

(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6月29日(29.06.2017)



(10) 国際公開番号

WO 2017/109936 A1

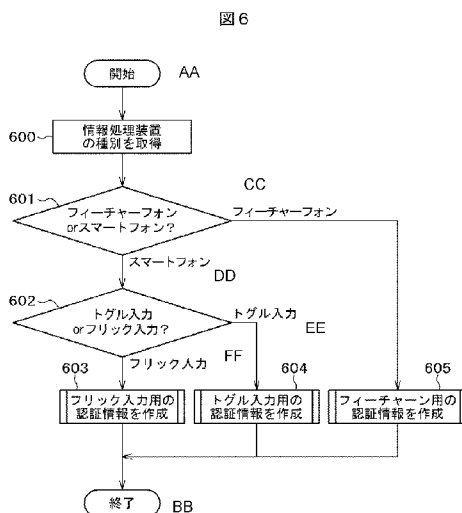
- (51) 国際特許分類:
G06F 3/0488 (2013.01) G06F 3/0489 (2013.01)
G06F 3/023 (2006.01) H03M 11/04 (2006.01)
- (21) 国際出願番号: PCT/JP2015/086223
- (22) 国際出願日: 2015年12月25日(25.12.2015)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人: 日立マクセル株式会社 (HITACHI MAXELL, LTD.) [JP/JP]; 〒5678567 大阪府茨木市丑寅一丁目1番88号 Osaka (JP).
- (72) 発明者: 野村 具徳 (NOMURA Tomonori); 〒5678567 大阪府茨木市丑寅一丁目1番88号 日立マクセル株式会社内 Osaka (JP). 鈴木 基之 (SUZUKI Motoyuki); 〒5678567 大阪府茨木市丑寅一丁目1番88号 日立マクセル株式会社内 Osaka (JP). 橋本 康宣 (HASHIMOTO Yasunobu); 〒5678567 大阪府茨木市丑寅一丁目1番88号 日立マクセル株式会社内 Osaka (JP). 渡辺 光信

- (WATANABE Mitsunobu); 〒5678567 大阪府茨木市丑寅一丁目1番88号 日立マクセル株式会社内 Osaka (JP). 吉澤 和彦 (YOSHIZAWA Kazuhiko); 〒5678567 大阪府茨木市丑寅一丁目1番88号 日立マクセル株式会社内 Osaka (JP). 清水 宏 (SHIMIZU Hiroshi); 〒5678567 大阪府茨木市丑寅一丁目1番88号 日立マクセル株式会社内 Osaka (JP). 益岡 信夫 (MASUOKA Nobuo); 〒5678567 大阪府茨木市丑寅一丁目1番88号 日立マクセル株式会社内 Osaka (JP).
- (74) 代理人: 青稜特許業務法人 (SEIRYO I.P.C.); 〒1040032 東京都中央区八丁堀二丁目24番2号 Tokyo (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,

[続葉有]

(54) Title: INPUT INFORMATION GENERATING METHOD, INFORMATION PROCESSING DEVICE, AND INFORMATION PROCESSING PROGRAM

(54) 発明の名称: 入力情報生成方法、情報処理装置、および情報処理プログラム



- 600 Acquire information processing device type
601 Feature phone or smartphone?
602 Toggle input or flick input?
603 Create authentication information for flick input
604 Create authentication information for toggle input
605 Create authentication information for feature phone
AA Start
BB End
CC Feature phone
DD Smartphone
EE Toggle input
FF Flick input

(57) Abstract: Provided is an input information generating method which generates input information which is configured from a plurality of text characters, said input information generating method: assessing a method by which text characters are inputted from an operation unit; and generating input information according to the assessed method by which the text characters are inputted.

(57) 要約: 複数の文字から構成される入力情報を生成する入力情報生成方法であって、操作部から入力される文字の入力方法を判定し、判定した文字の入力方法に応じて入力情報を生成する。

WO 2017/109936 A1



MY, MZ, NA, NG, NI, NO, 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))

明 細 書

発明の名称：

入力情報生成方法、情報処理装置、および情報処理プログラム

技術分野

[0001] 本発明は、入力情報生成方法、情報処理装置、および情報処理プログラムに関する。

背景技術

[0002] コンテンツを視聴する場合のように、電子商取引を行う際には、ライセンスキー等の認証情報を発行する必要がある。認証情報を発行するために、例えば、特許文献1には、乱数に基づいて認証情報を自動生成する技術が開示されている。

先行技術文献

特許文献

[0003] 特許文献1：特開2003-208408号公報

発明の概要

発明が解決しようとする課題

[0004] 認証情報の入力が煩雑であると、ユーザは入力を間違える可能性がある。このため、認証情報を容易に入力できることが望ましい。例えば、フィーチャーフォン、スマートフォン、リモコン、あるいはPC（Personal Computer）等の様々な情報処理装置では、その種別ごとに認証情報の入力方法が異なるため、入力方法が異なる情報処理装置で同じ認証情報を入力する場合、入力操作が煩雑となる。具体例を挙げると、ユーザがライセンスキーを購入した後、購入時にライセンスキーを入力した情報処理装置とは異なる種別の情報処理装置でコンテンツを再生する場合、ライセンスキーの入力方法が異なるため、入力操作が煩雑となる。

[0005] 認証情報の例としては、ライセンスキーのほか、ユーザIDやパスワードがあるが、上記のような場合にはライセンスキーと同様、入力操作の煩雑さ

が生じる。このような問題は、認証情報、ユーザIDやパスワードを入力する場合に限らず、あらかじめ定められた様々な入力情報を入力する様々な場面で生じ得る。このため、入力情報の入力方法が異なることによる入力操作の煩雑さが生じないように、入力方法に応じて入力情報を生成することができる技術が求められていた。上記特許文献1では、認証情報を自動的に生成しているが、入力方法に応じて入力情報を生成することについては考慮されていない。

[0006] 本発明は、上記に鑑みてなされたものであって、入力方法に応じて入力情報を生成することができる入力情報生成方法、情報処理装置、および情報処理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] 上記課題を解決するために、本発明にかかる入力情報生成方法は、複数の文字（ここで「文字」とは、A、B、C等の文字、1、2、3等の数字、+、-等の記号、符号等を含む）を含む入力情報を生成する入力情報生成方法であって、操作部から入力される前記文字の入力方法を判定し、判定した前記文字の入力方法に応じて前記入力情報を生成する、ことを特徴とする入力情報生成方法として構成される。

[0008] また、本発明は、上記入力情報生成方法を用いた情報処理装置、および上記入力情報生成方法を実行する情報処理プログラムとしても把握される。

発明の効果

[0009] 本発明によれば、入力方法に応じて入力情報を生成することができる。

図面の簡単な説明

[0010] [図1]本発明にかかる入力情報生成方法、情報処理装置、および情報処理プログラムを適用した情報処理システムの構成例を示す図である。

[図2(a)]情報処理装置の内部構成の一例を示すブロック図である。

[図2(b)]図2（a）に示した情報処理装置の内部構成の一例を示すソフトウェア構成図である。

[図3(a)]配信サーバがライセンスキーを生成して情報処理端末に配信する処

理のシーケンス図である。

[図3(b)]配信サーバがライセンスキーを生成して情報処理端末に配信する処理のシーケンス図である。

[図4]図3 (b) に示したS 3 1 8におけるライセンスキー入力画面の例を示す図である。

[図5]配信サーバの内部構成の一例を示すソフトウェア構成図である。

[図6]図3 に示したS 3 1 1におけるライセンスキー生成処理の処理手順を示すフローチャートである。

[図7]フィーチャーフォンが有する操作器の一例であるキーパッドの配置例を示す図である。

[図8]図6 に示した第1 認証情報生成処理の処理手順を示すフローチャートである。

[図9(a)]スマートフォンが有する操作器の一例であるキーパッドの配置例を示す図である。

[図9(b)]図9 (a) に示したキーパッドにタッチする指をスライドさせるフリック操作により文字を入力する場合の入力例の説明図である。

[図9(c)]図9 (a) に示したキーパッドにタッチする指をスライドさせるフリック操作により文字を入力する場合の入力例の説明図である(変形例)。

[図10]図6 に示した第2 認証情報生成処理の処理手順を示すフローチャートである。

[図11]図1 0 に示した第2 認証情報生成処理の処理手順の変形例を示すフローチャートである。

[図12]図6 に示した第3 認証情報生成処理の処理手順を示すフローチャートである。

[図13]決定処理、選択処理の処理手順を示すフローチャートである。

[図14(a)]入力されたライセンスキーの表示例を示す図である(フィーチャーフォン)。

[図14(b)]入力されたライセンスキーの表示例を示す図である(スマートフォ

ンによるフリック入力）。

[図14(c)]入力されたライセンスキーの表示例を示す図である（スマートフォンによるフリック入力の変形例）。

[図14(d)]入力されたライセンスキーの表示例を示す図である（スマートフォンによるトグル入力）。

[図15]情報処理装置の内部構成の一例を示すソフトウェア構成図である（実施例2）。

[図16(a)]情報処理装置においてユーザID及びパスワードを生成、登録する処理の処理手順を示すフローチャートである。

[図16(b)]図16(a)で登録したユーザIDおよびパスワードを用いてウェブサイトやアプリケーションにログインする処理の処理手順を示すフローチャートである。

[図17]S1604において情報処理装置のディスプレイに表示されるユーザIDおよびパスワードの入力画面の例を示す図である。

[図18]実施例2における第1認証情報生成処理の処理手順を示すフローチャートである。

[図19]実施例2における第2認証情報生成処理の処理手順を示すフローチャートである。

[図20]実施例2における第2認証情報生成処理の処理手順の変形例を示すフローチャートである。

[図21]実施例2における第3認証情報生成処理の処理手順を示すフローチャートである。

[図22]本発明にかかる入力情報生成方法、情報処理装置、および情報処理プログラムを適用した情報処理システムの構成例を示す図である（リモコンの場合）。

発明を実施するための形態

[0011] 以下に添付図面を参照して、本発明にかかる入力情報生成方法、情報処理装置、および情報処理プログラムの実施の形態を詳細に説明する。以下では

、認証情報の例として、実施例１にライセンスキー、実施例２にユーザＩＤおよびパスワードを挙げているが、上記に限らず、あらかじめ定められた様々な入力情報を入力する様々な場面に適用することができる。

(実施例１)

図１は、本発明にかかる入力情報生成方法、情報処理装置、および情報処理プログラムを適用した情報処理システム１０００の構成例を示す図である。図１に示すように、情報処理システム１０００は、情報処理装置１００と配信サーバ１０１とを有し、これらが、ネットワーク１０２を介してアクセスポイント装置１０３または基地局１０５に接続されている。なお、ネットワーク１０２、アクセスポイント装置１０３、移動体サーバ１０４、基地局１０５は、従来から知られている一般的な構成であるため、以下ではこれらの説明を省略している。

[0012] 情報処理装置１００は、例えば、フィーチャーフォン、スマートフォン等の携帯端末、リモコン等の操作機器、ＰＣ（Personal Computer）やウェアラブル端末等の情報処理端末をはじめ、入力情報の入力を受け付けることが可能な様々な種別の装置や端末、機器である。以下では、情報処理装置１００の例として、フィーチャーフォン、スマートフォン、リモコンを挙げているが、上記のとおり、入力情報の入力を受け付ける様々な装置や端末、機器を用いることができる。

[0013] 図２（ａ）は、情報処理装置１００の内部構成の一例を示すブロック図である。図２（ａ）に示すように、情報処理装置１００は、ＣＰＵ（Central Processing Unit）２０１と、システムバス２０２と、ＲＯＭ（Read Only Memory）２０３と、ＲＡＭ（Random Access Memory）２０４と、ストレージ２１０と、通信処理器２２０と、操作器２３０と、ビデオプロセッサ２４０と、オーディオプロセッサ２５０と、センサ２６０とを有して構成されている。

[0014] ＣＰＵ２０１は、情報処理装置１００全体を制御するマイクロプロセッサユニットである。システムバス２０２は、ＣＰＵ２０１と情報処理装置１００内の各動作ブロックとの間でデータを送受信するためのデータ通信路であ

る。

[0015] ROM 203は、オペレーティングシステム等の基本動作プログラムやその他の動作プログラムが格納されたメモリであり、例えば、EEPROM (Electrically Erasable Programmable Read-Only Memory) やフラッシュROMのような書き換え可能なROMが用いられる。

[0016] RAM 204は、基本動作プログラムやその他の動作プログラム実行時のワークエリアとなる。ROM 203及びRAM 204は、CPU 201と一体の構成であってもよい。また、ROM 203は、図2(a)に示したような独立構成ではなく、ストレージ210内の一部記憶領域を使用してもよい。

[0017] ストレージ210は、情報処理装置100の動作プログラムや動作設定値、情報処理装置100を使用するユーザの個人情報等のほか、上述した認証情報として、ライセンスキーを記憶する。以下では特に例示していないが、ネットワーク上からダウンロードした動作プログラムや、その動作プログラムが作成した各種データを記憶してもよい。また、ストレージ210の一部記憶領域をROM 203の機能の一部または全部を代替してもよい。ストレージ210には、例えば、フラッシュROMやSSD (Solid State Drive)、HDD (Hard Disk Drive) 等のデバイスが用いられる。

[0018] なお、ROM 203やストレージ210に記憶された上記動作プログラムは、ネットワーク102上の各装置からダウンロード処理を実行することにより、更新及び機能拡張することができる。

[0019] 通信処理器220は、LAN (Local Area Network) 通信器221、電話網通信器222、NFC (Near Field Communication) 通信器223、Bluetooth (登録商標) 通信器224を有して構成される。LAN通信器221は、アクセスポイント装置103を介してネットワーク102と接続され、ネットワーク102上の各装置との間でデータを送受信する。電話網通信器222は、移動体電話通信網の基地局105との間で通話およびデータを送受信する。NFC通信器223は、対応するリーダ／ライタが近接

した際に無線通信してデータを送受信する。BlueTooth通信器224は、近接する情報処理装置と無線通信してデータを送受信する。

[0020] 操作器230は、情報処理装置100に対する入力情報の入力を受け付ける装置である。操作器230は、例えば、ボタンスイッチを並べた操作キー、ディスプレイ241に重ねて配置したタッチパネルである。以下では、上記操作キー、タッチパネルを例に挙げて説明しているが、キーボードをはじめとする他の装置であってもよい。具体的には後述するが、ユーザは、操作器230を操作して、入力情報の一つであるライセンスキー、あるいはユーザIDおよびパスワードを入力する。操作器230が有するキーの配置、配置された各キーに割り当てられているグループおよびそのグループに属する文字、フリック操作時においてキーが選択されたときにそのキーの周囲に表示する文字、トグル操作時においてキーをタッチした回数により選択する文字（後述する図7、図9（a）～（c））については、例えば、ストレージ210にあらかじめ記憶されている。

[0021] ビデオプロセッサ240は、ディスプレイ241と、画像信号処理プロセッサ242と、カメラ243とを有して構成される。

[0022] ディスプレイ241は、例えば、液晶パネル等の表示デバイスであり、画像信号処理プロセッサ242が処理した画像データを表示する。画像信号処理プロセッサ242は、入力された画像データをディスプレイ241に表示させる。カメラ243は、CCD（Charge Coupled Device）やCMOS（Complementary Metal Oxide Semiconductor）センサ等の電子デバイスを用いてレンズから入力した光を電気信号に変換することにより、周囲や対象物の画像データを入力する撮像装置として機能するカメラユニットである。

[0023] オーディオプロセッサ250は、スピーカ251と、音声信号プロセッサ252と、マイク253とを有して構成される。

[0024] スピーカ251は、音声信号プロセッサ252が処理した音声信号を出力する。音声信号プロセッサ252は、入力された音声データをスピーカ251に出力する。マイク253は、音声を音声データに変換し、音声信号プロ

セッサ２５２に出力する。

[0025] センサ２６０は、情報処理装置１００の状態を検出するためのセンサ群であり、GPS受信機２６１と、ジャイロセンサ２６２と、地磁気センサ２６３と、加速度センサ２６４と、照度センサ２６５と、近接センサ２６６とを有して構成される。これらの各センサは従来から知られている一般的なセンサ群であるため、ここではその説明を省略する。図２（ａ）に示した情報処理装置１００の構成はあくまで一例であり、必ずしもこれらの全てを備えていなくてもよい。

[0026] 図２（ｂ）は、図２（ａ）に示した情報処理装置１００の内部構成の一例を示すソフトウェア構成図である。図２（ｂ）に示すように、情報処理装置１００には、ROM２０３に、基本動作プログラム２０３ａと、その他のプログラム２０３ｂとが記憶される。また、RAM２０４に、基本動作プログラム２０３ａを実行するための基本動作実行プログラム２０４ａと、ストレージ部２１０に記憶されたサーバ情報取得プログラム２１０ｂを実行するためのサーバ情報取得実行プログラム２０４ｂと、これらの実行プログラムの実行時に必要となる一時記憶領域２０４ｃとが記憶される。ストレージ部２１０に、サーバ情報取得プログラム２１０ｂと、その他のプログラム２１０ｃと、各種情報／データ記憶領域２１０ｄとが記憶される。各種情報／データ記憶領域２１０ｄには、配信サーバ１０１において生成された認証情報の一例であるライセンスキーを記憶する認証情報記憶領域２１０ａを有している。

[0027] 本実施例においては、ストレージ部２１０に記憶されたサーバ情報取得プログラム２１０ｂがRAM２０４にロードされ、サーバ情報取得実行プログラム２０４ｂが、配信サーバ１０１において生成された認証情報の一例であるライセンスキーを取得し、上記認証情報記憶領域２１０ａに記憶する。なお、認証情報記憶領域２１０ａは、RAM２０４の一時記憶領域２０４ｃに設けてもよい。サーバ情報取得実行プログラム２０４ｂの具体的な動作については後述する。

続いて、配信サーバ１０１について説明する。

[0028] 配信サーバ１０１は、情報処理装置１００にコンテンツを配信するサーバであり、一般的なサーバから構成される。配信サーバ１０１は一般的な構成であるため、以下では、その内部構成の一例を示すブロック図を省略し、ソフトウェア構成について説明する。

図５は、配信サーバ１０１の内部構成の一例を示すソフトウェア構成図である。図５に示すように、配信サーバ１０１には、ＲＡＭ５０３に、ストレージ部５０４に記憶された基本動作プログラム５０４ａを実行するための基本動作実行プログラム５０３ａと、ストレージ部５０４に記憶されたコンテンツ管理/配信プログラム５０４ｂを実行するためのコンテンツ管理/配信実行プログラム５０３ｂと、ストレージ部５０４に記憶された認証情報発生プログラム５０４ｄを実行するための認証情報発生実行プログラム５０３ｃと、ストレージ部５０４に記憶された認証情報照合プログラム５０４ｅを実行するための認証情報照合実行プログラム５０３ｄとが記憶される。

[0029] また、ストレージ部５０４に、基本動作プログラム５０４ａと、コンテンツ管理/配信プログラム５０４ｂと、配信されるコンテンツ５０４ｃと、コンテンツ管理/配信プログラム５０４ｄと、認証情報照合プログラム５０４ｅとが記憶される。なお、ＬＡＮ通信器５０５は、ネットワーク１０２に接続するためのインタフェースである。

[0030] 本実施例においては、ストレージ５０４に記憶されたコンテンツ管理/配信プログラム５０４ｂ、認証情報発生プログラム５０４ｄ、認証情報照合プログラム５０４ｅがＲＡＭ５０３にロードされ、コンテンツ管理/配信実行プログラム５０３ｂがコンテンツを配信し、認証情報発生実行プログラム５０３ｃがライセンスキーを生成し、認証情報照合実行プログラム５０３ｄがライセンスキーを照合する。これらの各プログラムの具体的な動作については後述する。

[0031] 図３（ａ）は、配信サーバ１０１がライセンスキーを生成して情報処理端末１００に配信する処理のシーケンス図である。図３（ａ）では、情報処理

装置 100 のアプリケーションを起動してからライセンスキーを表示するまでの処理の流れを示している。

[0032] 図 3 (a) に示すように、まず、情報処理装置 100 のサーバ情報取得実行プログラム 204 b は、ライセンスキーを購入してコンテンツを視聴するためのアプリケーションを起動する (S301)。上記アプリケーションとしては、例えば、ウェブブラウザプログラムがある。

[0033] サーバ情報取得実行プログラム 204 b は、上記ライセンスキーの購入または既にライセンスキーを購入したコンテンツの視聴を選択するための選択画面を、ディスプレイ 241 に表示する (S302)。

[0034] 操作器 230 が上記購入または視聴の選択を受け付けると (S303)、サーバ情報取得実行プログラム 204 b は、上記購入または視聴の選択のいずれが受け付けられたのかを判定する (S304)。

[0035] サーバ情報取得実行プログラム 204 b は、上記視聴の選択が受け付けられたと判定した場合、図 3 (b) に進み、以降の処理を実行する。一方、サーバ情報取得実行プログラム 204 b は、上記購入が受け付けられたと判定した場合、配信サーバ 101 に対して、販売用コンテンツの一覧を示す販売用コンテンツ一覧情報を要求する (S305)。配信サーバ 101 のコンテンツ管理／配信実行プログラム 503 b は、上記販売用コンテンツ一覧情報を、要求された情報処理装置 100 に送信する (S306)。

[0036] 情報処理装置 100 のサーバ情報取得実行プログラム 204 b は、上記販売用コンテンツ一覧情報をディスプレイ 241 に表示する (S307)。操作器 203 が上記販売用コンテンツ一覧情報の中から購入コンテンツの選択を受け付けると (S308)、サーバ情報取得実行プログラム 204 b は、操作器 203 から上記ライセンスキーを購入するために必要な情報の入力を要求する (S309)。サーバ情報取得実行プログラム 204 b は、受け付けられた上記必要な情報と、情報処理装置 100 の種別とを配信サーバ 101 に送信する (S310)。上記必要な情報としては、例えば、ユーザの住所や、コンテンツの購入に使用するクレジットカードのカード番号がある。

また、上記種別とは、フィーチャーフォン、スマートフォン等の携帯端末、リモコン等の操作機器、PC (Personal Computer) やウェアラブル端末等の情報処理端末をはじめとする装置や端末、機器を分類するための情報である。以下では、入力情報の入力方法が上記種別の違いによって生じている場合を例に説明しているが、上記種別の違いに限らず、他の様々な要因により入力情報の入力方法が異なる場合にも同様に適用することができる。

[0037] 配信サーバ101の認証情報発生実行プログラム503cは、購入されるコンテンツのライセンスキーを発生させるライセンスキー生成処理を実行し（S311）、生成したライセンスキーを、要求された情報処理装置100に送信する（S312）。ライセンスキー生成処理については、図6を用いて後述する。

[0038] 情報処理装置100のサーバ情報取得実行プログラム204bは、配信サーバ101から受信した上記ライセンスキーを、ディスプレイ241に表示する（S313）。

[0039] 一方、図3（b）に示すように、サーバ情報取得実行プログラム204bは、上記視聴の選択が受け付けられたと判定した場合、既に購入されているライセンスキーにより視聴可能なコンテンツの一覧を示す購入済コンテンツ一覧情報を、配信サーバ101に対して要求する（S314）。

[0040] 配信サーバ101のコンテンツ管理／配信実行プログラム503bは、上記購入済コンテンツ一覧情報を、要求された情報処理装置100に送信する（S315）。

[0041] 情報処理装置100のサーバ情報取得実行プログラム204bは、上記購入済コンテンツ一覧情報をディスプレイ241に表示する（S316）。操作器203が上記購入済コンテンツ一覧情報の中から購入済コンテンツの選択を受け付けると（S317）、サーバ情報取得実行プログラム204bは、選択した購入済コンテンツを視聴するための購入済ライセンスキーを入力するライセンスキー入力画面を、ディスプレイ241に表示する（S318）。

- [0042] サーバ情報取得実行プログラム204bは、操作器203が上記購入済ライセンスキーの入力を受け付けると（S319）、受け付けられた上記購入済ライセンスキーと、購入済コンテンツを識別するためのコンテンツIDとを、配信サーバ101に送信する（S320）。ここでは、複数のコンテンツに対して同じライセンスキーが生成される場合もあるため、それらを識別するために、コンテンツIDとライセンスキーとを配信サーバ101に送信している。
- [0043] 配信サーバ101の認証情報照合実行プログラム503dは、購入時にS311で生成された当該コンテンツIDのライセンスキーと、S320で情報処理装置100から受信したライセンスキーとが一致するか否かを判定し（S321）、両者が一致すると判定した場合（S321；Yes）、そのコンテンツIDによって識別されるコンテンツである視聴用データを、要求された情報処理装置100に送信する（S322）。
- [0044] 一方、認証情報照合実行プログラム503dは、両者が一致しないと判定した場合（S321；No）、S318に戻って、上記ライセンスキー入力画面を、ディスプレイ241に表示する。
- [0045] 情報処理装置100のサーバ情報取得実行プログラム204bは、配信サーバ101から受信したコンテンツを再生し（S323）、ユーザがそのコンテンツを視聴する。
- [0046] ユーザがライセンスキーを購入した後、異なる種別の情報処理装置100でコンテンツを視聴する場合、ユーザはライセンスキーを再度入力する必要が生じる。情報処理装置100の種別ごとにライセンスキーの入力方法が異なる。このため、種別が異なる情報処理装置間で同じライセンスキーを入力する場合であっても、その入力方法が異なり入力操作が煩雑となっていた。本実施例では、種別の異なる情報処理装置100からライセンスキーが入力される場合であっても、その入力が容易となるように、情報処理装置100の種別に応じてライセンスキーを生成している。
- [0047] 図4は、図3（b）に示したS318におけるライセンスキー入力画面の

例を示す図である。図4に示すように、ライセンスキー入力画面には、S317で選択したコンテンツIDの表示欄と、そのコンテンツIDに対応するライセンスキーの入力欄とが設けられている。

[0048] 図6は、図3に示したS311におけるライセンスキー生成処理の処理手順を示すフローチャートである。図6に示すように、ライセンスキー生成処理では、コンテンツ配信サーバ101の認証情報発生実行プログラム503cは、S310で受信した情報処理装置100の種別を読み取り（S600）、その種別が、フィーチャーフォンであるか、またはスマートフォンであるかを判定する（S601）。

[0049] 認証情報発生実行プログラム503cは、上記種別がフィーチャーフォンであると判定した場合、S605に進み、フィーチャーフォン用の認証情報を生成するための第1認証情報生成処理を実行する（S605）。

[0050] 一方、認証情報発生実行プログラム503cは、上記種別がスマートフォンであると判定した場合、さらに、そのスマートフォンがトグル入力方式のスマートフォンであるか、フリック入力方式のスマートフォンであるかを判定する（S602）。

[0051] 認証情報発生実行プログラム503cは、トグル入力方式のスマートフォンであると判定した場合、S604に進み、トグル入力方式のスマートフォン用の認証情報を生成するための第3認証情報生成処理を実行する（S604）。

[0052] 一方、認証情報発生実行プログラム503cは、フリック入力方式のスマートフォンであると判定した場合、S603に進み、フリック入力方式のスマートフォン用の認証情報を生成するための第2認証情報生成処理を実行する（S603）。

[0053] 上記第1認証情報生成処理、第2認証情報生成処理、第3認証情報生成処理については後述する。

[0054] 図7は、フィーチャーフォンが有する操作器203の一例であるキーパッドの配置例を示す図である。フィーチャーフォンが有する操作器203とし

て、図7では、テンキーおよび記号等の入力キーが配置された例を示している。このようなテンキーや入力キーの配置は、リモコンの場合も同様である。

[0055] 図7に示すように、上記キーパッドには、ライセンスキーの入力を受け付けるための複数のキーが規則的に配置されている。それぞれのキーには、1または複数の種類の文字を含むグループが割り当てられている。ユーザが操作器203を操作して入力した文字と次に入力する文字とが同じグループに属する場合、上記入力した文字の入力後にカーソルを右に一文字分ずらさなければ、上記次に入力する文字を入力することができない。このため、単純に続けて文字を入力する場合に比べて、カーソルをずらす等の手間が生じ、入力操作が煩雑となってしまう。

[0056] そこで、本実施例では、ライセンスキーの入力において上記のようにカーソルをずらす必要がないように、認証情報を構成する文字のうち、続けて入力される文字が直前に入力された文字と同じグループとならないように、すなわち、互いに隣接する文字が同じグループとならないように、認証情報を生成している。

[0057] 図8は、図6に示した第1認証情報生成処理の処理手順を示すフローチャートである。図8に示すように、第1認証情報生成処理では、コンテンツ配信サーバ101の認証情報発生実行プログラム503cは、認証情報を構成する最初の文字を生成する生成処理を実行し（S801）、認証情報の最初の文字を決定する。続いて、認証情報発生実行プログラム503cは、次に続く文字の候補を生成する生成処理を実行する（S802）。上記生成処理については後述する。

[0058] 認証情報発生実行プログラム503cは、上記生成処理で生成した文字が、認証情報として一つ前に決定した文字と同じグループに属する文字であるか否かを判定し（S803）、両者が同じグループに属する文字であると判定した場合（S803；Yes）、S802に戻って、再び上記生成処理を実行する。

- [0059] 一方、認証情報発生実行プログラム503cは、両者が同じグループに属する文字でない、すなわち両者が異なるグループに属する文字であると判定した場合（S803；No）、生成した文字を、認証情報として一つ前に決定した文字に続く文字として決定する（S804）。
- [0060] 認証情報発生実行プログラム503cは、認証情報を構成する全ての文字が決定したか否か、すなわち認証情報が設定文字数を満たしたか否かを判定し（S805）、設定文字数を満たしていないと判定した場合（S805；No）、S802に戻って、設定数を満たすまで上記各処理を繰り返す。一方、認証情報発生実行プログラム503cは、設定数を満たすと判定した場合（S805；Yes）、処理を終了する。
- [0061] このように、1つ前に並ぶ文字に続く文字が同じグループとならないように、認証情報を構成する各文字を決定する。したがって、上記したようなカーソルの移動といった煩雑な操作が不要となり、容易な入力操作で認証情報を入力することができる。
- [0062] 図9（a）は、スマートフォンが有する操作器203の一例であるキーパッドの配置例を示す図である。また、図9（b）は、図9（a）に示したキーパッドにタッチする指をスライドさせるフリック操作により文字を入力する場合の入力例の説明図である。キーパッドを構成する各キーは、実際には、フィーチャーフォンの場合と異なり、操作器203とディスプレイ240とを有したタッチパネル上に配置されている。各キーの配置やグループについては図7の場合と同様の説明となるため、ここではその説明を省略する。
- [0063] 図9（a）、9（b）において、A、B、C、2を一つのグループとしてタッチパネル上に表示されているキーK1を例に説明する。ユーザがキーK1の中央をタッチすると、図9（b）が表示される。ユーザがタッチをやめて指を離した場合、すなわち、フリック操作による移動なしの場合、文字として「A」が選択される。また、ユーザがタッチした指を左向きに移動させる左フリック操作をすると、文字「B」が選択される。同様に、ユーザがタッチした指を上向きに移動させる上フリック操作をすると、文字「C」が選

択され、ユーザがタッチした指を下向きに移動させる下フリック操作をすると、文字「2」が選択される。

[0064] ユーザが操作器203を入力した文字と次に入力する文字のフリック操作の向きが異なる向きとなる場合、上記入力した文字の入力後に異なる向きに指を動かさなければ、上記次に入力する文字を入力することができない。このため、同じ向きのフリック操作で続けて文字を入力する場合に比べて、異なる向きに指を動かさなければならない手間が生じ、入力操作が煩雑になってしまう。

[0065] そこで、本実施例では、ライセンスキーの入力において上記のように向きが異なるフリック操作とならないように、認証情報を構成する文字のうち、続けて入力される文字と直前に入力された文字とが同じ向きのフリック操作となるように、すなわち、隣接するすべての文字が同じ向きのフリック操作となるように、認証情報を生成している。

[0066] 図10は、図6に示した第2認証情報生成処理の処理手順を示すフローチャートである。第2認証情報生成処理は、上記したように、図9(b)に示したフリック操作により入力される認証情報を生成する処理である。図10に示すS1001、S1002、S1004、S1005は、それぞれ、図8に示したS801、S802、S804、S805と同様であるため、以下では、S1003について説明する。

[0067] 図10に示すように、S1002の生成処理が実行されると、認証情報発生実行プログラム503cは、上記生成処理で生成した文字が、認証情報として一つ前に決定した文字と同じフリック操作の向きの文字であるか否かを判定し(S1003)、両者が同じフリック操作の向きの文字でないと判定した場合(S1003; No)、S1002に戻って、再び上記生成処理を実行する。

[0068] 一方、認証情報発生実行プログラム503cは、両者が同じフリック操作の向きの文字であると判定した場合(S1003; Yes)、生成した文字を、認証情報として一つ前に決定した文字に続く文字として決定する(S1

004)。S1003の処理では、認証情報発生実行プログラム503cは、フリック操作の向きが同じであるか否かを判定しており、必ずしも認証情報として一つ前に決定した文字と上記生成した文字とが同じグループに属していなくてもよい。なお、上記フリック操作の向きが同じであるか否かは、例えば、認証情報発生実行プログラム503cが、認証情報として一つ前に決定した文字が、当該決定した文字が属するグループが割り当てられたキーに対してどの向きの位置に配置されているのかを判定し、さらに、上記生成した文字が、当該生成した文字が属するグループが割り当てられたキーに対してどの向きの位置に配置されているのかを判定し、当該決定した文字と当該生成した文字とが、それぞれが属するキーに対して同じ向きとなる位置に配置されていると判定した場合に、当該決定した文字に対するフリック操作と当該生成した文字に対するフリック操作とが同じ向きであると判定する。

[0069] このように、認証情報として一つ前に決定した文字に続く文字を入力するためのフリック操作の向きが同じとなるように、認証情報を構成する各文字を決定する。したがって、上記したような異なる向きのフリック操作といった煩雑な操作が不要となり、容易な入力操作で認証情報を入力することができる。

[0070] 図10に示した例では、上記フリック操作が同じ向きであれば煩雑な操作とならないことに着目し、その説明をした。しかし、フリック操作により指が移動した向きにあるキーに配置されたグループの中から次の文字を生成することも可能である。

[0071] 例えば、図9(b)において、A、B、C、2を一つのグループとしてタッチパネル上に表示されているキーK1の中央をタッチした後、指を下向きに移動させる下フリック操作をすると、文字「2」が選択される。このとき、図9(c)に示すように、上記キーK1に対して下フリック操作した向きにあるキーK2には、J、K、L、5を一つのグループとしたキーが配置されている。このため、このグループの中から上記次の文字を生成すると、より一層、入力操作が容易になる。

[0072] 図11は、図10に示した第2認証情報生成処理の処理手順の変形例を示すフローチャートである。本処理は、上記したように、図9(c)に示したフリック操作により入力される認証情報を生成する処理である。図11に示すS1101、S1102、S1104、S1105は、それぞれ、図8に示したS801、S802、S804、S805と同様であるため、以下では、S1103について説明する。

[0073] 図11に示すように、S1102の生成処理が実行されると、認証情報発生実行プログラム503cは、上記生成処理で生成した文字が、認証情報として一つ前に決定した文字を入力したときのフリック操作の向きにあるキーのグループに含まれる文字であるか否かを判定し(S1103)、認証情報として一つ前に決定した文字を入力したときのフリック操作の向きにあるキーのグループに含まれる文字でないと判定した場合(S1103; No)、S1102に戻って、再び上記選択処理を実行する。

[0074] 一方、認証情報発生実行プログラム503cは、認証情報として一つ前に決定した文字を入力したときのフリック操作の向きにあるキーのグループに含まれる文字であると判定した場合(S1103; Yes)、生成した文字を、認証情報として一つ前に決定した文字に続く文字として決定する(S1104)。S1103の処理では、認証情報発生実行プログラム503cは、次に入力される文字が、直前の文字が入力されたときのフリック操作の向きにあるキーに含まれる文字であるか否かを判定しており、必ずしも認証情報として一つ前に決定した文字と上記生成した文字とが隣接するグループに属していなくてもよい。

[0075] このように、認証情報として一つ前に決定した文字に続く文字を、決定した文字を入力したときのフリック操作の向きにあるキーに属する文字の中から決定する。したがって、上記したような異なる向きのフリック操作といった煩雑な操作が不要となるだけでなく、フリック操作後の指の位置で次のフリック操作ができるため、より一層、容易な入力操作で認証情報を入力することができる。

[0076] 図12は、図6に示した第3認証情報生成処理の処理手順を示すフローチャートである。第3認証情報生成処理は、上記したように、図9(a)に示したキーパッドに配置されたキーを1または複数回繰り返しタッチするトグル操作により入力される認証情報を生成する処理である。図12に示すS1201、S1202、S1204、S1205は、それぞれ、図8に示したS801、S802、S804、S805と同様であるため、以下では、S1203について説明する。

[0077] 図12に示すように、S1202の選択処理が実行されると、認証情報発生実行プログラム503cは、上記生成処理で生成した文字が、上記決定処理で決定した文字と同じ回数のトグル操作で入力された文字であるか否かを判定し(S1003)、上記決定処理で決定した文字と同じ回数のトグル操作で入力された文字でないと判定した場合(S1203; No)、S1202に戻って、再び上記選択処理を実行する。

[0078] 一方、認証情報発生実行プログラム503cは、認証情報として一つ前に決定した文字と同じ回数のトグル操作で入力された文字であると判定した場合(S1203; Yes)、生成した文字を、認証情報として一つ前に決定した文字に続く文字として決定する(S1204)。S1203の処理では、認証情報発生実行プログラム503cは、トグル操作の回数が同じであるか否かを判定しており、必ずしも認証情報として一つ前に決定した文字と上記生成した文字とが同じグループに属していなくてもよい。

[0079] このように、認証情報として一つ前に決定した文字に続く文字を入力するためのトグル操作の回数が同じとなるように、認証情報を構成する各文字を決定する。したがって、タッチする回数が異なるトグル操作といった煩雑な操作が不要となり、同じリズムで入力操作ができ、容易な入力操作で認証情報を入力することができる。

[0080] 続いて、図8に示したS801、S802、図10に示したS1001、S1002、図11に示したS1101、S1102、図12に示したS1201、S1202における生成処理について説明する。

[0081] 図13は、生成処理の処理手順を示すフローチャートである。図13に示すように、上記生成処理では、まず、コンテンツ配信サーバ101の認証情報発生実行プログラム503cは、所定の範囲にある数値（例えば、0～32768）から乱数を発生させ（S1501）、発生させた乱数を整数化する（S1502）。

[0082] 認証情報発生実行プログラム503cは、整数化した乱数を、求めたい範囲の数値が剰余となる数値（例えば、アルファベットの大文字、小文字と、0から9の数字の場合は62）除算し（S1503）、除算して得られた数値の剰余となる数値（例えば、0～61のいずれか）を、上記文字に割り当てる（S1504）。これらの乱数発生に関する処理は、従来から知られている様々な乱数発生のための処理を適用することができる。

[0083] 図14（a）～14（d）は、入力されたライセンスキーの表示例を示す図である。図14（a）は、フィーチャーフォンによる入力の場合の表示例を示し、図14（b）は、スマートフォンによるフリック入力の場合の表示例を示し、図14（c）は、スマートフォンによるフリック入力の変形例の場合の表示例を示し、図14（d）は、スマートフォンによるトグル入力の場合の表示例を示している。以下、各図面に表示されているライセンスキーの入力例について具体的に説明する。

[0084] 図14（a）では、ライセンスキーとして「AKUGP」が表示されている。ユーザは、ライセンスキー「AKUGP」を構成する文字のうち、「A」を入力する場合、図9（a）に示したキー配置では、「2」、「A」、「B」、「C」が属するキーK1を選択する。続いて、「A」を入力したときとは異なるグループに属する「K」を入力する。同様に、「K」とは異なるグループに属する「G」を入力し、続いて、「G」とは異なるグループに属する「P」を入力する。このように、本システムにより生成されたライセンスキーを構成する各桁の文字は、入力した桁の文字と次の桁の文字とは異なるグループのキーとなるように並べられている。したがって、上記したように、カーソルの移動といったユーザにとって面倒な操作が不要となる。

[0085] 図14(b)では、ライセンスキーとして「BENKH」が表示されている。ユーザは、ライセンスキー「BENKH」を構成する文字のうち、「B」を入力する場合、図14(a)の場合と同様、キーK1をタッチして「A」を選択した後、左フリック操作をする。続いて、「E」を入力する場合、「D」を選択した後、左フリック操作をする。同様に、「M」を選択した後、左フリック操作して「N」を入力し、続いて、「J」を選択した後、左フリック操作して「K」を入力し、「G」を選択した後、左フリック操作して「H」を入力する。このように、本システムにより生成されたライセンスキーを構成する各桁の文字は、直前の桁の文字を入力するためフリック操作と同じ向きのフリック操作で次の桁の文字が入力できるように各桁の文字が並べられている。したがって、上記したように、異なる向きのフリック操作といったユーザにとって面倒な操作が不要となる。

[0086] 図14(c)では、ライセンスキーとして「2K4SV」が表示されている。ユーザは、ライセンスキー「2K4SV」を構成する文字のうち、「2」を入力する場合、図14(b)の場合と同様、キーK1をタッチして「A」を選択した後、下フリック操作をする。続いて、「K」を入力する場合、「2」を入力して下フリック操作した向きにあるグループに属する「J」を選択した後、左フリック操作をする。続いて、「K」を入力したときに左フリック操作した向きにあるグループに属する「G」を選択した後、下フリック操作をして「4」を入力し、「4」を入力したときに下フリック操作した向きにあるグループに属する「P」を選択した後、右フリック操作をして「S」を入力し、「S」を入力したときに右フリック操作した向きにあるグループに属する「T」を選択した後、上フリック操作をして「V」を入力する。このように、本システムにより生成されたライセンスキーを構成する各桁の文字は、直前の桁の文字を入力したフリック操作の向きにあるキーに割り当てられた文字の中から次の桁の文字を選択して入力できるように各桁の文字が並べられている。したがって、上記したように、異なる向きのフリック操作といったユーザにとって面倒な操作が不要となる。

[0087] 図14(d)では、ライセンスキーとして「BKUHQ」が表示されている。ユーザは、ライセンスキー「BKUHQ」を構成する文字のうち、「B」を入力する場合、図14(c)の場合と同様、キーK1を2回タッチして「B」を入力する。続いて、「K」を入力する場合、「J」を含むグループのキーを2回タッチして「K」を入力する。同様に、「U」を入力する場合、「T」を含むグループのキーを2回タッチして「U」を入力し、「H」を入力する場合、「G」を含むグループのキーを2回タッチして「H」を入力し、「Q」を入力する場合、「P」を含むグループのキーを2回タッチして「Q」を入力する。このように、本システムにより生成されたライセンスキーを構成する各桁の文字は、直前の桁の文字を入力した際にキーをタッチした回数と同じタッチの回数で文字を選択して入力できるように各桁の文字が並べられている。したがって、上記したように、タッチする回数が異なるトグル操作といったユーザにとって面倒な操作が不要となる。

[0088] 上記実施例1では、ライセンスキーを認証情報とした場合において、その入力方法に応じた認証情報を自動的に生成することができる。したがって、例えば、上記認証情報を入力する情報処理端末の種別が異なることにより、その入力方法が異なる場合であっても、その異なる入力方法ごとにライセンスキーを生成するので、ユーザは、種別の異なる情報処理装置から、容易にライセンスキーを入力することができ、入力誤りの可能性を減らすことができる。

(実施例2)

図15は、本発明にかかる入力情報生成方法、情報処理装置、および情報処理プログラムを適用した情報処理システム1000のうち、実施例2における情報処理装置100の内部構成の一例を示すソフトウェア構成図である。実施例2では、上記したように、ライセンスキーに代えてユーザIDおよびパスワードを認証情報として入力する場合について説明するが、情報処理装置100の物理的な構成は図2(a)と同様であり、配信サーバ101については図5と同様である。したがって、以下ではこれらの説明については

省略している。

[0089] 図15に示すように、情報処理装置100は、図2(b)に示した場合と同様に、ROM203に、基本動作プログラム203aと、その他のプログラム203bとが記憶される。また、RAM204に、基本動作プログラム203aを実行するための基本動作実行プログラム204aと、ストレージ部210に記憶された認証情報照合プログラム210eを実行するための認証情報照合実行プログラム204dと、これらの実行プログラムの実行時に必要となる一時記憶領域204cとが記憶される。ストレージ部210に、認証情報照合プログラム210eと、その他のプログラム210cと、各種情報／データ記憶領域210dとが記憶される。各種情報／データ記憶領域210dには、配信サーバ101において生成された認証情報の一例であるユーザIDおよびパスワードを記憶する認証情報記憶領域210aを有している。

[0090] 本実施例においては、ストレージ部210に記憶された認証情報照合プログラム210eがRAM204にロードされ、認証情報照合実行プログラム204dが、情報処理装置100において生成された認証情報の一例であるユーザIDおよびパスワードを取得し、上記認証情報記憶領域210aに記憶する。なお、認証情報記憶領域210aは、RAM204の一時記憶領域204cに設けてもよい。認証情報照合実行プログラム204dの具体的な動作については後述する。

[0091] 図16(a)は、情報処理装置100においてユーザID及びパスワードを生成、登録する処理の処理手順を示すフローチャートである。図16(a)に示すように、情報処理装置100の認証情報照合実行プログラム204dは、操作器230がユーザから受け付けたユーザIDを読み取り、認証情報記憶領域210aに記憶させる(S1601)。同様に、認証情報照合実行プログラム204dは、操作器230がユーザから受け付けたパスワードを読み取り、認証情報記憶領域210aに記憶させる(S1602)。

[0092] 図16(b)は、図16(a)で登録したユーザIDおよびパスワードを

用いてウェブサイトやアプリケーションにログインする処理の処理手順を示すフローチャートである。図16(b)に示すように、情報処理装置100の認証情報照合実行プログラム204dは、ユーザIDおよびパスワードを入力してコンテンツを視聴するためのアプリケーションを起動する(S1603)。上記アプリケーションとしては、例えば、ウェブブラウザプログラムがある。

[0093] 操作器230がユーザIDおよびパスワードの入力を受け付けると(S1604)、認証情報照合実行プログラム204dは、図16(a)で登録したユーザIDおよびパスワードと、入力されたユーザIDおよびパスワードが一致するか否かを判定し(S1605)、両者が一致しないと判定した場合には(S1605; No)、S1602に戻って、以降の処理を繰り返す。

[0094] 一方、認証情報照合実行プログラム204dは、両者が一致すると判定した場合には(S1605; Yes)、ログインを完了して(S1606)、ウェブサイトやアプリケーションの利用を許可する。

[0095] 図17は、S1604において情報処理装置100のディスプレイ241に表示されるユーザIDおよびパスワードの入力画面の例を示す図である。図17に示すように、入力画面には、ユーザIDおよびパスワードの入力欄が設けられている。

[0096] 図18は、実施例2における第1認証情報生成処理の処理手順を示すフローチャートである。実施例2における第1認証情報生成処理のS1801～S1805までの処理は、図8に示したS801～S805までの処理と同様であるため、ここではその説明を省略し、S1806について説明する。

[0097] S1802の入力処理が終了すると、S1803において、情報処理装置100の認証情報照合実行プログラム204dは、上記入力処理で入力した文字が、S1801或いはS1804で認証情報として一つ前に決定した文字と同じグループに属する文字であるか否かを判定し(S1803)、両者が同じグループに属する文字であると判定した場合(S1803; Yes)

、その文字は入力できないことを示す警告を、スピーカ 251 から報知し、またはディスプレイ 241 に表示する。

[0098] 例えば、認証情報照合実行プログラム 204 d は、最初に決定した文字が「2」であり、次に入力された文字が「A」である場合、「「2」と「A」は同じグループのため、「2」に続いて「A」を入力することはできません。他のグループの中から選択して入力してください。」等、最初に決定した文字に続いて選択された文字が同じグループである旨および同じグループの文字は続けて入力できないため続いて入力する文字は他のグループから選択することを促す旨のメッセージを、スピーカ 251 から報知し、またはディスプレイ 241 に表示する。このとき、認証情報照合実行プログラム 204 d は、上記メッセージとともに、「5、J、K、L のグループの中から選択して入力してください。」というように、選択すべき他のグループをおすすめメッセージとして報知または表示してもよい。

[0099] このように、実施例 1 の場合と同様、1 つ前に並ぶ文字に続く文字が同じグループとならないように、認証情報を構成する各文字を決定する。したがって、ユーザ ID やパスワードを入力する場合でも、上記したようなカーソルの移動といった煩雑な操作が不要となり、容易な入力操作で認証情報を入力することができる。

[0100] なお、認証情報照合実行プログラム 204 d は、上記他のグループを選択する場合、同じグループではない任意のグループを選択することができる。しかし、例えば、認証情報照合実行プログラム 204 d が、過去にユーザが入力した文字およびその文字に続いて入力した文字と、これらの入力回数とを文字ごとに集計しておき、最初に入力した文字に続いて入力された文字の中で、続いて入力された文字の入力回数が多い文字を含むグループを、上記他のグループとして選択してもよい。この場合、ユーザによる入力頻度が高い文字を含むグループを、最初に入力した文字を含むグループに続くグループとして選択するので、ユーザは、日常使い慣れている操作で違和感なく文字を入力することができる。

- [0101] 図19は、実施例2における第2認証情報生成処理の処理手順を示すフローチャートである。実施例2における第2認証情報生成処理のS1901～S1905までの処理は、図10に示したS1001～S1005までの処理と同様であるため、ここではその説明を省略し、S1906について説明する。
- [0102] S1902の入力処理が終了すると、S1903において、情報処理装置100の認証情報照合実行プログラム204dは、上記入力処理で入力した文字が、S1901或いはS1904で認証情報として一つ前に決定した文字と同じフリック操作の向きの文字であるか否かを判定し（S1903）、両者が同じフリック操作の向きの文字でないと判定した場合（S1903；No）、その文字は入力できないことを示す警告を、スピーカ251から報知し、またはディスプレイ241に表示する。
- [0103] 例えば、認証情報照合実行プログラム204dは、最初に認証情報の文字として決定した文字が「B」であり、次に入力された文字が「3」である場合、「「B」と「3」は同じフリック操作の向きでないため、「B」に続いて「3」を入力することはできません。フリック操作の向きが同じ文字の中から選択して入力してください。」等、最初に決定した文字とその文字に続いて選択された文字とが同じフリック操作の向きでない旨およびフリック操作の向きが同じでない文字は続けて入力できないため続けて入力する文字はフリック操作の向きが同じ文字を選択することを促す旨のメッセージを、スピーカ251から報知し、またはディスプレイ241に表示する。このとき、認証情報照合実行プログラム204dは、上記メッセージとともに、「E、H、K、N、Q、U、Xの中から選択して入力してください。」というように、フリック操作が同じ向きの文字をおすすめメッセージとして報知または表示してもよい。
- [0104] このように、実施例1の場合と同様、認証情報の文字として決定した文字に続く文字を入力するためのフリック操作の向きが同じとなるように、認証情報を構成する各文字を決定する。したがって、ユーザIDやパスワードを

入力する場合でも、上記したような異なる向きのフリック操作といった煩雑な操作が不要となり、容易な入力操作で認証情報を入力することができる。

[0105] 図19に示した例では、上記フリック操作が同じ向きであれば煩雑な操作とならないことに着目し、その説明をした。しかし、実施例1の場合と同様、フリック操作により指が移動した向きにあるキーに配置されたグループの中から次の文字を入力することも可能である。実施例1と同様、ユーザIDやパスワードを入力する場合でも、このグループの中から上記次の文字を選択すると、より一層、入力操作が容易になる。

[0106] さらに、認証情報照合実行プログラム204dは、上記同じフリック操作の向きの文字を選択する場合、任意のグループの中からその文字を選択することができる。しかし、例えば、認証情報照合実行プログラム204dが、過去にユーザが入力した文字およびその文字に続いて入力した文字と、これらの入力回数とを文字ごとに集計しておき、最初に入力した文字に続いて入力された同じフリック操作の向きの文字のうち、入力回数が多い文字を続いて入力された文字として選択してもよい。この場合、ユーザによる入力頻度が高い同じフリック操作の向きの文字を、最初に入力した文字に続く文字として選択するので、ユーザは、日常使い慣れている操作で違和感なく文字を入力することができる。

[0107] 図20は、実施例2における第2認証情報生成処理の処理手順の変形例を示すフローチャートである。実施例2における第2認証情報生成処理の変形例のS2001～S2005までの処理は、図11に示したS1101～S1105までの処理と同様であるため、ここではその説明を省略し、S1106について説明する。

[0108] 図20に示すように、S2002の入力処理が終了すると、S2003において、情報処理装置100の認証情報照合実行プログラム204dは、上記入力処理で入力した文字が、S2001或いはS2004で認証情報として一つ前に決定した文字を入力したときのフリック操作の向きにあるキーのグループに含まれる文字であるか否かを判定し（S1103）、認証情報と

して一つ前に決定した文字を入力したときのフリック操作の向きにあるキーのグループに含まれる文字でないと判定した場合（S 2 0 0 3 ; N o）、その文字は入力できないことを示す警告を、スピーカ 2 5 1 から報知し、またはディスプレイ 2 4 1 に表示する。

[0109] 例えば、認証情報照合実行プログラム 2 0 4 d は、最初に決定した文字が「2」であり、次に選択された文字が「D」である場合、「「D」は「2」を入力したときのフリック操作の向きにあるキーのグループに含まれる文字でないため、「2」に続いて「D」を入力することはできません。フリック操作の向きにあるキーのグループに含まれる文字の中から選択して入力してください。」等、続いて入力された文字が最初に決定した文字とその文字を入力したときのフリック操作の向きにあるキーのグループに含まれる文字でない旨およびフリック操作の向きにあるキーのグループに含まれる文字でない文字は続けて入力できないため続いて入力する文字はフリック操作の向きにあるキーのグループに含まれる文字を選択することを促す旨のメッセージを、スピーカ 2 5 1 から報知し、またはディスプレイ 2 4 1 に表示する。このとき、認証情報照合実行プログラム 2 0 4 d は、上記メッセージとともに、「5、J、K、Lの中から選択して入力してください。」というように、フリック操作の向きにあるキーのグループに含まれる文字をおすすめメッセージとして報知または表示してもよい。

[0110] なお、実施例 1 の場合と同様、S 2 0 0 3 の処理では、認証情報照合実行プログラム 2 0 4 d は、次に入力される文字が、直前の文字が入力されたときのフリック操作の向きにあるキーに含まれる文字であるか否かを判定しており、必ずしも上記決定した文字と上記入力した文字とが隣接するグループに属していなくてもよい。

[0111] このように、実施例 1 の場合と同様、決定した文字に続く文字を、決定した文字を入力したときのフリック操作の向きにあるキーに属する文字の中から選択する。したがって、ユーザ I D やパスワードを入力する場合でも、上記したような異なる向きのフリック操作といった煩雑な操作が不要となり、

より一層、容易な入力操作で認証情報を入力することができる。

[0112] さらに、認証情報照合実行プログラム204dは、上記フリック操作の向きにあるキーのグループに含まれる文字を入力する場合、そのグループの中から任意の文字を選択することができる。しかし、例えば、認証情報照合実行プログラム204dが、過去にユーザが入力した文字およびその文字に続いて入力した文字と、これらの入力回数とを文字ごとに集計しておき、最初に入力した文字のフリック操作の向きにあるキーのグループに含まれる文字のうち、入力回数が多い文字を続いて入力された文字として選択してもよい。この場合、最初に入力した文字のフリック操作の向きにあるキーのグループの中からユーザによる入力頻度が高い文字を、最初に入力した文字に続く文字として選択するので、ユーザは、日常使い慣れている操作で違和感なく文字を入力することができる。

[0113] 図21は、実施例2における第3認証情報生成処理の処理手順を示すフローチャートである。実施例2における第3認証情報生成処理のS2101～S2105までの処理は、図12に示したS1201～S1205までの処理と同様であるため、ここではその説明を省略し、S2106について説明する。

[0114] S2102の入力処理が終了すると、S2103において、情報処理装置100の認証情報照合実行プログラム204dは、上記入力処理で入力した文字が、S2101或いはS2104で認証情報として一つ前に決定した文字と同じ回数のトグル操作で入力される文字であるか否かを判定し（S2103）、両者が同じ回数のトグル操作で入力される文字でないと判定した場合（S2103；No）、その文字は入力できないことを示す警告を、スピーカ251から報知し、またはディスプレイ241に表示する。

[0115] 例えば、認証情報照合実行プログラム204dは、最初に認証情報の文字として決定した文字が「B」であり、次に入力された文字が「D」である場合、「B」と「D」は同じ回数のトグル操作で入力される文字でないため、「B」に続いて「D」を入力することはできません。同じ回数のトグル操

作で入力される文字の中から選択して入力してください。」等、最初に決定した文字とその文字に続いて入力された文字とが同じ回数のトグル操作で入力される文字でない旨および同じ回数のトグル操作でない文字は続けて入力できないため続いて入力する文字は同じ回数のトグル操作で入力される文字を選択することを促す旨のメッセージを、スピーカ 251 から報知し、またはディスプレイ 241 に表示する。このとき、認証情報照合実行プログラム 204 d は、上記メッセージとともに、「E、H、K、N、Q、U、Xの中から選択して入力してください。」というように、同じ回数のトグル操作で入力される文字をおすすめメッセージとして報知または表示してもよい。

[0116] このように、実施例 1 の場合と同様、決定した文字に続く文字を入力するためのトグル操作の回数が同じとなるように、認証情報を構成する各文字を決定する。したがって、ユーザ ID やパスワードを入力する場合でも、タッチする回数が異なるトグル操作といった煩雑な操作が不要となり、同じリズムで入力操作ができ、容易な入力操作で認証情報を入力することができる。

[0117] なお、認証情報照合実行プログラム 204 d は、上記同じ回数のトグル操作で入力される文字を入力する場合、任意のグループの中からその文字を選択することができる。しかし、例えば、認証情報照合実行プログラム 204 d が、過去にユーザが入力した文字およびその文字に続いて入力した文字と、これらの入力回数とを文字ごとに集計しておき、最初に入力した文字に続いて入力された同じ回数のトグル操作で入力される文字のうち、入力回数が多い文字を続いて入力された文字として選択してもよい。この場合、ユーザによる入力頻度が高い同じフリック操作の向きの文字を、最初に入力した文字に続く文字として選択するので、ユーザは、日常使い慣れている操作で違和感なく文字を入力することができる。

[0118] また、実施例 2 の S1803 が Yes の場合、S1903 が No の場合、S2003 が No の場合、S2103 が No の場合に、警告をスピーカ 251 から報知し、またはディスプレイ 241 に表示することとしたが、実施例 1 の S803 が Yes の場合、S903 が No の場合、S1003 が No の

場合、S 1 1 0 3 が N o の場合にも同様の警告をスピーカ 2 5 1 から報知し、またはディスプレイ 2 4 1 に表示してもよい。

[0119] このように、本システムでは、ライセンスキー、ユーザ ID およびパスワード等の認証情報に限らず、あらかじめ定められた様々な入力情報について、その入力方法が異なる場合であっても、入力方法に応じて入力情報を生成することができる。

[0120] なお、上記実施例 1、実施例 2 では、ユーザが情報処理装置 1 0 0 の一例であるフィーチャーフォン、スマートフォン、リモコンを挙げたが、情報処理装置 1 0 0 がリモコンである場合には、例えば、図 2 2 に示すように、図 1 に示した構成とは異なる構成としてもよい。図 2 2 において、情報処理装置 1 0 0 にかわるリモコン 2 1 0 1 とテレビ 2 1 0 0 とが赤外線通信等の通信方法により通信し、テレビ 2 1 0 0 は、アンテナ 2 2 0 0 a を介して放送局 2 2 0 2 のアンテナ 2 2 0 0 t から番組等のコンテンツを受信する。もちろん、実施例 1 の場合と同様に、配信サーバ 1 0 1 から配信されるコンテンツを受信することもできる。したがって、このような環境下でも、リモコン 2 1 0 1 を情報処理装置 1 0 0 として利用することができる。

[0121] また、実施例 1、実施例 2 における各処理を実行するためのプログラムは、情報処理装置 1 0 0 やコンテンツ配信サーバ 1 0 1 にインストールされたプログラムを実行することにより実現されるが、これらのプログラムを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で C D - R O M、C D - R、D V D (Digital Versatile Disk) 等のコンピュータで読み取り可能な記録媒体に記録して提供したり、配布してもよい。さらには、上記プログラムを、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供したり、配布してもよい。

[0122] 例えば、図 3 (a) では、配信サーバ 1 0 1 が S 3 1 1 におけるライセンスキー生成処理を実行することとしたが、この処理を情報処理装置 1 0 0 が実行し、生成したライセンスキーを情報処理装置 1 0 0 の識別情報とともに

配信サーバ１００に送信し、記憶させて管理してもよい。この場合、情報処理装置１００がライセンスキーを生成するので、配信サーバ１０１の負荷を低減させることができ、視聴者の多いコンテンツを配信する場合ほど、その効果が期待できる。

符号の説明

[0123]	１０００	情報処理システム
	１００	情報処理装置
	１０１	配信サーバ
	１０２	ネットワーク
	１０３	アクセスポイント装置
	１０４	移動体サーバ
	１０５	基地局
	２０１	ＣＰＵ
	２０２	システムバス
	２０３	ＲＯＭ
	２０３ a	基本動作プログラム
	２０３ b	その他のプログラム
	２０４	ＲＡＭ
	２０４ a	基本動作実行プログラム
	２０４ b	サーバ情報取得実行プログラム
	２０４ c	一時記憶領域
	２０４ d	認証情報照合実行プログラム
	２１０	ストレージ
	２１０ a	認証情報記憶領域
	２１０ b	サーバ情報取得プログラム
	２１０ c	その他のプログラム
	２１０ d	各種情報／データ記憶領域
	２１０ e	認証情報照合プログラム

2 2 0	通信処理器
2 3 0	操作器
2 4 0	ビデオプロセッサ
2 5 0	オーディオプロセッサ
2 6 0	センサ
5 0 3	R A M
5 0 3 a	基本動作実行プログラム
5 0 3 b	コンテンツ管理/配信実行プログラム
5 0 3 c	認証情報発生実行プログラム
5 0 3 d	認証情報照合実行プログラム
5 0 4 a	基本動作プログラム
5 0 4 b	コンテンツ管理/配信プログラム
5 0 4 c	コンテンツ
5 0 4 d	認証情報発生プログラム
5 0 4 e	認証情報照合プログラム
5 0 5	L A N通信器。

請求の範囲

- [請求項1] 複数の文字を含む入力情報を生成する入力情報生成方法であって、
操作部から入力される前記文字の入力方法を判定し、
判定した前記文字の入力方法に応じて前記入力情報を生成する、
ことを特徴とする入力情報生成方法。
- [請求項2] 前記判定において、前記文字のうち、先に入力された文字と、続いて入力された文字とが、入力キーに割り当てられた同じグループに属する文字であるか否かを判定し、両者が同じグループに属しないと判定した場合に、前記入力情報を生成する、
ことを特徴とする請求項1に記載の入力情報生成方法。
- [請求項3] 前記判定において、前記文字のうち、先に入力された文字と、続いて入力された文字とが、同じ向きのフリック操作で入力された文字であるか否かを判定し、同じ向きのフリック操作で入力された文字であると判定した場合に、前記入力情報を生成する、
ことを特徴とする請求項1に記載の入力情報生成方法。
- [請求項4] 前記判定において、前記文字のうち、続いて入力された文字が、先に入力された文字を入力したときのフリック操作の向きにある入力キーに割り当てられたグループに属する文字であるか否かを判定し、前記続いて入力された文字が前記グループに属する文字であると判定した場合に、前記入力情報を生成する、
ことを特徴とする請求項1に記載の入力情報生成方法。
- [請求項5] 前記判定において、前記文字のうち、先に入力された文字と、続いて入力された文字とが、同じ回数のトグル操作で入力されたか否かを判定し、同じ回数のトグル操作で入力されたと判定した場合に、前記入力情報を生成する、
ことを特徴とする請求項1に記載の入力情報生成方法。
- [請求項6] 前記判定において、前記入力方法に応じて入力していないと判定した場合、前記操作部に警告を出力する、

ことを特徴とする請求項 1 に記載の入力情報生成方法。

[請求項7] 前記判定において、前記文字のうち、先に入力された文字に続いて入力する文字として、過去に入力した前記続いて入力する文字の中から、入力頻度が高い文字を選択する、

ことを特徴とする請求項 1 に記載の入力情報生成方法。

[請求項8] 複数の文字を含む入力情報を生成する情報処理装置であって、
操作部から入力される前記文字の入力方法を判定する第 1 の処理部と、

判定した前記文字の入力方法に応じて前記入力情報を生成する第 2 の処理部と、

を備えることを特徴とする情報処理装置。

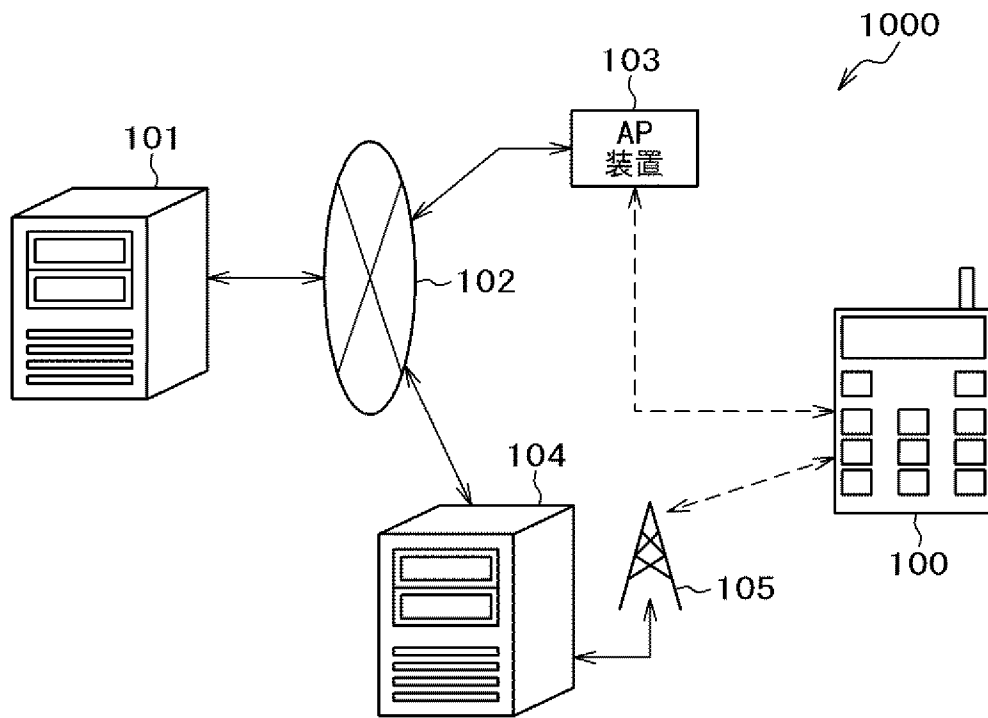
[請求項9] コンピュータに、
操作部から入力される入力情報を含む複数の文字の入力方法を判定する第 1 の処理と、

判定した前記文字の入力方法に応じて前記入力情報を生成する第 2 の処理と、

を実行させることを特徴とする情報処理プログラム。

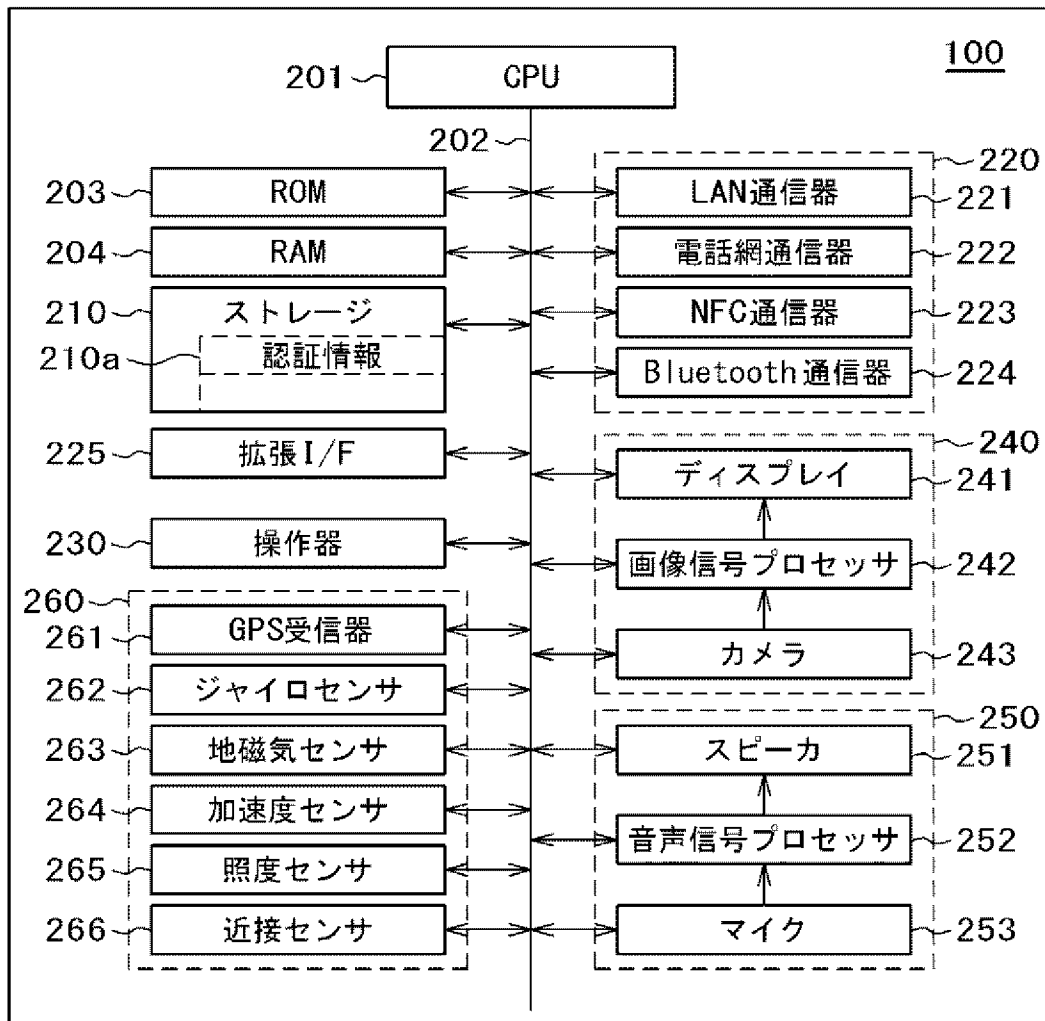
[図1]

図 1



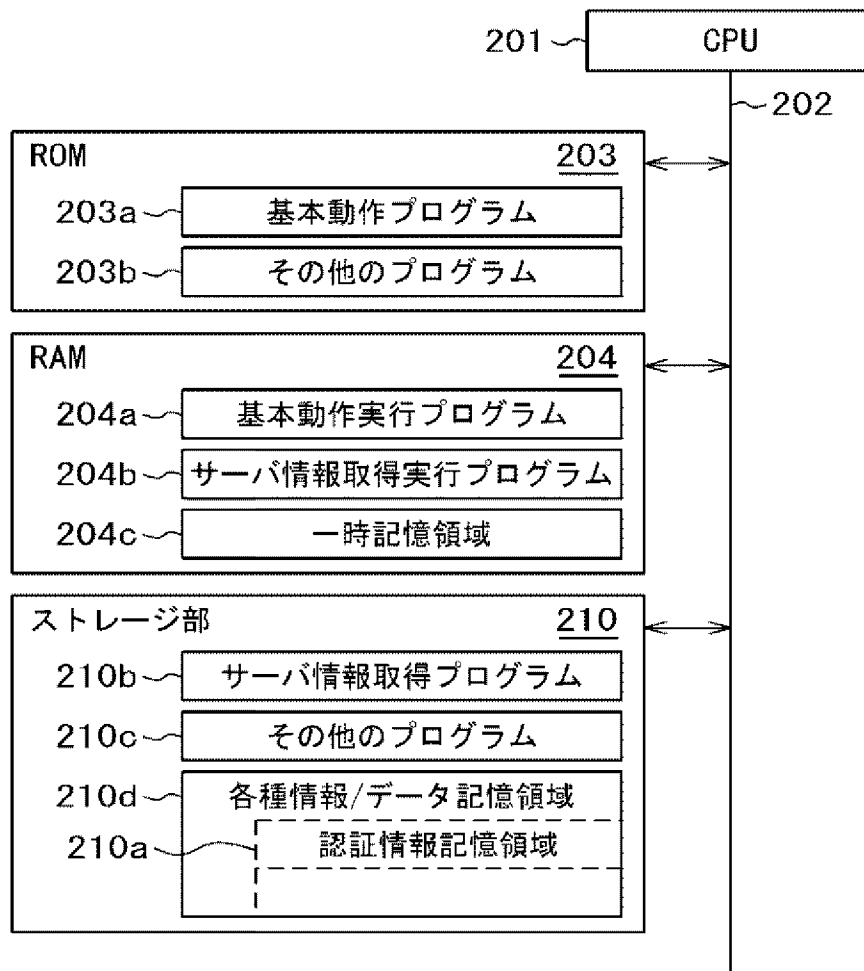
[図2(a)]

図 2 (a)



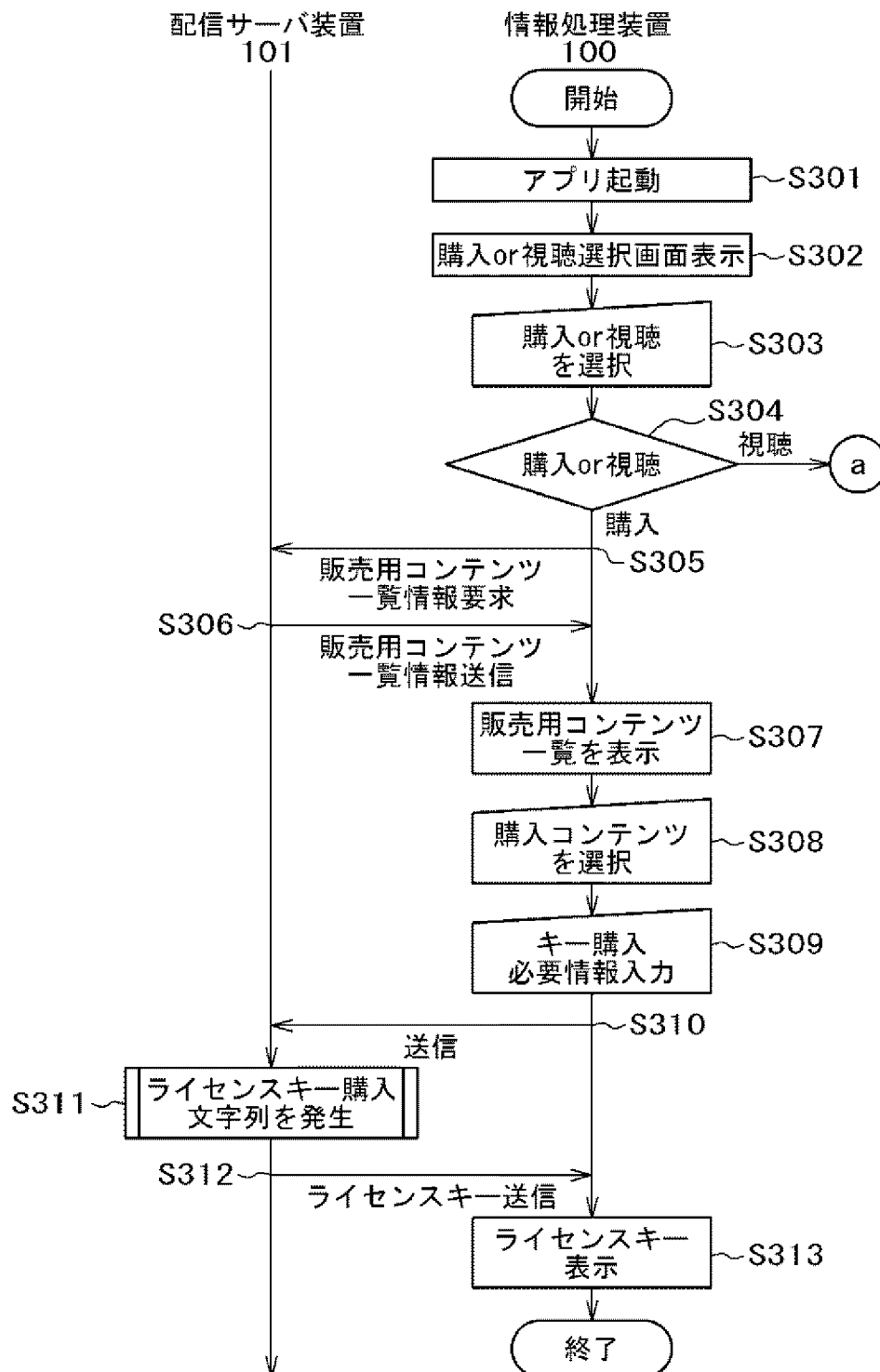
[図2(b)]

図 2 (b)



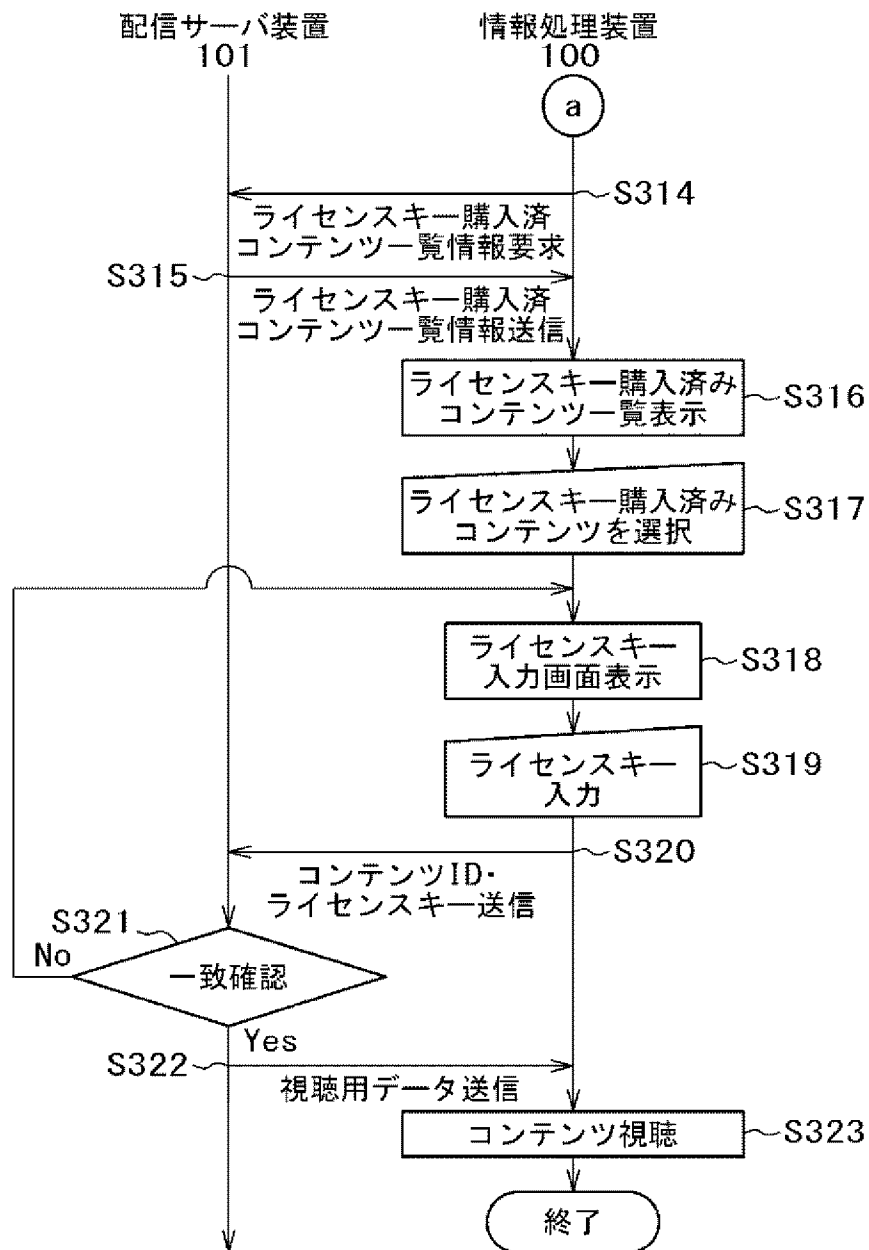
[図3(a)]

図 3 (a)



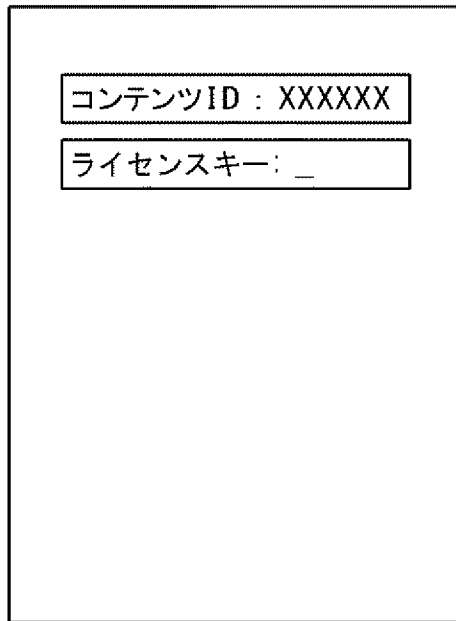
[図3(b)]

図 3 (b)



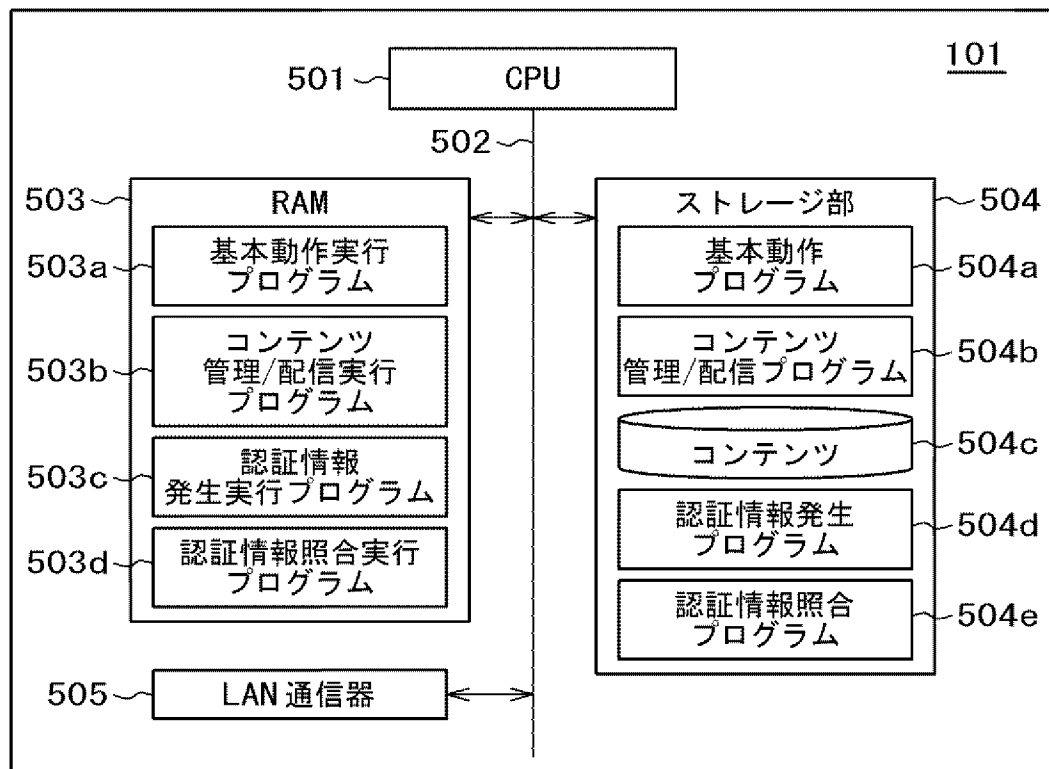
[図4]

図 4



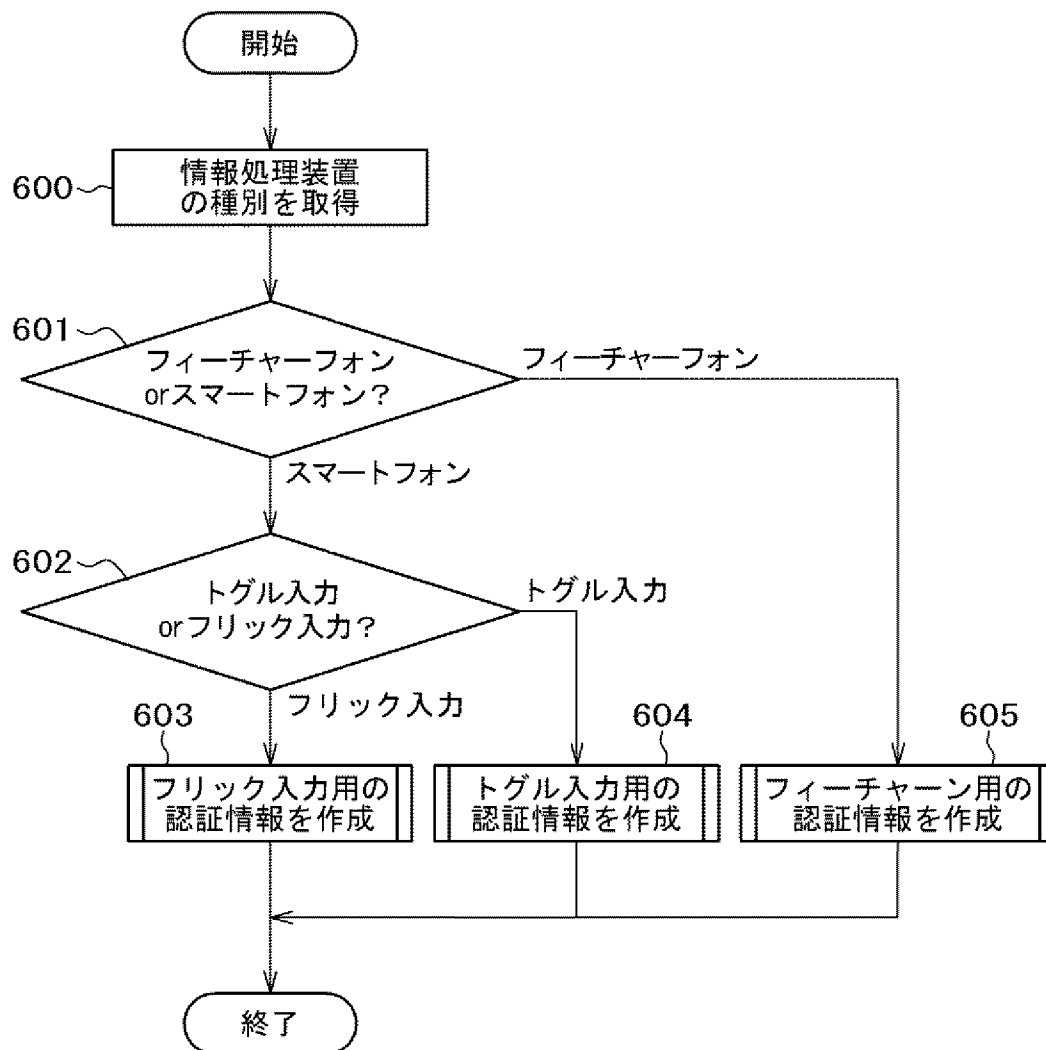
[図5]

図 5



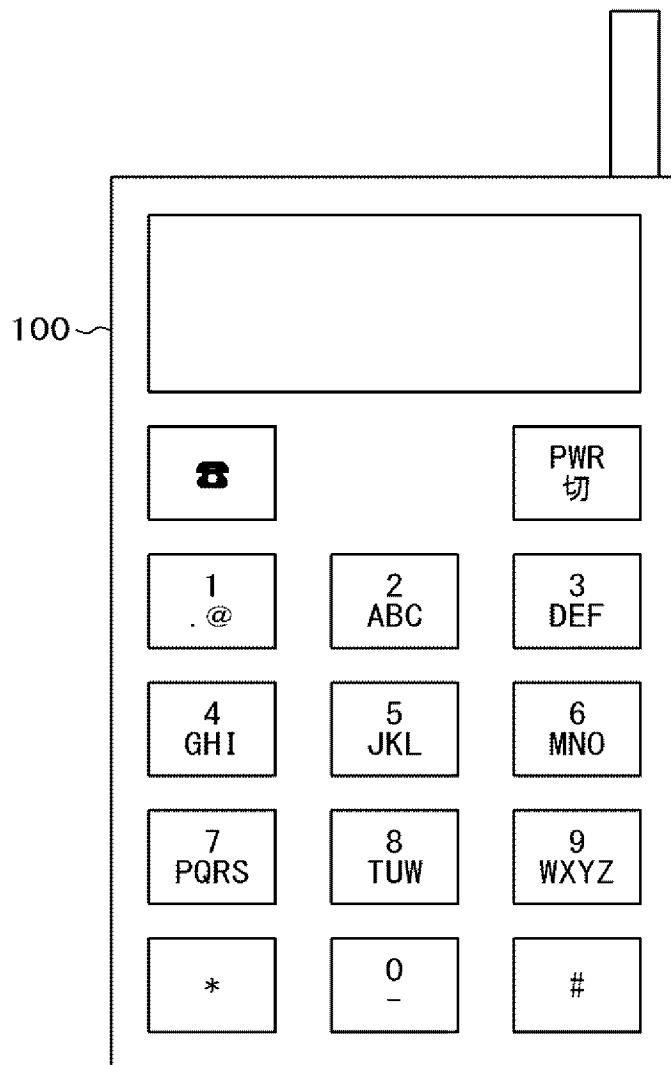
[図6]

図 6



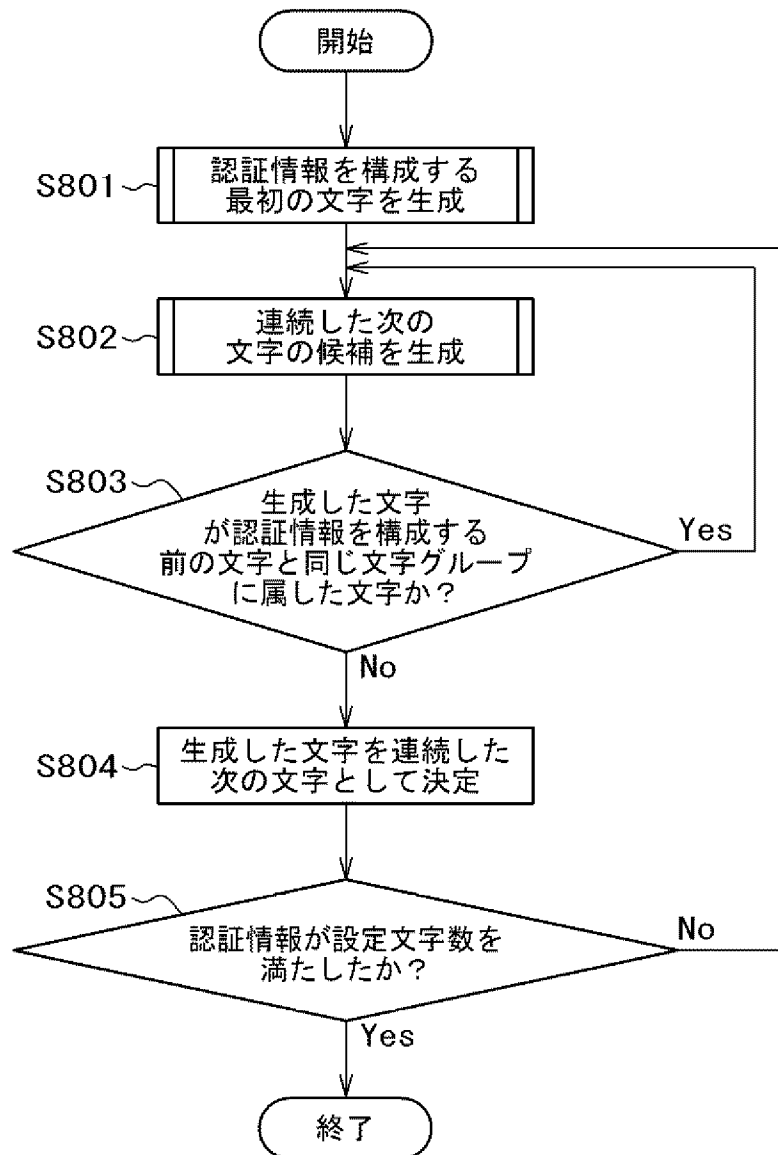
[図7]

図 7



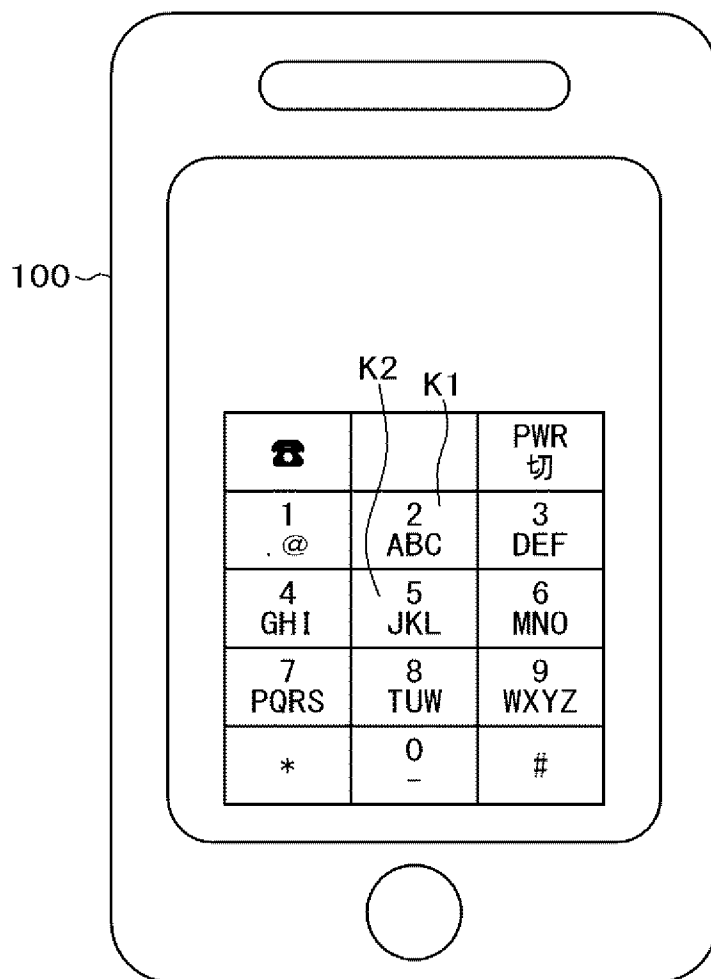
[図8]

図 8



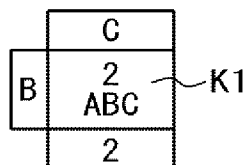
[図9(a)]

図 9 (a)



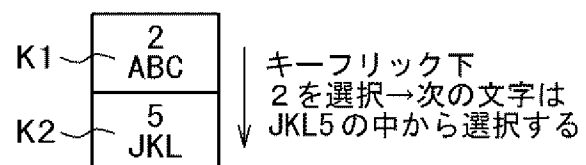
[図9(b)]

図 9 (b)



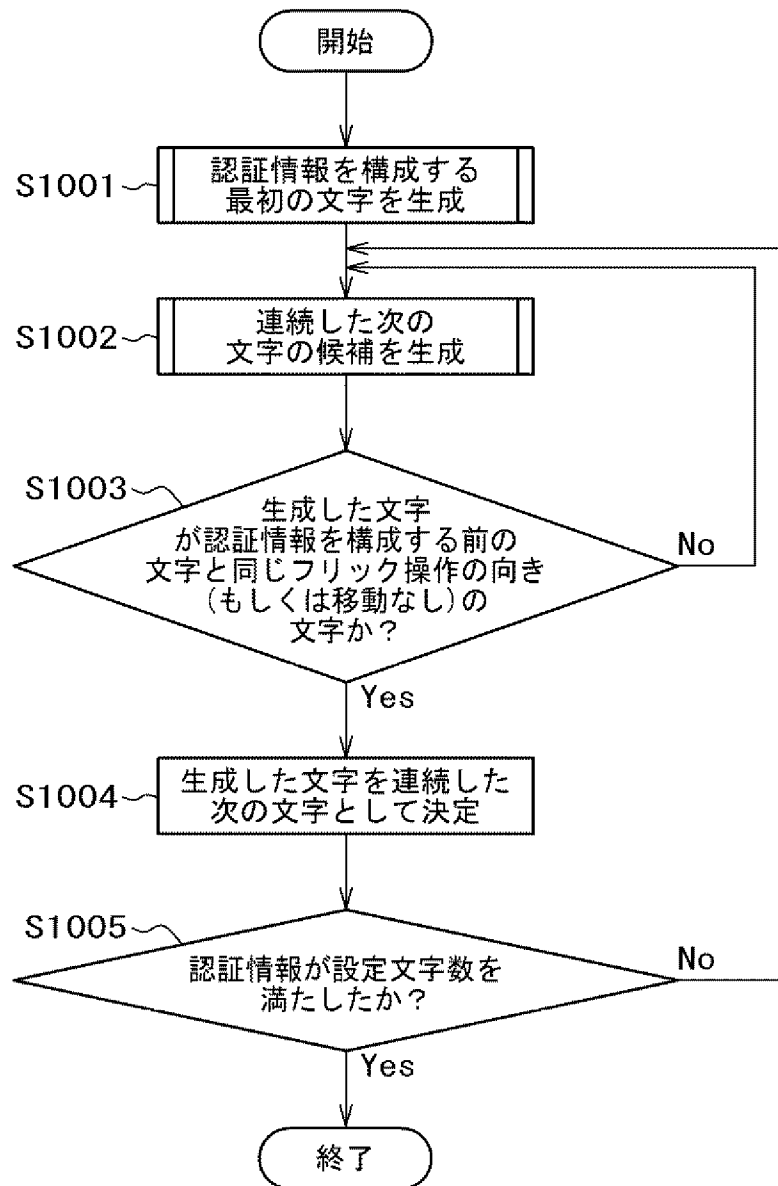
[図9(c)]

図 9 (c)



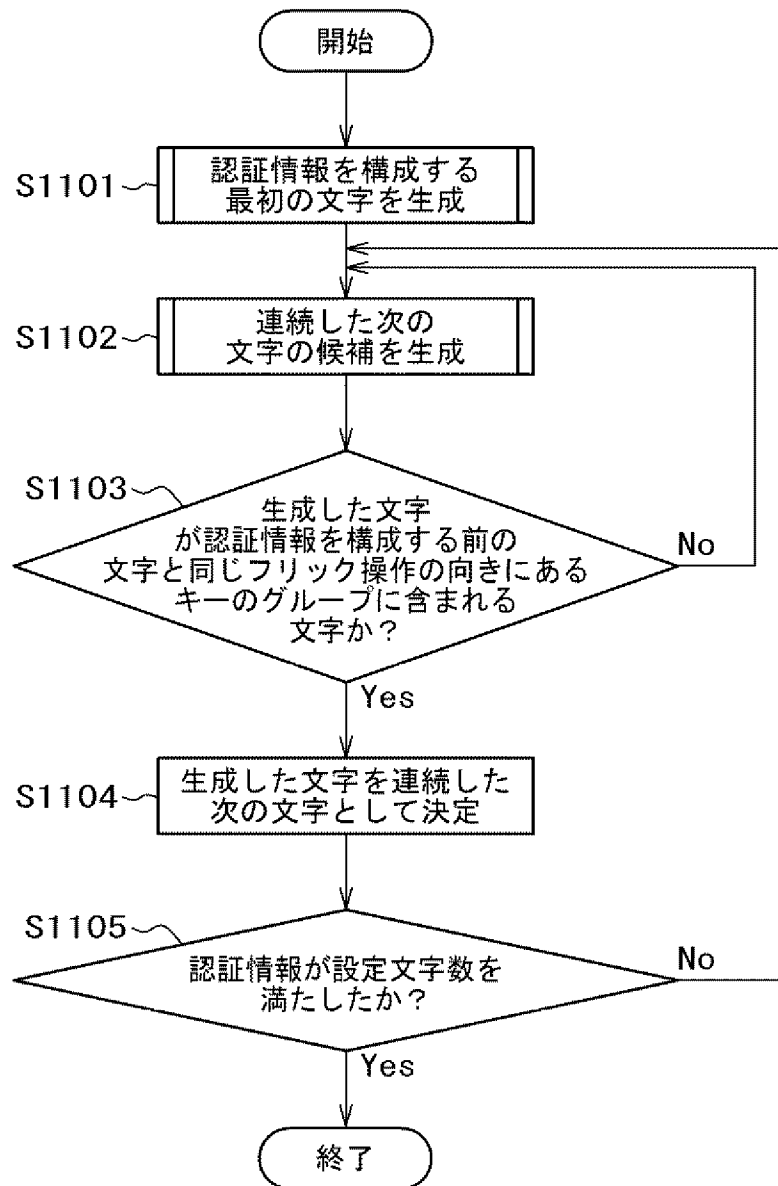
[図10]

図 10



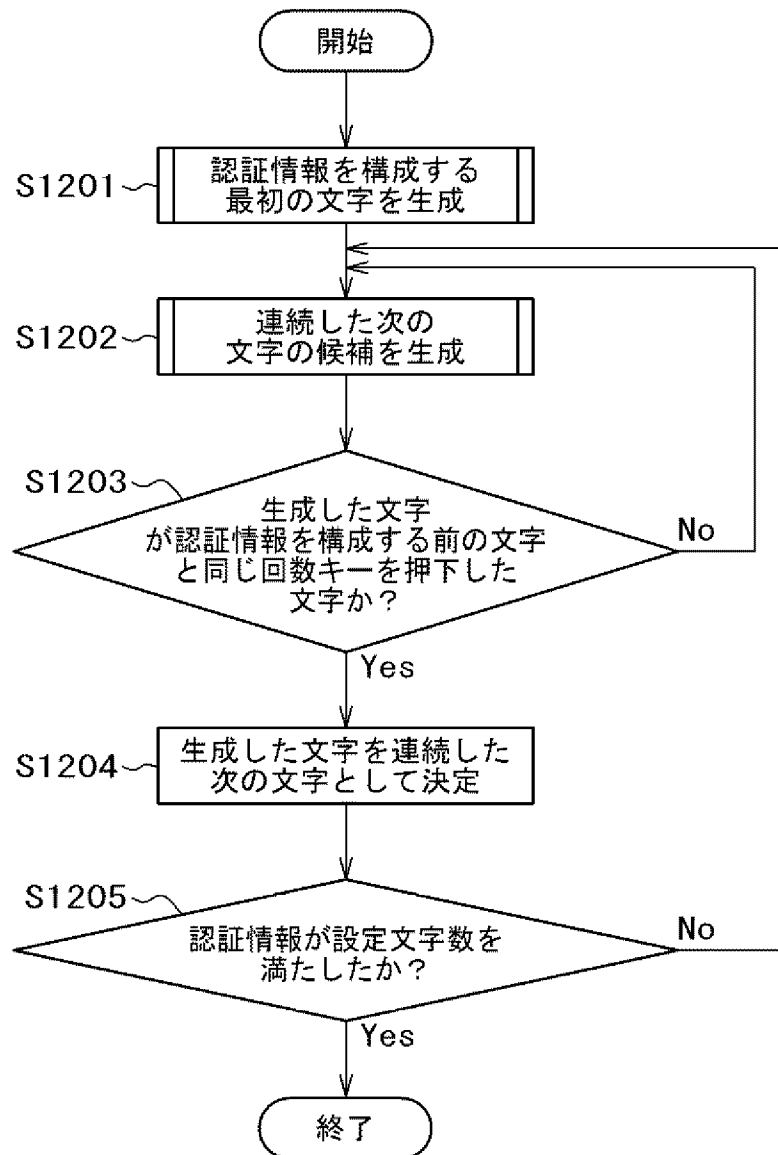
[図11]

図 1 1



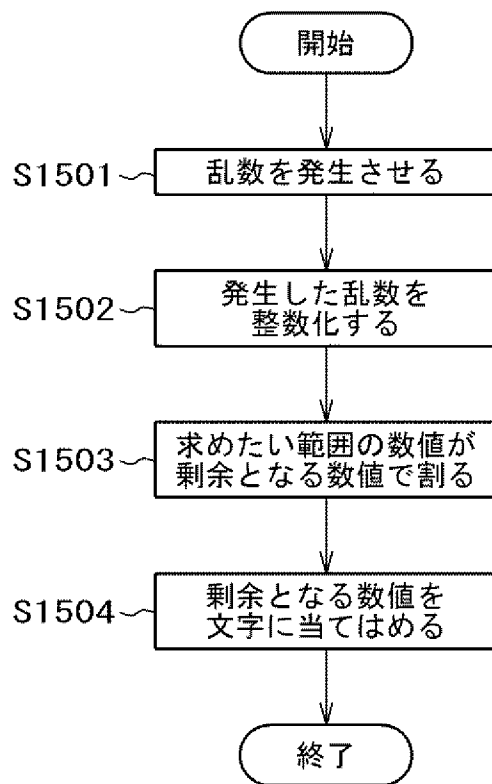
[図12]

図 1 2



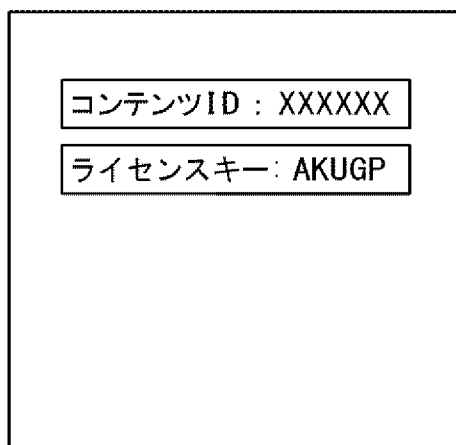
[図13]

図 1 3



[図14(a)]

図 1 4 (a)



[図14(b)]

図 1 4 (b)

コンテンツID : XXXXXX
ライセンスキー: BENKH

[図14(c)]

図 1 4 (c)

コンテンツID : XXXXXX
ライセンスキー: 2K4SV

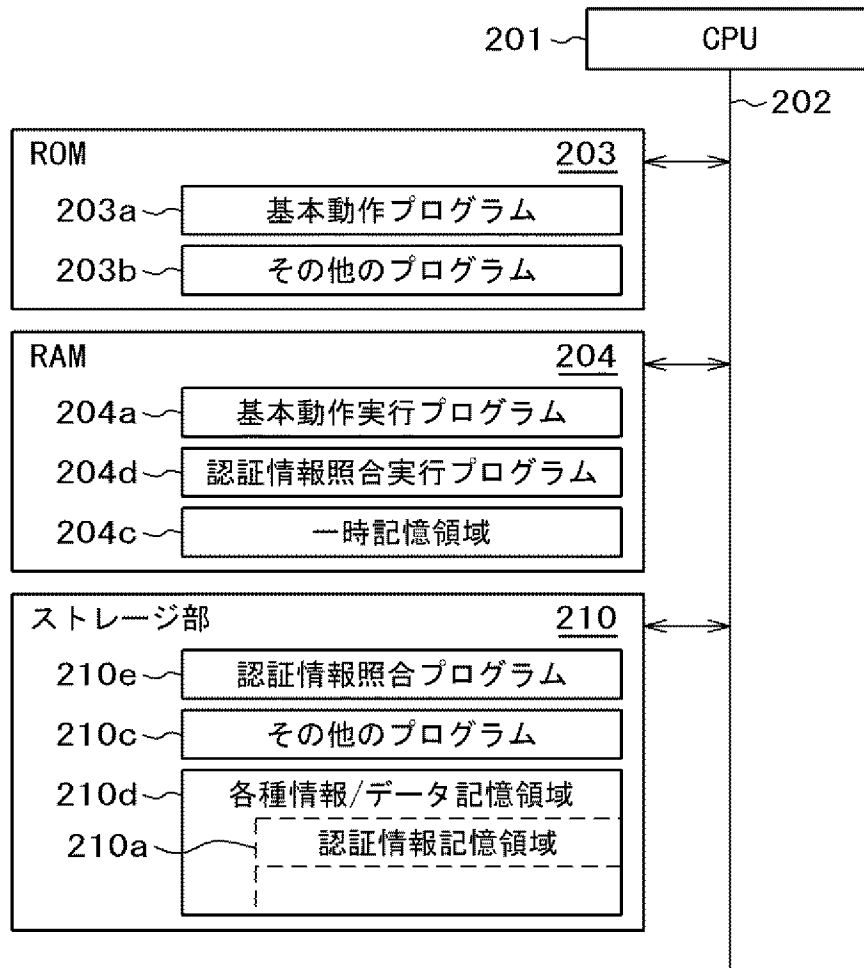
[図14(d)]

図 1 4 (d)

コンテンツID : XXXXXX
ライセンスキー: BKUHQ

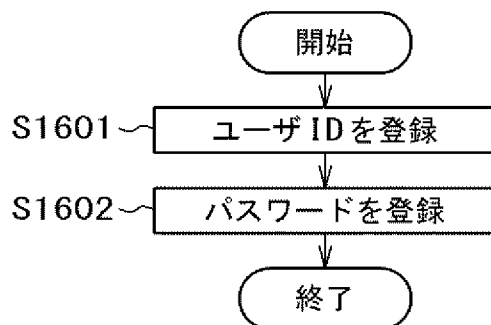
[図15]

図 1 5



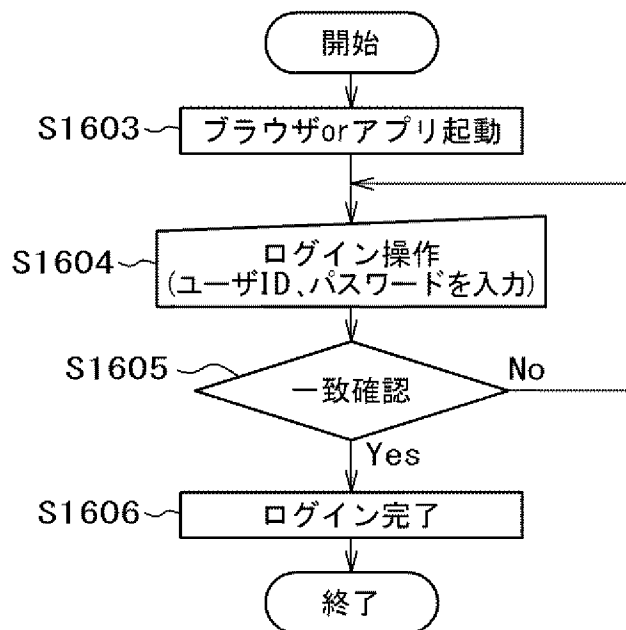
[図16(a)]

図 1 6 (a)



[図16(b)]

図 1 6 (b)



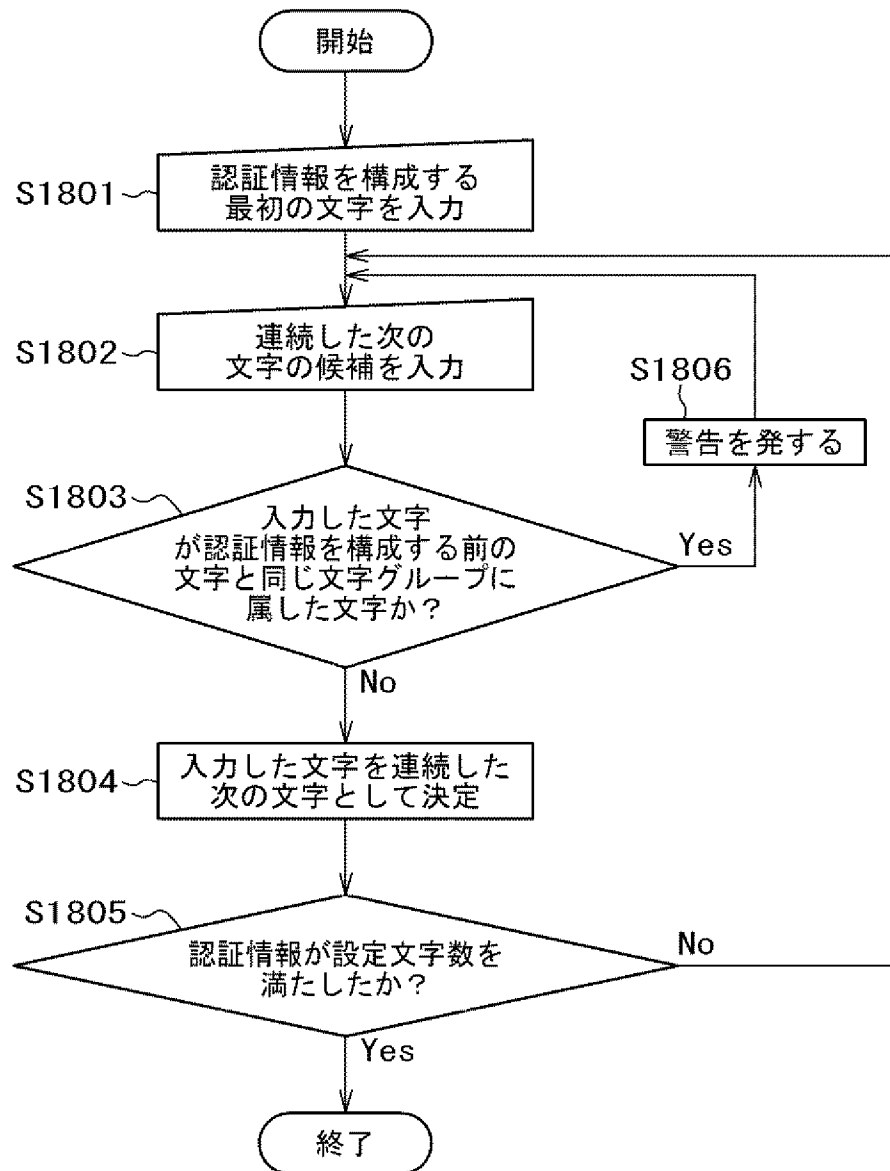
[図17]

図 1 7

ユーザID : _
パスワードPWD : _

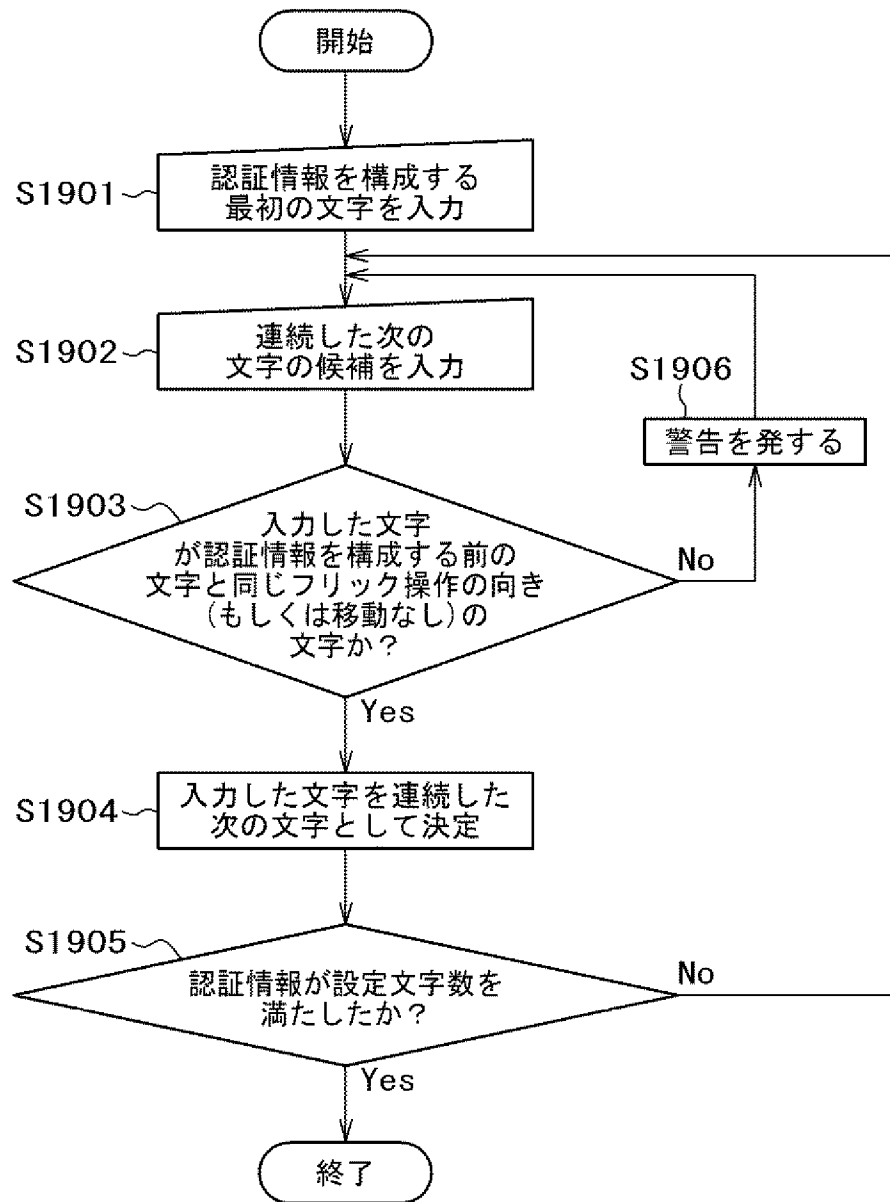
[図18]

図 1 8



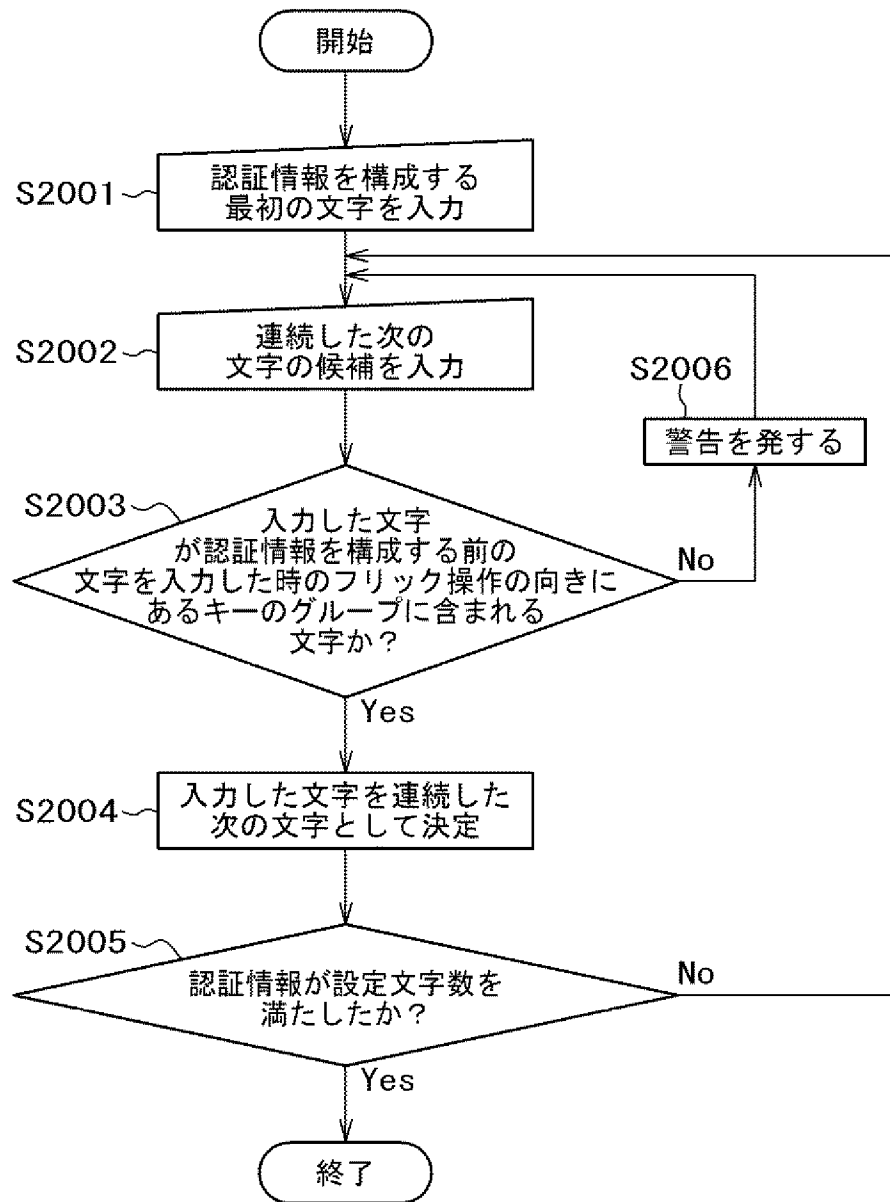
[図19]

図 19



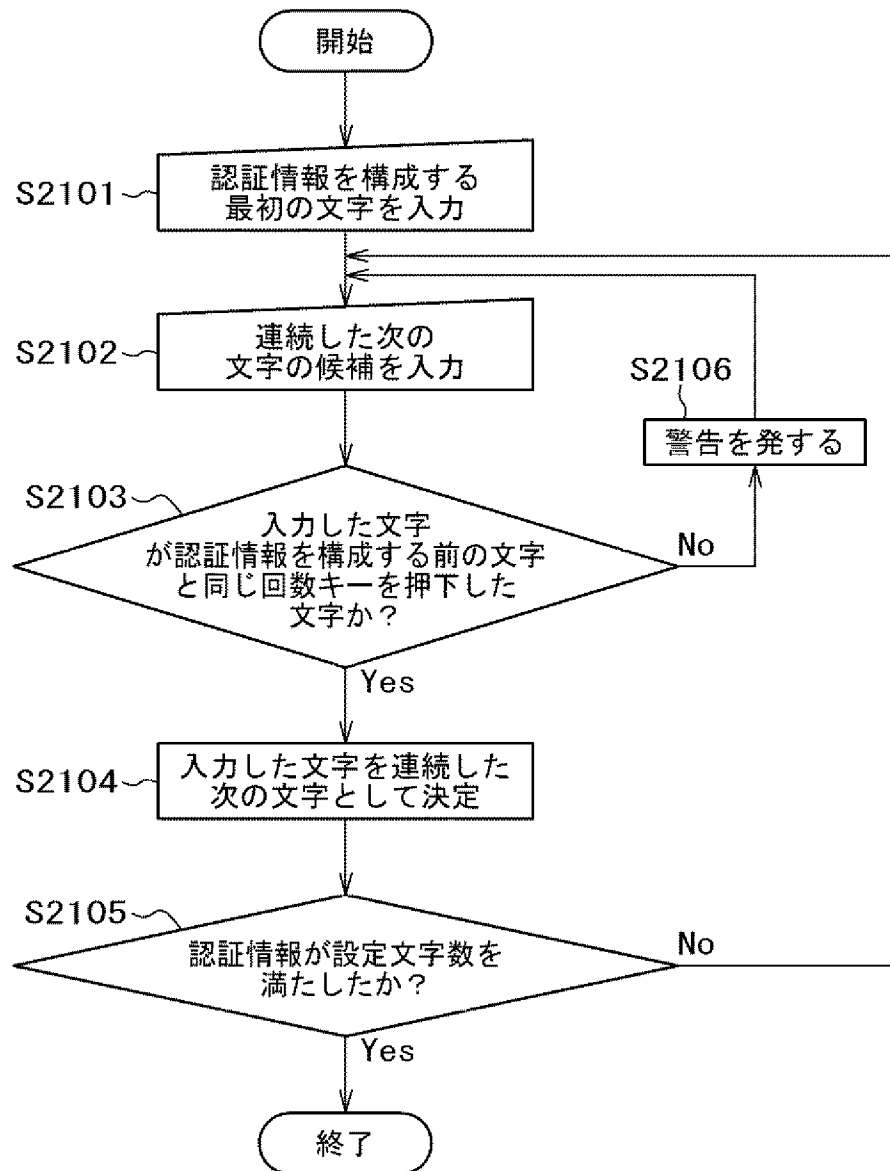
[図20]

図 20



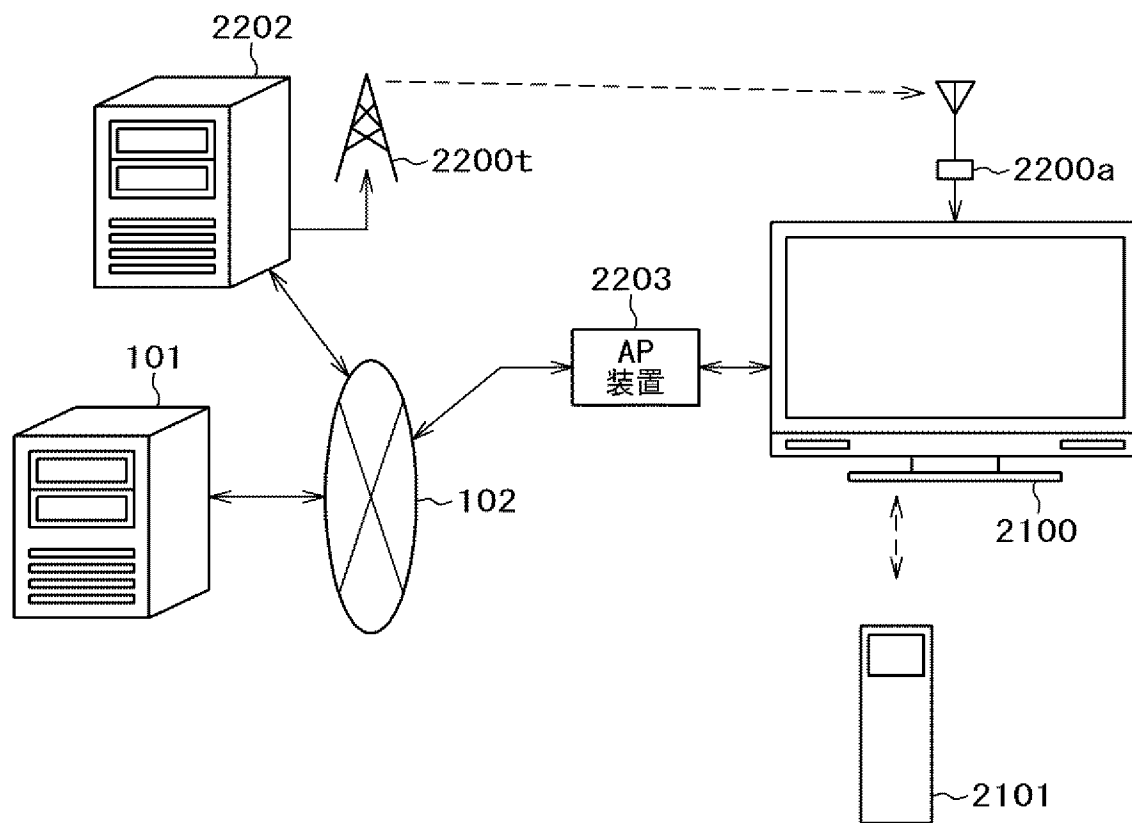
[図21]

図 2 1



[図22]

図 2 2



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2015/086223

A. CLASSIFICATION OF SUBJECT MATTER

G06F3/0488(2013.01)i, G06F3/023(2006.01)i, G06F3/0489(2013.01)i,
H03M11/04(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)

G06F3/0488, G06F3/023, G06F3/0489, H03M11/04

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.
Y A	JP 2004-139327 A (Avex Network Inc.), 13 May 2004 (13.05.2004), paragraph [0036] (Family: none)	1, 6-9 2-5
Y	JP 2015-176268 A (Toshiba Corp.), 05 October 2015 (05.10.2015), paragraph [0041] & US 2015/0261949 A1 paragraph [0057]	1, 6-9
Y	Hiroyuki INABA et al., "Notes on Secure and Smooth Typing Password Generation Method Using Markov Process(2)", IPSJ SIG Notes Security Psychology & Trust (SPT) 2014-SPT-010 [online], 26 June 2014 (26.06.2014), 2014-SPT-10 42, pages 1 to 6	7

☐ 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
24 February 2016 (24.02.16)

Date of mailing of the international search report
08 March 2016 (08.03.16)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F3/0488(2013.01)i, G06F3/023(2006.01)i, G06F3/0489(2013.01)i, H03M11/04(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（I P C））

Int.Cl. G06F3/0488, G06F3/023, G06F3/0489, H03M11/04

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 6 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 6 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 6 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
Y	JP 2004-139327 A (エイベックス ネットワーク株式会社)	1, 6-9
A	2004.05.13, [0036] (ファミリーなし)	2-5
Y	JP 2015-176268 A (株式会社東芝) 2015.10.05, [0041] & US 2015/0261949 A1 [0057]	1, 6-9

☒ 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

2 4 . 0 2 . 2 0 1 6

国際調査報告の発送日

0 8 . 0 3 . 2 0 1 6

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

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）

原 秀人

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 2 1

5 E

9 6 4 4

C (続き) . 関連すると認められる文献		
引用文献の カテゴリ*	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	稲葉 宏幸 外, マルコフ過程を用いた安全かつ入力が容易なパスワード生成法に関する考察 (2), 情報処理学会 研究報告 セキュリティ心理学とトラスト (SPT) 2014-SPT-010 [online], 2014.06.26, 2014-SPT-10 42, pp. 1-6	7