(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2017年11月23日(23.11.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/199353 A1

(51) 国際特許分類:
G06F 21/32 (2013.01) *H04M 11/00* (2006.01)
G06F 21/40 (2013.01) *H04Q 9/00* (2006.01)

(21) 国際出願番号： PCT/JP2016/064662

(22) 国際出願日： 2016年5月17日(17.05.2016)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: 株式会社オプティム (**OPTIM CORPORATION**) [JP/JP]; 〒8400047 佐賀県佐賀市与賀町４番１８号 Saga (JP).

(72) 発明者: 菅谷 俊二(**SUGAYA Shunji**); 〒1050022 東京都港区海岸１丁目２番２０号 汐留ビルディング２１Ｆ 株式会社オプティム内 Tokyo (JP).

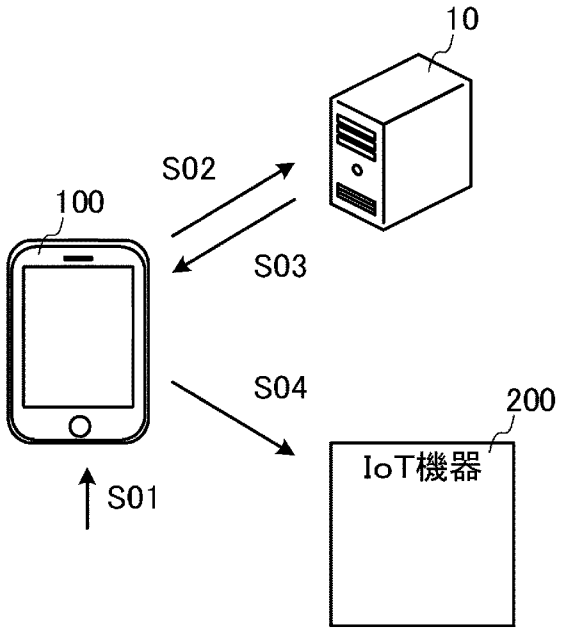
(74) 代理人: 小木 智彦(**KOGI Tomohiko**); 〒8800804 宮崎県宮崎市宮田町１１－２４ 黒木ビル１Ｆ Miyazaki (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO,

WO 2017/199353 A1

(54) **Title:** INFORMATION EQUIPMENT OPERATION SYSTEM, INFORMATION EQUIPMENT OPERATION METHOD AND PROGRAM

(54) 発明の名称： 情報機器操作システム、情報機器操作方法及びプログラム



200 IoT equipment

(57) **Abstract:** [Problem] The objective of the present invention is to provide an information equipment operation system and an information equipment operation method and program which have improved user-friendliness and security. [Solution] An information equipment operation system 1 comprising an information terminal 100 which is provided with a biometric authentication or a camera authentication and information equipment 200 which is connected to the information terminal 100 via a network detects that the biometric authentication or camera authentication has been done, and when

［続葉有］

NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告(条約第21条(3))

the system detects that the biometric authentication or camera authentication has been done, operates the information equipment 200 by using an application which is installed in the information terminal 100.

(57) 要約:【課題】利便性及びセキュリティを向上させた情報機器操作システム、情報機器操作方法及びプログラムを提供することを目的とする。【解決手段】生体認証又はカメラ認証を備えた情報端末１００と、当該情報端末１００とネットワークを介して接続された情報機器２００とからなる情報機器操作システム１は、生体認証又はカメラ認証がなされたことを検知し、生体認証又はカメラ認証がなされたことを検知した場合に、情報端末１００にインストールされたアプリケーションを利用して、情報機器２００を操作する。

明　細　書

発明の名称 ：

情報機器操作システム、情報機器操作方法及びプログラム

技術分野

[0001] 本発明は、生体認証又はカメラ認証を備えた情報端末と、この情報端末とネットワークを介して接続された情報機器とからなる情報機器操作システム、情報機器操作方法及びプログラムに関する。

背景技術

[0002] 近年、情報端末等の端末装置とインターネット等の公衆回線網を介して接続するＩｏＴ（Ｉｎｔｅｒｎｅｔ　ｏｆ　Ｔｈｉｎｇｓ）機器が存在する。このようなＩｏＴ機器において、情報端末により操作する際、ユーザ名やパスワード等による認証やＳＳＨを利用した認証が行われている。ユーザは、認証された情報端末を操作することにより、ＩｏＴ機器を操作することが可能となる。

[0003] このようなＩｏＴ機器の操作認証として、情報端末上で認証処理を実行し、認証がなされた場合には、ＩｏＴ機器を制御可能にする構成が開示されている（特許文献１参照）。

先行技術文献

特許文献

[0004] 特許文献1：特開２００５－３０３３７６号公報

発明の概要

発明が解決しようとする課題

[0005] しかしながら、特許文献１に記載の構成では、ＩｏＴ機器を操作するために、アプリケーション毎に公開鍵による認証を実行する必要があった。操作者は、操作するＩｏＴ機器の認証をその都度入力する必要があるため、利便性が低かった。また、情報端末の操作者が本来の操作者とは異なる不正な操作者である場合であっても、認証が実行されてしまい、不正な操作者がＩｏ

Ｔ機器を操作することが可能となってしまうおそれがあった。そのため、セキュリティが低かった。

[0006] 本発明は、利便性及びセキュリティを向上させた情報機器操作システム、情報機器操作方法及びプログラムを提供することを目的とする。

課題を解決するための手段

[0007] 本発明では、以下のような解決手段を提供する。

[0008] 第１の特徴に係る発明は、生体認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作システムであって、

前記生体認証がなされたことを検知する検知手段と、

前記生体認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作する操作手段と、

を備えることを特徴とする情報機器操作システムを提供する。

[0009] 第１の特徴に係る発明によれば、生体認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作システムは、前記生体認証がなされたことを検知し、前記生体認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作する。

[0010] 第１の特徴に係る発明は、情報機器操作システムのカテゴリであるが、方法及びプログラム等の他のカテゴリにおいても、そのカテゴリに応じた同様の作用・効果を発揮する。

[0011] 第２の特徴に係る発明は、カメラ認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作システムであって、

前記カメラ認証がなされたことを検知する検知手段と、

前記カメラ認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作する操作手

段と、

を備えることを特徴とする情報機器操作システムを提供する。

[0012] 第２の特徴に係る発明によれば、カメラ認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作システムは、前記カメラ認証がなされたことを検知し、前記カメラ認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作する。

[0013] 第２の特徴に係る発明は、情報機器操作システムのカテゴリであるが、方法及びプログラム等の他のカテゴリにおいても、そのカテゴリに応じた同様の作用・効果を発揮する。

[0014] 第３の特徴に係る発明は、前記アプリケーションは、標準化されたアプリケーションであり、

前記操作手段は、前記標準化されたアプリケーションを利用して、前記情報機器を操作する、

ことを特徴とする第１又は第２の特徴に係る発明である情報機器操作システムを提供する。

[0015] 第３の特徴に係る発明によれば、第１又は第２の特徴に係る発明である情報機器操作システムは、標準化されたアプリケーションであり、前記標準化されたアプリケーションを利用して、前記情報機器を操作する。

[0016] 第４の特徴に係る発明は、前記操作手段が、所定の人数の生体認証がなされたことを検知した場合に、前記アプリケーションを利用して、前記情報機器を操作する、

ことを特徴とする第１の特徴に係る発明である情報機器操作システムを提供する。

[0017] 第４の特徴に係る発明によれば、第１の特徴に係る発明である情報機器操作システムは、所定の人数の生体認証がなされたことを検知した場合に、前記アプリケーションを利用して、前記情報機器を操作する。

[0018] 第５の特徴に係る発明は、前記操作手段が、所定の人数のカメラ認証がな

されたことを検知した場合に、前記アプリケーションを利用して、前記情報機器を操作する、

ことを特徴とする第２の特徴に係る発明である情報機器操作システムを提供する。

[0019] 第５の特徴に係る発明によれば、第２の特徴に係る発明である情報機器操作システムは、所定の人数のカメラ認証がなされたことを検知した場合に、前記アプリケーションを利用して、前記情報機器を操作する。

[0020] 第６の特徴に係る発明は、生体認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作方法であって、

前記生体認証がなされたことを検知するステップと、

前記生体認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作するステップと、

を備えることを特徴とする情報機器操作方法を提供する。

[0021] 第７の特徴に係る発明は、カメラ認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作方法であって、

前記カメラ認証がなされたことを検知するステップと、

前記カメラ認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作するステップと、

を備えることを特徴とする情報機器操作方法を提供する。

[0022] 第８の特徴に係る発明は、生体認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作システムに、

前記生体認証がなされたことを検知するステップ、

前記生体認証がなされたことを検知した場合に、前記情報端末にインスト

ールされたアプリケーションを利用して、前記情報機器を操作するステップ、

を実行させることを特徴とするプログラムを提供する。

[0023] 第９の特徴に係る発明は、カメラ認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作システムに、

前記カメラ認証がなされたことを検知するステップ、

前記カメラ認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作するステップ、

を実行させることを特徴とするプログラムを提供する。

発明の効果

[0024] 本発明によれば、利便性及びセキュリティを向上させた情報機器操作システム、情報機器操作方法及びプログラムを提供することが可能となる。

図面の簡単な説明

[0025] [図1]図１は、情報機器操作システム１の概要を示す図である。

[図2]図２は、情報機器操作システム１の全体構成図である。

[図3]図３は、サーバ１０、情報端末１００、情報機器２００の機能ブロック図である。

[図4]図４は、情報端末１００、情報機器２００が実行する機器認証処理を示すフローチャートである。

[図5]図５は、サーバ１０、情報端末１００が実行するユーザ情報登録処理を示すフローチャートである。

[図6]図６は、サーバ１０、情報端末１００、情報機器２００が実行する機器操作処理を示すフローチャートである。

[図7]図７は、サーバ１０、情報端末１００、情報機器２００が実行する機器操作処理を示すフローチャートである。

[図8]図８は、サーバ１０、情報端末１００、情報機器２００が実行する機器

操作処理を示すフローチャートである。

[図9]図９は、サーバ１０、情報端末１００、情報機器２００が実行する機器操作処理を示すフローチャートである。

[図10]図１０は、情報端末１００が表示する認証内容決定画面の一例を示す図である。

発明を実施するための形態

[0026] 以下、本発明を実施するための最良の形態について図を参照しながら説明する。なお、これはあくまでも一例であって、本発明の技術的範囲はこれに限られるものではない。

[0027] ［情報機器操作システム１の概要］

本発明の概要について、図１に基づいて説明する。図１は、本発明の好適な実施形態である情報機器操作システム１の概要を説明するための図である。情報機器操作システム１は、サーバ１０、情報端末１００、情報機器２００から構成される。なお、情報端末１００、情報機器２００は１つに限らず複数であってもよい。また、後述する各処理は、サーバ１０、情報端末１００又は情報機器２００のいずれか又は複数の組み合わせにより実現されてもよい。また、情報機器操作システム１は、サーバを有さない構成であってもよい。この場合、後述する各処理は、情報端末１００又は情報機器２００のいずれか又は双方により実現されてもよい。

[0028] サーバ１０は、情報端末１００とデータ通信可能なサーバ装置である。

[0029] 情報端末１００は、サーバ１０と情報機器２００とデータ通信可能な端末装置である。情報端末１００は、例えば、携帯電話、携帯情報端末、タブレット端末、パーソナルコンピュータに加え、ネットブック端末、スレート端末、電子書籍端末、携帯型音楽プレーヤ等の電化製品や、スマートグラス、ヘッドマウントディスプレイ等のウェアラブル端末や、その他の物品である。

[0030] 情報機器２００は、情報端末１００とデータ通信可能なＩｏＴ機器である。情報機器２００は、例えば、ドローン、電化製品、エネルギー監視システ

ム等のインターネット等の公衆回線網と接続可能な機器又はシステムである。

[0031] はじめに、情報端末１００は、生体認証又はカメラ認証によるユーザ認証を受け付ける（ステップＳ０１）。生体認証とは、例えば、指紋認証、虹彩認証、静脈認証、声紋認証である。また、カメラ認証とは、例えば、情報端末１００が有するカメラ等の撮像装置により自身を撮像し、この撮像した撮像画像を画像解析することによる認証、ユーザによるジェスチャー操作を受け付ける認証である。なお、ユーザ認証は、上述した構成以外の構成を受け付けてもよい。

[0032] 情報端末１００は、受け付けたユーザ認証に関するデータである認証データを、サーバ１０に送信する（ステップＳ０２）。サーバ１０は、認証データを受信する。サーバ１０は、受信した認証データが、予め登録されたユーザの特徴と一致するか否かを判断し、認証結果を情報端末１００に送信する（ステップＳ０３）。

[0033] 情報端末１００は、認証結果を受信する。情報端末１００は、受信した認証結果が、一致していることを示していた場合、アプリケーションにより、情報機器２００の操作を実行可能にする（ステップＳ０４）。一方、情報端末１００は、受信した認証結果が、一致していないことを示していた場合、アプリケーションにより、情報機器２００の操作を実行不可能にする。

[0034] なお、一のアプリケーションに対して、一の情報機器２００が対応しており、この一のアプリケーションにより、一の情報機器２００を操作する構成であってもよいし、複数の情報機器２００に対応する標準化された標準アプリケーションにより、複数の情報機器２００を操作する構成であってもよい。例えば、一のアプリケーションに対して、一の情報機器２００が対応している場合、情報機器２００毎に上述した認証を実行し、各アプリケーションにより、対応する情報機器２００を操作する。標準アプリケーションとは、複数の情報機器２００を操作することを可能としたアプリケーションのことを意味する。標準アプリケーションに対して、複数の情報機器２００が対応

している場合、標準アプリケーションにおいて上述した認証を実行し、この標準アプリケーションにより、複数の情報機器２００を操作する。

[0035] 以上が、情報機器操作システム１の概要である。

[0036] ［情報機器操作システム１のシステム構成］

図２に基づいて、情報機器操作システム１のシステム構成について説明する。図２は、本発明の好適な実施形態である情報機器操作システム１のシステム構成を示す図である。情報機器操作システム１は、サーバ１０、情報端末１００、情報機器２００、公衆回線網（インターネット網や、第３、第４世代通信網等）５から構成される。なお、情報端末１００及び情報機器２００は、複数であってもよい。また、後述する各処理は、サーバ１０、情報端末１００又は情報機器２００のいずれか又は複数の組み合わせにより実現されてもよい。

[0037] サーバ１０は、後述の機能を備えた上述したサーバ装置である。

[0038] 情報端末１００は、後述の機能を備えた上述した端末装置である。

[0039] 情報機器２００は、後述の機能を備えた上述したＩｏＴ機器である。

[0040] ［各機能の説明］

図３に基づいて、情報機器操作システム１の機能について説明する。図３は、サーバ１０、情報端末１００、情報機器２００の機能ブロック図を示す図である。

[0041] サーバ１０は、制御部１１として、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）等を備え、通信部１２として、他の機器と通信可能にするためのデバイス、例えば、ＩＥＥＥ８０２．１１に準拠したＷｉＦｉ（Ｗｉｒｅｌｅｓｓ Ｆｉｄｅｌｉｔｙ）対応デバイスを備える。また、サーバ１０は、記憶部１３として、ハードディスクや半導体メモリ、記録媒体、メモリカード等によるデータのストレージ部を備える。

[0042] サーバ１０において、制御部１１が所定のプログラムを読み込むことによ

り、通信部１２と協働して、ユーザ情報受信モジュール２０、エラー通知送信モジュール２１、一致通知送信モジュール２２を実現する。また、サーバ１０において、制御部１１が所定のプログラムを読み込むことにより、記憶部１３と協働して、ユーザ情報記憶モジュール３０、情報比較モジュール３１を実現する。

[0043] 情報端末１００は、サーバ１０と同様に、制御部１１０として、ＣＰＵ、ＲＡＭ、ＲＯＭ等を備え、通信部１２０として、他の機器と通信可能にするためのデバイス等を備える。また、情報端末１００は、入出力部１４０として、制御部１１０で制御したデータや画像を出力表示する表示部や、ユーザからの入力を受け付けるタッチパネルやキーボード、マウス等の入力部や、レンズや撮像素子等の撮像デバイスや、ユーザの生体認証情報を読み取る読取デバイス等を備える。

[0044] 情報端末１００において、制御部１１０が所定のプログラムを読み込むことにより、通信部１２０と協働して、認証情報送信モジュール１５０、ユーザ情報送信モジュール１５１、エラー通知受信モジュール１５２、一致通知受信モジュール１５３、機器通信モジュール１５４を実現する。また、情報端末１００において、制御部１１０が所定のプログラムを読み込むことにより、入出力部１４０と協働して、アプリケーションモジュール１６０、生体認証情報入力受付モジュール１６１、カメラ認証情報入力受付モジュール１６２、認証画面表示モジュール１６３、エラー通知表示モジュール１６４を実現する。

[0045] 情報機器２００は、サーバ１０及び情報端末１００と同様に、制御部２１０として、ＣＰＵ、ＲＡＭ、ＲＯＭ等を備え、通信部２２０として、他の機器と通信可能にするためのデバイス等を備える。また、情報機器２００は、各ＩｏＴ機器が様々な機能を実行する様々なデバイス等を備える。例えば、情報機器２００がドローンである場合、飛行デバイスや、撮像デバイス等を備える。

[0046] 情報機器２００は、制御部２１０が所定のプログラムを読み込むことによ

り、通信部２２０と協働して、認証情報受信モジュール２５０、認証モジュール２５１、操作入力情報受信モジュール２５２を実現する。

[0047] ［機器認証処理］

図４に基づいて、情報機器操作システム１が実行する機器認証処理について説明する。図４は、情報端末１００、情報機器２００が実行する機器認証処理のフローチャートを示す図である。上述した各装置のモジュールが実行する処理について、本処理に併せて説明する。

[0048] アプリケーションモジュール１６０は、アプリケーションを起動し、情報機器２００を新たに接続する入力を受け付けたか否かを判断する（ステップＳ１０）。ステップＳ１０において、アプリケーションモジュール１６０が起動するアプリケーションは、一の情報機器２００に対応する一のアプリケーションであってもよいし、複数の情報機器２００に対応する標準化されたアプリケーションである標準アプリケーションであってもよい。新たに接続する入力とは、例えば、新規に接続する情報機器２００を検出する入力である。アプリケーションモジュール１６０は、起動したアプリケーションにより、今まで接続したことがない情報機器２００を検出する。

[0049] ステップＳ１０において、アプリケーションモジュール１６０は、情報機器２００を新たに接続する入力を受け付けていないと判断した場合（ステップＳ１０　ＮＯ）、本処理を終了する。一方、ステップＳ１０において、アプリケーションモジュール１６０は、情報機器２００を新たに接続する入力を受け付けたと判断した場合（ステップＳ１０　ＹＥＳ）、アプリケーションモジュール１６０は、認証情報の入力を受け付ける（ステップＳ１１）。認証情報とは、アプリケーションがインストールされた情報端末１００と、新たに検出された情報機器２００とを関連付ける入力である。具体的には、情報機器２００のＳＳＩＤ、パスワード等の入力を受け付ける。

[0050] 認証情報送信モジュール１５０は、受け付けた認証情報を情報機器２００に送信する（ステップＳ１２）。

[0051] 認証情報受信モジュール２５０は、認証情報を受信する。認証モジュール

２５１は、受信した認証情報と、自身の認証情報とが一致するか否かを判断する（ステップＳ１３）。ステップＳ１３において、認証モジュール２５１は、自身のＳＳＩＤやパスワード等が一致するか否かを判断する。ステップＳ１３において、認証モジュール２５１は、一致していないと判断した場合（ステップＳ１３　ＮＯ）、本処理を終了する。なお、このとき、情報機器２００は、認証情報が一致していない旨を示すエラー通知を情報端末１００に送信し、情報端末１００は、このエラー通知を表示する構成であってもよい。

[0052] 一方、ステップＳ１３において、認証モジュール２５１は、一致していると判断した場合（ステップＳ１３　ＹＥＳ）、認証モジュール２５１は、認証情報を送信した情報端末１００と自身と関連付ける（ステップＳ１４）。

[0053] なお、本処理は、認証情報として、後述する生体認証又はカメラ認証を用いる構成であってもよい。この場合、生体認証又はカメラ認証により取得した認証情報に基づいて、サーバ１０又は情報端末１００が認証させたか否かを判断し、情報端末１００と情報機器２００とを関連付ける構成としてもよい。

[0054] 以上が、機器認証処理である。

[0055] ［ユーザ情報登録処理］

次に、図５に基づいて、情報機器操作システム１が実行するユーザ情報登録処理について説明する。図５は、サーバ１０、情報端末１００が実行するユーザ情報登録処理のフローチャートを示す図である。上述した各装置のモジュールが実行する処理について、本処理に併せて説明する。

[0056] アプリケーションモジュール１６０は、ユーザ認証を実行するアプリケーションの起動入力を受け付けたか否かを判断する（ステップＳ２０）。ユーザ認証とは、生体認証やカメラ認証である。生体認証とは、例えば、指紋、虹彩、静脈、声紋に基づいた認証である。また、カメラ認証とは、撮像装置等により撮像した撮像画像を画像解析することにより特徴量を抽出し、この抽出した特徴量に基づいた認証である。例えば、ユーザの顔写真の特徴量、

ユーザの身体の動きによるジェスチャーである。

[0057] ステップＳ２０において、アプリケーションモジュール１６０は、入力を受け付けていないと判断した場合（ステップＳ２０　ＮＯ）、本処理を終了する。一方、ステップＳ２０において、アプリケーションモジュール１６０は、入力を受け付けたと判断した場合（ステップＳ２０　ＹＥＳ）、生体認証情報入力受付モジュール１６１は、生体認証の入力を受け付ける（ステップＳ２１）。ステップＳ２１において、生体認証情報入力受付モジュール１６１は、各種センサや撮像装置等により入力を受け付ける。

[0058] なお、ステップＳ２１において、生体認証情報入力受付モジュール１６１は、複数の生体認証を受け付けてもよいし、一の生体認証を受け付けてもよい。また、生体認証は、上述した構成以外の構成であってもよい。

[0059] 次に、カメラ認証情報入力受付モジュール１６２は、カメラ認証の入力を受け付ける（ステップＳ２２）。

[0060] なお、ステップＳ２２において、カメラ認証情報入力受付モジュール１６２は、複数のカメラ認証を受け付けてもよいし、一のカメラ認証を受け付けてもよい。また、カメラ認証は、上述した構成以外の構成であってもよい。

[0061] また、上述したステップＳ２１及びステップＳ２２の処理は、いずれか一方のみを実行する構成であってもよい。この場合、実行しない一方の処理は、省略されてもよい。また、ステップＳ２１及びステップＳ２２の処理は、順番が逆であってもよい。

[0062] アプリケーションモジュール１６０は、情報端末１００の識別子、電話番号、製造番号、ＩＰアドレス、ＭＡＣアドレス等の端末情報や、この情報端末１００のユーザの氏名、メールアドレス、電話番号、属性等の個人情報を取得する（ステップＳ２３）。属性とは、例えば、年齢、職業、住所である。ステップＳ２３において、アプリケーションモジュール１６０は、電話帳アプリケーションや設定アプリケーション等から端末情報や個人情報を取得する。なお、アプリケーションモジュール１６０は、上述した構成以外の構成により、端末情報及び個人情報を取得する構成であってもよい。

[0063] ユーザ情報送信モジュール１５１は、上述した生体認証情報、カメラ認証情報、端末情報及び個人情報を含むユーザ情報をサーバ１０に送信する（ステップＳ２４）。なお、ステップＳ２４において、ユーザ情報は、少なくとも、生体認証情報又はカメラ認証情報を含んでいればよく、その他の情報については適宜変更可能である。

[0064] ユーザ情報受信モジュール２０は、ユーザ情報を受信する。ユーザ情報記憶モジュール３０は、受信したユーザ情報を記憶する（ステップＳ２５）。ステップＳ２５において、ユーザ情報記憶モジュール３０は、生体認証情報、カメラ認証情報、端末情報及び個人情報を対応付けて記憶する。

[0065] 以上が、ユーザ情報登録処理である。

[0066] ［機器操作処理］

次に、図６及び図７に基づいて、情報機器操作システム１が実行する機器操作処理について説明する。図６及び図７は、サーバ１０、情報端末１００、情報機器２００が実行する機器操作処理のフローチャートを示す図である。上述した各装置のモジュールが実行する処理について、本処理に併せて説明する。

[0067] アプリケーションモジュール１６０は、情報機器２００を操作するアプリケーションの起動入力を受け付けたか否かを判断する（ステップＳ３０）。このアプリケーションは、一の情報機器２００に対応する一のアプリケーションであってもよいし、複数の情報機器２００に対応する標準化された標準アプリケーションであってもよい。ステップＳ３０において、アプリケーションモジュール１６０は、起動入力を受け付けていないと判断した場合（ステップＳ３０　ＮＯ）、本処理を終了する。

[0068] 一方、ステップＳ３０において、アプリケーションモジュール１６０は、起動入力を受け付けたと判断した場合（ステップＳ３０　ＹＥＳ）、認証画面表示モジュール１６３は、認証内容決定画面を表示する（ステップＳ３１）。

[0069] 図１０に基づいて、認証画面表示モジュール１６３が表示する認証内容決

定画面について説明する。図１０は、認証画面表示モジュール１６３が表示する認証内容決定画面の一例を示す図である。図１０において、認証画面表示モジュール１６３は、認証内容決定画面として、認証内容を決定する画面であることを示す通知と、生体認証入力選択領域３００、カメラ認証入力選択領域３１０、決定アイコン３２０、終了アイコン３３０を表示する。認証画面表示モジュール１６３は、生体認証入力選択領域３００又はカメラ認証入力選択領域３１０のいずれか又は双方への入力を受け付ける。認証画面表示モジュール１６３は、決定アイコン３２０への入力を受け付けることにより、入力された生体認証入力又はカメラ認証入力のいずれか又は双方を実行する。また、認証画面表示モジュール１６３は、終了アイコン３３０への入力を受け付けることにより、本処理を終了する。

[0070] 認証画面表示モジュール１６３は、生体認証情報又はカメラ認証情報の選択入力が行われたか否かを判断する（ステップＳ３２）。ステップＳ３２において、認証画面表示モジュール１６３は、生体認証入力選択領域３００又はカメラ認証入力選択領域３１０のいずれか又は双方への入力を受け付けるとともに、決定アイコン３２０の入力を受け付けたか否かを判断する。ステップＳ３２において、認証画面表示モジュール１６３は、選択入力が行われていないと判断した場合（ステップＳ３２　ＮＯ）、本処理を繰り返す。

[0071] ステップＳ３２において、認証画面表示モジュール１６３は、選択入力が行われたと判断した場合（ステップＳ３２　ＹＥＳ）、選択入力が行われた生体認証情報又はカメラ認証情報のいずれか又は双方のユーザ認証の入力を受け付ける（ステップＳ３３）。

[0072] ステップＳ３３において、認証画面表示モジュール１６３は、生体認証情報の入力を受け付けた場合、アプリケーションモジュール１６０は、センサ等により、生体認証を受け付ける。生体認証は、上述した構成である。

[0073] また、ステップＳ３３において、認証画面表示モジュール１６３は、カメラ認証情報の入力を受け付けた場合、アプリケーションモジュール１６０は、撮像装置等により、カメラ認証を受け付ける。カメラ認証は、上述した構

成である。

[0074] アプリケーションモジュール１６０は、上述した端末情報、個人情報を取得する（ステップＳ３４）。ステップＳ３４の処理は、上述したステップＳ２３の処理と同様である。

[0075] ユーザ情報送信モジュール１５１は、受け付けた生体認証情報又はカメラ認証情報、端末情報及び個人情報を含むユーザ情報をサーバ１０に送信する（ステップＳ３５）。ステップＳ３５の処理は、上述したステップＳ２４の処理と同様である。

[0076] ユーザ情報受信モジュール２０は、ユーザ情報を受信する。情報比較モジュール３１は、自身が記憶するユーザ情報と、今回受信したユーザ情報とを比較し、ユーザ情報が一致するか否かを判断する（ステップＳ３６）。ステップＳ３６において、情報比較モジュール３１は、ユーザ情報のうち、少なくとも生体認証情報又はカメラ認証情報が一致するか否かを判断する。

[0077] ステップＳ３６において、情報比較モジュール３１は、記憶したユーザ情報に含まれる生体認証情報と、受信したユーザ情報に含まれる生体認証情報とを比較し、同一内容において一致するか否かを判断する。同一内容とは、例えば、受信した生体認証が指紋である場合、記憶した生体認証情報における指紋を比較して、一致するか否かを判断する等である。

[0078] また、ステップＳ３６において、情報比較モジュール３１は、記憶したユーザ情報に含まれるカメラ認証情報と、受信したユーザ情報に含まれるカメラ認証情報とを比較し、同一内容において一致するか否かを判断する。同一内容とは、例えば、受信したカメラ認証情報がユーザの顔画像に関する情報である場合、記憶したカメラ認証情報における顔画像を比較して、特徴量が一致するか否かを判断する等である。また、例えば、受信したカメラ認証情報がユーザが行ったジェスチャーに関する情報である場合、記憶したカメラ認証情報におけるジェスチャーに関する情報を比較して、特徴量が一致するか否かを判断する。

[0079] なお、ステップＳ３６において、情報比較モジュール３１は、記憶したユ

ーザ情報に含まれる生体認証情報及びカメラ認証情報と、受信したユーザ情報に含まれる生体認証情報及びカメラ認証情報とを比較する構成であってもよい。この場合、両者が一致するか否かを判断する構成であればよい。また、情報比較モジュール３１は、生体認証情報又はカメラ認証情報に加え、端末情報や個人情報が一致するか否かを判断する構成であってもよい。例えば、情報比較モジュール３１は、全ての情報が一致するか否かを判断する等である。

[0080] ステップＳ３６において、情報比較モジュール３１は、ユーザ情報が一致していないと判断した場合（ステップＳ３６　ＮＯ）、エラー通知送信モジュール２１は、ユーザ情報が一致していないことを示すエラー通知を情報端末１００に送信する（ステップＳ３７）。

[0081] エラー通知受信モジュール１５２は、エラー通知を受信する。エラー通知表示モジュール１６４は、受信したエラー通知を表示し（ステップＳ３８）、アプリケーションモジュール１６０は、アプリケーションの起動を停止させ、アプリケーションを終了する（ステップＳ３９）。ステップＳ３８及びステップＳ３９の処理により、情報端末１００は、生体認証又はカメラ認証が一致していない場合、アプリケーションの動作を停止することにより、情報機器２００の操作を実行させないようにすることが可能となる。

[0082] 一方、ステップＳ３６において、情報比較モジュール３１は、ユーザ情報が一致していると判断した場合（ステップＳ３６　ＹＥＳ）、一致通知送信モジュール２２は、ユーザ情報が一致していることを示す一致通知を情報端末１００に送信する（ステップＳ４０）。

[0083] 一致通知受信モジュール１５３は、一致通知を受信する。機器通信モジュール１５４は、情報端末１００と情報機器２００との通信を開始する（ステップＳ４１）。

[0084] アプリケーションモジュール１６０は、情報機器２００への操作入力を受け付ける（ステップＳ４２）。

[0085] 機器通信モジュール１５４は、受け付けた操作入力を示す操作入力情報を

、情報機器２００に送信する（ステップＳ４３）。

[0086] 操作入力情報受信モジュール２５２は、操作入力情報を受信する。情報機器２００は、操作入力情報に基づいて、動作を実行する（ステップＳ４４）。

[0087] 以上が、機器操作処理である。

[0088] なお、上述した機器操作処理において、サーバ１０が実行する処理を、情報端末１００又は情報機器２００のいずれか又は双方により実行する構成としてもよい。すなわち、情報機器操作システム１は、情報端末１００及び情報機器２００から構成されてもよい。この場合、例えば、上述したサーバ１０によりユーザ情報の認証を、情報端末１００が実行する構成とすることも可能である。

[0089] このようにしたことにより、番号やＰＩＮコード認証の場合では、操作者を特定することができないのに対して、生体認証又はカメラ認証の場合では、操作者を特定することが容易となる。また、情報端末１００で行う生体認証又はカメラ認証によって操作者を認証するため、公衆回線網５を介して接続された情報機器２００を操作する場合に、アプリケーション毎にログインする必要性がなくなる。

[0090] ［変形例］

次に、上述した本実施形態における変形例について説明する。本変形例において、情報機器操作システム１は、サーバ１０、複数の情報端末１００、情報機器２００、公衆回線網５から構成される。すなわち、上述した実施形態との相違点は、情報端末１００が複数個存在している点である。なお、上述した実施形態と同様の構成については、同様の符号を付し、その詳細な説明は省略する。

[0091] ［機器操作処理］

本変形例における機器操作処理について説明する。なお、複数の情報端末１００の各々は、上述した機器認証処理及びユーザ情報登録処理を実行する。

[0092] 図８及び図９に基づいて、情報機器操作システム１が実行する機器操作処理について説明する。図８及び図９は、サーバ１０、情報端末１００、情報機器２００が実行する機器操作処理のフローチャートを示す図である。上述した各装置のモジュールが実行する処理について、本処理に併せて説明する。

[0093] 情報端末１００及びサーバ１０は、上述したステップＳ３０～ステップＳ３９の処理を実行する（ステップＳ５０～ステップＳ５９）。

[0094] 一方、ステップＳ５６において、情報比較モジュール３１は、ユーザ情報が一致していると判断した場合（ステップＳ５６　ＹＥＳ）、情報比較モジュール３１は、一致したと判断したユーザの数が所定の人数以上であるか否かを判断する（ステップＳ６０）。所定の人数とは、例えば、情報機器２００の使用者として予め登録された全員の人数、この登録された人数のうちの半数、この登録された人数のうちの複数人、予め設定した一のグループに属する全員の人数、この登録された一のグループに属する人数のうちの半数、この登録された人数のうちの複数人等である。ステップＳ６０において、情報比較モジュール３１は、所定の人数以上ではないと判断した場合（ステップＳ６０　ＮＯ）、上述したステップＳ５７の処理を実行する。

[0095] なお、所定の人数以外の構成として、例えば、情報端末１００の各使用者に対して異なる重みを予め付与しておき、この重みの合計値が所定の値以上であるか否かを判断する構成としてもよい。例えば、一のグループに属する使用者の地位や立場に応じて重み付けを行い、人数によらず、重みの合計値により判断することも可能となる。具体的には、一のグループに属する使用者Ｄには１０の重み、使用者Ｅには５の重み、使用者Ｆ，Ｇ，Ｈには２の重みを付与し、重みの合計値が５以上であるか否かを判断する構成とすることも可能となる。すなわち、使用者Ｄ又は使用者Ｅのみユーザ情報が一致した場合や、使用者Ｆ、使用者Ｇ及び使用者Ｈの３人のユーザ情報が一致した場合に、一致したと判断する。このようにすることにより、責任や地位に応じた人物が、情報機器２００の操作を実行することも可能となる。

[0096] 一方、ステップＳ６０において、情報比較モジュール３１は、所定の人数以上であると判断した場合（ステップＳ６０　ＹＥＳ）、一致通知送信モジュール２２は、ユーザ情報及び人数が一致したことを示す一致通知を、この情報機器２００の使用者が保有する情報端末１００に送信する（ステップＳ６１）。ステップＳ６１において、一致通知送信モジュール２２は、一致通知を複数の情報端末１００に送信する。

[0097] 情報端末１００及び情報機器２００は、上述したステップＳ４１～ステップＳ４４の処理を実行する（ステップＳ６２～ステップＳ６５）。

[0098] 以上が、変形例における機器操作処理である。

[0099] なお、上述した変形例において、ユーザ情報として、端末情報及び個人情報を含めたユーザ情報を判断しているが、端末情報及び個人情報をユーザ情報に含めなくともよい。この場合、生体認証又はカメラ認証を実行する情報端末１００は、情報機器２００において認証が実行された情報端末１００であればよい。また、上述した情報機器２００を操作するアプリケーションは、一の情報端末１００において、複数存在していてもよい。例えば、複数のユーザの各ユーザに対して、一のアプリケーションを設定し、この一のアプリケーションにより、上述した処理を実行する構成であればよい。すなわち、あるユーザＡが使用するアプリケーションと、別のユーザＢが使用するアプリケーションとは異なっていてもよい。この場合であっても、サーバ１０が所定の人数以上のユーザ情報が一致していることに基づいて、一致通知を送信する構成であればよい。

[0100] このようにしたことにより、番号やＰＩＮコード認証の場合では、操作者を特定することができないのに対して、生体認証又はカメラ認証の場合では、操作者を特定することが容易となる。また、情報端末１００で行う生体認証又はカメラ認証によって操作者を認証するため、公衆回線網５を介して接続された情報機器２００を操作する場合に、アプリケーション毎にログインする必要性がなくなる。

[0101] 上述した手段、機能は、コンピュータ（ＣＰＵ、情報処理装置、各種端末

を含む）が、所定のプログラムを読み込んで、実行することによって実現される。プログラムは、例えば、フレキシブルディスク、ＣＤ（ＣＤ－ＲＯＭなど）、ＤＶＤ（ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭなど）等のコンピュータ読取可能な記録媒体に記録された形態で提供される。この場合、コンピュータはその記録媒体からプログラムを読み取って内部記憶装置又は外部記憶装置に転送し記憶して実行する。また、そのプログラムを、例えば、磁気ディスク、光ディスク、光磁気ディスク等の記憶装置（記録媒体）に予め記録しておき、その記憶装置から通信回線を介してコンピュータに提供するようにしてもよい。

[0102] 以上、本発明の実施形態について説明したが、本発明は上述したこれらの実施形態に限るものではない。また、本発明の実施形態に記載された効果は、本発明から生じる最も好適な効果を列挙したに過ぎず、本発明による効果は、本発明の実施形態に記載されたものに限定されるものではない。

符号の説明

[0103] １　情報機器操作システム、１０　サーバ、１００　情報端末、２００　情報機器

請求の範囲

[請求項1] 生体認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作システムであって、

前記生体認証がなされたことを検知する検知手段と、

前記生体認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作する操作手段と、

を備えることを特徴とする情報機器操作システム。

[請求項2] カメラ認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作システムであって、

前記カメラ認証がなされたことを検知する検知手段と、

前記カメラ認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作する操作手段と、

を備えることを特徴とする情報機器操作システム。

[請求項3] 前記アプリケーションは、標準化されたアプリケーションであり、

前記操作手段は、前記標準化されたアプリケーションを利用して、前記情報機器を操作する、

ことを特徴とする請求項１又は２に記載の情報機器操作システム。

[請求項4] 前記操作手段は、所定の人数の生体認証がなされたことを検知した場合に、前記アプリケーションを利用して、前記情報機器を操作する、

ことを特徴とする請求項１に記載の情報機器操作システム。

[請求項5] 前記操作手段は、所定の人数のカメラ認証がなされたことを検知した場合に、前記アプリケーションを利用して、前記情報機器を操作する、

ことを特徴とする請求項２に記載の情報機器操作システム。

[請求項6] 生体認証を備えた情報端末と、当該情報端末とネットワークを介し

て接続された情報機器とからなる情報機器操作方法であって、

前記生体認証がなされたことを検知するステップと、

前記生体認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作するステップと、

を備えることを特徴とする情報機器操作方法。

[請求項7] カメラ認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作方法であって、

前記カメラ認証がなされたことを検知するステップと、

前記カメラ認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作するステップと、

を備えることを特徴とする情報機器操作方法。

[請求項8] 生体認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作システムに、

前記生体認証がなされたことを検知するステップ、

前記生体認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作するステップ、

を実行させることを特徴とするプログラム。

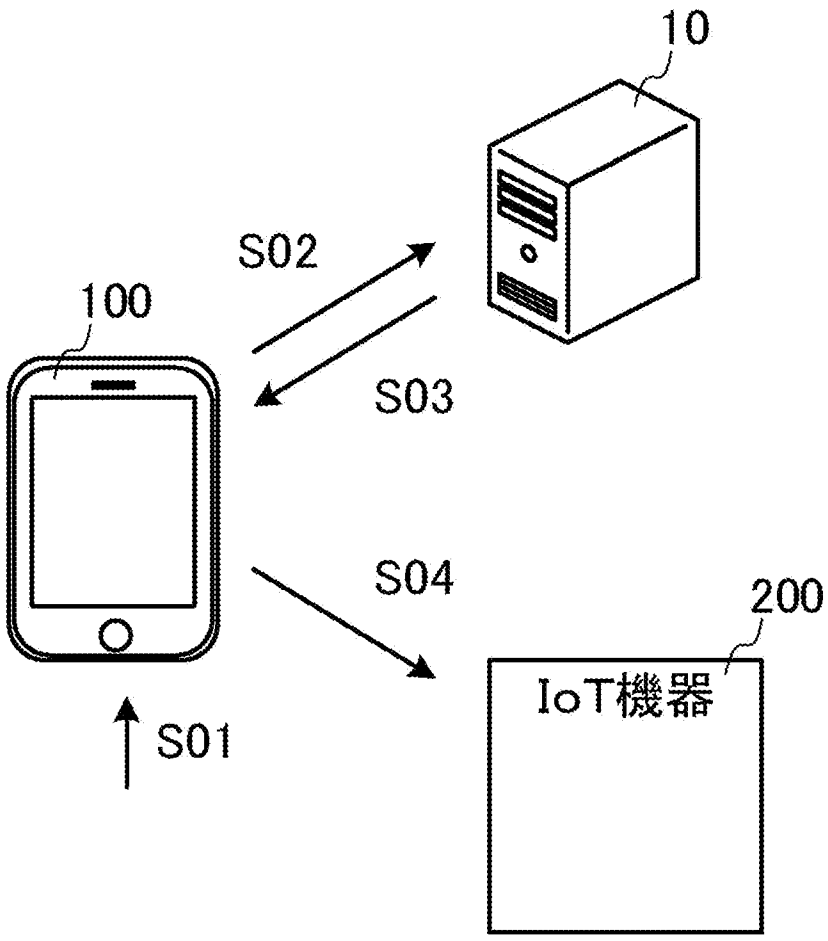
[請求項9] カメラ認証を備えた情報端末と、当該情報端末とネットワークを介して接続された情報機器とからなる情報機器操作システムに、

前記カメラ認証がなされたことを検知するステップ、

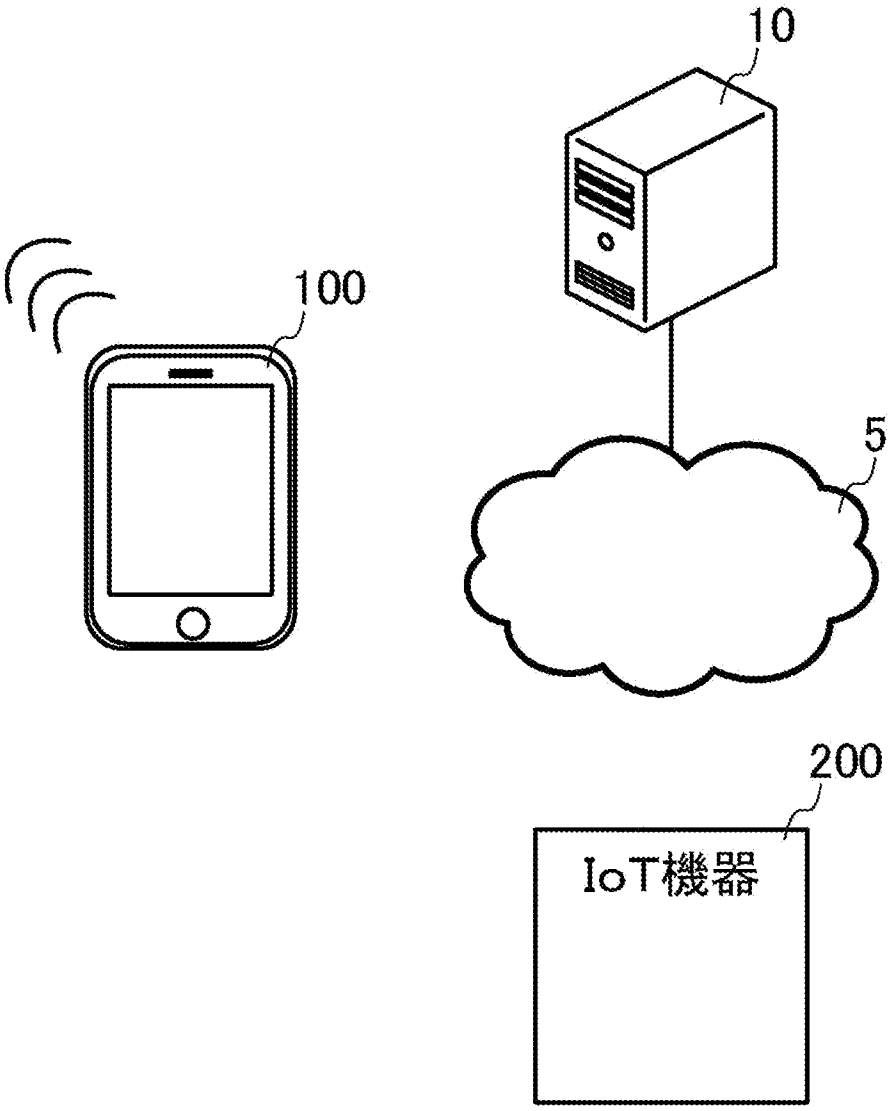
前記カメラ認証がなされたことを検知した場合に、前記情報端末にインストールされたアプリケーションを利用して、前記情報機器を操作するステップ、

を実行させることを特徴とするプログラム。

[図1]



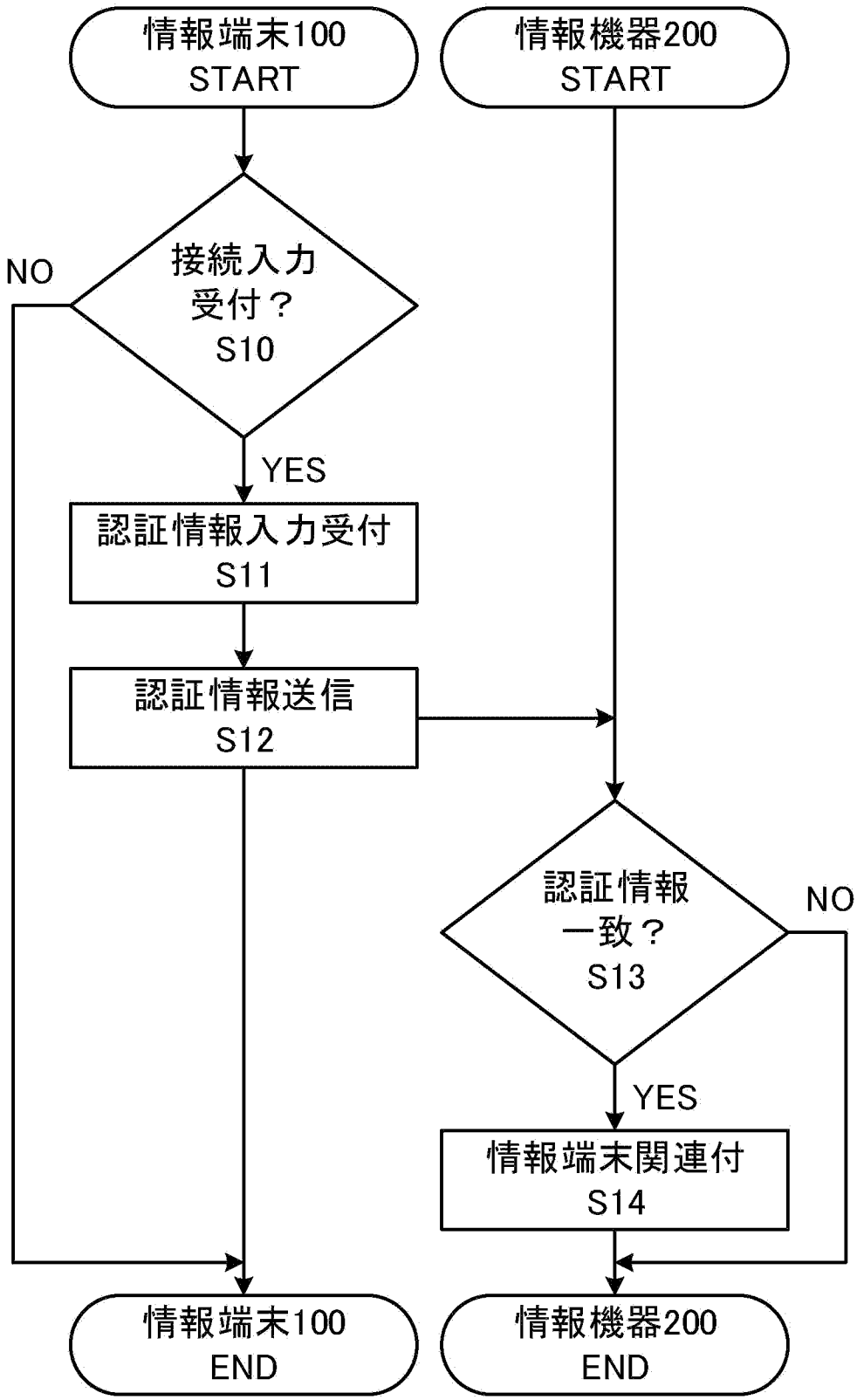
[図2]



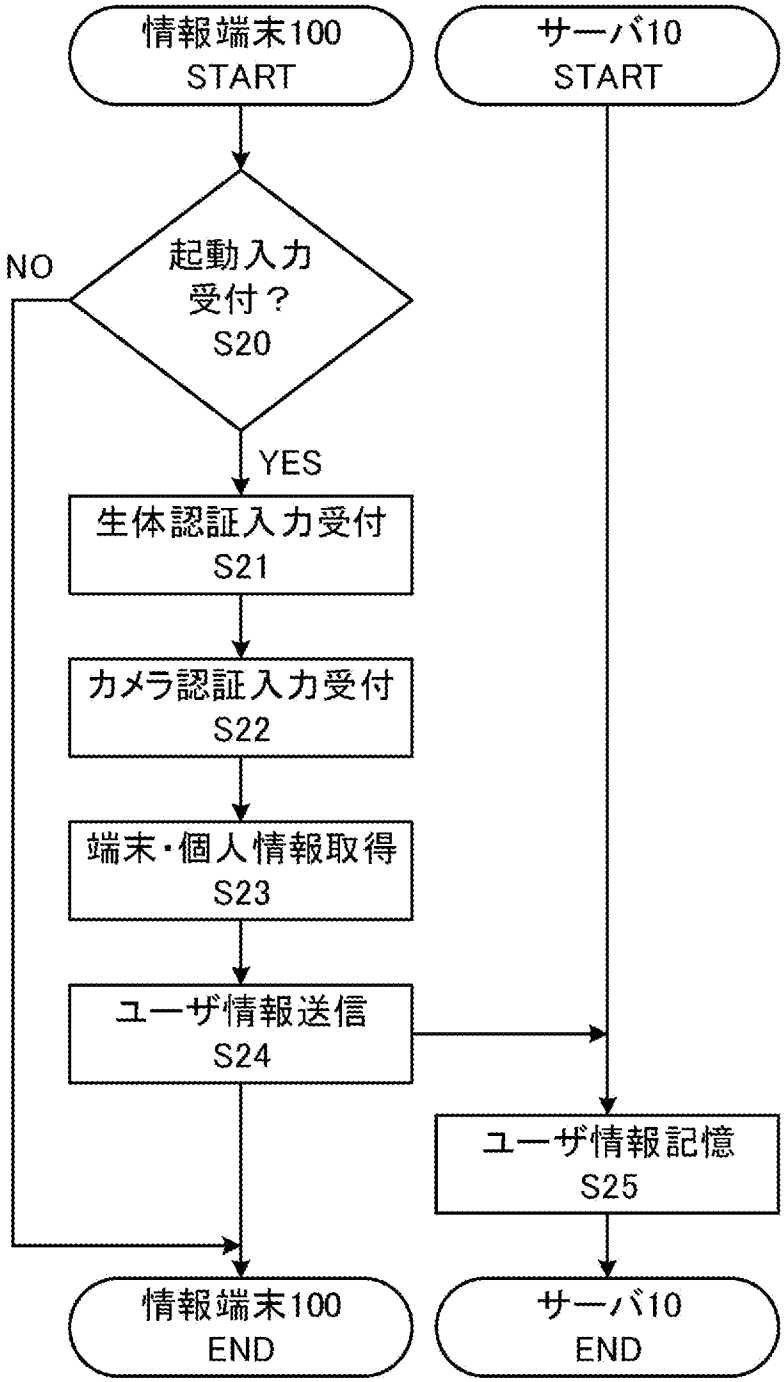
[図3]


情報端末100
制御部
110
通信部
120
認証情報送信
モジュール150
ユーザ情報送信
モジュール151
エラー通知受信
モジュール152
一致通知受信
モジュール153
機器通信
モジュール154
入出力部
140
アプリケーション
モジュール160
生体認証情報入力
受付モジュール161
カメラ認証情報入力
受付モジュール162
認証画面表示
モジュール163
エラー通知表示
モジュール164
サーバ10
制御部
11
通信部
12
ユーザ情報受信
モジュール20
エラー通知送信
モジュール21
一致通知送信
モジュール22
記憶部
13
ユーザ情報記憶
モジュール30
情報比較
モジュール31
情報機器200
制御部
210
通信部
220
認証情報受信
モジュール250
認証
モジュール251
操作入力情報受信
モジュール252

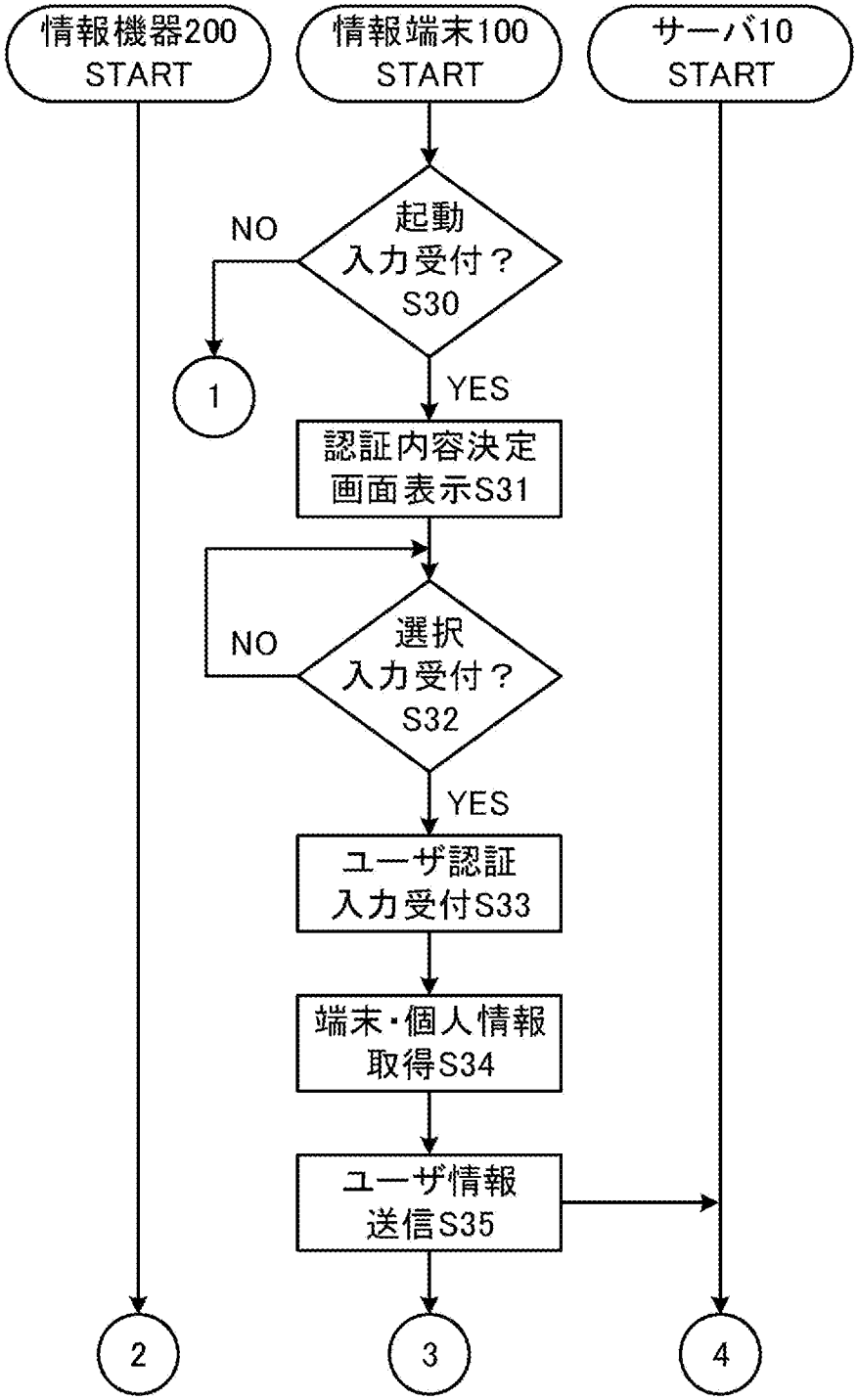
[図4]


情報端末100
START
情報機器200
START
接続入力
受付？
S10
NO
YES
認証情報入力受付
S11
認証情報送信
S12
認証情報
一致？
S13
NO
YES
情報端末関連付
S14
情報端末100
END
情報機器200
END

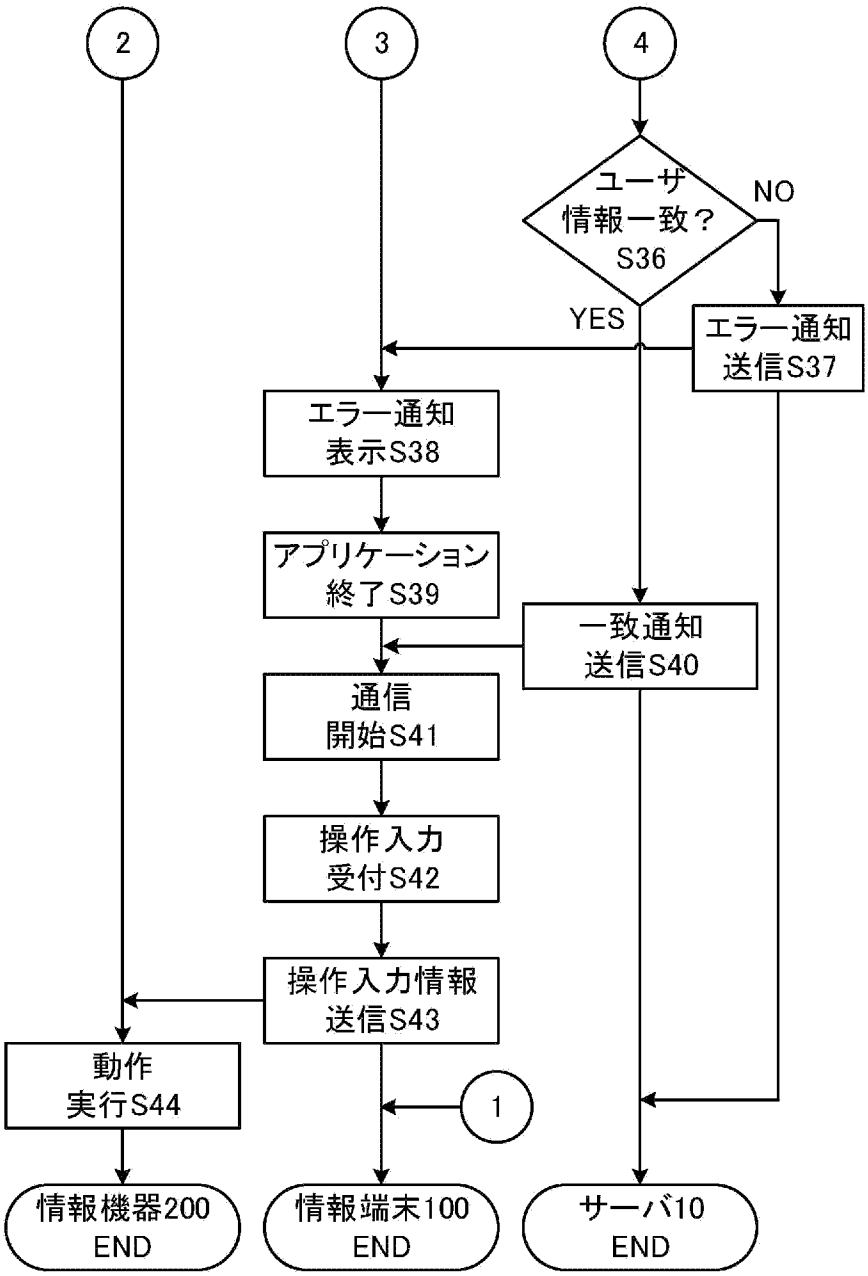
[図5]


情報端末100
START
サーバ10
START
起動入力
受付？
S20
NO
YES
生体認証入力受付
S21
カメラ認証入力受付
S22
端末・個人情報取得
S23
ユーザ情報送信
S24
ユーザ情報記憶
S25
情報端末100
END
サーバ10
END

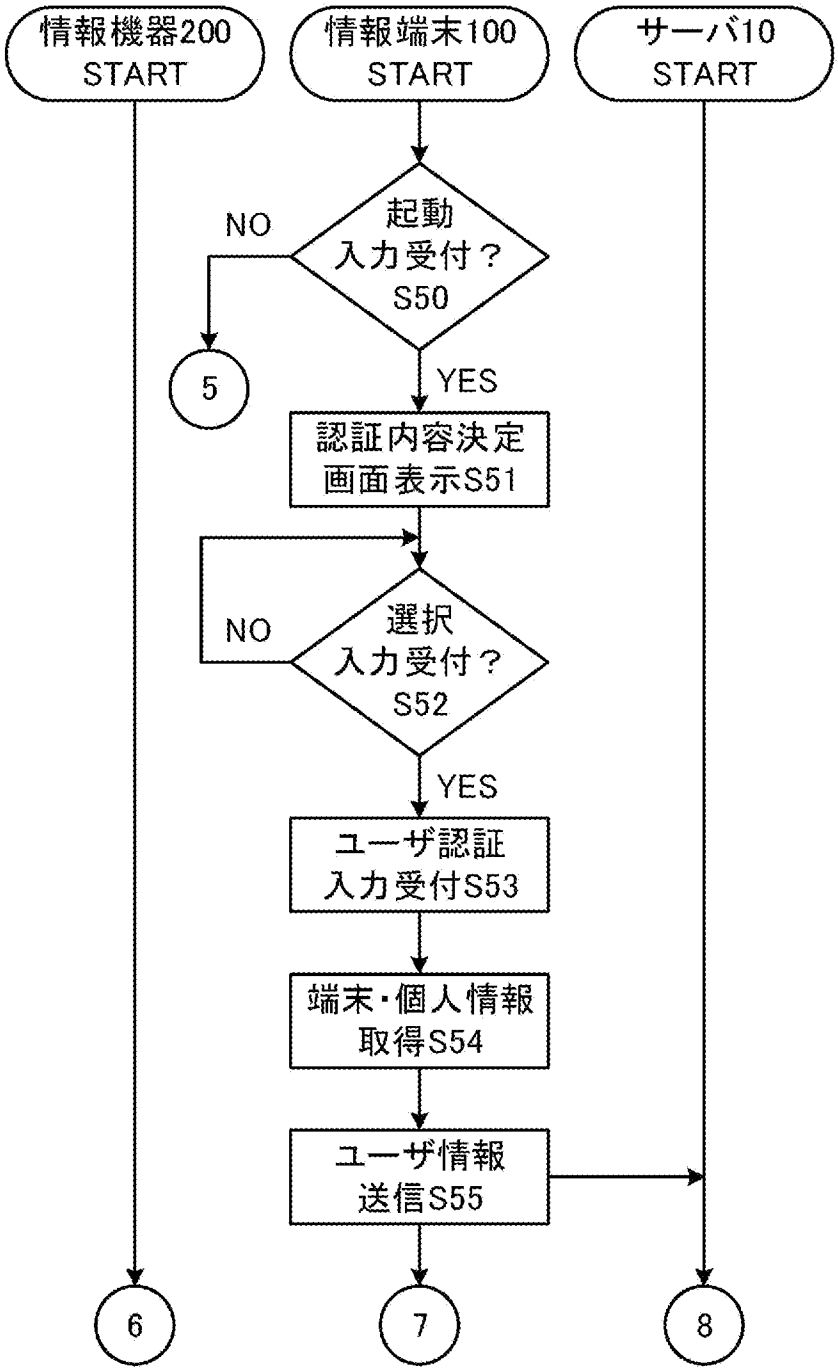
[図6]


情報機器200
START
情報端末100
START
サーバ10
START
起動
入力受付？
S30
NO
YES
1
認証内容決定
画面表示S31
選択
入力受付？
S32
NO
YES
ユーザ認証
入力受付S33
端末・個人情報
取得S34
ユーザ情報
送信S35
2
3
4

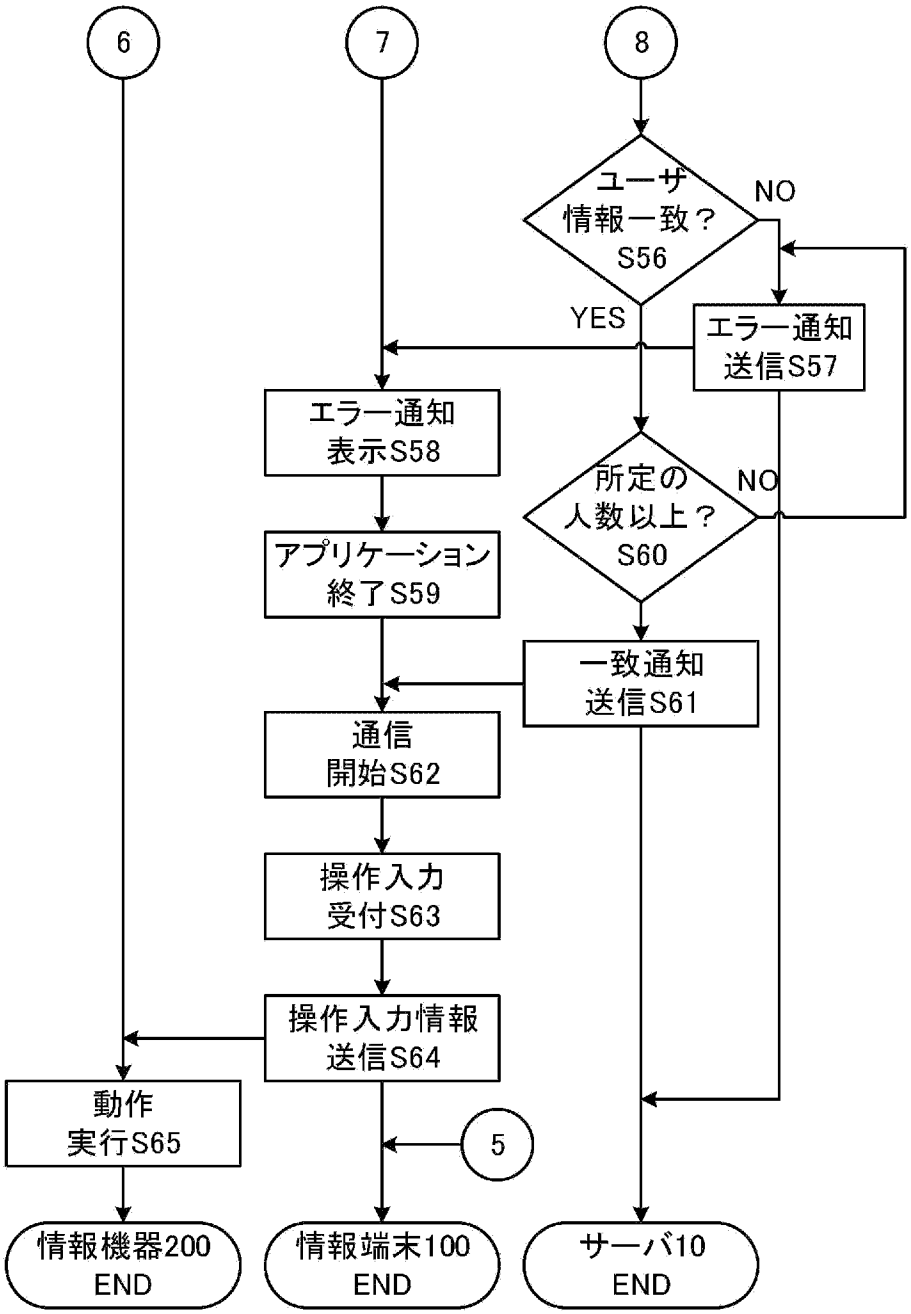
[図7]


2
3
4
ユーザ
情報一致？
S36
NO
YES
エラー通知
送信S37
エラー通知
表示S38
アプリケーション
終了S39
一致通知
送信S40
通信
開始S41
操作入力
受付S42
操作入力情報
送信S43
動作
実行S44
1
情報機器200
END
情報端末100
END
サーバ10
END

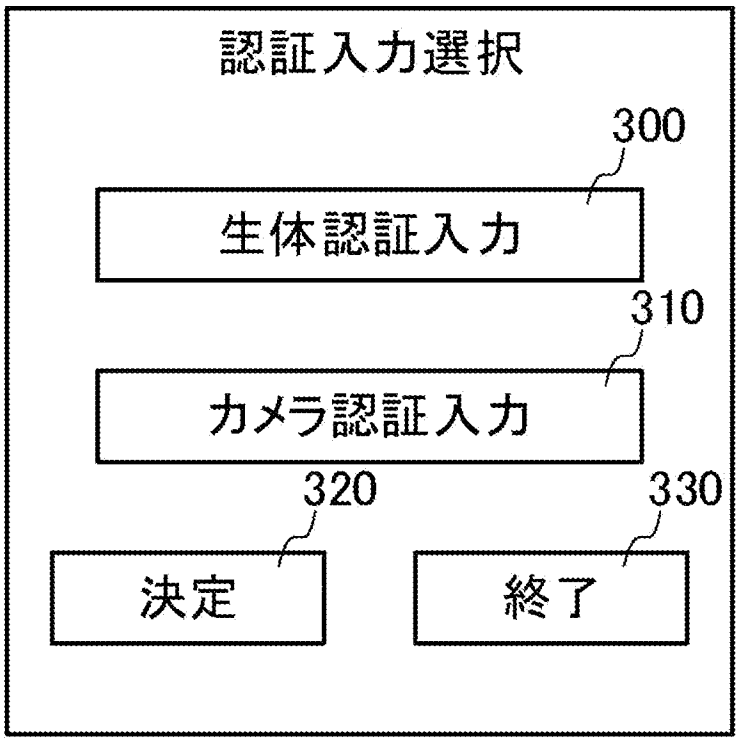
[図8]


情報機器200
START
情報端末100
START
サーバ10
START
起動
入力受付？
S50
NO
YES
5
認証内容決定
画面表示S51
選択
入力受付？
S52
NO
YES
ユーザ認証
入力受付S53
端末・個人情報
取得S54
ユーザ情報
送信S55
6
7
8

[図9]


6
7
8
ユーザ
情報一致？
S56
NO
YES
エラー通知
送信S57
エラー通知
表示S58
所定の
人数以上？
S60
NO
アプリケーション
終了S59
一致通知
送信S61
通信
開始S62
操作入力
受付S63
操作入力情報
送信S64
動作
実行S65
5
情報機器200
END
情報端末100
END
サーバ10
END

[図10]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/064662

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/32(2013.01)i, *G06F21/40*(2013.01)i, *H04M11/00*(2006.01)i, *H04Q9/00*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/32, G06F21/40, H04M11/00, H04Q9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO 2014/103308 A1 (Panasonic Corp.), 03 July 2014 (03.07.2014), paragraphs [0039] to [0040], [0056] to [0060], [0068] to [0073]; fig. 1 to 2, 4 & US 2015/0012863 A1 paragraphs [0053] to [0054], [0070] to [0074], [0082] to [0087]; fig. 1 to 2, 4	1-3,6-9 4-5
Y	JP 2015-36918 A (Fuji Xerox Co., Ltd.), 23 February 2015 (23.02.2015), abstract; paragraphs [0019] to [0020]; fig. 1, 4 to 5 & US 2015/0049923 A1 paragraphs [0026] to [0029]; fig. 1, 4A to 4D, 5E to 5H	4-5

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2016 (20.07.16)	02 August 2016 (02.08.16)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/064662

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-150551 A (Yokogawa Electric Corp.), 23 May 2003 (23.05.2003), abstract; paragraphs [0012] to [0013] (Family: none)	4-5
A	JP 2005-248542 A (Toshiba Corp.), 15 September 2005 (15.09.2005), paragraphs [0006] to [0007], [0022], [0037] to [0038], [0045]; fig. 5 (Family: none)	1-9
A	JP 2014-164359 A (NEC Networks & System Integration Corp.), 08 September 2014 (08.09.2014), paragraphs [0023] to [0027], [0046] to [0055]; fig. 1, 4 (Family: none)	1-9
A	JP 2010-74782 A (Optim Corp.), 02 April 2010 (02.04.2010), paragraphs [0028] to [0029], [0069]; fig. 1 to 2, 9B (Family: none)	1-9
A	JP 2008-199197 A (Sharp Corp.), 28 August 2008 (28.08.2008), paragraphs [0137] to [0149]; fig. 4, 13 (Family: none)	1-9
A	JP 2008-131081 A (Pioneer Corp.), 05 June 2008 (05.06.2008), paragraph [0068]; fig. 1 to 2 (Family: none)	1-9
A	JP 2012-161001 A (Toshiba Carrier Corp.), 23 August 2012 (23.08.2012), paragraphs [0016] to [0017]; fig. 1 to 2 (Family: none)	1-9
A	US 2015/0312041 A1 (CHOI, Unho), 29 October 2015 (29.10.2015), paragraphs [0128] to [0165]; fig. 8A to 10B & US 2012/0278614 A1 & WO 2011/062364 A2	1-9

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／０６４６６２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/32(2013.01)i, G06F21/40(2013.01)i, H04M11/00(2006.01)i, H04Q9/00(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/32, G06F21/40, H04M11/00, H04Q9/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１６年
日本国実用新案登録公報	１９９６－２０１６年
日本国登録実用新案公報	１９９４－２０１６年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
X Y	WO 2014/103308 A1 (パナソニック株式会社) 2014.07.03, [0039]-[0040], [0056]-[0060], [0068]-[0073], 図 1-2, 4 & US 2015/0012863 A1, [0053]-[0054], [0070]-[0074], [0082]-[0087], FIGs. 1-2, 4	1-3, 6-9 4-5
Y	JP 2015-36918 A (富士ゼロックス株式会社) 2015.02.23, 要約, [0019]-[0020], 図 1, 4-5 & US 2015/0049923 A1, [0026]-[0029], FIGs. 1, 4A-4D, 5E-5H	4-5

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２０．０７．２０１６	０２．０８．２０１６

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　３９８３
岸野　徹
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2003-150551 A (横河電機株式会社) 2003.05.23, 要約, [0012]-[0013] (ファミリーなし)	4-5
A	JP 2005-248542 A (株式会社東芝) 2005.09.15, [0006]-[0007], [0022], [0037]-[0038], [0045], 図５ (ファミリーなし)	1-9
A	JP 2014-164359 A (ＮＥＣネッツエスアイ株式会社) 2014.09.08, [0023]-[0027], [0046]-[0055], 図１, ４ (ファミリーなし)	1-9
A	JP 2010-74782 A (株式会社オプティム) 2010.04.02, [0028]-[0029], [0069], 図 1-2, 9B (ファミリーなし)	1-9
A	JP 2008-199197 A (シャープ株式会社) 2008.08.28, [0137]-[0149], 図 4, 13 (ファミリーなし)	1-9
A	JP 2008-131081 A (パイオニア株式会社) 2008.06.05, [0068], 図 1-2 (ファミリーなし)	1-9
A	JP 2012-161001 A (東芝キヤリア株式会社) 2012.08.23, [0016]-[0017], 図 1-2 (ファミリーなし)	1-9
A	US 2015/0312041 A1 (CHOI, Unho) 2015.10.29, [0128]-[0165], FIG.8A-10B & US 2012/0278614 A1 & WO 2011/062364 A2	1-9