審決

不服２０２１－　　５４３８

（省略）
請求人　　リセンティア グループ リミテッド

（省略）
代理人弁理士　　菊池 徹

（省略）
代理人弁理士　　菊池 新一

（省略）
代理人弁理士　　松本 英俊

（省略）
請求人　　マイピンパッド リミテッド

（省略）
代理人弁理士　　菊池 徹

（省略）
代理人弁理士　　菊池 新一

（省略）
代理人弁理士　　松本 英俊

特願２０１７－５６１７５５「認証方法及び認証システム」拒絶査定不服審判事件〔平成２８年１２月　１日国際公開、ＷＯ２０１６／１８９３２２、平成３０年　９月２０日国内公表、特表２０１８－５２７６３９〕について、次のとおり審決する。

結　論

本件審判の請求は、成り立たない。

理　由

結　論

本件の審判請求は，成り立たない。
理　由
第１　手続の経緯
　本件審判請求に係る出願（以下，「本願」という。）は，２０１６年５月２７日（パリ条約による優先権主張外国庁受理２０１５年５月２７日，英国，２０１５年５月２７日，英国，２０１５年１１月２４日，英国，２０１５年１１月２４日，英国）を国際出願日とする特許出願であって，その手続の経緯は以下のとおりである。
　平成３０年　１月２６日　　：翻訳文提出
　令和　２年　４月２７日付け：拒絶理由通知書
　令和　２年　８月１１日　　：意見書，手続補正書の提出
　令和　２年１２月２１日付け：拒絶査定
　令和　３年　４月２７日　　：審判請求書，手続補正書の提出

第２　本願発明
　本願請求項１－１７に係る発明は，令和３年４月２７日にされた手続補正で補正された特許請求の範囲の請求項１－１７に記載された事項により特定される発明であり，請求項１に係る発明（以下，「本願発明」という。）は，以下のとおりの発明である。なお，符号「Ａ」～「Ｆ」は，当審において付与したものであり，それぞれの構成を，「構成Ａ」などという。
「【請求項１】
Ａ　電子デバイスに関連したスクリーンのディスプレイ領域内で操作可能なキーパッド上にキーパッド画像を提示し，
Ｂ　前記キーパッド画像及び／又は操作可能なキーパッドは，前記電子デバイスにローカルに生成される少なくとも1つのスクランブルキーパッド配列を用いて生成され，
Ｃ　前記キーパッド画像を介して前記操作可能なキーパッドをユーザが操作することによって前記電子デバイスに入力された識別子の符号化されたバージョンを記憶し，
Ｄ　前記識別子の符号化されたバージョンを遠隔のコンピューティング資源に送信し，
Ｅ　前記少なくとも１つのスクランブルキーパッド配列を前記遠隔のコンピューティング資源に送信して前記識別子の符号化されたバージョンを復号化することができるようにする
Ｆ　認証方法。」

第３　原査定の拒絶の理由
　原査定の拒絶の理由は，この出願の請求項１－１７に係る発明は，本願の優先権主張の日（以下「優先日」という。）前に日本国内又は外国において

，頒布された又は電気通信回線を通じて公衆に利用可能となった下記の引用文献１に記載された発明及び引用文献２-５に記載された事項に基づいて，その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから，特許法２９条２項の規定により特許を受けることができない，というものである。

記

引用文献１．国際公開第２０１４／０１３２５２号
引用文献２．米国特許出願公開第２０１４／０３２４７０８号明細書
引用文献３．特表２００８-５０６１９８号公報
引用文献４．特開２００６-３０９４１７号公報
引用文献５．特開２０００-１６５３７８号公報

ここで，本願発明については，引用文献１に記載された発明及び引用文献２に記載された事項に基づいて，当業者が容易に発明することができたものであるとしている。

第４　引用文献

１　引用文献１の記載

原査定の拒絶の理由に引用された，国際公開第２０１４／０１３２５２号（以下，「引用文献１」という。）には，図面とともに以下の記載がなされている（下線は強調のため当審で付与。「・・・」は省略部分を示す。）。

ア「This invention relates generally to the field of user authentication, and more particularly to the field of PIN-based verification. The invention is suited for use in situations where a user is required to enter a code, such as a Personal Identification Number (PIN), which is validated prior to completing an operation. The operation might be any type of operation.」（第１頁第３行～同頁第６行）

（当審訳）

「本発明は，一般的には，ユーザ認証の分野に関し，更に詳細に述べると，ＰＩＮによる検証の分野に関する。本発明は，ある操作を完了する前に確認される個人識別番号（ＰＩＮ）等のコードを入力することがユーザに要求される状況で使用するのに適している。この操作は，どんな種類の操作であってもよい。」

イ「According to a first aspect of the invention, there may be provided a computer- implemented verification method comprising the step of:
enabling a user to input an identifier into an electronic device hav

ing:
i) a screen; and
ii) a keypad operable within a keypad zone of the screen;
by operating at least one key of the keypad via an image of at least part of a scrambled keypad which is displayed at least partially within the keypad zone.

The image may be referred to as a 'scrambled keypad image' for ease of reference.
. . .
The scrambled keypad image is not a keypad per se because it is devoid of any functionality. It is merely a representation of a grid of keys. Touching, clicking on or otherwise selecting any 'key' depicted in the image does not, in and of itself, produce any effect or generate an input.

However, it should be noted that the scrambled keypad image may sometimes be referred to as a 'keypad' 'scrambled keypad' or an Overlying keypad' purely for ease of reference because in use it appears to function as a keypad. Areas of the image may be referred to as 'keys', again only for ease of reference because this is what the user appears to see and use. However, it should be remembered that this is not actually the case, and that the image is not a keypad in reality.

The invention may enable the user to enter his identifier via the same device component that is used to display the scrambled keypad image (the screen). Phrased another way, the screen may serve as both the output (display) device for the scrambled keypad image and the input device via which the user's identifier may be entered. This contrasts with any prior art disclosure wherein the keypad is displayed on one device component (e.g. screen) and the user's input is received via another device component (e.g. keyboard).

An advantage of this feature is that it may enable the user's input from the image to be mapped to the electronic keypad which may be at least partially hidden from the user's view such that the user's input is automatically encoded upon entry by the user. The input is automatically encoded in the sense that the electronic device may not

need to convert, encode or in any way process the user's input. The keypad may be generated by a procedure call executed on the electronic device. The operable, electronic keypad may be referred to as a 'reference' or 'underlying' keypad for ease of reference.

Preferably, the user's operation of the keypad key via the image generates an encoded version of the user's intended input. Preferably, the image is displayed within the keypad zone such that as the user touches, clicks on or otherwise identifies a location within the image, an operable keypad key at that location is activated to provide an encoded version of the user's input.
・・・
Thus, in one sense the invention may be viewed as enabling a scrambled keypad image to be 'superimposed' over an 'underlying' keypad such that when the user enters his input via the overlaid scrambled keypad image it is encoded in accordance with the layout of the underlying (preferably unseen) keypad.

The 'underlying' keypad may be viewed as an object generated and residing in the device's volatile memory at run-time to provide a model of a conventional mechanical keypad.

Thus, the invention provides the advantage that the user's 'real' identifier is never stored within the device and is not transmitted for verification. Therefore, the user's identifier cannot be derived by any potential interceptor without knowledge of the mapping between the overlaid image and underlying, functional keypad. Preferably, the mapping between the overlaid image and underlying keypad is not stored in the electronic device, or derivable by the electronic device. The mapping (or correlation) between the positions of the two sets of 'keys' may be stored on a server remote from the electronic device.」（第８頁第２６行～第１１頁第２８行）
（当審訳）
「本発明の第１の態様によれば，
ユーザが，
ｉ）画面と，
ｉｉ）画面のキーパッドゾーン内で操作可能なキーパッドと
を有する電子デバイスに識別名を入力することを可能にする工程から成っているが，この工程は，前記キーパッドゾーン内に少なくとも部分的に表示さ

れるスクランブルキーパッドの少なくとも一部の画像を介して，前記キーパッドの少なくとも１つのキーを操作することによって行われるコンピュータ実施の検証方法を提供することができる。

参照を容易にするために，この画像は，「スクランブルキーパッド画像」と称する。

・・・

スクランブルキーパッド画像は，いかなる機能もないので，それ自体はキーパッドではない。これは，単に，キーの格子を表現したものである。画像内に描写されたいずれかの「キー」に触れたり，クリックしたり，又は別の方法で選択しても，それ自体としては何の効果も生じさせないか，又は入力を生成することはない。

しかし，スクランブルキーパッド画像は，使用時にキーパッドとして機能するように見えるので，参照しやすくするだけのために，「キーパッド」，「スクランブルキーパッド」又は「上にあるキーパッド」と呼ばれることが場合によってあることに留意されたい。画像の領域は，ユーザが見て使用するものであるようなので，同様に，参照しやすくするだけのために，「キー」と呼ばれることがある。しかし，これは，実際にはそうではないこと，また画像は実際にはキーパッドではないことを記憶にとどめるべきである。

本発明は，ユーザが自分の識別名を，スクランブルキーパッド画像を表示するために使用されるのと同じデバイス構成要素（画面）を介して入力することを可能にし得る。言い換えると，画面は，スクランブルキーパッド画像用の出力（表示）デバイスとしても，ユーザの識別名を入力できる入力デバイスとしても機能することができる。これは，キーパッドが１つのデバイス構成要素（例えば，画面）上に表示され，ユーザの入力が別のデバイス構成要素（例えば，キーボード）を介して受け取られる，いかなる従来技術の開示とも対照的である。

この特徴の利点は，ユーザが入力すると，ユーザの入力が自動的に符号化されるように，画像からのユーザの入力を，ユーザの視野から少なくとも部分的に隠すことができる電子的キーパッドにマッピングすることを可能にし得ることである。この入力は，電子デバイスがユーザの入力を変換する，符号化する，又は何らか処理する必要がない可能性があるという意味において，自動的に符号化される。キーパッドは，電子デバイスで実行される手続き呼出しによって生成することができる。操作可能な電子的キーパッドは，参照しやすくするために，「参照」キーパッド又は「下にある」キーパッドと呼ばれることがある。

好ましくは，画像を介したユーザのキーパッドの操作により，ユーザの意図した入力の符号化バージョンが生成される。好ましくは，画像がキーパッドゾーン内に表示され，その結果，ユーザが画像内のある場所に触れたり，その場所をクリックしたり，又は別の方法で識別すると，その場所の操作可

能なキーパッドのキーが活性化されてユーザの入力の符号化バージョンが得られるようになる。
・・・
従って，ある意味で本発明は，ユーザが自分の入力を重ね合わされたスクランブルキーパッド画像を介して入力したときに，この入力が，下にある（好ましくは見えない）キーパッドのレイアウトに応じて符号化されるように，スクランブルキーパッド画像が「下にある」キーパッドの上に「重ね合わされる」ことを可能にするものとみなすことができる。
「下にある」キーパッドは，従来の機械的キーパッドのモデルを得るため，実行時に，デバイスの揮発性メモリ内に生成され存在するオブジェクトとみなすことができる。
従って，本発明は，ユーザの「実」識別名がデバイス内に保管されることが決してなく，また検証のために送信されることがないという利点を有する。従って，ユーザの識別名は，重ね合わされた画像と下にある動作可能なキーパッドとの間のマッピングについての知識がなければ，いかなる潜在的な傍受者でも導出することができない。好ましくは，重ね合わされた画像と下にあるキーパッドとの間のマッピングは，電子デバイス内に保管されることはないし，あるいは電子デバイスによって導出されることはない。２組の「キー」の位置の間のマッピング（又は対応関係）は，電子デバイスから離れているサーバに保管することができる。」

ウ「Preferably, the scrambled keypad image may be sent from a remotely located computer- based resource to the electronic device. The resource may be a server. Thus, the scrambled keypad image may not be generated on the electronic device. A version of the scrambled keypad image may be stored on the server. The version may be a record of the order of the symbols (”keys”) in the scrambled keypad image.

The keypad zone may be a defined area or portion of the screen. Thus, the keypad zone may occupy the entire screen area or a portion of the screen. The scrambled keypad image may be displayed such that it covers the keypad zone completely, exactly or partially. Preferably, the underlying keypad is at least partially hidden from view so that the user is not able to see at least some of the keys of the keypad.

The identifier may be a Personal Identification Code. It may be a PIN (Personal Identification Number). It may comprise any number, type or combination of symbols or indicia (as explained above). The iden

tifier may have been pre-selected by the user prior to executing the presently claimed method. The identifier may be stored remotely from the electronic device e.g. on a server. The scrambled keypad image and/or keypad may comprise numeric digits, alphabetical characters, punctuation, symbols or any other indicia, or a combination thereof. One or more symbols may be associated with each key.

Preferably, the user may be able to select a plurality of "keys" in the scrambled keypad image to input an identifier comprising more than one symbol.

The scrambled keypad image may be scrambled with respect to a reference keypad. The keypad image may depict a block or grid comprising a plurality of adjacent keys. It may be 'scrambled' in the sense that the symbols on the "keys" are not in sequential order and/or not in the order which one would expect, perhaps with reference to the reference keypad. The scrambling may be in accordance with a random generation process, or a process that approximates to a random process. The reference keypad may be the keypad operable within the keypad zone, or a default keypad associated as standard with a make, model, type of electronic device.

Thus, the same indicia may be present in both the underlying keypad and the scrambled keypad image but they are provided in different positions. Put yet another way, the order of the keys in the reference keypad is different from that of the scrambled image. The scrambled keypad image may provide the same 'look and feel' as the default keypad associated with the electronic device, but with the "keys" in different relative positions.

The respective positions of one, some or all "key(s)" in the scrambled keypad image may be different from the position of the same key(s) in the underlying keypad.

The user may operate the keys of the underlying keypad via the scrambled keypad image by interacting with the "keys" displayed on the screen. For example, the user's input may be entered by the user touching the screen (with a finger or other device) or by selecting the desired "key(s)" using a pointing device such as a mouse or tracker b

all. Other selection methods may be used to similar effect, thus fal
ling within the scope of the invention.
・・・
Preferably, the scrambled keypad image is received by the electronic
device from a computer-based resource (e.g. a server) located remot
ely from the electronic device. It may be sent to the electronic dev
ice from the server in respect to a request for an image, the reques
t being sent from the device to the server. The scrambled keypad ima
ge may be generated by the server.

Preferably, the scrambled keypad image is pre-generated. In one embo
diment this may mean that it is generated prior to, not in response
to, the request from the electronic device. The image may be generat
ed prior to execution of the verification method.

The encoded version of the user's input (identifier) may be sent fro
m the electronic device to a remote computer-based resource. This re
source may be a server. Preferably, the server receives the encoded
version of the user's input and processes it. The processing may pro
vide a decoded version of the user's inputted identifier.

Thus, the user's 'real' identifier may not be transmitted. Only the
encoded version may be transmitted, which may be meaningless to an u
nauthorised party who does not know the mapping between the the "key
s" in the scrambled keypad image and the keys in the underlying keyp
ad.

The decoding may be performed using a stored version or form of the
scrambled keypad image. The stored version or form of the configurat
ion of the keys may be a filename. The decoding step may provide a d
ecoded version of the user's input. Thus, the user's 'real' identifi
er may be generated by translating each symbol in the encoded versio
n into its corresponding counterpart in the scrambled keypad image.

The user's decoded input may be compared with a stored version of th
e identifier. The user's input may be deemed to be correct if the in
put matches the stored identifier.」（第１１頁第３０行～第１４頁第２
２行）
（当審訳）

「好ましくは，スクランブルキーパッド画像は，遠隔に設置されたコンピュータベースの資源から電子デバイスへ送信することができる。この資源は，サーバであってもよい。従って，スクランブルキーパッド画像は，電子デバイスで生成されることがないものとすることができる。スクランブルキーパッド画像の１つのバージョンをサーバに保管することができる。このバージョンは，スクランブルキーパッド画像内の記号（「キー」）の配列の記録とすることができる。

キーパッドゾーンは，画面の画定された領域又は部分とすることができる。従って，キーパッドゾーンは，画面領域全体を占めてもよいし，画面の一部分を占めていてもよい。スクランブルキーパッド画像は，それがキーパッドゾーンを完全に，正確に，又は部分的に覆うように表示することができる。好ましくは，下にあるキーパッドは，ユーザがキーパッドのキーの少なくとも幾つかは見ることができないように，少なくとも部分的に視野から隠される。

識別名は，個人識別コードとすることができる。これは，ＰＩＮ（個人識別番号）であってもよい。ＰＩＮは，任意の数字，種類又は組合せの記号若しくは印を含むことができる（上記した通り）。識別名は，現に特許請求された方法を実行する前に，ユーザによって事前選択されていたのものであってよい。識別名は，電子デバイスから遠隔にある，例えばサーバに保管することができる。スクランブルキーパッド画像及び／又はキーパッドは，数字，英字，句読点，記号若しくは他の印，又はこれらの組合せを含むことができる。１つ又は複数の記号をそれぞれのキーに関連させることができる。

好ましくは，ユーザは，スクランブルキーパッド画像内の複数の「キー」を選択して，２つ以上の記号を含む識別名を入力することができる。

スクランブルキーパッド画像は，参照キーパッドに対してスクランブルすることができる。キーパッド画像は，複数の隣り合うキーを含むブロック又は格子を描写することができる。キーパッド画像は，「キー」上の記号が順番になっていないか，且つ／又は，おそらく参照キーパッドに関連して人が予測するであろう配列になっていないという意味において，「スクランブル」することができる。スクランブルは，ランダム生成処理，又はランダム処理に近い処理に従うことができる。参照キーパッドは，キーパッドゾーン内で操作可能なキーパッド，又は電子デバイスのメーカ，モデル，種類に標準として関連している初期設定キーパッドとすることができる。

従って，下にあるキーパッドとスクランブルキーパッド画像の両方に同じ印が存在し得るが，これらは異なる位置に設けられる。言い換えると，参照キーパッド内のキーの配列は，スクランブル画像のものとは異なる。スクランブルキーパッド画像は，電子デバイスに関連している初期設定キーパッドと同じ「ルック・アンド・フィール」を与えることができるが，「キー」は異なる相対位置にある。

スクランブルキーパッド画像内の１つ，幾つか，又はすべての「キー」のそれぞれの位置は，下にあるキーパッド内の同じキーの位置とは異なるものとすることができる。

ユーザは，画面に表示された「キー」と対話することによって，下にあるキーパッドのキーをスクランブルキーパッド画像を介して操作することができる。例えば，ユーザの入力は，ユーザが画面に触れることによって（指，又は別のデバイスで），又はマウス若しくはトラッカボール等のポインティングデバイスを使用して所望の「キー」を選択することによって，入力することができる。同様の効果をもたらして，それによって本発明の範囲内に入る，他の選択方法を用いることもできる。

・・・

好ましくは，スクランブルキーパッド画像は，電子デバイスから遠隔に設置されたコンピュータベースの資源（例えば，サーバ）から，電子デバイスで受信される。スクランブルキーパッド画像は，電子デバイスからサーバへ送信される画像の要求に対して，サーバから電子デバイスへ送信することができる。スクランブルキーパッド画像は，サーバで生成することができる。

好ましくは，スクランブルキーパッド画像は，事前生成される。一実施形態では，このことは，スクランブルキーパッド画像が，電子デバイスからの要求に応じてではなく，要求前に生成されることを意味する。画像は，検証方法を実行する前に生成することができる。

ユーザの入力（識別名）の符号化バージョンは，電子デバイスから，遠隔のコンピュータベースの資源へ送信することができる。この資源は，サーバとすることができる。好ましくは，サーバは，ユーザの入力の符号化バージョンを受信し，それを処理する。この処理により，ユーザの入力識別名の復号化バージョンを得ることができる。

従って，ユーザの「実」識別名は伝送されることがないものとすることができる。符号化バージョンだけを伝送することができ，この符号化バージョンは，スクランブルキーパッド画像内の「キー」と下にあるキーパッド内のキーとの間のマッピングを知らない，許可されていない者には意味のないものである。

復号化は，スクランブルキーパッド画像の保管バージョン又は保管形式を用いて実施することができる。キーの構成の保管バージョン又は保管形式は，ファイル名とすることができる。復号化ステップにより，ユーザの入力の復号化バージョンを得ることができる。従って，ユーザの「実」識別名は，符号化バージョン内のそれぞれの記号を，スクランブルキーパッド画像内のその対応するものに変換することによって生成することができる。

ユーザの復号化入力は，識別名の保管バージョンと比較することができる。入力が保管識別名と一致した場合，ユーザの入力は正しいと認められる。

エ「Pin Pad Production
The 'PIN Pad Production Program' 6 is responsible for generating all of the scrambled keypad images 3 used throughout the system. An overview of this aspect of the invention is shown in Figure 5.

If simply randomly scrambled keypads are used, there is a risk that one or more keys may not be positionally scrambled. This could resort in one or more keys of the users input PIN corresponding positionally on the standard and scrambled PIN. This is not ideal.

Consequently, during PIN pad (image) generation, scrambled key pad images that would have one or more keys positionally corresponding to the standard keypad are discarded. The PIN pad production is therefore preferably not purely random, but is subjected to a selection process to select/discard according to a specific criteria.

The PIN pad (image) generation takes place in a secure environment, typically complaint with payment card industry data security standard. The output resolution and file type must be initially set up before use on a particular target device 1 (in this case the type of mobile phone). This ensures that outputted images are generated to the optimum resolution for that device e.g. 256 x 184.

A master 'Background Image' 7 is then selected which matches the resolution as set above, and a 'Permutations File' 5 selected containing all the required permutations of digits (keys) for the final keypad images. In one implementation, this file 5 must be a comma separated text file with each permutation on a new line. However, a variety of implementations may be devised to the same effect. For example, each permutation could be separated by a # or *.

The 'Permutations File' 5 is then merged with the 'Background Image' 7 using the user's selection of Font Type, Size and Colour to produce the completed keypad image 3. The completed keypad image 3 is then optimized and reduced in size to be as small as possible for optimum transmission speed.」（第２４頁第２５行～第２５頁第２４行）
（当審訳）
「Ｐｉｎパッド生成
‘ＰＩＮパッド生成プログラム’６は，システム全体を通して使用される

スクランブルキーパッド画像３のすべてを生成することを担う。本発明のこの態様の概要が図５に示されている。
ただ単にランダムにスクランブルされたキーパッドが使用される場合，１つ又は複数のキーを位置的にスクランブルされないというリスクがある。これは，標準ＰＩＮ及びスクランブルＰＩＮに位置的に一致するユーザの入力ＰＩＮの１つ又は複数のキーに頼ることもできる。これは，理想的ではない。
その結果，ＰＩＮパッド（画像）生成中，標準キーパッドに位置的に一致する１つ又は複数のキーを有するスクランブルキーパッド画像は破棄される。従って，ＰＩＮパッド生成は，好ましくは全くランダムではないが，特定の基準に従って選択／破棄する選択処理にかけられる。
ＰＩＮパッド（画像）生成は，典型的には，ペイメントカード業界データセキュリティ標準に従う安全な環境で行われる。出力解像度及びファイルタイプは，特定のターゲットデバイス１（この場合にはモバイル電話のタイプ）で使用する前に最初に設定されなければならない。これにより，出力画像は，そのデバイスに最適な解像度，例えば２５６×１８４で生成されることが保証される。
次に，上記で設定された解像度に適合するマスタ‘背景画像’７が選択され，また，最終キーパッド画像に必要な数字（キー）の順列をすべて含む‘順列ファイル’５が選択される。一実施態様では，このファイル５は，新たな行にそれぞれの順列があるカンマ区切りテキストファイルでなければならない。しかし，同じ効果を得るのに種々の実施態様を工夫することができる。例えば，それぞれの順列は，＃又は＊によって区切ることもできる。
次に，‘順列ファイル’５は，フォントタイプ，サイズ，色についてのユーザの選択を用いて‘背景画像’７と合成されて，完成したキーパッド画像３を生成する。その後，この完成したキーパッド画像３は，最適な伝送速度を得るために可能な限り小さくなるようにサイズが最適化され低減される。」

オ「It should be noted that in certain alternative embodiments, 12 smaller key pictures (one for each number or hotspot) may be provided. The phone or other device may be arranged to to select a random number and rearrange the individual pictures into a 3x4 array (and thus making up a virtual keypad on demand). However, such embodiments present potential security loopholes and may provide several access points for malware to obtain the user’s PIN (as the handset/device would have to transmit the random number and thus the order of the PIN pad back to the server). Therefore, such an embodiment is suitable for applications where required security levels are somewhat relaxe

d.」（第３３頁第６行～同頁第１３行）
（当審訳）
「幾つかの他の実施形態では，１２個の小さいキーピクチャ（番号又はホットスポット毎に１つ）を設けることができることに留意すべきである。電話又は他のデバイスは，ランダム番号を選択し，個々のピクチャを３×４アレイの中に再配置するように構成することができる（また，それによって，要望に応じて仮想キーパッドを構成することができる）。しかし，このような実施形態は，潜在的にセキュリティの抜け穴を提供し，またユーザのＰＩＮを入手するためのマルウェアに幾つかのアクセスポイントを与える恐れがある（ハンドセット／デバイスがランダム番号，従ってＰＩＮパッドの順序をサーバに返送しなければならない。）。従って，このような実施形態は，所要のセキュリティレベルが幾分緩やかな用途に適している。」

カ「Additional PinPad Encryption

In order to further enhance the security of the system, the invention may employ one or more techniques for making it more difficult for an unauthorised party to figure out, discern or calculate the mapping between the displayed keypad image (i.e. the one that the user uses to enter his PIN) and the underlying keypad.

For example, if the user has selected a PIN which contains the same digit more than once (e.g. 1223) this may make it easier to compute the correlation between the input and the 'underlying' keypad.

One possible approach to overcoming this could be to create more than one underlying keypad. For example, a virtual keypad could be generated for each key press. An example is given below.

Figure 16a shows a scrambled keypad image, and Figure 16b shows an 'underlying' keypad. If the user's PIN is 1111 then the encoded PIN sent back to the server would be 9999. This provides a potential hacker with a starting point for an attempt at calculating or guessing the user's PIN.

However, if 4 different 'underlying' keypads are used instead of one, this problem is overcome. Thus, a sequence of digits can be sent to the target device (e.g. terminal, phone, PC) and the sequence is used by the target device to form the keypad. For the keypad in Figur

e 16b, the sequence would be. 3156790482. Using this approach, it is possible to generate a new keypad for each required key press.

Thus, the top pin pad as per Figure 16a is sent to the target device as an image, in accordance with the description set out above. Then, 4 numeric sequences are sent for the creation of the underlying keypad e.g. 3156790482, 0746189352, 0347156289, 2581673904. This produces the keypads shown in figures 16b to 16e.

Suppose now that the user's input is 1111. Instead of 9999 being produced, the code 9857 is produced and sent back to the server for decryption. As the server 'knows' which scrambled keypad image was sent, and which sequences of digits, the resulting encoded PIN appears to be much more random and is therefore much harder to decipher by an interceptor. The decryption process at the server end remains as set out above.
」（第３５頁第２７行～第３５頁第２７行）
（当審訳）
「追加のＰｉｎパッド暗号化
　システムのセキュリティを更に強化するために，本発明は，表示されたキーパッド画像（すなわち，ユーザが自分のＰＩＮを入力するために使用するもの）と，下にあるキーパッドとの間のマッピングを許可されていない者が解明，識別又は計算することを一層困難にする１つ又は複数の技法を用いることができる。
　例えば，ユーザが２回以上同じ数字を含むＰＩＮ（例えば，１２２３）を選択した場合，これにより，入力と「下にある」キーパッドの間の相関関係を計算することが容易になり得る。
　これを克服するために実現可能な１つの手法は，２つ以上の下にあるキーパッドを作成することである。例えば，キーを押すごとに仮想キーパッドを生成することもできる。一例を以下に示す。
　図１６Ａは，スクランブルキーパッド画像を示し，図１６Ｂは「下にある」キーパッドを示す。ユーザのＰＩＮが１１１１である場合，サーバに返送される符号化ＰＩＮは９９９９になる。これにより，ユーザのＰＩＮを計算又は推測してみようとするきっかけが潜在的ハッカーに与えられる。
　しかし，１つではなく４つの異なる「下にある」キーパッドが使用されるならば，この問題は克服される。すなわち，一連の数字をターゲットデバイス（例えば，端末，電話，パーソナルコンピュータ（ＰＣ））へ送信することができ，この一連のものがターゲットデバイスで用いられてキーパッドが形成される。図１６Ｂのキーパッドでは，この一連のものは３１５６７９０

４８２になる。この手法を用いると，要求されたキー押しごとに新しいキーパッドを生成することができる。

従って，図１６Ａによる上ｐｉｎパッドが，前述の説明通りに，画像としてターゲットデバイスへ送信される。次に，４つの数列，例えば３１５６７９０４８２，０７４６１８９３５２，０３４７１５６２８９，２５８１６７３９０４が，下にあるキーパッドを作成するためへ送信される。これにより，図１６Ｂ～１６Ｅに示されたキーパッドが生成される。

ところで，ユーザの入力が１１１１であると仮定する。９９９９が生成される代わりに，符号９８５７が生成され，復号化のためにサーバに返送される。サーバは，どのスクランブルキーパッド画像が送信されたか，またどの数字の列が送信されたかを「知っている」ので，結果として得られた符号化ＰＩＮはよりいっそうランダムに見え，従って傍受者が解読するのはずっと困難になる。サーバ末端部での復号化処理は，前述の通りに存続する。」

キ「FIG.5

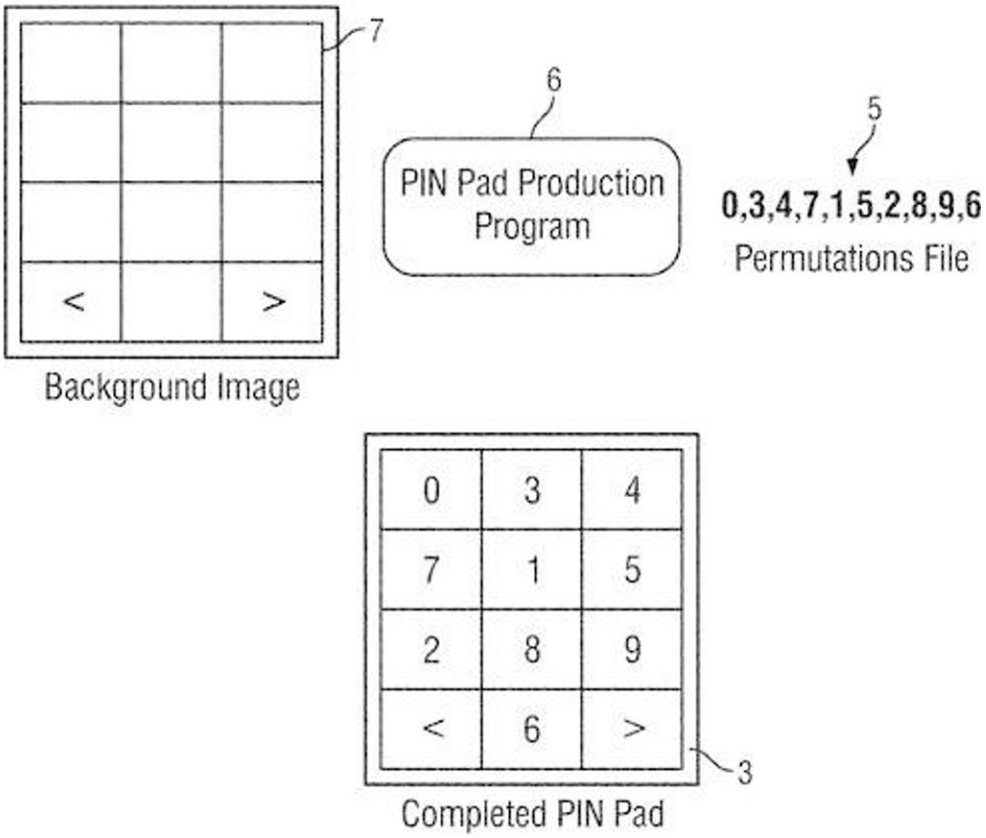

FIG. 5

」

ク「FIG.16

6	3	4
5	0	1
7	2	8
<	9	>

Top PinPad

FIG. 16A

3	1	5
6	7	9
0	4	8
<	2	>

Bottom PinPad

FIG. 16B

0	7	4
6	1	8
9	3	5
<	2	>

2nd PinPad

FIG. 16C

0	3	4
7	1	5
6	2	8
<	9	>

3rd PinPad

FIG. 16D

2	5	8
1	6	7
3	9	0
<	4	>

4th PinPad

FIG. 16E

」

2　引用発明

ア　上記１アによれば，引用文献１には，ユーザ認証の分野に関する「ＰＩＮによる検証」について記載されている。

イ　上記１イによれば，引用文献１には，「画面のキーパッドゾーン内で操作可能なキーパッド」を有する「電子デバイス」に「識別名を入力することを可能にする工程」から成る「検証方法」が記載されており，当該工程は，「キーパッドゾーン内に少なくとも部分的に表示されるスクランブルキーパッド」である，「スクランブルキーパッド画像」を介して，「キーパッドのキーを操作することによって行われる」ものである。
　ここで，「スクランブルキーパッド画像」は，画像からのユーザの入力を，キーパッドにマッピングすることを可能にするもので，スクランブルキーパッド画像が「下にある」キーパッドの上に「重ね合わされる」ことにより，「スクランブルキーパッド画像」を介して行われるユーザの入力が，下にあるキーパッドのレイアウトに応じて符号化されるようになっており，「画像を介したユーザのキーパッドの操作により，ユーザの意図した入力の符号化バージョンが生成される」ものである。
　したがって，引用文献１には，「ユーザが入力した識別名の検証方法」に用いる電子デバイスについて，「電子デバイスの画面のキーパッドゾーン内で操作可能なキーパッド」と，「キーパッドゾーン内に表示されるスクランブルキーパッド画像」とを備え，「スクランブルキーパッド画像を介したユーザのキーパッドの操作により，ユーザの意図した入力の符号化バージョンが生成される」ことが記載されているといえる。

ウ　上記１ウによれば，引用文献１には，「スクランブルキーパッド画像」について，「遠隔に設置されたコンピュータベースの資源であるサーバ」で生成し，「電子デバイスへ送信」するものであること，また，「スクランブルキーパッド画像」のキーの位置は，操作可能なキーパッド内の同じキーの位置とは異なるものとすることが記載されている。
　そして，ユーザは，「スクランブルキーパッド画像」内の複数のキーを選択して，識別名として用いるＰＩＮを入力し，入力されたＰＩＮの符号化バージョンは，電子デバイスからサーバへ送信され，サーバは，これを処理して，識別名であるＰＩＮの復号化バージョンを得ることが記載されている。
　したがって，引用文献１には，ユーザの識別名として「ＰＩＮ」を用いること，「スクランブルキーパッド画像は，遠隔に設置されたコンピュータベースの資源であるサーバから電子デバイスに送信されること」，「ＰＩＮの符号化バージョンは，電子デバイスから，サーバへ送信され，サーバにおいて，ＰＩＮの符号化バージョンを復号化すること」が記載されているといえる。

エ　上記１エ，キによれば，引用文献１の「スクランブルキーパッドの画像」は，「最終キーパッド画像に必要なキーの順列をすべて含む順列ファイル」を用いて生成されることが記載されている。

オ　以上より，引用文献１には，次の発明（以下，「引用発明」という。）が記載されていると認められる。なお，各構成の符号「ａ」ないし「ｆ」は，説明のために当審において付与したものである（以下，符号を付した構成を「構成ａ」ないし「構成ｆ」という。）。

（引用発明）
ａ　電子デバイスの画面のキーパッドゾーン内で操作可能なキーパッドと，キーパッドゾーン内に表示されるスクランブルキーパッド画像とを用い，
ｂ　スクランブルキーパッド画像は，最終キーパッド画像に必要なキーの順列をすべて含む順列ファイルを用いて生成され，遠隔に設置されたコンピュータベースの資源であるサーバから電子デバイスに送信され，
ｃ　スクランブルキーパッド画像を介したユーザのキーパッドの操作により，ユーザの意図した入力のＰＩＮの符号化バージョンが生成され，
ｄ　ＰＩＮの符号化バージョンは，電子デバイスから，サーバへ送信され，
ｅ　サーバにおいて，ＰＩＮの復号化バージョンを得る，
ｆ　ユーザが入力したＰＩＮの検証方法。

３　引用文献２の記載
原査定の拒絶の理由に引用された，米国特許出願公開第２０１４／０３２４７０８号明細書（以下，「引用文献２」という。）には，図面とともに以下の記載がなされている（下線は強調のため当審で付与。）。

ア「[0014] A technique to secure passcode entry on an electronic device is disclosed herein. The technique involves encrypting raw input events from an input device of an electronic device. A complete passcode entry may produce multiple raw input events, such as multiple touch events on a touch screen. In such instances, each raw input may represent the location of a touch event on a touch screen, and each event representing a touch location is encrypted. Thus, encryption of individual input events serves as a measure to prevent unauthorized discovery (e.g., by malware) of the passcode.」
（当審訳）
「[0014]　電子デバイス上へのパスコード入力をセキュアに行う技術が，本明細書に開示される。該技術は，電子デバイスのインプットデバイスからの生のインプットイベントを暗号化することを含む。パスコード入力が完了す

ることにより，複数の生のインプットイベントが生成され得る。該複数の生のインプットイベントは，例えば，タッチスクリーン上における複数のタッチイベントである。そのような場合では，各々の生のインプットがタッチスクリーン上におけるタッチイベントの位置を表し得ると共に，タッチ位置を表す各イベントは，暗号化される。したがって，個々のインプットイベントの暗号化は，パスコードの（例えば，マルウェアによる）認可されない発見を防止するための尺度として役立つ。」

イ「[0017] The raw input events can be touch events as recorded by a touch screen of the electronic device. A passcode interface, such as a PIN or key pad, may be displayed on the touch screen. The user may enter the passcode entry for authentication on the touch screen. The electronic device may encrypt the touch events resulting from the interaction with the touchscreen. The electronic device may then transmit the encrypted touch events represented by touch screen coordinates to a trusted computing system to cause the trusted computing system to decipher the passcode, as entered by the user, based on the encrypted touch events. To cause in this context is intended to include sending a command, a request, or any other type of message or signal that results in the stated action, such as deciphering the passcode based on the encrypted touch events.
[0018] In various embodiments, only the trusted computing system performs the transformation from the encrypted raw input events into the passcode entry. Instead of deciphering the passcode entry on the electronic device, the input events are sent to the trusted computing system for interpretation. The trusted computing system, which may be external to the electronic device, can then decrypt each input event to decipher the passcode entered by the user.
[0019] Deciphering of the passcode may include comparing the decrypted touch event to a passcode interface configuration. For example, the passcode interface configuration may be or include a key pad layout, which can be represented as a data structure or object. As a more specific example, the key pad layout can be generated by the trusted computing system and sent to the electronic device for presentation. As another specific example, the key pad layout can be generated by the electronic device, and sent to the trusted computing system for deciphering. Either way, the trusted computing system may use the passcode interface configuration, e.g., key pad layout, to map sensor input events to a sequence of characters used to compose the pas

scode entry.
[0020] The key pad layout may include geometry, position, relative position, animation sequence, or other variations of the presentation of the key pad. The key pad may include multiple buttons taking up regions of the touch screen of the electronic device. Each touch event may be represented by an (X,Y) location coordinate, where each coordinate or set of coordinates is encrypted in accordance with various embodiments of the disclosed technique. The passcode can then be deciphered by mapping each (X,Y) coordinate to a two dimensional space corresponding to a specific soft-button representing a character used to compose a passcode entry.」
（当審訳）
「[0017] 上記生のインプットイベントは，上記電子デバイスのタッチスクリーンにより記録されるタッチイベントであり得る。ＰＩＮ又はキーパッドのようなパスコードインタフェースは，該タッチスクリーン上に表示され得る。上記ユーザは，該タッチスクリーン上での認証のために，上記パスコード入力を入力し得る。該電子デバイスは，該タッチスクリーンとの相互作用によって生じる該タッチイベントを暗号化し得る。該電子デバイスは，その後，タッチスクリーンの座標によって表される暗号化された該タッチイベントをトラステッドコンピューティングシステムに伝送し，それによって，該トラステッドコンピューティングシステムに，該ユーザによって入力された該パスコードを，該暗号化されたタッチイベントに基づいて解読するようにさせる。この文脈では，「させる（to cause）」が，該暗号化されたタッチイベントに基づいてパスコードを解読するような規定の動作を結果的にもたらす命令，要求，又は任意の他のタイプのメッセージ若しくは信号を送信することを含むことを企図されている。
[0018] 種々の実施形態では，上記トラステッドコンピューティングシステムのみが，上記暗号化された生のインプットイベントから上記パスコード入力への変換を行う。上記電子デバイス上で該パスコード入力を解読する代わりに，該インプットイベントは，解釈のために該トラステッドコンピューティングシステムに送信される。該トラステッドコンピューティングシステムは，該電子デバイスの外部にあってもよい。該トラステッドコンピューティングシステムは，その後，上記ユーザが入力したパスコードを解読するために，各インプットイベントを復号化し得る。
[0019] パスコードの解読は，上記復号化されたタッチイベントをパスコードインタフェースの構成と比較することを含んでいてもよい。例えば，該パスコードインタフェースの構成は，キーパッドレイアウトであってもよく，キーパッドレイアウトを含んでいてもよい。該キーパッドレイアウトは，データ構造またはオブジェクトとして表現され得る。より具体的な例としては

，該キーパッドレイアウトは，トラステッドコンピューティングシステムにより生成され得ると共に，解読のために上記電子デバイスに送られ得る。別の具体的な例としては，該キーパッドレイアウトは，該電子デバイスによって生成され得ると共に，解読のために該トラステッドコンピューティングシステムに送られ得る。いずれにしても，該トラステッドコンピューティングシステムは，上記パスコード入力を編成するように用いられる一連の文字にセンサインプットイベントをマッピングするために，キーパッドレイアウト等のパスコードインタフェースの構成を使用していてもよい。
[0020] 上記キーパッドレイアウトは，ジオメトリ，位置，相対位置，アニメーションシーケンス，又は他のバリエーションのキーパッドの提示を含んでいてもよい。該キーパッドは，電子デバイスのタッチスクリーン領域を占有する複数のボタンを含んでいてもよい。各タッチイベントは（Ｘ，Ｙ）位置座標により表されてもよく，各座標又は各座標集合は，開示の技術の種々の実施形態に従って暗号化される。その後，上記パスコードは，各（Ｘ，Ｙ）座標を，パスコード入力を編成するのに用いられる文字を表す特定のソフトボタンに対応する二次元空間にマッピングすることによって解読されてもよい。」

ウ「[0023] FIG. 1 is a data flow diagram illustrating a technique 100 of sensor entry encryption. As shown, the technique 100 involves an electronic device 102 and an authentication system 104. The electronic device 102 may be a general purpose device with data processing capabilities. For example, the electronic device 102 may be a mobile phone, a tablet, an e-reader, other mobile or portable computing devices, or other stationary computing devices. The authentication system 104 may be a trusted computing system in data communications with the electronic device 102, such as over a network. The authentication system 104 may be one or more computing devices. For example, the authentication system 104 may be a server computer, a network of computing systems, a cloud computing environment, a virtualized computing environment, or any combination thereof. Communication between the authentication system 104 and the electronic device 102 may be any form of data communication, including mobile telecommunication (e.g., cellular), WiFi, wireless Ethernet, wired Ethernet, or any other form of Internet connection.
[0024] The electronic device 102 may be a mobile device, such as a smartphone or a tablet computer, that presents a passcode interface 106 on an output device. In the illustrated embodiment, the output device is a touch screen 108. A user seeking authentication may input

through a sensor (i.e. an input device) of the electronic device 102, a series of inputs composing a passcode, such as a PIN, a passphrase, a digital key, or any combination thereof. In the illustrated embodiment, the sensor is the touch screen 108. Note, however, that the sensor (e.g., a touch panel or a cursor device) for detecting an input may be different from the output device (e.g., a display, a projection device, a speaker, or other devices capable of presenting the passcode interface 106).」

（当審訳）

「[0023] 図１は，センサ入力の暗号化技法１００を表すデータフロー図である。図示のように，技法１００は，電子デバイス１０２と，認証システム１０４とを含む。電子デバイス１０２は，データ処理機能を備えた汎用デバイスであってもよい。例えば，電子デバイス１０２は，携帯電話，タブレット，電子書籍リーダ（e-reader），他のモバイル若しくはポータブルコンピューティングデバイス又は他の据置コンピューティングデバイスであってもよい。認証システム１０４は，電子デバイス１０２とのデータ通信，例えばネットワーク越しのデータ通信におけるトラステッドコンピューティングシステムであってもよい。認証システム１０４は，１つ以上のコンピューティングデバイスであってもよい。例えば，認証システム１０４は，サーバコンピュータ，コンピューティングシステムのネットワーク，クラウドコンピューティング環境，仮想化されたコンピューティング環境又はそれらの任意の組み合わせであってもよい。認証システム１０４と電子デバイス１０２との間の通信は，モバイル通信（例えば，セルラー），ＷｉＦｉ，無線イーサネット，有線イーサネット又は任意の他の形態のインターネット接続を含む任意の形態のデータ通信であってもよい。

[0024] 電子デバイス１０２は，スマートフォン又はタブレットコンピュータのような，出力デバイス上にパスコードインタフェース１０６を提示するモバイルデバイスであってもよい。図示の実施形態では，該出力デバイスは，タッチスクリーン１０８である。認証を求めるユーザは，電子デバイス１０２のセンサ（すなわち，インプットデバイス）を通じて，ＰＩＮ，パスフレーズ，デジタル鍵又はそれらの任意の組み合わせ等の，パスコードを編成するインプットのシーケンスをインプットしてもよい。図示の実施形態では，該センサは，タッチスクリーン１０８である。もっとも，インプットを検出するための該センサ（例えば，タッチパネル又はカーソルデバイス）は，出力デバイス（例えば，ディスプレイ，投射デバイス，スピーカ又は他のパスコードインタフェース１０６を提示可能なデバイス）とは異なってもよい。」

エ「[0027] In various embodiments, a portion of the sensor input str

eam 114 is sent to the authentication system 104 for deciphering. In various embodiments, when the authentication system 104 receives the portion of the sensor input stream 114, the authentication system 104 may decrypt the sensor entries 110 prior to deciphering the passcode entry 116 by the user. A passcode interface configuration 118, which defines the mechanism of interaction with the passcode interface, may be generated by the electronic device 102 and then sent over to the authentication system 104 as well. The passcode interface configuration may specify a mapping between sensor values of the sensor entries and a set of characters used to compose a passcode entry As an example, where the passcode interface is displayed on the touch screen 108, the passcode interface configuration may include geometric definition of the passcode interface on the touch screen 108. In other embodiments, the passcode interface configuration is generated by the authentication system 104. The passcode interface configuration may be generated specifically for a session with a user interacting with the passcode entry interface.」

（当審訳）

「[0027] 種々の実施形態では、センサインプットストリーム１１４の部分は、復号を行うために認証システム１０４に送信される。種々の実施形態では、認証システム１０４がセンサインプットストリーム１１４の一部を受信した際に、認証システム１０４は、ユーザに入力されたパスコード入力１１６を解読する前にセンサ入力１１０を復号化してもよい。パスコードインタフェース構成１１８は、該パスコードインタフェースと対話する機構を規定するものであって、電子デバイス１０２によって生成された後、同様に認証システム１０４まで送信されてもよい。該パスコードインタフェース構成は、該センサ入力に係るセンサ値と該パスコード入力を編成するのに使用される文字のセットとのマッピングを指定してもよい。例として、該パスコードインタフェースがタッチスクリーン１０８上に表示される場合には、該パスコードインタフェース構成は、タッチスクリーン１０８上の該パスコードインタフェースのジオメトリの規定を含んでいてもよい。他の実施形態では、該パスコードインタフェース構成は、認証システム１０４により生成される。該パスコードインタフェース構成は、特に該パスコード入力インタフェースと対話するユーザとのセッションのために生成されてもよい。」

オ「[0034] FIG. 2 is a block diagram illustrating an electronic device 200, which may represent device 102 in FIG. 1, for passcode entry. The electronic device 200 may be a general-purpose computing device. The electronic device 200 includes various modules and storage as

described below. The electronic device 200 includes a passcode interface module 202, which is configured to present and maintain a passcode interface.

[0035] In various embodiments, the passcode interface module 202 is configured to generate the passcode interface. The passcode interface module 202 may generate the passcode interface randomly or pseudo-randomly. As an example, the passcode interface may be configured as a PIN pad layout. The size, arrangement, position, orientation, shape, and other absolute or relative geometric characteristics of the passcode interface and elements within the passcode interface are all examples of the passcode interface configuration. The passcode interface configuration may be selected to promote concealment of a user's entry of a passcode on the passcode interface. For example, the elements on the passcode interface may be characters from which the passcode combination (e.g., the passcode entry 116) may be chosen. The arrangement of the characters and the geometric shapes and sizes of the characters may be randomized. Other attributes of the passcode interface configuration may be wholly or partially randomly generated. The passcode interface configuration, such as the absolute and relative (e.g., relative to a display of the electronic device 200) geometric characteristics of the passcode interface, may be stored in an interface configuration store 204.

[0036] In other embodiments, the passcode interface configuration is provided by a remote system through a network, such as the authentication system 104 of FIG. 1. For example, the passcode interface configuration may be received through an authentication communication module 206. In those embodiments, once received, the passcode interface configuration may be stored in the interface configuration store 204. The passcode interface configuration may then be used by the passcode interface module 202 to present the passcode interface to the user.

[0037] When the passcode interface configuration is generated on the electronic device 200, the authentication communication module 206 may transmit the passcode interface configuration to the remote system such that the remote system may use a portion of the sensor input stream and the passcode interface configuration to decipher the passcode entry.」

（当審訳）

「[0034] 図２は，パスコード入力のための電子デバイス２００を表すブロ

ック図である。電子デバイス２００は，図１のデバイス１０２を表すものであってもよい。電子デバイス２００は，汎用コンピューティングデバイスであってもよい。電子デバイス２００は，以下に説明するような種々のモジュール及び記憶装置を含む。電子デバイス２００は，パスコードインタフェースを提示及び維持するように構成されたパスコードインタフェースモジュール２０２を含む。

[0035] 種々の実施形態では，パスコードインタフェースモジュール２０２は，上記パスコードインタフェースを生成するように構成されている。パスコードインタフェースモジュール２０２は，該パスコードインタフェースをランダムに又は擬似ランダムに生成してもよい。一例として，該パスコードインタフェースは，ＰＩＮパッドレイアウトとして構成されていてもよい。該パスコードインタフェースのサイズ，配置，位置，向き，形状及び他の絶対的または相対的なジオメトリ特性，並びに該パスコードインタフェース内の要素は，全てパスコードインタフェース構成の例である。該パスコードインタフェース構成は，ユーザのパスコード入力を該パスコードインタフェース上において隠蔽することを促進するように選択されてもよい。例えば，該パスコードインタフェースの該要素は，パスコードの組み合わせ（例えば，パスコード入力１１６）を選択するための文字であってもよい。該文字の配列並びに該文字のジオメトリ形状及びサイズは，ランダム化されてもよい。該パスコードインタフェース構成の他の属性は，全体的又は部分的にランダム生成されてもよい。該パスコードインタフェースの絶対的及び相対的（例えば，電子デバイス２００のディスプレイに対して相対的）なジオメトリ特性のような該パスコードインタフェース構成は，インタフェース構成記憶機構２０４内に格納されてもよい。

[0036] 他の実施形態では，上記パスコードインタフェース構成は，図１の認証システム１０４のように，ネットワークを通じてリモートシステムにより提供される。例えば，該パスコードインタフェース構成は，認証通信モジュール２０６を通じて受信されてもよい。これらの実施形態では，該パスコードインタフェース構成は，いったん受信された後に，インタフェース構成記憶機構２０４に格納されてもよい。該パスコードインタフェース構成は，ユーザに該パスコードインタフェースを提示するために，パスコードインタフェースモジュール２０２に使用されてもよい。

[0037] パスコードインタフェース構成が電子デバイス２００上に生成された際，認証通信モジュール２０６は上記パスコードインタフェース構成を上記リモートシステムに伝送してもよく，それによって，該リモートシステムは上記センサインプットストリームの一部と該パスコードインタフェース構成とを使用してパスコード入力を解読してもよい。」

カ「FIG.1

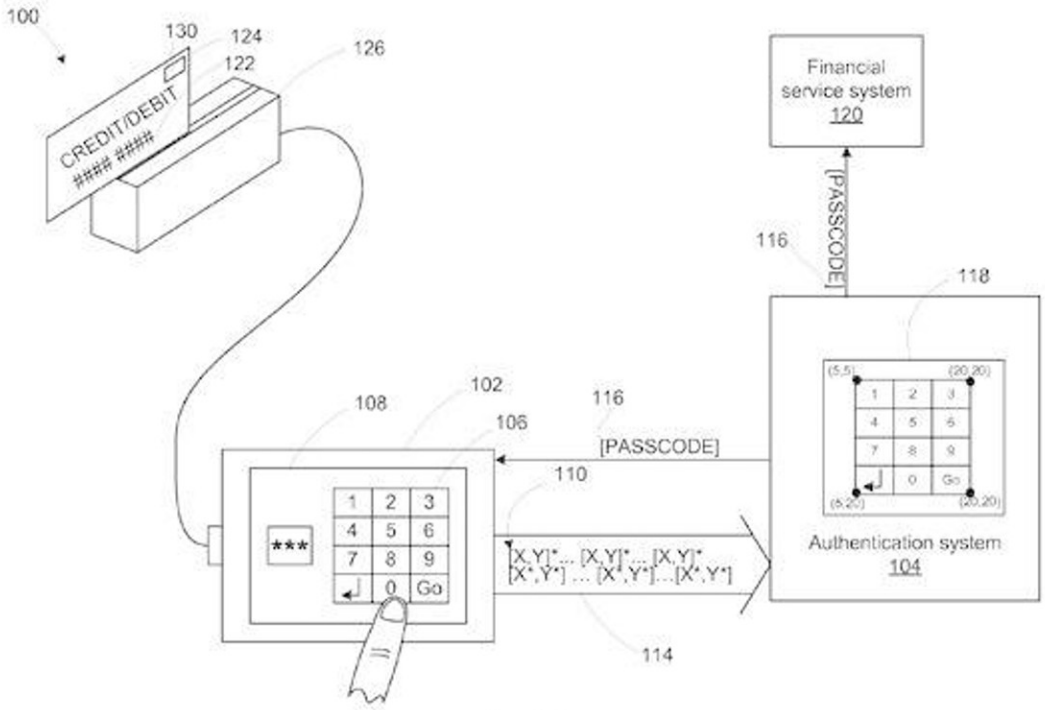

FIG. 1

」

キ「FIG.2

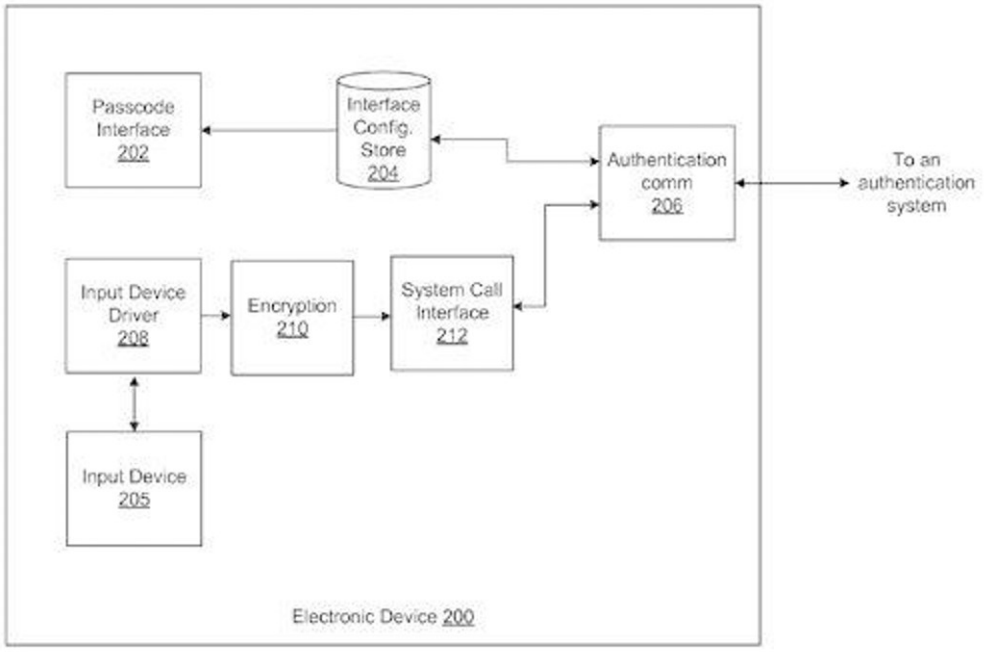

FIG. 2

」

ク　以上より，引用文献２には，「パスコード入力をセキュアに行う技術」として，「パスコードの入力と解読に用いるパスコードインターフェイス構成を，電子デバイスによって生成して，復号のために，トラステッドコンピューティングシステムに送る」ことが記載されている。

ケ　また，引用文献２には，「パスコードインターフェイス構成」について，「電子デバイスの外部に設けたトラステッドコンピューティングシステムにより生成して，電子デバイスに送る」こととした具体例も記載されていることからすると，「パスコードインターフェイス構成」を「トラステッドコンピューティングシステムにより生成して，電子デバイスに送る」ことと，「電子デバイスによって生成して，トラステッドコンピューティングシステムに送る」こととは，相互に置換可能であることが示唆されていると認められる。
　さらに，引用文献２は，「パスコードインターフェイス構成」として，「文字の配列をランダム化すること」にも言及していると認められる。

第５　対比
１　本願発明と引用発明との対比
ア　本願発明の構成Ａと引用発明の構成ａについて
　引用発明の「電子デバイスの画面のキーパッドゾーン」は，本願発明の「電子デバイスに関連したスクリーンのディスプレイ領域」に相当し，引用発明において，「キーパッドゾーン内に表示」される「スクランブルキーパッドの画像」は，本願発明の「操作可能なキーパッド上」に「提示」される「キーパッド画像」に相当する。
　したがって，引用発明の構成ａと本願発明の構成Ａとの間には差異がない。

イ　本願発明の構成Ｂと引用発明の構成ｂについて
　引用発明の「最終キーパッド画像に必要なキーの順列をすべて含む順列ファイル」は，「スクランブルキーパッドの画像」に用いられる，キーパッドの配列である点で，本願発明において，「キーパッド画像及び／又は操作可能なキーパッド」の生成に用いられる「少なくとも１つのスクランブルキーパッド配列」と共通する。
　一方，本願発明の「少なくとも１つのスクランブルキーパッド配列」は，「電子デバイスにローカルに生成される」のに対し，引用発明は，「スクランブルキーパッドの画像」が，遠隔に設置されたコンピュータベースの資源であるサーバから電子デバイスに送信されるものであり，その生成に用いる「順列ファイル」が，電子デバイスでローカルに生成されていない点で相違する。

ウ　本願発明の構成Ｃ，Ｄと引用発明の構成ｃ，ｄについて
　引用発明において，ユーザが意図して入力する「ＰＩＮ」は，本願発明の「識別子」に相当するから，引用発明の「スクランブルキーパッドの画像を介したユーザのキーパッドの操作」により生成される「ユーザの意図した入力のＰＩＮの符号化バージョン」は，本願発明の「前記キーパッド画像を介して前記操作可能なキーパッドをユーザが操作することによって前記電子デバイスに入力された識別子の符号化されたバージョン」に相当する。
　ここで，本願発明は，「識別子の符号化されたバージョン」を「記憶」する構成であるが，「記憶」に先立って，「生成」することは明らかであり，その限りにおいて，引用発明との差異はない。
　また，引用発明が，ＰＩＮの符号化バージョンを送信する「サーバ」は，本願発明の，識別子の符号化されたバージョンを送信する「遠隔のコンピューティング資源」に相当する。
　したがって，本願発明の構成Ｃ，Ｄと引用発明の構成ｃ，ｄとは，本願発明が，識別子の符号化バージョンを「記憶」する構成を有するのに対し，引用発明は，ＰＩＮの符号化バージョンを記憶するかどうか明らかでない点では相違するものの，その余の点では一致するといえる。

エ　本願発明の構成Ｅと引用発明の構成ｅについて
　引用発明において，「ＰＩＮの復号化バージョンを得る」ことは，本願発明が，電子デバイスから送信された「識別子の符号化されたバージョン」を「復号化」することに相当する。
　ここで，復号化できるようにするために，本願発明は，「前記少なくとも１つのスクランブルキーパッド配列を前記遠隔のコンピューティング資源に送信」する構成を有するのに対し，引用発明は，これに相当する構成を備えていない点で相違する。

オ　本願発明の構成Ｆと引用発明の構成ｆについて
　上記第４の１アの記載によれば，引用発明の「ユーザが入力したＰＩＮの検証方法」は，ユーザの認証のための手順であるといえるから，引用発明の「ユーザが入力したＰＩＮの検証方法」は，本願発明の「認証方法」に相当するといえる。

２　一致点，相違点
　したがって，本願発明と引用発明とは，以下の点で一致ないし相違している。

（一致点）

電子デバイスに関連したスクリーンのディスプレイ領域内で操作可能なキーパッド上にキーパッド画像を提示し，
前記キーパッド画像は，スクランブルキーパッド配列を用いて生成され，
前記キーパッド画像を介して前記操作可能なキーパッドをユーザが操作することによって前記電子デバイスに入力された識別子の符号化されたバージョンを生成し，
前記識別子の符号化されたバージョンを遠隔のコンピューティング資源に送信し，
遠隔のコンピューティング資源において，前記識別子の符号化されたバージョンを復号化することができるようにする
認証方法。

（相違点１）
本願発明の「スクランブルキーパッド配列」は，「電子デバイスにローカルに生成される」のに対し，引用発明の「順列ファイル」は，電子デバイスにローカルに生成されるものでない点。

（相違点２）
本願発明は，生成した識別子の符号化バージョンを記憶するのに対し，引用発明は生成したＰＩＮの符号化バージョンを記憶するかどうか明らかでない点。

（相違点３）
本願発明は，「スクランブルキーパッド配列」を「遠隔のコンピューティング装置に送信」するのに対し，引用発明は，そのような構成を備えていない点。

第６　判断
１　相違点についての判断
ア　相違点１及び３について
上記第４の３のとおり，引用文献２には，「パスコード入力をセキュアに行う技術」として，「パスコードの入力と解読に用いるパスコードインターフェイス構成を，電子デバイスによって生成して，復号のために，トラステッドコンピューティングシステムに送ること」が開示されている。
ここで，引用文献２に記載の「パスコードインターフェイス構成」は，「タッチスクリーン１０８上の該パスコードインタフェースのジオメトリの規定」を含み，「センサ入力に係るセンサ値とパスコード入力を編成するのに使用される文字のセットとのマッピングを指定」するものである（上記第４の３エ）から，引用発明の「最終キーパッド画像に必要なキーの順列をすべ

て含む順列ファイル」に相当するものであることは，当業者に明らかである。
そして，引用文献２には，「パスコードインターフェイス構成」として，「文字の配列をランダム化すること」が開示されていること（上記第４の３オ）や，「パスコードインターフェイス構成」を，「トラステッドコンピューティングシステムにより生成して，電子デバイスに送る」ことと，「電子デバイスによって生成して，トラステッドコンピューティングシステムに送る」こととは，相互に置換可能であることが示唆されていること（上記第４の３ケ）に鑑みれば，引用発明において，「最終キーパッド画像に必要なキーの順列をすべて含む順列ファイル」及び「スクランブルキーパッド画像」を，電子デバイスにおいて用いて生成する構成とし，復号に必要となる「順列ファイル」をサーバに送信する構成を採用することにより，相違点１，３に係る本願発明の構成を得ることに，当業者が格別の創作能力を要するものとは認められない。
そして，そのような構成とした場合には，電子デバイスにおいて「順列ファイル」等の作成が必要となり，当該電子デバイスの処理負担は増す一方で，サーバにおける「順列ファイル」や「スクランブルキーパッド画像」の作成は不要となるから，サーバの処理負担が軽減される作用を有することは，当業者が普通に想到し得る程度の事項に過ぎない。

イ　相違点２について
引用発明において，生成したＰＩＮの符号化バージョンを電子デバイスからサーバに送信するにあたり，電子デバイスに記憶させる工程を介在させることは，当業者が普通に採用する事項に過ぎない。

ウ　まとめ
上記のとおり，上記相違点１乃至３に係る構成は，いずれも，当業者であれば容易に想到し得るものであり，本願発明に関する作用，効果も，引用文献１及び２の記載に基づいて，当業者が予測できる範囲のものである。
したがって，本願発明は，引用文献１に記載された発明及び引用文献２に記載された技術事項に基づいて，当業者が容易に発明をすることができたものであるから，特許法２９条２項の規定により，特許を受けることができないものである。

２　請求人の主張について
請求人は，本願発明が進歩性を有するとして，（１）「引用文献１には，ローカルに生成される配列についての開示がないため，当業者は，引用文献１を出発点として，本願発明に到達することはできません。」，（２）「引用文献１は本願の請求項１に記載されている特徴について沈黙しているだけ

でなく，ユーザーのローカルデバイスからリモートで生成され，ユーザーのデバイスに送信されるスクランブルされた配列の使用を明確に教示しているので，実際には本発明の特徴からはかけ離れております。これは，本願の請求項１に記載されている特徴とは全く逆のものであり，実際には逆の方法で動作する装置を考案するためには，当業者は，引用文献１の教示から１８０度方向を変える必要があります。これは，当業者にはできないことです。」，（３）「本発明の方法は，引用文献１よりも技術的利点を提供します。・・・これは，サーバーが配列生成のための処理要件から解放されることを意味し，また，サーバーからデバイスに配列を送信する場合と比較して，必要な時間が少なくなることを意味しています。これにより，引用文献１と比較して，より効率的で，より迅速に動作する認証のソリューションが実現されます。」等と主張する（数字（１）～（３）は当審で付与した。以下同じ。）。

しかしながら，引用発明において，引用文献２の開示に基づいて，上記相違点１及び３に係る本願発明の構成を得ることが，当業者にとって容易であることは，上記アのとおりであるから，請求人の主張（１）～（３）は採用することができない。

また，請求人は，（４）「スクランブルされた配列をローカルに生成することは，遠隔のサーバーからユーザーのデバイスへの送信中にスクランブル配列が傍受されることないことを意味します。スクランブル配列が傍受されると，権限のない者がユーザーの入力とキーパッド／画像のレイアウトとの間のマッピングを知ったり，計算したりすることができ，ユーザーの秘密の入力を解読することができてしまいます。これは，引用文献１の潜在的な脆弱性でありますが，この脆弱性は，本願発明によって克服されます。」とも主張する。

しかしながら，本願発明は，「前記少なくとも１つのスクランブルキーパッド配列を前記遠隔のコンピューティング資源に送信して前記識別子の符号化されたバージョンを復号化することができるようにする」との構成Ｅを備えているから，「スクランブルされた配列をローカルに生成すること」により，「遠隔のサーバーからユーザーのデバイスへの送信中にスクランブル配列が傍受されること」はないものの，ローカルに生成した配列を，「ユーザーのデバイスから遠隔のコンピューティング資源への送信中にスクランブル配列が傍受されること」が，新たに起こり得るものであることは，当業者が普通に想起する事項であって，本願発明は，請求人のいう「引用文献１の潜在的な脆弱性」の克服と引き替えに，新たな脆弱性を潜在的に生じるものであるといえる。このことは，引用文献１においても，上記第４の１オのとおり，ユーザのデバイスにおいて，ランダムに配置したＰＩＮパッドを構成する形態について，「潜在的にセキュリティの抜け穴を提供し，またユーザのＰＩＮを入手するためのマルウェアに幾つかのアクセスポイントを与える恐

れがある（ハンドセット／デバイスがランダム番号，従ってＰＩＮパッドの順序をサーバに返送しなければならない。）。従って，このような実施形態は，所要のセキュリティレベルが幾分緩やかな用途に適している。」と記載されていることからも明らかであるといえる。そうすると，請求人の主張（４）に係る事項は，本願発明について，その進歩性を肯定し得るような，当業者の予測を超える顕著な作用効果であるということはできないから，請求人の主張（４）も採用することができない。

また，請求人は，引用文献２について，（５）「キーパッド画像に描かれたキーと下にある操作可能なキーパッドのキーとの間のマッピングを生成すること」，（６）「ユーザーの識別子の符号化されたバージョンを，下層の操作可能なキーパッドによって電子デバイスに入力することを可能にすること」，（７）「ユーザーのローカルな電子デバイス上でローカルに生成された少なくとも１つのスクランブルキーパッド配列を用いてキーパッド画像及び／又は操作可能なキーパッドを生成すること」の教示がないとして，引用文献１に欠けている機能を付与することはできないと主張する。

しかしながら，上記（５）乃至（７）の教示の有無にかかわらず，引用文献２には，上記第４の３ク，ケに記載したとおりの技術事項の開示が認められること，また，その開示に基づいて，引用発明において，上記相違点１及び３に係る本願発明の構成を得ることが，当業者にとって容易想到であることは，上記１アのとおりであり，引用文献２において，請求人の主張にかかる（５）乃至（７）についての教示がないことが，上記相違点１，３に係る構成を得ることについて，阻害要因を構成しているということもできない。したがって，引用文献２に関する上記の請求人の主張も採用することができない。

３　付記

本願発明の構成Ｂは，「前記キーパッド画像及び／又は操作可能なキーパッドは，前記電子デバイスにローカルに生成される少なくとも１つのスクランブルキーパッド配列を用いて生成され，」というものであり，上記で検討した「キーパッド画像」を「スクランブルキーパッド配列を用いて生成」する場合だけでなく，「キーパッド画像」に代えて，あるいは，「キーパッド画像」に加えて，「操作可能なキーパッド」を「スクランブルキーパッド配列を用いて生成」する構成を含むものである。そこで，「操作可能なキーパッド」を「スクランブルキーパッド配列を用いて生成」する構成についても一応検討する。

上記第４の１カ，クによれば，引用文献１には，「スクランブルキーパッド画像」に加えて，サーバから受信した「順列ファイル」を用いて電子デバイスにて「操作可能なキーパッド」を生成して使用することが記載されている。

ここで，引用文献１に記載の発明において，「スクランブルキーパッド画像」の生成に用いる「順列ファイル」を，電子デバイスにローカルに作成して，復号のためにサーバに送信することが，当業者にとって容易想到であることは，上記１アのとおりであり，また，上記第４の１オのとおり，引用文献１には，デバイスにてランダム番号を選択することも記載されているのであるから，電子デバイスにて「操作可能なキーパッド」を生成するための「順列ファイル」について，電子デバイスにローカルに作成し，復号のためにサーバに送信する構成とすることにも，当業者が困難を要するものとは認められない。

第７　むすび

以上のとおり，本願発明は，特許法２９条２項の規定により特許を受けることができないから，他の請求項に係る発明について検討するまでもなく，本願は拒絶されるべきものである。

よって，結論のとおり審決する。

令和　３年１１月１９日

審判長　　特許庁審判官　石井 茂和
特許庁審判官　篠原 功一
特許庁審判官　金子 秀彦

（行政事件訴訟法第４６条に基づく教示）

この審決に対する訴えは、この審決の謄本の送達があった日から３０日（附加期間がある場合は、その日数を附加します。）以内に、特許庁長官を被告として、提起することができます。

審判長　石井　茂和

出訴期間として在外者に対し９０日を附加する。

〔審決分類〕Ｐ１８　．１２１-Ｚ　（Ｇ０６Ｆ）

審判長	特許庁審判官	石井　茂和	8837
	特許庁審判官	金子　秀彦	3661
	特許庁審判官	篠原　功一	9176