

(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
2022年3月17日(17.03.2022)



(10) 国際公開番号

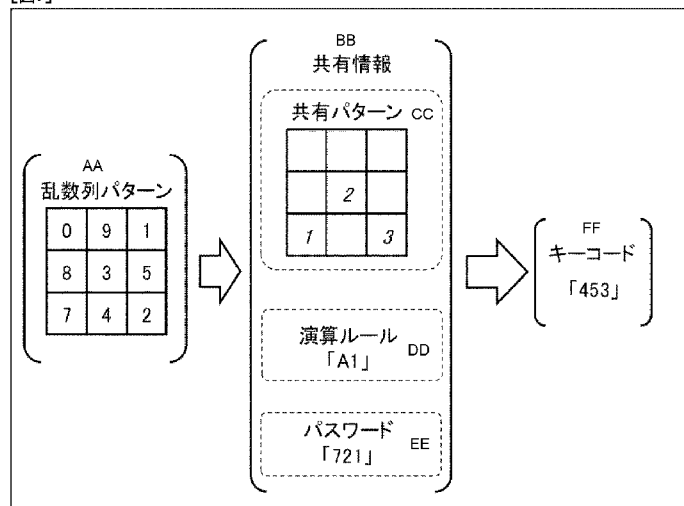
WO 2022/054519 A1

- (51) 国際特許分類:
G06F 21/31 (2013.01)
- (21) 国際出願番号: PCT/JP2021/030279
- (22) 国際出願日: 2021年8月19日(19.08.2021)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2020-153425 2020年9月14日(14.09.2020) JP
- (71) 出願人: NECプラットフォームズ株式会社
(NEC PLATFORMS, LTD.) [JP/JP]; 〒2138511
神奈川県川崎市高津区北見方二丁目
6番1号 Kanagawa (JP).
- (72) 発明者: 奥村 藤男 (OKUMURA Fujio);
〒2138511 神奈川県川崎市高津区北見方二
丁目6番1号 NECプラットフォーム
ズ株式会社内 Kanagawa (JP).
- (74) 代理人: 北嶋 啓至, 外 (KITAJIMA Hiroshi et
al.); 〒1088001 東京都港区芝五丁目7番1号 日
本電気株式会社 知的財産本部 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, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, KE, KG, KH,
KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,
MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

(54) Title: AUTHENTICATION DEVICE, AUTHENTICATION METHOD, AND RECORDING MEDIUM

(54) 発明の名称: 認証装置、認証方法、および記録媒体

[図7]



AA Random number sequence pattern
BB Shared information
CC Shared pattern
DD Computation rule
EE Password
FF Key code

(57) Abstract: An authentication device comprising: a storage unit in which shared information that includes passwords previously set for each user and shared rules is stored in order to prevent the leakage of authentication information such as passwords; a random number sequence generation unit for generating a random number sequence pattern configured from a plurality of different numerals; a computation unit for generating a key code on the basis of the shared rules, using a plurality of provisional numerals selected from the random number sequence pattern and a plurality of secret numerals constituting passwords; a transceiver for receiving identification information of a user to be authenticated from an input terminal operated by the user to be authenticated, transmitting the random number sequence pattern in association with the identification information to the input terminal, and receiving, from the input terminal, a key code that is composed of the

NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, 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:

- 一 国際調査報告(条約第21条(3))

numerals selected on the basis of the shared rules from the random number sequence pattern by the user to be authenticated; and an authentication unit for authenticating the user to be authenticated, on the basis of the key code received from the input terminal and the key code generated by the computation unit.

(57) 要約: パスワード等の認証情報の漏洩を防止するために、ユーザごとに予め設定されたパスワードおよび共有ルールを含む共有情報が記憶される記憶部と、複数の異なる数字によって構成される乱数列パターンを生成する乱数列生成部と、共有ルールに基づいて、乱数列パターンから選択された複数の仮数字と、パスワードを構成する複数の秘密数字とを用いてキーコードを生成する演算部と、認証対象ユーザの操作する入力端末から認証対象ユーザの識別情報を受信し、乱数列パターンを識別情報に対応付けて入力端末に送信し、認証対象ユーザによって共有ルールに基づいて乱数列パターンから選択された数字からなるキーコードを入力端末から受信する送受信部と、入力端末から受信されたキーコードと、演算部によって生成されたキーコードとに基づいて、認証対象ユーザを認証する認証部と、を備える認証装置とする。

明 細 書

発明の名称： 認証装置、認証方法、および記録媒体

技術分野

[0001] 本開示は、認証情報を用いて認証を行う認証装置等に関する。

背景技術

[0002] 公共の場に設置されたＡＴＭ（Automatic Teller Machine）などの認証システムには、パスワードや暗証番号などの認証情報を入力するための入力端末が設置されている。例えば、認証システムの利用者は、入力端末のタッチパネルに表示されたテンキーに従って認証情報を入力する。一般的な入力端末では、利用者が入力装置に認証情報を入力している際に、第三者によって認証情報が覗き見られる可能性がある。

[0003] 特許文献１には、他人に容易に暗証番号を知られることなく、確実にユーザ本人を認証することを目的とする個人認証方法について開示されている。まず、特許文献１の方法では、認証対象のユーザからのユーザＩＤ（Identifier）の入力に応答してランダム数字を生成する。次に、特許文献１の方法では、ユーザから入力される第１暗証番号とランダム数字とから特定の計算方法により算出される第１文字列を取得する。次に、特許文献１の方法では、複数のユーザＩＤに対応付けられた第２暗証番号と第２ランダム数字とから第２文字列を算出する。そして、特許文献１の方法では、第１文字列と第２文字列とを比較することにより、ユーザの認証を行う。

[0004] 特許文献２には、ワンタイムパスワードシステムにおいて、第三者へのキーの漏洩を防止することを目的とする電子認証装置について開示されている。まず、顧客を管理するホストコンピュータは、顧客の端末に所定の乱数データを送信する。顧客の端末は、ディスプレイ上に２次元に配列された所定の乱数データの任意の位置に重ねられた、ホストコンピュータと共有する所定形状の暗号鍵に基づいてパスワードを生成する。顧客の端末は、生成されたパスワードをホストコンピュータに送信する。ホストコンピュータは、デ

ィスプレイ上に２次元に配列された所定の乱数データに所定形状の暗号鍵を重ね合わせ、複数の選択可能なデータ列を生成する。ホストコンピュータは、顧客の端末から受信されたパスワードと、生成された複数のデータ列とを比較し、一致するものがあるときは、受信したデータ列は顧客の端末から送信されたパスワードと判定し、顧客の認証を行う。

先行技術文献

特許文献

[0005] 特許文献１：特開２００６－１４６３２７号公報

特許文献２：特開２００１－００５７８５号公報

発明の概要

発明が解決しようとする課題

[0006] 特許文献１の手法では、携帯端末計算部による解読不能文字列の計算のために、ユーザが第１暗証番号を携帯端末部に入力する。このとき、第三者によって、携帯端末部の画面に入力された暗証番号を覗き込まれる可能性があった。

[0007] 特許文献２の手法では、所定形状の暗号鍵に基づくキーの入力順番が固定されている。そのため、第三者によって、端末を介したパスワードの入力が複数回の覗き込まれると、キーの入力順番が漏洩する可能性があった。

[0008] 本開示の目的は、パスワード等の認証情報の漏洩を防止できる認証装置等を提供することにある。

課題を解決するための手段

[0009] 本開示の一態様の認証装置は、ユーザごとに予め設定されたパスワードおよび共有ルールを含む共有情報が記憶される記憶部と、認証対象ユーザの認証機会ごとに、複数の異なる数字によって構成される乱数列パターンを生成する乱数列生成部と、共有ルールに基づいて、乱数列パターンから複数の仮数字を選択し、選択された複数の仮数字と、パスワードを構成する複数の秘密数字とを用いてキーコードを生成する演算部と、認証対象ユーザの認証機

会において、認証対象ユーザの操作する入力端末から認証対象ユーザの識別情報を受信し、認証対象ユーザの認証機会に生成された乱数列パターンを識別情報に対応付けて入力端末に送信し、認証対象ユーザによって共有ルールに基づいて乱数列パターンから選択された数字からなるキーコードを入力端末から受信する送受信部と、入力端末から受信されたキーコードと、演算部によって生成されたキーコードとに基づいて、認証対象ユーザを認証する認証部と、を備える。

[0010] 本開示の一態様の認証方法においては、ユーザごとに予め設定されたパスワードおよび共有ルールを含む共有情報を記憶部に記憶しておき、認証対象ユーザの操作する入力端末から認証対象ユーザの識別情報を受信し、認証対象ユーザの識別情報の受信に応じて、複数の異なる数字によって構成される乱数列パターンを生成し、生成された乱数列パターンを識別情報に対応付けて入力端末に送信し、共有ルールに基づいて、乱数列パターンから複数の仮数字を選択し、選択された複数の仮数字と、パスワードを構成する複数の秘密数字とを用いてキーコードを生成し、共有ルールに基づいて認証対象ユーザによって乱数列パターンから選択された数字からなるキーコードを入力端末から受信し、入力端末から受信されたキーコードと、自装置で生成されたキーコードとに基づいて、認証対象ユーザを認証する。

[0011] 本開示の一態様のプログラムは、ユーザごとに予め設定されたパスワードおよび共有ルールを含む共有情報を記憶部に記憶しておく処理と、認証対象ユーザの操作する入力端末から認証対象ユーザの識別情報を受信する処理と、認証対象ユーザの識別情報の受信に応じて、複数の異なる数字によって構成される乱数列パターンを生成する処理と、生成された乱数列パターンを識別情報に対応付けて入力端末に送信する処理と、共有ルールに基づいて、乱数列パターンから複数の仮数字を選択する処理と、選択された複数の仮数字と、パスワードを構成する複数の秘密数字とを用いてキーコードを生成する処理と、共有ルールに基づいて認証対象ユーザによって乱数列パターンから選択された数字からなるキーコードを入力端末から受信する処理と、入力端

末から受信されたキーコードと、自装置で生成されたキーコードとに基づいて、認証対象ユーザを認証する処理と、をコンピュータに実行させる。

発明の効果

[0012] 本開示によれば、パスワード等の認証情報の漏洩を防止できる認証装置等を提供することが可能になる。

図面の簡単な説明

[0013] [図1]第1の実施形態の認証システムの構成の一例を示すブロック図である。

[図2]第1の実施形態の認証システムの入力端末のユーザインタフェースに表示される乱数列パターンの一例を示す概念図である。

[図3]第1の実施形態の認証システムの認証装置の記憶部に記憶される共有パターンの一例を示す概念図である。

[図4]第1の実施形態の認証システムの入力端末の構成の一例を示すブロック図である。

[図5]第1の実施形態の認証システムの認証装置の構成の一例を示すブロック図である。

[図6]第1の実施形態の認証システムの認証装置の記憶部に記憶される共有情報テーブルの一例である。

[図7]第1の実施形態の認証システムの認証装置によるキーコードの演算の一例について説明するための概念図である。

[図8]第1の実施形態の認証システムの認証装置の記憶部に記憶される共有情報テーブルの一例である。

[図9]第1の実施形態の認証システムの認証装置によるキーコードの演算の一例について説明するための概念図である。

[図10]第1の実施形態の認証システムの認証装置の記憶部に記憶される共有情報テーブルの一例である。

[図11]第1の実施形態の認証システムの認証装置によるキーコードの演算の一例について説明するための概念図である。

[図12]第1の実施形態の認証システムの認証装置の記憶部に記憶される共有

情報テーブルの一例である。

[図13]第1の実施形態の認証システムの認証装置によるキーコードの演算の一例について説明するための概念図である。

[図14]第1の実施形態の認証システムの認証装置の記憶部に記憶される共有情報テーブルの一例である。

[図15]第1の実施形態の認証システムの認証装置によるキーコードの演算の一例について説明するための概念図である。

[図16]第1の実施形態の認証システムの認証装置の記憶部に記憶される共有情報を変更するための共有情報変更画面の一例を示す概念図である。

[図17]第1の実施形態の認証システムの入力端末の動作の一例について説明するためのフローチャートである。

[図18]第1の実施形態の認証システムの認証装置の動作の一例について説明するためのフローチャートである。

[図19]第2の実施形態の認証システムの構成の一例を示すブロック図である。

[図20]第2の実施形態の認証システムの認証装置の構成の一例を示すブロック図である。

[図21]第2の実施形態の認証システムの認証装置から受信されたキーコードが携帯端末の画面に表示される一例を示す概念図である。

[図22]第2の実施形態の認証システムの入力端末の動作の一例について説明するためのフローチャートである。

[図23]第2の実施形態の認証システムの認証装置の動作の一例について説明するためのフローチャートである。

[図24]第2の実施形態の認証システムの携帯端末の動作の一例について説明するためのフローチャートである。

[図25]第3の実施形態の認証システムの構成の一例を示すブロック図である。

[図26]各実施形態に係る認証システムを構成する装置のハードウェア構成の

一例を示すブロック図である。

発明を実施するための形態

[0014] 以下に、本発明を実施するための形態について図面を用いて説明する。ただし、以下に述べる実施形態には、本発明を実施するために技術的に好ましい限定がされているが、発明の範囲を以下に限定するものではない。なお、以下の実施形態の説明に用いる全図においては、特に理由がない限り、同様箇所には同一符号を付す。また、以下の実施形態において、同様の構成・動作に関しては繰り返しの説明を省略する場合がある。

[0015] (第1の実施形態)

まず、第1の実施形態に係る認証システムについて図面を参照しながら説明する。本実施形態の認証システムは、認証対象人物（認証対象ユーザとも呼ぶ）によって入力された認証情報に基づいて、その認証対象人物を認証する。例えば、本実施形態の認証システムは、ATM (Automatic Teller Machine) 等の認証に用いられるパスワード（パスコードやパスフレーズなどとも呼ぶ）や暗証番号等の認証情報を用いた認証に適用される。以下においては、認証情報として、複数の数字によって構成されるパスワードを用いる例について説明する。本実施形態の手法は、数字を用いた認証であれば、任意の認証に用いることができる。

[0016] (構成)

図1は、本実施形態に係る認証システム1の構成の一例を示すブロック図である。認証システム1は、入力端末11および認証装置12を備える。入力端末11と認証装置12は、インターネット等のネットワークを介して、通信可能に接続される。例えば、入力端末11は、ATMのような専用端末として提供される。また、入力端末11は、パーソナルコンピュータやスマートフォン等の携帯端末にインストールされたアプリケーションソフトウェア（以下、アプリとも呼ぶ）として提供されてもよい。認証装置12は、サーバやクラウドに構築される。認証装置12は、ハードウェアであってもよいし、ソフトウェアであってもよい。

[0017] 以下においては、ユーザを一意に特定するために、ユーザのID (IDentifier) 情報 (識別情報とも呼ぶ) が記録された磁気カードやIC (Integrated Circuit) カード等の認証カード (図示しない) を用いるものとする。なお、ウェブを介した認証を行う場合は、ユーザのID情報をウェブ上で入力するように構成すればよい。入力端末11は、入力端末11への認証カードの挿入や、ウェブ上でID情報が入力されたことを、認証操作の開始として検出する。ただし、認証カードに登録された識別情報や、ウェブ上で入力されるID情報 (識別情報) 以外で、ユーザを一意に特定してもよい。例えば、顔認証や指紋認証、掌紋認証、歩容認証などの生体認証によって、ユーザを一意に特定してもよい。例えば、入力端末11のユーザインタフェース (UI : User Interface) に初期状態で表示される数字や文字、記号等の中から選択された数値や文字列、記号列に基づいて、ユーザを一意に特定してもよい。ユーザを一意に特定する手法には、特に限定を加えない。

[0018] 入力端末11は、ユーザによる認証操作の開始を検出すると、そのユーザのID情報を認証装置12に送信する。認証装置12は、ユーザのID情報を受信すると、そのID情報に対応付けて乱数列パターンを生成する。認証装置12は、0~9の10個の整数の中から選択された9個の整数によって構成され、3行×3列のマトリックス状に配列された乱数列パターンを生成する。入力端末11は、ID情報の送信元の入力端末11に対して、生成された乱数列パターンを送信する。入力端末11は、受信した乱数列パターンをUIに表示させる。本実施形態において、入力端末11は、3行×3列のマトリックス状に配列された乱数列パターンを含むUIに表示させる。

[0019] 認証装置12は、ユーザと認証装置12との間で共有される共有情報を記憶する。共有情報は、ユーザごとに設定されたパスワードおよび共有ルールを含む。パスワードは、ユーザによって予め設定された認証情報である。本実施形態においては、3桁の数字からなるパスワードを用いる例をあげる。共有ルールは、ユーザと認証装置12との間で共有されるルールである。ユーザは、入力端末11のUIに表示された乱数列パターンに含まれる数字を

用いて、予め設定された共有ルールに従ってキーコードを計算する。キーコードは、入力端末 11 の UI に表示された乱数列パターンにおいて、ユーザによって認証情報として入力される数字列である。キーコードは、一度の認証機会においてのみ有効であり、数字の配置も毎回変わるため、漏洩したとしてもユーザの認証情報が漏洩することはない。認証装置 12 も、ユーザと同様に、乱数列パターンを用いて、予め設定された共有ルールに従ってキーコードを計算する。認証装置 12 は、ユーザによって計算されるキーコードと、認証装置 12 によって計算されるキーコードとが一致した場合、そのユーザを認証する。

[0020] 共有ルールは、ユーザごとに設定された共有パターンおよび演算ルールを含む。共有パターンは、入力端末 11 の UI に表示された乱数列パターンに含まれる複数の数字を選択する順序を示すパターンである。演算ルールは、共有パターンに基づいて、乱数列パターンに含まれる複数の数字の中から選択された各々の数字に対して行われえる演算に関するルールである。

[0021] 図 2 は、入力端末 11 の UI 111 に表示される乱数列パターンの一例を示す概念図である。図 2 は、0～9 の 10 個の整数の中から選択された異なる 9 個の整数（0、1、2、3、4、5、7、8、9）を 3 行×3 列のマトリックス状に配列させた乱数列パターンの例である。本実施形態においては、乱数列パターンの各セルに一桁の数字を配置する例を示すが、乱数列パターンの各セルに表示させる数字の桁数は一桁に限定されない。

[0022] 図 3 は、共有パターンの一例を示す概念図である。共有パターンは、乱数列パターンから数字を選択する順番を示す。乱数列パターンから選択される個々の数字を仮数字と呼ぶ。仮数字は、選択される順番に従って、第 1 仮数字、第 2 仮数字、・・・、第 m 仮数字と表記される（m は自然数）。図 3 の共有パターンは、3 行×3 列のマトリックス状に配列させた乱数列パターンにおいて、第 1 仮数字を 3 行 1 列目から選択し、第 2 仮数字を 2 行 2 列目から選択し、第 3 仮数字を 3 行 3 列目から選択することを示す。図 2 に対応させると、第 1 仮数字は「7」であり、第 2 仮数字は「3」であり、第 3 仮数

字は「2」である。

[0023] 例えば、あるユーザのパスワードを「7 2 1」とする。パスワードに関しては、3桁の数字の左から順番に、第1秘密数字、第2秘密数字、第3秘密数字と表記される。すなわち、パスワードの数字がn桁であれば、その数字の左から順番に、第1秘密数字、第2秘密数字、・・・、第n秘密数字と表記される（nは自然数）。また、キーコードについては、キーコードの数字がn桁であれば、その数字の左から順番に、第1鍵数字、第2鍵数字、・・・、第n鍵数字と表記される。

[0024] 例えば、演算ルールは、第1秘密数字に第1仮数字を足し、第2秘密数字に第2仮数字を足し、第3秘密数字に第3仮数字を足し、それらの数値の下一桁の数字を順番に並べることとする。この場合、キーコードの第1鍵数字は、第1秘密数字である「7」と第1仮数字である「7」とを足した数値である「14」の一桁目の数字の「4」になる。キーコードの第2鍵数字は、第2秘密数字である「2」と、第2仮数字である「3」とを足した数値である「5」の一桁目の数字の「5」になる。キーコードの第3鍵数字は、第3秘密数字である「1」と、第3仮数字である「2」とを足した数値である「3」の一桁目の数字の「3」になる。すなわち、キーコードは、「4 5 3」である。ユーザと認証装置12は、認証機会ごとに、上記の共有ルールに基づいて、予め定められたパスワードと、認証の開始時に生成された乱数列パターンとを用いた演算を行ってキーコードを計算する。

[0025] 入力端末11は、ユーザによって入力されたキーコードを認証装置12に送信する。認証装置12は、ユーザによって計算されたキーコードと、認証装置12によって計算されたキーコードとを比較する。認証装置12は、ユーザによって計算されたキーコードと、認証装置12によって計算されたキーコードとが一致した場合、そのユーザを認証する。一方、認証装置12は、ユーザによって計算されたキーコードと、認証装置12によって計算されたキーコードとが一致しなかった場合、そのユーザを認証しない。

[0026] 上記の手順でユーザによって入力端末11のUIに入力されるキーコード

は、毎回異なるため、予測することができない数字列である。また、入力端末 11 の UI に表示されるキーコードの数字は、毎回不定の位置に表示されるため、表示位置を予測することはできない。すなわち、本実施形態の手法によれば、ユーザのパスワードや共有情報を特定することができないため、ユーザによるキーコードの入力が盗み見られたとしても、パスワードや共有情報が流出することがない。すなわち、本実施形態の認証方法によれば、セキュリティレベルが高い認証システムを構築できる。

[0027] 続いて、認証システム 1 を構成する入力端末 11 および認証装置 12 の詳細構成について図面を参照しながら説明する。以下においては、入力端末 11 および認証装置 12 について、機能ブロックを用いて説明する。実際には、入力端末 11 および認証装置 12 は、プログラムを記憶する記憶部や、記憶部に記憶されたプログラムを実行するプロセッサを含む情報処理装置等との協調的な処理によって実現される。

[0028] [入力端末]

図 4 は、入力端末 11 の構成の一例を示すブロック図である。入力端末 11 は、UI 111、表示制御部 112、および送受信部 113 を有する。図 4 には、入力端末 11 に接続される認証装置 12 も併せて図示する。

[0029] UI 111 は、操作画面等の表示情報が表示され、操作画面に対する操作を受け付けるインタフェースである。例えば、UI 111 は、表示機能と入力機能を兼ね備えるタッチパネル等によって実現される。例えば、UI 111 は、パスワード等の認証情報の入力に用いられる。UI 111 は、グラフィカルユーザインタフェースやタッチインタフェース等として提供される。入力端末 11 が ATM として実現される場合、例えば、UI 111 は、タッチインタフェースとして提供される。例えば、ウェブを介して認証情報が入力される場合、UI 111 は、ウェブユーザインタフェースとして提供されてもよい。

[0030] 表示制御部 112 は、操作画面等の表示情報を UI 111 に表示させる。表示制御部 112 は、予め設定されたプログラムに従って、UI 111 に表

示させる表示情報を切り替える。例えば、U 1 1 1 に表示させる表示情報や、表示情報を切り替えるプログラムは、図示しない記憶部に記憶させておく。

[0031] 送受信部 1 1 3 は、ユーザによる認証操作の開始を検出すると、そのユーザの I D 情報を認証装置 1 2 に送信する。例えば、送受信部 1 1 3 は、ユーザのカードが入力端末 1 1 に挿入された際に、そのユーザによる認証操作の開始を検出し、そのカードに記録された I D 情報を認証装置 1 2 に送信する。例えば、送受信部 1 1 3 は、U 1 1 1 を介して I D 情報が入力された際に、ユーザによる認証操作の開始を検出し、入力された I D 情報を認証装置 1 2 に送信する。送受信部 1 1 3 は、I D 情報の受信をトリガーとして認証装置から送信された乱数列パターンを認証装置 1 2 から受信する。また、送受信部 1 1 3 は、U 1 1 1 を介して入力された認証情報を認証装置 1 2 に送信する。送受信部 1 1 3 は、認証装置 1 2 から認証結果を受信する。

[0032] [認証装置]

図 5 は、認証装置 1 2 の構成の一例を示すブロック図である。認証装置 1 2 は、送受信部 1 2 1、乱数列生成部 1 2 2、記憶部 1 2 3、演算部 1 2 4、および認証部 1 2 5 を有する。図 5 には、認証装置 1 2 に接続される入力端末 1 1 も併せて図示する。

[0033] 送受信部 1 2 1 は、入力端末 1 1 からユーザ I D を受け付ける。送受信部 1 2 1 は、入力端末 1 1 からユーザ I D を受け付けると、乱数列生成部 1 2 2 によって生成された乱数列パターンを、そのユーザ I D に対応付けて入力端末 1 1 に送信する。また、送受信部 1 2 1 は、ユーザによって入力されたキーコードを入力端末 1 1 から受信する。受信されたユーザごとのキーコードは、認証部 1 2 5 によって認証される。送受信部 1 2 1 は、認証部 1 2 5 による認証結果を入力端末 1 1 に送信する。なお、送受信部 1 2 1 は、ユーザ I D や乱数列パターン、キーコード、認証結果以外のデータを入力端末 1 1 と送受信し合ってもよい。

[0034] 乱数列生成部 1 2 2 は、送受信部 1 2 1 がユーザ I D を受け付けるたびに

乱数列パターンを生成する。例えば、乱数列生成部 1 2 2 は、0～9 の 1 0 個の整数から異なる 9 個の数字をランダムに選択し、選択された 9 個の数字が 3 行×3 列のマトリックス状に配置された乱数列パターンを生成する。なお、乱数列生成部 1 2 2 が選択する数字の数や配置は、ここであげた例に限定されない。

[0035] 記憶部 1 2 3 には、ユーザごとの共有情報が記憶される。共有情報は、ユーザごとに設定されたパスワードおよび共有ルールを含む。パスワードは、ユーザによって予め設定された認証情報である。例えば、パスワードは、3 桁や 4 桁の数字列である。共有ルールは、ユーザと認証装置 1 2 との間で共有されるルールである。共有ルールは、ユーザごとに設定された共有パターンおよび演算ルールを含む。共有パターンは、入力端末 1 1 の UI に表示された乱数列パターンに含まれる複数の数字を選択する順序を示すパターンである。演算ルールは、乱数列パターンに含まれる複数の数字の中から、共有パターンに基づいて順番に選択された各々の数字に対して行われる演算に関するルールである。例えば、演算ルールは、第 1 秘密数字に第 1 仮数字を足し、第 2 秘密数字に第 2 仮数字を足し、第 3 秘密数字に第 3 仮数字を足し、それらの数値の下一桁の数字を選択することである。演算ルールは、ユーザごとに異なるルールが設定されるため、特定することができない。

[0036] 演算部 1 2 4 は、認証中のユーザに対応付けられた共有パターンに基づいて、乱数列パターンに含まれる複数の数字の中から数字を選択し、選択された各々の数字に対して所定の演算を実行してキーコードを生成する。キーコードは、入力端末 1 1 の UI に表示された乱数列パターンにおいて、ユーザによって認証情報として入力される数字列である。

[0037] 例えば、演算部 1 2 4 は、共有パターンに基づいて選択された仮数字に対して、パスワードに含まれるいずれかの秘密数字を足し合わせ、その計算結果の数値の下一桁目の数字を選択する演算を、所定の演算として実行する。例えば、演算部 1 2 4 は、共有パターンに基づいて選択された仮数字から、パスワードに含まれるいずれかの秘密数字を引き、その計算結果の数値の絶

対値の下一桁目の数字を選択する演算を、所定の演算として実行してもよい。例えば、演算部 124 は、共有パターンに基づいて選択された仮数字に対して、パスワードに含まれるいずれかの秘密数字を掛け合わせ、その計算結果の数値の下一桁目の数字を選択する演算を、所定の演算として実行する。例えば、演算部 124 は、共有パターンに基づいて選択された仮数字で、パスワードに含まれるいずれかの秘密数字を割り、その計算結果の数値の下一桁目や、小数点以下のいずれかの桁、余りなどの数値を選択する演算を、所定の演算として実行する。なお、演算部 124 が実行する演算は、ユーザと認証装置 12 との間で共有されていれば、ここであげた方法に限定されない。

[0038] 認証部 125 は、認証中のユーザによって計算されたキーコードと、演算部 124 によって計算されたキーコードとを比較し、そのユーザの認証可否を判定する。認証部 125 は、ユーザによって計算されたキーコードと、演算部 124 によって計算されたキーコードとが一致した場合、そのユーザを認証するという認証結果を生成する。一方、認証部 125 は、ユーザによって計算されたキーコードと、演算部 124 によって計算されたキーコードとが一致しなかった場合、そのユーザを認証しないという認証結果を生成する。認証部 125 による認証結果は、認証中のユーザが操作する入力端末 11 に送信される。

[0039] [共有情報]

次に、ユーザと認証装置 12 との間で共有される共有情報について、いくつかの例をあげて説明する。以下の例は、一例であって、ユーザと認証装置 12 との間で共有される共有情報について限定するものではない。

[0040] <第 1 例>

まず、共有情報の第 1 例について図面を参照しながら説明する。図 6 と図 7 は、ユーザと認証装置 12 との間で共有される共有情報の第 1 例に関する。図 6 は、第 1 例において、記憶部 123 に記憶される共有情報の一例を示す共有情報テーブル（共有情報テーブル 131）である。共有情報テーブル

1 3 1 には、ユーザ ID（識別情報とも呼ぶ）ごとの共有情報が格納される。図 7 は、第 1 例におけるキーコードの演算について説明するための概念図である。以下においては、ユーザ ID「A A A」について一例をあげて説明し、ユーザ ID「B B B」とユーザ ID「C C C」については説明を省略する。

[0041] 例えば、ユーザ ID「A A A」には、パスワード「7 2 1」と、ユーザ ID「A A A」の共有パターンと、演算ルール「A 1」とが対応付けられる。ユーザ ID「A A A」の共有パターンは、3 行×3 列の乱数列パターンにおいて、3 行目 1 列目から第 1 仮数字を選択し、2 行目 2 列目から第 2 仮数字を選択し、3 行目 3 列目から第 3 仮数字を選択することを示す。演算ルール「A 1」は、第 1 秘密数字に第 1 仮数字を足し、第 2 秘密数字に第 2 仮数字を足し、第 3 仮数字に第 3 秘密数字を足し、それらの数値の下一桁の数字を選択することと定義する。

[0042] ここで、図 7 を参照しながら、第 1 例において、乱数列パターンを用いて、ユーザ ID「A A A」の共有情報に基づいてキーコードを計算する例について説明する。

[0043] 図 7 の例では、乱数列パターンと共有パターンに基づく、第 1 仮数字が「7」であり、第 2 仮数字が「3」であり、第 3 仮数字が「2」である。キーコードの第 1 鍵数字は、パスワードの第 1 秘密数字である「7」と、第 1 仮数字である「7」とを足した数値である「14」の一桁目の数字の「4」になる。キーコードの第 2 鍵数字は、パスワードの第 2 秘密数字である「2」と、第 2 仮数字である「3」とを足した数値である「5」の一桁目の数字の「5」になる。キーコードの第 3 鍵数字は、パスワードの第 3 秘密数字である「1」と、第 3 仮数字である「2」とを足した数値である「3」の一桁目の数字の「3」になる。すなわち、キーコードは、「4 5 3」である。

[0044] 第 1 例によれば、ユーザによるキーコードの入力が盗み見られたとしても、キーコードの規則性を特定することができないので、ユーザのパスワードが漏洩する可能性はない。例えば、0～9 の 10 個の数字の中から 9 個の数

字が乱数列パターンとして選ばれた際に、キーコードに対応する数字が乱数列パターンに含まれない場合がある。そのような場合は、ユーザからの要求に応じて、乱数列パターンを再生成するように構成すればよい。

[0045] <第2例>

次に、共有情報の第2例について図面を参照しながら説明する。第1例では、0～9の10個の数字から異なる9個の数字を選択するため、算出された鍵数字が乱数列パターンに含まれない場合がある。第2例は、算出された鍵数字が乱数列パターンに含まれない場合に対応する例である。図8と図9は、ユーザと認証装置12との間で共有される共有情報の第2例に関する。図8は、第2例において、記憶部123に記憶される共有情報の一例を示す共有情報テーブル（共有情報テーブル132）である。共有情報テーブル132には、ユーザIDごとの共有情報が格納される。図9は、第2例におけるキーコードの演算について説明するための概念図である。

[0046] 例えば、ユーザID「AAA」には、パスワード「721」と、ユーザID「AAA」の共有パターンと、演算ルール「A2」とが対応付けられる。ユーザID「AAA」の共有パターンは、3行×3列の乱数列パターンにおいて、3行目1列目から第1仮数字を選択し、2行目2列目から第2仮数字を選択し、3行目3列目から第3仮数字を選択することを示す。演算ルール「A2」は、二つの演算を含む。演算ルール「A2」に含まれる一つ目の演算は、第1秘密数字に第1仮数字を足し、第2秘密数字に第2仮数字を足し、第3仮数字に第3秘密数字を足し、それらの数値の下一桁の数字を選択するという演算である。演算ルール「A2」に含まれる二つ目の演算は、選択された数字が乱数列パターンに含まれない場合、その数字に1を足すという演算である。このように、演算ルールは、複数の演算を組み合わせたものであってもよい。

[0047] ここで、図9を参照しながら、第2例において、乱数列パターンを用いて、ユーザID「AAA」の共有情報に基づいてキーコードを計算する例について説明する。

[0048] 図9の例では、乱数列パターンと共有パターンに基づく、第1仮数字が「8」であり、第2仮数字が「5」であり、第3仮数字が「0」である。キーコードの第1鍵数字は、パスワードの第1秘密数字である「7」と、第1仮数字である「8」とを足した数値である「15」の一桁目の数字の「5」になる。キーコードの第2鍵数字は、パスワードの第2秘密数字である「2」と、第2仮数字である「5」とを足した数値である「7」の一桁目の数字の「7」になる。キーコードの第3鍵数字は、パスワードの第3秘密数字である「1」と、第3仮数字である「0」とを足した数値である「1」の一桁目の数字の「1」になるはずである。しかし、乱数列パターンには「1」が含まれないので、パスワードの第3秘密数字である「1」と、第3仮数字である「0」とを足した数値である「1」の一桁目の数字の「1」に1を足した数値である「2」が第3鍵数字になる。すなわち、キーコードは、「572」である。

[0049] 第2例によれば、第1例の方法で演算されたキーコードに含まれる数字が乱数列パターンに含まれない場合にも対応できる。また、第2例によれば、複数の演算が組み合わされた演算ルールが用いられるため、ユーザの認証情報が漏洩する可能性がさらに低くなる。

[0050] <第3例>

次に、共有情報の第3例について図面を参照しながら説明する。第3例は、共有パターンを日替わりで変更する例である。図10と図11は、ユーザと認証装置12との間で共有される共有情報の第3例に関する。図10は、第3例において、記憶部123に記憶される共有情報の一例を示す共有情報テーブル（共有情報テーブル133）である。共有情報テーブル133には、ユーザIDごとの共有情報が格納される。図11は、第3例におけるキーコードの演算について説明するための概念図である。

[0051] 例えば、ユーザID「AAA」には、パスワード「721」と、ユーザID「AAA」の日替わりの共有パターンと、演算ルール「A2」とが対応付けられる。ユーザID「AAA」の共有パターンは、月曜日、火曜日、水曜

日、・・・と、曜日に対応付けて日替わりで設定される。なお、図10においては、木曜日、金曜日、土曜日、日曜日の共有パターンは省略する。「月曜日」の共有パターンは、3行×3列の乱数列パターンにおいて、2行目1列目から第1仮数字を選択し、1行目1列目から第2仮数字を選択し、1行目2列目から第3仮数字を選択することを示す。「火曜日」の共有パターンは、3行×3列の乱数列パターンにおいて、1行目2列目から第1仮数字を選択し、1行目3列目から第2仮数字を選択し、2行目3列目から第3仮数字を選択することを示す。「水曜日」の共有パターンは、3行×3列の乱数列パターンにおいて、2行目3列目から第1仮数字を選択し、3行目3列目から第2仮数字を選択し、3行目2列目から第3仮数字を選択することを示す。演算ルール「A2」は、二つの演算を含む。演算ルール「A2」に含まれる一つ目の演算は、第1秘密数字に第1仮数字を足し、第2秘密数字に第2仮数字を足し、第3仮数字に第3秘密数字を足し、それらの数値の下一桁の数字を選択するという演算である。演算ルール「A2」に含まれる二つ目の演算は、選択された数字が乱数列パターンに含まれない場合、その数字に1を足すという演算である。

[0052] ここで、図11を参照しながら、第3例において、乱数列パターンを用いて、ユーザID「AAA」の共有情報に基づいてキーコードを計算する例について説明する。以下の例では、木曜日、金曜日、土曜日、日曜日については説明を省略する。実際には、乱数列パターンの配列は認証ごとに生成されるが、説明を簡略化するために同じ配列を用いて説明する。

[0053] 月曜日に関しては、乱数列パターンと、月曜日の共有パターンに基づく、第1仮数字が「8」であり、第2仮数字が「0」であり、第3仮数字が「9」である。キーコードの第1鍵数字は、パスワードの第1秘密数字である「7」と、第1仮数字である「8」とを足した数値である「15」の一桁目の数字の「5」になる。キーコードの第2鍵数字は、パスワードの第2秘密数字である「2」と、第2仮数字である「0」とを足した数値である「2」の一桁目の数字の「2」になる。キーコードの第3鍵数字は、パスワードの

第3秘密数字である「1」と、第3仮数字である「9」とを足した数値である「10」の一桁目の数字の「0」である。すなわち、月曜日のキーコードは、「520」である。

[0054] 火曜日に関しては、乱数列パターンと、火曜日の共有パターンに基づく、第1仮数字が「9」であり、第2仮数字が「1」であり、第3仮数字が「5」である。キーコードの第1鍵数字は、パスワードの第1秘密数字である「7」と、第1仮数字である「9」とを足した数値である「16」の一桁目の数字の「6」になるはずである。しかし、乱数列パターンには「6」が含まれないので、パスワードの第1秘密数字である「7」と、第1仮数字である「9」とを足した数値である「16」の一桁目の数字の「6」に1を足した数値である「7」が第1鍵数字になる。キーコードの第2鍵数字は、パスワードの第2秘密数字である「2」と、第2仮数字である「1」とを足した数値である「3」の一桁目の数字の「3」になる。キーコードの第3鍵数字は、パスワードの第3秘密数字である「1」と、第3仮数字である「5」とを足した数値である「6」の一桁目の数字の「6」になるはずである。しかし、乱数列パターンには「6」が含まれないので、パスワードの第3秘密数字である「1」と、第3仮数字である「5」とを足した数値である「6」の一桁目の数字の「6」に1を足した数値である「7」が第3鍵数字になる。すなわち、火曜日のキーコードは、「727」である。

[0055] 同様に、水曜日のキーコードは「245」であり、木曜日のキーコードは「199」であり、金曜日のキーコードは「413」であり、土曜日のキーコードは「778」であり、日曜日のキーコードは「803」である。実際には、乱数列パターンに含まれる数字の配列が認証ごとに新たに生成されるので、曜日ごとの共有パターンに基づく仮数字は、異なる乱数列パターンから選択される。第3例によれば、共有パターンが日替わりで異なるので、何週間にわたって継続的にキー入力を盗み見られたとしても、パスワードが漏れる可能性は極めて低くなる。

[0056] <第4例>

次に、共有情報の第4例について図面を参照しながら説明する。第4例は、乱数列パターンのマトリクスにおいて仮数字を選択する位置と順番ではなく、乱数列パターンに含まれるいずれかの数字を起点として仮数字を選択するパターンを共有パターンとして用いる例である。図12と図13は、ユーザと認証装置12との間で共有される共有情報の第4例に関する。図12は、第4例において、記憶部123に記憶される共有情報の一例を示す共有情報テーブル（共有情報テーブル134）である。共有情報テーブル134には、ユーザIDごとの共有情報が格納される。図13は、第4例におけるキーコードの演算について説明するための概念図である。以下においては、ユーザID「AAA」について一例をあげて説明し、ユーザID「BBB」とユーザID「CCC」については説明を省略する。

[0057] 例えば、ユーザID「AAA」には、パスワード「721」と、ユーザID「AAA」の共有パターンと、演算ルール「A2」とが対応付けられる。ユーザID「AAA」の共有パターンは、第1中心数字「7」と、第2中心数字「3」と、仮数字の選択順序「時計回り」とを含む。演算ルール「A2」は、二つの演算を含む。演算ルール「A2」に含まれる一つ目の演算は、第1秘密数字に第1仮数字を足し、第2秘密数字に第2仮数字を足し、第3仮数字に第3秘密数字を足し、それらの数値の下一桁の数字を選択するという演算である。演算ルール「A2」に含まれる二つ目の演算は、選択された数字が乱数列パターンに含まれない場合、その数字に1を足すという演算である。

[0058] 第1中心数字「7」は、乱数列パターンから仮数字を選択する際に中心となる数字である。例えば、乱数列パターンに「7」が含まれる場合、「7」を中心とする時計回りの順番で仮数字が順番に選択される。第2中心数字「3」は、乱数列パターンに第1中心数字「7」が含まれない場合に、乱数列パターンから仮数字を選択する際に中心となる数字である。例えば、乱数列パターンに「7」が含まれない場合、「3」を中心とする時計回りの順番で仮数字が順番に選択される。第1～第3仮数字は、乱数列パターンに含まれ

る中心数字を中心として、時計回りの順番で連続する数字が選択される。仮数字の選択の優先順位は、中心数字を中心として、上、右斜め上、右、右斜め下、下、左斜め下、左、左斜め上の時計回りの順番になる。例えば、乱数列パターンにおいて、中心数字の上の数字が第1仮数字として選択され、中心数字の右斜め上の数字が第2仮数字として選択され、中心数字の右の数字が第3仮数字として選択される。例えば、乱数列パターンにおいて、中心数字の上に数字がない場合、中心数字の右の数字が第1仮数字として選択され、中心数字の右斜め下の数字が第2仮数字として選択され、中心数字の下の数字が第3仮数字として選択される。例えば、乱数列パターンにおいて、中心数字の右に数字がない場合、中心数字の下の数字が第1仮数字として選択され、中心数字の左斜め下の数字が第2仮数字として選択され、中心数字の左の数字が第3仮数字として選択される。例えば、乱数列パターンにおいて、中心数字の下に数字がない場合、中心数字の左の数字が第1仮数字として選択され、中心数字の左斜め上の数字が第2仮数字として選択され、中心数字の上の数字が第3仮数字として選択される。なお、共有パターンに含まれる仮数字の選択順序が「反時計回り」の場合、仮数字の選択の優先順位は、中心数字を中心として、上、左斜め上、左、左斜め下、下、右斜め下、右、右斜め上の反時計回りの順番になる。

[0059] ここで、図13を参照しながら、第4例において、乱数列パターンを用いて、ユーザID「AAA」の共有情報に基づいてキーコードを計算する例について説明する。以下の例では、AA、BB、CC、DDという乱数列パターンの各々についてキーコードを生成する例を示す。以下の説明においては、乱数列パターンから仮数字を選択する際に、中心数字を中心として時計回りの順番で仮数字を選択する例を示す。図13には、各乱数列パターンに対応するパターンを共有パターンの箇所に示す。共有パターンの上の記号「AA」、「BB」、「CC」、「DD」は、対応する乱数列パターンを示す。

[0060] 乱数列パターン「AA」には、第1中心数字「7」が含まれる。そのため、乱数列パターン「AA」に関しては、共有パターンに基づく、第1中心

数字「7」の上の「1」が第1仮数字であり、第2仮数字が「2」であり、第3仮数字が「0」である。キーコードの第1鍵数字は、パスワードの第1秘密数字である「7」と、第1仮数字である「1」とを足した数値である「8」の一桁目の数字の「8」になる。キーコードの第2鍵数字は、パスワードの第2秘密数字である「2」と、第2仮数字である「2」とを足した数値である「4」の一桁目の数字の「4」になる。キーコードの第3鍵数字は、パスワードの第3秘密数字である「1」と、第3仮数字である「0」とを足した数値である「1」の一桁目の数字の「1」である。すなわち、乱数列パターン「AA」を用いた場合のキーコードは、「841」である。

[0061] 乱数列パターン「BB」には、第1中心数字「7」が含まれる。そのため、乱数列パターン「BB」に関しては、共有パターンに基づく、第1中心数字「7」の上の「0」が第1仮数字であり、第2仮数字が「6」であり、第3仮数字が「2」である。キーコードの第1鍵数字は、パスワードの第1秘密数字である「7」と、第1仮数字である「0」とを足した数値である「7」の一桁目の数字の「7」になる。キーコードの第2鍵数字は、パスワードの第2秘密数字である「2」と、第2仮数字である「6」とを足した数値である「8」の一桁目の数字の「8」になるはずである。しかし、乱数列パターン「BB」には「8」が含まれないので、パスワードの第2秘密数字である「2」と、第2仮数字である「6」とを足した数値である「8」の一桁目の数字の「8」に1を足した数値である「9」が第2鍵数字になる。キーコードの第3鍵数字は、パスワードの第3秘密数字である「1」と、第3仮数字である「2」とを足した数値である「3」の一桁目の数字の「3」である。すなわち、乱数列パターン「BB」を用いた場合のキーコードは、「793」である。

[0062] 乱数列パターン「CC」には、第1中心数字「7」が含まれるが、第1中心数字「7」の右と下に数字がないため、第1中心数字「7」の上の数字から時計回りの順番に仮数字を選択できない。そのため、乱数列パターン「CC」に関しては、共有パターンに基づく、第1中心数字「7」の左の「5

」が第1仮数字であり、第2仮数字が「2」であり、第3仮数字が「3」である。キーコードの第1鍵数字は、パスワードの第1秘密数字である「7」と、第1仮数字である「5」とを足した数値である「12」の一桁目の数字の「2」になる。キーコードの第2鍵数字は、パスワードの第2秘密数字である「2」と、第2仮数字である「2」とを足した数値である「4」の一桁目の数字の「4」になる。キーコードの第3鍵数字は、パスワードの第3秘密数字である「1」と、第3仮数字である「3」とを足した数値である「4」の一桁目の数字の「4」である。すなわち、乱数列パターン「CC」を用いた場合のキーコードは、「244」である。

[0063] 乱数列パターン「DD」には、第1中心数字「7」が含まれないため、第2中心数字「3」が中心数字である。そのため、乱数列パターン「DD」に関しては、共有パターンに基づく、第2中心数字「3」の右の「4」が第1仮数字であり、第2仮数字が「8」であり、第3仮数字が「5」である。キーコードの第1鍵数字は、パスワードの第1秘密数字である「7」と、第1仮数字である「4」とを足した数値である「11」の一桁目の数字の「1」になる。キーコードの第2鍵数字は、パスワードの第2秘密数字である「2」と、第2仮数字である「8」とを足した数値である「10」の一桁目の数字の「0」になる。キーコードの第3鍵数字は、パスワードの第3秘密数字である「1」と、第3仮数字である「5」とを足した数値である「6」の一桁目の数字の「6」である。すなわち、乱数列パターン「DD」を用いた場合のキーコードは、「106」である。

[0064] 第4例によれば、共有パターンに従った仮数字の選択ルールが非常に複雑なので、継続的にキー入力を盗み見られたとしても、パスワードが漏れる可能性は極めて低くなる。

[0065] <第5例>

次に、共有情報の第5例について図面を参照しながら説明する。第5例は、所定の期間ごとにパスワードを変更する例である。図14と図15は、ユーザと認証装置12との間で共有される共有情報の第5例に関する。図14

は、第5例において、記憶部123に記憶される共有情報の一例を示す共有情報テーブル（共有情報テーブル135）である。共有情報テーブル135には、ユーザIDごとの共有情報が格納される。図15は、第5例におけるキーコードの演算について説明するための概念図である。以下においては、ユーザID「AAA」について一例をあげて説明し、ユーザID「BBB」とユーザID「CCC」については説明を省略する。

[0066] 例えば、ユーザID「AAA」には、所定の期間ごとに所定のルールに従って変更されるパスワードと、ユーザID「AAA」の共有パターンと、演算ルール「A2」とが対応付けられる。ユーザID「AAA」のパスワードは、1～3月の期間では「3721」、4～6月の期間では「7213」、7～9月の期間では「2137」、10～12月の期間では「1372」である。図14の例では、所定の期間ごとに、パスワードの先頭数字を末尾に移動することによって、パスワードを変更する。なお、パスワードを変更する規則は、ユーザと認証装置12との間で共有されれば、ここであげた例に限定されない。例えば、パスワードは、月ごとに変更されたり、週ごとに変更されたりしてもよい。例えば、パスワードは、所定の期間ごとに変更されるのではなく、何らかのルールに従って不定期に変更されるようにしてもよい。

[0067] ユーザID「AAA」の共有パターンは、3行×3列の乱数列パターンにおいて、3行目1列目から第1仮数字を選択し、2行目2列目から第2仮数字を選択し、3行目3列目から第3仮数字を選択し、1行目1列目から第4仮数字を選択することを示す。演算ルール「A2」は、二つの演算を含む。演算ルール「A2」に含まれる一つ目の演算は、第1秘密数字に第1仮数字を足し、第2秘密数字に第2仮数字を足し、第3仮数字に第3秘密数字を足し、それらの数値の下一桁の数字を選択するという演算である。演算ルール「A2」に含まれる二つ目の演算は、選択された数字が乱数列パターンに含まれない場合、その数字に1を足すという演算である。

[0068] ここで、図15を参照しながら、第5例において、乱数列パターンを用い

て、ユーザID「AAA」の共有情報に基づいてキーコードを計算する例について説明する。以下の例では、1～3月、4～6月、7～9月、10～12月の各々の期間のパスワードについてキーコードを生成する例を示す。図15の例では、乱数列パターンと共有パターンに基づく、第1仮数字が「8」であり、第2仮数字が「5」であり、第3仮数字が「0」であり、第4仮数字が「4」である。

[0069] 1～3月に関しては、キーコードの第1鍵数字は、パスワードの第1秘密数字である「3」と、第1仮数字である「8」とを足した数値である「11」の一桁目の数字の「1」になるはずである。しかし、乱数列パターンには「1」が含まれないので、パスワードの第1秘密数字である「3」と、第1仮数字である「8」とを足した数値である「11」の一桁目の数字の「1」に1を足した数値である「2」が第1鍵数字になる。キーコードの第2鍵数字は、パスワードの第2秘密数字である「7」と、第2仮数字である「5」とを足した数値である「12」の一桁目の数字の「2」になる。キーコードの第3鍵数字は、パスワードの第3秘密数字である「2」と、第3仮数字である「0」とを足した数値である「2」の一桁目の数字の「2」である。キーコードの第4鍵数字は、パスワードの第4秘密数字である「1」と、第4仮数字である「4」とを足した数値である「5」の一桁目の数字の「5」である。すなわち、キーコードは、「2225」である。

[0070] 4～6月に関しては、キーコードの第1鍵数字は、パスワードの第1秘密数字である「7」と、第1仮数字である「8」とを足した数値である「15」の一桁目の数字の「5」である。キーコードの第2鍵数字は、パスワードの第2秘密数字である「2」と、第2仮数字である「5」とを足した数値である「7」の一桁目の数字の「7」になる。キーコードの第3鍵数字は、パスワードの第3秘密数字である「2」と、第3仮数字である「0」とを足した数値である「2」の一桁目の数字の「2」である。キーコードの第4鍵数字は、パスワードの第4秘密数字である「3」と、第4仮数字である「4」とを足した数値である「7」の一桁目の数字の「7」である。すなわち、キ

ーコードは、「５７２７」である。

[0071] 同様に、７～９月のキーコードは「０６３２」であり、１０～１２月のキーコードは「９８７６」である。実際には、乱数列パターンに含まれる数字の配列が認証ごとに新たに生成されるので、共有パターンに基づく仮数字は、異なる乱数列パターンから選択される。第５例によれば、所定の期間が経過すると所定のルールに従ってパスワードが変わるので、何カ月にもわたって継続的にキー入力を盗み見られたとしても、パスワードが漏れる可能性は極めて低くなる。

[0072] 上記の共有情報の例は、任意に組み合わせてもよい。例えば、日替わりで共有パターンを変更し、所定の期間ごとに所定のルールに従ってパスワードを変更すれば、ユーザによって入力されるキーコードからパスワードを推測することは非常に難しくなる。

[0073] 図１６は、共有パターン、演算ルール、およびパスワードの変更を受け付けるウィンドウの一例（共有情報変更ウィンドウ１５０）である。例えば、共有情報変更ウィンドウ１５０には、認証システム１を利用するシステムのウェブページ等に表示されたリンクからアクセスできる。共有パターン、演算ルール、およびパスワードを含む共有情報は、同時に同じ画面上に表示されると、互いに関連付けられやすくなるので、異なる画面上に表示させるように構成することが好ましい。そのため、共有情報変更ウィンドウ１５０には、共有パターン、演算ルール、およびパスワードを変更するウィンドウへのリンクのみを表示させることが好ましい。例えば、「共有パターンの変更」をクリックすると、そのリンク先の画面上で共有パターンを変更できるように構成する。例えば、「演算ルールの変更」をクリックすると、そのリンク先の画面上で演算ルールを変更できるように構成する。例えば、「パスワードの変更」をクリックすると、そのリンク先の画面上でパスワードを変更できるように構成する。これらのリンク先で変更された共有パターン、演算ルール、およびパスワードは、ユーザと認証装置１２との間で共有されるようにすればよい。

[0074] (動作)

次に、本実施形態の認証システム 1 の動作について図面を参照しながら説明する。以下においては、認証システム 1 を構成する入力端末 1 1 および認証装置 1 2 の各々を動作主体とする例について説明する。

[0075] [入力端末]

図 1 7 は、入力端末 1 1 の動作について説明するためのフローチャートである。図 1 7 のフローチャートに沿った説明においては、入力端末 1 1 を動作主体として説明する。

[0076] 図 1 7 において、まず、入力端末 1 1 は、認証対象のユーザによるユーザ ID を受け付ける (ステップ S 1 1 1)。例えば、入力端末 1 1 は、入力端末 1 1 への認証カードの挿入や、ウェブ上の認証専用ページ等で ID 情報が入力されたことを、認証操作の開始として検出する。

[0077] 次に、入力端末 1 1 は、受け付けたユーザ ID を認証装置 1 2 に送信する (ステップ S 1 1 2)。

[0078] 次に、入力端末 1 1 は、自装置から送信されたユーザ ID に応じて送信された乱数列パターンを認証装置 1 2 から取得する (ステップ S 1 1 3)。

[0079] 次に、入力端末 1 1 は、取得された乱数列パターンを自装置の U I 1 1 1 に表示させる (ステップ S 1 1 4)。入力端末 1 1 には、認証対象ユーザによって、共有ルールに基づいて選択された数字からなるキーコードが入力される。

[0080] 次に、入力端末 1 1 は、ユーザによって入力されたキーコードを認証装置 1 2 に送信する (ステップ S 1 1 5)。

[0081] 次に、入力端末 1 1 は、認証装置 1 2 から認証結果を受信する (ステップ S 1 1 6)。

[0082] 次に、入力端末 1 1 は、認証結果に応じた情報を U I 1 1 1 に表示させる (ステップ S 1 1 7)。例えば、認証装置 1 2 によって認証された場合、認証対象ユーザには、認証結果に応じたサービスが提供される。

[0083] [認証装置]

図 1 8 は、認証装置 1 2 の動作について説明するためのフローチャートである。図 1 8 のフローチャートに沿った説明においては、認証装置 1 2 を動作主体として説明する。

[0084] 図 1 8 において、まず、認証装置 1 2 は、認証対象ユーザのユーザ ID を入力端末 1 1 から受信する（ステップ S 1 2 1）。

[0085] 次に、認証装置 1 2 は、ユーザ ID に対応付けて、乱数列パターンを生成する（ステップ S 1 2 2）。

[0086] 次に、認証装置 1 2 は、生成された乱数列パターンを入力端末 1 1 に送信する（ステップ S 1 2 3）。

[0087] 次に、認証装置 1 2 は、生成された乱数列パターンと、ユーザ ID に対応する共有情報とを用いて、キーコードを生成する（ステップ S 1 2 4）。

[0088] 次に、認証装置 1 2 は、入力端末からキーコードを受信する（ステップ S 1 2 5）。

[0089] 次に、認証装置 1 2 は、入力端末 1 1 から受信されたキーコードと、自装置で生成されたキーコードとを比較する（ステップ S 1 2 6）。認証装置 1 2 は、入力端末 1 1 から受信されたキーコードと、自装置で生成されたキーコードとが一致する場合、認証中のユーザを認証するという認証結果を生成する。認証装置 1 2 は、入力端末 1 1 から受信されたキーコードと、自装置で生成されたキーコードとが一致しない場合、認証中のユーザを認証しないという認証結果を生成する。

[0090] 次に、認証装置 1 2 は、入力端末 1 1 に認証結果を送信する（ステップ S 1 2 7）。例えば、認証されたユーザに対してサービスを提供するシステムは、認証装置 1 2 によって認証されたユーザに対してサービスを提供する。

[0091] 以上のように、本実施形態の認証システムは、入力端末および認証装置を備える。入力端末と認証装置は、通信可能に接続される。入力端末は、認証対象ユーザの識別情報を受け付け、受け付けた識別情報を認証装置に送信する。認証装置は、ユーザごとに予め設定されたパスワードおよび共有ルールを含む共有情報を記憶しておく。認証装置は、認証対象ユーザの操作する入

力端末から認証対象ユーザの識別情報を受信する。認証装置は、認証対象ユーザの識別情報の受信に応じて、複数の異なる数字によって構成される乱数列パターンを生成する。認証装置は、生成された乱数列パターンを識別情報に対応付けて入力端末に送信する。認証装置は、共有ルールに基づいて、乱数列パターンから複数の仮数字を選択する。認証装置は、選択された複数の仮数字と、パスワードを構成する複数の秘密数字とを用いてキーコードを生成する。入力端末は、識別情報に対応付けられて認証装置によって生成された乱数列パターンを認証装置から受信する。入力端末は、乱数列パターンを自装置のユーザインタフェースに表示させる。入力端末は、ユーザインタフェースを介して乱数列パターンから選択されたキーコードを認証装置に送信する。認証装置は、認証対象ユーザによって共有ルールに基づいて乱数列パターンから選択された数字からなるキーコードを、入力端末から受信する。認証装置は、入力端末から受信されたキーコードと、自装置で生成されたキーコードとに基づいて、認証対象ユーザを認証する。

[0092] 認証装置は、送受信部、乱数列生成部、記憶部、演算部、および認証部を有する。乱数列生成部は、認証対象ユーザの認証機会ごとに、複数の異なる数字によって構成される乱数列パターンを生成する。演算部は、共有ルールに基づいて、乱数列パターンから複数の仮数字を選択し、選択された複数の仮数字と、パスワードを構成する複数の秘密数字とを用いてキーコードを生成する。送受信部は、認証対象ユーザの認証機会において、認証対象ユーザの操作する入力端末から認証対象ユーザの識別情報を受信する。送受信部は、認証対象ユーザの認証機会に生成された乱数列パターンを識別情報に対応付けて入力端末に送信する。送受信部は、認証対象ユーザによって共有ルールに基づいて乱数列パターンから選択された数字からなるキーコードを入力端末から受信する。認証部は、入力端末から受信されたキーコードと、演算部によって生成されたキーコードとに基づいて、認証対象ユーザを認証する。

[0093] 本実施形態の一態様において、記憶部は、ユーザによって予め設定された

共有パターンおよび演算ルールを含む共有ルールを記憶する。共有パターンは、複数の異なる数字がマトリックス状に配置された乱数列パターンから仮数字を選択する順番を示すパターンである。演算ルールは、乱数列パターンから選択された仮数字と、パスワードを構成する秘密数字とを用いた演算に関するルールである。

[0094] 例えば、記憶部は、乱数列パターンから選択された仮数字と、パスワードを構成する秘密数字とを用いた演算によって算出された数値が、乱数列パターンを構成する複数の数字に含まれない場合のルールを含む演算ルールを記憶する。例えば、演算ルールは、算出された数値に所定の演算を行うというルールを含む。

[0095] 例えば、記憶部は、ユーザと共有された規則に基づいて所定の期間ごとに変更される共有パターンを記憶する。例えば、記憶部は、基準となる中心数字と、中心数字を基準として仮数字を選択するパターンとを含む共有パターンを記憶する。例えば、記憶部は、ユーザと共有された規則に基づいて所定の期間ごとに変更されるパスワードを記憶する。

[0096] 本実施形態の認証装置によれば、ユーザと認証装置との間で共有しておいた共有情報に基づいて、認証装置によって一時的に生成された乱数列パターンを用いて計算されるキーコードを用いて認証するので、認証情報の漏洩を防止できる。

[0097] 例えば、本実施形態の認証装置は、銀行や郵便局、コンビニエンスストア、駅等に設置されたＡＴＭの認証に用いられる。例えば、本実施形態の認証装置は、クレジットカードやオンラインショッピング等の決済における認証に用いられる。例えば、本実施形態の認証装置は、セキュリティレベルの高いドアの開閉における認証に用いられる。例えば、本実施形態の認証装置は、指紋認証や静脈認証、顔認証、虹彩認証、歩容認証等の生体認証と組み合わせて用いられてもよい。なお、本実施形態の認証装置は、ここであげた例に限定されず、パスワード等の認証情報を用いた任意の認証に適用できる。

[0098] (第２の実施形態)

次に、第２の実施形態に係る認証システムについて図面を参照しながら説明する。本実施形態の認証システムは、ユーザによるキーコードの演算を認証装置の側で行い、そのキーコードをユーザの使用する携帯端末に送信する点において、第１の実施形態とは異なる。

[0099] (構成)

図１９は、本実施形態の認証システム２の構成の一例を示すブロック図である。認証システム２は、入力端末２１、認証装置２２、および携帯端末２３を備える。入力端末２１と認証装置２２は、インターネット等のネットワークを介して、通信可能に接続される。また、認証装置２２と携帯端末２３は、インターネット等のネットワークを介して、通信可能に接続される。

[0100] 例えば、入力端末２１は、銀行やコンビニエンスストア等に設置されたＡＴＭのような専用端末として提供される。また、入力端末２１は、パーソナルコンピュータやスマートフォン等の携帯端末にインストールされたアプリケーションソフトウェア（以下、アプリとも呼ぶ）として提供されてもよい。入力端末２１は、第１の実施形態の入力端末１１と同様であるので、詳細な説明は省略する。認証装置２２は、サーバやクラウドに構築される。認証装置２２は、ハードウェアであってもよいし、ソフトウェアであってもよい。携帯端末２３は、ユーザが所有する汎用の携帯機器であってもよいし、認証専用の携帯機器であってもよい。携帯端末２３を汎用の携帯機器で実現する場合、認証システム２の構成に携帯端末２３を含めなくてもよい。

[0101] 入力端末２１は、ユーザによる認証操作の開始を検出すると、そのユーザのＩＤ情報を認証装置２２に送信する。認証装置２２は、ユーザのＩＤ情報を入力端末２１から受信すると、そのＩＤ情報に対応付けて乱数列パターンを生成する。認証装置２２は、ＩＤ情報の送信元の入力端末２１に対して、生成された乱数列パターンを送信する。入力端末２１は、受信した乱数列パターンを自装置のユーザインタフェース（ＵＩ：User Interface）に表示させる。

[0102] 認証装置２２は、ユーザと認証装置２２との間で共有される共有情報を記

憶する。共有情報は、ユーザごとに設定されたパスワードおよび共有ルールを含む。パスワードは、ユーザによって予め設定された認証情報である。共有ルールは、ユーザと認証装置 2 2 との間で共有されるルールである。認証装置 2 2 は、ユーザの認証時に生成された乱数列パターンを用いて、予め設定された共有ルールに従ってキーコードを計算する。認証装置 2 2 は、算出したキーコードを携帯端末 2 3 に送信する。

[0103] 携帯端末 2 3 は、認証装置 2 2 からキーコードを受信する。携帯端末 2 3 は、認証装置 2 2 から受信されたキーコードを自装置の画面に表示させる。携帯端末 2 3 は、ユーザの操作に応じて、画面に表示されたキーコードを消す。また、携帯端末 2 3 は、所定時間が経過したら、画面に表示されたキーコードを消す。携帯端末 2 3 は、画面からキーコードを消すと、そのキーコードを自装置から削除する。

[0104] 例えば、携帯端末 2 3 は、キーコードを構成する数字を一つずつ順番に表示させてもよい。例えば、携帯端末 2 3 は、ユーザの操作に応じて、キーコードを構成する数字を表示させてもよい。例えば、携帯端末 2 3 は、キーコードを構成する数字を一つずつ順番に、フォントや大きさ、色、太さ、傾き、囲い等の表示状態を変更させて表示させてもよい。このように、キーコードを構成する数字を一括で表示させなかったり、異なる表示形態で表示されたりすれば、携帯端末 2 3 の画面に表示されたキーコードが盗み見られても、特定される可能性は低減する。

[0105] ユーザは、自身が所持する携帯端末 2 3 に表示されたキーコードを確認する。キーコードは、入力端末 2 1 の UI に表示された乱数列パターンにおいて、ユーザによって認証情報として入力される数字列である。ユーザは、携帯端末 2 3 に表示されたキーコードを、入力端末 2 1 の UI に表示された乱数列パターンに入力する。入力端末 2 1 は、UI を介して入力されたキーコードを認証装置 2 2 に送信する。

[0106] 認証装置 2 2 は、ユーザの操作する入力端末 2 1 からキーコードを受信する。認証装置 2 2 は、入力端末 2 1 から受信されたキーコードと、認証装置

２２によって算出されたキーコードとを比較する。認証装置２２は、入力端末２１から受信されたキーコードと、認証装置２２によって算出されたキーコードとが一致した場合、そのユーザを認証する。

[0107] 図２０は、認証装置２２の構成の一例を示すブロック図である。認証装置２２は、送受信部２２１、乱数列生成部２２２、記憶部２２３、演算部２２４、認証部２２５、およびキーコード送信部２２６を有する。図２０には、認証装置２２に接続される入力端末２１と携帯端末２３も併せて図示する。送受信部２２１、乱数列生成部２２２、記憶部２２３、演算部２２４、および認証部２２５は、第１の実施形態の認証装置１２に含まれる対応する構成と同様であるため、詳細な説明は省略する。

[0108] キーコード送信部２２６は、認証中のユーザに関して演算部２２４が算出したキーコードを、そのユーザの所持する携帯端末２３に送信する。送受信部２２１とキーコード送信部２２６を単一の構成としてもよい。

[0109] 図２１は、携帯端末２３の画面２３１にキーコードが表示される一例を示す概念図である。携帯端末２３は、自装置を所持するユーザによって認証に用いられるキーコードを認証装置から受信すると、そのキーコードを自装置の画面２３１に表示させる。図２１の例は、「４５３」というキーコードが、異なる表示状態で携帯端末２３の画面２３１に表示されている状態を示す。図２１には、キーコードを表示させた画面２３１に、キーコードの表示を消すための終了ボタン２３２を表示させる例を示す。例えば、携帯端末２３を所持するユーザは、携帯端末２３の画面２３１に表示されたキーコードを確認すると、終了ボタン２３２を押す。携帯端末２３の画面２３１に表示されたキーコードは、終了ボタン２３２が押されると画面２３１から消える。セキュリティを向上させるために、携帯端末２３の画面２３１に表示されたキーコードは、終了ボタン２３２が押されたタイミングで携帯端末２３から削除されることが好ましい。ユーザによる誤動作でキーコードが消えてしまった場合は、入力端末２１を用いた認証をやり直して、新たな乱数列パターンに基づいてキーコードを生成し直せばよい。また、セキュリティを向上さ

せるために、携帯端末 2 3 の画面 2 3 1 に表示されたキーコードは、所定時間が経過したタイミングで消されることが好ましい。

[0110] (動作)

次に、本実施形態の認証システム 2 の動作について図面を参照しながら説明する。以下においては、認証システム 2 を構成する入力端末 2 1、認証装置 2 2、および携帯端末 2 3 を動作主体とする例について説明する。

[0111] [入力端末]

図 2 2 は、入力端末 2 1 の動作について説明するためのフローチャートである。図 2 2 のフローチャートに沿った説明においては、入力端末 2 1 を動作主体として説明する。図 2 2 のフローチャートに沿った入力端末 2 1 の処理は、図 1 7 のフローチャートに沿った入力端末 1 1 の処理と同様である。

[0112] 図 2 2 において、まず、入力端末 2 1 は、認証対象ユーザのユーザ ID を受け付ける（ステップ S 2 1 1）。例えば、入力端末 2 1 は、入力端末 2 1 への認証カードの挿入や、ウェブ上の認証専用ページ等で ID 情報が入力されたことを、認証操作の開始として検出する。

[0113] 次に、入力端末 2 1 は、受け付けたユーザ ID を認証装置 2 2 に送信する（ステップ S 2 1 2）。

[0114] 次に、入力端末 2 1 は、自装置から送信されたユーザ ID に応じて送信された乱数列パターンを認証装置 2 2 から取得する（ステップ S 2 1 3）。

[0115] 次に、入力端末 2 1 は、取得された乱数列パターンを自装置の UI に表示させる（ステップ S 2 1 4）。入力端末 2 1 には、認証対象ユーザによって、共有ルールに基づいて選択された数字からなるキーコードが入力される。

[0116] 次に、入力端末 2 1 は、ユーザによって入力されたキーコードを認証装置 2 2 に送信する（ステップ S 2 1 5）。

[0117] 次に、入力端末 2 1 は、認証装置 2 2 から認証結果を受信する（ステップ S 2 1 6）。

[0118] 次に、入力端末 2 1 は、認証結果に応じた情報を自装置の UI に表示させる（ステップ S 2 1 7）。例えば、認証装置 2 2 によって認証された場合、

認証対象ユーザには、認証結果に応じたサービスが提供される。

[0119] 〔認証装置〕

図 2 3 は、認証装置 2 2 の動作について説明するためのフローチャートである。図 2 3 のフローチャートに沿った説明においては、認証装置 2 2 を動作主体として説明する。

[0120] 図 2 3 において、まず、認証装置 2 2 は、認証対象ユーザのユーザ ID を入力端末 2 1 から受信する（ステップ S 2 2 1）。

[0121] 次に、認証装置 2 2 は、ユーザ ID に対応付けて、乱数列パターンを生成する（ステップ S 2 2 2）。

[0122] 次に、認証装置 2 2 は、生成された乱数列パターンを入力端末 2 1 に送信する（ステップ S 2 2 3）。

[0123] 次に、認証装置 2 2 は、生成された乱数列パターンと、ユーザ ID に対応する共有情報とを用いて、キーコードを生成する（ステップ S 2 2 4）。

[0124] 次に、認証装置 2 2 は、生成されたキーコードを携帯端末 2 3 に送信する（ステップ S 2 2 5）。

[0125] 次に、認証装置 2 2 は、入力端末 2 1 からキーコードを受信する（ステップ S 2 2 6）。

[0126] 次に、認証装置 2 2 は、入力端末 2 1 から受信されたキーコードと、自装置で生成されたキーコードとを比較する（ステップ S 2 2 7）。認証装置 2 2 は、入力端末 2 1 から受信されたキーコードと、自装置で生成されたキーコードとが一致する場合、認証中のユーザを認証するという認証結果を生成する。認証装置 2 2 は、入力端末 2 1 から受信されたキーコードと、自装置で生成されたキーコードとが一致しない場合、認証中のユーザを認証しないという認証結果を生成する。

[0127] 次に、認証装置 2 2 は、入力端末 2 1 に認証結果を送信する（ステップ S 2 2 8）。例えば、認証されたユーザに対してサービスを提供するシステムは、認証装置 2 2 によって認証されたユーザに対して所定のサービスを提供する。

[0128] 〔携帯端末〕

図 2 4 は、携帯端末 2 3 の動作について説明するためのフローチャートである。図 2 4 のフローチャートに沿った説明においては、携帯端末 2 3 を動作主体として説明する。

[0129] 図 2 4 において、まず、携帯端末 2 3 は、自装置を所持するユーザが認証で用いるキーコードを認証装置 2 2 から受信する（ステップ S 2 3 1）。

[0130] 次に、携帯端末 2 3 は、受信されたキーコードを自装置の画面に表示させる（ステップ S 2 3 2）。

[0131] 自装置の画面に表示された終了ボタンが押されると（ステップ S 2 3 3 で Y e s）、携帯端末 2 3 は、画面からキーコードを消す（ステップ S 2 3 5）。

[0132] 自装置の画面に表示された終了ボタンが押されていなくても（ステップ S 2 3 3 で N o）、所定時間が経過したら（ステップ S 2 3 4 で Y e s）、携帯端末 2 3 は、画面からキーコードを消す（ステップ S 2 3 5）。所定時間が経過していない場合（ステップ S 2 3 4 で N o）、携帯端末 2 3 は、終了ボタンの押下または所定時間の経過を待機する。

[0133] 以上のように、本実施形態の認証システムは、入力端末、認証装置、および携帯端末を備える。入力端末と認証装置は、通信可能に接続される。また、携帯端末は、認証対象ユーザに所持され、認証装置と通信可能に接続される。入力端末は、認証対象ユーザの識別情報を受け付け、受け付けた識別情報を認証装置に送信する。認証装置は、ユーザごとに予め設定されたパスワードおよび共有ルールを含む共有情報を記憶しておく。認証装置は、認証対象ユーザの操作する入力端末から認証対象ユーザの識別情報を受信する。認証装置は、認証対象ユーザの識別情報の受信に応じて、複数の異なる数字によって構成される乱数列パターンを生成する。認証装置は、生成された乱数列パターンを識別情報に対応付けて入力端末に送信する。認証装置は、共有ルールに基づいて、乱数列パターンから複数の仮数字を選択する。認証装置は、選択された複数の仮数字と、パスワードを構成する複数の秘密数字とを

用いてキーコードを生成する。認証装置は、認証対象ユーザの使用する携帯端末に、生成されたキーコードを送信する。入力端末は、識別情報に対応付けられて認証装置によって生成された乱数列パターンを認証装置から受信する。入力端末は、乱数列パターンを自装置のユーザインタフェースに表示させる。携帯端末は、認証装置から受信されたキーコードを自装置の画面に表示させる。入力端末は、携帯端末のキーコードを確認したユーザによって、ユーザインタフェースを介して入力されたキーコードを認証装置に送信する。認証装置は、認証対象ユーザによって共有ルールに基づいて乱数列パターンから選択された数字からなるキーコードを、入力端末から受信する。認証装置は、入力端末から受信されたキーコードと、自装置で生成されたキーコードとに基づいて、認証対象ユーザを認証する。

[0134] 本実施形態によれば、認証対象ユーザが共有ルールを思い出せない状況であっても、外部からは特定できない演算方法によって生成されたキーコードを介して認証を行うので、認証情報の漏洩を防止できる。

[0135] (第3の実施形態)

次に、第3の実施形態に係る認証装置について図面を参照しながら説明する。本実施形態の認証装置は、第1～第2の実施形態の認証装置を簡略化した構成である。

[0136] 図25は、本実施形態の認証装置32の構成の一例を示すブロック図である。認証装置32は、送受信部321、乱数列生成部322、記憶部323、演算部324、および認証部325を備える。

[0137] 送受信部321は、認証対象ユーザの認証機会において、認証対象ユーザの操作する入力端末から認証対象ユーザの識別情報を受信する。送受信部321は、認証対象ユーザの認証機会に生成された乱数列パターンを識別情報に対応付けて入力端末に送信する。送受信部321は、認証対象ユーザによって共有ルールに基づいて乱数列パターンから選択された数字からなるキーコードを入力端末から受信する。

[0138] 乱数列生成部322は、認証対象ユーザの認証機会ごとに、複数の異なる

数字によって構成される乱数列パターンを生成する。

[0139] 記憶部 323 には、ユーザごとに予め設定されたパスワードおよび共有ルールを含む共有情報が記憶される。

[0140] 演算部 324 は、共有ルールに基づいて、乱数列パターンから複数の仮数字を選択する。演算部 324 は、選択された複数の仮数字と、パスワードを構成する複数の秘密数字とを用いてキーコードを生成する。

[0141] 認証部 325 は、入力端末から受信されたキーコードと、演算部によって生成されたキーコードとに基づいて、認証対象ユーザを認証する。

[0142] 本実施形態の認証装置によれば、ユーザと認証装置との間で共有しておいた共有情報に基づいて、認証装置によって一時的に生成された乱数列パターンを用いて計算されるキーコードを用いて認証するので、認証情報の漏洩を防止できる。

[0143] (ハードウェア)

ここで、各実施形態に係る入力端末や認証端末、携帯端末等の装置による処理を実行するハードウェア構成について、図 26 の情報処理装置 90 を一例としてあげて説明する。なお、図 26 の情報処理装置 90 は、各実施形態の装置の処理を実行するための構成例であって、本発明の範囲を限定するものではない。

[0144] 図 26 のように、情報処理装置 90 は、プロセッサ 91、主記憶装置 92、補助記憶装置 93、入出力インタフェース 95、および通信インタフェース 96 を備える。図 26 においては、インタフェースを I/F (Interface) と略して表記する。プロセッサ 91、主記憶装置 92、補助記憶装置 93、入出力インタフェース 95、および通信インタフェース 96 は、バス 98 を介して互いにデータ通信可能に接続される。また、プロセッサ 91、主記憶装置 92、補助記憶装置 93 および入出力インタフェース 95 は、通信インタフェース 96 を介して、インターネットやイントラネットなどのネットワークに接続される。

[0145] プロセッサ 91 は、補助記憶装置 93 等に格納されたプログラムを主記憶

装置 9 2 に展開し、展開されたプログラムを実行する。本実施形態においては、情報処理装置 9 0 にインストールされたソフトウェアプログラムを用いる構成とすればよい。プロセッサ 9 1 は、各実施形態に係る装置による処理を実行する。

[0146] 主記憶装置 9 2 は、プログラムが展開される領域を有する。主記憶装置 9 2 は、例えば D R A M (Dynamic Random Access Memory) などの揮発性メモリとすればよい。また、M R A M (Magnetoresistive Random Access Memory) などの不揮発性メモリを主記憶装置 9 2 として構成・追加してもよい。

[0147] 補助記憶装置 9 3 は、種々のデータを記憶する。補助記憶装置 9 3 は、ハードディスクやフラッシュメモリなどのローカルディスクによって構成される。なお、種々のデータを主記憶装置 9 2 に記憶させる構成とし、補助記憶装置 9 3 を省略することも可能である。

[0148] 入出力インタフェース 9 5 は、情報処理装置 9 0 と周辺機器とを接続するためのインタフェースである。通信インタフェース 9 6 は、規格や仕様に基づいて、インターネットやイントラネットなどのネットワークを通じて、外部のシステムや装置に接続するためのインタフェースである。入出力インタフェース 9 5 および通信インタフェース 9 6 は、外部機器と接続するインタフェースとして共通化してもよい。

[0149] 情報処理装置 9 0 には、必要に応じて、キーボードやマウス、タッチパネルなどの入力機器を接続するように構成してもよい。それらの入力機器は、情報や設定の入力に使用される。なお、タッチパネルを入力機器として用いる場合は、表示機器の表示画面が入力機器のインタフェースを兼ねる構成とすればよい。プロセッサ 9 1 と入力機器との間のデータ通信は、入出力インタフェース 9 5 に仲介させればよい。

[0150] また、情報処理装置 9 0 には、情報を表示するための表示機器を備え付けてもよい。表示機器を備え付ける場合、情報処理装置 9 0 には、表示機器の表示を制御するための表示制御装置（図示しない）が備えられていることが好ましい。表示機器は、入出力インタフェース 9 5 を介して情報処理装置 9

0に接続すればよい。

[0151] 以上が、各実施形態に係る装置を可能とするためのハードウェア構成の一例である。なお、図26のハードウェア構成は、各実施形態に係る装置の演算処理を実行するためのハードウェア構成の一例であって、本発明の範囲を限定するものではない。また、各実施形態に係る装置に関する処理をコンピュータに実行させるプログラムも本発明の範囲に含まれる。さらに、各実施形態に係るプログラムを記録した記録媒体も本発明の範囲に含まれる。記録媒体は、例えば、CD (Compact Disc) やDVD (Digital Versatile Disc) などの光学記録媒体で実現できる。また、記録媒体は、USB (Universal Serial Bus) メモリやSD (Secure Digital) カードなどの半導体記録媒体や、フレキシブルディスクなどの磁気記録媒体、その他の記録媒体によって実現してもよい。

[0152] 各実施形態の装置の構成要素は、任意に組み合わせることができる。また、各実施形態の装置の構成要素は、ソフトウェアによって実現してもよいし、回路によって実現してもよい。

[0153] 以上、実施形態を参照して本発明を説明してきたが、本発明は上記実施形態に限定されるものではない。本発明の構成や詳細には、本発明のScope内で当業者が理解し得る様々な変更をすることができる。

[0154] この出願は、2020年9月14日に提出された日本出願特願2020-153425を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

- [0155] 1、2 認証システム
- 11、21 入力端末
- 12、22、32 認証装置
- 23 携帯端末
- 111 UI
- 112 表示制御部
- 113 送受信部

1 2 1、2 2 1、3 2 1	送受信部
1 2 2、2 2 2、3 2 2	乱数列生成部
1 2 3、2 2 3、3 2 3	記憶部
1 2 4、2 2 4、3 2 4	演算部
1 2 5、2 2 5、3 2 5	認証部
2 2 6	キーコード送信部

請求の範囲

- [請求項1] ユーザごとに予め設定されたパスワードおよび共有ルールを含む共有情報が記憶される記憶部と、
- 認証対象ユーザの認証機会ごとに、複数の異なる数字によって構成される乱数列パターンを生成する乱数列生成部と、
- 前記共有ルールに基づいて、前記乱数列パターンから複数の仮数字を選択し、選択された前記複数の仮数字と、前記パスワードを構成する複数の秘密数字とを用いてキーコードを生成する演算部と、
- 前記認証対象ユーザの認証機会において、前記認証対象ユーザの操作する入力端末から前記認証対象ユーザの識別情報を受信し、前記認証対象ユーザの認証機会に生成された前記乱数列パターンを前記識別情報に対応付けて前記入力端末に送信し、前記認証対象ユーザによって前記共有ルールに基づいて前記乱数列パターンから選択された数字からなる前記キーコードを前記入力端末から受信する送受信部と、
- 前記入力端末から受信された前記キーコードと、前記演算部によって生成された前記キーコードとに基づいて、前記認証対象ユーザを認証する認証部と、を備える認証装置。
- [請求項2] 前記記憶部は、
- 前記ユーザによって予め設定された共有パターンおよび演算ルールを含む前記共有ルールを記憶し、
- 前記共有パターンは、
- 複数の異なる数字がマトリックス状に配置された前記乱数列パターンから前記仮数字を選択する順番を示すパターンであり、
- 前記演算ルールは、
- 前記乱数列パターンから選択された前記仮数字と、前記パスワードを構成する前記秘密数字とを用いた演算に関するルールである請求項1に記載の認証装置。
- [請求項3] 前記記憶部は、

前記乱数列パターンから選択された前記仮数字と、前記パスワードを構成する前記秘密数字とを用いた演算によって算出された数値が、前記乱数列パターンを構成する前記複数の数字に含まれない場合、算出された前記数値に所定の演算を行うというルールを含む前記演算ルールを記憶する請求項2に記載の認証装置。

[請求項4]

前記記憶部は、

前記ユーザと共有された規則に基づいて所定の期間ごとに変更される前記共有パターンを記憶する請求項2または3に記載の認証装置。

[請求項5]

前記記憶部は、

基準となる中心数字と、前記中心数字を基準として前記仮数字を選択するパターンとを含む前記共有パターンを記憶する請求項2または3に記載の認証装置。

[請求項6]

前記記憶部は、

前記ユーザと共有された規則に基づいて所定の期間ごとに変更される前記パスワードを記憶する請求項2または3に記載の認証装置。

[請求項7]

前記認証対象ユーザの使用する携帯端末に、前記演算部によって生成された前記キーコードを送信するキーコード送信部を備える請求項1乃至6のいずれか一項に記載の認証装置。

[請求項8]

請求項1乃至7のいずれか一項に記載の認証装置と、

前記認証装置に通信可能に接続される入力端末と、を備え、

前記入力端末は、

認証対象ユーザから受け付けた識別情報を前記認証装置に送信し、

前記識別情報に対応付けられて前記認証装置によって生成された乱数列パターンを前記認証装置から受信し、

前記乱数列パターンを自装置のユーザインタフェースに表示させ、

前記ユーザインタフェースを介して前記認証対象ユーザによって前記乱数列パターンから選択された数字からなるキーコードを前記認証装置に送信する認証システム。

[請求項9] ユーザごとに予め設定されたパスワードおよび共有ルールを含む共有情報を記憶部に記憶しておき、

認証対象ユーザの操作する入力端末から前記認証対象ユーザの識別情報を受信し、

前記認証対象ユーザの識別情報の受信に応じて、複数の異なる数字によって構成される乱数列パターンを生成し、

生成された前記乱数列パターンを前記識別情報に対応付けて前記入力端末に送信し、

前記共有ルールに基づいて、前記乱数列パターンから複数の仮数字を選択し、

選択された前記複数の仮数字と、前記パスワードを構成する複数の秘密数字とを用いてキーコードを生成し、

前記認証対象ユーザによって前記共有ルールに基づいて前記乱数列パターンから選択された数字からなる前記キーコードを前記入力端末から受信し、

前記入力端末から受信された前記キーコードと、自装置で生成された前記キーコードとに基づいて、前記認証対象ユーザを認証する認証方法。

[請求項10] ユーザごとに予め設定されたパスワードおよび共有ルールを含む共有情報を記憶部に記憶しておく処理と、

認証対象ユーザの操作する入力端末から前記認証対象ユーザの識別情報を受信する処理と、

前記認証対象ユーザの識別情報の受信に応じて、複数の異なる数字によって構成される乱数列パターンを生成する処理と、

生成された前記乱数列パターンを前記識別情報に対応付けて前記入力端末に送信する処理と、

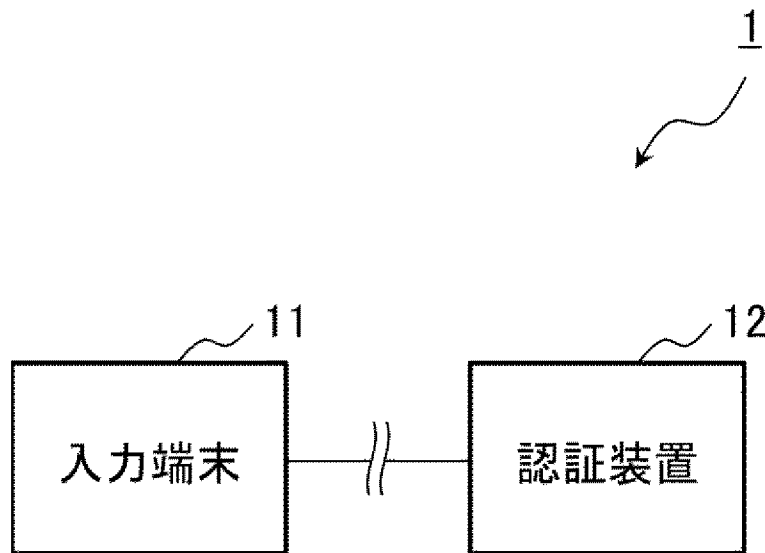
前記共有ルールに基づいて、前記乱数列パターンから複数の仮数字を選択する処理と、

選択された前記複数の仮数字と、前記パスワードを構成する複数の秘密数字とを用いてキーコードを生成する処理と、

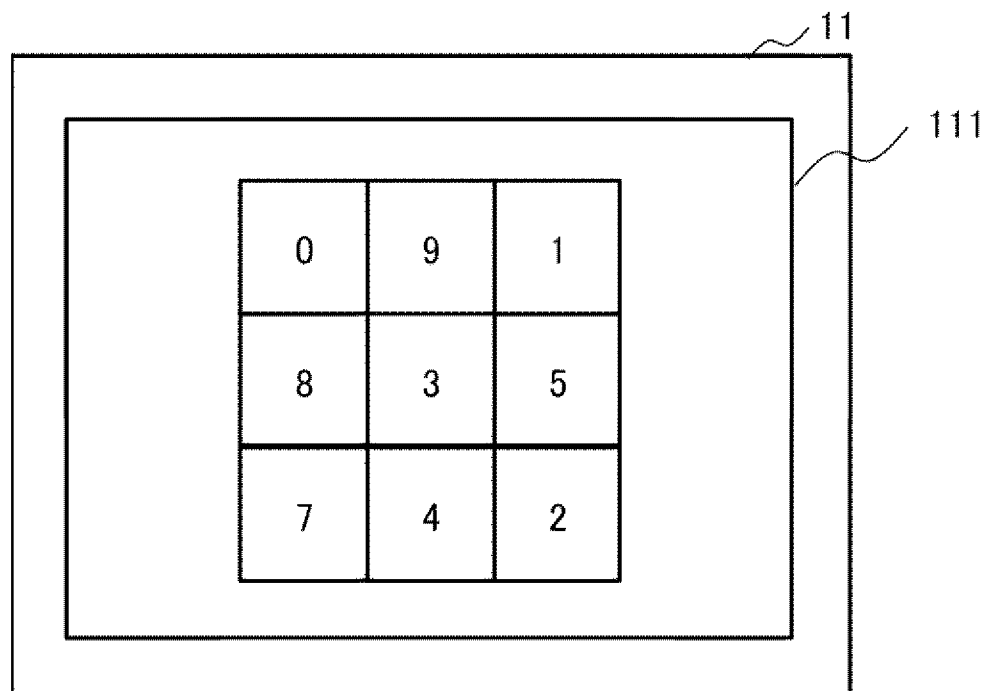
前記共有ルールに基づいて前記認証対象ユーザによって前記乱数列パターンから選択された数字からなる前記キーコードを前記入力端末から受信する処理と、

前記入力端末から受信された前記キーコードと、自装置で生成された前記キーコードとに基づいて、前記認証対象ユーザを認証する処理と、をコンピュータに実行させるプログラムが記録された非一過性の記録媒体。

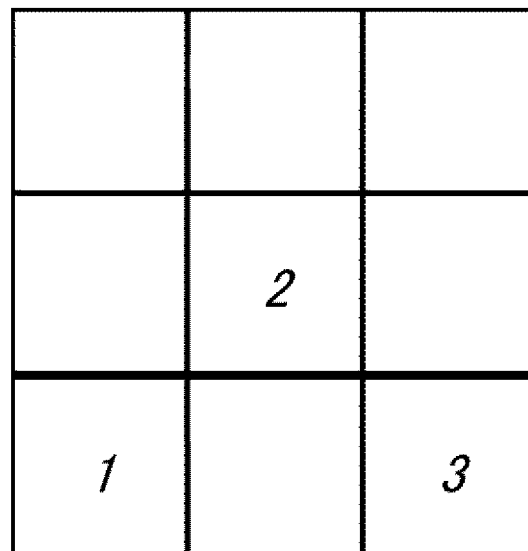
[図1]



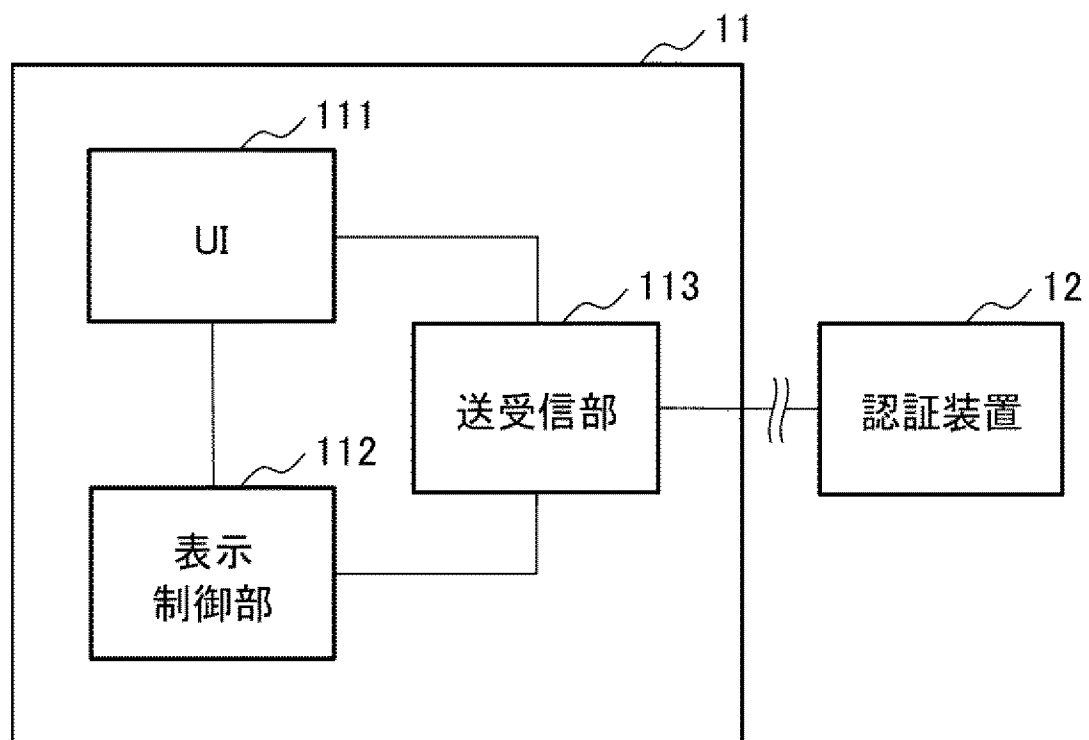
[図2]



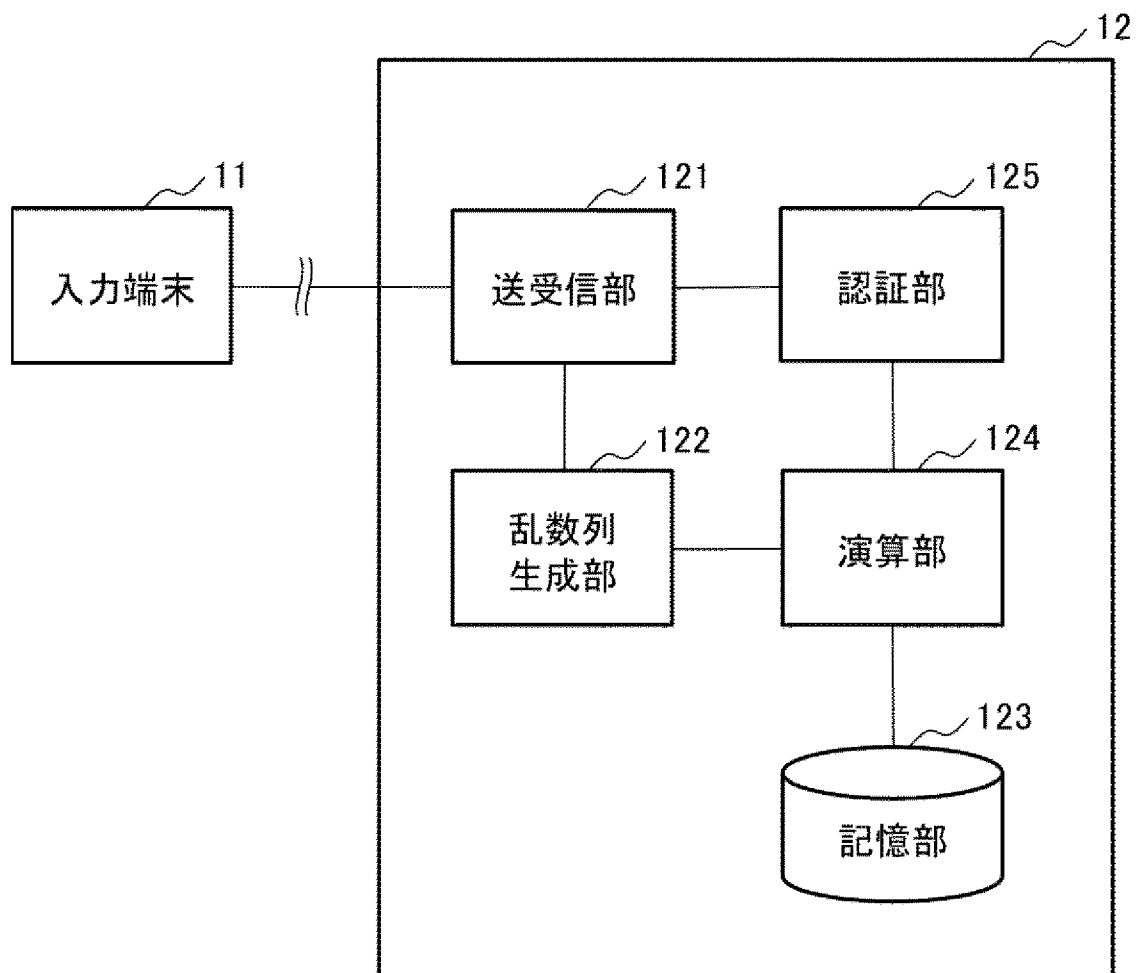
[図3]



[図4]



[図5]

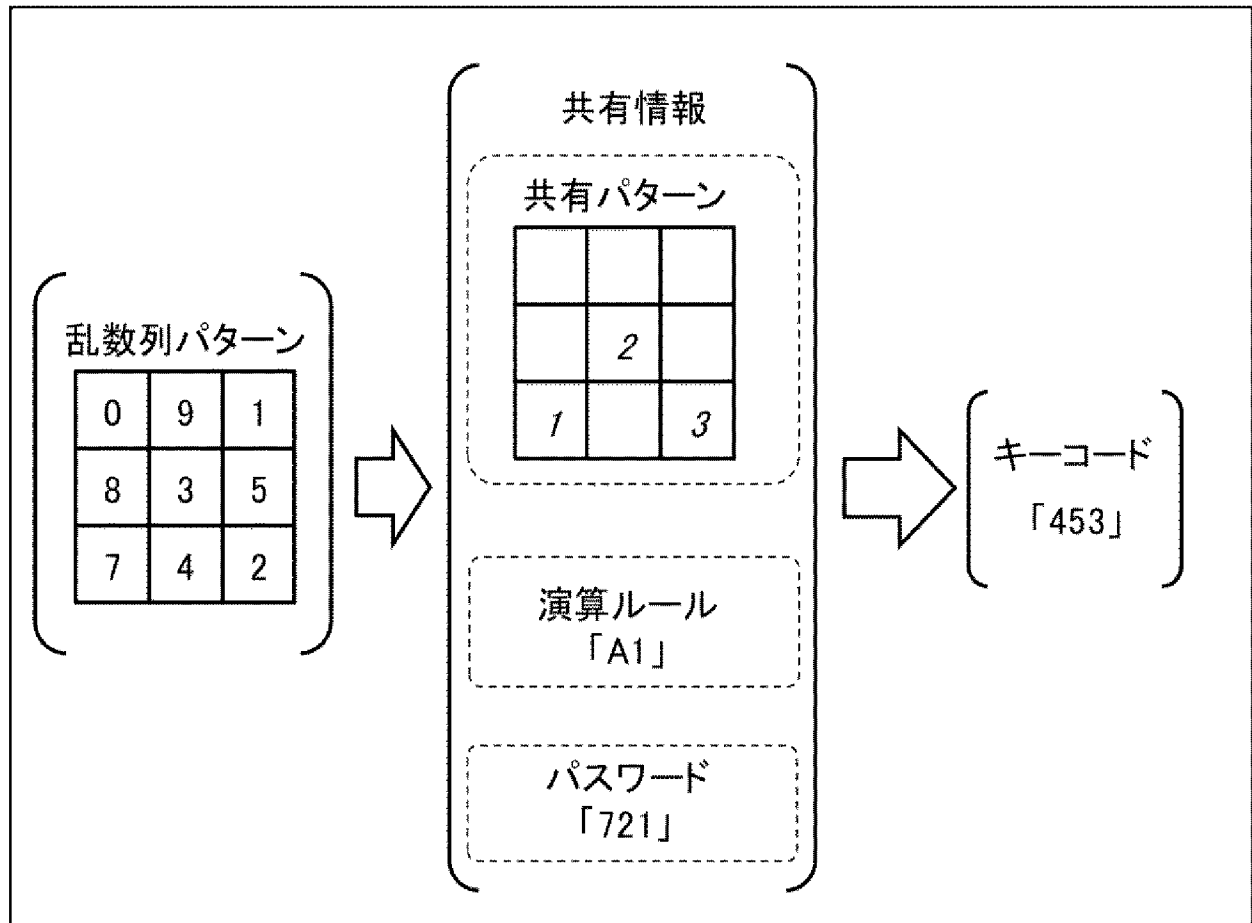


[図6]

131

ユーザID	共有情報			...									
	パスワード	共有ルール											
		共有パターン	演算ルール										
AAA	721	<table><tr><td></td><td></td><td></td></tr><tr><td></td><td>2</td><td></td></tr><tr><td>1</td><td></td><td>3</td></tr></table>					2		1		3	A1	
	2												
1		3											
BBB	853	<table><tr><td>1</td><td></td><td>2</td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td>3</td></tr></table>	1		2						3	B1	
1		2											
		3											
CCC	224	<table><tr><td></td><td></td><td>1</td></tr><tr><td></td><td>2</td><td>3</td></tr><tr><td></td><td></td><td></td></tr></table>			1		2	3				C1	
		1											
	2	3											
...	...	...	...	...									

[図7]

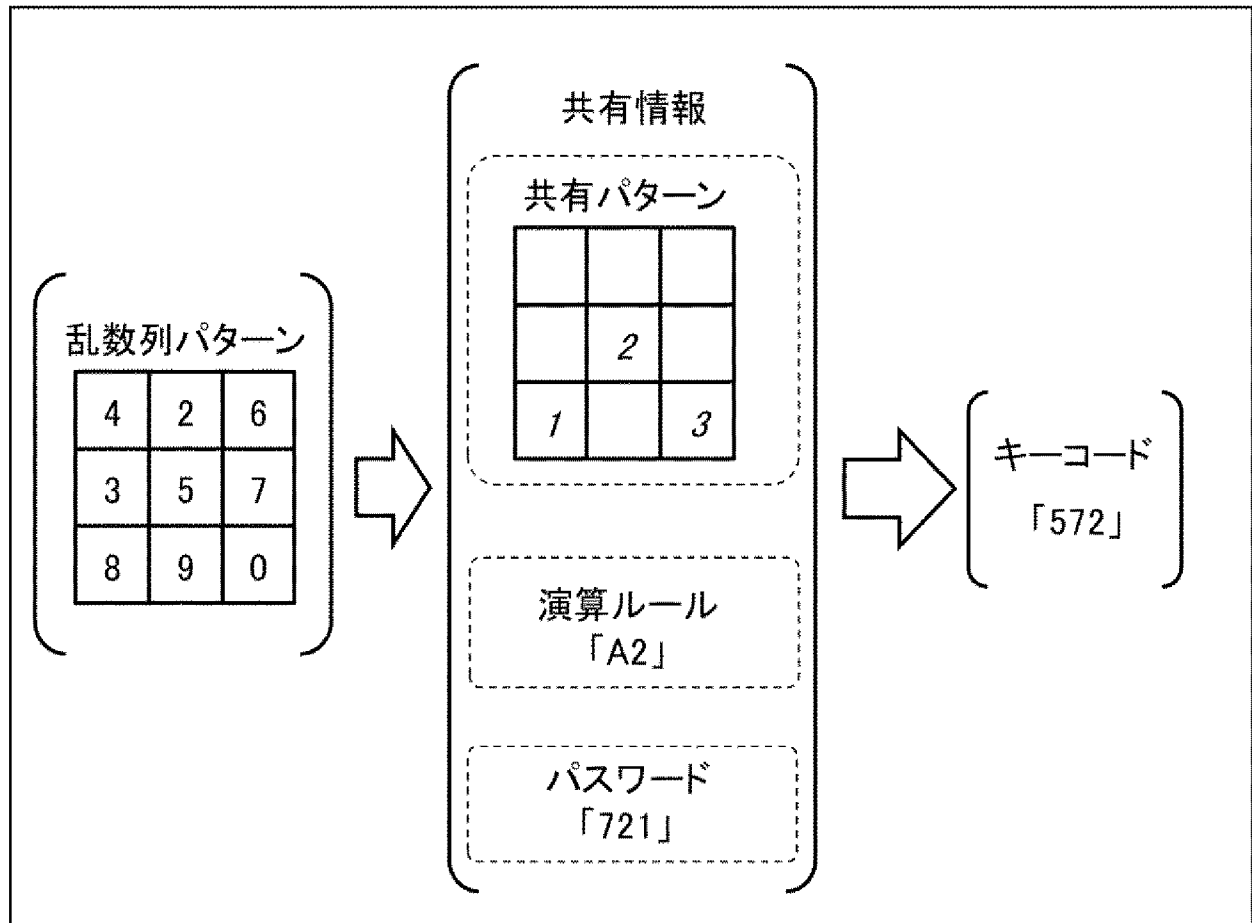


[図8]

132

ユーザID	共有情報			...									
	パスワード	共有ルール											
		共有パターン	演算ルール										
AAA	721	<table><tr><td></td><td></td><td></td></tr><tr><td></td><td>2</td><td></td></tr><tr><td>1</td><td></td><td>3</td></tr></table>					2		1		3	A2	
	2												
1		3											
BBB	853	<table><tr><td>1</td><td></td><td>2</td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td>3</td></tr></table>	1		2						3	B2	
1		2											
		3											
CCC	224	<table><tr><td></td><td></td><td>1</td></tr><tr><td></td><td>2</td><td>3</td></tr><tr><td></td><td></td><td></td></tr></table>			1		2	3				C2	
		1											
	2	3											
...	...	...	...	...									

[図9]

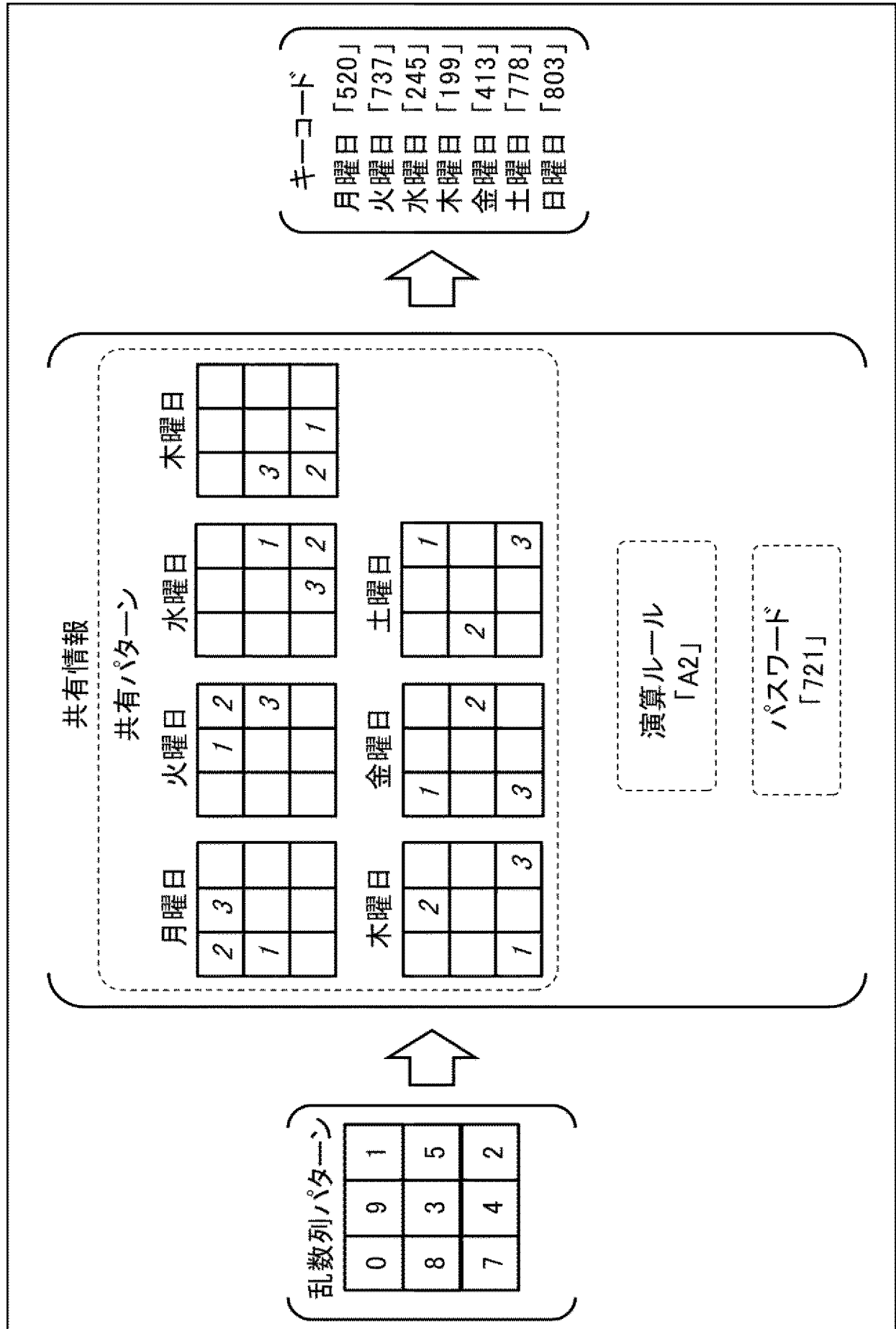


[図10]

133

ユーザID	共有情報			...													
	パスワード	共有ルール															
		共有パターン	演算ルール														
AAA	721	月曜日	<table><tr><td>2</td><td>3</td><td></td><td></td></tr><tr><td>1</td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>	2	3			1								A2	...
		2	3														
		1															
火曜日	<table><tr><td></td><td>1</td><td>2</td><td></td></tr><tr><td></td><td></td><td></td><td>3</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>		1	2					3								
	1	2															
			3														
水曜日	<table><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td>1</td></tr><tr><td></td><td></td><td>3</td><td>2</td></tr></table>								1			3	2				
			1														
		3	2														
...	...	...															
...	...	...	...	...	...												

[図11]

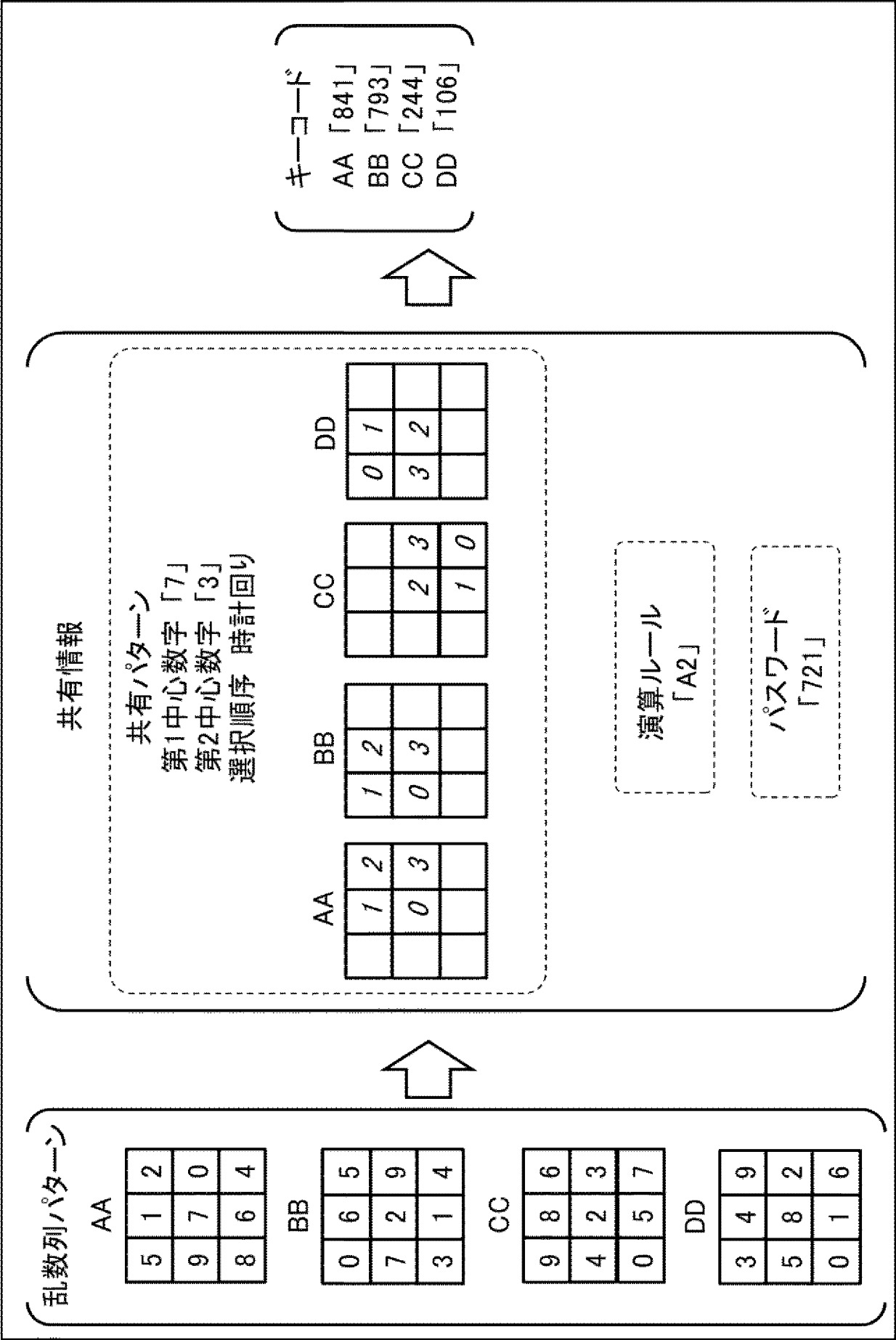


[図12]

134

ユーザID	共有情報			...
	パスワード	共有ルール		
		共有パターン	演算ルール	
AAA	721	第1中心数字:7 第2中心数字:3 選択順序:時計回り	A2	...
BBB	853	第1中心数字:5 第2中心数字:1 選択順序:時計回り	B2	...
CCC	224	第1中心数字:1 第2中心数字:9 選択順序:反時計回り	C2	...
...	...	...	...	...

[図13]

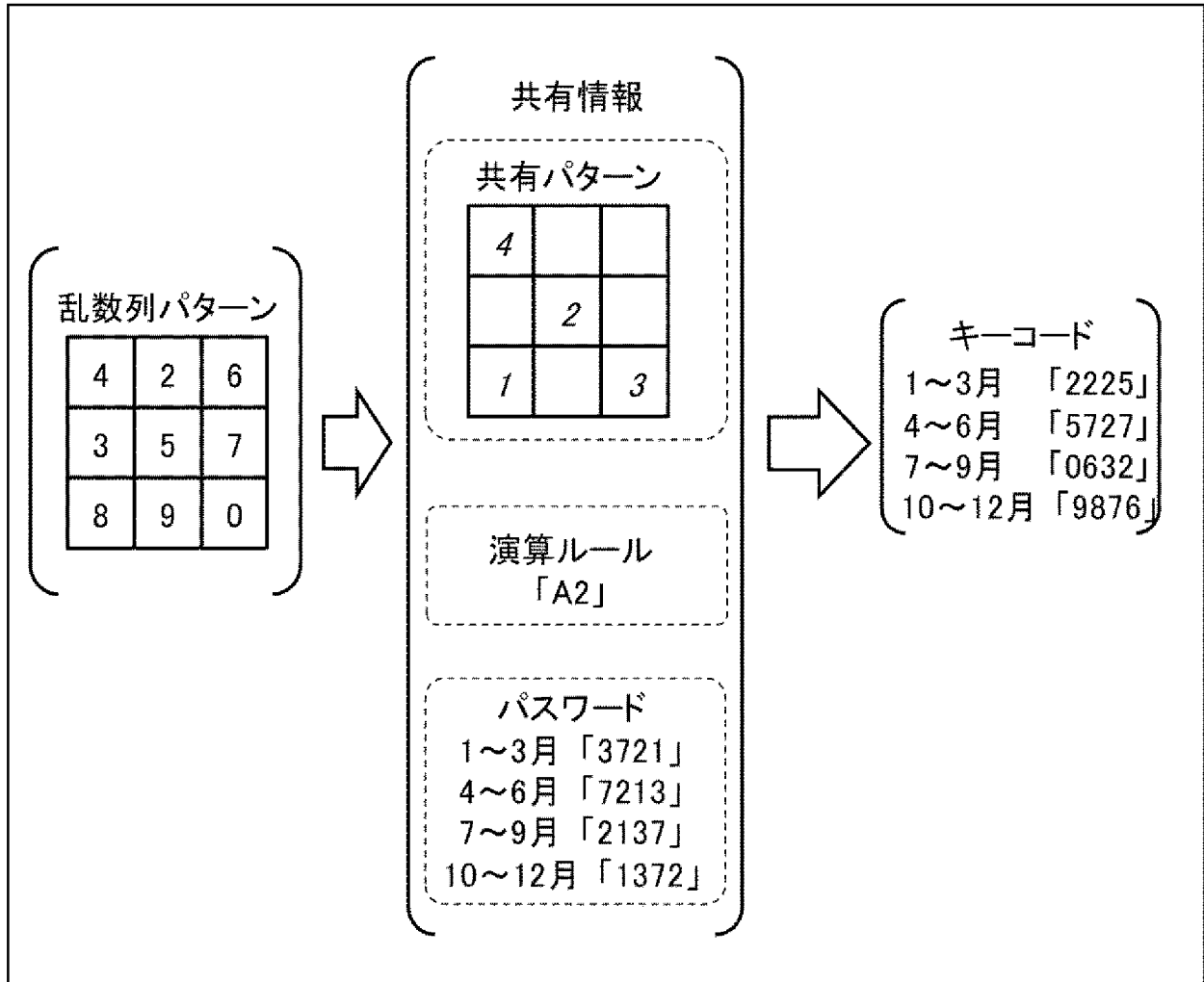


[図14]

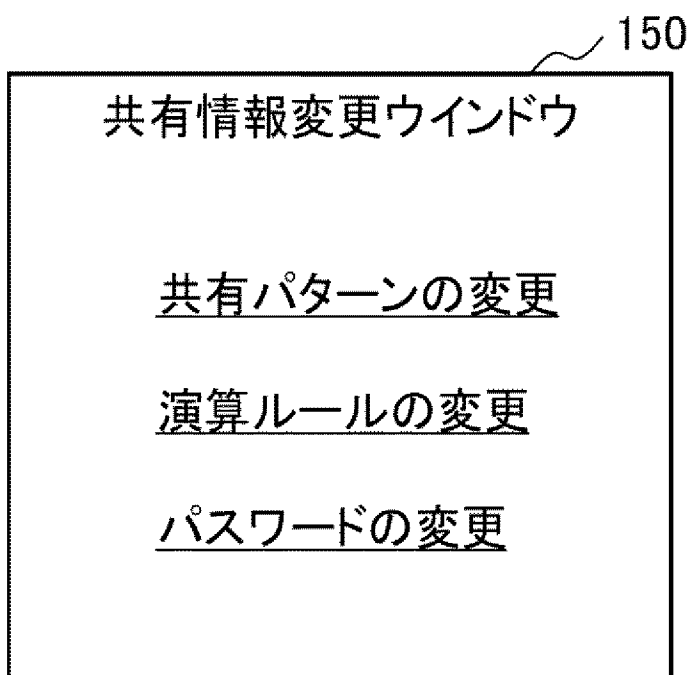
135

ユーザID	共有情報				...								
	パスワード	共有ルール		演算ルール	...								
		共有パターン			...								
AAA	1～3月:3721 4～6月:7213 7～9月:2137 10～12月:1372	<table><tr><td>4</td><td></td><td></td></tr><tr><td></td><td>2</td><td></td></tr><tr><td>1</td><td></td><td>3</td></tr></table>	4				2		1		3	A2	...
4													
	2												
1		3											
BBB	1～3月:8531 4～6月:5318 7～9月:3185 10～12月:1853	<table><tr><td>1</td><td></td><td>2</td></tr><tr><td></td><td>4</td><td></td></tr><tr><td></td><td></td><td>3</td></tr></table>	1		2		4				3	B2	...
1		2											
	4												
		3											
CCC	1～3月:2241 4～6月:2412 7～9月:4122 10～12月:1224	<table><tr><td>4</td><td></td><td>1</td></tr><tr><td></td><td>2</td><td>3</td></tr><tr><td></td><td></td><td></td></tr></table>	4		1		2	3				C2	...
4		1											
	2	3											
...	...	...	...	...									

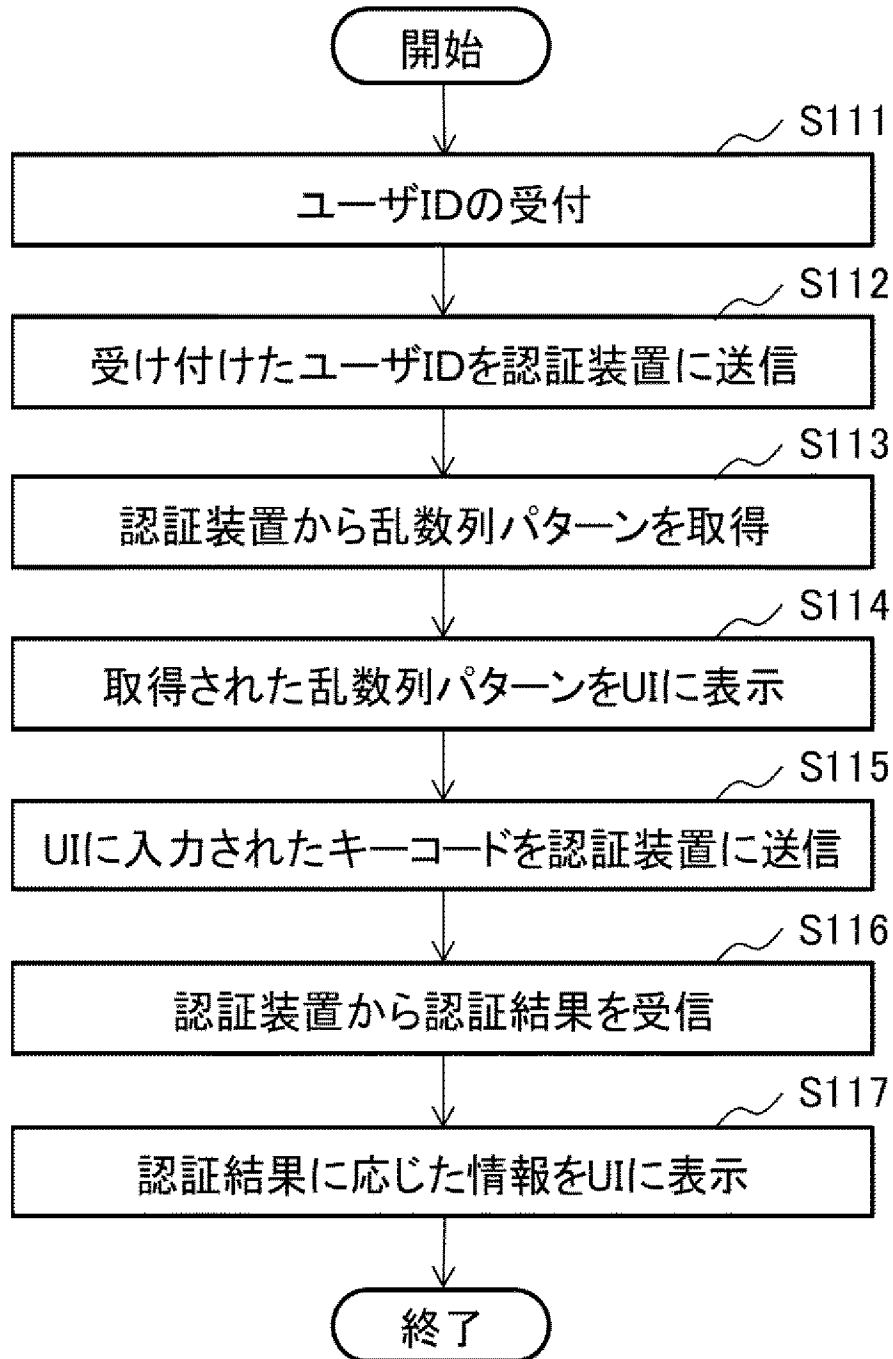
[図15]



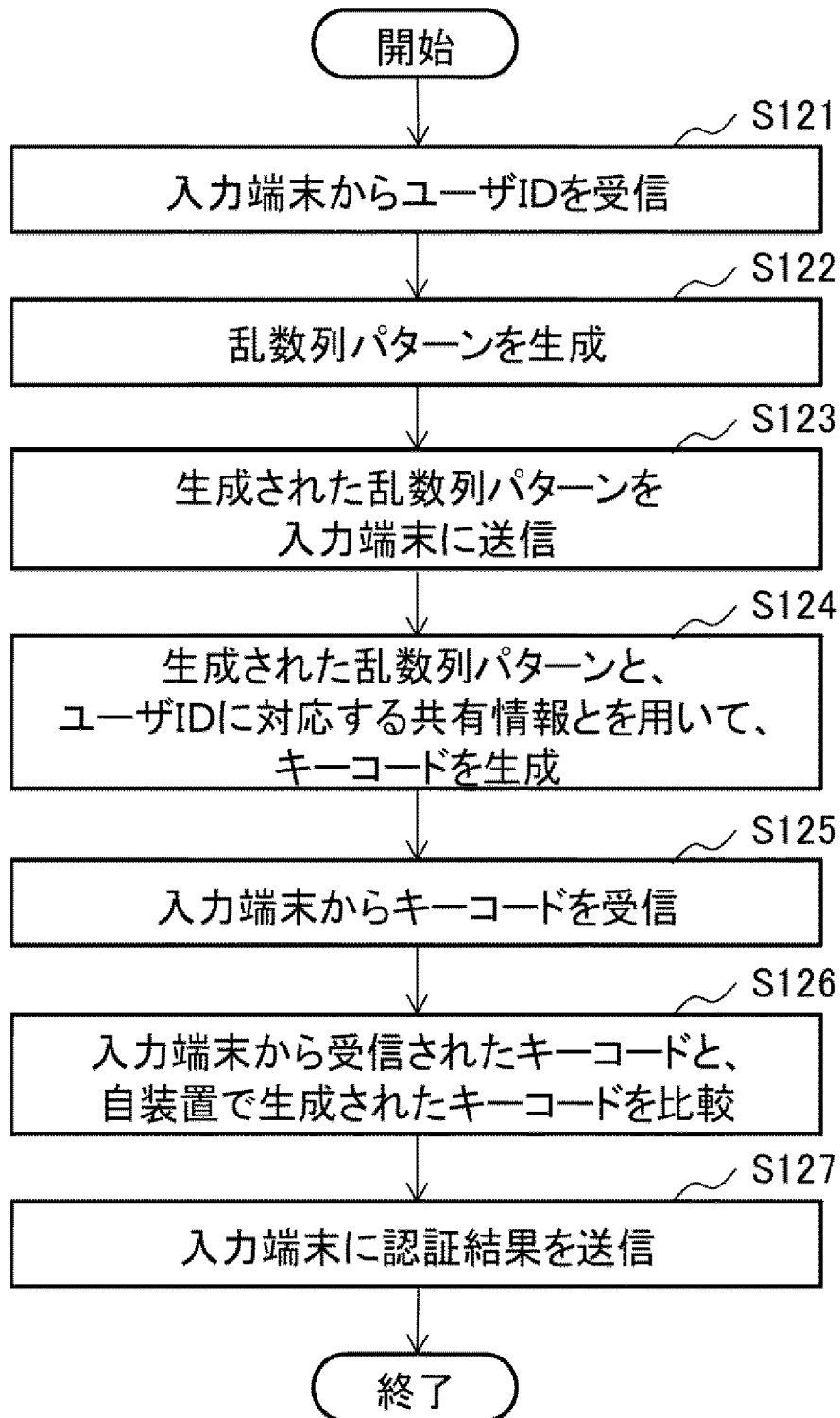
[図16]



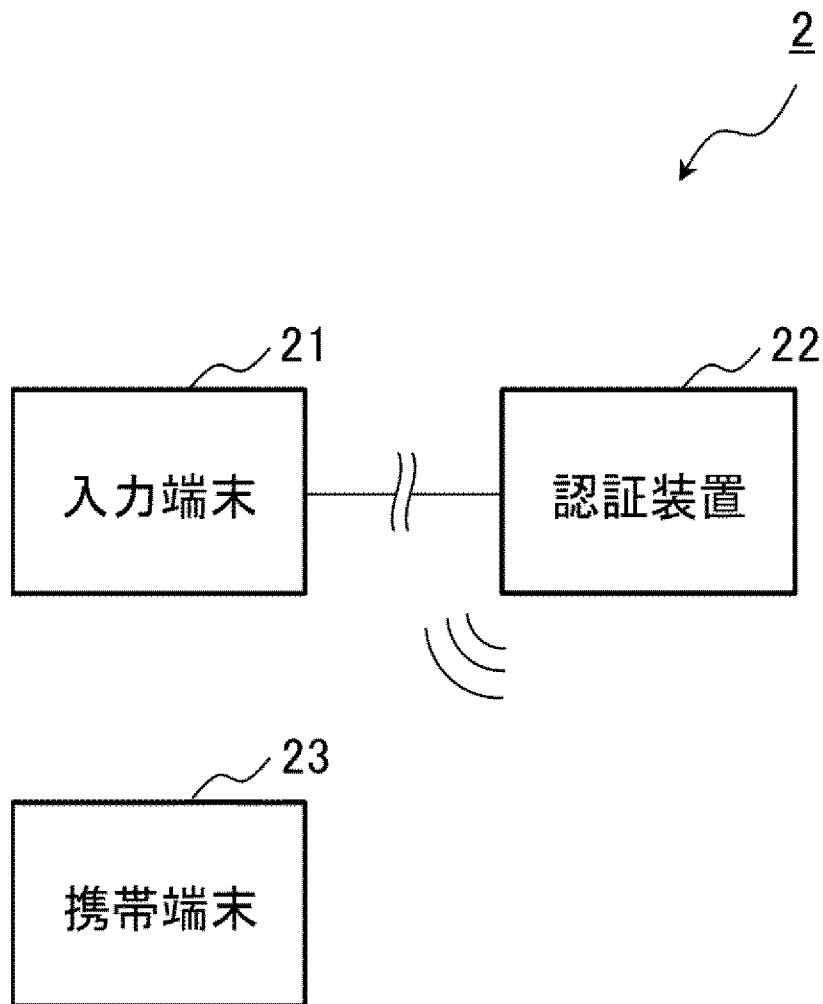
[図17]



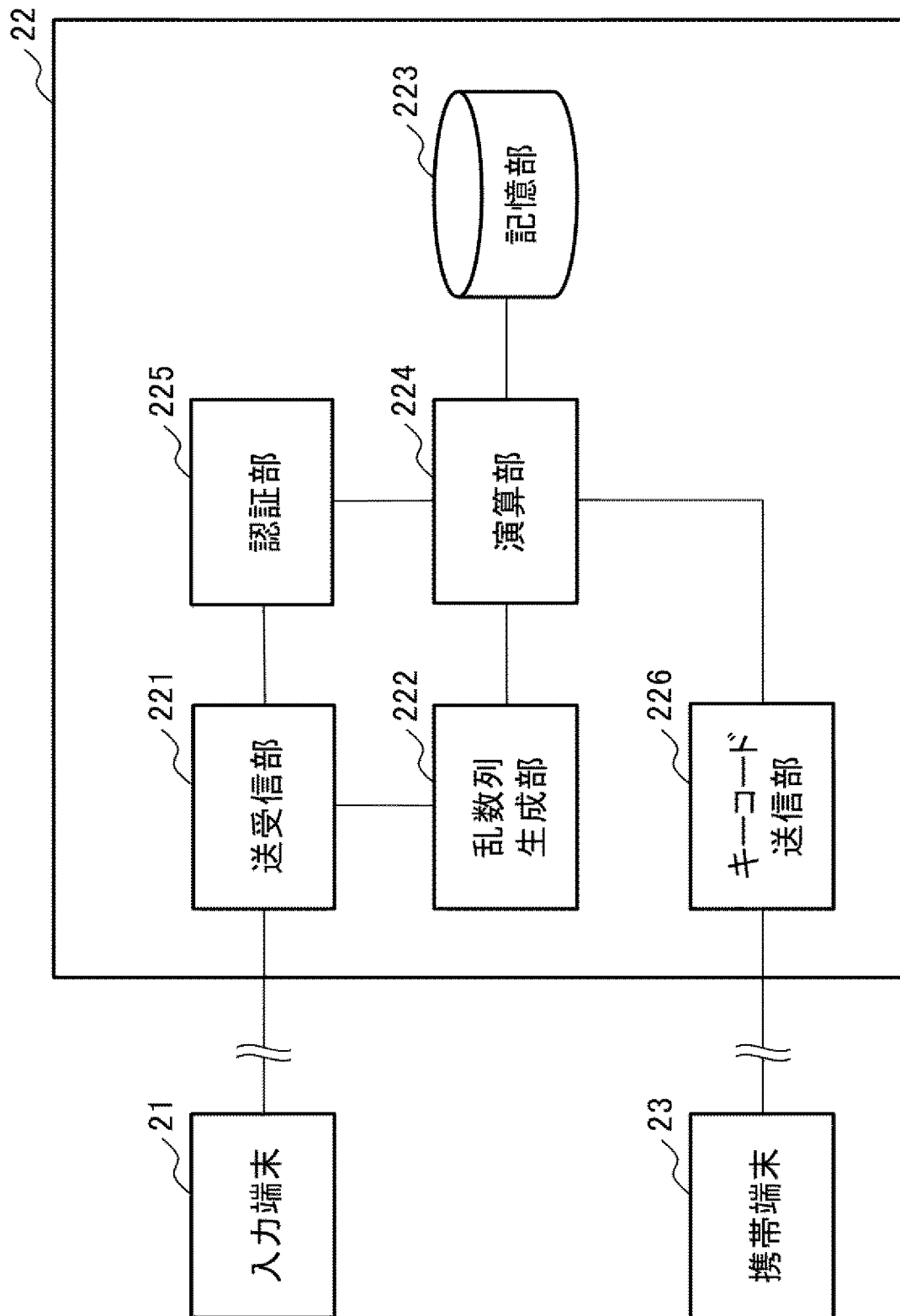
[図18]



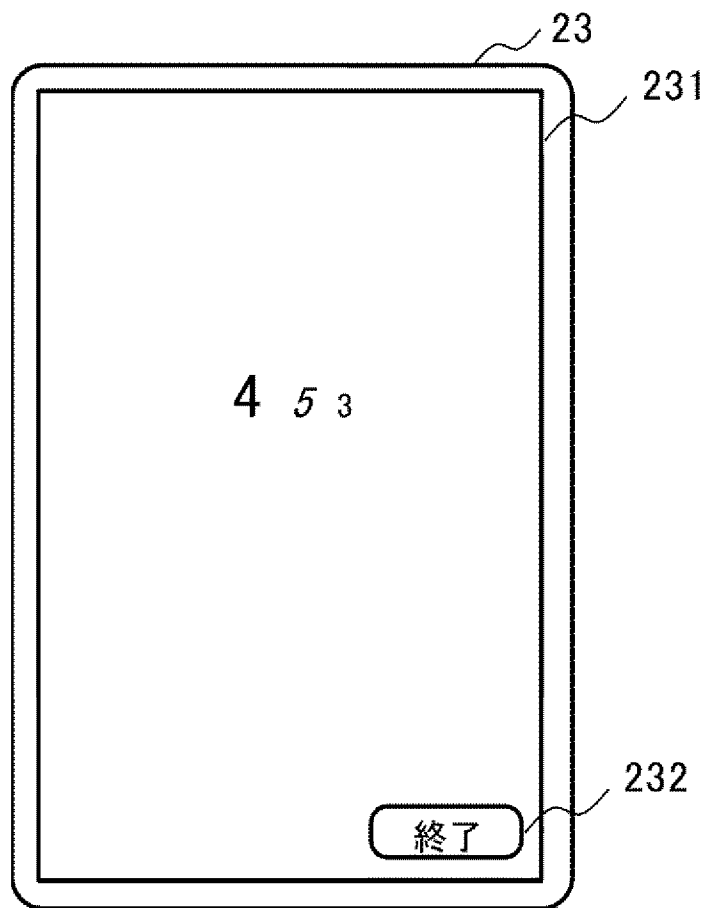
[図19]



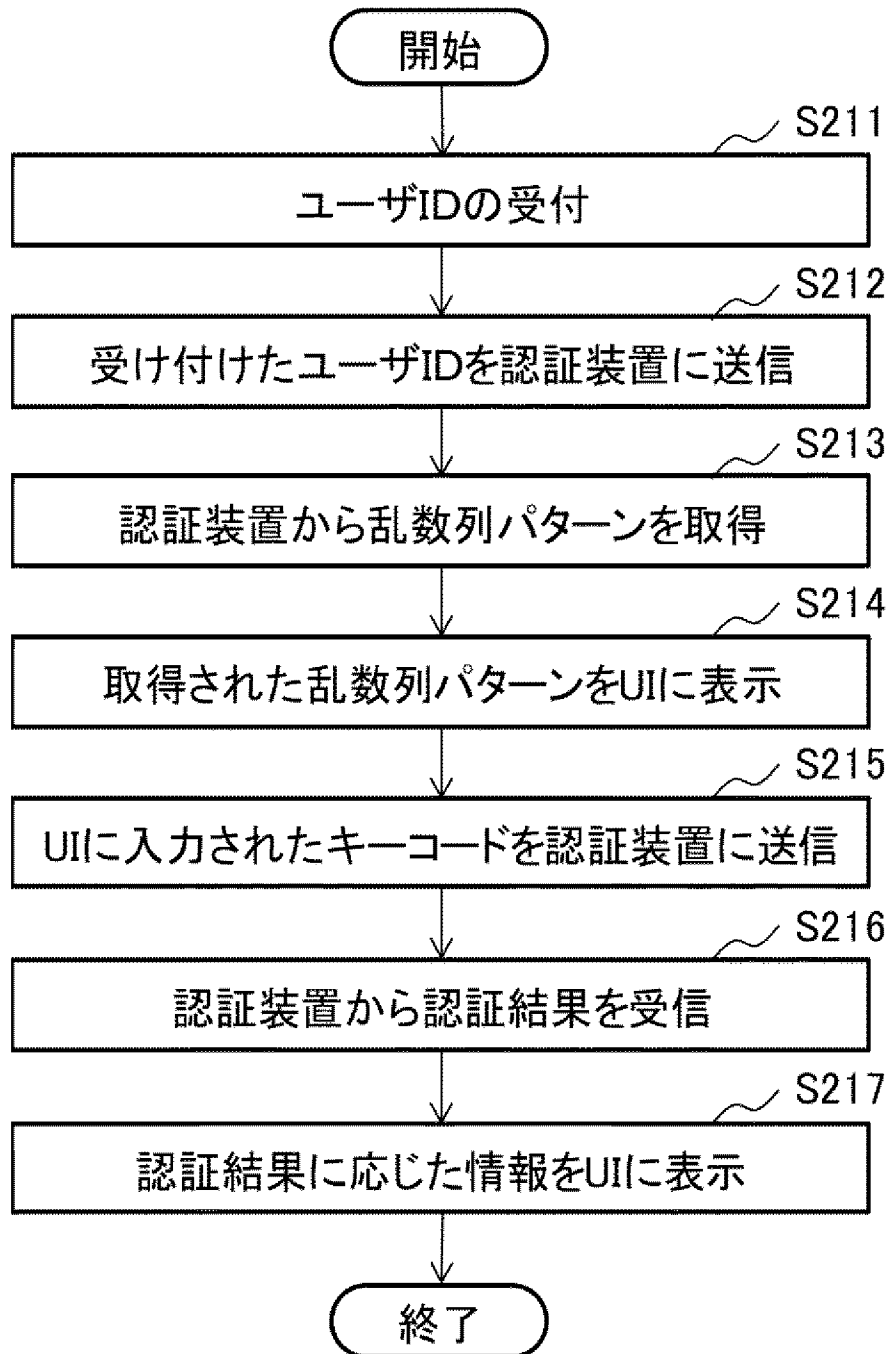
[図20]



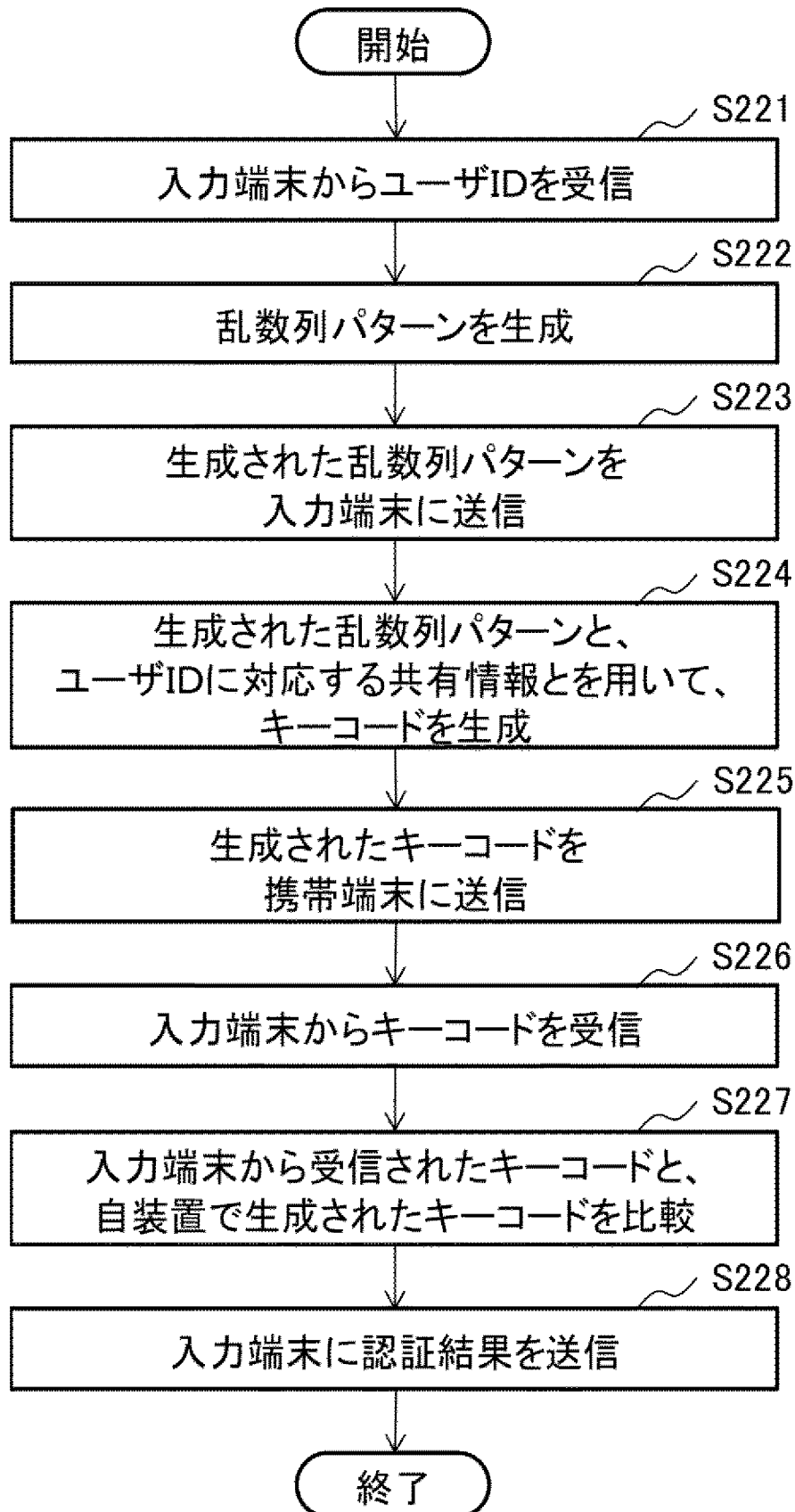
[図21]



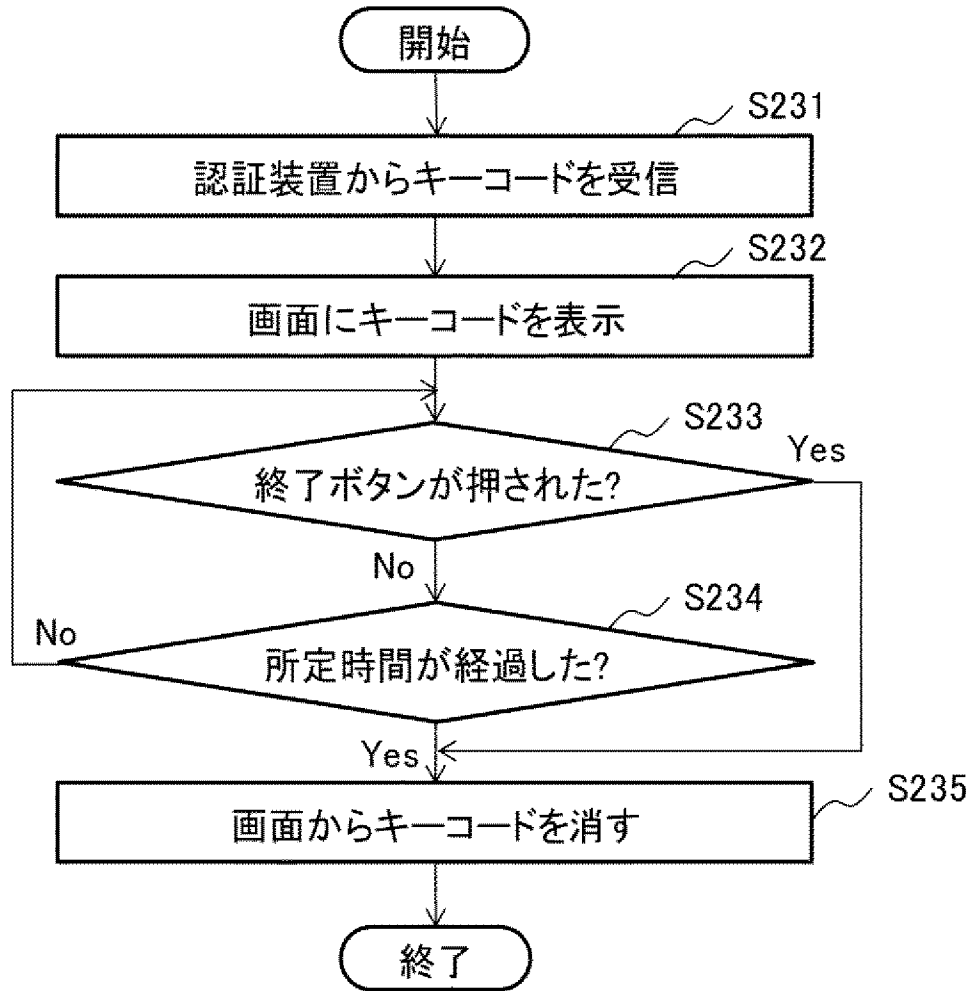
[図22]



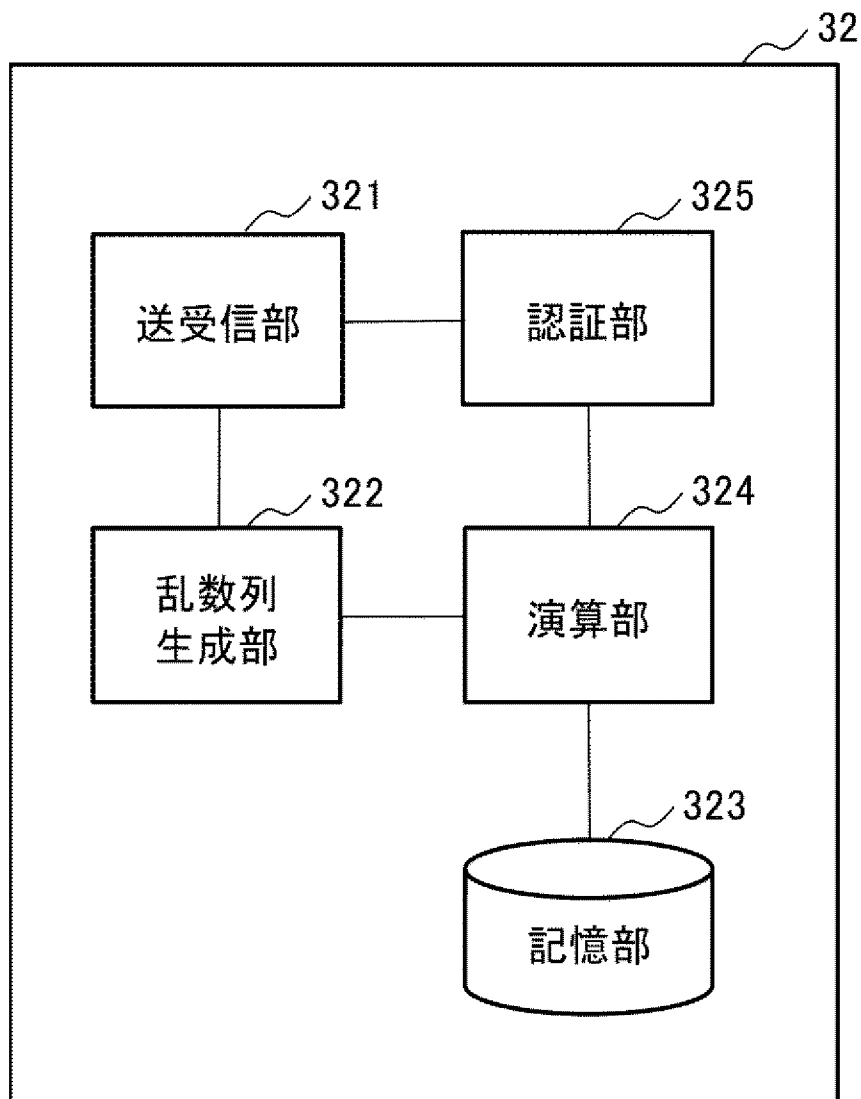
[図23]



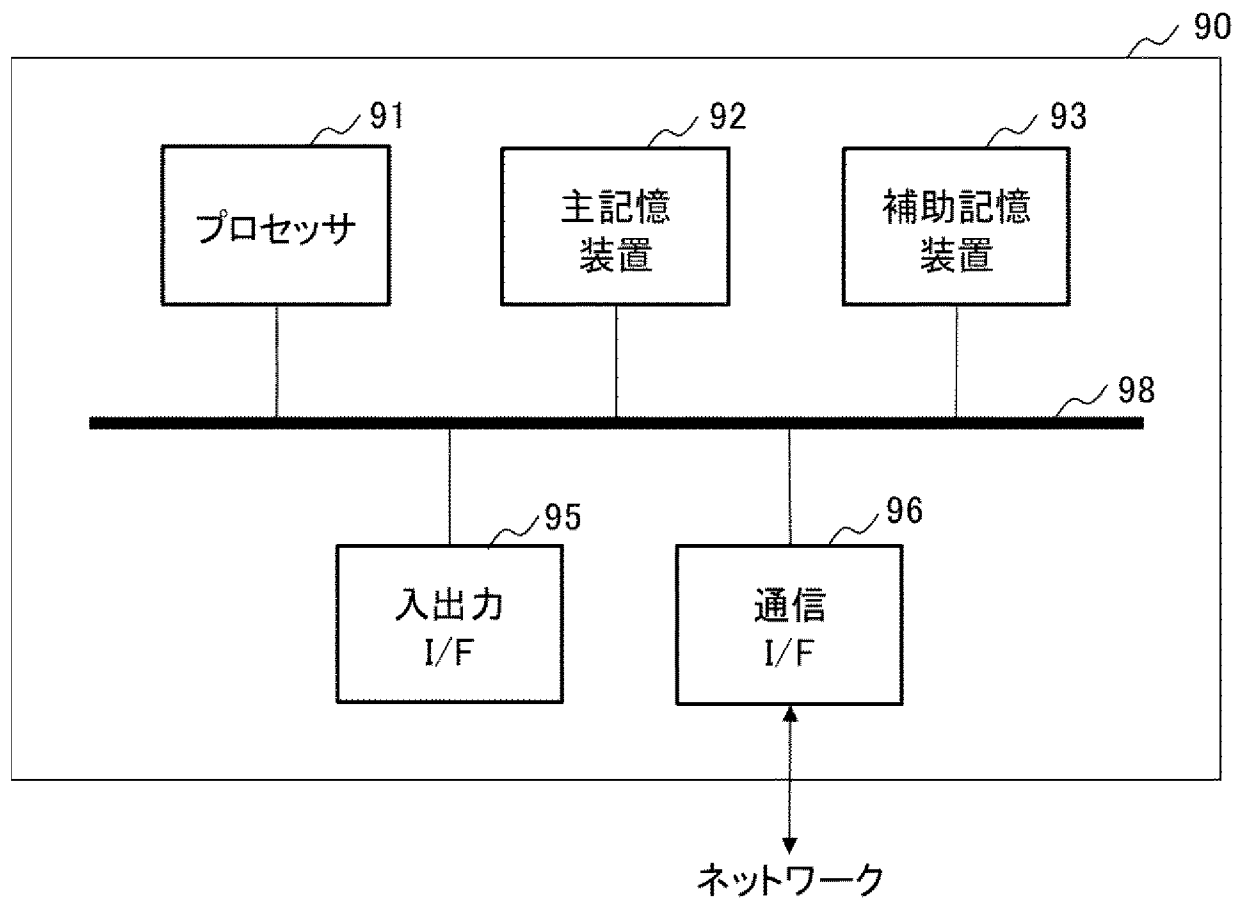
[図24]



[図25]



[図26]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/030279

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/31**(2013.01)i

FI: G06F21/31

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)

G06F21/31

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

Published examined utility model applications of Japan 1922-1996
 Published unexamined utility model applications of Japan 1971-2021
 Registered utility model specifications of Japan 1996-2021
 Published registered utility model applications of Japan 1994-2021

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	JP 2005-196800 A (OGAWA, Hideji) 21 July 2005 (2005-07-21)	1-4, 6-10
A	paragraphs [0048]-[0049], [0060]-[0064], fig. 9, 14	5
Y	JP 2007-264839 A (CSE KK) 11 October 2007 (2007-10-11)	1-4, 6-10
A	paragraphs [0004], [0009], fig. 7, 9	5
Y	JP 2008-276602 A (CHUGOKU ELECTRIC POWER CO INC) 13 November 2008 (2008-11-13)	4, 6-7
	paragraph [0031], fig. 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

11 October 2021

Date of mailing of the international search report

19 October 2021

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)
 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915
 Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2021/030279

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	2005-196800	A	21 July 2005	US 2005/0160297 A1 paragraphs [0079]-[0080], [0091]-[0095], fig. 9, 14 WO 2003/069490 A1 EP 1475721 A1 CA 2475822 A1 CN 1633650 A KR 10-2004-0093055 A	
JP	2007-264839	A	11 October 2007	US 2007/0226784 A1 paragraphs [0005], [0010], fig. 7, 9	
JP	2008-276602	A	13 November 2008	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/31(2013.01)i FI: G06F21/31														
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）） G06F21/31 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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2021年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2021年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2021年</td> </tr> </table> 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）			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2021年	日本国実用新案登録公報	1996 - 2021年	日本国登録実用新案公報	1994 - 2021年				
日本国実用新案公報	1922 - 1996年													
日本国公開実用新案公報	1971 - 2021年													
日本国実用新案登録公報	1996 - 2021年													
日本国登録実用新案公報	1994 - 2021年													
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 A	JP 2005-196800 A (小川 秀治) 21.07.2005 (2005 - 07 - 21) 段落[0048]-[0049], [0060]-[0064], 図9, 14	1-4, 6-10 5												
Y A	JP 2007-264839 A (株式会社シー・エス・イー) 11.10.2007 (2007 - 10 - 11) 段落[0004], [0009], 図7, 9	1-4, 6-10 5												
Y	JP 2008-276602 A (中国電力株式会社) 13.11.2008 (2008 - 11 - 13) 段落[0031], 図5	4, 6-7												
☐ 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。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの</td> </tr> <tr> <td>“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“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</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの	“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“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	“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	“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	“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）	“&” 同一パテントファミリー文献	“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	
* 引用文献のカテゴリー	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの													
“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“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													
“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	“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													
“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）	“&” 同一パテントファミリー文献													
“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														
国際調査を完了した日 11.10.2021	国際調査報告の発送日 19.10.2021													
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 平井 誠 5S 9071 電話番号 03-3581-1101 内線 3546													

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2021/030279

引用文献			公表日	パテントファミリー文献	公表日
JP	2005-196800	A	21.07.2005	US 2005/0160297 A1 pars. [0079]-[0080], [0091]-[0095], figs. 9, 14 WO 2003/069490 A1 EP 1475721 A1 CA 2475822 A1 CN 1633650 A KR 10-2004-0093055 A	
JP	2007-264839	A	11.10.2007	US 2007/0226784 A1 pars. [0005], [0010], figs. 7, 9	
JP	2008-276602	A	13.11.2008	(ファミリーなし)	