(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6050760号
(P6050760)
(45)発行日　平成28年12月21日(2016.12.21)　(24)登録日　平成28年12月2日(2016.12.2)

(51)Int.Cl.		F I		
G06F 21/36	(2013.01)	G06F	21/36	
H04L 9/32	(2006.01)	H04L	9/00	673C
H04L 9/28	(2006.01)	H04L	9/00	661

請求項の数 15　(全 26 頁)

(21)出願番号　特願2013-549154(P2013-549154)
(86)(22)出願日　平成24年10月18日(2012.10.18)
(86)国際出願番号　PCT/JP2012/076922
(87)国際公開番号　WO2013/088837
(87)国際公開日　平成25年6月20日(2013.6.20)
審査請求日　平成27年10月6日(2015.10.6)
(31)優先権主張番号　特願2011-276099(P2011-276099)
(32)優先日　平成23年12月16日(2011.12.16)
(33)優先権主張国　日本国(JP)

(73)特許権者　311012169
ＮＥＣパーソナルコンピュータ株式会社
東京都千代田区外神田四丁目１４番１号
秋葉原ＵＤＸ
(74)代理人　100084250
弁理士　丸山　隆夫
(72)発明者　白川　貴久
東京都品川区大崎一丁目１１番１号　ＮＥＣパーソナルコンピュータ株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】入力情報認証装置、サーバ装置、入力情報認証システムおよび装置のプログラム

(57)【特許請求の範囲】
【請求項１】
複数のキーを有する入力手段の操作されたキーに対応する情報と予め記憶された認証情報とが照合することの判断である認証を行う入力情報認証装置であって、
前記複数のキーは、第１の領域と第２の領域に割り当てられ、
前記第１の領域および前記第２の領域は、一方の領域が第１の状態であるときに他方の領域が前記第１の状態でない第２の状態となるよう遷移し、
前記認証情報に照合する入力を行うために操作すべきキーの配置されている領域が前記第１の状態であるときに操作された前記入力手段のキーに対応する情報を前記認証に使用し、前記認証情報に照合する入力を行うために操作すべきキーの配置されている領域が前記第２の状態であるときに操作された前記入力手段のキーに対応する情報を前記認証に使用しないことを特徴とする入力情報認証装置。
【請求項２】
前記複数のキーが前記第１の領域および前記第２の領域の何れに割り当てられるかは、初期状態としてランダムに選択され、
前記第１の領域および前記第２の領域は、前記入力手段から１文字入力される度に、前記第１の状態と前記第２の状態とを遷移することを特徴とする請求項１記載の入力情報認証装置。
【請求項３】
表示入力制御手段を備え、

前記表示入力制御手段は、
前記複数のキーを前記第１の領域および前記第２の領域の何れかに割り当て、
前記第１の領域および前記第２の領域を、前記第１の状態と前記第２の状態とに遷移させ、
前記認証情報に照合する入力を行うために操作すべきキーの配置されている領域が前記第２の状態であるときに操作された前記入力手段のキーに対応する情報を前記認証に使用しないことを特徴とする請求項１または２記載の入力情報認証装置。
【請求項４】
前記表示入力制御手段は、
前記入力手段により入力された１文字目が、予め記憶された認証情報の１文字目と一致する場合、該１文字目のキーが属す領域を前記第１の状態、他方の領域を前記第２の状態に割り当て、その後、該１文字目のキーが属す領域および該他方の領域を前記第１の状態と前記第２の状態とに遷移させ、
前記入力手段により入力された１文字目が、予め記憶された認証情報の１文字目と一致しない場合、該１文字目のキーが属す領域を前記第２の状態、他方の領域を前記第１の状態に割り当て、その後、該１文字目のキーが属す領域および該他方の領域を前記第１の状態と前記第２の状態とに遷移させることを特徴とする請求項３記載の入力情報認証装置。
【請求項５】
予め記憶される認証情報は数字列として表記可能な情報であり、
数字列として表記された認証情報を各桁毎に分解して一方向関数で暗号化する第１の暗号化手段と、
前記入力手段から入力された入力情報を数字列として表記して各桁毎に分解し、前記一方向関数で暗号化する第２の暗号化手段と、
前記第１の暗号化手段による暗号化文字列および前記第２の暗号化手段による暗号化文字列を照合する照合手段と、を備えたことを特徴とする請求項３記載の入力情報認証装置。
【請求項６】
前記第１の暗号化手段は、数字列として表記された認証情報を各桁毎の数字に分解し、ダミー入力を含めた入力文字数分の数字列に対して該分解された数字が存在する桁を認証情報に用いられない数字で桁取りし、該桁取りされた数字を一方向関数で暗号化し、
前記第２の暗号化手段は、前記入力手段から入力された入力情報を数字列として表記して各桁毎の数字に分解し、該分解された数字が該入力情報の数字列中で存在する桁を認証情報に用いられない数字で桁取りし、該桁取りされた数字を一方向関数で暗号化することを特徴とする請求項５記載の入力情報認証装置。
【請求項７】
予め記憶される認証情報は数字列として表記可能な情報であり、
数字列として表記された認証情報を一方向関数で暗号化する第１の暗号化手段と、
前記入力手段から入力された入力情報から前記認証に使用する情報を、該認証に使用する情報の入力操作としてあり得る各パターンについて抽出して前記一方向関数で暗号化する第２の暗号化手段と、
前記第１の暗号化手段による暗号化文字列および前記第２の暗号化手段による暗号化文字列を照合する照合手段と、を備えたことを特徴とする請求項３記載の入力情報認証装置。
【請求項８】
装置外部の表示入力制御手段からの制御を受信する通信手段を備え、
前記通信手段を介した前記表示入力制御手段からの制御により、
前記複数のキーを前記第１の領域および前記第２の領域の何れかに割り当て、
前記認証情報に照合する入力を行うために操作すべきキーの配置されている領域が前記第２の状態であるときに操作された前記入力手段のキーに対応する情報を前記認証に使

用しないことを特徴とする請求項１または２記載の入力情報認証装置。
【請求項９】
前記通信手段は、前記入力手段から入力された内容をサーバ装置に送信し、
前記サーバ装置は、
前記認証情報を予め記憶する記憶手段と、
前記入力手段から入力された内容に基づいて前記認証情報との照合を行う照合手段と、を備えることを特徴とする請求項８記載の入力情報認証装置。
【請求項１０】
前記複数のキーそれぞれについて、前記第１の領域に割り当てられているか、前記第２の領域に割り当てられているかをキー画像の表示により示す表示手段を備えたことを特徴とする請求項１から９の何れか１項に記載の入力情報認証装置。
【請求項１１】
前記入力手段は、前記表示手段の表面画面への接触位置を検出し、該接触位置の位置情報に基づいて前記複数のキーの何れへの入力かを判別することを特徴とする請求項１０記載の入力情報認証装置。
【請求項１２】
入力情報認証装置に、有線、無線、またはそれらの組み合わせにより接続されて用いられるサーバ装置であって、
前記入力情報認証装置への制御を行う表示入力制御手段を備え、
前記入力情報認証装置は、キー入力を行うための入力手段と、前記表示入力制御手段による制御を受信する通信手段と、を有し、
前記入力手段は複数のキーを有し、
前記表示入力制御手段は、前記複数のキーを、第１の領域と第２の領域の何れかに割り当て、
前記第１の領域および前記第２の領域は、一方の領域が第１の状態であるときに他方の領域が前記第１の状態でない第２の状態となるよう遷移し、
前記表示入力制御手段は、認証情報に照合する入力を行うために操作すべきキーの配置されている領域が前記第１の状態であるときに操作された前記入力手段のキーに対応する情報を認証に使用し、前記認証情報に照合する入力を行うために操作すべきキーの配置されている領域が前記第２の状態であるときに操作された前記入力手段のキーに対応する情報を認証に使用しないことを特徴とするサーバ装置。
【請求項１３】
前記表示入力制御手段は、前記複数のキーそれぞれに対する前記第１の領域および前記第２の領域の何れかへの割り当てと、該割り当てられた前記複数のキーの表示画像を、前記通信手段を介して前記入力情報認証装置に送信することを特徴とする請求項１２記載のサーバ装置。
【請求項１４】
入力情報認証装置とサーバ装置とが、有線、無線、またはそれらの組み合わせにより接続されて構成される入力情報認証システムであって、
前記サーバ装置は、前記入力情報認証装置への制御を行う表示入力制御手段を備え、
前記入力情報認証装置は、キー入力を行うための入力手段と、前記表示入力制御手段による制御を受信する通信手段と、を有し、
前記入力手段は複数のキーを有し、
前記表示入力制御手段は、前記複数のキーを、第１の領域と第２の領域の何れかに割り当て、
前記第１の領域および前記第２の領域は、一方の領域が第１の状態であるときに他方の領域が前記第１の状態でない第２の状態となるよう遷移し、
前記表示入力制御手段は、認証情報に照合する入力を行うために操作すべきキーの配置されている領域が前記第１の状態であるときに操作された前記入力手段のキーに対応する情報を認証に使用し、前記認証情報に照合する入力を行うために操作すべきキーの配置さ

れている領域が前記第２の状態であるときに操作された前記入力手段のキーに対応する情報を認証に使用しないことを特徴とする入力情報認証システム。
【請求項１５】
複数のキーを有する入力手段の操作されたキーに対応する情報と予め記憶された認証情報とが照合することの判断である認証を行う入力情報認証装置のプログラムであって、
コンピュータに、
前記複数のキーを、第１の領域と第２の領域の何れかに割り当てる手順と、
前記第１の領域および前記第２の領域に対して、一方の領域が第１の状態であるときに他方の領域が前記第１の状態でない第２の状態となるよう遷移させる手順と、
前記認証情報に照合する入力を行うために操作すべきキーの配置されている領域が前記第１の状態であるときに操作された前記入力手段のキーに対応する情報を前記認証に使用し、前記認証情報に照合する入力を行うために操作すべきキーの配置されている領域が前記第２の状態であるときに操作された前記入力手段のキーに対応する情報を前記認証に使用しないようにする手順と、を実行させることを特徴とする入力情報認証装置のプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、例えば暗証番号などの認証情報の入力を受け、その入力内容と予め登録された認証情報とを照合し、一致するか否かの判断である認証を行うための入力情報認証装置、サーバ装置、入力情報認証システムおよび装置のプログラムに関する。
【背景技術】
【０００２】
認証情報を入力時に盗み見られることを防止するための技術として、表示画面の視野角を狭くしたり、入力した数字を「＊」印などで表示して入力桁数だけを示すようにすることが行われている。
【０００３】
また、金融自動機（ＡＴＭ）などの端末から利用者がテンキーを使って暗証番号を入力する暗証番号入力装置として、入力テンキー画面と偽の入力テンキー画面とを表示し、暗証番号にダミー数字を嵌め込ませることで、入力している手の動きを見られた場合でも暗証番号を盗まれることのないようにしたものがある（例えば、特許文献１参照）。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特許第２９８５８８８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、特許文献１など、盗み見を防止するための上述した従来の技術は、例えば金融自動機（ＡＴＭ）など、第三者がある程度離れた距離の場所にいることを想定したものであり、至近距離から第三者に見られた場合への対策についてまで考慮されたものではなかった。すなわち、ユーザに対しダミー番号か暗証番号かのどちらを入力して欲しいかを指示する情報が偽の入力テンキーなどに提示されているものであった。このため、例えば入力しているユーザの肩越しや隠しカメラなどにより、入力しているユーザの手の動きだけでなく、入力画面そのものまで見られている場合には、どの入力がダミーであるかが識別されてしまい、暗証番号が知られてしまう虞があった。
【０００６】
本発明はこのような状況に鑑みてなされたものであり、認証情報の入力時に第三者から手元および入力画面を見られた場合であっても、認証情報を類推困難とすることができる入力情報認証装置、サーバ装置、入力情報認証システムおよび装置の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】
かかる目的を達成するために、本発明に係る入力情報認証装置は、
複数のキーを有する入力手段の操作されたキーに対応する情報と予め記憶された認証情報とが照合することの判断である認証を行う入力情報認証装置であって、
複数のキーは、第１の領域と第２の領域に割り当てられ、
第１の領域および第２の領域は、一方の領域が第１の状態であるときに他方の領域が第１の状態でない第２の状態となるよう遷移し、
認証情報に照合する入力を行うために操作すべきキーの配置されている領域が第１の状態であるときに操作された入力手段のキーに対応する情報を認証に使用し、認証情報に照合する入力を行うために操作すべきキーの配置されている領域が第２の状態であるときに操作された入力手段のキーに対応する情報を認証に使用しないことを特徴とする。
【０００８】
また、本発明に係るサーバ装置は、
入力情報認証装置に、有線、無線、またはそれらの組み合わせにより接続されて用いられるサーバ装置であって、
入力情報認証装置への制御を行う表示入力制御手段を備え、
入力情報認証装置は、キー入力を行うための入力手段と、表示入力制御手段による制御を受信する通信手段と、を有し、
入力手段は複数のキーを有し、
表示入力制御手段は、複数のキーを、第１の領域と第２の領域の何れかに割り当て、
第１の領域および第２の領域は、一方の領域が第１の状態であるときに他方の領域が第１の状態でない第２の状態となるよう遷移し、
表示入力制御手段は、認証情報に照合する入力を行うために操作すべきキーの配置されている領域が第１の状態であるときに操作された入力手段のキーに対応する情報を認証に使用し、認証情報に照合する入力を行うために操作すべきキーの配置されている領域が第２の状態であるときに操作された入力手段のキーに対応する情報を認証に使用しないことを特徴とする。
【０００９】
また、本発明に係る入力情報認証システムは、
入力情報認証装置とサーバ装置とが、有線、無線、またはそれらの組み合わせにより接続されて構成される入力情報認証システムであって、
サーバ装置は、入力情報認証装置への制御を行う表示入力制御手段を備え、
入力情報認証装置は、キー入力を行うための入力手段と、表示入力制御手段による制御を受信する通信手段と、を有し、
入力手段は複数のキーを有し、
表示入力制御手段は、複数のキーを、第１の領域と第２の領域の何れかに割り当て、
第１の領域および第２の領域は、一方の領域が第１の状態であるときに他方の領域が第１の状態でない第２の状態となるよう遷移し、
表示入力制御手段は、認証情報に照合する入力を行うために操作すべきキーの配置されている領域が第１の状態であるときに操作された入力手段のキーに対応する情報を認証に使用し、認証情報に照合する入力を行うために操作すべきキーの配置されている領域が第２の状態であるときに操作された入力手段のキーに対応する情報を認証に使用しないことを特徴とする。
【００１０】
また、本発明に係る入力情報認証装置のプログラムは、
複数のキーを有する入力手段の操作されたキーに対応する情報と予め記憶された認証情報とが照合することの判断である認証を行う入力情報認証装置のプログラムであって、
コンピュータに、

複数のキーを、第１の領域と第２の領域の何れかに割り当てる手順と、
第１の領域および第２の領域に対して、一方の領域が第１の状態であるときに他方の領域が第１の状態でない第２の状態となるよう遷移させる手順と、
認証情報に照合する入力を行うために操作すべきキーの配置されている領域が第１の状態であるときに操作された入力手段のキーに対応する情報を認証に使用し、認証情報に照合する入力を行うために操作すべきキーの配置されている領域が第２の状態であるときに操作された入力手段のキーに対応する情報を認証に使用しないようにする手順と、を実行させることを特徴とする。
【発明の効果】
【００１１】
以上のように、本発明によれば、認証情報の入力時に第三者から手元および入力画面を見られた場合であっても、認証情報を類推困難とすることができる。
【図面の簡単な説明】
【００１２】
【図１】本発明の第１の実施形態としての入力情報認証装置１００の構成例を示すブロック図である。
【図２】タッチキーボード例と、パスコード認証ＯＫである場合の入力コード列例を示す図である。
【図３】初期パターンの変化例とリプレーアタックへのセキュリティを説明する図である。
【図４】第１の実施形態としての入力情報認証装置１００の動作例を示すフローチャートである。
【図５】第２の実施形態としての入力情報認証システムの構成例を示すブロック図である。
【図６】第２の実施形態としての入力情報認証システムの動作例を示すフローチャートである。
【図７】第３の実施形態としての入力情報認証装置１００の構成例を示すブロック図である。
【図８】第３の実施形態におけるパスコード登録時の動作例を示すフローチャートである。
【図９】抽出パターンを桁毎に分解してハッシュ化する一例を示す図である。
【図１０】パスコードをハッシュ化のために桁毎に分解した例を示す図である。
【図１１】第３の実施形態としての入力情報認証装置１００の動作例を示すフローチャートである。
【図１２】第４の実施形態としての入力情報認証装置１００の動作例を示すフローチャートである。
【発明を実施するための形態】
【００１３】
次に、本発明に係る入力情報認証装置、サーバ装置、入力情報認証システムおよび装置のプログラムを適用した一実施形態について、図面を用いて詳細に説明する。
【００１４】
まず、本発明の各実施形態に共通する概略について説明する。
本発明の実施形態は、入力キーが表示色によって２つの領域に分けられ、認証ＯＫとなるパスコードを入力していく上で次に操作すべきキーがどちらの領域に割り当てられているかによって、キー入力を認証に使用する入力パスコードとするか、認証に使用しないダミーコードとするか、分けるようにしている。
このように、本発明の実施形態では、入力されたキーが属していた領域でダミー入力とするか、認証情報の入力とするかを判別しているわけではないので、どの入力がダミーであるかを、認証情報を知らない第三者には識別できないようにできる。このため、仮に第三者から入力時の手元および表示画面を見られた場合であっても、認証情報を類推困難と

することができる。
【００１５】
〔第１の実施形態〕
次に、本発明の第１の実施形態について説明する。
以下に述べる各実施形態では、認証情報として数字によるパスコードを用いる場合の例について説明する。
【００１６】
第１の実施形態としての入力情報認証装置１００は、図１に示すように、タッチパネルディスプレイなどの表示入力部１１０と、表示入力制御部１２０と、入力されたパスコードを照合する照合部１３０と、登録されたパスコード等を記憶する記憶部１４０と、を備えて構成される。
【００１７】
表示入力部１１０は、複数のキーを画面表示し、その表面画面への接触位置を検出し、その接触位置の位置情報に基づいて、表示された複数のキーの何れへの入力かを判別する。
表示入力制御部１２０は、表示入力部１１０に表示する入力キーの表示制御や、入力情報からの入力パスコードの抽出などの制御を行う。
表示入力制御部１２０は、入力キーの表示における初期パターンを生成する初期パターン生成部１２１と、入力キーの表示パターンを反転させるパターン反転部１２２と、ユーザによる入力パスコードが含まれる可能性があるキー色としての入力色を判定する入力色判定部１２３と、入力されたパスコードを抽出する入力パスコード抽出部１２４と、を備えて構成される。
【００１８】
本実施形態の入力情報認証装置１００は、こうした構成を備えることで、数字入力用の複数のキーからなるタッチキーボードを表示入力部１１０に表示し、ユーザによるパスコードの入力を受ける。
【００１９】
図２に、表示入力部１１０による画面表示例と、パスコード認証ＯＫである場合の入力コード列の例を示す。
本発明の各実施形態では、表示入力部１１０に表示される入力キーとして、数字入力用の１～９の数字が割り当てられている場合の例について説明する。また、図２の例では、パスコードが「１２３」である場合について示す。
【００２０】
入力キーは、図２に示すように、着色キーと白色キーに分けられ、何れか一方がユーザによる入力パスコードが含まれる可能性があるキー色として認識対象とするキー色となり、他方は入力パスコードとして認識対象外を示すキー色となる。すなわち、入力色判定部１２３により入力色と判定されたキー色のキーが、入力パスコードが含まれる可能性があるキーとして認識対象とされ、入力色でないと判定されたキー色のキーは、入力パスコードが含まれる可能性のないキーとして認識対象外とされる。
【００２１】
また、この着色キーと白色キーの表示によるキーの領域分けでは、まず初期パターンが表示され、１文字入力する毎にパターンが反転する。すなわち、１文字入力する毎に、着色キーの部分は白色キーとなり、白色キーの部分は着色キーとなり、この動作を繰り返す。
【００２２】
ユーザに提示する入力ルールとしては、認証ＯＫとなるパスコードを入力していく上で次に操作すべきキーが認識対象のキー色である場合には、そのキーを入力しないとパスコードとして認証されないこととする。
【００２３】
このため、パスコードを入力していくための最初の１文字目は、１回目または２回目の

どちらかで必ず入力される必要がある。この最初の１文字目が入力された時点でのキー色を、入力色判定部１２３は、認識対象を示す入力色として判定する。
　また、認証ＯＫとなるパスコードを入力していく上で次に操作すべきキーが入力色でない色であれば、入力キーがどのキーであってもダミーコードとして扱うこととなる。
【００２４】
　ユーザに提示する入力ルールとしては、同じ色のキーのみを入力するようにしておくことが好ましい。このようにすることで、どのキー入力がダミーなのかを分かりにくくすることができる。
【００２５】
　また、パスコードの入力時には、ダミーコードをパスコードの桁数と同桁数だけ混ぜて入力することとする。図２の例では、パスコードが３桁の数字であり、ダミーコードを３桁含ませた合計６桁の数字を入力する場合について示す。
　ユーザに提示する入力ルールとしては、パスコードを入力し終えても、ダミーコードを含んだ所定桁数（図２の例では６桁）までは、何らかの入力をしないとパスコードの照合に移行しないようにしておく。このため、パスコードを入力し終えた後、ダミーコードを含んだ所定桁数（図２の例では６桁）までの入力は、全てダミー入力として扱うこととなる。
【００２６】
　次に、図２（ａ）、（ｂ）の具体例を用いて、本実施形態でパスコードの認証ＯＫとなる場合の動作例について説明する。
【００２７】
　図２（ａ）では、初期パターンとして、「１，２，６，７，９」が着色キーとして表示され、パスコード「１，２，３」の最初の１文字である「１」が、１文字目の入力で入力された場合の例を示す。このため、入力色判定部１２３は、着色キーが認識対象を示す入力色のキーであることと判定し、入力パスコード抽出部１２４は、この１文字目の入力を、ユーザによる入力パスコードの１桁目として認識する。
【００２８】
　２文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について次に操作すべきキーである「２」が白色キー、すなわち認識対象外となっている。このため、この２文字目の入力は、どのキーへの入力であってもダミー入力となる。図２の例では、ダミー入力を「＊」で示す。
【００２９】
　３文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について次に操作すべきキーである「２」が着色キー、すなわち認識対象となっている。このため、入力パスコード抽出部１２４は、この３文字目の入力を、ユーザによる入力パスコードの２桁目として認識する。認証ＯＫとするためには、ユーザはこの３文字目の入力で「２」を入力することとなる。
【００３０】
　４文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について次に操作すべきキーである「３」が着色キー、すなわち認識対象となっている。このため、入力パスコード抽出部１２４は、この４文字目の入力を、ユーザによる入力パスコードの３桁目として認識する。認証ＯＫとするためには、ユーザはこの４文字目の入力で「３」を入力することとなる。
【００３１】
　５文字目および６文字目の入力時には、すでにユーザによる入力パスコードの３桁全てを入力し終えているため、どのキーへの入力であってもダミー入力となる。こうしてパスコード入力が終了する。
【００３２】
　図２（ｂ）では、初期パターンとして、「１，２，６，７，９」が着色キーとして表示されている状態で、パスコード「１，２，３」の最初の１文字である「１」が、１文字目

の入力で入力されない場合の例を示す。すなわち、１文字目の入力である「＊」は、パスコード「１，２，３」の最初の１文字である「１」以外がダミーとして入力されたことを示す。

このため、入力色判定部１２３は、白色キーが認識対象を示す入力色のキーであることと判定する。

【００３３】

２文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について最初の１文字目として操作すべきキーである「１」が白色キー、すなわち認識対象となっている。このため、入力パスコード抽出部１２４は、この２文字目の入力を、ユーザによる入力パスコードの１桁目として認識する。認証ＯＫとするためには、ユーザはこの２文字目の入力で「１」を入力することとなる。

【００３４】

３文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について次に操作すべきキーである「２」が着色キー、すなわち認識対象外となっている。このため、この３文字目の入力は、どのキーへの入力であってもダミー入力となる。図２の例では、ダミー入力を「＊」で示す。

【００３５】

４文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について次に操作すべきキーである「２」が白色キー、すなわち認識対象となっている。このため、入力パスコード抽出部１２４は、この４文字目の入力を、ユーザによる入力パスコードの２桁目として認識する。認証ＯＫとするためには、ユーザはこの４文字目の入力で「２」を入力することとなる。

【００３６】

５文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について次に操作すべきキーである「３」が白色キー、すなわち認識対象となっている。このため、入力パスコード抽出部１２４は、この５文字目の入力を、ユーザによる入力パスコードの３桁目として認識する。認証ＯＫとするためには、ユーザはこの５文字目の入力で「３」を入力することとなる。

【００３７】

６文字目の入力時には、すでにユーザによる入力パスコードの３桁全てを入力し終えているため、どのキーへの入力であってもダミー入力となる。こうしてパスコード入力が終了する。

【００３８】

次に、本実施形態の入力情報認証装置１００によるリプレーアタックへのセキュリティについて、図３の具体例を参照して説明する。

【００３９】

図３（ａ）は、図２（ａ）の場合と同様に、初期パターンとして、「１，２，６，７，９」が着色キーとして表示され、パスコード「１，２，３」の最初の１文字である「１」が、１文字目の入力で入力された場合の例を示す。このため、図３（ａ）の例では、２文字目、５文字目、６文字目がダミー入力となっており、このダミー入力を含めて、「１，５，２，３，６，４」の６桁が入力された場合を示す。

【００４０】

ここで、図３（ａ）のようにユーザがパスコード入力をしている時に、そのユーザの肩越しなどの至近距離から、キー入力している手の動作および入力画面を第三者に見られてしまっていたとする。さらにその後、本実施形態の入力情報認証装置１００をその第三者に入手されてしまったとする。

【００４１】

こうして、その第三者が本実施形態の入力情報認証装置１００に、先ほど盗み見たのと同じ「１，５，２，３，６，４」の６桁を入力した場合の例を、図３（ｂ）に示す。

【００４２】

初期パターンはランダムに決定されるため、図３（ｂ）の入力時には、先ほどの図３（ａ）の入力時とは異なる初期パターンで表示されている。図３（ｂ）では、この初期パターンの例として、「２，３，５，７」が着色キーとして表示されている場合の例を示す。

【００４３】

この初期パターンが表示された状態で、入力情報認証装置１００を入手した第三者が、先ほど盗み見たのと同じ「１，５，２，３，６，４」の６桁を入力すると、まず１文字目としてパスコード「１，２，３」の最初の１文字である「１」が入力されているため、入力色判定部１２３は、白色キーが認識対象を示す入力色のキーであることと判定する。また、入力パスコード抽出部１２４は、この１文字目の入力キーである「１」を、ユーザによる入力パスコードの１桁目として認識する。

【００４４】

２文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について次に操作すべきキーである「２」が白色キー、すなわち認識対象となっている。このため、入力パスコード抽出部１２４は、この２文字目の入力キーである「５」を、ユーザによる入力パスコードの２桁目として認識する。

【００４５】

３文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について次に操作すべきキーである「３」が着色キー、すなわち認識対象外となっている。このため、この３文字目の入力である「２」はダミー入力として扱われる。

【００４６】

４文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について次に操作すべきキーである「３」が白色キー、すなわち認識対象となっている。このため、入力パスコード抽出部１２４は、この４文字目の入力キーである「３」を、ユーザによる入力パスコードの３桁目として認識する。

【００４７】

５文字目および６文字目の入力時には、すでにユーザによる入力パスコードの３桁目まで入力し終えているため、５文字目の入力である「６」、および６文字目の入力である「４」はダミー入力として扱われる。

【００４８】

こうして、入力パスコード抽出部１２４は、入力されたパスコードが「１，５，３」であると認識するため、正しいパスコード「１，２，３」とは一致せず、認証結果はＮＧとなる。

【００４９】

このため、パスコード入力を盗み見た第三者が入力情報認証装置１００を入手して、先ほど盗み見たのと同じ６桁を入力したとしても、その盗み見た入力内容では認証ＯＫとすることができない。こうして、キー入力している手の動作および入力画面を見られた場合であっても、正しいパスコードを知られてしまうことのない、高いセキュリティを実現することができる。

【００５０】

また、パスコード認証が一度ＮＧになると、次回のパスコード入力時には、入力のためのウエイト時間が倍になる構成としてもよい。こうして、パスコード認証がＮＧになる度にウエイト時間が倍になっていくことで、リプレーアタックの繰り返しに対するセキュリティを向上させることができる。また、パスコード認証がＮＧになる度にウエイト時間を指数的に長くしていく構成としてもよい。

【００５１】

図３（ｂ）のようにして認証ＮＧとなった後、パスコードの認証ＯＫとさせる場合の入力例について、図３（ｃ）を参照して説明する。

【００５２】

パスコード認証でＮＧとなると、次回のパスコード入力時にも同じ初期パターンが表示される。このため、第三者がパスコードを盗み見た時（図３（ａ）の初期パターン）と同

じ初期パターンが表示されてしまう確率をゼロにすることができる。すなわち、ランダムに決定される初期パターンが偶然に図３（ａ）の初期パターンと同じになってしまう可能性をゼロにすることができる。

【００５３】

ここで、１文字目の入力が「１」であるとすると、パスコード「１，２，３」の最初の１文字である「１」が、１文字目の入力で入力されているため、入力色判定部１２３は、白色キーが認識対象を示す入力色のキーであることと判定する。また、入力パスコード抽出部１２４は、この１文字目の入力を、ユーザによる入力パスコードの１桁目として認識する。

【００５４】

２文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について次に操作すべきキーである「２」が白色キー、すなわち認識対象となっている。このため、入力パスコード抽出部１２４は、この２文字目の入力を、ユーザによる入力パスコードの２桁目として認識する。認証ＯＫとするためには、ユーザはこの２文字目の入力で「２」を入力することとなる。

【００５５】

３文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について次に操作すべきキーである「３」が着色キー、すなわち認識対象外となっている。このため、この３文字目の入力は、どのキーへの入力であってもダミー入力となる。図３の例では、ダミー入力を「＊」で示す。

【００５６】

４文字目の入力時には、着色キーと白色キーの表示が反転し、パスコード「１，２，３」について次に操作すべきキーである「３」が白色キー、すなわち認識対象となっている。このため、入力パスコード抽出部１２４は、この４文字目の入力を、ユーザによる入力パスコードの３桁目として認識する。認証ＯＫとするためには、ユーザはこの４文字目の入力で「３」を入力することとなる。

【００５７】

５文字目および６文字目の入力時には、すでにユーザによる入力パスコードの３桁全てを入力し終えているため、どのキーへの入力であってもダミー入力となる。こうしてパスコード入力が終了する。

【００５８】

次に、第１の実施形態としての入力情報認証装置１００の動作例について、図４のフローチャートを参照して説明する。

【００５９】

まず、初期パターン生成部１２１が、表示入力部１１０としてのタッチパネルディスプレイに表示するタッチキーボードの初期パターンを生成する（ステップＳ１）。

タッチキーボードを構成する各キーの色は、予め定められた２色の何れかとされ、こうしたキー色の初期パターンはランダムに設定される。ランダムに設定する方法は、乱数を用いる既知の方法など、各種の方法を用いてよい。

【００６０】

初期パターンによりタッチキーボードが表示入力部１１０に表示され、そのタッチキーボードに１文字目が入力されると（ステップＳ２）、その１文字目の入力内容に基づいて、入力色判定部１２３は、認識対象とする入力色を判定する（ステップＳ３）。

ステップＳ３の判定では、１文字目の入力キーが、認証ＯＫとなるパスコード入力として操作すべきキーである登録パスコードの１桁目である場合、入力色判定部１２３は、その１文字目の入力キーのキー色を入力色と判定する。１文字目の入力キーが、その登録パスコードの１桁目でない場合、入力色判定部１２３は、その１文字目の入力キーのキー色とは異なるキー色の方を入力色と判定する。

【００６１】

こうして１文字目が入力されると、次のキー入力のため、パターン反転部１２２は、初

期パターンを反転させた表示パターンを生成し、その反転パターンによりタッチキーボードが表示入力部１１０に表示される（ステップＳ４）。

【００６２】

反転パターンにより表示されたタッチキーボードに次のキー入力がなされると（ステップＳ５）、入力文字数が規定数となるまで、ステップＳ４，Ｓ５の動作を繰り返す（ステップＳ６）。すなわち、パターン反転部１２２が先のキー入力の際の表示パターンを反転させた表示パターンを生成し、次のキー入力を受ける動作を繰り返す。

【００６３】

こうして規定数、すなわちパスコードの桁数に同じ桁数のダミーコードを加えた倍の桁数が入力されると、入力パスコード抽出部１２４は、ステップＳ１で生成された初期パターン、ステップＳ３で判定された入力色、およびパスコードに基づいて、ダミーコードとユーザによる入力パスコードとを区別し、６桁のキー入力内容からユーザによる入力パスコードのみを抽出するための抽出パターンを生成する（ステップＳ７）。

【００６４】

この抽出パターンは、上述した図２（ａ）の例では、６桁のキー入力に対して、ユーザによる入力パスコードの「１桁目，ダミー，２桁目，３桁目，ダミー，ダミー」である。

また、上述した図２（ｂ）の例では、６桁のキー入力に対して、ユーザによる入力パスコードの「ダミー，１桁目，ダミー，２桁目，３桁目，ダミー」である。

また、上述した図３（ｂ）の例では、６桁のキー入力に対して、ユーザによる入力パスコードの「１桁目，２桁目，ダミー，３桁目，ダミー，ダミー」である。

【００６５】

入力パスコード抽出部１２４は、こうして抽出パターンを生成すると、その抽出パターンに沿って、６桁のキー入力内容から、ユーザによる入力パスコードの「１桁目，２桁目，３桁目」を抽出する（ステップＳ８）。

【００６６】

照合部１３０は、入力パスコード抽出部１２４により抽出された３桁の入力パスコード（照合用パスコード）と、記憶部１４０に登録されているパスコードとを照合する。この照合により、両者が一致する場合に認証ＯＫ、一致しない場合に認証ＮＧとする（ステップＳ９）。

【００６７】

以上のように、上述した本発明の実施形態では、初期パターンがランダムに生成され、初期パターンが変わると、図３により上述のように、同じキー入力列を入力しても認証結果がＮＧとなってしまう。このように、実質的にワンタイムパスワードのように機能し、同じパスコードであっても、認証ＯＫとするためのキー入力内容が入力の度に変化することとなるため、入力している手の動きおよび表示画面を第三者から盗み見られた場合への対策としても、十分に高度なセキュリティを確保することができる。

【００６８】

また、正しくパスコード認証ができるキー入力列として、図２（ａ）および（ｂ）のようにパスコードの１文字目を入力するタイミングの２パターンに加えて、それぞれのダミー入力に所定のキー色である任意のキーを選択できるようになっている。このため、特定の入力桁がユーザによる入力パスコードの何れかの桁に該当するといった特徴もない。このため、第三者から入力時に手元および入力画面を見られた場合であっても、その第三者がパスコードを類推することは極めて困難となる。

さらに、リトライを繰り返すといったリプレーアタックに対しても十分な暗号強度を持つことも可能となっている。

【００６９】

さらに、パスコードにダミーコードを同じ桁数だけ含ませ、倍の桁数として入力させることとなるため、セキュリティを強固なものとすることができる。

【００７０】

それでいて、ユーザは、パスコードを所定のキー色の時に入力し、他のキー色である場

合にはそのキー色の適当なキーを入力していくだけの簡単な手間で操作することができる。このように、ユーザの利便性を損ねることなく、上述のような高度なセキュリティを実現することができる。

【００７１】

また、パスコードの認証ＯＫの際には、次回のパスコード入力時に初期パターンをランダムに再設定し、認証ＮＧの際には、次回のパスコード入力時にも初期パターンをそのままとしている。このため、初期パターンが偶然に一致する確率をゼロにすることができ、さらに高度なセキュリティを実現することができる。

【００７２】

特に、本実施形態の入力情報認証装置１００がタッチパネル式の携帯情報端末である場合、電車の中や人ごみの中などで認証情報を入力することも考えられ、こうした場合に入力している手元および表示画面を肩越しなどで至近距離から第三者に見られてしまう可能性がある。このように、認証情報を入力している手元および表示画面を見られた場合であっても、その見られた情報からではパスコードを類推することが困難な、セキュリティに優れた入力情報認証装置とすることができる。

【００７３】

また、特に初心者や高齢者などの場合、パスコード入力の際にもキー入力の速度が非常にゆっくりであることが考えられる。従って、第三者に見られている場合、手の動きや表示画面を容易に記憶されてしまう可能性がある。

上述した実施形態によれば、こうした場合であっても、上述のように十分に高度なセキュリティを確保することができる。

【００７４】

〔第２の実施形態〕

次に、本発明の第２の実施形態について説明する。

第２の実施形態は、上述した第１の実施形態における初期パターンの生成やパスコードの記憶、照合といった機能を、サーバ装置を用いて実現するようにしたものである。

上述した第１の実施形態と同様のものについては、説明を省略する。

【００７５】

第２の実施形態としての入力情報認証システムは、図５に示すように、入力情報認証装置１００と、サーバ装置２００とがネットワークを介して接続されて構成される。

【００７６】

入力情報認証装置１００は、表示入力部１１０と、表示入力制御部３１０と、通信部１５０とを備える。

【００７７】

通信部１５０は、有線、無線、またはそれらの組み合わせにより、ネットワークを介してサーバ装置２００の通信部２５０と接続され、サーバ装置２００との間での通信を行う。

【００７８】

表示入力制御部３１０は、通信部１５０によるサーバ装置２００との送受信内容に基づいて、表示入力部１１０に表示する入力キーの表示制御等を行う。また、表示入力制御部３１０は、上述した第１の実施形態と同様のパターン反転部１２２を備える。

【００７９】

サーバ装置２００は、表示入力制御部３２０と、照合部２３０と、記憶部２４０と、通信部２５０とを備える。

【００８０】

通信部２５０は、有線、無線、またはそれらの組み合わせにより、ネットワークを介して入力情報認証装置１００の通信部１５０と接続され、入力情報認証装置１００との間での通信を行う。

【００８１】

表示入力制御部３２０は、通信部２５０で入力情報認証装置１００と通信を行うことに

より、入力情報認証装置１００の表示入力部１１０に表示する入力キーの表示制御等を行う。また、表示入力制御部３２０は、上述した第１の実施形態と同様の初期パターン生成部２２１、入力色判定部２２３、入力パスコード抽出部２２４を備える。

【００８２】

次に、第２の実施形態としての入力情報認証システムの動作例について、図６のフローチャートを参照して説明する。以下に説明する本実施形態の動作では、入力情報認証装置１００で用いるパスコードが、予めサーバ装置２００の記憶部２４０に登録されていることとする。

【００８３】

まず、サーバ装置２００の初期パターン生成部２２１が、入力情報認証装置１００における表示入力部１１０としてのタッチパネルディスプレイに表示するタッチキーボードの初期パターンを生成する（ステップＳ１１）。初期パターンの生成は、上述した第１の実施形態と同様であってよい。

【００８４】

初期パターン生成部２２１が初期パターンを生成すると、生成された初期パターンおよび入力文字数を通信部２５０が入力情報認証装置１００に送信する（ステップＳ１２）。入力文字数は、パスコードの桁数に同じ桁数のダミーコードを加えた倍の桁数であり、上述した第１の実施形態における図２、図３の例では６文字である。

【００８５】

入力情報認証装置１００の表示入力制御部３１０は、通信部１５０によりサーバ装置２００から受信した初期パターンおよび入力文字数に基づいて、まず、初期パターンによりタッチキーボードを表示入力部１１０に表示する（ステップＳ１３）。

【００８６】

タッチキーボードに１文字目が入力されると（ステップＳ１４）、次のキー入力のため、パターン反転部１２２は、初期パターンを反転させた表示パターンを生成し、その反転パターンによりタッチキーボードが表示入力部１１０に表示される（ステップＳ１５）。

【００８７】

反転パターンにより表示されたタッチキーボードに次のキー入力がなされると（ステップＳ１６）、入力文字数が規定数となるまで、ステップＳ１５，Ｓ１６の動作を繰り返す（ステップＳ１７）。すなわち、パターン反転部１２２が先のキー入力の際の表示パターンを反転させた表示パターンを生成し、次のキー入力を受ける動作を繰り返す。

【００８８】

こうして規定数、すなわちサーバ装置２００から受信した入力文字数が入力されると、表示入力制御部３１０は、その入力文字数の入力コード列を、通信部１５０によりサーバ装置２００に送信する（ステップＳ１８）。

【００８９】

サーバ装置２００の入力色判定部２２３は、通信部２５０により入力情報認証装置１００から入力コード列が受信されると、その１文字目の入力内容に基づいて、認識対象とする入力色を判定する（ステップＳ１９）。判別方法は、上述した第１の実施形態と同様であってよい。

【００９０】

入力パスコード抽出部２２４は、ステップＳ１１で生成された初期パターン、ステップＳ１９で判定された入力色、およびパスコードに基づいて、ダミーコードとユーザによる入力パスコードとを区別し、６桁のキー入力内容からユーザによる入力パスコードのみを抽出するための抽出パターンを生成する（ステップＳ２０）。抽出パターンの生成は、上述した第１の実施形態と同様に行うこととしてよい。

【００９１】

入力パスコード抽出部２２４は、こうして抽出パターンを生成すると、その抽出パターンに沿って、入力情報認証装置１００から受信した６桁の入力コード列から、ユーザによる入力パスコードの「１桁目，２桁目，３桁目」を抽出する（ステップＳ２１）。

【００９２】
照合部２３０は、入力パスコード抽出部２２４により抽出された３桁の入力パスコード（照合用パスコード）と、記憶部２４０に登録されているパスコードとを照合する。この照合により、両者が一致する場合に認証ＯＫ、一致しない場合に認証ＮＧとする（ステップＳ２２）。
【００９３】
以上のように、上述した第２の実施形態によれば、上述した第１の実施形態と同様の効果が得られると共に、端末である入力情報認証装置１００よりも強固なセキュリティで防御しているサーバ装置２００をパスコードの保存場所とできるため、セキュリティをさらに向上させることができる。
【００９４】
また、初期パターンをサーバ装置２００で生成し、その初期パターンに基づいた入力コード列をサーバ装置２００が入力情報認証装置１００から受信して処理を行うことにより、チャレンジ・アンド・レスポンスのような認証効果が得られ、端末自体のなりすまし（端末上のプログラムのなりすましを含む）に対する防御の効果が得られる。
【００９５】
〔第３の実施形態〕
次に、本発明の第３の実施形態について説明する。
第３の実施形態は、登録されたパスコードをハッシュ関数などの一方向関数で暗号化してから記憶し、その状態でユーザによる入力パスコードの照合ができるようにするものである。
上述した第１の実施形態と同様のものについては、説明を省略する。
【００９６】
第３の実施形態としての入力情報認証装置１００は、図７に示すように、上述した第１の実施形態の構成に加え、ハッシュ関数などの一方向関数でパスコードを暗号化する暗号化登録部１６０を備える。記憶部１４０は、暗号化登録部１６０により暗号化されたパスコードを記憶する。
【００９７】
本実施形態の入力情報認証装置１００により、パスコードが装置に登録される際に暗号化して記憶しておく動作について、図８のフローチャートを参照して説明する。
以下の動作例では、ハッシュ関数としてｍｄ５を用いる場合について示し、数値ｘをハッシュ化したハッシュコードをｍｄ５（ｘ）として示す。
【００９８】
登録するパスコードが入力されると、入力パスコード抽出部１２４は、タッチキーボードの初期パターンと入力色の組み合わせ全てについて、抽出パターンを予め生成する（ステップＳ３１）。この初期パターンと入力色の組み合わせは、入力キーの数の組み合わせから考えられる全パターン（入力キーが９つであれば2^9通り）について用意してもよく、用いる初期パターンと入力色の組み合わせを予め決めておき（例えば３０パターンなど）、その決めた数だけ用意してもよい。
【００９９】
暗号化登録部１６０は、生成された抽出パターンにパスコードの各桁を割り当て、その抽出パターンを桁毎に分解してハッシュ化する（ステップＳ３２）（第１の暗号化手段）。こうしてハッシュ化された各桁についてのハッシュコードをひとまとまりとして、タッチキーボードの初期パターンと入力色の組み合わせに関連付け、記憶部１４０に記憶する（ステップＳ３３）。
【０１００】
図９に、抽出パターンを桁毎に分解してハッシュ化する一例を示す。図９の例では、抽出パターンが、上述した図２（ａ）の例のように、６桁のキー入力に対して、ユーザによる入力パスコードの「１桁目，ダミー，２桁目，３桁目，ダミー，ダミー」であり、パスコードが「１，２，３」である場合について示す。

【０１０１】
この抽出パターンにパスコードの各桁を割り当て、ダミーコードを「＊」で示すと、図９に例示するように、「１，＊，２，３，＊，＊」となる。ここで、３桁のパスコードを桁毎に分解すると、「１０００００」，「２０００」，「３００」となる。分解されたパスコードの抽出パターンにおける桁を示すために、他の桁を「０」として示している。
【０１０２】
他の桁を表す数字は、パスコードに用いられない数字を用いる。本実施形態では、認証情報が１～９の数字の何れかからなるパスコードであることとして説明しているため、他の桁を「０」として示す。例えば認証情報が０～９の数字の何れかからなるパスコードである場合、１６進数で表記される数字列における「１０」を他の桁とすることで同様に実現することができる。
【０１０３】
こうして桁毎に分解されたパスコードの数字を、パスコードに用いられない「０」を用いて桁取りした「１０００００」，「２０００」，「３００」のそれぞれをｍｄ５でハッシュ化する。こうしたハッシュ化されたハッシュコードのひとまとまりであるｍｄ５（１０００００）、ｍｄ５（２０００）、ｍｄ５（３００）を、タッチキーボードの初期パターンと入力色の組み合わせ（図９の例では、図２（ａ）の組み合わせ）に関連付けて記憶部１４０に記憶する。
【０１０４】
図１０に、パスコードの桁毎の分解例を示す。図１０の例では、パスコードが「１，２，３」である場合について示す。
【０１０５】
図９により上述したような抽出パターンの桁毎の分解について、パスコード入力の際には初期パターンにおける２つのキー色を順次反転させて入力を受けるため、連続して入力される２文字のどちらかが、次のパスコードの文字となっているはずである。
【０１０６】
例えば図１０に示すように、パスコードが「１，２，３」であれば、パスコード１桁目の「１」は、ユーザによる入力コード列の１文字目または２文字目の何れかとなるはずである。すなわち、抽出パターンの桁毎に分解した状態で示すと、「１０００００」または「１００００」の何れかとなる。
【０１０７】
同様に、パスコード２桁目の「２」は、ユーザによる入力コード列の２文字目から４文字目の何れかとなるはずである。すなわち、抽出パターンの桁毎に分解した状態で示すと、「２００００」、「２０００」、「２００」の何れかとなる。
【０１０８】
また、パスコード３桁目の「３」は、ユーザによる入力コード列の３文字目から６文字目の何れかとなるはずである。すなわち、抽出パターンの桁毎に分解した状態で示すと、「３０００」、「３００」、「３０」、「３」の何れかとなる。
【０１０９】
こうして、図１０に示すように、パスコードが「１，２，３」であれば、パスコードを抽出パターンの桁毎に分解した状態として８通りが存在しうることとなる。
【０１１０】
上述した図８のステップＳ３３では、タッチキーボードの初期パターンと入力色の組み合わせに対して、この８通りの何れかにより、図９の例で上述したような各桁毎に分解されてハッシュ化されたハッシュコードのまとまりを関連付けて記憶部１４０に記憶することとなる。
【０１１１】
このようにすることで、仮に入力情報認証装置１００を入手した第三者が記憶部１４０内の記憶情報を解析しようとした場合であっても、登録パスコードが分からないだけでなく、抽出パターンにおけるどの入力桁がユーザによる入力パスコードの何れかの桁に該当

するのかも不明とすることができる。

【０１１２】

次に、第３の実施形態による入力情報認証装置１００がユーザからパスコード入力を受ける際の動作例について、図１１のフローチャートを参照して説明する。

【０１１３】

パスコード入力を受ける際の動作として、ステップＳ４１～Ｓ４６の動作は、第１の実施形態で上述した図４のフローチャートにおけるステップＳ１～Ｓ６の動作と同様である。

【０１１４】

こうして規定数、すなわちパスコードの桁数に同じ桁数のダミーコードを加えた倍の桁数が入力されると、暗号化登録部１６０は、ユーザによる入力コード列を、パスコード登録時と同様に各桁毎に分解してｍｄ５によりハッシュ化する（ステップＳ４７）（第２の暗号化手段）。

【０１１５】

照合部１３０は、タッチキーボードの初期パターンおよび入力色に関連付けられて記憶部１４０に記憶されたハッシュコードと、ステップＳ４７でハッシュ化されたハッシュコードとを照合する（ステップＳ４８）。

【０１１６】

ここで、入力コード列はダミーコードを含むため、タッチキーボードの初期パターンおよび入力色に関連付けられたハッシュコードの数よりも、ステップＳ４７でハッシュ化された入力コード列からのハッシュコードの数の方が多くなる。例えばパスコードが３桁であれば、タッチキーボードの初期パターンおよび入力色に関連付けられたハッシュコードは３つであり、ステップＳ４７でハッシュ化された入力コード列からのハッシュコードは６つとなる。

【０１１７】

このため、ステップＳ４７でハッシュ化された入力コード列からのハッシュコードのそれぞれについて、入力された上位桁から、タッチキーボードの初期パターンおよび入力色に関連付けられたハッシュコードの中に一致するものがあるか否かを検索することとなる。そして、タッチキーボードの初期パターンおよび入力色に関連付けられたハッシュコード、すなわち登録パスコードからのハッシュコードの全てに対して一致するか否かの照合を行い、一致するハッシュコードが検出された場合に、照合ＯＫとなり、パスコード認証ＯＫとなる。

【０１１８】

具体例を挙げると、例えば図３（ａ）に例示したタッチキーボードの初期パターンおよび入力色に対して、この図３（ａ）に例示した入力コード列「１，５，２，３，６，４」である場合、ステップＳ４７でハッシュ化される入力コード列からのハッシュコードは、

「ｍｄ５（１０００００）」
「ｍｄ５（５００００）」
「ｍｄ５（２０００）」
「ｍｄ５（３００）」
「ｍｄ５（６０）」
「ｍｄ５（４）」

の６つとなる。

【０１１９】

これに対し、例えば図３（ａ）に例示したタッチキーボードの初期パターンおよび入力色に関連付けられて記憶部１４０に記憶されたハッシュコードは、

「ｍｄ５（１０００００）」
「ｍｄ５（２０００）」
「ｍｄ５（３００）」

の３つである。

【０１２０】
この両者を上述のように照合すると、タッチキーボードの初期パターンおよび入力色に関連付けられた３つのハッシュコードの全てに対して、ステップＳ４７でハッシュ化された６つのハッシュコードの中から一致するハッシュコードが検出される。このため、ステップＳ４８での照合がＯＫとなり、パスコード認証ＯＫとなる。
【０１２１】
以上のように、上述した第３の実施形態によれば、上述した第１の実施形態と同様の効果が得られると共に、パスコードをハッシュ関数などの一方向関数で暗号化してから記憶しているため、入力情報認証装置１００が第三者に入手された場合であっても、メモリ内の記憶情報の解析に対して防御することができる。それでいて、上述した第１の実施形態と同様のダミーコードを含むパスコード入力であっても、確実に入力パスコードの照合を行うことができる。このため、より高度なセキュリティを実現することができる。
【０１２２】
また、上述した第３の実施形態の照合方法では、暗号化された状態で照合のための計算を行うといった高度な計算技法を用いるよりも、格段に少ない計算量で照合することができる。このため、特にモバイル端末など、処理能力が比較的低いコンピュータであっても、容易に実現することができる。
【０１２３】
〔第４の実施形態〕
次に、本発明の第４の実施形態について説明する。
第４の実施形態は、登録されたパスコードをハッシュ関数などの一方向関数で暗号化してから記憶し、その状態でユーザによる入力パスコードの照合ができるようにする他の構成例を示すものである。
上述した第３の実施形態と同様のものについては、説明を省略する。
【０１２４】
本実施形態の入力情報認証装置１００で、ユーザによりパスコードが登録される際に暗号化して記憶しておく動作について説明する。
【０１２５】
登録するパスコードが入力されると、暗号化登録部１６０は、登録パスコードの数字列をハッシュ化し（第１の暗号化手段）、記憶部１４０に記憶させる。
例えば上述した図２の例のように登録パスコードが「１２３」である場合、暗号化登録部１６０は、ハッシュ化したｍｄ５（１２３）を記憶部１４０に記憶させる。
【０１２６】
次に、第４の実施形態による入力情報認証装置１００がユーザからパスコード入力を受ける際の動作例について、図１２のフローチャートを参照して説明する。
【０１２７】
パスコード入力を受ける際の動作として、ステップＳ４１～Ｓ４６の動作は、上述した第３の実施形態と同様である。
【０１２８】
こうして規定数、すなわちパスコードの桁数に同じ桁数のダミーコードを加えた倍の桁数が入力されると、入力パスコード抽出部１２４は、ユーザによる入力パスコードとダミーコードとによるあり得る全てのパターンに基づいて、ユーザによる入力コード列から、各パターンの場合における入力パスコードを抽出する。暗号化登録部１６０は、抽出された入力パスコードのそれぞれをｍｄ５によりハッシュ化する（ステップＳ５１）。
【０１２９】
照合部１３０は、こうしてハッシュ化されたハッシュコードと、記憶部１４０に記憶されたハッシュコードとを照合する（ステップＳ５２）。この照合により照合一致の場合、認証ＯＫとし、他の場合、認証ＮＧとする。
【０１３０】
以下に、ユーザによる入力パスコードとダミーコードとによるあり得る全てのパターン

として予め用意されるパターンについて説明する。

【０１３１】

まず、パスコード１桁目はユーザによる入力コード列の１文字目または２文字目の何れかとなるはずである。

また、パスコード２桁目は、パスコード１桁目がユーザによる入力コード列の１文字目である場合、入力コード列の２文字目または３文字目の何れかとなるはずである。また、パスコード２桁目は、パスコード１桁目がユーザによる入力コード列の２文字目である場合、入力コード列の３文字目または４文字目の何れかとなるはずである。

【０１３２】

このようにして、入力パスコードがユーザによる入力コード列の何文字目に配置されるかのパターン数は、図１０により上述のように、パスコードが３桁であれば2^3＝８通り存在することとなる。

【０１３３】

以上のようにして、登録パスコードが３桁の場合、ユーザによる入力パスコードとダミーコードとであり得る全てのパターンは、下記の８通りとなる。

「（１桁目），（２桁目），（３桁目），＊，＊，＊」
「（１桁目），（２桁目），＊，（３桁目），＊，＊」
「（１桁目），＊，（２桁目），（３桁目），＊，＊」
「（１桁目），＊，（２桁目），＊，（３桁目），＊」
「＊，（１桁目），（２桁目），（３桁目），＊，＊」
「＊，（１桁目），（２桁目），＊，（３桁目），＊」
「＊，（１桁目），＊，（２桁目），（３桁目），＊」
「＊，（１桁目），＊，（２桁目），＊，（３桁目）」

【０１３４】

具体例を挙げると、例えば図３（ａ）に例示した入力コード列「１，５，２，３，６，４」である場合、ステップＳ５１で入力パスコード抽出部１２４により抽出される入力パスコード候補は、「１５２」，「１５３」，「１２３」，「１２６」，「５２３」，「５２６」，「５３６」，「５３４」の８通りとなる。

【０１３５】

このため、暗号化登録部１６０によりハッシュ化されるハッシュコードは、下記の８通りとなる。

「ｍｄ５（１５２）」
「ｍｄ５（１５３）」
「ｍｄ５（１２３）」
「ｍｄ５（１２６）」
「ｍｄ５（５２３）」
「ｍｄ５（５２６）」
「ｍｄ５（５３６）」
「ｍｄ５（５３４）」

【０１３６】

これに対し、登録パスコードにより記憶部１４０に記憶されたハッシュコードは「ｍｄ５（１２３）」である。この両者を上述のように照合すると一致するハッシュコードが検出されるため、ステップＳ５２での照合がＯＫとなり、パスコード認証ＯＫとなる。

【０１３７】

以上のように、上述した第４の実施形態によれば、上述した第３の実施形態と同様の効果を得ることができる。

また、この第４の実施形態では、パスコード登録時に、単純に登録パスコードをハッシュ化するだけで、登録パスコードを解析不能にできるだけでなく、入力コード列におけるダミーコードの配置も不明にできる。さらに、どの初期パターンの場合に認証ＯＫとするための入力内容がどうなるかの対応関係も全く不明とすることができる。このため、初期

パターンと入力色の組み合わせに対して、どの入力桁が入力パスコードとされるのかの情報も保護することができる。

【０１３８】

また、以上により、ハッシュ化されたパスコードに対する力尽くの攻撃に対する耐性を、キー数のパスコード桁数乗（図２の例では９キーにパスコード３桁で9^3＝７２９通り）にすることができる。すなわち、登録パスコードをハッシュ化した状態で照合する構成とすることにより、力尽くで登録パスコードを推測する攻撃に対する耐性を損なってしまうことがない。

【０１３９】

また、入力パスコードとダミーコードの配置についてあり得るパターンをハッシュ化して照合するため、正しいタイミングで押されなかったパスコードが偶然一致することもない。すなわち、登録パスコードを入力すべきタイミングで入力せず、その後にユーザがキー入力した場合であっても、入力すべきタイミングで入力しない時点で認証ＮＧとするルールを確実に実行することができる。

【０１４０】

〔各実施形態について〕

なお、上述した各実施形態は本発明の好適な実施形態であり、本発明はこれに限定されることなく、本発明の技術的思想に基づいて種々変形して実施することが可能である。

【０１４１】

例えば、上述した各実施形態では、パスコードが「１，２，３」の３桁の場合の例について説明したが、パスコードの桁数はこの数に限定されず、装置の性能等に応じて任意に定められるものであってよい。当然、パスコードの桁数を多くすることで、セキュリティをより高めることができる。

【０１４２】

また、上述した実施形態では、認証情報として数字によるパスコードを用いることとして説明したが、認証情報は数字列として表記しうるものであればこのものに限定されず、アルファベット等の文字や、ストローク、またはそれらの組み合わせなどであってもよい。

この場合、例えばアルファベットであれば、表示入力部１１０がアルファベットのキーによるタッチキーボードを表示し、入力されたアルファベットのＡ～Ｚを１～２６の番号として扱う、あるいはアスキーコードにより文字列を数字列化するなどの方法により、上述した実施形態と同様に実現することができる。また、ストロークであれば、入力開始点の座標と終了点の座標を数字列として扱うことで、上述した実施形態と同様に実現することができる。

【０１４３】

また、キーをユーザが識別する表示情報として文字や数字ではなく画像を用いてもよい。この場合、入力キーを２つの領域に分けて各領域のキーを２つの状態に状態分けして表示する方法としては、一方の状態であるキーの表示範囲を白、灰色、黒などでマスクし、他方の状態であるキーの表示範囲を異なる色でマスクするまたはマスクなしとする方法などを用いることができる。また、上述した入力情報の認証については、画像における各入力キーとして割り当てる領域にキー番号やキーの表示座標などの数字を割り当てることで同様に処理を行うことができる。

また、上述した第２の実施形態のように、サーバ装置２００に認証情報が登録される構成である場合、サーバ装置２００がこうした領域分けおよび状態分けした画像情報を生成し、上述した初期パターンとして入力情報認証装置１００に送信し、入力情報認証装置１００がその画像情報を初期パターンの画像として表示し、２つの状態を反転させていくことで、上述した第２の実施形態と同様に処理を行うことができる。

【０１４４】

このように、上述した実施形態で用いることのできる認証情報は、予め定められた変換を行うなどにより数字列として表記できるものであれば、数字列、文字列、画像列、座標

情報、またはそれらの組み合わせなどであってもよい。

【０１４５】

また、上述した実施形態では、２つの領域を表示色により分けて１文字入力毎に反転させることとして説明したが、反転のタイミングは１文字入力毎に限定されず、２文字毎など所定回数の入力操作が行われる度に反転させる構成であってもよい。また、例えば３文字目の入力操作後と５文字目の入力操作後など、予め定められたタイミングで適宜反転させる構成であってもよい。

この場合、パターン反転部１２２がその予め定められたタイミングで初期パターンを反転させることとなる。

また、上述した第４の実施形態では、入力パスコード抽出部１２４が図１２のステップＳ５１で、所定のタイミングでの反転によりあり得る入力パスコードとダミーコードの全てのパターンについて、入力コード列から入力パスコードを抽出する。こうして、所定のタイミングでの反転によりあり得る全てのパターンについて抽出された入力パスコードを、暗号化登録部１６０がハッシュ化し、照合部１３０により照合を行うことにより、同様に実現することができる。

【０１４６】

また、上述した第３、第４の実施形態では、一方向関数による暗号化として、ｍｄ５によりハッシュ化する場合の例について説明したが、一方向関数を用いた暗号化には任意の方法を用いてよく、例えばＨＭＡＣによりハッシュ化する場合などでも本発明は同様に実現することができる。

【０１４７】

また、上述した実施形態は、表示色によりキーを２つの領域に分けることとして説明したが、キーを２つの領域に分けることができれば表示色で分けることに限定されず、例えばキーに触れた感じを変えるなど、２種類の異なる状態であると人が認識可能であるように状態分けすることができれば任意の状態分け方法であってよい。

【０１４８】

また、上述した各実施形態では、表示入力部１１０のタッチパネルディスプレイに表示されるタッチキーボードにユーザがキー入力することとして説明したが、入力部と表示部は、キー色や触感などキーの状態を変化させる機構を備えたものであれば、タッチキーボードに限定されず、物理的なキーボードであってもよい。

【０１４９】

また、上述した各実施形態は、入力部と表示部とが一体である構成に限定されず、入力部と表示部が別体、あるいは別装置であっても、本発明は同様に実現することができる。

入力部と表示部が別体である場合、表示部に入力部と同じキーを表示し、その表示部におけるキー色により、入力部の各キーが認識対象のキー色となっているか、認識対象外のキー色となっているかを示し、キー入力を受けることとなる。こうした構成によっても、上述した各実施形態を同様に実現でき、同様の効果を得ることができる。

【０１５０】

また、上述した各実施形態の入力情報認証装置１００は、携帯情報端末に限定されず、デスクトップＰＣなどの据え置き型装置についても同様に適用することができる。

【０１５１】

また、上述した各実施形態では、入力キーを着色キーと白色キーの２つの領域にパターン分けすることとして説明したが、認識対象外とするキー領域を予め決めておき、その領域のキーを灰色等でハイド表示としてもよい。この場合、上述した各実施形態における入力色判定部１２３および判定ステップが不要となる。

このようにすることで、同じ色のキーしか入力すべきでないことをユーザに分かりやすく示すことができる。

【０１５２】

また、入力色とするキー色を予め決めておき、その入力色でない色のキーについては、入力することができない入力不可能状態としておく構成であってもよい。この場合、上述

した各実施形態における入力色判定部１２３および判定ステップが不要となる。また、こうした構成の場合、ユーザが入力色を決め、装置に予め入力色を設定する構成であってもよい。

このようにすることで、同じ色のキーしか入力できない構成とし、入力ルールをユーザにとって分かりやすいものとすることができる。

【０１５３】

また、上述した各実施形態としての入力情報認証装置１００やサーバ装置２００を実現するための処理手順をプログラムとして記録媒体に記録することにより、本発明の各実施形態による上述した各機能を、その記録媒体から供給されるプログラムによって、システムを構成するコンピュータのＣＰＵに処理を行わせて実現させることができる。

この場合、上記の記録媒体により、あるいはネットワークを介して外部の記録媒体から、プログラムを含む情報群を出力装置に供給される場合でも本発明は適用されるものである。

すなわち、記録媒体から読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードを記憶した記録媒体および該記録媒体から読み出された信号は本発明を構成することになる。

この記録媒体としては、例えばハードディスク、光ディスク、光磁気ディスク、フロッピー（登録商標）ディスク、磁気テープ、不揮発性のメモリーカード、ＲＯＭ等を用いてよい。

【０１５４】

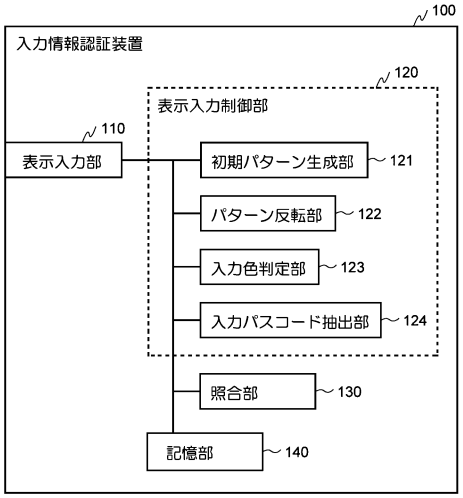
この本発明に係るプログラムによれば、当該プログラムによって制御されるコンピュータに、上述した各実施形態における各機能を実現させることができる。

【符号の説明】

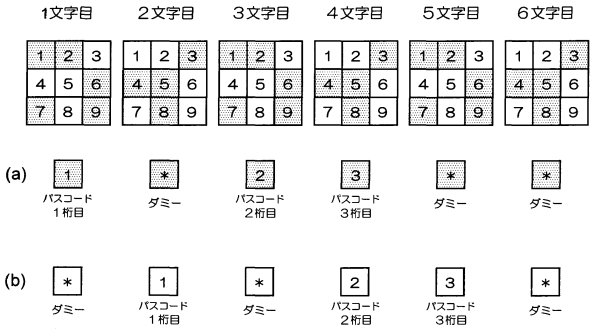
【０１５５】

１００　入力情報認証装置
１１０　表示入力部
１２０　表示入力制御部
１２１　初期パターン生成部
１２２　パターン反転部
１２３　入力色判定部
１２４　入力パスコード抽出部
１３０　照合部
１４０　記憶部
１５０　通信部
１６０　暗号化登録部（第１の暗号化手段および第２の暗号化手段の一例）
２００　サーバ装置

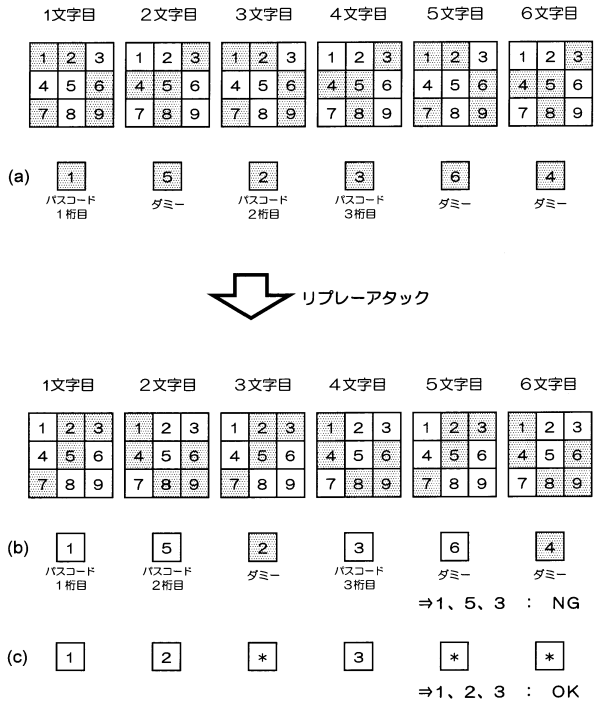
【図１】


100
入力情報認証装置
120
表示入力制御部
110
表示入力部
初期パターン生成部
121
パターン反転部
122
入力色判定部
123
入力パスコード抽出部
124
照合部
130
記憶部
140

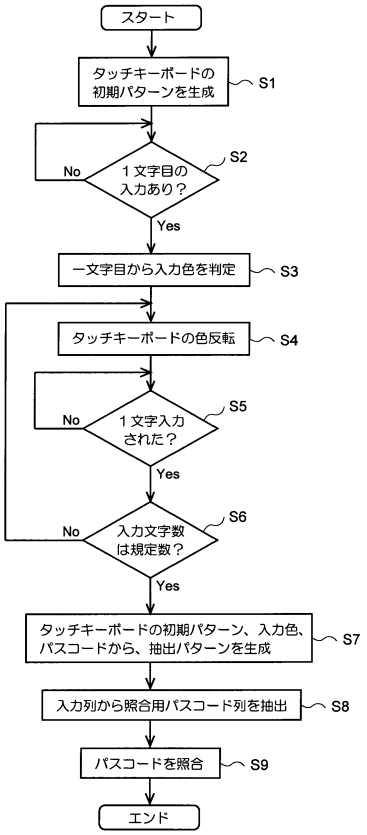
【図２】


1文字目
2文字目
3文字目
4文字目
5文字目
6文字目
(a)
パスコード 1桁目
ダミー
パスコード 2桁目
パスコード 3桁目
ダミー
ダミー
(b)
ダミー
パスコード 1桁目
ダミー
パスコード 2桁目
パスコード 3桁目
ダミー

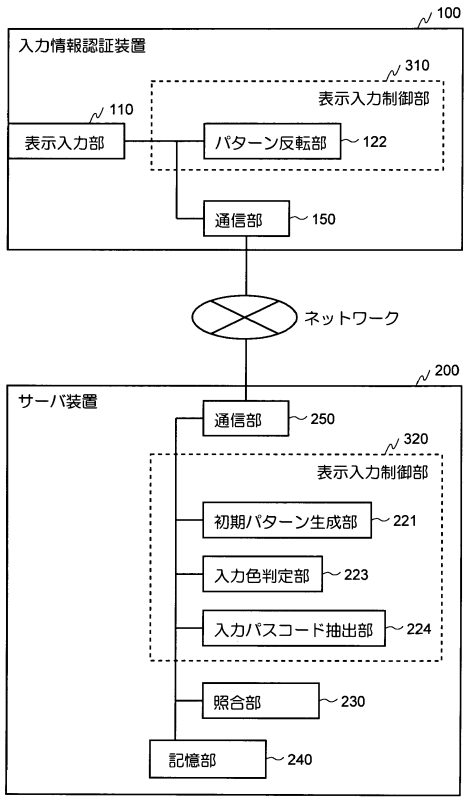
【図３】


1文字目
2文字目
3文字目
4文字目
5文字目
6文字目
(a)
パスコード 1桁目
ダミー
パスコード 2桁目
パスコード 3桁目
ダミー
ダミー
リプレーアタック
(b)
パスコード 1桁目
パスコード 2桁目
ダミー
パスコード 3桁目
ダミー
ダミー
⇒1、5、3 ： NG
(c)
⇒1、2、3 ： OK

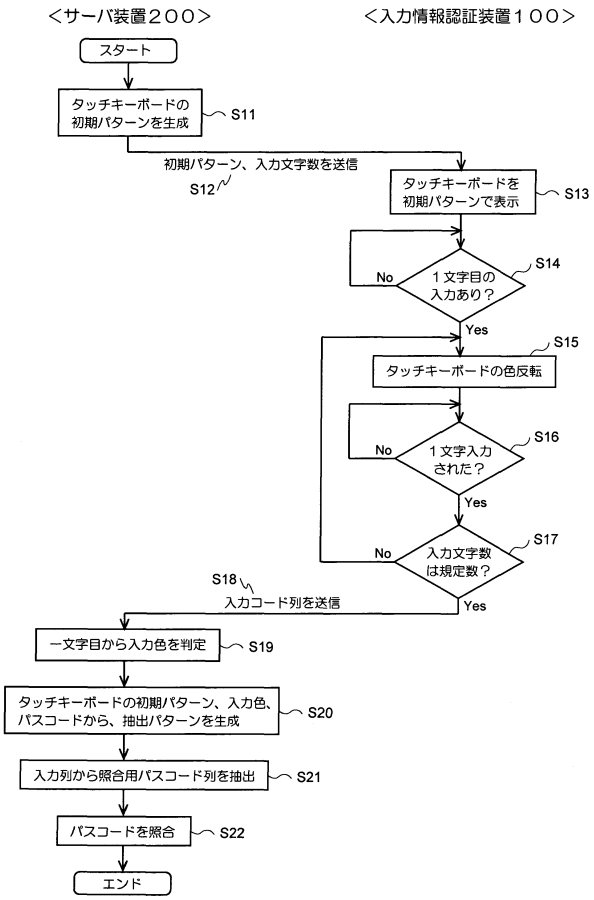
【図４】


スタート
タッチキーボードの初期パターンを生成
S1
1文字目の入力あり？
S2
No
Yes
一文字目から入力色を判定
S3
タッチキーボードの色反転
S4
1文字入力された？
S5
No
Yes
入力文字数は規定数？
S6
No
Yes
タッチキーボードの初期パターン、入力色、パスコードから、抽出パターンを生成
S7
入力列から照合用パスコード列を抽出
S8
パスコードを照合
S9
エンド

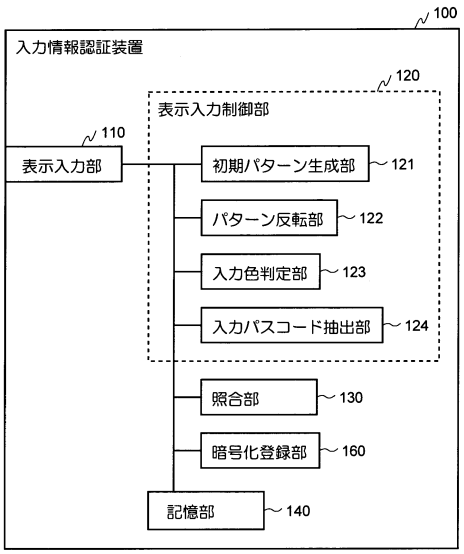
【図５】



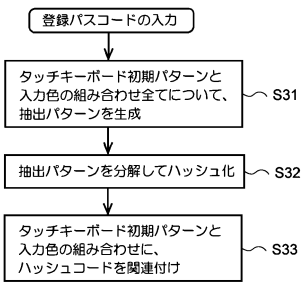
【図６】



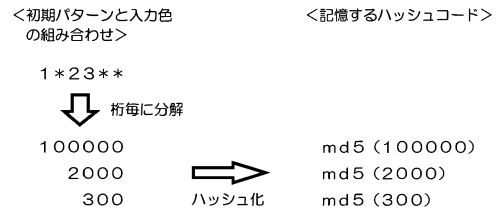
【図７】



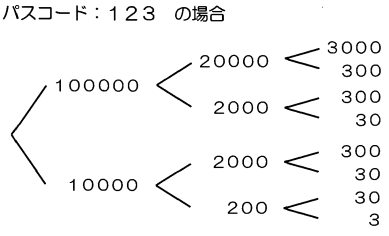
【図８】



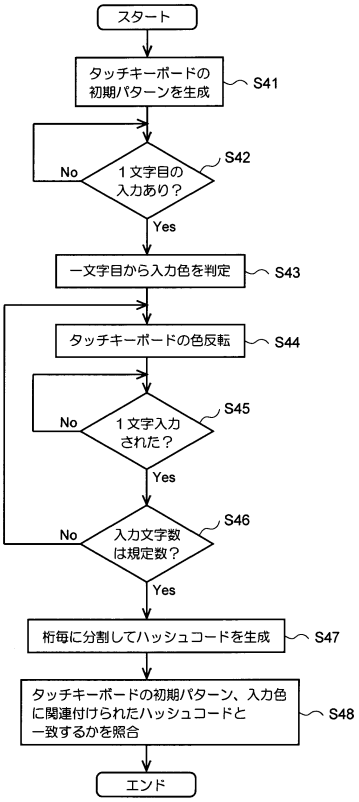
【図９】



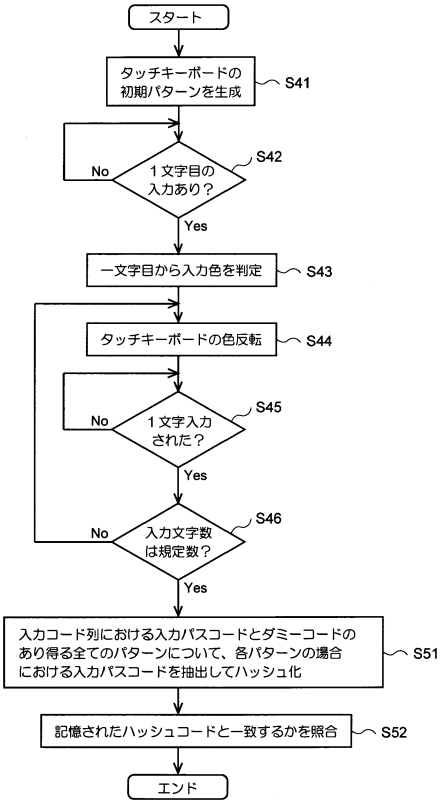
【図１０】



【図１１】


スタート
タッチキーボードの初期パターンを生成
S41
No
１文字目の入力あり？
S42
Yes
一文字目から入力色を判定
S43
タッチキーボードの色反転
S44
No
１文字入力された？
S45
Yes
No
入力文字数は規定数？
S46
Yes
桁毎に分割してハッシュコードを生成
S47
タッチキーボードの初期パターン、入力色に関連付けられたハッシュコードと一致するかを照合
S48
エンド

【図１２】


スタート
タッチキーボードの初期パターンを生成
S41
No
１文字目の入力あり？
S42
Yes
一文字目から入力色を判定
S43
タッチキーボードの色反転
S44
No
１文字入力された？
S45
Yes
No
入力文字数は規定数？
S46
Yes
入力コード列における入力パスコードとダミーコードのあり得る全てのパターンについて、各パターンの場合における入力パスコードを抽出してハッシュ化
S51
記憶されたハッシュコードと一致するかを照合
S52
エンド

フロントページの続き

(56)参考文献 特開２０１０－９５４３（ＪＰ，Ａ）
特開２００９－１６９８５７（ＪＰ，Ａ）
特開２００６－２５１９８５（ＪＰ，Ａ）
韓国公開特許第１０－２０１０－００４９７４８（ＫＲ，Ａ）
北林　良太　ほか，複数回の覗き見に耐性を有するパスワード認証方式の提案，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００９年　６月２５日，Vol．109，No．115，pp．21-26

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３６
Ｈ０４Ｌ　９／２８
Ｈ０４Ｌ　９／３２