

明 細 書

発明の名称：

アクセス制御装置、通信システム、プログラム、及びアクセス制御方法
技術分野

[0001] 本発明は、通信端末からアプリケーションへのアクセスを制御する発明に関する。

背景技術

[0002] 近年、出張経費及び出張時間を削減する要請に伴い、インターネットや専用線等の通信ネットワークを介して通信を行う通信システムが普及している。通信システムのうち、例えば、テレビ会議システムでは、複数の通信端末間で、画像データ及び音データの送受信が行われることにより、テレビ会議を実現することができる（特許文献1参照）。

[0003] また、テレビ会議システムにおいては、通信端末の認証に用いられる端末証明書情報に基づいて、伝送管理システムや、アップデートシステム、画面提供システム等のURIを通信端末へ通知する方法が知られている（特許文献2参照）。この方法によると、一度の認証により、伝送管理システム等の各サービスプロバイダにアクセスすることが可能となるので利便性が向上する。

[0004] 一方、サービスを提供するためのアプリケーションとしては、例えば、Java（登録商標）アプリケーションなど、プラットフォームに依存することなく動作するものが開発されている。これにより、PC(Personal Computer)とテレビ会議専用端末などの異なるプラットフォームの通信端末が、それぞれ同じアプリケーションを動作させることにより、異端末間の通信等の異端末間を連携させるサービスの提供が可能となる。

先行技術文献

特許文献

[0005] 特許文献1：特開2008-227577号公報

特許文献2：特開2012-134940号公報

発明の概要

発明が解決しようとする課題

- [0006] しかしながら、通信端末のプラットフォームが異なる場合、それぞれの通信端末において利用可能な認証方式は異なることがある。このため、それぞれの通信端末が利用した認証方式による認証に基づいてアプリケーションへのアクセスを許可した場合には、認証方式毎に信頼性が異なるため、アプリケーション側が期待する安全性を担保しにくくなるという課題が生じる。

課題を解決するための手段

- [0007] 本発明の第一の側面によれば、通信端末からアプリケーションへのアクセスを制御するアクセス制御装置であって、前記アプリケーション毎に、前記アプリケーションへのアクセス要求元を認証するために有効な認証方式を示す認証情報を関連付けて管理する認証方式管理手段と、通信端末からの要求に基づいて、前記通信端末において利用可能な認証方式により要求元を認証する認証手段と、前記通信端末から、所望のアプリケーションへのアクセスを伴う要求を受け付けるアクセス要求受付手段と、前記認証方式管理手段において、前記所望のアプリケーションに関連付けられて、前記認証に用いられた認証方式を示す認証情報が管理されていない場合には、前記通信端末を前記所望のアプリケーションにアクセスさせないようにする一方で、前記認証方式管理手段において、前記所望のアプリケーションに関連付けられて、前記認証に用いられた認証方式を示す認証情報が管理されている場合には、前記通信端末から前記所望のアプリケーションへのアクセスを制御するアクセス制御手段と、を有することを特徴とするアクセス制御装置である。

発明の効果

- [0008] 以上説明したように本発明によれば、アクセス制御装置は、アプリケーション毎に、このアプリケーションへのアクセス要求元を認証するために有効な認証方式を示す認証情報を関連付けて管理する。これにより、アプリケー

ションへのアクセス要求元を、任意の認証方式により認証していた場合でも、この認証方式が有効な認証方式でない場合には、アクセス要求元をアプリケーションにアクセスさせないようにすることが可能となるので、アプリケーション側が期待する安全性を担保しやすくなるという効果を奏する。

図面の簡単な説明

[0009] [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]認証・認可方式を示すフロー図である。

[図3]通信端末の外観図の一例である。

[図4]通信端末のハードウェア構成図である。

[図5]通信端末のハードウェア構成図である。

[図6]通信管理システム及び中継装置のハードウェア構成図である。

[図7]通信端末のソフトウェア構成図である。

[図8]通信端末、通信管理システム、及びアプリケーションサーバの各機能ブロック図である。

[図9]端末認証管理テーブルを示す概念図である。

[図10]アプリ利用管理テーブルを示す概念図である。

[図11]アプリURL管理テーブルを示す概念図である。

[図12]アプリ認可管理テーブルを示す概念図である。

[図13]アクセストークン管理テーブルを示す概念図である。

[図14]通信システムにおける各種情報の送受信の状態を示した概念図である。

[図15]通信を開始する準備段階の処理を示したシーケンス図である。

[図16]通信端末が起動してからアプリアイコンを表示させるまでの処理を示したシーケンス図である。

[図17]アプリケーションの起動を要求する処理を示したシーケンス図である。

[図18]アプリケーションリストの画面例を示した図である。

[図19]アプリケーションの起動の可否を判断する処理を示したフロー図であ

る。

[図20]通信管理システムの機能ブロック図である。

[図21]アプリケーションのリストを作成する処理を示したフロー図である。

発明を実施するための形態

[0010] 以下、図面を用いて、本発明の一実施形態について説明する。

[0011] [第1の実施形態]

まず、本発明の第1の実施形態について説明する。

[0012] <<実施形態の全体構成>>

図1は、本発明の第1の実施形態に係る通信システムの概略図である。図1に示されているように、通信システム1は、複数の通信端末(10a a, 10a b, …)、各通信端末(10a a, 10a b, …)用のディスプレイ(120a a, 120a b, …)、複数の中継装置(30a, 30b, 30c, 30d)、通信管理システム50、アプリケーションサーバ80、プログラム提供システム90、及びメンテナンスシステム100によって構築されている。

[0013] なお、以下、「アプリケーション」は「アプリ」と省略して説明する。また、以下では、「通信端末」は単に「端末」として表され、「通信管理システム」は単に「管理システム」として表されている。また、複数の端末(10a a, 10a b, …)のうち任意の端末は、「端末10」と表され、複数のディスプレイ(120a a, 120a b, …)のうち任意のディスプレイは「ディスプレイ120」と表され、複数の中継装置(30a, 30b, 30c)のうち任意の中継装置は「中継装置30」と表されている。また、ルータ(70a, 70b, 70c, 70d, 70a b, 70c d)のうち任意のルータは、「ルータ70」と表されている。なお、この通信は、音、映像(画像)、又は、音及び映像(画像)によって実現することができる。

[0014] この通信システム1によって、通信データの一例としての画像データ及び音データの通信が行われることで、遠隔地間のテレビ会議等を実現することができる。なお、複数のルータ(70a, 70b, 70c, 70d, 70a

b, 70cd)は、通信データの最適な経路の選択を行う。また、アプリサーバ80は、各端末10で動作する各種アプリ（オンラインアプリ）を管理する。各端末10は、アプリサーバ80から各種アプリをダウンロードして利用する。

[0015] また、端末(10aa, 10ab, 10ac, ...)、中継装置30a、及びルータ70aは、LAN2aによって通信可能に接続されている。通信端末(10ba, 10bb, 10bc, ...)、中継装置30b、及びルータ70bは、LAN2bによって通信可能に接続されている。また、LAN2a及びLAN2bは、ルータ70abが含まれた専用線2abによって通信可能に接続されている。更に、LAN2a、LAN2b、及び専用線2abは、会社の一例としてX社内で構築されている。例えば、LAN2aはX社のA事業所内で構築されており、LAN2bはX社のB事業所内で構築されている。

[0016] また、X社の保有する端末10のうち、端末(10aa, 10bc)は、テレビ会議の用途の他、テレビ会議に関連しない用途でも利用可能な汎用端末である。X社の保有する残りの端末10は、テレビ会議の用途で利用可能な専用端末である。専用端末と汎用端末とは、それぞれ、プラットフォームが異なっている。

[0017] 一方、通信端末(10ca, 10cb, 10cc, ...)、中継装置30c、及びルータ70cは、LAN2cによって通信可能に接続されている。通信端末10d(10da, 10db, 10dc, ...)、中継装置30d、及びルータ70dは、LAN2dによって通信可能に接続されている。また、LAN2c及びLAN2dは、ルータ70cdが含まれた専用線2cdによって通信可能に接続されている。更に、LAN2c、LAN2d、及び専用線2cdは、所定の会社の一例としてY社内で構築されている。例えば、LAN2cはY社のC事業所内で構築されており、LAN2dはY社のD事業所内で構築されている。X社及びY社は、それぞれルータ(70ab, 70cd)からインターネット2iを介して通信可能に接続されている。

。

[0018] また、Ｙ社の保有する端末１０のうち、端末（１０ｃｃ，１０ｄｃ）は、テレビ会議の用途の他、テレビ会議に関連しない用途でも利用可能な汎用端末である。Ｙ社の保有する残りの端末１０は、テレビ会議の用途で利用可能な専用端末である。専用端末と汎用端末とは、それぞれ、プラットフォームが異なっている。

[0019] また、管理システム５０、アプリサーバ８０、プログラム提供システム９０、及びメンテナンスシステム１００は、インターネット２ｉに接続されている。なお、管理システム５０、プログラム提供システム９０、及びメンテナンスシステム１００の設置場所は限定されず、それぞれのシステムが同一地域あるいは同一国内に設置されていても、異なる地域あるいは異なる国内にそれぞれ設置されていても良い。

[0020] また、本実施形態では、ＬＡＮ２ａ、ＬＡＮ２ｂ、専用線２ａｂ、インターネット２ｉ、専用線２ｃｄ、ＬＡＮ２ｃ、及びＬＡＮ２ｄによって、本実施形態の通信ネットワーク２が構築されている。この通信ネットワーク２には、有線だけでなく、ＷｉＦｉ (Wireless Fidelity)やＢｌｕｅｔｏｏｔｈ（登録商標）等の無線による通信が行われる箇所があってもよい。

[0021] また、図１において、各端末１０、各中継装置３０、管理システム５０、各ルータ７０、プログラム提供システム９０、及びメンテナンスシステム１００の下に示されている４組の数字は、一般的なＩＰｖ４におけるＩＰアドレスを簡易的に示している。例えば、端末１０ａａのＩＰアドレスは「１．２．１．３」である。また、ＩＰｖ４ではなく、ＩＰｖ６を用いてもよいが、説明を簡略化するため、ＩＰｖ４を用いて説明している。

[0022] なお、各端末１０は、複数の事業所間での通信や、同じ事業所内の異なる部屋間での通信だけでなく、同じ部屋内での通信や、屋外と屋内又は屋外と屋外での通信で使われてもよい。各端末１０が屋外で使われる場合には、携帯電話通信網等の無線による通信が行われる。

[0023] また、図１に示されている各端末１０は、通信データの送受信により、ユ

ーザの通信を実現する端末であり、例えば、テレビ会議用端末である。更に、端末10は、所定の通信方式（通信の宛先と接続又は切断をするための呼制御方式、及び通信データをIPパケット化するための符号化方式）を利用して、通信データの送受信を行う。

[0024] なお、この呼制御方式としては、(1)SIP(Session Initiation Protocol)、(2)H.323、(3)SIPを拡張したプロトコル、(4)インスタントメッセンジャーのプロトコル、(5)SIPのMESSAGEメソッドを利用したプロトコル、(6)インターネットリレーチャットのプロトコル(IRC(Internet Relay Chat))、(7)インスタントメッセンジャーのプロトコルを拡張したプロトコル等が挙げられる。このうち、(4)インスタントメッセンジャーのプロトコルは、例えば、(4-1)XMPP(Extensible Messaging and Presence Protocol)、又は(4-2)ICQ（登録商標）、AIM（登録商標）、若しくはSkype（登録商標）などで利用されるプロトコルである。また、(7)インスタントメッセンジャーのプロトコルを拡張したプロトコルは、例えば、Jingleである。

[0025] また、端末10は、ユーザの操作に基づいて、テレビ会議用あるいは他の用途のアプリを、アプリサーバ80からダウンロードして利用する。複数の端末10は、お互いに同じアプリを利用した場合、通信ネットワーク2を介して通信を実現することができる。ここで、アプリは、通信及びメッセージアプリを含み、テレビ会議用のアプリの他に、例えば、Skype, Google Talk, LINE, FaceTime, カカオトーク, Tango（登録商標又は未登録商標）等が挙げられる。

[0026] また、管理システム50は、端末10の認証・認可に必要な情報を管理しており、端末10を認証し、アプリへのアクセスを認可するアクセス認可システムの機能を有している。アプリサーバ80は、アプリの実体であるURI (Uniform Resource Identifier) をホストしているサーバである。

[0027] 端末10は、通信ネットワーク2を介して各種アプリを利用することができる。この場合、端末10は、アプリをホストしているアプリサーバ80へのURIを取得し、そこへアクセスする。本発明の一実施形態によると、な

りすまし等の不正利用や、情報漏洩を防止するために、これらのアプリを利用する際に、図2に示したような、認証・認可方式を用いることができる。なお、図2は、認証・認可方式を示すフロー図である。ステップS101で認証が成功したかを確認し、NOの場合はフローを終了する。一方、YESの場合は、ステップS102で認可情報を作成する。ステップS103で認可情報を送信する。ステップS104でアプリを起動する。以上でフローを終了する。すなわち、端末10は、管理システム50へ認証要求を行う。この認証に成功した場合には、管理システム50は、アプリへのアクセスが認可されていることを示すアクセストークン等の認可情報を作成して端末10へ送信する。端末10では、認可情報をアプリサーバ80へ送信することにより、アプリへアクセスしアプリを起動する。

[0028] 管理システム50は、専用端末と汎用端末等の多様なプラットフォームの端末10から認証要求を受け付け、アプリ側に代わって一括して端末10の認証を行う。これにより、各アプリ側において、認証に要するコストを削減することが可能となる。この場合、プラットフォームの違いから、端末10毎に利用可能な認証方式は異なっている。このため、正規に認証済みのアカウントによって、端末10にアプリへのアクセスが認可された場合であっても、用いられた認証方式によっては、アプリ側が期待した信頼性が担保されない場合がある。そこで、本実施形態の通信システム1では、アカウント（端末10）、アカウントの認証方式、アプリの認可情報を関連付けて管理することで、アプリ利用の認可時に、アプリを利用するアカウント方式を限定して、安全性を担保している。

[0029] <<実施形態のハードウェア構成>>

次に、本実施形態のハードウェア構成を説明する。まず、端末10のハードウェア構成について説明する。端末10には、通話アプリを利用して端末10間のテレビ会議を実現するテレビ会議専用端末（専用端末）と、通話アプリを利用可能であるとともにテレビ会議に関連しない用途でも利用可能なPC（Personal Computer）（汎用端末）と、が含まれている。以下、専用端

末の外観について説明する。

[0030] 図3は、本実施形態に係る端末10の外観図である。図3に示されているように、端末10は、筐体1100、アーム1200、及びカメラハウジング1300を備えている。このうち、筐体1100の前側壁面1110には、複数の吸気孔によって形成された不図示の吸気面が設けられており、筐体1100の後側壁面1120には、複数の排気孔が形成された排気面1121が設けられている。これにより、筐体1100に内蔵された冷却ファンの駆動によって、不図示の吸気面を介して端末10の後方の外気を取り込み、排気面1121を介して端末10の後方へ排気することができる。筐体1100の右側壁面1130には、收音用孔1131が形成され、後述する内蔵型のマイク114によって音声、物音、雑音等の音が收音可能となっている。

[0031] 筐体1100の右側壁面1130側には、操作パネル1150が形成されている。この操作パネル1150には、後述の複数の操作ボタン（108a～108e）、後述の電源スイッチ109、及び後述のアラームランプ119が設けられていると共に、後述の内蔵型のスピーカ115からの出力音を通すための複数の音声出力孔によって形成された音出面1151が形成されている。また、筐体1100の左側壁面1140側には、アーム1200及びカメラハウジング1300を収容するための凹部としての収容部1160が形成されている。筐体1100の右側壁面1130には、後述の外部機器接続I/F118に対して電氣的にケーブルを接続するための複数の接続口（1132a～1132c）が設けられている。一方、筐体1100の左側壁面1140には、後述の外部機器接続I/F118に対して電氣的にディスプレイ120用のケーブル120cを接続するための不図示の接続口が設けられている。

[0032] なお、以下では、操作ボタン（108a～108e）のうち任意の操作ボタンを示す場合には「操作ボタン108」を用い、接続口（1132a～1132c）のうち任意の接続口を示す場合には「接続口1132」を用いて

説明する。

[0033] 次に、アーム 1200 は、トルクヒンジ 1210 を介して筐体 1100 に取り付けられており、アーム 1200 が筐体 1100 に対して、135度のチルト角 $\theta 1$ の範囲で、上下方向に回転可能に構成されている。図3は、チルト角 $\theta 1$ が90度の状態を示している。カメラハウジング 1300 には、後述の内蔵型のカメラ 112 が設けられており、ユーザ、書類、及び部屋等を撮像することができる。また、カメラハウジング 1300 には、トルクヒンジ 1310 が形成されている。カメラハウジング 1300 は、トルクヒンジ 1310 を介して、アーム 1200 に取り付けられている。そして、カメラハウジング 1300 は、トルクヒンジ 1310 を介してアーム 1200 に取り付けられており、カメラハウジング 1300 がアーム 1200 に対して、図3で示されている状態を0度として ± 180 度のパン角 $\theta 2$ の範囲で、且つ、 ± 45 度のチルト角 $\theta 3$ の範囲で、上下左右方向に回転可能に構成されている。

[0034] なお、上記図3の外観図はあくまで一例であってこの外観に限定するものではない。端末 10 は例えば汎用的なPC、スマートフォン、タブレット型端末、電子黒板、プロジェクターなどの投影装置、自動車に搭載されるカーナビゲーション端末、複合機やプリンタなどの画像形成装置、ウェアラブル端末であってもよい。カメラやマイクは必ずしも内蔵型である必要はなく外付けであってもよい。

[0035] なお、端末 10 のうち汎用端末、並びに、管理システム 50、プログラム提供システム 90、及びメンテナンスシステム 100 は、それぞれ一般のサーバコンピュータの外観と同じであるため、外観の説明を省略する。

[0036] 続いて端末 10 のうち専用端末のハードウェア構成について説明する。図4は、本実施形態に係る端末 10 のハードウェア構成図である。図4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CPU 101の駆動に用いられるプログラムを記憶したROM (Read Onl

y Memory) 102、CPU 101のワークエリアとして使用されるRAM(Random Access Memory) 103、通信端末10用のプログラム、画像データ、及び音声データ等の各種データを記憶するフラッシュメモリ104、CPU 101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ドライブ107、端末10の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。

[0037] また、端末10は、CPU 101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/F 113、音声を入力する内蔵型のマイク114、音声を出力する内蔵型のスピーカ115、CPU 101の制御に従ってマイク114及びスピーカ115との間で音声信号の入出力を処理する音声入出力I/F 116、CPU 101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/F 117、各種の外部機器を接続するための外部機器接続I/F 118、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4に示されているように電氣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。

[0038] ディスプレイ120は、被写体の画像や操作用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/F 117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。

[0039] 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。

[0040] 外部機器接続 I / F 118 には、図 6 に示されている筐体 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氣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、CPU 101 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、CPU 101 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。

[0041] 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、CPU 101 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。

[0042] 続いて端末 10 のうち汎用端末のハードウェア構成について、専用端末と異なる点を説明する。図 5 は、本実施形態に係る端末 10 のハードウェア構成図である。汎用端末において、カメラ 112、マイク 114、スピーカ 115 は外付けの外部機器であり、それぞれケーブル (112c, 114c, 115c) によって、外部機器接続 I / F 118 に接続している。

[0043] また、汎用端末には、操作ボタン 108 が設けられておらず、代わりに、ユーザから文字や選択結果等の入力を受け付ける手段として、キーボード 120 及びマウス 121 が設けられている。また、汎用端末には、アラームランプ 119 が設けられておらず、端末 10 の異常を、スピーカ 115 あるいはディスプレイ 120 により通知するように構成されている。

[0044] 図 6 は、本発明の本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CPU201、IPL等のCPU201の駆動に用いられるプログラムを記憶したROM202、CPU201のワークエリアとして使用されるRAM203、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HD204、CPU201の制御にしたがってHD204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)205、フラッシュメモリ等の記録メディア206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207、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208、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/F209、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211、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212、着脱可能な記録媒体の一例としてのCD-ROM(Compact Disc Read Only Memory)213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214、及び、上記各構成要素を図6に示されているように電氣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210を備えている。

[0045] 一方、中継装置30、アプリサーバ80、プログラム提供システム90、及びメンテナンスシステム100は、上記管理システム50と同様のハードウェア構成を有しているため、その説明を省略する。

[0046] 続いて、端末10のソフトウェア構成について説明する。図7は、端末10のソフトウェア構成図である。図7に示されているように、OS1020、通話アプリ1031、残高照会アプリ1032、遠隔医療アプリ1033は、RAM103の作業領域1010上で動作する。OS1020は、特に限定されないが、工場出荷前から端末10にインストールされている。また、通話アプリ1031、残高照会アプリ1032、遠隔医療アプリ1033は、工場出荷後にアプリサーバ80から取得してインストールされたものであっても良い。

[0047] また、これらのうち、OS 1020は、基本的な機能を提供し、端末10全体を管理する基本ソフトウェアである。ブラウザは、OS 1020上で動作するソフトウェアであって、情報を一定の目的に沿って表示し閲覧に供するために用いられる。通話アプリ1031、残高照会アプリ1032、遠隔医療アプリ1033は、ブラウザ1021上で動作するソフトウェアであって、他の端末10との通信や、通信料の照会などの目的で用いられる。なお、本発明の一実施形態によると、各通話アプリ1031、残高照会アプリ1032、遠隔医療アプリ1033は、それぞれ異なる通信プロトコルに対応したものであっても良い。

[0048] なお、通話アプリ1031、残高照会アプリ1032、遠隔医療アプリ1033は、一例であって、他のアプリがインストールされていてもよいが、説明の簡略化のために、3種類のアプリを説明した。また、複数の通話アプリがインストールされる場合は、上記(1)～(7)のように、異なるプロトコルの通話アプリがインストールされてもよい。

[0049] <<実施形態の機能構成>>

次に、本実施形態の機能構成について説明する。図8は、本実施形態の通信システム1の一部を構成する端末10、管理システム50、及びアプリサーバ80の機能ブロック図である。図8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。

[0050] <通信端末の機能構成>

端末10は、装置制御部1050及び通信制御部1060を有している。このうち、装置制御部1050は、図7に示されているOS 1020およびブラウザ1021が起動することによって実現される。また、通信制御部1060は、図7に示されている通話アプリ1031、残高照会アプリ1032、遠隔医療アプリ1033の何れかが起動されることによって実現される。

[0051] また、装置制御部1050は、送受信部11、操作入力受付部12、表示

制御部 13、起動要求部 14、及び記憶・読出部 19を有している。これら各部は、図4あるいは図5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RAM 103上に展開されたプログラムに従ったCPU 101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。

[0052] 一方、通信制御部 1060は、送受信部 21、起動部 22、表示制御部 24、機能実行部 25、及び記憶・読出部 29を有している。これら各部は、図4あるいは図5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RAM 103上に展開された通話アプリ（プログラム）に従ったCPU 101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。

[0053] また、端末 10は、図4あるいは図5に示されているROM 102、RAM 103、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。

[0054] （認証用データ）

端末 10の記憶部 1000には、端末 10が管理システム 50にログイン要求するときに、ログイン要求元を認証するために用いられる認証情報として認証用データ 1001が記憶されている。本発明の一実施形態によると、端末 10のうち、専用端末には証明書情報が記憶されており、さらに、任意にパスワードが記憶されている。これにより、専用端末ではクライアント証明書認証が利用可能であり、任意にパスワード認証が利用可能となる。汎用端末にはパスワードが記憶されている。これにより、汎用端末ではパスワード認証が利用可能となる。

[0055] （装置制御部の各機能構成）

次に、図8を用いて、端末 10における装置制御部 1050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における装置制御部 1050の各機能構成を説明するにあたって、図4あるいは図5に示されている各構成要素のうち、装置制御部 1050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。

[0056] 図8に示されている端末 10の送受信部 11は、図4あるいは図5に示さ

れているCPU101からの命令、及びネットワーク1/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。

[0057] 操作入力受付部12は、図4あるいは図5に示されているCPU101からの命令、並びに図3に示されている操作ボタン（108a、108b、108c、108d、108e）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又は各種選択を受け付ける。例えば、ユーザが、図3に示されている電源スイッチ109をONにすると、図8に示されている操作入力受付部12が電源オンを受け付けて、電源をONにする。

[0058] 表示制御部13は、図4あるいは図5に示されているCPU101からの命令、及びディスプレイ/F117によって実現され、通信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。

[0059] 記憶・読出部19は、図4あるいは図5に示されている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読み出す処理を行う。

[0060] 起動要求部14は、図4あるいは図5に示されているCPU101からの命令に基づいて、ブラウザ1021によって実現される機能であって、通信制御部1060に対して、通話アプリ（1031、1032、1033、1034）の起動を要求する。

[0061] （通信制御部の各機能構成）

次に、図4、図5、及び図8を用いて、端末10における通信制御部1060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における通信制御部1060の各機能構成を説明するにあたって、図4あるいは図5に示されている各構成要素のうち、通信制御部1060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。

[0062] 図8に示されている送受信部21は、図4あるいは図5に示されているC

P U 1 0 1からの命令、及びネットワーク1/F 1 1 1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。

[0063] 起動部22は、図4あるいは図5に示されているC P U 1 0 1からの命令によって実現され、装置制御部1050の操作入力受付部12がユーザによるアプリの選択を受け付けた場合に、操作入力受付部12の起動要求に基づいて通信制御部1060（通話アプリ）の動作を起動する。

[0064] 表示制御部24は、図4あるいは図5に示されているC P U 1 0 1からの命令、及びディスプレイ1/F 1 1 7によって実現され、画面のデータをディスプレイ120に送信するための制御を行う。

[0065] 機能実行部25は、図4あるいは図5に示されているC P U 1 0 1からの命令、及びカメラ112、マイク114、又はスピーカ115等によって実現され、画像又は音等による通信を実現するための制御を行う。

[0066] 記憶・読出部29は、図4あるいは図5に示されているC P U 1 0 1からの命令及びS S D 1 0 5によって実行され、又はC P U 1 0 1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読み出す処理を行う。

[0067] <管理システムの機能構成>

管理システム50は、送受信部51、認証部52、起動制御部55、及び記憶・読出部59を有している。これら各部は、図6に示されている各構成要素のいずれかが、H D 2 0 4からR A M 2 0 3上に展開された管理システム50用のプログラムに従ったC P U 2 0 1からの命令によって動作することで実現される機能又は手段である。また、管理システム50は、図6に示されているH D 2 0 4により構築される記憶部5000を有している。この記憶部5000には、以下に示すような各テーブルによって構成されているD B（5001，5003，5004，5006，5007）が構築される。

[0068] （端末認証管理テーブル）

図9は、端末認証管理テーブルを示す概念図である。記憶部5000には、図9に示されているような端末認証管理テーブルによって構成されている端末認証管理DB5001が構築されている。この端末認証管理テーブルでは、管理システム50によって管理される全ての端末10の各端末IDに対して、認証用のパスワード、及び、クライアント証明書認証の許否を示す情報が関連付けられて管理される。例えば、図9に示されている端末認証管理テーブルにおいて、端末IDが「01aa」である端末10aaは、パスワード認証を利用可能であり、パスワード認証用のパスワードは「aaaa」であることが示されている。また、端末認証管理テーブルにおいて、端末IDが「01ab」である端末10abは、クライアント証明書認証を利用可能であることが示されている。更に、端末認証管理テーブルにおいて、端末IDが「01ac」である端末10acは、パスワード認証、及びクライアント証明書認証を利用可能であり、パスワード認証用のパスワードは「cccc」であることが示されている。なお、端末10毎に利用可能な認証方式を限定することにより、端末10毎に、利用可能なアプリ全体に対して、利用可能な認証方式を限定することができる。なお、本実施形態において、端末IDは、通信先の端末10を特定可能な情報であればよく、端末10固有の情報以外に端末10に固有ではない情報であってもよい。例えば端末10を利用するユーザを識別する情報であってもよいし、端末10が読み込み可能な記録媒体に記憶された識別情報であってもよい。

[0069] （アプリ利用管理テーブル）

図10は、アプリ利用管理テーブルを示す概念図である。記憶部5000には、図10に示されているようなアプリ利用管理テーブルによって構成されているアプリ利用管理DB5003が構築されている。このアプリ利用管理テーブルでは、端末10を識別するための端末ID及びテレビ会議用のアプリのそれぞれを識別するためのアプリID毎に、アプリの利用可否を示す利用可否情報を関連付けて管理している。なお、利用可否情報「On」は利用可能である旨を示し、利用可否情報「Off」は利用可能でない旨を示す

。

[0070] また、アプリ利用管理テーブルでは、アプリを利用可能である場合に、その条件を追加して管理することができる。例えば、図10に示されているアプリ利用管理テーブルにおいて、端末IDが「01aa」である端末10aaでは、アプリIDが「a001」で識別される通話アプリ、及び、アプリIDが「a002」で識別される残高照会アプリを利用可能であり、アプリIDが「a003」で識別される遠隔医療アプリを利用可能でない旨が示されている。この場合、通話アプリの利用可能期間は、「2014年1月1日」から「2014年9月30日」までである。

[0071] (アプリURL管理テーブル)

図11は、アプリURL管理テーブルを示す概念図である。記憶部5000には、図11に示されているようなアプリURL管理テーブルによって構成されているアプリURL管理DB5004が構築されている。このアプリURL管理テーブルでは、複数のアプリIDのそれぞれに、これらのアプリのアイコンデータの通信ネットワーク2におけるURL情報及びこれらのアプリの通信ネットワーク2におけるURL情報を関連付けて管理している。

[0072] (アプリ認可管理テーブル)

図12は、アプリ認可管理テーブルを示す概念図である。記憶部5000には、図12に示されているようなアプリ認可管理テーブルによって構成されているアプリ認可管理DB5006が構築されている。このアプリ認可管理テーブルでは、各アプリを識別するためのアプリID毎に、このアプリの起動要求元の認証方法として有効な認証方式を関連付けて管理している。これにより、管理システム50は、端末10から所望のアプリの起動要求を受け付けたときに、所望のアプリにおいて有効な認証方式で端末10が認証されていることを条件として、アプリへのアクセスを認可することが可能となる。なお、図12に示すアプリ認可管理テーブルでは、アプリID「a001」で識別される通話アプリは、起動要求元がパスワード認証またはクライアント証明書認証により認証されている場合には、アプリへのアクセスが認

可されることが示されている。また、アプリ認可管理テーブルでは、アプリ I D「a 0 0 3」で識別される遠隔医療アプリは、起動要求元がクライアント証明書認証により認証されている場合には、アプリへのアクセスが認可されることが示されている。

[0073] (アクセストークン管理テーブル)

図 1 3 は、アクセストークン管理テーブルを示す概念図である。記憶部 5 0 0 0 には、に示されているようなアクセストークン管理テーブルによって構成されているアクセストークン管理 D B 5 0 0 7 が構築されている。このアクセストークン管理テーブルでは、端末 1 0 の端末 I D、及び、テレビ会議用のアプリのそれぞれを識別するためのアプリ I D 毎に、アプリへのアクセスが認可されたことを示す認可情報としてのアクセストークンを関連付けて管理している。例えば、図 1 3 に示すアクセストークン管理テーブルでは、端末 I D「0 1 a a」で識別される端末 1 0 a a が、アプリ I D「a 0 0 1」で識別される通話アプリへのアクセスが認可されたときに、認可情報としてアクセストークン「a b c d e f g」が発行されることが示されている。

[0074] (管理システムの各機能構成)

次に、通信管理システム 5 0 の各機能構成について詳細に説明する。なお、以下では、通信管理システム 5 0 の各機能構成を説明するにあたって、図 6 に示されている各構成要素のうち、通信管理システム 5 0 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。

[0075] 送受信部 5 1 は、図 6 に示されている C P U 2 0 1 からの命令、及び図 6 に示されているネットワーク 1 / F 2 0 9 によって実行され、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。

[0076] 認証部 5 2 は、図 6 に示されている C P U 2 0 1 からの命令によって実現され、送受信部 5 1 で受信された端末 I D 及びパスワードを検索キーとして、端末認証管理テーブル（図 9 参照）を検索し、この端末認証管理テーブル

に同一の端末ＩＤ及びパスワードが管理されているかを判断することによって端末の認証を行う。

[0077] 起動制御部５５は、図６に示されているＣＰＵ２０１からの命令によって実現され、起動要求にかかるアプリの起動の可否を判断して、アプリの起動を制御する。

[0078] 記憶・読出部５９は、図６に示されているＣＰＵ２０１からの命令及び図６に示すＨＤＤ２０５によって実行され、又はＣＰＵ２０１からの命令によって実現され、記憶部５０００に各種データを記憶したり、記憶部５０００に記憶された各種データを抽出する処理を行う。

[0079] <アプリサーバの機能構成>

アプリサーバ８０は、送受信部８１、及び記憶・読出部８９を有している。これら各部は、図６に示されている各構成要素のいずれかが、ＨＤ２０４からＲＡＭ２０３上に展開されたアプリサーバ８０用のプログラムに従ったＣＰＵ２０１からの命令によって動作することで実現される機能又は手段である。また、アプリサーバ８０は、図６に示されているＨＤ２０４により構築される記憶部８０００を有している。

[0080] (アプリホスティングＤＢ)

記憶部８０００には、アプリホスティングＤＢ８００１が構築されている。アプリホスティングＤＢは、アプリサーバ８０にアップロードされたアプリを記憶して管理する。

[0081] 送受信部８１は、図６に示されているＣＰＵ２０１からの命令、及び図６に示されているネットワーク１／Ｆ２０９によって実行され、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。

[0082] 記憶・読出部８９は、図６に示されているＣＰＵ２０１からの命令及び図６に示すＨＤＤ２０５によって実行され、又はＣＰＵ２０１からの命令によって実現され、記憶部８０００に各種アプリを記憶したり、記憶部８０００に記憶された各種アプリを抽出する処理を行う。

[0083] <<実施形態の処理または動作>>

続いて、図14を用いて本実施形態の処理または動作の概要について説明する。図14は、通信システム1における各種情報の送受信の状態を示した概念図である。管理システム50（アクセス制御装置の一例）は、端末10からの要求に基づいて、アプリの起動を制御（通信端末からアプリケーションへのアクセスの制御の一例）する。管理システム50のアプリ認可管理DB5006（認証方式管理手段の一例）は、アプリを識別するためのアプリID毎に、このアプリの起動要求元（アクセス要求元の一例）を認証するために有効な認証方式（認証情報の一例）を関連付けて管理する。管理システム50の認証部52（認証手段の一例）は、端末10からのログイン要求に基づいて、この端末10において利用可能な認証方式により、ログイン要求元である端末10を認証する。管理システム50の送受信部51（アクセス要求受付手段の一例）は、端末10から、所望のアプリの起動の要求（所望のアプリケーションへのアクセスを伴う要求の一例）を受け付ける。アプリ認可管理DB5006において、上記の所望のアプリのアプリIDに関連付けられて、上記の端末10の認証に用いられた認証方式が管理されていない場合には、起動制御部55（アクセス制御手段の一例）は、上記の所望のアプリにアクセスさせないように制御する。一方、アプリ認可管理DB5006において、上記の所望のアプリのアプリIDに関連付けられて、上記の端末10の認証に用いられた認証方式が含まれている場合には、起動制御部55は、端末10を上記の所望のアプリのURIを端末10へ通知することにより、端末10から所望のアプリへアクセス可能となるように制御する。これにより、管理システム50は、各端末10を任意の認証方式により認証していた場合でも、この認証方式が、アプリの起動要求元を認証するための有効な認証方式でない場合には、アプリへアクセスさせないようにすることが可能となるので、アプリ側が期待する安全性を担保しやすくなる。

[0084] 管理システム50のアプリ利用管理DB5003（アプリケーション管理手段の一例）は、アプリの起動要求元（アクセス要求元の一例）である端末

１０の端末ＩＤ毎に、この端末１０において利用可能なアプリのアプリＩＤ（アプリケーション情報の一例）を関連付けて管理する。起動制御部５５は、アプリ利用管理ＤＢ５００３において、所望のアプリの起動の要求元である端末１０の端末ＩＤに関連付けられて、所望のアプリを示すアプリＩＤが管理されていない場合には、所望のアプリが起動しないように制御する。一方、アプリ利用管理ＤＢ５００３において、所望のアプリの起動の要求元である端末１０の端末ＩＤに関連付けられて、所望のアプリを示すアプリＩＤが管理されている場合には、所望のアプリの起動を制御する。この場合、アプリの利用の可否および認証方式の有効性の両方に基づいて、アプリへのアクセスを制御できるようになるので、安全性が向上する。

[0085] アプリ利用管理ＤＢ５００３は、アプリの起動要求元である端末１０の端末ＩＤ及びアプリＩＤ毎に、アプリを利用可能な期間（期間情報の一例）を関連付けて管理する。これにより、端末１０において利用可能なアプリ毎に、利用可能な期間を設定することが可能となる。

[0086] 通信システム１のアプリサーバ８０におけるアプリホスティングＤＢ８００１（記憶手段の一例）は、端末１０上で動作するアプリを記憶する。管理システム５０の起動制御部５５は、アプリホスティングＤＢ８００１に記憶されたアプリにアクセスするためのＵＲＬ（アクセス情報の一例）を端末１０へ通知することにより、端末１０におけるアプリの起動を制御することができる。

[0087] 続いて、本実施形態の処理または動作について、詳細に説明する。まず、図１５を用いて、端末１０において通信を開始する準備段階の処理について説明する。図１５は、通信を開始する準備段階の処理を示したシーケンス図である。ユーザが、図３に示されている電源スイッチ１０９をＯＮにすると、図８に示されている操作入力受付部１２が電源ＯＮを受け付けて、端末１０を起動させる（ステップＳ１）。そして、送受信部１１は、上記電源ＯＮの受け付けを契機とし、端末１０において利用可能な認証方式により、通信ネットワーク２を介して管理システム５０に、ログイン要求を行う（ステッ

プS 2)。これにより、管理システム50の送受信部51は、ログイン要求を受け付ける。なお、ログイン要求はログイン要求元の端末10のユーザによる指示入力を契機としてもよい。

[0088] このログイン要求には、要求元としての自端末である端末10を識別するための端末ID及び端末10において利用可能な認証方式に応じて、ログイン要求元を認証するための認証情報が含まれている。なお、認証情報としては、パスワードあるいはクライアント証明書情報などが挙げられる。これら端末ID及び認証情報は、記憶・読出部19を介して記憶部1000から読み出されて、送受信部11に送られたデータである。なお、これら端末ID及びパスワードは、ログイン要求元の端末10のユーザによって入力されてもよい。また、端末10から管理システム50へログイン要求情報が送信される際は、受信側である管理システム50は、送信側である端末10のIPアドレスを取得することができる。

[0089] 次に、管理システム50の認証部52は、送受信部51を介して受信したログイン要求情報に含まれている端末ID及び認証情報に基づいて、ログイン要求元である端末10の認証を行う（ステップS3）。この場合、端末10が、パスワード認証を要求してきた場合には、端末10から送信されたパスワードを検索キーとして、記憶部5000の端末認証管理テーブル（図9参照）を検索し、この端末認証管理テーブルに同一の端末ID及びパスワードが管理されているかを判断することによって端末認証を行う。また、端末10が、クライアント証明書認証を要求してきた場合には、端末10から送信された端末IDを検索キーとして、記憶部5000の端末認証管理テーブル（図9参照）を検索し、この端末10のクライアント証明書認証が許可されているか否かを参照する。クライアント証明書認証が許可されている場合には、端末10から送信されたクライアント証明書情報が正当なものであるか否かを判断することによって端末認証を行う。

[0090] 端末10の認証に成功した場合には、記憶・読出部59は、ログイン要求元の端末10の端末IDに関連付けて、認証に用いた認証方式に関連付けて

記憶部 5000 に記憶して管理させる（ステップ S4）。そして、管理システム 50 の送受信部 51 は、上記認証部 52 によって得られた認証結果が示された認証結果情報を、通信ネットワーク 2 を介して、ログイン要求元の端末 10 に送信する（ステップ S5）。これにより、ログイン要求元の端末 10 の送受信部 11 は、認証結果情報を受信する。続いて、認証部 52 によって正当な利用権限を有する端末であると判断された場合につき、以下説明する。

[0091] 続いて、図 16 を用いて、端末 10 において、起動要求するアプリの候補を示すアプリアイコンを表示させるまでの処理を説明する。図 16 は、アプリアイコンを表示させるまでの処理を示したシーケンス図である。

[0092] 端末 10 が、ステップ S1 からステップ S5 の処理を経て管理システム 50 にログインした後、端末 10 の送受信部 11 は、通信ネットワーク 2 を介して管理システム 50 に、利用可能アプリの候補のリストを要求する（ステップ S31）。これにより、管理システム 50 の送受信部 51 は、利用可能アプリの要求を受け付ける。この要求には、リスト要求元の端末 10 の端末 ID が含まれている。

[0093] 次に、管理システム 50 の記憶・読出部 59 は、上記ステップ S31 によって受信されたリスト要求元の端末 10 の端末 ID を検索キーとしてアプリ利用管理テーブル（図 10 を参照）を検索することにより、この端末 ID に対応するアプリ ID、および利用条件（有効期間開始日、および有効期間終了日）を読み出す（ステップ S32）。更に、記憶・読出部 59 は、上記ステップ S32 によって読み出されたアプリ ID のうち、利用条件が設定されている場合には、この処理の時点で有効期間内（有効期間開始日から有効終了日までの期間）を抽出し、抽出されたアプリ ID を検索キーとして、アプリ URL 管理テーブル（図 11 を参照）を検索することにより、このアプリ ID に対応するアイコンの URL 情報を読み出す（ステップ S33）。

[0094] 次に、送受信部 11 は、通信ネットワーク 2 を介してリスト要求元の端末 10 に、利用可能なアプリの候補のリストとして利用可能アプリ情報を送信

する（ステップS 3 4）。この利用可能アプリ情報には、上記ステップS 3 3で読み出されたアイコンのURL情報が含まれている。これにより、リスト要求元の端末1 0の送受信部1 1は、利用可能アプリ情報を受信する。

[0095] 次に、端末1 0の送受信部1 1は、上記ステップS 3 4によって受信したアイコンのURLで示される、アプリホスティングDB 8 0 0 1内のリソースにアクセスして、アイコンの画像情報の取得を要求する（ステップS 3 5）。これにより、アプリサーバ8 0の送受信部8 1は、アイコンの画像情報の取得要求を受け付ける。

[0096] 次に、アプリサーバ8 0の記憶・読出部8 9は、記憶部8 0 0 0のアプリホスティングDB 8 0 0 1から、上記ステップS 3 5によって要求されたアイコンの画像情報を読み出す（ステップS 3 6）。そして、送受信部8 1は、通信ネットワーク2を介して取得要求元の端末1 0に、アイコンの画像情報を送信する（ステップS 3 7）。これにより、要求元の端末1 0の送受信部1 1は、アイコンの画像情報を受信する。

[0097] 次に、表示制御部1 3は、ディスプレイ1 2 0上に、図1 8に示されているような「アプリリスト」画面1 4 0を表示させる（ステップS 3 8）。なお、図1 8は、アプリリストの画面例を示した図である。この画面1 4 0には、有効期間内のアプリのアイコンが表示される。ここでは、3つの各アプリID（a 0 0 1, a 0 0 2, a 0 0 3）で示される3つのアプリのアイコン（1 4 1, 1 4 2, 1 4 3）が表示される。

[0098] 続いて、図1 7を用いて、アプリのリストの中から所望のアプリを示すアプリアイコンの選択することにより、選択されたアプリの起動を要求する処理を説明する。なお、図1 7は、アプリの起動を要求する処理を示したシーケンス図である。

[0099] まず、ユーザの操作により、図1 8に示されている複数のアイコンのうち、所望のアイコンが選択されると、端末1 0の操作入力受付部1 2は、ユーザによるアプリアイコンの選択を受け付ける（ステップS 4 1）。続いて、端末1 0の送受信部1 1は、通信ネットワーク2を介して管理システム5 0

へ、選択されたアプリの起動の要求を示す起動要求情報を送信する（ステップS 4 2）。起動要求情報には、起動要求元の端末10の端末ID、及び、選択されたアプリのアプリIDが含まれている。

[0100] 管理システム50の送受信部51は、起動要求情報を受信することにより起動要求を受け付ける。起動要求を受け付けられると管理システム50の起動制御部55は、起動要求にかかるアプリの起動の可否を判断する（ステップS 4 3）。ステップS 4 3の処理について図19を用いて詳細に説明する。図19は、アプリの起動の可否を判断する処理を示したフロー図である。

[0101] まず、管理システム50の記憶・読出部59は、起動要求元の端末10の端末IDを検索キーとして、記憶部5000を検索することにより、起動要求元の端末10の利用した認証方式を抽出する（ステップS 4 3-1）。続いて、記憶・読出部59は、起動要求にかかるアプリのアプリIDを検索キーとして、アプリ認可管理テーブル（図12参照）を検索することにより、対応する認証方式を抽出する（ステップS 4 3-2）。

[0102] 続いて、起動制御部55は、ステップS 4 3-2で抽出された認証方式に、ステップS 4 3-1で抽出された認証方式が含まれているか否かを判断する（ステップS 4 3-3）。ステップS 4 3-2で抽出された認証方式に、ステップS 4 3-1で抽出された認証方式が含まれている場合（ステップS 4 3-3のYES）、起動制御部55は、アプリの起動要求を許可し、アプリの起動を制御する（ステップS 4 3-4）。

[0103] この場合、起動制御部55は、起動要求元の端末10の端末IDおよび起動要求にかかるアプリのアプリIDを検索キーとして、アクセストークン管理テーブル（図13参照）を検索することにより対応するアクセストークンを抽出する（ステップS 4 3-5）。続いて、起動制御部55は、起動要求に係るアプリのアプリIDを検索キーとして、アプリURL管理テーブル（図11を参照）を検索することにより、対応するアプリのURL情報を読み出す（ステップS 4 3-6）。

[0104] 一方、ステップS 4 3-2で抽出された認証方式に、ステップS 4 3-1

で抽出された認証方式が含まれていない場合（ステップS 4 3－3のNO）、起動制御部5 5は、アプリの起動要求を拒否する（ステップS 4 3－7）。この場合、送受信部5 1は、起動要求元の端末1 0へ、エラーメッセージを送信することにより処理を終了する（ステップS 4 3－8）。

[0105] 起動制御部5 5によって、アプリの起動が許可された場合について説明を続ける。まず、管理システム5 0の送受信部5 1は、起動要求元の端末1 0へ、アプリの起動の許可を示す起動可否情報を送信する（ステップS 4 4）。なお、ステップS 4 3－4において、起動が許可された場合には、起動要求に係るアプリにアクセスするための情報として、ステップS 4 3－5で抽出されたアクセストークンと、ステップS 4 3－6で抽出されたアプリのURL情報も送信されることになる。

[0106] 起動要求元の端末1 0の送受信部1 1が、起動可否情報を受信すると、表示制御部1 3は、起動可否を示す起動可否情報をディスプレイ1 2 0に表示させる。起動が許可された場合には、図8に示される装置制御部1 0 5 0の起動要求部1 4は、通信制御部1 0 6 0の起動部2 2に対して、起動を命令することで、通信制御部1 0 6 0が起動する（ステップS 4 5）。即ち、ユーザに選択されたアプリが起動することになる。なお、これよりも前の処理は、装置制御部1 0 5 0による処理であったが、これ以降は、通信制御部1 0 6 0による処理となる。

[0107] アプリが起動すると、送受信部2 1は、ステップS 4 4で送信されたアクセストークンをアプリサーバ8 0に送信するとともに、起動可否情報に含まれるアプリのURLにアクセスして、アプリのダウンロードを要求する（ステップS 4 6）。アプリのダウンロード要求がアプリサーバ8 0の送受信部8 1で受け付けられると、記憶読出部8 9はURLにより特定されるアプリを読み出す（ステップS 4 7）。読み出されたアプリは、送受信部8 1によってダウンロードの要求元の端末1 0へ送信される。これにより、起動要求元の端末1 0では、ブラウザ1 0 2 1上でアプリを動作させることが可能となる。

[0108] 〔第２の実施形態〕

続いて、第２の実施形態について、第１の実施形態と異なる点を説明する。第２の実施形態の通信システム１は、図２０に示されているように管理システム５０が、リスト作成部５６を有している点で第１の実施形態とは、異なる。なお、図２０は、管理システム５０の機能ブロック図である。リスト作成部５６は、端末１０において起動の要求が可能なアプリのリストを作成する。

[0109] 続いて、図２１を用いて、第２の実施形態の処理又は動作について詳細に説明する。図２１は、アプリのリストを作成する処理を示したフロー図である。第２の実施形態では、第１の実施形態におけるステップＳ３２の処理が、図２１に示された一連の処理に変更されている。

[0110] まず、管理システム５０の記憶・読出部５９は、リスト要求元の端末１０の端末ＩＤを検索キーとしてアプリ利用管理テーブル（図１０を参照）を検索することにより、この端末ＩＤに対応するアプリＩＤ、有効期間開始日、および有効期間終了日を読み出す（ステップＳ３２－１）。続いて、リスト作成部５６は、読み出されたアプリＩＤの中から、処理の時点で有効期間内ではないアプリＩＤを除くことによりリストに含めるアプリの候補を特定する（ステップＳ３２－２）。

[0111] 続いて、記憶・読出部５９は、リスト要求元の端末１０の端末ＩＤを検索キーとして、記憶部５０００を検索することにより、リスト要求元の端末１０の利用した認証方式を抽出する（ステップＳ３２－３）。更に、記憶・読出部５９は、ステップＳ３２－２で特定された各候補のアプリのアプリＩＤを検索キーとして、アプリ認可管理テーブル（図１２参照）を検索することにより、対応する認証方式を抽出する（ステップＳ３２－４）。

[0112] 続いて、リスト作成部５６は、ステップＳ３２－３で抽出された認証方式と、ステップＳ３２－４で抽出された認証方式とが一致するか否かを候補となるアプリ毎に判断する（ステップＳ３２－５）。

[0113] 認証方式が一致する場合（ステップＳ３２－５のＹＥＳ）、リスト作成部

５６は、候補のアプリを起動要求可能なアプリのリストに含める旨の判断をする（ステップＳ３２－６）。認証方式が一致しない場合（ステップＳ３２－５のＮＯ）、候補のアプリを起動要求可能なアプリのリストに含めない旨の判断をする（ステップＳ３２－７）。

[0114] 各アプリについてリストに含めるか否かの判断が完了すると、リスト作成部５６は、リストに含めると判断されたアプリＩＤにより、端末１０において起動の要求が可能なアプリのリストを作成する（ステップＳ３２－８）

リストが完成すると、記憶・読出部５９は、上記ステップＳ３２によって作成されたリストに含まれる各アプリＩＤを検索キーとして、アプリＵＲＬ管理テーブル（図１１を参照）を検索することにより、このアプリＩＤに対応するアイコンのＵＲＬ情報を読み出す（ステップＳ３３）。以後の処理は、第１の実施形態と同様であるので説明を省略する。

[0115] <<実施形態の補足>>

上記実施形態における中継装置３０、管理システム５０、プログラム提供システム９０、及びメンテナンスシステム１００は、単一のコンピュータによって構築されてもよいし、各部（機能又は手段）を分割して任意に割り当てられた複数のコンピュータによって構築されていてもよい。また、プログラム提供システム９０が単一のコンピュータによって構築されている場合には、プログラム提供システム９０によって送信されるプログラムは、複数のモジュールに分けて送信されるようにしてもよいし、分けずに送信されるようにしてもよい。更に、プログラム提供システム９０が複数のコンピュータによって構築されている場合には、複数のモジュールが分けられた状態で、各コンピュータから送信されるようにしてもよい。

[0116] また、上記各実施形態の端末用プログラム、中継装置用プログラム、又は伝送管理用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ＨＤ２０４、及びこのＨＤ２０４を備えたプログラム提供システム９０は、いずれもプログラム製品(Program Product)として、国内又は国外へ、上記端末用プログラム、中継装置用プログラム、及び

伝送管理用プログラムが利用者等に提供される場合に用いられる。

[0117] 更に、上記実施形態の各IDは、それぞれを一意に識別するために使われる言語、文字、記号、又は各種のしるし等の識別情報を示す。また、各IDは、上記言語、文字、記号、及び各種のしるしのうち、少なくとも2つが組み合わせられた識別情報であってもよい。

[0118] 例えば、アプリIDは、アプリ識別情報の一例であって、このアプリ識別情報には、アプリIDの他に、アプリの名称等も含まれる。また、端末IDは、端末識別情報の一例であって、この端末識別情報には、端末IDの他に、端末10の製造番号、端末10のユーザに割り当てられたユーザID等も含まれる。

[0119] また、図18に示されているアイコンは、文字、絵記号、又は、絵記号に文字もしくは記号が含まれていてもよい。

[0120] また、上記では、端末10の一例としてテレビ会議端末について説明したが、これに限るものではない。例えば、要求元端末と宛先端末のうちの一方又は両方が、IP(Internet Protocol)電話機、インターネット電話機、PC(Personal Computer)等であってもよい。更に、通信が可能な端末だけでなく、通信以外に様々なデータ通信が可能な情報処理端末として、スマートフォン、タブレット端末、ゲーム機、カーナビゲーション装置等の通信端末であってもよい。この場合、通信管理システム50は、通信管理システムとして各種処理を実行する。

[0121] 本国際出願は、2014年1月31日に出願した日本国特許出願2014-016922号に基づく優先権を主張するものであり、2014-016922号の全内容をここに本国際出願に援用する。

符号の説明

[0122] 1 通信システム

10 通信端末

11 送受信部（アクセス要求受付手段の一例）

12 操作入力受付部

- 1 3 表示制御部
- 1 4 起動制御部
- 1 9 記憶・読出部
- 2 1 送受信部
- 2 2 起動部
- 2 4 表示制御部
- 2 5 機能実行部
- 2 9 記憶・読出部
- 5 0 通信管理システム（アクセス制御装置の一例）
- 5 1 送受信部
- 5 2 認証部（認証手段の一例）
- 5 5 起動制御部（アクセス制御手段の一例）
- 5 6 リスト作成部
- 5 9 記憶・読出部
- 8 0 アプリサーバ
- 8 1 送受信部
- 8 9 記憶・読出部
- 1 0 0 0 記憶部
- 5 0 0 0 記憶部
- 5 0 0 1 端末認証管理DB
- 5 0 0 3 アプリ利用管理DB（アプリケーション管理手段の一例）
- 5 0 0 4 アプリURL管理DB
- 5 0 0 6 アプリ認可管理DB（認証方式管理手段の一例）
- 5 0 0 7 アクセストークン管理DB
- 8 0 0 0 記憶部
- 8 0 0 1 アプリホスティングDB（記憶手段の一例）

請求の範囲

[請求項1] 通信端末からアプリケーションへのアクセスを制御するアクセス制御装置であって、

前記アプリケーション毎に、前記アプリケーションへのアクセス要求元を認証するために有効な認証方式を示す認証情報を関連付けて管理する認証方式管理手段と、

通信端末からの要求に基づいて、前記通信端末において利用可能な認証方式により要求元を認証する認証手段と、

前記通信端末から、所望のアプリケーションへのアクセスを伴う要求を受け付けるアクセス要求受付手段と、

前記認証方式管理手段において、前記所望のアプリケーションに関連付けられて、前記認証に用いられた認証方式を示す認証情報が管理されていない場合には、前記通信端末を前記所望のアプリケーションにアクセスさせないように制御し、前記認証方式管理手段において、前記所望のアプリケーションに関連付けられて、前記認証に用いられた認証方式を示す認証情報が管理されている場合には、前記通信端末から前記所望のアプリケーションへのアクセスを制御するアクセス制御手段と、

を有することを特徴とするアクセス制御装置。

[請求項2] 前記アプリケーションへのアクセス要求元毎に、前記アクセス要求元において利用可能なアプリケーションを示すアプリケーション情報を関連付けて管理するアプリケーション管理手段を有しており、

前記アクセス制御手段は、前記アプリケーション管理手段において、前記所望のアプリケーションへのアクセス要求元に関連付けられて、前記所望のアプリケーションを示すアプリケーション情報が管理されていない場合には、前記通信端末を前記所望のアプリケーションにアクセスさせないように制御し、前記アクセス要求元に関連付けられて、前記所望のアプリケーションを示すアプリケーション情報が管理

されている場合には、前記通信端末から前記所望のアプリケーションへのアクセスを制御することを特徴とする請求項1に記載のアクセス制御装置。

[請求項3] 前記アプリケーション管理手段は、前記アクセス要求元および前記アプリケーション情報毎に、前記アプリケーションを利用可能な期間を示す期間情報を関連付けて管理することを特徴とする請求項2に記載のアクセス制御装置。

[請求項4] 請求項1乃至3のいずれか一項に記載のアクセス制御装置と、
前記アプリケーションを記憶した記憶手段を有するアプリケーションサーバと、
を有することを特徴とする通信システム。

[請求項5] 前記アクセス制御手段は、前記アプリケーションサーバの前記記憶手段に記憶された前記所望のアプリケーションにアクセスするためのアクセス情報を前記通信端末に通知することにより、前記所望のアプリケーションへのアクセスを制御することを特徴とする請求項4に記載の通信システム。

[請求項6] 前記アクセス要求元としての通信端末を更に有することを特徴とする請求項4又は5に記載の通信システム。

[請求項7] 通信端末からアプリケーションへのアクセスを制御するアクセス制御装置のプロセッサに、

前記通信端末からの要求に基づいて、前記通信端末において利用可能な認証方式により要求元を認証する認証ステップと、

前記通信端末から、前記所望のアプリケーションへのアクセスを伴う要求を受け付けるアクセス要求受付ステップと、

前記認証方式管理手段において、前記所望のアプリケーションに関連付けられて、前記認証に用いられた認証方式を示す認証情報が管理されていない場合には、前記通信端末を前記所望のアプリケーションにアクセスさせないように制御し、前記認証方式管理手段において、

前記所望のアプリケーションに関連付けられて、前記認証に用いられた認証方式を示す認証情報が管理されている場合には、前記通信端末から前記所望のアプリケーションへのアクセスを制御するアクセス制御ステップと、

を実行させることを特徴とするプログラム

[請求項8]

通信端末からアプリケーションへのアクセスを制御するアクセス制御装置のプロセッサに、

前記通信端末からの要求に基づいて、前記通信端末において利用可能な認証方式により要求元を認証する認証ステップと、

前記通信端末から、前記所望のアプリケーションへのアクセスを伴う要求を受け付けるアクセス要求受付ステップと、

前記認証方式管理手段において、前記所望のアプリケーションに関連付けられて、前記認証に用いられた認証方式を示す認証情報が管理されていない場合には、前記通信端末を前記所望のアプリケーションにアクセスさせないように制御し、前記認証方式管理手段において、前記所望のアプリケーションに関連付けられて、前記認証に用いられた認証方式を示す認証情報が管理されている場合には、前記通信端末から前記所望のアプリケーションへのアクセスを制御するアクセス制御ステップと、

を実行させることを特徴とするアクセス制御方法。