第１のコネクションを確立する。認証システムのトークン発行部３２は、クライアント証明書に対応するアクセストークンを出力する。認証システムの送受信部は、第２のコネクションにより、リソース提供システム６０へアクセストークンを送信させる。
【選択図】図４



【特許請求の範囲】
【請求項１】
通信端末によって送信されるクライアント証明書で認証してから、前記通信端末との間の第１のコネクションを確立する確立手段と、
前記通信端末によるリソースへのアクセスの認可を示す認可情報として、前記クライアント証明書に対応する認可情報を出力する出力手段と、
前記第１のコネクションとは異なる第２のコネクションにより、前記リソースを提供するリソース提供システムへ前記認可情報を送信させる送信手段と、
を有する認証システム。
【請求項２】
前記第１のコネクションで、認可情報の要求を受け付ける受付手段を有し、
前記出力手段は、前記認可情報の要求元の前記クライアント証明書に対応する前記認可情報を出力する請求項１に記載の認証システム。
【請求項３】
前記クライアント証明書に含まれる識別情報と、前記リソースの識別情報と、を関連付けて管理する管理手段を有し、
前記出力手段は、前記クライアント証明書に含まれる識別情報に関連付けられている前記リソースの識別情報を、前記管理手段から取得し、取得される前記リソースの識別情報を含む認可情報を出力する請求項２に記載の認証システム。
【請求項４】
請求項１乃至３のいずれか一項に記載の認証システムと、
前記認可情報を検証して、前記通信端末に前記リソースを提供する前記リソース提供システムと、
を有する通信システム。
【請求項５】
前記リソース提供システムは、
前記第２のコネクションにより、前記認可情報を受信する請求項４に記載の通信システム。
【請求項６】
更に通信端末を有する請求項４又は５に記載の通信システム。
【請求項７】
前記通信端末は、
前記認証システムとの間で確立される前記第１のコネクションにより前記認可情報を受信し、前記リソース提供システムとの間で確立される前記第２のコネクションにより前記認可情報を送信する請求項６に記載の通信システム。
【請求項８】
認証システムに、
通信端末によって送信されるクライアント証明書で認証してから、前記通信端末との間の第１のコネクションを確立する確立処理と、
前記通信端末によるリソースへのアクセスの認可を示す認可情報として、前記クライアント証明書に対応する認可情報を出力する出力処理と、
前記第１のコネクションとは異なる第２のコネクションにより、前記リソースを提供するリソース提供システムへ前記認可情報を送信させる送信処理と、
を実行させる認証認可方法。
【請求項９】
前記リソース提供システムに、
前記認可情報を検証して、前記リソースを前記通信端末に提供する処理を実行させる請求項８に記載の認証認可方法。
【請求項１０】
認証システムに、

通信端末によって送信されるクライアント証明書で認証してから、前記通信端末との間の第１のコネクションを確立する確立処理と、
前記通信端末によるリソースへのアクセスの認可を示す認可情報として、前記クライアント証明書に対応する認可情報を出力する出力処理と、
前記第１のコネクションとは異なる第２のコネクションにより、前記リソースを提供するリソース提供システムへ前記認可情報を送信させる送信処理と、
を実行させるプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、認証システム、通信システム、認証認可方法、及びプログラムに関する。

【背景技術】

【０００２】

クライアント証明書を用いたクライアント認証後に通信端末によるコネクションを確立するTLS(Transport Layer Security)などのプロトコルが知られている。また、リソースの要求元が認証され、かつ認可されてから、要求元にリソースへアクセスさせるOAuth2.0などのプロトコルが知られている。

【０００３】

特許文献１には、サードパーティーアプリケーションによって、その識別子、認証クレデンシャル、およびアクセス許可を区別可能な様式で集中型セキュアマネージメントシステムへ送信するステップと、サードパーティーアプリケーションを成功裏に認証した後に、集中型セキュアマネージメントシステムによって、識別子およびアクセス許可を許可サーバへ転送するステップと、アクセス許可が有効である場合には、許可サーバによって、ユーザの保護されているリソースにアクセスするためのアクセストークンを、集中型セキュアマネージメントシステムを通じてサードパーティーアプリケーションに発行するステップとを含む方法が開示されている。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

サービス側の機能が複数のシステムに分散された通信システムにおいて、通信端末は、認証システムによって認証され、認証システムとのコネクションを確立してから、リソース提供システムにリソースへのアクセスを要求するプロセスも想定される。ここで、リソース提供システムは、上記のコネクションに接続していない場合、通信端末をリソースへアクセスさせるための認証情報として、認証システムによる認証で用いられたクライアント証明書を共有できないという課題が生じる。

【課題を解決するための手段】

【０００５】

請求項１に係る発明の認証システムは、通信端末によって送信されるクライアント証明書で認証してから、前記通信端末との間の第１のコネクションを確立する確立手段と、前記通信端末によるリソースへのアクセスの認可を示す認可情報として、前記クライアント証明書に対応する認可情報を出力する出力手段と、前記第１のコネクションとは異なる第２のコネクションにより、前記リソースを提供するリソース提供システムへ前記認可情報を送信させる送信手段と、を有する。

【発明の効果】

【０００６】

以上説明したように本発明によれば、リソース提供システムは、リソース提供システムとは異なるコネクションに接続する認証システムによる認証情報を、認証システムとの間で共有可能になるという効果を奏する。

【図面の簡単な説明】

【０００７】

【図１】本発明の一実施形態に係る通信システムの概略図である。
【図２】一実施形態に係る端末のハードウェア構成図である。
【図３】一実施形態に係る管理システムのハードウェア構成図である。
【図４】一実施形態に係る端末、及び管理システムの各機能ブロック図である。
【図５】一実施形態における処理を示すシーケンス図である。
【発明を実施するための形態】
【０００８】
以下、本発明の実施形態について説明する。
【０００９】
＜＜通信システムの概略＞＞
図１は、本発明の一実施形態に係る通信システムの概略図である。図１は、通信ネットワーク２上に認証、及びリソース提供に係るサービス側を示し、利用者側は、通信ネットワーク２に接続されていることを示している。
【００１０】
以下、通信端末を「端末」と表し、端末のうち任意の端末を端末１０と表す。通信システム１は、端末１０、及び管理システム５０によって構築されている。管理システム５０には、認証システム３０及びリソース提供システム６０が含まれる。
端末１０は、例えば、タブレット、スマートフォン、ＰＣ（personal computer）等の汎用端末、若しくは、テレビ会議端末、電子黒板、電子看板、カメラなどの専用端末である。なお、通信システム１において、端末の種類、及び数は限定されるものではない。また、各端末１０は、同種であっても、異種であっても良い。
【００１１】
通信システム１においてリソースは、任意の場所として、例えば、管理システム５０、又は通信ネットワーク２上の任意のサーバに記憶される。リソースは、例えば、アドレス帳、又は会議履歴などのデータ、若しくは通話用、又は会議用のアプリケーションである。
【００１２】
認証システム３０は、認証の要求元の端末１０から送られてくるクライアント証明書を用いて要求元を認証し、端末１０との間でＴＬＳ(Transport Layer Security)コネクションを確立する。
リソース提供システム６０は、リソースの要求元の端末１０をリソースにアクセスさせる。
【００１３】
＜＜ハードウェア構成＞＞
次に、通信システム１を構成する各装置のハードウェア構成を説明する。
【００１４】
図２は、一実施形態に係る端末１０のハードウェア構成図である。なお、端末１０は、通信可能であれば、端末１０のハードウェア構成は図２の構成に限定されない。例えば、端末１０は、図２に記載されていない構成が含まれていても、図２に記載の構成の一部が含まれていなくても良い。また、図２に記載の構成の一部は端末１０に接続可能な外部装置等であっても良い。図２に示されているように、本実施形態の端末１０は、端末１０全体の動作を制御するＣＰＵ(Central Processing Unit)１０１、ＩＰＬ(Initial Program Loader)等のＣＰＵ１０１の駆動に用いられるプログラムを記憶したＲＯＭ(Read Only Memory)１０２、ＣＰＵ１０１のワークエリアとして使用されるＲＡＭ(Random Access Memory)１０３、端末１０の各種端末用のプログラム、画像データ、及び音データ等の各種データを記憶するフラッシュメモリ１０４、ＣＰＵ１０１の制御にしたがってフラッシュメモリ１０４に対する各種データの読み出し又は書き込みを制御するＳＳＤ（Solid State Drive）１０５、フラッシュメモリやＩＣカード（Integrated Circuit Card）等の記録メディア１０６に対するデータの読み出し又は書き込み（記憶）を制御するメディアＩ／Ｆ１０７、宛先を選択する場合などに操作される操作ボタン１０８、端末１０の電源のＯＮ

／ＯＦＦを切り換えるための電源スイッチ１０９、通信ネットワーク２を利用してデータ伝送をするためのネットワークＩ／Ｆ(Interface)１１１を備えている。

【００１５】

また、端末１０は、ＣＰＵ１０１の制御に従って被写体を撮像して画像データを得る内蔵型のカメラ１１２、このカメラ１１２の駆動を制御する撮像素子Ｉ／Ｆ１１３、音を入力する内蔵型のマイク１１４、音を出力する内蔵型のスピーカ１１５、ＣＰＵ１０１の制御に従ってマイク１１４及びスピーカ１１５との間で音信号の入出力を処理する音入出力Ｉ／Ｆ１１６、ＣＰＵ１０１の制御に従って外付けのディスプレイ１２０に画像データを伝送するディスプレイＩ／Ｆ１１７、各種の外部機器を接続するための外部機器接続Ｉ／Ｆ１１８、端末１０の各種機能の異常を知らせるアラームランプ１１９、及び上記各構成要素を図２に示されているように電気的に接続するためのアドレスバスやデータバス等のバスライン１１０を備えている。

【００１６】

ディスプレイ１２０は、被写体の画像や操作等を表示する液晶や有機ＥＬ(Organic Electroluminescence)によって構成された表示部である。また、ディスプレイ１２０は、ケーブル１２０ｃによってディスプレイＩ／Ｆ１１７に接続される。このケーブル１２０ｃは、アナログＲＧＢ（ＶＧＡ）信号用のケーブルであってもよいし、コンポーネントビデオ用のケーブルであってもよいし、ＨＤＭＩ（登録商標）(High-Definition Multimedia Interface)やＤＶＩ(Digital Video Interactive)信号用のケーブルであってもよい。

【００１７】

カメラ１１２は、レンズや、光を電荷に変換して被写体の画像（映像）を電子化する固体撮像素子を含み、固体撮像素子として、ＣＭＯＳ(Complementary Metal Oxide Semiconductor)や、ＣＣＤ（Charge Coupled Device）等が用いられる。

【００１８】

外部機器接続Ｉ／Ｆ１１８には、筐体１１００の接続口１１３２に差し込まれたＵＳＢ(Universal Serial Bus)ケーブル等によって、外付けカメラ、外付けマイク、及び外付けスピーカ等の外部機器がそれぞれ電気的に接続可能である。外付けカメラが接続された場合には、ＣＰＵ１０１の制御に従って、内蔵型のカメラ１１２に優先して、外付けカメラが駆動する。同じく、外付けマイクが接続された場合や、外付けスピーカが接続された場合には、ＣＰＵ１０１の制御に従って、それぞれが内蔵型のマイク１１４や内蔵型のスピーカ１１５に優先して、外付けマイクや外付けスピーカが駆動する。

【００１９】

なお、記録メディア１０６は、端末１０に対して着脱自在な構成となっている。また、ＣＰＵ１０１の制御にしたがってデータの読み出し又は書き込みを行う不揮発性メモリであれば、フラッシュメモリ１０４に限らず、ＥＥＰＲＯＭ（Electrically Erasable and Programmable ROM）等を用いてもよい。

【００２０】

図３は、一実施形態に係る管理システム５０のハードウェア構成図である。管理システム５０は、管理システム５０全体の動作を制御するＣＰＵ５０１、ＩＰＬ等のＣＰＵ５０１の駆動に用いられるプログラムを記憶したＲＯＭ５０２、ＣＰＵ５０１のワークエリアとして使用されるＲＡＭ５０３、管理システム５０用のプログラム等の各種データを記憶するＨＤ５０４、ＣＰＵ５０１の制御にしたがってＨＤ５０４に対する各種データの読み出し又は書き込みを制御するＨＤＤ(Hard Disk Drive)５０５、フラッシュメモリ等の記録メディア５０６に対するデータの読み出し又は書き込み（記憶）を制御するメディアドライブ５０７、カーソル、メニュー、ウィンドウ、文字、又は画像などの各種情報を表示するディスプレイ５０８、通信ネットワーク２を利用してデータ通信するためのネットワークＩ／Ｆ５０９、文字、数値、各種指示などの入力のための複数のキーを備えたキーボード５１１、各種指示の選択や実行、処理対象の選択、カーソルの移動などを行うマウス５１２、着脱可能な記録媒体の一例としてのＣＤ－ＲＯＭ(Compact Disc Read Only Memory)５１３に対する各種データの読み出し又は書き込みを制御するＣＤ－ＲＯＭドライブ

５１４、及び、上記各構成要素を図３に示されているように電気的に接続するためのアドレスバスやデータバス等のバスライン５１０を備えている。

【００２１】

なお、管理システム５０を構築する認証システム３０、及びリソース提供システム６０は、それぞれ図３に示す構成を有している。

【００２２】

＜＜機能構成＞＞

次に、一実施形態の機能構成について説明する。図４は、一実施形態に係る通信システム１の一部を構成する端末１０、及び管理システム５０の機能ブロック図である。図４では、端末１０、及び管理システム５０が、通信ネットワーク２を介してデータ通信することができるように接続されている。

【００２３】

＜端末の機能構成＞

端末１０は、送受信部１１、操作入力受付部１２、表示制御部１３、及び記憶・読出部１９を有している。これら各部は、図２に示されている各構成要素のいずれかが、フラッシュメモリ１０４からＲＡＭ１０３上に展開されたプログラムに従ったＣＰＵ１０１からの命令によって動作することで実現される機能である。また、端末１０は、図２に示されているＲＯＭ１０２、ＲＡＭ１０３、フラッシュメモリ１０４によって構築される記憶部１０００を有している。

【００２４】

（端末の各機能構成）

次に、図２及び図４を用いて、端末１０の各機能構成について詳細に説明する。なお、以下では、端末１０の各機能構成を説明するにあたって、図２に示されている各構成要素のうち、端末１０の各機能構成を実現させるための主な構成要素との関係も説明する。

【００２５】

送受信部１１は、ＣＰＵ１０１からの命令、及びネットワークＩ／Ｆ１１１によって実現され、通信ネットワーク２を介して、相手側の端末、各装置又はシステム等と各種データ（または情報）の送受信を行う。

【００２６】

操作入力受付部１２は、ＣＰＵ１０１からの命令、並びに操作ボタン１０８及び電源スイッチ１０９によって実現され、ユーザによる各種入力を受け付けたり、ユーザによる各種選択を受け付けたりする。

【００２７】

表示制御部１３は、ＣＰＵ１０１からの命令、及びディスプレイＩ／Ｆ１１７によって実現され、通話する際に相手側から送られてきた画像データをディスプレイ１２０に送信するための制御を行う。

【００２８】

記憶・読出部１９は、ＣＰＵ１０１からの命令及びＳＳＤ１０５によって実行され、又はＣＰＵ１０１からの命令によって実現され、記憶部１０００に各種データを記憶したり、記憶部１０００に記憶された各種データを抽出したりする処理を行う。

【００２９】

＜管理システムの機能構成＞

管理システム５０の認証システム３０は、送受信部３１、トークン発行部３２、及び記憶・読出部３９を有している。これら各部は、図３に示されている各構成要素のいずれかが、ＨＤ５０４からＲＡＭ５０３上に展開された認証システム３０用のプログラムに従ったＣＰＵ５０１からの命令によって動作することで実現される機能である。また、認証システム３０は、ＨＤ５０４により構築される記憶部３０００を有している。

【００３０】

（アカウント管理テーブル）

表１はアカウント管理テーブルを示す概念図である。記憶部３０００には、アカウント

管理テーブルによってアカウント管理ＤＢ３００１が構築される。アカウント管理テーブルでは、アカウントＩＤ（identifier, identification）ごとに、Common Name、及びアカウントによるアクセスが認可されるリソースのリソースＩＤが関連付けられて管理される。アカウントＩＤは、リソースへのアクセスの権限を示すアカウントを識別する。Common NameはTLSコネクションの確立時に利用されるクライアント証明書に含まれており、TLSコネクションの相手側、即ち端末１０側を識別する。本実施形態においてＩＤ及び名称は、文字、数字、記号などの任意の情報によって表される。また、ＩＤは、メールアドレスや、電話番号などの対象を一意に特定できるものであっても良い。

【００３１】

【表１】

アカウントID	Common Name	リソースID
A101	CN101	R1001, R1002
A102	CN102	R2001, R2002, R2003
…	…	…

【００３２】

送受信部３１は、ＣＰＵ５０１からの命令、及びネットワークＩ／Ｆ５０９によって実現され、通信ネットワーク２を介して各端末、装置又はシステムと各種データ（または情報）の送受信を行う。

【００３３】

トークン発行部３２は、ＣＰＵ５０１からの命令によって実現され、端末１０による要求に応じて、アクセストークンを発行する。

【００３４】

記憶・読出部３９は、ＣＰＵ５０１からの命令及びＨＤＤ５０５によって実現され、記憶部３０００に各種データを記憶したり、記憶部３０００に記憶された各種データを抽出したりする処理を行う。

【００３５】

管理システム５０のリソース提供システム６０は、送受信部６１、トークン検証部６２、リソース提供部６３、及び記憶・読出部６９を有している。これら各部は、図３に示されている各構成要素のいずれかが、ＨＤ５０４からＲＡＭ５０３上に展開されたリソース提供システム６０用のプログラムに従ったＣＰＵ５０１からの命令によって動作することで実現される機能である。また、リソース提供システム６０は、ＨＤ５０４により構築される記憶部６０００を有している。

【００３６】

記憶部６０００には、リソースＩＤに対応付けられて、リソース５０３０が管理されている。端末１０から取得されるアクセストークンが正当なものであると検証された場合、リソース５０３０は、リソース提供部６３によって端末１０へ提供される。

【００３７】

送受信部６１は、ＣＰＵ５０１からの命令、及びネットワークＩ／Ｆ５０９によって実現され、通信ネットワーク２を介して各端末、装置又はシステムと各種データ（または情報）の送受信を行う。

【００３８】

トークン検証部６２は、ＣＰＵ５０１からの命令によって実現され、端末１０から送られてくるアクセストークンを検証する。

【００３９】

リソース提供部６３は、ＣＰＵ５０１からの命令によって実現され、アクセストークンの検証結果に応じて、端末１０へリソースを提供する。

【００４０】

記憶・読出部６９は、ＣＰＵ５０１からの命令及びＨＤＤ５０５によって実行され、記

憶部６０００に各種データを記憶したり、記憶部６０００に記憶された各種データを抽出したりする処理を行う。

【００４１】

＜＜処理または動作＞＞

続いて、通信システム１を構成する端末１０、及び管理システム５０の処理または動作について説明する。まずは、図５を用いて、一実施形態における認証処理について説明する。図５は、一実施形態における認証処理を示すシーケンス図である。

【００４２】

端末１０の送受信部１１、及び認証システム３０の送受信部３１は、TLS通信の基本的な機能を有する。端末１０の送受信部１１、及び認証システム３０の送受信部３１は、ＴＬＳのハンドシェイクプロトコルにより、コネクションtls1を確立する（ステップＳ２１）。ハンドシェイクプロトコルにおいて、端末１０の送受信部１１は、暗号化されたクライアント証明書を認証システムへ送信する。クライアント証明書は、端末１０の記憶部１０００、フラッシュメモリ１０４、又は記録メディア１０６に記憶されているものであっても、外部機器接続Ｉ／Ｆによって外部機器から取得されるものであっても良い。クライアント証明書には、端末１０側を識別するためのCommon Nameが含まれている。認証システム３０の送受信部３１は、暗号化されたクライアント証明書を受信し、これを復号化することでクライアントとしての端末１０側を認証する。

【００４３】

コネクションtls1が確立すると、端末１０の送受信部１１、及び認証システム３０の送受信部３１は、コネクションtls1の共通鍵で暗号化されたデータによる通信を開始する。この通信で、端末１０の送受信部１１は、リソース１０３０へアクセスするためのアクセストークンの要求を認証システム３０へ送信する（ステップＳ２２）。アクセストークンの要求を受信した認証システム３０の送受信部３１は、ステップＳ２１で受信したクライアント証明書に含まれるCommon Nameをアクセストークンの要求に付加して、トークン発行部３２へ転送する。

【００４４】

認証システム３０のトークン発行部３２は、アクセストークンの要求に付加されたCommon Nameを検索キーとしてアカウント管理テーブル（表１参照）を検索して、対応するアカウントＩＤ、及びリソースＩＤを取得する（ステップＳ２３）。これにより、トークン発行部３２は、リソースへのアクセス要求元を、アカウントＩＤのアカウントとして認証する。また、トークン発行部３２は、認証されたアカウントによる取得されたリソースＩＤのリソースへのアクセスを認可する。

【００４５】

認証システム３０のトークン発行部３２は、リソースへのアクセスの許可を示すアクセス許可情報として、ステップＳ２３で取得されたアカウントＩＤ、及びリソースＩＤを含み、電子署名が付加されたアクセストークンを発行する（ステップＳ２４）。

【００４６】

管理システム５０の送受信部１１は、アクセストークンの要求に対する応答で、ステップＳ２４で発行されたアクセストークンを端末１０へ送信する（ステップＳ２５）。端末１０の送受信部１１は、管理システム５０による応答でアクセストークンを受信する。

【００４７】

リソース提供システム６０の送受信部６１は、TLS通信の基本的な機能を有する。端末１０の送受信部１１、及びリソース提供システム６０の送受信部６１は、コネクションtls1とは異なるコネクションtls2を確立する（ステップＳ３１）。

【００４８】

コネクションtls2が確立すると、端末１０の送受信部１１、及びリソース提供システム６０の送受信部６１は、コネクションtls2の共通鍵で暗号化されたデータによる通信を開始する。この通信で、端末１０の送受信部１１は、ステップＳ２５で受信したアクセストークン、及びアクセスを要求するリソースのリソースＩＤを含むリソース要求をリソース

提供システム６０へ送信する（ステップＳ３２）。リソース提供システム６０の送受信部６１は、コネクションtls2でリソース要求を受信する。

【００４９】

リソース提供システム６０のトークン検証部６２は、アクセストークンに含まれる電子署名により、アクセストークンが認証システム３０のトークン発行部３２によって発行されたものであるか検証する（ステップＳ３３）。

【００５０】

アクセストークンが認証システム３０のトークン発行部３２によって発行されたものであることが検証された場合、トークン検証部６２は、リソース要求に含まれるリソースＩＤと、アクセストークンのアクセス許可情報に含まれるリソースＩＤが同じであるか検証する（ステップＳ３４）。リソースＩＤが同じであると検証された場合、トークン検証部６２は、アクセス許可判定をリソース提供部６３へ出力する。

【００５１】

アクセス許可判定が出力されると、リソース提供部６３は、リソース要求に含まれるリソースＩＤに対応するリソース５０３０を記憶部６０００から取得する（ステップＳ３５）。

【００５２】

リソース提供システム６０の送受信部６１は、リソース提供部６３によって取得されるリソース５０３０を、リソース要求の応答として、要求元の端末１０へ送信する（ステップＳ３６）。端末１０の送受信部１１は、リソース提供システム６０によって送信されるリソース５０３０を受信する。これにより、端末１０はリソース５０３０にアクセスすることができる。

【００５３】

なお、リソース提供システム６０の記憶部６０００は、リソースＩＤに対応付けてリソース５０３０を管理する実施形態に変えて、リソースＩＤに対応付けてリソース５０３０のURL（Uniform Resource Locator）を管理しても良い。この場合、リソース提供部６３は、リソース要求に含まれるリソースＩＤに対応するリソース５０３０のURLを取得する。リソース提供システム６０の送受信部６１は、取得されたURLをリソースの要求元の端末１０へ送信する。これにより、端末１０は、URLに基づいてリソースへアクセスできる。

【００５４】

＜＜実施形態の主な効果＞＞

上記実施形態の認証認可方法によると、認証システム３０の送受信部３１（確立手段の一例）は、端末１０から送られてくるクライアント証明書で認証してから、端末１０との間のコネクションtls1（第１のコネクションの一例）を確立する（確立処理の一例）。認証システム３０のトークン発行部３２（出力手段の一例）は、端末１０によるリソースへのアクセスの認可を示す認可情報として、上記のクライアント証明書に対応するアクセストークンを出力する（出力処理の一例）。認証システム３０の送受信部３１（送信手段の一例）は、端末１０へアクセストークンを送信する（送信処理の一例）。これにより、端末１０は、リソース提供システム６０へ、コネクションtls1とは異なるコネクションtls2（第２のコネクションの一例）でアクセストークンを送信する。リソース提供システム６０の送受信部６１（受信手段の一例）は、コネクションtls2でアクセストークンを受信する。

この認証認可方法によると、コネクションtls2に接続するリソース提供システム６０は、異なるコネクションtls1に接続する認証システム３０による端末１０の認証情報を、認証システム３０との間で共有可能になる。これにより、リソース提供システム６０は、認証、認可に用いる情報の管理の付加が低減する。

【００５５】

認証システム３０の送受信部３１（受付手段の一例）は、コネクションtls1で、アクセストークンの要求を受け付ける。認証システム３０のトークン発行部３２（出力手段の一

例）は、アクセストークンの要求元のクライアント証明書に対応する認可情報が含まれたアクセストークンを出力する。これにより、認証システム３０は、アクセストークンの要求元ごとに、要求元に対応するアクセストークンを発行できる。

【００５６】

認証システム３０のアカウント管理ＤＢ３００１（管理手段の一例）は、クライアント証明書に含まれるCommon Name（識別情報の一例）と、リソースＩＤと、を関連付けて管理する。認証システム３０のトークン発行部３２は、アクセストークンの要求元のクライアント証明書のCommon Nameに関連付けられているリソースＩＤをアカウント管理ＤＢ３００１から取得し、このリソースＩＤを含むアクセストークンを出力する。これにより、認証システム３０は、クライアント証明書に含まれるCommon Nameに基づいてアクセストークンを発行できる。

【００５７】

＜＜実施形態の補足＞＞

端末１０、及び管理システム５０用の各プログラムは、インストール可能な形式又は実行可能な形式のファイルによって、コンピュータで読み取り可能な記録媒体（記録メディア１０６等）に記録されて流通されるようにしてもよい。また、上記記録媒体の他の例として、ＣＤ－R(Compact Disc Recordable)、ＤＶＤ(Digital Versatile Disk)、ブルーレイディスク等が挙げられる。

【００５８】

また、上記実施形態の各プログラムが記憶されたＣＤ－ＲＯＭ等の記録媒体、並びに、これらプログラムが記憶されたＨＤ５０４は、プログラム製品(Program Product)として、国内又は国外へ提供されることができる。

【００５９】

また、上記実施形態における端末１０、及び管理システム５０は、単一のコンピュータによって構築されてもよいし、複数のコンピュータによって構築されていてもよい。なお、上記実施形態では、認証システム３０及びリソース提供システム６０に、管理システム５０の各部（機能又は手段）が任意に割り当てられている。また、管理システム５０は、一つの認証システム３０及び複数のリソース提供システム６０を有しても良い。この場合、認証システム３０は、通信システム１全体の管理者によって管理され、各リソース提供システム６０は各リソースの提供者によって管理されても良い。

【００６０】

上記で説明した実施形態の各機能は、一又は複数の処理回路によって実現することが可能である。ここで、本明細書における「処理回路」とは、電子回路を含むプロセッサのようにソフトウェアによって各機能を実行するようプログラミングされたプロセッサや、上記で説明した各機能を実行するよう設計されたASIC(Application Specific Integrated Circuit)や従来の回路モジュール等のデバイスを含むものとする。

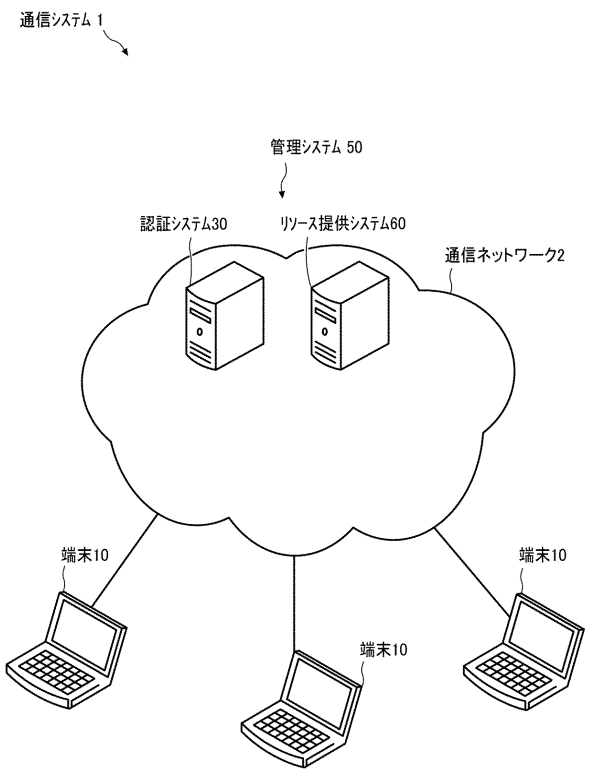
【符号の説明】

【００６１】

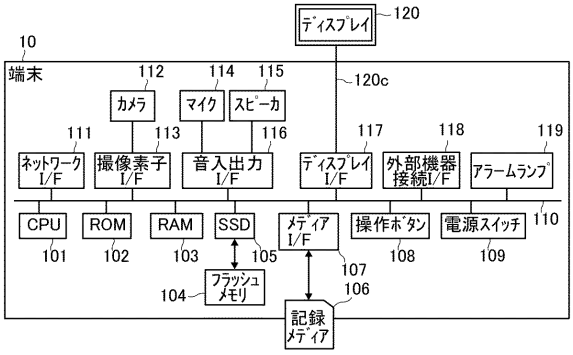
１　通信システム
２　通信ネットワーク
１０　端末
１１　送受信部
１２　操作入力受付部
１３　表示制御部
１９　記憶・読出部
３０　認証システム
３１　送受信部
３２　トークン発行部
３９　記憶・読出部
５０　管理システム

６０　リソース提供システム
６１　送受信部
６２　トークン検証部
６３　リソース提供部
６９　記憶・読出部
１０００　記憶部
３０００　記憶部
３００１　アカウント管理ＤＢ
５０３０　リソース
６０００　記憶部
【先行技術文献】
【特許文献】
【００６２】
【特許文献１】特表２０１４－５３１１６３号公報

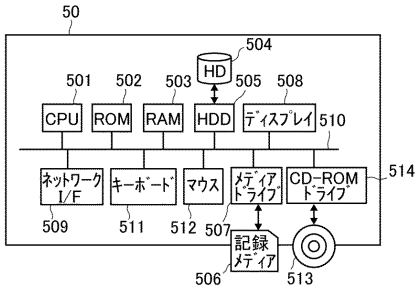
【図１】



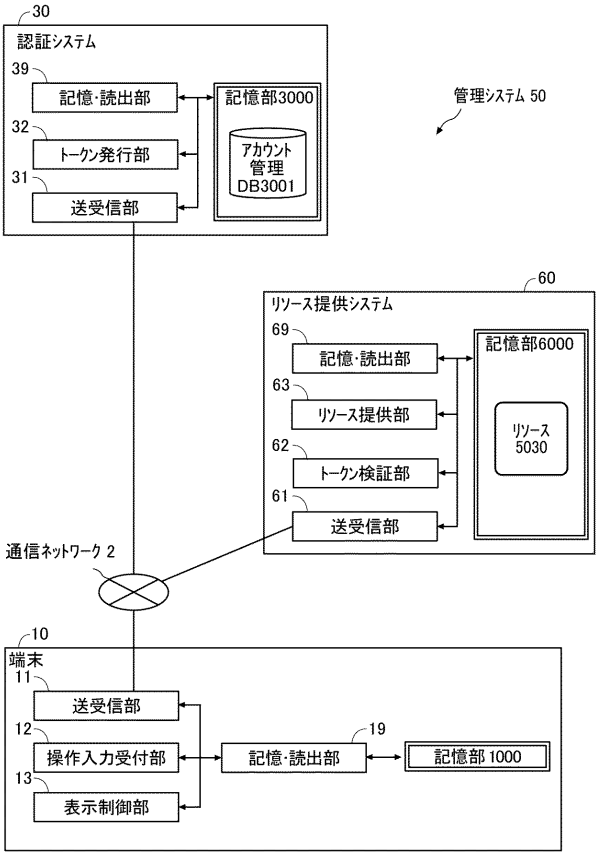
【図２】



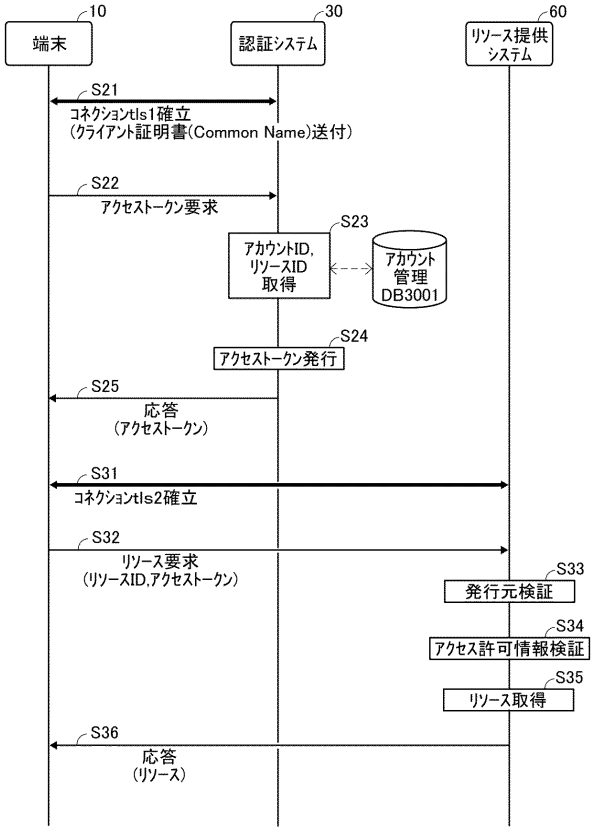
【図３】


50
504
HD
501
502
503
505
508
CPU
ROM
RAM
HDD
ディスプレイ
510
ネットワーク I/F
キーボード
マウス
メディアドライブ
CD-ROM ドライブ
514
509
511
512
507
記録メディア
506
513

【図４】


30
認証システム
39
記憶・読出部
記憶部3000
アカウント管理 DB3001
32
トークン発行部
31
送受信部
管理システム 50
60
リソース提供システム
69
記憶・読出部
記憶部6000
リソース 5030
63
リソース提供部
62
トークン検証部
61
送受信部
通信ネットワーク 2
10
端末
11
送受信部
12
操作入力受付部
19
記憶・読出部
記憶部 1000
13
表示制御部

【図５】


10
端末
30
認証システム
60
リソース提供システム
S21
コネクションtls1確立
（クライアント証明書(Common Name)送付）
S22
アクセストークン要求
S23
アカウントID, リソースID 取得
アカウント管理 DB3001
S24
アクセストークン発行
S25
応答
（アクセストークン）
S31
コネクションtls2確立
S32
リソース要求
（リソースID,アクセストークン）
S33
発行元検証
S34
アクセス許可情報検証
S35
リソース取得
S36
応答
（リソース）

フロントページの続き

(72)発明者　曽根田　拓也
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 EA01 EA04 EA18 EA19 JA03 JA21 KA02
NA02 NA36 NA37 NA38 PA07
5K067 AA21 BB21 HH22 HH23