平成３０年９月６日判決言渡

平成２９年（行ケ）第１０２１９号　審決取消請求事件（第１事件）

平成２９年（行ケ）第１０２２１号　審決取消請求事件（第２事件）

口頭弁論終結日　平成３０年６月２１日

判　　決

第１事件原告・第２事件被告（以下，単に「原告」という。）

株式会社シー・エス・イー

訴訟代理人弁護士　田　中　伸一郎

奥　村　直　樹

山　本　飛　翔

訴訟代理人弁理士　近　藤　直　樹

山　崎　貴　明

第１事件被告・第２事件原告（以下，単に「被告」という。）

パスロジ株式会社

訴訟代理人弁護士　笠　原　基　広

坂　生　雄　一

中　村　京　子

田久保　敦　子

訴訟代理人弁理士　塩　谷　英　明

主　　文

１　原告の第１事件に係る請求及び被告の第２事件に係る請求をいずれも棄却する。

２　訴訟費用は，第１事件及び第２事件を通じてこれを２分し，その１を原告の，その余を被告の各負担とする。

事　実　及　び　理　由

第１　請求

１　第１事件

特許庁が無効２０１５－８００２１８号事件について平成２９年１０月２５日にした審決のうち，「特許第４４５５６６６号の請求項８乃至９に係る発明についての審判請求は，成り立たない。」との部分を取り消す。

２　第２事件

特許庁が無効２０１５－８００２１８号事件について平成２９年１０月２５日にした審決のうち，「特許第４４５５６６６号の請求項１乃至７に係る発明についての特許を無効とする。」との部分を取り消す。

第２　事案の概要

１　特許庁における手続の経緯等

(1) 被告は，発明の名称を「ユーザ認証方法およびユーザ認証システム」とする特許第４４５５６６６号（請求項の数９。以下「本件特許」という。）の特許権者である。

本件特許に係る出願は，平成２０年４月１５日に出願した特願２００８－１０５６８６号の一部を分割して，平成２１年９月２４日に新たな特許出願をし，平成２２年２月１２日に設定登録を受けたものである。

また，特願２００８－１０５６８６号は，平成１５年２月１３日に国際出願（優先権主張：平成１４年２月１３日）した特願２００３－５６８５４６号の一部を分割して平成１７年１月３１日に新たな特許出願をした特願２００５－２３６２２号の一部を，更に分割して特許出願したものである。

(2) 原告は，平成２７年１１月２７日，本件特許につき特許無効審判を請求した（無効２０１５－８００２１８号事件）。

同事件の審理において，特許庁は，平成２９年４月１０日，審決の予告をし，被告は，同年６月１２日，別紙訂正請求の内容（訂正事項１ないし９）のとおり特許請求の範囲の訂正を請求した（以下「本件訂正」という。）。

原告は，同年９月４日，無効理由を追加すべく審判請求書の補正（以下「本件補正」という。）を行ったが，特許庁は，同年１０月５日，特許法１３１条の２第２項の規定に基づき，本件補正を許可しないとの決定をした（甲７０，７１）。

特許庁は，同年１０月２５日，「特許第４４５５６６６号の特許請求の範囲を訂正請求書に添付された訂正特許請求の範囲のとおり，訂正後の請求項〔１乃至７〕，〔８乃至９〕について訂正することを認める。」「特許第４４５５６６６号の請求項１乃至７に係る発明についての特許を無効とする。」「特許第４４５５６６６号の請求項８乃至９に係る発明についての審判請求は，成り立たない。」との審決をし，その謄本は，同年１１月６日，原告及び被告それぞれに送達された。

(3) 原告は，平成２９年１１月２９日，審決のうち，「特許第４４５５６６６号の請求項８乃至９に係る発明についての審判請求は，成り立たない。」との部分の取消しを求める第１事件訴訟を提起し，被告は，同年１２月６日，審決のうち，「特許第４４５５６６６号の請求項１乃至７に係る発明についての特許を無効とする。」との部分の取消しを求める第２事件訴訟を提起した。

２　特許請求の範囲の記載

本件訂正後の，本件特許の特許請求の範囲請求項１ないし９の記載は，次のとおりである（以下，「本件発明」と総称し，個別に特定するときは，請求項の番号に従って「本件発明１」ないし「本件発明９」という。また，本件発明に係る明細書〔甲８〕を「本件明細書」という。なお，請求項１及び８についての構成要件の分説は，審決によるものである。）。

「【請求項１】

Ａ　ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録方法であって，

Ｂ　複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを無線端末装置が表示し，これにより，前記提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促すステップと，

Ｃ　前記入力されたキャラクタに基づいて，前記入力されたキャラクタの数に等しい数の要素からなるパスワード導出パターンが２回で特定されるように，新たな提示用パターンを前記無線端末装置が表示する処理を繰り返し行い，これにより，前記新たな提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す処理を繰り返すステップと，

Ｄ　前記無線端末装置と通信回線を介して接続されたサーバが，前記入力されたキャラクタに基づいて特定されたパスワード導出パターンを登録するステップと，

を含むパスワード導出パターンの登録方法。

【請求項２】

前記サーバが登録するパスワード導出パターンは，

前記サーバが，前記無線端末装置から前記入力されたキャラクタを受け取り，受け取った前記入力されたキャラクタに基づいて特定したものである，

請求項１に記載のパスワード導出パターンの登録方法。

【請求項３】

前記所定のキャラクタは，０～９までの整数である，

請求項１に記載のパスワード導出パターンの登録方法。

【請求項４】

前記所定のパターンは，Ｋ行Ｌ列のマトリックスであり，

前記所定のキャラクタは，０～９までの整数であり，

前記提示用パターンは，前記Ｋ行Ｌ列のマトリックスの各要素に０～９までの整数を割り当てたものであり，

前記Ｋ行Ｌ列のマトリックスは，前記所定のキャラクタの数字列がＪ桁のとき，以下の数式：

１０＾Ｊ＜（Ｋ＊Ｌ）＊（Ｋ＊Ｌ－１）・・（Ｋ＊Ｌ－Ｊ＋１）

に従って，構成される，

請求項１に記載のパスワード導出パターンの登録方法。

【請求項５】

前記所定のパターンは，マトリックスであり，

前記所定のキャラクタは，０～９までの整数であり，

前記提示用パターンは，マトリックスの各要素に０～９までの整数からなる乱数を割り当てたものである，

請求項１に記載のパスワード導出パターンの登録方法。

【請求項６】

請求項１又は５に記載のパスワード導出パターンの登録方法により登録されたパスワード導出パターンを用いたユーザ認証方法であって，

認証用パターンを前記無線端末装置が表示し，これにより，前記認証用パターンについての特定の要素に割り当てられたキャラクタの入力を促すステップであって，

前記認証用パターンは前記提示用パターンと同一の要素から構成される前記所定のパターンの要素のそれぞれに，前記提示用パターンとは異なるキャラクタを割り当てたものであり，

前記サーバが，前記認証用パターンに関する情報と，前記認証用パターンに基づいて入力されたキャラクタとに基づいて，前記登録された特定されたパスワード導出パターンを有するユーザと，前記新たな提示用パターンに基づいて

キャラクタを入力したユーザとが一致しているか否か判断するステップと，を含む，

ユーザ認証方法。

【請求項７】

前記所定のパターンは，マトリックスであり，

前記所定のキャラクタは，０～９までの整数であり，

前記提示用パターンは，マトリックスの各要素に０～９までの整数を割り当てたものであり，

前記認証用パターンは，前記提示用パターンと同一のマトリックスであり，

前記認証用パターンに割り当てられた前記提示用パターンとは異なるキャラクタは，０～９までの整数であり，前記マトリックスの各要素における０～９までの整数の割り当てられ方が前記提示用パターンと異なるものである，

請求項６に記載のユーザ認証方法。

【請求項８】

Ｅ　端末装置と，前記端末装置と通信回線を介して接続されたサーバとを含む，ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録システムであって，

Ｆ　前記端末装置は，複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを表示し，これにより，前記提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促すための手段と，

Ｇ　前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，新たな提示用パターンを表示する処理を繰り返し，これにより，前記新たな提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す処理を繰り返す手段と，

Ｈ　前記パスワード導出パターンが特定されたとき，前記特定されたパスワー

ド導出パターンを含む登録確認画面を前記無線端末装置が表示して，これにより，前記パスワード導出パターンを登録するか又は前記表示及び入力を最初からやり直すかの選択を促す手段と，

を有し，

Ｉ　前記端末装置と通信回線を介して接続されたサーバは，

前記登録が選択されたとき，前記特定されたパスワード導出パターンを登録させるための手段を備える，

パスワード導出パターンの登録システム。

【請求項９】

前記所定のパターンは，Ｋ行Ｌ列のマトリックスであり，

前記所定のキャラクタは，０～９までの整数であり，

前記提示用パターンは，前記Ｋ行Ｌ列のマトリックスの各要素に０～９までの整数を割り当てたものであり，

前記Ｋ行Ｌ列のマトリックスは，前記所定のキャラクタの数字列がＪ桁のとき，以下の数式：

$$10^{J} < (K*L)*(K*L-1)\cdots(K*L-J+1)$$

に従って，構成される，

請求項８に記載のパスワード導出パターンの登録システム。」

３　審決の理由の要旨

(1) 審決の理由は，別紙審決書の写しに記載のとおりである。

要するに，原告が以下のとおり本件発明について無効理由を主張したのに対し，審決は，①本件発明１ないし７は，先願である甲１に記載された発明（甲１発明）と同一であるが，本件発明８及び９は，甲１発明と同一であるとはいえない，②甲１発明の発明者は，本件発明の発明者（Ｐ）のみではないことから，特許法２９条の２本文括弧書の例外規定（発明者が同一）は適用されない，③したがって，本件発明１ないし７についての特許は無効とす

べきであるが，本件発明８及び９についての特許は無効とすることができない，としたものである。

（原告主張の無効理由）

本件発明は，本件特許出願の日前に出願され，本件特許出願後に出願公開（甲１：特開２００２－３６６５１７号公報）がされた他の特許出願（特願２００１－１６８８７９号）（本件特許と発明者及び出願人が同一でない）の願書に最初に添付した明細書又は図面に記載された発明であるため特許法２９条の２の規定により特許を受けることができないものであり，その特許は同法１２３条１項２号に該当し，無効とすべきである。

(2) 審決が認定した甲１発明は，以下のとおりである。

「サービス提供システムにおける端末装置でユーザ認証を行うためのワンタイムパスワード発行の方法であって，

初期登録時点において，認証サーバは，ウエブサーバを介してアクセス元の端末装置に初期ワンタイムパスワード情報登録ＵＲＬを通知する電子メールを送信し，

前記端末装置は，前記初期ワンタイムパスワード情報登録ＵＲＬを用いて，前記認証サーバのウエブページの（Ａ，１）から（Ｄ，１２）までの座標が付与された縦４個×横１２個の数字からなるランダムパスワードを，４個の数字群と数字群の間に所定の記号を挿入して表示するとともに，『パスワード』と表示された箇所にユーザによって選択された複数の数字からなるランダムパスワードの入力を可能とし，

前記ユーザは，前記端末装置に表示されているランダムパスワードに基づき，登録したい位置のランダムパスワードを入力し，

前記端末装置は，前記認証サーバから送信される２回目のランダムパスワードを表示するとともに，前記ユーザによって選択される２回目のランダムパスワードの入力を可能とし，

前記ユーザは，前記端末装置に表示されている２回目のランダムパスワードに基づき，前記登録したい位置のランダムパスワードを入力し，

前記認証サーバは，前記端末装置からの２回の入力により，前記ユーザによって選択されたランダムパスワードの複数の位置情報を確定し，確定した前記位置情報をワンタイムパスワードとしてデータベースに登録し，

ユーザ認証を行う時点においては，前記端末装置は，縦４個×横１２個の数字からなるランダムパスワードに，４個の数字群と数字群の間に所定の記号を挿入して，初期登録時とランダムパスワードの配置が異なるように表示するとともに，『パスワード』と表示された箇所にユーザによって選択された複数の数字からなるランダムパスワードの入力を可能とし，

前記認証サーバは，ユーザによって入力されたランダムパスワードの複数の位置情報と初期登録時に登録された複数の位置情報とを照合して，同一位置であれば，ユーザ本人と判断する，方法。」

(3) 審決が認定した本件発明８と甲１発明の一致点及び相違点は，次のとおりである。

ア　一致点

「端末装置と，前記端末装置と通信回線を介して接続されたサーバとを含む，ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録システムであって，

前記端末装置は，複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを表示し，これにより，前記提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促すための手段と，

前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで,新たな提示用パターンを表示する処理を繰り返し,これにより,前記新たな提示用パターンについての特定の要素に割り当てられたキャラ

クタの入力を促す処理を繰り返す手段と，

を有し，

前記端末装置と通信回線を介して接続されたサーバは，

前記パスワード導出パターンが特定されると，前記特定されたパスワード導出パターンを登録させるための手段を備える，

パスワード導出パターンの登録システム。」

イ　相違点

本件発明８は，「前記パスワード導出パターンが特定されたとき，前記特定されたパスワード導出パターンを含む登録確認画面を前記無線端末装置が表示して，これにより，前記パスワード導出パターンを登録するか又は前記表示及び入力を最初からやり直すかの選択を促す手段」（H）を備え，「前記端末装置と通信回線を介して接続されたサーバは，前記登録が選択されたとき，前記特定されたパスワード導出パターンを登録させる」（Ｉ）のに対して，

甲１発明は，“サーバ”（認証サーバ）は，“特定されたパスワード導出パターンを登録させるための手段”を有するものの，当該特定された“パスワード導出パターン”（ユーザによって選択された複数の位置とその選択順序の情報）を含む登録確認画面を無線端末装置に表示して，前記パスワード導出パターンを登録するか又は前記表示及び入力を最初からやり直すかの選択を促す手段，および，前記登録が選択されたとき，前記特定されたパスワード導出パターンを登録させる手段を備えていない点。

４　取消事由

⑴ 第１事件

ア　発明の同一性の認定の誤り（取消事由１）

イ　特許法１３１条の２第２項の裁量権の逸脱・濫用の有無（取消事由２）

⑵ 第２事件

ア　甲１発明の認定の誤り（取消事由１）

イ　一致点及び相違点の認定の誤り（取消事由２）

ウ　発明の同一性の認定の誤り（取消事由３）

エ　発明者同一の認定の誤り（取消事由４）

第３　第１事件の取消事由に関する当事者の主張

１　取消事由１（発明の同一性の認定の誤り）について

（原告の主張）

(1) 訂正事項５及び６（以下，併せて「本件訂正事項」という。）に係る構成が甲１発明にはないとの認定は明らかに誤っており，本件訂正事項の構成を含む本件発明８及び９は，先願の甲１発明と同一で，これらの発明に係る特許は，特許法２９条の２に違反し，特許法１２３条１項２号により無効されるべきものである。

(2) すなわち，本件訂正事項は，単にサーバに登録すべきものとして特定した情報を登録前に表示して確認を求め,確認の後に登録するということであり，周知慣用のことにすぎない。

本件特許の出願前より，オンライン上での商品購入等における事前登録，注文内容の確認の各種手続において，登録すべき内容が画面に表示され，入力者に対して確認した上で，登録操作を行うこととされていた（甲７３ないし７８）。パスワード登録の技術分野においても，入力した内容をＰＣ等の画面に表示し，確認後登録確認ボタンで登録する構成は明らかに周知であった（甲１５の【００１４】，甲１６の図１６，甲１７の図１３，甲１８の図３６，甲１９の図３）。

甲１５ないし１７のパスワード登録に関して，審決は，「これは，入力したパスワードをそのまま表示し確認する技術にとどまり，本件発明８のような『パスワード導出パターン』（複数の位置）をユーザが確認できるように，複数の位置がどのような順序で選択されたかが分かるように表示することを

開示するものではない」（４８頁２７行ないし３０行）とするが，情報の内容が異なっても，表示方法が異なるものではなく，特定した情報をサーバに登録する前に表示して確認を求める以上，情報の内容，すなわちパスワード導出パターンの内容を分かるように表示することに何ら技術的な困難はないから，パスワード登録の技術分野において，入力した内容をＰＣ等の画面に表示し，確認後登録確認ボタンでサーバに登録する構成は周知であったのであり，本件訂正事項も周知慣用のものであるといえる。

また，ＮＴＴコミュニケーションズ株式会社（以下「ＮＴＴコム社」という。）による甲１発明の実施（甲２の添付資料６，甲７）においても，特定されたパスワード導出パターンを登録前に表示し，確認された後にサーバへの登録がなされ，特許出願自体（甲１）に明示的には記載しなかったにもかかわらず，実施において当然に本件訂正事項を用いている。

(3) 以上のとおり，本件訂正事項は，入力内容を登録する際に行われている周知慣用技術にすぎず，甲１に明示的記載はなくとも，甲１発明の実施において当業者であれば当然に行うことである。換言すれば，本件訂正事項は，本件発明１に対して何らの技術的意義を有するものではない。したがって，本件発明８及び９は甲１発明と実質的に同一であり，これらの発明についての特許には特許法２９条の２に違反した無効原因が存する。

（被告の主張）

(1) 甲１に本件訂正事項の開示も示唆もないこと

本件訂正事項は，「前記特定されたパスワード導出パターンを含む登録確認画面を前記無線端末装置が表示して，これにより，前記パスワード導出パターンを登録するか又は前記表示及び入力を最初からやり直すかの選択を促す手段」を含むものであり，「特定されたパスワード導出パターン」をユーザが確認できるように，複数の位置がどのような順序で選択されたかが分かるように表示することを意味する。当該技術は原告の提出する文献に開示も

示唆もなく，本件訂正事項は周知慣用ではない。

本件発明８及び９が前提とするパスワードは，単なる任意の文字や数字の組合せとは異なり，提示される複数の要素の中から，パスワード導出パターンに従って要素値を抜き出して決定されるものである。そして，本件発明８及び９のパスワード導出パターンの特定方法は，数字列等とは異なり１回の入力のみでは特定ができず，ユーザの意図するパスワード導出パターンの特定そのものに複数回の入力を要する。したがって，ユーザが自ら意図するパスワード導出パターンとして選択できたかどうかを確認するためには，「複数の位置がどのような順序で選択されたか」を，改めてユーザに分かるように確認画面を表示させなければならず，これは，ユーザが登録しようと入力したパスワードをそのまま表示するという周知技術とは，全く異なる技術的意義を有するものであって，新たな効果を奏させる技術的創作である。

以上のとおり，甲１発明には本件訂正事項について参酌すべき示唆すら開示されておらず，当然その効果も奏していないから，甲１発明と本件発明８及び９との相違は，単なる表現上のものとも，設計上の微差とも，奏される効果に差がないともいえない。したがって，両者は実質的に同一の範囲とされるものではない。

(2) 証拠によっても本件訂正事項が周知慣用技術とはいえないこと

仮に，登録すべき対象（甲１発明の場合，甲１発明のパスワード導出パターン）を含む登録確認画面を表示して，これによって登録すべきかやり直すかの選択をさせることが本件訂正事項の技術的意義であるとしても，本件発明８及び９においては，「複数の位置がどのような順序で選択されたか」に相当する画面を表示することが重要である。

これに対し，原告提出の各証拠を参酌しても，次のとおり，周知技術といえるのは，「情報セキュリティの技術分野において，パスワードの登録時に，ユーザが入力した文字，数字等の内容を端末装置の画面にそのまま表示し，

入力に誤りがないことを確認した上で登録確認ボタンで登録すること」にとどまり，甲１発明に上記周知技術を組み合わせても，本件発明８及び９との相違点は解消されないから，両発明は同一ではない。

ア　甲７３ないし７８について

甲７３ないし７８は，オンライン上での商品購入等における事前登録や注文内容の確認手続に関するものであり，「複数の位置がどのような順序で選択されたかが分かるように表示する登録確認画面」を開示するものではなく，情報セキュリティ分野におけるパスワード登録とは技術分野は異なるから，本件訂正事項が周知慣用技術であったことの証拠とはいえない。

イ　甲１５ないし１９について

甲１５に開示された技術は，ユーザの入力したパスワードについて確認を行うものではなく，ユーザに，コンピュータの提案するパスワードを入力するか否かを決定させるものである（【００１４】）。そして，決定されたパスワードを新パスワードとして仮登録入力し，さらに新パスワードをユーザに入力させて，これが一致したか否かを見る。これを数回繰り返して確認し，一致した場合は，このパスワードを本登録する（【００１６】）。要するに，甲１５に開示された技術は，ユーザに新パスワードを提示して本登録するか否かを決定させるものではなく，コンピュータが，仮登録したパスワードと，ユーザによって入力されるパスワードが一致するか否かを見て，仮パスワードを本登録するというものであるから，ユーザがパスワードの内容を確認して登録するかやり直すかの判断を行う手段を有する本件訂正事項の確認画面とは技術的意義が異なる。

甲１６ないし１８は，いずれも，確認画面ではなく，パスワード設定画面におけるパスワードの表示及び確認，取消ボタンの表示であり，ユーザがパスワード登録のために入力したパスワードをそのまま表示し確認する技術にとどまる。さらにいえば，これらの明細書の各記載および各図には，

設定画面においてユーザが入力したパスワードをそのまま表示していることまでの開示は無い。甲１７は，他人に見られないようにするため，パスワードの入力画面においてパスワードがアスタリスクで表示されている(【００７０】及び図１４）。甲１８では，設定画面においてパスワードを２回入力することを要求している（図３６）。パスワードがそのまま表示されているのであれば，パスワードを目視で確認することができるため，２回入力する必要性が乏しい。したがって，これらの発明では，設定画面においても，他人に見られないようにするため，入力したパスワードをそのまま表示するのではなく，アスタリスク等で伏せ字にして，入力文字数のみが分かるように表示されている可能性がある。その場合，これらの設定画面はユーザにパスワードを含む確認画面を表示したものとはいえない。

甲１９には，パスワード登録画面に限り，作成したパスワードの確認が可能な確認画面を設けてもよいとの記載がある（【００７７】）。しかし，甲１９の【００７７】にも図３にも，前記確認画面を表示して，パスワード登録又は入力のやり直しを選択させる手段の開示はないから，甲１９のみをもって，本件訂正事項が当業者にとって周知慣用技術であったということはできない。

ウ　甲２の添付資料６及び甲７

甲２の添付資料６及び甲７は,いずれも同一のサービス提供システム(ＭＣＯＰ）の技術について開示するものであり，これらの記載をもって本件訂正事項が甲１の出願時における技術常識であったということはできない。また,パスワード登録の確認画面について何らの示唆もない甲１発明から，甲１の出願後に発行された文献である甲２の添付資料６及び甲７を参酌して，甲１発明に本件訂正事項が記載されているに等しいと判断することはできない。

(3) 以上のとおり，本件訂正事項は，原告が主張する周知慣用技術とは技術的

意義が全く異なるものであり，甲１の出願当時における周知技術はない。したがって，本件発明８及び９に無効原因がないとした審決の認定に誤りはなく，取消事由１は理由がない。

２　取消事由２（特許法１３１条の２第２項の裁量権の逸脱・濫用の有無）について

（原告の主張）

本件審判においては，被告が甲１発明と訂正前の本件発明８が同一であることを認めた上で，これらはいずれも被告の代表者であるＰの単独発明であると主張したのに対して，審決（予告審決も同様）は，被告の代表者であるＰの単独発明ではないと認定しており，本件特許は共同出願違反（特許法３８条違反）であることを明確にしているところ，同違反は本件訂正事項が構成に付加されたとしても，Ｐが単独で想到したものではない構成への付加であり，同条違反は何ら変わるものではない。

したがって，万が一特許法２９条の２違反が認められないのであれば，少なくとも特許法３８条違反の無効理由については審判請求書の補正（本件補正）を認めて審理をし，本件発明８及び９の特許について無効審決をすべきであった。

それにもかかわらず，審判長が本件補正を認めなかったことには，特許法１３１条の２第２項において認められた裁量権を逸脱・濫用した違法があり，かかる違法は審決の結論に影響を及ぼすものである。

（被告の主張）

特許法１３１条の２第１項本文，同第２項及び同第４項の規定によれば，審判長の補正の許可又は不許可の決定に対しては不服を申し立てることができないとしたのであるから，請求の理由の要旨変更にわたる審判請求書の補正の許可又は不許可の決定に対する不服は，審決取消訴訟における審決取消事由とはなり得ない。また，特許無効審判請求において当該補正に係る請求の理由を審

理しなかったことも，審決取消事由とはなり得ないものと解すべきである。

特許法１３１条の２第２項は，例外的に補正を許可することができる要件を規定する。本件においては，本件補正に対する被告の同意はないため，①当該補正が審理を不当に遅延させるおそれがないことが明らかなものであること，②当該特許無効審判において第１３４条の２第１項の訂正の請求があり，その訂正の請求により請求の理由を補正する必要が生じたこと，の２点を満たす必要があるが，本件補正はいずれの要件も充足しない。

したがって，補正の不許可に対する不服は取消事由とはならず，また，本件補正は，特許法１３１条の２第２項が規定する許可要件を充足しないから，不許可決定に関し何らの違法もない。よって，取消事由２は理由がない。

第４　第２事件の取消事由に関する当事者の主張

１　取消事由１（甲１発明の認定の誤り）について

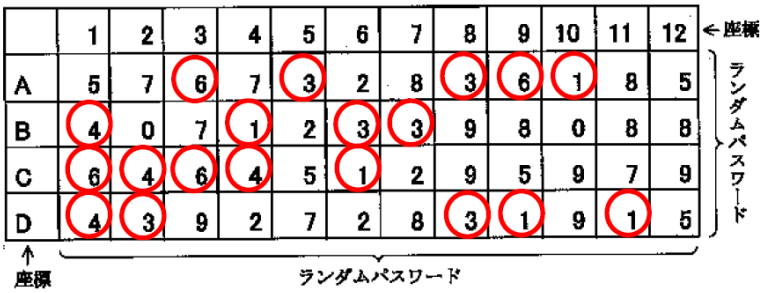
（被告の主張）

(1) 審決は，甲１発明について，認証サーバは，端末装置からの２回の入力により，ユーザによって選択されたランダムパスワードの複数の位置情報を確定し，確定した前記位置情報をワンタイムパスワードとしてデータベースに登録するものと認定しているが，次のとおり，甲１発明は，端末装置からの２回の入力によっては，ユーザによって選択された４個のランダムパスワードの位置情報を確定することはできず，その認定は誤っている。

(2) 甲１の【００１９】の第２文及び【００２０】の第１文に従って，図４（ａ）に示される縦４個×横１２個のランダムパスワードに対し，入力されたランダムパスワード「６」，「３」，「４」，「１」によりその座標を特定すると，次の１９個のランダムパスワードが特定される。

【図４】

（ａ）

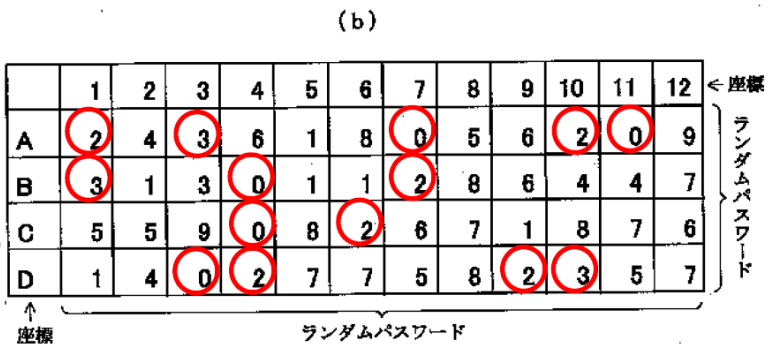



甲１発明において，端末装置１から入力される情報は，飽くまでも単なる数字列であって座標情報ではないから，１回目の入力で必ずしも４つの座標が特定されるわけではない。このため，甲１発明は，異なるパターンを表示してさらなる入力を要求する。

すなわち，【００２０】の第２文以降に従って，図４（ｂ）に示される縦４個×横１２個のランダムパスワードに対し，入力されたランダムパスワード「３」，「２」，「０」，「２」によりその座標を特定すると，次の１４個のランダムパスワードが特定される。

【図４】

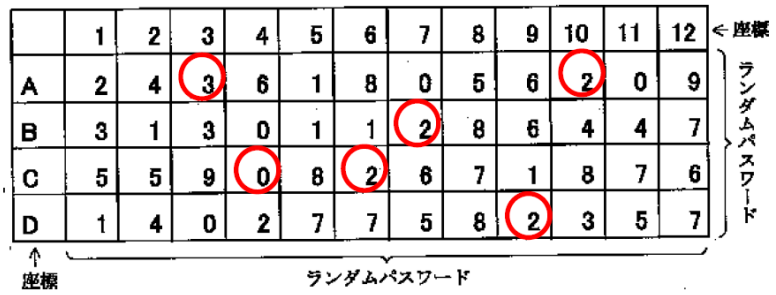
（ｂ）




以上より，１番目のランダムパスワードの組合せが「６」と「３」，２番目のランダムパスワードの組合せが「３」と「２」，３番目のランダムパスワードの組合せが「４」と「０」，及び４番目のランダムパスワードの組合せが「１」と「２」であるランダムパスワードは，次の６個となる。

【参考図】

（b）




| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | 2 | 4 | 3 | 6 | 1 | 8 | 0 | 5 | 6 | 2 | 0 | 9 |
| B | 3 | 1 | 3 | 0 | 1 | 1 | 2 | 8 | 6 | 4 | 4 | 7 |
| C | 5 | 5 | 9 | 0 | 8 | 2 | 6 | 7 | 1 | 8 | 7 | 6 |
| D | 1 | 4 | 0 | 2 | 7 | 7 | 5 | 8 | 2 | 3 | 5 | 7 |

つまり，甲１の記載によれば，位置登録したい座標を４つ選択する場合に，図４（ａ）及び（ｂ）という２パターンの縦４個×横１２個のランダムパスワードを用いて，当該位置登録したい４つの座標のそれぞれに配置されているランダムパスワード（数字）の入力を２回繰り返すことにより，６個のランダムパスワードの位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ａ，１０），（Ｃ，６），（Ｄ，９）が確定するのであって，位置登録したい座標の数に等しい４個のランダムパスワードの位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）がこの順番で確定するわけではない。

しかるに，審決は，甲１の【００１９】の「認証サーバ４２は，２回の入力により，ユーザによって選択されたランダムパスワードの位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）を確定し，確定した位置情報を前記ユーザ情報としてデータベース４５に登録する。」との記載に殊更着目し，４個の座標及びその順番が必ず確定するとの先入観ありきで，甲１発明を認定している。

しかしながら，甲１の【００１９】及び【００２０】の記載は，図４に記載された縦４個×横１２個のランダムパスワードに基づいて，位置登録したい座標のランダムパスワードに割り当てられた数字を入力する手順を説明するものであり，当該明細書の記載と図４の記載とを一体として解釈しなければ，甲１発明の特徴的部分であるランダムパスワードの位置特定方法を正し

く理解することはできない。そうすると，図４の記載に基づいて，甲１の【００１９】及び【００２０】の記載を客観的に読めば，甲１発明は，位置登録したい４つの座標のそれぞれに配置されているランダムパスワード（数字）の２回の入力により，６個のランダムパスワードの位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ａ，１０），（Ｃ，６），（Ｄ，９）が確定し，少なくとも，（Ａ，１０），（Ｃ，６），（Ｄ，９）については，その順番が確定しないものであると認定されるべきである。

以上のとおり，図４の記載は，甲１発明の特徴的部分を理解する上で欠かすことができないものであるにもかかわらず，審決は，その記載を全く考慮することなく，甲１発明を認定しており，その結果，一致点及び相違点の判断を誤り，本件発明１と甲１発明との同一性の判断を誤った。

(3) 仮に，審決が認定するとおり，図４の記載を前提に，２回の入力によって特定される位置情報が複数存在し得る結果になるとしても，４つの位置情報と順番とが特定されると理解できるということであるなら，図４の記載によれば，４番目のランダムパスワードの組合せが（１，２）である座標が３つあることから，甲１発明は，入力されたランダムパスワードに加え，別の何らかの構成が介在して最終的に４個のランダムパスワードの座標を特定しているものと認定されるべきである。

しかしながら，審決は，そのような別の何らかの構成が介在しているかどうかにつき，認定ないし判断を示しておらず，手続違背がある。

(4) 以上のとおり，審決が甲１発明の認定を誤り，この誤りが審決の結論に影響を与えることは明らかであるから，審決は取り消されるべきである。

(原告の主張)

(1) 被告の主張は，甲１の図４におけるささいな誤記を指摘しているだけであり，審決の甲１発明に関する認定には誤りはない。

１００個以下の升目は，各升目に００から９９までの２桁の数を振ること

ができ，それによって特定できることは常識であり，２桁の数字を入力すればどの升目かが示される。

そうであるところ，甲１の【００１８】ないし【００２０】においては，認証サーバから縦４個×横１２個の升目に０から９までの数字が配置されたランダムパスワードが２回送られ，送付されたそれぞれに対して合計２回，端末装置においてユーザが選択した位置に示された数字を選択した順序で入力することによって，ユーザにより選択されたランダムパスワード，すなわち升目の位置と順序が確定され，認証サーバへの登録を経てワンタイムパスワードの発行に係る升目の位置と順序（本件特許の各請求項の発明における「パスワード導出パターン」）の初期登録が行われる旨が記載されている。

ところで，甲１の図４（ａ）及び（ｂ）に，甲１の【００１９】及び【００２０】に記載のとおり数字を入力すると，１回目で「１」，２回目に「２」で示される４番目の位置が（D，９）だけでなく，被告が指摘するように（A，１０）及び（C，６）をも示すことになるが，甲１の記載内容からすれば，（ａ）又は（ｂ）の（A，１０）及び（C，６）の位置に示された数字に誤記があったことは明らかである。

(2) 以上のとおり，審決が認定するとおり（３３頁下から７行目以下），甲１において本件発明のパスワード導出パターンが開示されていることが否定されない。

(3) また，被告は，２回で特定されるとの構成を限定する訂正事項１について，本件明細書には，抽象的に記載されているだけであり，具体的な絞り込み方法については記載されていないにもかかわらず，本件特許の請求項１について訂正事項１の訂正を行っているのであり，甲１の図４の誤記の存在を指摘し，甲１発明が訂正事項１の構成を有しないとの主張にはそもそも理由がない。

(4) よって，審決の甲１発明に関する認定には誤りはなく，被告の主張する取

消事由１は理由がない。

２　取消事由２（一致点及び相違点の認定の誤り）について

（被告の主張）

(1) 審決は，甲１発明の認定を誤ったことに起因して，次のとおり，本件発明と甲１発明との一致点及び相違点の認定を誤り，その結果，本件発明１と甲１発明との同一性の判断を誤った。

(2) 対比判断

ア　本件発明１について

審決が，「前記入力されたキャラクタの数に等しい数の要素からなるパスワード導出パターンが２回で特定されるように」と認定したのは，誤りである。

すなわち，審決は，甲１の【００１９】の記載から４個の座標が必ず確定するとし，甲１発明につき，２回の入力によって複数の位置情報が確定すると認定しているが，甲１の図４の記載に基づいて，【００１９】及び【００２０】の記載を読めば，正しくは，２回の入力によって６個の位置情報が確定すると認定されなければならない。

そうしてみれば，甲１発明においては，２回の入力によっては，入力されたキャラクタの数とは異なる数の要素が特定されるにすぎないのであるから，次の点が，本件発明１と甲１発明との相違点として認定されるべきである。

「本件発明１は，入力されたキャラクタに基づいて，前記入力されたキャラクタの数に等しい数の要素からなるパスワード導出パターンが２回で特定されるように新たな提示用パターンを前記無線端末装置が表示する処理を繰り返し行うのに対して，甲１発明は，新たな提示用パターンを前記無線端末装置が表示する処理を繰り返し行うものの，２回の繰り返しでは，入力されたキャラクタに基づいて，入力されたキャラクタの数とは異なる

数の要素を特定する点。」

イ　本件発明２，３及び５ないし７について

請求項２，３及び５ないし７は，請求項１を直接又は間接に引用する請求項であり，したがって，本件発明２，３及び５ないし７は，本件発明１の構成要件の全てを含むものであるから，前記アと同様に，本件発明２，３及び５ないし７と甲１発明との一致点及び相違点の認定に誤りがあることは明らかである。

ウ　本件発明４について

請求項４は，請求項１を直接に引用する請求項であり，したがって，本件発明４は，本件発明１の構成要件の全てを含むものであるから，前記アと同様に，本件発明４と甲１発明との一致点及び相違点の認定に誤りがあることは明らかである。

加えて，本件発明４については，次に述べる点においても，本件発明４と甲１発明との一致点及び相違点の認定に誤りがある。

すなわち，審決は，「マトリックスの全要素の数（Ｋ＊Ｌ）が，入力されるＪ桁のキャラクタの数字列における各キャラクタがとり得る種類（整数０～９までの１０種類）より大きいことを特定するに過ぎ」ないと説示しているが，例えば，Ｋ＝３，Ｌ＝４，Ｊ＝５とした場合，実際に各数値を本件発明４の数式（以下「当該数式」という。）に当てはめてみると，

左辺：１０＾５＝１００００

右辺：１２×１１×１０×９×８＝９５０４０

であるから，左辺の方が右辺よりも大きくなり，当該数式を満たさない。この場合において，マトリックスの全要素数１２は，５桁の数字のそれぞれがとり得る整数０～９までの個数１０より大きいのであるから，当該数式が「マトリックスの全要素の数（Ｋ＊Ｌ）が，入力されるＪ桁のキャラクタの数字列における各キャラクタがとり得る種類（整数０～９までの１

０種類）より大きいことを特定するに過ぎ」ないものであると意義付けすることはできないのである。審決は，当該数式におけるＫ，Ｌ，及びＪの間の関係を捨象しており，その結果，その意義の理解を誤っている。

これに対して，本件発明４は，当該数式により，パスワード導出パターンの組合せの数が従来型のパスワードにおけるＪ桁の数字の組合せの数（１０のＪ乗）よりも大きくなるように，全体パターンであるマトリックスの大きさ（Ｋ行Ｌ列）を規定するものである。ここで，パスワード導出パターンの組合せの数とは，ユーザが提示用パターンに対して特定の要素に割り当てられたキャラクタを入力するごとに，当該提示用パターンから選択し得る要素の数を一つずつ減じた上，それらの数を掛け合わせた数を意味する。本件発明の発明者であるＰは，その経験に照らして，ユーザが提示用パターンに対して要素を順次に選択するという状況下においては，同じ位置の要素を選択しないという傾向が見られることに着目し，選択した要素と重複する要素を選択しない組合せの数（順列の総数）を当該数式において規定したのである。

また，審決は，「安全性の高い認証のために，『提示用パターン』の要素の総数を，入力されるキャラクタの数字列の順列の総数より大きくすることは自明であ」ると認定しているが，これも誤りである。

すなわち，甲１の記載を客観的にみれば，認証における安全性のレベルを従来型のパスワード認証と比較してどのように設定するかという命題を，入力されるパスワードの桁数Ｊとマトリックスの構成（Ｋ行Ｌ列）との関係で規定することまで自明であるとはいえない。

本件発明４は，従来型のパスワードよりも安全性が低いか否かを基準として，従来型のものより安全性の低くなるマトリックスを少なくとも排除する条件として，パスワード導出パターンの組合せの数が従来型のパスワードにおけるＪ桁の数字の組合せの数（１０のＪ乗）よりも大きくなるよ

うに，全体パターンであるマトリックスの大きさ（K行L列）を規定するものである。審決は，何らの具体的な証拠を示さずにこれが自明であると判断しており，手続違背がある。

さらに，審決は，「甲１発明における『縦４個×横１２個の数字からなるランダムパスワード』は，Ｋ＝４，Ｌ＝１２，Ｊ＝４である場合の前記『数式』の条件を満たす『K行L列のマトリックス』とみることができる」と認定しているが，この認定も誤りである。

すなわち，甲１のどこにも，パスワード導出パターンの利用に際してユーザは同じ位置の要素を選択しないという傾向が見られることに鑑みて，従来型のパスワードの数字の組合せの総数とマトリックスの大きさに基づく順列の総数との関係を規定している記載は見当たらない。

甲１発明は，縦４個×横１２個のランダムパスワードの中から例えば４つを選択すること以上のことを開示しておらず，Ｋ＝４，Ｌ＝１２，Ｊ＝４との関係においてユーザは同じ位置の要素を選択しないことを前提にしたランダムパスワードが構成されていることを開示していない。

以上のとおりであるから，審決の，「甲１発明の『縦４個×横１２個の数字からなるランダムパスワード』と本件発明４の『提示用パターン』とに実質的な違いはない。」との認定は誤りである。

(3) 以上のとおり，審決が本件発明１ないし７と甲１発明との一致点及び相違点の認定を誤り，この誤りが審決の結論に影響を及ぼすことが明らかであるから，審決は取り消されるべきである。

(原告の主張)

(1) 前記のとおり，甲１の【００１８】ないし【００２０】には，前記入力されたキャラクタの数である４つの要素からなるパスワード導出パターンが２回で特定されることが記載されており，甲１発明は，本件発明１ないし７の「前記入力されたキャラクタの数に等しい数の要素からなるパスワード導出

パターンが２回で特定されるように」という構成を有しているから，審決の一致点の認定に誤りはない。

(2) 本件発明４について

ア　マトリックスがＫ行Ｌ列の格子で，入力するパスワードの数字の桁数がＪ桁のとき，本件発明においてはパスワードが格子の位置と場所とその順序で特定されるところ，その選択可能数は当然に（Ｋ＊Ｌ）＊（Ｋ＊Ｌ－１）・・（Ｋ＊Ｌ－Ｊ＋１）になる。当該数式は，その選択可能性が１０のＪ乗より大きいと限定しようとするものであるが，升目の数（Ｋ＊Ｌ）が１０をある程度超えれば当然にこの限定を充足し，技術的に特に意義あるものではない。更に指摘すれば，甲２１等においても升目の数（Ｋ＊Ｌ）が１０を大きく超えており，このような構成は，出願前に公知のことである。

イ　また，いずれにしても，甲１には本件発明４の構成が開示されている。

すなわち，甲１の【００１９】には，「端末装置１のユーザは，初期ワンタイムパスワード情報登録ＵＲＬにおいて，認証サーバ４２からウエブサーバ４３を介して送られた図３のようなウエブページを見て，縦４個×横１２個のランダムパスワードの中から例えば４つを選択し，選択したパスワードを図３の「パスワード」と表示された箇所に入力する。縦４個×横１２個の各ランダムパスワードには，図４（ａ）に示すように，（Ａ，１）から（Ｄ，１２）までの座標が付与されている。」と記載されており，縦４個×横１２個のランダムパスワードの中から，升が重複しないように４つ選択する構成が開示されている。

したがって，パスワードの選択可能数は，重複しないように，第１の要素選択時に（４＊１２）個，第２の要素選択時に（４＊１２－１）個，第３の要素選択時に（４＊１２－２）個，第４の要素選択時に（４＊１２－３）個である。甲１の縦４個，横１２個及び重複しない要素４つは，それ

ぞれ，本件発明４のマトリックスのＫ行，Ｌ列及びキャラクタの数字列のＪ桁に対応するから，Ｊ＝４，Ｋ＝４，Ｌ＝１２として，当該数式に値を代入すると，１０＾４＜（４＊１２）＊（４＊１２－１）＊（４＊１２－２）＊（４＊１２－４＋１）が得られる。実際に計算すると，１００００＜（４８）＊（４７）＊（４６）＊（４５）＝４６６９９２０である。

ウ　以上のとおり，甲１は，当該数式を明確に充足しており，甲１発明と本件発明４の間に相違点は存在しない。

(3) よって，審決が行った，本件発明１ないし７と甲１発明の一致点及び相違点の認定に誤りはなく，原告が主張する取消事由２は理由がない。

３　取消事由３（発明の同一性の認定の誤り）について

（被告の主張）

前記のとおり，審決は，甲１発明の認定並びに本件発明１ないし７と甲１発明の一致点及び相違点の認定を誤り，その結果，本件発明１と甲１発明の同一性の判断を誤った。この誤りは，審決の結論に影響を与えることは明らかであるから，審決は取り消されるべきである。

（原告の主張）

前記のとおり，甲１発明の認定並びに本件発明１ないし７と甲１発明の一致点及び相違点の認定には誤りは存在せず，その結果，本件発明１と甲１発明の同一性の判断にも誤りは存在しないことから，被告の主張する取消事由３は理由がない。

４　取消事由４（発明者同一の認定の誤り）について

（被告の主張）

(1) 仮に，甲１発明が，２回の入力でランダムパスワードの位置が一意に確定するものであるとされるなら，以下に述べるとおり，甲１発明の特徴的部分と本件発明の特徴的部分の発明者は同一である。そうすると，審決は，甲１発明の特徴的部分がＰのみによりなされたことの認定につき誤った判断をし

た違法があるから，取り消されるべきである。

とりわけ，審決は，発明者同一の判断の前提となる甲１発明について，その特徴的部分への関与がＰのみであったかどうかを判断するのではなく，数字群と数字群との間に記号等を入れるアイデアを含む発明にまで不当に拡張し，それへの関与がＰのみであったかどうかを判断しているのであるから，この判断が審決の結論に影響を与えることは明らかである。

また，審決は，甲１発明の特徴的部分に対する方式Ｃの特徴的部分が株式会社セキュアプロバイダ（商号変更前の被告を指す。以下「セキュア社」という。）からＮＴＴコム社に提供された事実が認められないと判断しているのであるから，この判断が，審決の結論に影響を与えることは明らかである。

(2) 発明者の認定について

本件発明はいわゆるソフトウェアの技術分野に属するところ，このような分野においては，課題とその解決手段ないし方法が具体的に認識され，技術に関する思想として概念化されたものが着想として把握されることも少なくなく，また，新しい着想を具体化することが，当業者にとってみれば自明のことである場合は，着想者のみが発明者と認められ，これを単に具体化した者は発明者たり得ないというべきである。

この点，甲１の発明者欄にはＱと記載されているが，甲１の【発明の実施の形態】に記載された甲１発明の特徴的部分を当業者が実施できる程度にまで具体的・客観的なものとして構成する創作活動を行ったのは本件発明の発明者であるＰのみであり，Ｐ以外の者はこれに全く関与していない。したがって，後記するように，甲１発明の特徴的部分の発明者はＰのみである。

(3) 発明者が同一であることについての立証責任の負担及びその程度について

特許法２９条の２は，その適用除外について，出願人同一の場合はただし書に規定しているのに対し，発明者同一の場合は本文括弧書に規定している。このような条文の構造からは，特許法２９条の２本文の適用を主張する者が，

先願の発明者が誰であるかを主張立証することにより，後願の発明者がこれと同一でないことの主張立証責任を負うべきである。

また，特許法２９条の２が，発明者が同一の場合を適用除外としている趣旨は，発明者が自己の発明によって拒絶されないようにすることに加え，冒認出願により排除されることとなる真の発明者の後願を救済するためである。したがって，特許法２９条の２本文括弧書における発明の発明者についても，冒認出願に関する事案において，特許権者が当該特許に係る発明の発明者自身又は発明者から特許を受ける権利を承継した者によりされたことについての主張立証責任を負担するものと解されるのと同様に，特許法２９条の２本文の適用を主張する側が，先願の公報に記載された発明の発明者が誰によってなされたものであるかについて主張立証し，先願と後願の発明者が同一でないことの主張立証責任を負担すべきである。

また，仮に，先願と後願の発明者が同一であることの主張立証責任を後願の特許権者等が負担するとしても，後願の特許発明の発明者が先願の発明者であることの主張立証を具体的に行い，かつそれを裏付ける証拠を提出した場合には，特許法２９条の２本文の適用を主張する者において，他に共同発明者が存在することを疑わせる具体的な事情を主張し，かつその裏付けとなる証拠を提出して立証できなければ，後願の特許権者等における発明者同一の主張立証責任が尽くされたものと判断されるべきである。

本件事案においては，発明者同一性の判断の前提として，甲１発明の特徴的部分への関与者がＰのみであるかどうかが判断されなければならず，その判断において，特許法２９条の２本文の適用を主張する者に対して，先願の発明に関し，Ｐ以外に発明者がいることの立証責任を負担させるべきである。

(4) 本件発明の特徴的部分

本件明細書の記載によれば，本件発明の技術的課題は，携帯電話機のようにユーザインターフェースが十分でない場合であっても，極めて簡単に，パ

スワード導出パターンを登録できるようにすることにあり，したがって，従来技術に見られない，本件発明特有の課題解決手段を基礎付ける部分，すなわち，本件発明の特徴的部分は，パスワード導出パターンが特定されるまで，新たな提示用パターンを無線端末装置が表示する処理を繰り返し行い，これにより，新たな提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す処理を繰り返すことにある。

(5) 甲１発明の特徴的部分

発明者とは，発明の特徴的部分を当業者が実施できる程度にまで具体的・客観的なものとして構成する創作活動に関与した者をいうのであるから，甲１発明の発明者を認定するに当たっては，甲１発明の特徴的部分が何であるのかを明らかにする必要がある。ここで，発明の特徴的部分とは，特許請求の範囲に記載された発明の構成のうち，従来技術には見られない部分，すなわち，当該発明特有の課題解決手段を基礎付ける部分を指すものと解される。しかしながら，特許法２９条の２にいう，先願の特許公報の明細書記載の発明（先願発明）は，上記「特許請求の範囲に記載された発明」ではない。したがって，先願発明の特徴的部分の認定に当たっては，先願発明の構成のうち，後願の特許出願に係る発明（後願発明）と同一とされる構成の範囲に限定して，先願発明の特徴的部分を認定すべきである。

本件においては，甲１の記載及び本件発明の特許請求の範囲に照らせば，甲１発明の特徴的部分は，次のとおり認定されるべきである。

「位置情報が確定されるまで，縦４個×横１２個の新たなランダムパスワードを端末装置１が表示する処理を繰り返し行い，これにより，縦４個×横１２個の新たなランダムパスワードについての特定の座標位置に配置されているパスワード（すなわち数字）の入力を促す処理を繰り返す。」

しかるに，審決は，発明者同一の判断に当たって，甲１発明の特徴的部分が何であるのかを何ら判断しないまま，むしろ不当に拡張した発明を認定し

ており，手続違背がある。そして，甲１発明は，後述するとおり，甲２２の方式Ｃに基づいてなされた発明であるから，甲１発明の特徴的部分と方式Ｃの特徴的部分とは当然に一致する。

(6) 甲１発明の特徴的部分の発明者はＰのみであること

ア　方式Ｃの特徴的部分

方式Ｃの技術的課題は，携帯電話端末のみを利用して，ユーザによるワンタイムパスワードの設定を操作性良くできるようにすることにある（甲２２）。そうすると，方式Ｃの特徴的部分は，入力位置がユーザの意図するものに推察できるまで，ＯＦＦＩＣ画面を携帯電話が表示する処理を繰り返し行い，これにより，ＯＦＦＩＣ画面についての抜き出し位置の数字の入力を促す処理を繰り返すことにある。

方式Ｃの特徴的部分と甲１発明の特徴的部分を対比すると，方式Ｃの特徴的部分でいう「入力位置が意図するものに推察できるまで」は，甲１発明の特徴的部分でいう「位置情報が確定されるまで」に相当し，方式Ｃの特徴的部分でいう「ＯＦＦＩＣ画面」及び「携帯電話」は，甲１発明の特徴的部分でいう「縦４個×横１２個の新たなランダムパスワード」及び「端末装置１」にそれぞれ相当し，方式Ｃの特徴的部分でいう「抜き出し位置の数字」は，甲１発明の特徴的部分でいう「特定の座標位置に配置されているパスワード（すなわち数字）」に相当するから，方式Ｃの特徴的部分と甲１発明部分の特徴的部分とは同一であることが明らかである。

イ　方式Ｃの特徴的部分への関与はＰのみであること

Ｐは，開発初期のＯＦＦＩＣについて，当時のＯＦＦＩＣ方式が有していた，「マトリクス表が表示されている画面に，パスワードとなる数字を直接入力するのみの方式では，『マトリクス表』と『入力パスワード』の組合せを２，３回程度把握できれば，抜き出し位置が把握できてしまうおそれがある」という弱点についての改良技術を構想していた。そして，当

該弱点を克服する改良技術を開発するとともに，パスワード登録に当たって，当該弱点を逆に利用し，ユーザ側に提示用パターンから数字列を選択して入力させ，入力された数字列からサーバ側で抜き出し位置を特定するという，パスワードの登録方法を着想した（甲２７）。Ｐは，かかる着想を，以下のとおり，ＮＴＴコム社の開発プロジェクトでの要請を機に，当業者が実施できる程度に具体的・客観的なものとして甲２２にまとめあげた。

すなわち，審決が認定しているとおり，ＮＴＴコム社の開発プロジェクトへのセキュア社の参加が決まり，ｉモード携帯電話に対応した「ＯＦＦＩＣ」を開発することとなり，最初のミーティングを経て（甲３０），セキュア社がＯＦＦＩＣを用いたユーザのパスワード認証技術を，ベーステクノロジー株式会社（以下「ベース社」という。）がｉモードとＯＦＦＩＣとの連携技術を担当する分担の取り決めがなされた（甲２０）。その後，Ｐは，ＮＴＴコム社の要請により，携帯電話におけるサービスであるｉモードの特性に鑑みたＯＦＦＩＣのパスワード登録方法についての開発に着手した。

Ｐは，パスワード導出パターンの登録方法について，それまでに発案していたもの，あるいは構想していた複数のパスワード登録方法をｉモードに適するように具現化して，平成１２年１２月，方式Ｃを含む「ｉモードでのＯＦＦＩＣ利用開始手順案」（甲２２）にまとめた。

上記手順案（甲２２）は，セキュア社の担当者から，ＮＴＴコム社の担当者に対し，電子メールにて送信されたものであるところ，これは，甲２３の電子メールが言及する「ｉモードでのＯＦＦＩＣ利用開始手順案」そのものであり，遅くとも平成１２年１２月２６日には，ＮＴＴコム社内で回覧中であった。

以上のとおりであるから，ＮＴＴコム社は，Ｐから甲２２の方式Ｃを知

得したのであって，ＮＴＴコム社において方式Ｃが発案されたわけではない。

ウ　Ｐ以外の者の方式Ｃの特徴的部分への関与がないこと

(ｱ) ＮＴＴコム社の担当者が関与していないこと

ＮＴＴコム社の担当者は，Ｐから提供された甲２２が回覧されたことにより（甲２３），そこに記載された方式Ｃを知得したのであるから，方式Ｃの特徴的部分，すなわち，甲１発明の特徴的部分の創作活動に何ら関与していない。

すなわち，甲１に発明者として記載されたＱは，開発プロジェクトの担当部下をまとめる実務責任者であるところ，モバイルコネクトサービスについての個々の具体的な技術については，少なくともベース社の代表取締役であるＲの協力を受ける必要があった（甲３３）。したがって，Ｑは，いわゆるビジネスモデル特許と称される，モバイルコネクトサービスの全体的な仕組みを発案したとしても，かかる仕組みにおける個々の技術，とりわけ，方式Ｃの特徴的部分について，当業者が実施できる程度にまで具体的・客観的なものとして構成する創作能力を備えていなかった。

また，Ｓは，開発プロジェクトのメンバーであったが，Ｑ同様，Ｐから提供された甲２２により方式Ｃを知得したにすぎず，方式Ｃの特徴的部分，すなわち，甲１発明の特徴的部分の創作活動に何ら関与していない。

(ｲ) ベース社の担当者が関与していないこと

前記のとおり，開発プロジェクトを進めるに当たり，セキュア社がＯＦＦＩＣを用いたユーザのパスワード認証技術を，ベース社がｉモードとＯＦＦＩＣとの連携技術をそれぞれ担当する分担の取り決めがなされていた。したがって，Ｒを含むベース社の担当者は，ＯＦＦＩＣに関す

るパスワード認証技術には直接関与していない。

なお，甲１０には，「ＯＦＦＩＣ認証のモバイルコネクトへの実装について私（被告注：Ｒ）の方からパスワード導出パターンについて数字の入力を２回繰り返すことで登録可能か，セキュアプロバイダ社に打診したことを記憶しています。」との記載があるが，ここでいう「２回」とは，パスワードの登録時，誤入力を防止するため，ユーザにパスワードを２回入力させるという，昔からありふれた入力スタイルを意味するにすぎない。Ｒは，ＯＦＦＩＣにおけるパスワードの登録方法がこのような昔からありふれた入力スタイルに沿って行うことが可能か否かをＰに問い合わせたのであって，いわゆる乱数表の２回の提示及び数字の入力により入力位置を特定するという技術的思想を具体化したわけではない（甲６４の２）。

(ｳ) セキュア社のＴが関与していないこと

当時，セキュア社は，株式会社アクロネット（以下「アクロネット社」という。）との間で業務委託契約を締結し，かかる業務委託契約の下，アクロネット社からＴの派遣を受けた。Ｔは，所属はアクロネット社のままであったが，対外的には，セキュア社の営業担当者として業務を遂行しており，ＮＴＴコム社のＳも，Ｔをセキュア社の一担当者として認識していた。Ｔの受託業務は，営業支援業務，より具体的には，潜在的顧客の開拓であり，システムの開発業務には一切携わっていなかった。

(ｴ) Ｐ以外に方式Ｃの特徴的部分に関与したことを名乗り出る者がいないこと

前記のとおり，方式Ｃは，当時のＯＦＦＩＣ方式の弱点を逆に利用したものであり，ＯＦＦＩＣ技術に関する知見がなければ，生まれることはない技術的思想である。当時，ＯＦＦＩＣ技術に関する知見を有する者は，Ｐしかおらず，当然に，方式Ｃを含むパスワード登録方法を，当

業者が実施できる程度にまで具体的・客観的なものとして甲２２にまとめ得る者もＰしかいなかった。事実，Ｐのみが甲２２を作成したのであるから（甲３６の３），他に関与した者の存在を示すものなど存在しない。ＱやＲを含むＮＴＴコム社の開発プロジェクトのメンバーの誰も，方式Ｃを発案し，甲２２を作成したと名乗り出ないのは，発明に関与していなかったからにほかならない。

エ　ＮＴＴコム社が被告からワンタイムパスワード認証特許のライセンスを得ていること

審決は，「確かに，乙第７号証には，現在も，ＮＴＴコム社がパスロジ社からワンタイムパスワード認証技術の特許ライセンスを得ていることが公開されておりＮＴＴコム社が，同社が提供するサービスで使用するワンタイムパスワード認証技術についてのパスロジ社（セキュア社）の貢献を一定程度認めていることは明らかではあるが，そのことをもって甲１発明がＰ氏のみによりなされたことを認めることはできない。」と認定しているが，審決のこの認定は誤りである。

ＮＴＴコム社は，マトリックスの数字を用いたワンタイムパスワード認証技術，つまり，本件発明に係る特許に価値を認めたからこそ，被告と特許ライセンスを締結しているのである。

オ　以上のとおり，方式Ｃの特徴的部分への創作活動に関与した者は，Ｐのみであって，方式Ｃを含むパスワード登録方法を，当業者が実施できる程度にまで具体的･客観的なものとして甲２２にまとめた者もＰのみである。そして，甲２２は，ＰからＮＴＴコム社に提供されたのであるから，方式Ｃの特徴的部分に一致する甲１発明の特徴的部分を発明した者はＰのみである。

(7) 審決の誤り

審決は，発明者同一性の判断を，甲１発明の特徴的部分の発明者と本件発

明の特徴的部分の発明者が同一であるかどうかで判断しておらず，手続違背がある。

すなわち，審決は，甲１発明を，パスワード入力画面の提案の一部（４桁の数字群と数字群の間に何か記号等を入れること）を含む発明として認定し，これに関連して，パスワード入力画面イメージの提案の一部（４桁の数字群と数字群の間に何か記号等を入れること）がＮＴＴコム社のＳによりなされたものと認定している。

しかし，甲１発明の特徴的部分は，位置情報が確定されるまで，縦４個×横１２個の新たなランダムパスワードを端末装置１が表示する処理を繰り返し行い，これにより，縦４個×横１２個の新たなランダムパスワードについての特定の座標位置に配置されているパスワード（すなわち数字）の入力を促す処理を繰り返すことにあるところ，４桁の数字群と数字群の間に何か記号等を入れることは，ユーザの視認性や記憶の便宜性に資するものにすぎず，前記特徴的部分とは全く関係がない。

したがって，前記認定に基づく審決の判断は誤りである。

(8) 以上のとおり，甲１発明の特徴的部分がＰのみによりなされたことが高度の蓋然性を持ち得る水準で立証されており，本件発明１ないし７の発明者は，先願発明（甲１発明）の特徴的部分の発明者と同一であるから，特許法２９条の２本文括弧書の規定が適用されるべきである。

（原告の主張）

(1) 甲１発明は２回の入力でランダムパスワードの位置が一意に確定するものであるが，ＮＴＴコム社の「モバイルコネクトサービス」の開発においてなされたものであり，公報（甲１）に発明者として記載されたＱはもちろん，同社の社員であったＳ，さらには，ベース社の代表取締役であるＲ等，複数人がその創作に関与したものであり，本件発明と甲１発明の発明者は同一といえない。

したがって，本件において特許法２９条の２本文括弧書が適用されることはなく，甲１発明の発明者がＰのみではないとする審決の認定判断に誤りはない。

(2) 発明者が同一であることの立証責任について

特許法２９条の２本文括弧書は，後願の出願人又は特許権者がその利益のために，先願に記載された発明の発明者が後願，すなわち後になって出願された特許出願の発明者と同一であるという社会通念上通常はあり得ないことを主張するのであり，少なくとも本件発明の発明者と甲１発明の発明者とが同一でないとの推定を覆すに足る水準までは後願の出願人又は特許権者が立証責任を負うことは当然である。したがって，被告の主張は失当である。

(3) 甲１発明の特徴的部分の発明者について

ア　審決は，甲２３の電子メールで言及されている「ｉモードでのＯＦＦＩＣ利用開始手順案」には，方式Ｃのような，携帯電話端末でのＯＦＦＩＣワンタイムパスワードの入力画面が必須となるパスワード初回登録時のパスワード入力方法に係る提案が含まれておらず，また，甲２４の電子メールの内容からも，セキュア社からＮＴＴコム社に対して，升による乱数表を用いない携帯電話端末でのＯＦＦＩＣワンタイムパスワードの入力画面を用いたパスワード初回登録時のパスワード入力方法に係る提案はまだされていなかった旨,正しく認定した(審決５８頁２７行ないし６０頁５行)。

そうすると，甲２２の方式Ｃは，平成１３年１月に入ってからのＮＴＴコム社の関係者，Ｒほかベース社の関係者との議論を経た成果であり，およそＰ単独の創作ではない。

イ　被告は，Ｐが甲２２をＮＴＴコム社に提供したと主張するが，方式Ｃが記載された甲２２が甲２３より前にＰからＮＴＴコム社に送信されていたとは考え難い。すなわち，審決が指摘するとおり，甲２３でＮＴＴコム社のＳは「実際のｉモードでのパスワード入力につきまして（改行）限度あ

る携帯画面端末でのパスワードの入力方法になんらかの方向性は見えたでしょうか。（改行）有力案等，途中経過で結構でございますのでご連絡いただければと存じます。」と記載しているが，甲２２に方式Ｃとして示されている画面は「実際のｉモードでのパスワード入力画面」と同じであるはずであり，もし同画面を含む甲２２がＮＴＴコム社に事前に提出されていたら，Ｓがこのようなことを述べるとは考えられない。この点については，甲２４を見ても，Ｓは「一度イメージ画面で結構でございますので，実際の画面パターンをお送りいただければ幸いでございます。（改行）なお，それでは最終的にマスによる乱数表を画面上に表す，との見解でよろしいでしょうか。」と記載しているが，甲２２の「方式Ｃ」の頁は実際の画面パターンを表示しており，もし被告が主張するように甲２３及び２４の前に甲２２がＮＴＴコム社に示されていれば，あり得ない記載である。そして，平成１３年１月１５日付けの甲２５にて，ＮＴＴコム社のＳは「ｉモードでのＯＦＦＩＣ入力イメージのサンプルをどうもありがとうございました。」と述べているのであり，「ｉモードでのＯＦＦＩＣ入力イメージのサンプル」が送付されているのはこのメールの直前のはずであり，甲２２の「方式Ｃ」の頁の記載が被告主張のように平成１２年１２月中にＮＴＴコム社に提供されていたことはあり得ない。

ウ　そもそも甲２２の方式Ｃの内容について，平成１３年１月以降のＮＴＴコム社のプロジェクトチームの議論が反映されていることに加え，携帯電話での初期登録を行うことはＮＴＴコム社からの提案であり（甲２０），２回の入力もＲから提案されており，およそＰが単独で想到したものでないことは明らかである。

エ　甲２３における「ｉモードでのＯＦＦＩＣ利用開始手順案」は，甲２２とは異なる。もし甲３６の１が言及する「ｉモードでのＯＦＦＩＣ利用開始手順案」が甲２３で言うものであれば，その段階でＲが参加するＮＴＴ

コム社のプロジェクトチーム内で回覧されているのであるから（甲２３参照），それから１か月も経った平成１３年１月２２日になってＲが知らないものとして送付されることはない。

(4) ４桁の数字群と数字群の間に何か記号等を入れることを含む発明を甲１発明として認定し発明者同一を判断した点について

審決は，Ｓが４桁の数字群と数字群の間に何か記号等を入れることを提案した事実のみをもって，ＳやＲが甲１発明の発明者であると認定し，その結果として甲１発明がＰ単独による発明ではないと認定したのではない。すなわち，審決は，Ｓが４桁の数字群と数字群の間に何か記号等を入れることを提案した事実等から，ＳやＲが，「ＮＴＴコム社の開発企画会議を通じて，パスワード初回登録時にも使用する，ｉモード携帯電話画面上でのパスワード入力画面の検討に参加し，提案を行っていた」（審決６１頁下から４行ないし末行）ことを認定し，かかる認定等から，「甲１発明について，『ＯＦＦＩＣ』をｉモード携帯電話端末で実現するに当たり，ＮＴＴコム社のモバイルプラットフォーム開発プロジェクトに参加した，ＮＴＴコム社のＳ氏やベース社のＲ氏の関与（数字群と数字群の間に記号等を入れること）が少なくとも認められるから，甲１発明の着想，具体化がＰ氏のみによりなされたとまでは認めることはできず」（審決６２頁１３行ないし１８行）としており，４桁の数字群と数字群の間に何か記号等を入れること以外の提案がＳやＲからなされていた可能性を排除できず，その結果，原告により甲１発明がＰのみによりなされたことが高度の蓋然性を持ち得る程度に証明されたとはいえないとしているにすぎない。

(5) 以上より，甲１発明の発明者がＰのみではないとする審決の認定判断に誤りはなく，被告が主張する取消事由４は理由がない。

第５　当裁判所の判断

１　本件発明について

(1) 本件訂正後の，本件特許の特許請求の範囲請求項１ないし９の記載は，前記第２の２のとおりである。

(2) また，本件明細書（甲８）には，おおむね次のとおりの記載がある（図面については，別紙本件明細書の図参照）。

ア　技術分野

【０００１】

本発明は，ユーザ認証方法およびこれを実現するためのユーザ認証システムに関する。また，本出願は，下記の日本国特許出願に関連する。文献の参照による組み込みが認められる指定国については，下記の出願に記載された内容を参照により本出願に組み込み，本出願の記載の一部とする。

【０００２】

特願２００２－３６０５６　　（出願日：平成１４年２月１３日）

イ　背景技術

【０００３】

近年，コンピュータに代表されるさまざまな情報機器が普及している。特に，電子メール機能やインターネット接続機能を備えた携帯電話機は急速に普及し，人々の必須の情報アイテムとなっている。

【０００４】

このような情報化社会の進展に伴い，システムに対する不正アクセス等のセキュリティ問題は非常に重要になっている。システムに対する不正アクセスを防止するために，伝統的には，予め登録されたユーザＩＤとパスワードとを利用してユーザ認証を行う手法が一般的であるが，セキュリティレベルをより強化するという要求に応えるべく，使用環境や目的に応じたさまざまなユーザ認証方法が提案されている。

【０００５】

その１つは，システムに対してアクセス可能な端末装置を制限したユー

ザ認証である。これは，その端末装置を所有しているユーザが本人であるという前提に立っている。例えば，携帯電話機からあるシステムにアクセスする場合，その携帯電話機に割り当てられた固体識別播号をさらに利用することで，よりセキュアなユーザ認証を行うことができる。

【０００６】

また，乱数表を用いたユーザ認証も知られている。この乱数表を用いたユーザ認証は，乱数表を記した乱数表カードをユーザごとに予め発行しておき，ユーザ認証の都度，システムが乱数表内の任意の位置の数字を指定してユーザに入力させるというものである。これにより，入力される数字は毎回異なるため，「盗聴」に対して有効である。

ウ　発明が解決しようとする課題

【０００７】

システムにおけるユーザ認証において，そこで利用されるパスワードの漏洩（盗聴）は，非常に深刻なセキュリティ問題を招く結果となる。従って，ユーザによるパスワードの管理はきわめて重要であり，また，個々のユーザが自身の行動に「責任」を持つことが，システムのセキュリティ問題を考慮する上で，基本となる。

【０００８】

一般に，ユーザ認証に利用されるパスワードは，システムごとに要求されるものであり，また，その書式もさまざまである。このため，多くのシステムを利用するユーザは，それに応じて多くのパスワードを管理しなければならず，パスワードの管理は，ユーザに対してある種の負担を与えていた。ユーザは，その性質上，パスワードを記憶に留めるように努めているはずであるが，多くのパスワードを管理するような場合には，それらを手帳等に書き留めることも少なくなかった。また，パスワードの管理を煩わしく感じるユーザは，パスワードを記憶しやすい数字に設定したり，シ

ステムごとのパスワードを同一の数字に設定して統一的に管理していた。

【０００９】

しかしながら，このようなパスワードの管理に対するユーザの行動は，そのシステムをセキュリティリスクに晒すことを意味しており，ユーザがこのような行動をとる限り，従来の単なるパスワードによるユーザ認証では，本質的なセキュリティ問題が存在する。

【００１０】

また，ユーザが細心の注意を払ってパスワードの管理をしていたとしても，例えば，店舗に設置された端末装置上で入力しているパスワードを盗み見られたり，また，その端末装置自体に「盗聴」機構が組み込まれ，これによりパスワードが第三者に漏洩するというセキュリティ問題も存在していた。

【００１１】

さらに，上述したような，システムにアクセス可能な携帯電話機を制限したユーザ認証であっても，ユーザがその携帯電話機を紛失し，またはその盗難に遭い，第三者が入手した場合には，もはや伝統的なユーザ認証と同等のセキュリティレベルがあるにすぎず，この種のユーザ認証では，システムに対する不正アクセスを有効に防止することは困難であった。これは，乱数表を用いたユーザ認証においても同様であった。

【００１２】

そこで，本発明は，これらの課題を解決するために，システムに対する第三者の不正アクセスを有効に防止する新たなユーザ認証方法およびこれを実現するシステムを提供することを目的としている。

【００１３】

また，本発明は，既存のシステムインフラストラクチャを最大限活用することにより，余分なコスト負担をかけることなく，このようなユーザ認

証方法およびこれを実現するシステムを提供することを目的としている。

【００１４】

さらに,本発明は,システムに対する不正アクセスを有効に防止しつつ,ユーザによるパスワード管理を容易にして，あらゆるユーザにとって使い勝手のよいユーザ認証方法およびこれを実現するシステムを提供することを目的とし，ひいてはユーザの行動に起因する本質的なセキュリティ問題を排除することを目的としている。

【００１５】

さらにまた，本発明は，このようなユーザ認証方法およびこれを実現するシステムにおいて用いられる「パスワード」の登録方法およびこれを実現するユーザインターフェースを提供することを目的としている。

エ　課題を解決するための手段

【００１６】

本発明は，ユーザごとのパスワード導出パターンを認証サーバに予め登録しておき，ユーザによる利用対象システムの利用の際に，認証サーバが提示用パターンを生成してユーザに提示して，この提示用パターンについてユーザ自身のパスワード導出パターンに対応するキャラクタ列を入力させ，認証サーバは，提示した提示用パターンとユーザ自身のパスワード導出パターンとに基づいて，入力されたキャラクタ列に対して認証を行い，その認証結果を利用対象システムに通知するユーザ認証方法およびユーザ認証システムである。

【００１７】

パスワード導出パターンとは，ある全体パターンを構成する要素群の中から，ユーザによって任意に選択された特定の要素（群）を示したものである。より具体的に説明すれば，パスワード導出パターンは，全体パターンであるマトリックス中のどの要素群がどのように選択されたかを示した

配列パターンないしは配列規則である。ここで注意すべきことは，パスワード導出パターンは，全体パターン中の特定の要素の具体的な値そのものをいうのではなく，あくまでもどの要素を選択したかという情報にすぎないということである。

【００１８】

より具体的には，第１の観点に従う本発明は，所定のパターンを構成する要素群の中から選択された特定の要素に基づくパスワード導出パターンを登録する登録ステップと，ユーザの情報端末装置から送信された，利用対象システムに割り当てられたシステム識別情報を受け付ける受付ステップと，前記情報端末装置から前記システム識別情報を受け付けた場合に，前記所定のパターンを構成する要素群のそれぞれに所定のキャラクタを割り当てた提示用パターンを生成する生成ステップと，前記情報端末装置上に前記生成した提示用パターンを含む所定の画面を提示して，前記パスワード導出パターンに対応する特定の要素に割り当てられたキャラクタの入力を前記ユーザに促す入力ステップと，前記利用対象システムから入力された前記キャラクタを受け付け，前記提示用パターンと前記ユーザのパスワード導出パターンとに基づいて，前記受け付けたキャラクタが正当であるか否かを判断する判断ステップと，前記判断した結果を前記利用対象システムに通知する通知ステップと，を備えるユーザ認証方法である。

【００１９】

また，第２の観点に従う本発明は，所定のパターンを構成する要素群の中から選択された特定の要素に基づくパスワード導出パターンを登録するステップと，ユーザの情報端末装置から送信された，利用対象システムに割り当てられたシステム識別情報を受け付ける受付ステップと，前記情報端末装置から前記所定の識別情報を受け付けた場合に，前記所定のパターンを構成する要素群のそれぞれに所定のキャラクタを割り当てた提示用パ

ターンを生成するステップと，前記情報端末装置上に前記生成した提示用パターンを含む所定の画面を提示して，前記パスワード導出パターンに対応する特定の要素に割り当てられたキャラクタの入力を前記ユーザに促すステップと，前記情報端末装置から入力された前記キャラクタを受け付け，前記提示用パターンと前記ユーザのパスワード導出パターンとに基づいて，前記受け付けたキャラクタが正当であるか否かを判断するステップと，前記判断した結果を前記利用対象システムに通知するステップと，を備えるユーザ認証方法である。

【００２０】

また，第３の観点に従う本発明は，ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録方法であって，複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを無線端末装置に表示させ，これにより，前記提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促すステップと，前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，新たな提示用パターンを無線端末装置に表示させる作業を繰り返し行い，これにより，前記新たな提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す作業を繰り返すステップと，前記無線端末装置と通信回線を介して接続されたサーバが，前記入力されたキャラクタに基づいて特定されたパスワード導出パターンを登録するステップと，を含むパスワード導出パターンの登録方法である。

【００２１】

また，第４の観点に従う本発明は，上記第３の観点に従うパスワード導出パターンの登録方法により登録されたパスワード導出パターンを用いたユーザ認証方法であって，認証用パターンを無線端末装置に表示させ，これにより，前記認証用パターンについての特定の要素に割り当てられたキ

ャラクタの入力を促すステップであって，前記認証用パターンは前記提示用パターンと同一の要素から構成される前記所定のパターンの要素のそれぞれに，前記提示用パターンとは異なるキャラクタを割り当てたものと，前記サーバが，前記認証用パターンに関する情報と，前記認証用パターンに基づいて入力されたキャラクタとに基づいて，前記登録された特定されたパスワード導出パターンを有するユーザと，前記新たな提示用パターンに基づいてキャラクタを入力したユーザとが一致しているか否か判断するステップと，を含む，ユーザ認証方法である。

【００２２】

また，第５の観点に従う本発明は，ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録システムであって，複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを端末装置に表示させ，これにより，前記提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促すための手段と，前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，新たな提示用パターンを前記端末装置に表示させる作業を繰り返し，これにより，前記新たな提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す作業を繰り返すステップと，前記端末装置と通信回線を介して接続されたサーバに，前記端末装置から前記入力されたキャラクタを受け取り，受け取った前記入力されたキャラクタに基づいてパスワード導出パターンを特定させるための手段と，前記サーバに，前記特定されたパスワード導出パターンを登録させるための手段と，を備えるパスワード導出パターンの登録システムである。

【００２３】

上記方法の発明は，装置の発明として把握することができる。また，こ

れらの発明は，コンピュータに実行されることで，所定のハードウェアと相まって所定の機能を実現させるプログラムおよび該プログラムを記録した記録媒体としても成立する。

【００２４】

なお，本明細書において，手段とは，単に物理的手段を意味するものではなく，その手段が有する機能をソフトウェアによって実現する場合も含む。また，１つの手段が有する機能が２つ以上の物理的手段により実現されても，２つ以上の手段の機能が１つの物理的手段により実現されても良い。

オ　発明を実施するための形態

【００３５】

図２は，パスワード導出パターンを説明するための図である。図２（ａ）は，４行１２列のマトリックスが全体パターンである例を示す図である。図２において，選択された要素にハッチングがなされ，また，選択された順番にその要素内に数字が付されている。従って，この場合のパスワード導出パターンは，マトリックス表現を用いれば，“（３，２）－（０，５）－（３，７）－（０，１０）”と表すことができる。

【００３６】

図２（ｂ）は，４行４列のマトリックスが全体パターンである例を示す図である。この場合のパスワード導出パターンは，マトリックス表現を用いれば，“（０，０）－（１，２）－（２，１）－（３，２）”と表すことができる。

【００３７】

パスワード導出パターンは，利用対象システム１１に対するユーザ認証を行うために用いられ，そのためユーザが記憶すべきものである。その意味で，パスワード導出パターンは，ある種のパスワードということができ

る。パスワード導出パターンを構成する要素の数，配列は任意であり，ユーザ認証におけるセキュリティレベルに応じて適宜設定される。

【００３８】

パスワードがＪ桁の数字列である場合，全体パターンは，以下の条件を満たすようなＫ行Ｌ列のマトリックスであることが好ましい。

$$10^{J} < (K*L)*(K*L-1)\cdots(K*L-J+1)$$

・・・式（１）

従来の認証方法では，パスワードがＪ桁の数字列である場合，パスワードの組み合わせは，１０のＪ乗通りある。一方，本実施形態における認証方法によれば，全体パターンがＫ行Ｌ列のマトリックスである場合，パスワード導出パターンの組み合わせは，（Ｋ＊Ｌ）＊（Ｋ＊Ｌ－１）・・（Ｋ＊Ｌ－Ｊ＋１）通りある。従って，上記（１）式を満たすように全体パターンを構成することにより，従来の認証方法より組み合わせ数を増やし，セキュリティレベルを上げることができる。すなわち，本実施形態によれば，利用対象システム１１に対して入力すべきパスワードの桁数が，従来の認証方法と同じ場合であっても，マトリックスの構成を変えるだけで，従来の認証方法よりもセキュリティレベルを容易に上げることができる。…（中略）…

【００４３】

このように，ユーザが入力すべきパスワードは，ユーザ認証の都度，生成された乱数表から，予め登録しておいたパスワード導出パターンに従って決定される一過性のものである。従って，仮に，入力したパスワードが第三者に漏洩したとしても，そのパスワード自体は，次回のユーザ認証においては全く意味をなさないため，不正アクセスは有効に防止されること

になる。また,ユーザが記憶すべきこのようなパスワード導出パターンは,従来のような「具体的な数字」でなく，パターンという「概念的・図形的なもの」であり，従って，ユーザにとって覚えやすく，忘れにくいという特質を有し，パスワード管理に適したものである。

【００４４】

次に，ユーザ認証に用いられる登録データについて説明する。ユーザが利用対象システム１１を利用するためには，その利用に先立って，ユーザはその利用対象システム１１に対するユーザアカウント（ユーザ名）を取得するとともに，そのユーザ名に対するパスワード導出パターンを登録しなければならない。このため，認証データベース１４は，どの利用対象システム１１がどのようなユーザに利用権限を与え，利用権限が与えられた個々のユーザがどのようなパスワード導出ルールを登録しているかを登録データとして管理している。

【００４５】

利用対象システム１１に対するユーザアカウントの登録においては，典型的には，利用対象システム１１の管理者がユーザからの申請を受けて行う形態と，ユーザ自身が行う形態とが考えられる。どのような形態でユーザアカウントを登録するかは，その利用対象システム１１の運用ポリシーに応じて適宜に採用することができ，また，その実現手段は，既存のさまざまな技術を適用することができる。以下では，利用対象システム１１に対するユーザアカウントについては，その管理者によって認証データベース１４に登録されたものとして，ユーザによるパスワード導出パターンの登録手順について説明する。

【００４６】

図３は，パーソナルコンピュータ１５上に表示されたパスワード導出パターン登録画面の一例を示している。このような登録画面は，ＨＴＭＬ等

のページ記述言語に従って記述されるページデータにより構成される。ユーザは,Ｗｅｂブラウザを操作して認証サーバ１２にアクセスすることで,パーソナルコンピュータ１５上にこのような登録画面を表示させる。例えば，利用対象システム１１に対するユーザアカウントを登録した時点で,管理者はこのような登録画面を構成するページデータのＵＲＬを含むメールコンテンツを，そのユーザのメールアドレスに対してメールで送信し,これを受信したユーザがそのメールコンテンツ中のＵＲＬを選択するという方法で，このような登録画面をユーザに提供する。

【００４７】

同図において，ユーザ名入力フィールド３１は，利用対象システム１１を利用するユーザの名前（ユーザアカウント）を入力するためのフィールドである。ユーザアカウントは，管理者においてすでに登録されているので，ユーザに改めて入力させるのでなく，ユーザ名入力フィールド３１に予め埋め込まれるように構成してもよい。

【００４８】

グループ名入力フィールド３２は，そのユーザが属するグループの名前を入力するためのフィールドである。ただし，本実施形態では，説明を簡単にするため，グループ名の入力は要しないものとする。

【００４９】

携帯電話番号入力フィールド３３は，利用対象システム１１の利用に際してユーザ認証に用いる携帯電話機１３を特定するための個体識別情報を入力するためのフィールドである。本実施形態では，ユーザが所有する携帯電話機１３に割り当てられた携帯電話番号をそのまま用いるものとする。なお，この携帯電話番号についても，管理者において登録し，携帯電話番号入力フィールド３３に予め埋め込まれるように構成してもよい。

【００５０】

全体パターン３４は，４行１２列のマトリックス状に配置された４８個の要素群としてのボタンオブジェクトによって構成されている。それぞれの要素には，個々の要素を識別するために，要素名として１から４８の一連の番号が付されている。

【００５１】

位置指定入力フィールド３５は，全体パターン３４の中から選択される１以上の特定の要素をその要素名で指定して入力するためのフィールドである。本例では，要素“１”，“１７”，“３３”および“４８”が入力されている。複数の要素が入力される場合には，個々の要素はデリミタ（例えばカンマ）で区切られるものとする。また，同じ要素の入力がされてもよい。ここで，入力された要素のシーケンスがパスワード導出パターンとなる。要素のシーケンスには，ダミー“＊”を含めることができる。ユーザがダミー“＊”を入力した場合，任意の文字の設定要求として扱われる。これは，以下に示す変換法則とともに，パスワード導出パターンが第三者に類推されるのを防止するためのものである。つまり，パスワード導出パターンは，ユーザにとって覚えやすいパターンになる傾向があるため，実際のパスワードを構成する文字の間に無意味な文字を挿入することによって類推を防止している。例えば，最初の４要素分をダミーとした８要素からなるシーケンスでは，ユーザは最初の４桁については無意味な数字を入力することができる。なお，ユーザが，位置指定入力フィールド３５に“Ｆ”のみを入力した場合，これは固定パスワードの設定要求として扱われ，この場合には，固定パスワード入力フィールド３７に所定桁の数字を入力する。

【００５２】

変換法則入力フィールド３６は，ユーザが提示用パターンを参照して実際にパスワードを入力する際に，パスワード導出パターンから導き出され

る要素値に対してさらに変換法則を与えることを希望する場合に，その変換法則を入力するためのフィールドである。つまり，パスワード導出パターンから導き出される要素値に対してさらに変換法則を施して得られた結果が入力すべき真のパスワードになる。変換法則には，例えば，パスワード導出パターンから導き出される要素値に対する四則演算操作が定義されている。より具体的には，この変換法則入力フィールド３６に，単に“＋１”と入力した場合，パスワード導出パターンから導き出される要素値に対してそれぞれ１を加算した結果が，ユーザが入力すべき真のパスワードとなる。また，この変換法則入力フィールド３６に，“＋１，＋２，＋３，＋４”というようにカンマで区切って，位置指定入力フィールド３５に入力された要素のシーケンスに対応するように演算式を入力した場合，パスワード導出パターンから導き出されるそれぞれの要素値に対してそれぞれの演算式を施した結果が，ユーザが入力すべき真のパスワードとなる。

【００５３】

なお，入力した演算式によっては，要素値に演算を施した結果，繰り上がり（または繰り下がり）が生じる場合がある。このような場合には，１の位を採用するというように定義しておけば,パスワードの桁数(文字数)が変動することなく，固定長にすることができる。また，要素値に演算を施した結果をそのまま用いるというように定義して，可変長のパスワードにすることもできる。

【００５４】

このような登録画面において，ユーザは，キーボードを用いて直接的に要素（要素名）をカンマで区切りながら順番に入力してもよいが，標準的なグラフィカルユーザインターフェースを用いることによっても,同様に,入力することができる。このようなグラフィカルユーザインターフェースでは，ユーザが，所望の要素にマウスカーソルを当てて，その上で選択（ク

リック）すると，位置指定入力フィールド３５にその要素がデリミタで区切られて表示される。選択された要素は，例えば，画面上，視覚的に区別して表示されることが好ましい。

【００５５】

なお，候補ボタン３８は，選択すべき要素のシーケンスを自動的に生成させるためのものである。すなわち，ユーザがこの候補ボタン３８にマウスカーソルを当てて，その上で選択すると，例えば予め登録された要素のシーケンスを位置指定入力フィールド３５にランダムに入力，表示する。これは，ユーザがパスワード導出パターンを設定する場合，隣り合った要素ボタンを選択する傾向があり，類推されやすいため，このような状況を回避すべく，補助的に設けられている。

【００５６】

ユーザが所定の入力フィールドに必要な情報を入力した後，設定の確認ボタン３９を選択すると，Ｗｅｂブラウザは，入力された情報を含んだ登録要求を認証サーバ１２に送信する。認証サーバ１２は，受信した登録要求に基づいて，ユーザのパスワード導出パターンを登録データとして仮登録して，設定の確認画面をＷｅｂブラウザに表示させる。

【００５７】

設定の確認画面は，ユーザが設定したパスワード導出パターンに従ってユーザに実際にパスワードを入力させることで，パスワード導出パターンを確認させる画面である。図４は，パーソナルコンピュータ１５上に表示された設定の確認画面の一例を示している。ただし，パーソナルコンピュータ１５の代わりに，ユーザの携帯電話機１３上に設定の確認画面を表示させて,そこから設定の確認を行わせるようにしてもよい。この場合には，利用対象システム１１の利用に際してユーザが使用する携帯電話機１３を併せて確認することができる。

【００５８】

同図に示すように，設定の確認画面には，認証サーバ１２によって生成された，全体パターン３４の要素群のそれぞれにランダムな数字を割り当てた提示用パターン４１が表示される。ユーザは，提示用パターンのうち，先に設定したパスワード導出パターンに対応する要素に割り当てられた数字（要素値）をパスワード入力フィールド４２にパスワードとして入力する。ユーザがパスワード入力フィールド４２にパスワードを入力した後，Ｇｏボタン４３を選択すると，Ｗｅｂブラウザは，入力されたパスワードを含んだ確認要求を認証サーバ１２に送信する。認証サーバ１２は，受信した確認要求に含まれるパスワードが，生成した提示用パターンと先に仮登録したパスワード導出パターンとから導き出される数字列に一致するか否かを判断し，一致する場合には，認証データベース１４にユーザのパスワード導出パターンを登録データとして正式に登録する。

【００５９】

なお，認証サーバ１２は，パーソナルコンピュータ１５を用いたこのようなパスワード導出パターンの登録手続きにおいて，ユーザが所有する携帯電話機１３を確認するため，受け付けた携帯電話番号に対して，所定のメッセージを送信し，ユーザにそのメッセージに対する返信を要求することが好ましい。

…（中略）…

【００８６】

［第４の実施形態］

本実施形態は，携帯電話機１３を用いたパスワード導出パターンの登録方法に関するものであり，提示される提示用パターンに対して，ユーザが意図したパスワード導出パターンに対応する要素値の入力を繰り返すことによって，そのパスワード導出パターンを特定していくことを特徴として

いる。

【００８７】

図１８は，本実施形態に係るパスワード導出パターンの登録方法の処理の流れを説明するためのフローチャートである。このような処理は，携帯電話機１３と認証サーバ１２とによるクライアント／サーバモデルにおけるそれぞれのプログラムによって実現することができるが，本実施形態では，このような処理を実現するための所定のプログラムを含むページデータを認証サーバ１２から携帯電話機１３に送信し，携帯電話機１３においてこれを実行することにより実現している。

【００８８】

上記実施形態と同様に，例えば，利用対象システム１１に対するユーザアカウントが登録された時点で，認証サーバ１２は，この登録画面を構成するページデータのＵＲＬを含むメールコンテンツをユーザの携帯電話機１３に対してメールで送信し，これを受信したユーザが携帯電話機１３上に表示されたメールコンテンツ中のＵＲＬを選択する。これにより，認証サーバ１２は，所定のプログラムを含むページデータを携帯電話機１３に送信する。

【００８９】

ページデータを受信した携帯電話機１３は，そのページデータを解釈して，そこに含まれる所定のプログラムに従って図１８に示す処理を実行し，登録画面を表示する。すなわち，携帯電話機１３は，まず，全体パターン３４の要素群のすべてに対して，乱数発生関数により発生させた乱数をそれぞれ割り当てて提示用パターンを生成し，他の画面要素と相まってパスワード導出パターン登録画面として表示して，ユーザに入力を促す（ＳＴＥＰ１８０１）。ユーザは，この登録画面に対して，登録しようとするパスワード導出パターンの要素に割り当てられた数字を入力する。携帯電話機１

３は，ユーザから要素のシーケンスを受け付けると（ＳＴＥＰ１８０２），提示した提示用パターンのうち，入力された要素値を持つ要素を該当要素として抽出し，その数を保持しておく（ＳＴＥＰ１８０３）。

次に，携帯電話機１３，抽出した該当要素の数が入力された要素数と等しいか否かを判断し（ＳＴＥＰ１８０４），等しくないと判断する場合には，要素の絞り込みを行うため，全体パターン３４中の該当要素のみに乱数を割り当てて提示用パターンを生成し，同様に，登録画面として表示して，ユーザに入力を促す（ＳＴＥＰ１８０５）。一方，抽出した該当要素の数が入力された要素数と等しいと判断する場合，携帯電話機は，要素の絞り込みができたものとして，登録確認画面を提示して，ユーザに確認を促す（ＳＴＥＰ１８０６）。そして，ユーザによって例えば「ＯＫ」ボタンが選択された場合には（ＳＴＥＰ１８０７のＹｅｓ），携帯電話機１３は，要素のシーケンスをパスワード導出パターンとして登録するため，登録要求を認証サーバ１２に送信し（ＳＴＥＰ１８０６），処理を終了する。

【００９０】

このようにして，登録しようとするパスワード導出パターンに対応する要素値の入力を繰り返すことによって提示用パターンの要素を絞り込んでいき，ユーザが意図しているパスワード導出パターンを特定する。

【００９１】

図１９および図２０は，パスワード導出パターンの登録方法を説明する画面例である。まず，図１９（ａ）に示す画面が携帯電話機１３上に表示されたとする。ここで，この画２０面に対して，ユーザが“９８９３”と入力すると，携帯電話機１３は，入力された要素のシーケンスに基づいて，新たな提示用パターンを生成する。すなわち，携帯電話機１３は，先の提示用パターンの各要素のうち，その値が“９”，“８”または“３”であった要素を該当要素として抽出するが，この場合，該当要素の数は入力し

た要素の数にまで絞り込まれていないので，携帯電話機１３は，該当要素に乱数を割り当てた新たな提示用パターンを生成し，図１９（ｂ）に示すような登録画面を表示する。

【００９２】

ユーザは，この画面に対して，登録しようとするパスワード導出パターンの要素に割り当てられた数字を，再度，入力して，該当要素を絞り込む作業を行う。この場合，ユーザが入力すべき数字は“６５４１”となる。携帯電話機１３は，該当要素を絞り込むことができない場合には，新たな提示用パターンを生成し，図１９（ｃ）に示すような登録画面を表示し，ユーザに入力を促す。そこで，ユーザは，この画面に対して，登録しようとするパスワード導出パターンの要素に割り当てられた数字“８５０１”を入力する。

【００９３】

この入力によって，携帯電話機１３は，該当要素を絞り込むことができたため，図２０に示すような登録確認画面を提示して，ユーザに確認を促す(ＳＴＥＰ１８０６)。この５画面に対して，ユーザが「ＯＫ」ボタン２０１を選択すると，携帯電話機１３は，要素のシーケンスをパスワード導出パターンとして認証サーバ１２に送信する。一方，ユーザが「やり直し」ボタン２０２を選択すると，携帯電話機１３は，パスワード導出パターンの登録処理を最初からやり直す。

【００９４】

以上のように，本実施形態によれば，提示用パターンの提示と，登録しようとするパスワード導出パターンに対応する要素値の入力とを繰り返すことによって，提示用パターンの要素を絞り込んでいくことができるので，ユーザが意図しているパスワード導出パターンを特定することができるようになる。従って，携帯電話機１３のようにユーザインターフェースが十

分でない場合であっても，きわめて簡単に，パスワード導出パターンを登録することができる。

【００９５】

また，本実施形態によれば，パスワード導出パターンの登録操作は，実際のパスワードの入力操作と同じ手順で行われるので，パスワード入力の練習を兼ねることができ，ユーザにパスワード導出パターンを早く，確実に覚えさせることができる。

【００９６】

なお，本実施形態では，ランダムに提示用パターンを生成して，ユーザが意図している該当要素を絞り込むようにしているため，生成された提示用パターンの組み合わせによっては３回以上の絞り込み作業を要する場合がある。このような事態を避けるため，２回の絞り込み作業で必ず完了する固定の提示用パターンの組み合わせを用いるようにしてもよい。

(3) 以上によれば，本件発明の特徴は，次のとおりであると認められる。

ア　発明の属する分野

本件発明は，ユーザ認証方法およびこれを実現するためのユーザ認証システムに関する（【０００１】）。

イ　発明が解決しようとする課題

情報化社会の進展に伴い，システムに対する不正アクセス等のセキュリティ問題は非常に重要になっている。システムに対する不正アクセスを防止するために，伝統的には，予め登録されたユーザＩＤとパスワードとを利用してユーザ認証を行う手法が一般的であるが，セキュリティレベルをより強化するという要求に応えるべく，使用環境や目的に応じたさまざまなユーザ認証方法が提案されている（【０００４】）。

その１つは，システムに対してアクセス可能な端末装置を制限したユーザ認証であり，その端末装置を所有しているユーザが本人であるという前

提に立ち，例えば，携帯電話機からあるシステムにアクセスする場合，その携帯電話機に割り当てられた固体識別番号をさらに利用することで，よりセキュアなユーザ認証を行うことができる（【０００５】）。

また，乱数表を用いたユーザ認証も知られている。この乱数表を用いたユーザ認証は，乱数表を記した乱数表カードをユーザごとに予め発行しておき，ユーザ認証の都度，システムが乱数表内の任意の位置の数字を指定してユーザに入力させることにより，入力される数字は毎回異なるため，「盗聴」に対して有効である（【０００６】）。

多くのシステムを利用するユーザは，それに応じて多くのパスワードを管理しなければならず，パスワードを手帳等に書き留めることも少なくなく，パスワードの管理を煩わしく感じるユーザは，パスワードを記憶しやすい数字に設定したり，システムごとのパスワードを同一の数字に設定して統一的に管理していた（【０００８】）。

しかしながら，このようなパスワードの管理に対するユーザの行動は，そのシステムをセキュリティリスクに晒すことを意味しており，従来の単なるパスワードによるユーザ認証では，本質的なセキュリティ問題が存在する（【０００９】）。

また，ユーザが細心の注意を払ってパスワードの管理をしていたとしても，例えば，店舗に設置された端末装置上で入力しているパスワードを盗み見られたり，また，その端末装置自体に「盗聴」機構が組み込まれ，これによりパスワードが第三者に漏洩するというセキュリティ問題も存在していた（【００１０】）。

システムにアクセス可能な携帯電話機を制限したユーザ認証であっても，ユーザがその携帯電話機を紛失し，またはその盗難に遭い，第三者が入手した場合には，システムに対する不正アクセスを有効に防止することは困難であり，乱数表を用いたユーザ認証においても同様であった（【００１

１】）。

そこで，本件発明は，これらの課題を解決するために，システムに対する第三者の不正アクセスを有効に防止する新たなユーザ認証方法およびこれを実現するシステムを提供することを目的としている（【００１２】）。

また，本件発明は，既存のシステムインフラストラクチャを最大限活用することにより，余分なコスト負担をかけることなく，このようなユーザ認証方法およびこれを実現するシステムを提供することを目的としている（【００１３】）。

さらに，本件発明は，システムに対する不正アクセスを有効に防止しつつ，ユーザによるパスワード管理を容易にして，あらゆるユーザにとって使い勝手のよいユーザ認証方法およびこれを実現するシステムを提供することを目的とし，ひいてはユーザの行動に起因する本質的なセキュリティ問題を排除することを目的としている（【００１４】）。

さらにまた，本件発明は，このようなユーザ認証方法およびこれを実現するシステムにおいて用いられる「パスワード」の登録方法およびこれを実現するユーザインターフェースを提供することを目的としている（【００１５】）。

ウ　課題を解決するための手段

本件発明は，ユーザごとのパスワード導出パターンを認証サーバに予め登録しておき，ユーザによる利用対象システムの利用の際に，認証サーバが提示用パターンを生成してユーザに提示して，この提示用パターンについてユーザ自身のパスワード導出パターンに対応するキャラクタ列を入力させ，認証サーバは，提示した提示用パターンとユーザ自身のパスワード導出パターンとに基づいて，入力されたキャラクタ列に対して認証を行い，その認証結果を利用対象システムに通知するユーザ認証方法およびユーザ認証システムである。

より具体的には，ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録方法であって，複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを無線端末装置が表示し，これにより，前記提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促すステップと，前記入力されたキャラクタに基づいて，前記入力されたキャラクタの数に等しい数の要素からなるパスワード導出パターンが２回で特定されるように，新たな提示用パターンを前記無線端末装置が表示する処理を繰り返し行い，これにより，前記新たな提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す処理を繰り返すステップと，前記無線端末装置と通信回線を介して接続されたサーバが，前記入力されたキャラクタに基づいて特定されたパスワード導出パターンを登録するステップと，を含むパスワード導出パターンの登録方法である。

（【００１６】，【００２０】，【００９６】，本件訂正後の特許請求の範囲〔甲６８〕）

エ　発明の効果

本件発明によれば，提示用パターンの提示と，登録しようとするパスワード導出パターンに対応する要素値の入力とを繰り返すことによって，提示用パターンの要素を絞り込んでいくことができるので，ユーザが意図しているパスワード導出パターンを特定することができるようになり，携帯電話機のようにユーザインターフェースが十分でない場合であっても，極めて簡単に，パスワード導出パターンを登録することができる（【００９４】）。

また，本件発明によれば，パスワード導出パターンの登録操作は，実際のパスワードの入力操作と同じ手順で行われるので，パスワード入力の練習を兼ねることができ，ユーザにパスワード導出パターンを早く，確実に

覚えさせることができる（【００９５】）。

また，２回の絞り込み作業で必ず完了する固定の提示用パターンの組合せを用いることにより，３回以上の絞り込み作業を行う必要がない（【００９６】）。

２　甲１発明について

(1) 本件特許に係る出願の優先日前の平成１３年６月４日に出願された他の特許出願であって，本件特許に係る出願の優先日後，原出願（特願２００３－５６８５４６号）の出願日前の平成１４年１２月２０日に出願公開された特願２００１―１６８８７９号（特開２００２－３６６５１７号公報：甲１）（出願人：ＮＴＴコム社，発明者：Ｑ）の願書に最初に添付した明細書及び図面には，おおむね次のとおりの記載がある（図面については，別紙甲１の図参照）。

ア　発明の属する技術分野

【０００１】

本発明は，ネットワークを介して端末装置にサービスを提供するサービス提供方法，サービス提供システム，処理センタ装置及びプログラムに関するものである。

イ　従来の技術

【０００２】

近年，ウエブ（Ｗｅｂ）ブラウザを搭載した携帯通信端末装置を用いてサイトにアクセスし，情報を検索したり情報を入手したりする移動体通信サービスが普及している。

ウ　発明が解決しようとする課題

【０００３】

しかしながら，従来の移動体通信サービスでは，個々の携帯通信端末装置を特定することが難しく，正規の登録ユーザ以外の第三者によって不正

にアクセスされる可能性があるため，サービス提供者にとってはセキュリティ管理が難しいという問題点があった。また，従来の移動体通信サービスでは，セッション管理に手間がかかるという問題点があった。特に，通常のＨＴＭＬ(Hyper Text Markup Language)と異なり，クッキー(Cookie)を利用できない場合，サービス提供者にとってはセッション管理に著しく手間がかかる。さらに，従来の移動体通信サービスでは，サービス提供者側で端末装置に提供するコンテンツ等のデータを端末装置が認識可能な言語形式のデータに変換していたため，サービス提供者にとってはデータ変換に手間がかかるという問題点があった。

【０００４】

以上のように，従来の移動体通信サービスでは，セキュリティ管理とセッション管理とデータ変換処理とをサービス提供者側で行う必要があったため，コストと手間がかかるという問題点があった。なお，以上のような問題点の少なくとも一部は，移動体通信サービス以外の通信サービスでも発生する可能性がある。本発明は，上記課題を解決するためになされたもので，サービス提供者の負担を軽減することができるサービス提供方法，サービス提供システム，処理センタ装置及びプログラムを提供することを目的とする。

エ　課題を解決するための手段

【０００５】

本発明は，ネットワーク（２）を介してサービス提供を受ける端末装置（１）とサービス提供者装置（３－１～３－３）との間を処理センタ装置（４）によって仲介するサービス提供方法であって，サービス提供を希望する前記端末装置からのアクセスがあったとき，このアクセス元の端末装置の認証を前記処理センタ装置で行う認証手順と，前記認証の終了後に，前記アクセス元の端末装置で選択されたサービスに対応するアクセス先を

識別するための，前記アクセス毎に固有の識別子を発行して前記処理センタ装置から前記アクセス元の端末装置に送信し，前記選択されたサービスを提供する前記サービス提供者装置にアクセスして，このサービス提供者装置に前記選択されたサービスに対応する処理要求を送信するセッション管理手順と，前記処理要求に対する結果として前記サービス提供者装置から返送されたデータを，前記アクセス元の端末装置に適した表示形式で，かつこの端末装置が認識可能な言語形式のデータに変換して，変換後のデータを前記処理センタ装置から前記ネットワークを介して前記アクセス元の端末装置に送信するデータ変換手順とを実行するようにしたものである。また，本発明のサービス提供方法の１構成例において，前記認証手順は，前記端末装置のユーザに固有のユーザＩＤ及びワンタイムパスワードを用いて前記端末装置の認証を行う手順である。

…（以下略）…

オ　発明の実施の形態

【０００７】

以下，本発明の実施の形態について図面を参照して詳細に説明する。図１は本発明の実施の形態となるサービス提供システムの構成を示すブロック図である。本実施の形態のサービス提供システムは，ウエブブラウザを搭載した携帯電話機等の端末装置１と，移動体通信網２と，端末装置１に対してサービスを提供するサービス提供者装置３（３－１～３－３）と，移動体通信網２とサービス提供者装置３との間に設けられた処理センタ装置４とから構成される。

【０００８】

移動体通信網２と処理センタ装置４との間は，専用線５によって接続され，サービス提供者装置３と処理センタ装置４との間は，専用線，フレームリレー等の通信回線６によって接続されている。各サービス提供者装置

３－１～３－３は，後述するサーバ３２及びメールサーバ３４と通信回線６とを接続するファイアウォール・ルータ（以下，ＦＷ・ＲＴと略する）３１と，データベースを管理するサーバ３２と，在庫管理・受発注システム，勤務管理システム，電子稟議システムあるいはグループウエア等のデータベース３３（３３－１～３３－４）と，電子メールの送受信を行うためのメールサーバ３４とを有している。

【０００９】

サーバ３２は，処理センタ装置４からの処理要求に対応するデータベース３３にアクセスして，処理結果のデータを処理センタ装置４に返送するデータベースアクセス手段３２１を有している。

【００１０】

処理センタ装置４は，後述するウエブ（Ｗｅｂ）サーバと専用線５とを接続するファイアウォール（以下，ＦＷと略する）４１と，サービス提供を希望する端末装置１からのアクセスがあったとき，この端末装置の認証を行う認証サーバ４２と，端末装置１で選択されたサービスに対応する処理要求をサービス提供者装置３に送信し，このサービス提供者装置３からの処理結果のデータを端末装置１に送信するウエブサーバ４３と，ウエブサーバ４３と通信回線６とを接続するルータ（以下，ＲＴと略する）４４と，端末装置１のユーザ情報を予め記憶するためのデータベース４５とを有している。

【００１１】

ウエブサーバ４３は，アクセス元１の端末装置で選択されたサービスに対応するアクセス先を識別するための，アクセス毎に固有のＵＲＬを発行してアクセス元の端末装置１に送信し，前記選択されたサービスを提供するサービス提供者装置３にアクセスして，このサービス提供者装置３に前記選択されたサービスに対応する処理要求を送信するセッション管理手段

４３１と，処理要求に対する結果としてサービス提供者装置３から返送されたデータを，アクセス元の端末装置１に適した表示形式で，かつこの端末装置１が認識可能な言語形式のデータに変換して，変換後のデータをアクセス元の端末装置１に送信するデータ変換手段４３２とを有している。

【００１２】

以下，本実施の形態のサービス提供システムについて図２を用いて説明する。最初に，端末装置１のユーザは，端末装置１に対して，所望のサービスに対応した既知のＵＲＬ（Uniform Resource Locators）を入力する等の操作を行う。端末装置１は，移動体通信網２を通じて，このＵＲＬを持つ装置（処理センタ装置４）にアクセスする（図２ステップ１０１）。なお，ユーザが入力するＵＲＬは，ユーザ毎及びサービス提供者装置３－１～３－３毎に予め設定されるものである。以下，ユーザが入力したＵＲＬを第１のＵＲＬと呼ぶ。

【００１３】

処理センタ装置４の認証サーバ４２は，サービス提供者装置３－１～３－３の何れかに対応する第１のＵＲＬを用いたアクセスが行われると，ユーザに対してユーザ識別子（以下，ユーザＩＤとする）の入力を促すウエブページのファイルをＦＷ４１，専用線５及び移動体通信網２を介してアクセス元の端末装置１に送信する。こうして，端末装置１の画面に処理センタ装置４のＷｅｂページが表示される。

【００１４】

ユーザは,表示されたウエブページを見ながら,端末装置１を操作して，所望のサービスに対応した既知のユーザＩＤを入力する。入力されたユーザＩＤは，端末装置１から移動体通信網２を通じて処理センタ装置４に送られる。ユーザＩＤは，ユーザ毎及びサービス提供者装置３－１～３－３毎に予め設定されるものである。したがって，同一ユーザがサービス提供

者装置３－１～３－３の各々からサービス提供を受ける場合には，サービス提供者装置３－１～３－３の各々についてユーザＩＤが設定される。

【００１５】

データベース４５には，サービス提供者装置３－１～３－３毎にユーザ情報が予め登録されている。ユーザ情報としては，例えば端末装置１の電話番号，前述のユーザＩＤ，後述するランダムパスワードの位置情報，メールサーバ３４のメールアカウント及びパスワード等がある。端末装置１のユーザは，サービス提供を希望するサービス提供者装置３－１～３－３について，自身のユーザ情報を処理センタ装置４（データベース４５）に予め登録しておく。

【００１６】

認証サーバ４２は，アクセス元の端末装置１から送られた第１のＵＲＬに基づいて対応するサービス提供者装置３を特定し，特定したサービス提供者装置３に対応するユーザ情報のリストをデータベース４５上で検索して，検索したリストから端末装置１の電話番号に対応するユーザＩＤを取得する。そして，認証サーバ４２は，データベース４５から取得したユーザＩＤと端末装置１から送られたユーザＩＤとを照合することで，ユーザ認証を行う。以上により，ユーザＩＤを用いた認証が行われる（ステップ１０２）。

【００１７】

ユーザＩＤを用いた認証の結果がＯＫである場合，認証サーバ４２は，端末装置１に対してワンタイムパスワード（One-Time Password）を発行して認証を行う（ステップ１０３）。ワンタイムパスワードは，サービス提供者（企業）毎及びサービス提供者装置３－１～３－３毎に発行される。

【００１８】

以下，ワンタイムパスワード発行の手順について説明する。最初に，端

末装置１から前記ユーザ情報をデータベース４５に登録する初期登録時点において，認証サーバ４２は，ウエブサーバ４３を介してアクセス元の端末装置１に初期ワンタイムパスワード情報登録ＵＲＬを通知する電子メールを送信する。

【００１９】端末装置１のユーザは，初期ワンタイムパスワード情報登録ＵＲＬにおいて，認証サーバ４２からウエブサーバ４３を介して送られた図３のようなウエブページを見て，縦４個×横１２個のランダムパスワードの中から例えば４つを選択し，選択したパスワードを図３の「パスワード」と表示された箇所に入力する。縦４個×横１２個の各ランダムパスワードには，図４（ａ）に示すように，（Ａ，１）から（Ｄ，１２）までの座標が付与されている。

【００２０】

端末装置１のユーザは，例えば座標（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）を位置登録したい場合，これらの各座標位置に配置されているランダムパスワード，すなわち「６」，「３」，「４」，「１」を入力する。次に，認証サーバ４２からは図４（ｂ）に示すような２回目のランダムパスワードが送られる。端末装置１のユーザは，図４（ｂ）のランダムパスワードの配置を見て，前述の座標位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）に配置されているランダムパスワード，すなわち「３」，「２」，「０」，「２」を入力する。認証サーバ４２は，２回の入力により，ユーザによって選択されたランダムパスワードの位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）を確定し，確定した位置情報を前記ユーザ情報としてデータベース４５に登録する。

【００２１】

最後に，認証サーバ４２は，アクセス元の端末装置１のユーザ毎及びアクセス先のサービス提供者装置３－１～３－３毎に異なる前記第１のＵＲ

Ｌを通知する電子メールを，ウエブサーバ４３を介してアクセス元の端末装置１に送信する。以上で，初期登録が終了する。

【００２２】

次に，サービス提供を希望するユーザが前述のように第１のＵＲＬを用いて処理センタ装置４にアクセスした後（ステップ１０１），ステップ１０３において，認証サーバ４２から再び図３と同様のウエブページがアクセス元の端末装置１に送られる。このとき，縦４個×横１２個のランダムパスワードの配置は，初期登録時と異なるようになっている。端末装置１のユーザは，初期登録時に位置情報を登録したときと同位置にあるランダムパスワードを図３の「パスワード」と表示された箇所に入力する。

【００２３】

ここでは，例えば図５に示すような縦４個×横１２個のランダムパスワードが表示されたとする。この場合，端末装置１のユーザは，初期登録時に登録した座標（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）に配置されているランダムパスワード，すなわち「４」，「８」，「３」，「０」を順次入力する。認証サーバ４２は，ユーザによって入力されたパスワードの位置と初期登録時に登録された位置とを照合して，同一位置であれば，ユーザ本人と判断する。以上により，ワンタイムパスワードを用いた認証が行われる（ステップ１０３）。

…（以下略）…

(2) 上記(1)の記載から，甲１には，次の技術的事項が記載されているものと認められる。

ア　【００１８】には，「以下，ワンタイムパスワード発行の手順について説明する。」と記載され，【００１７】の記載によれば，ワンタイムパスワードは，認証サーバ４２が，端末装置１に対して，サービス提供装置３－１～３－３毎に発行するものであるから，甲１には，「ワンタイムパス

ワード発行の方法」が記載されている。

また，【０００７】の「本実施の形態のサービス提供システムは，ウエブブラウザを搭載した携帯電話機等の端末装置１と，移動体通信網２と，端末装置１に対してサービスを提供するサービス提供者装置３（３－１～３－３）と，移動体通信網２とサービス提供者装置３との間に設けられた処理センタ装置４とから構成される。」との記載，【００２３】の「認証サーバ４２は，ユーザによって入力されたパスワードの位置と初期登録時に登録された位置とを照合して，同一位置であれば，ユーザ本人と判断する。以上により，ワンタイムパスワードを用いた認証が行われる（ステップ１０３）。」との記載によれば，「端末装置」は，「サービス提供システム」においてユーザが使用するものであり，「ワンタイムパスワード」は，ユーザが「端末装置」を用いて，ユーザ認証を行うために入力するものであるから，甲１には，

「サービス提供システムにおける携帯電話機等の端末装置でユーザ認証を行うためのワンタイムパスワード発行の方法」

が記載されているものと認められる。

イ　【００１８】の「以下，ワンタイムパスワード発行の手順について説明する。最初に，端末装置１から前記ユーザ情報をデータベース４５に登録する初期登録時点において，認証サーバ４２は，ウエブサーバ４３を介してアクセス元の端末装置１に初期ワンタイムパスワード情報登録ＵＲＬを通知する電子メールを送信する。」との記載によれば，甲１には，

「初期登録時点において，認証サーバは，ウエブサーバを介してアクセス元の端末装置に初期ワンタイムパスワード情報登録ＵＲＬを通知する電子メールを送信」すること

が記載されているものと認められる。

ウ　【００１９】の「端末装置１のユーザは，初期ワンタイムパスワード情

報登録ＵＲＬにおいて，認証サーバ４２からウエブサーバ４３を介して送られた図３のようなウエブページを見て，縦４個×横１２個のランダムパスワードの中から例えば４つを選択し，選択したパスワードを図３の『パスワード』と表示された箇所に入力する。縦４個×横１２個の各ランダムパスワードには，図４（ａ）に示すように，（Ａ，１）から（Ｄ，１２）までの座標が付与されている。」との記載によれば，「端末装置」は電子メールにより受信した「初期ワンタイムパスワード情報登録ＵＲＬ」を用いて，「認証サーバ」の「ウエブページ」の「ランダムパスワード」をユーザが視認可能に表示するとともに，「ランダムパスワード」は（Ａ，１）から（Ｄ，１２）までの座標が付与された縦４個×横１２個の数字から構成され，さらに，【図３】によれば，「ランダムパスワード」の４個の数字群と数字群の間に数字以外の所定の記号が挿入されていると認められる。

また，「ランダムパスワード」から選択された数字は，「端末装置」に表示された「ランダムパスワード」近傍の「パスワード」と表示された箇所に入力されるのであるから，甲１には，

「端末装置は，初期ワンタイムパスワード情報登録ＵＲＬを用いて，認証サーバのウエブページの（Ａ，１）から（Ｄ，１２）までの座標が付与された縦４個×横１２個の数字からなるランダムパスワードを，４個の数字群と数字群の間に所定の記号を挿入して表示するとともに，『パスワード』と表示された箇所にユーザによって選択された複数の数字からなるランダムパスワードの入力を可能と」すること

が記載されているものと認められる。

エ　【００１９】の「端末装置１のユーザは，初期ワンタイムパスワード情報登録ＵＲＬにおいて，認証サーバ４２からウエブサーバ４３を介して送られた図３のようなウエブページを見て，縦４個×横１２個のランダムパスワードの中から例えば４つを選択し，選択したパスワードを図３の『パ

スワード』と表示された箇所に入力する。」との記載，【００２０】の「端末装置１のユーザは，例えば座標（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）を位置登録したい場合，これらの各座標位置に配置されているランダムパスワード，すなわち『６』，『３』，『４』，『１』を入力する。」との記載によれば，ユーザは，表示された「ランダムパスワード」の中から，登録したい位置にある「ランダムパスワード」を複数選択して入力するから，甲１には，

「ユーザは，端末装置に表示されているランダムパスワードに基づき，登録したい位置のランダムパスワードを入力」すること

が記載されているものと認められる。

オ　上記ウ及び【００２０】の「次に，認証サーバ４２からは図４（ｂ）に示すような２回目のランダムパスワードが送られる。端末装置１のユーザは，図４（ｂ）のランダムパスワードの配置を見て，前述の座標位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）に配置されているランダムパスワード，すなわち『３』，『２』，『０』，『２』を入力する。」との記載によれば，甲１には，

「端末装置は，認証サーバから送信される２回目のランダムパスワードを表示するとともに，ユーザによって選択される２回目のランダムパスワードの入力を可能と」すること

が記載されているものと認められる。

カ　上記エ，【００２０】の「端末装置１のユーザは，図４（ｂ）のランダムパスワードの配置を見て，前述の座標位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）に配置されているランダムパスワード，すなわち『３』，『２』，『０』，『２』を入力する。」との記載及び図４（ａ），（ｂ）によれば，ユーザは，表示された２回目の「ランダムパスワード」に基づき，先に入力したのと同じ位置の「ランダムパスワード」を複数選択して

入力しているから，甲１には，

「ユーザは，端末装置に表示されている２回目のランダムパスワードに基づき，登録したい位置のランダムパスワードを入力」すること

が記載されているものと認められる。

キ　上記ア及び【００２０】の「認証サーバ４２は，２回の入力により，ユーザによって選択されたランダムパスワードの位置（A，3），（B，7），（C，４），（D，９）を確定し，確定した位置情報を前記ユーザ情報としてデータベース４５に登録する。」との記載によれば，「認証サーバ」は「端末装置」からユーザが入力した２回の「ランダムパスワード」から共通する複数の「位置情報」を確定し，確定された「位置情報」が「ユーザ情報」の１つである「ワンタイムパスワード」として「データベース」に登録されるから，甲１には，

「認証サーバは，端末装置からの２回の入力により，ユーザによって選択されたランダムパスワードの複数の位置情報を確定し，確定した前記位置情報をワンタイムパスワードとしてデータベースに登録」すること

が記載されているものと認められる。

ク　上記ウ及び【００２２】の「次に，サービス提供を希望するユーザが前述のように第１のＵＲＬを用いて処理センタ装置４にアクセスした後（ステップ１０１），ステップ１０３において，認証サーバ４２から再び図３と同様のウエブページがアクセス元の端末装置１に送られる。このとき，縦４個×横１２個のランダムパスワードの配置は，初期登録時と異なるようになっている。端末装置１のユーザは，初期登録時に位置情報を登録したときと同位置にあるランダムパスワードを図３の『パスワード』と表示された箇所に入力する。」との記載によれば，ここでのランダムパスワードの配置を含む「図３と同様のウエブページ」は，サービス提供時のユーザ認証において表示されるものであり，ユーザ認証を行う時点においては，

初期登録時と「縦４個×横１２個の数字からなるランダムパスワード」の配置が異なるように表示されるから，甲１には，

「ユーザ認証を行う時点においては，前記端末装置は，縦４個×横１２個の数字からなるランダムパスワードに，４個の数字群と数字群の間に所定の記号を挿入して，初期登録時とランダムパスワードの配置が異なるように表示するとともに，『パスワード』と表示された箇所にユーザによって選択された複数の数字からなるランダムパスワードの入力を可能と」すること

が記載されているものと認められる。

ケ　【００２３】の「ここでは，例えば図５に示すような縦４個×横１２個のランダムパスワードが表示されたとする。この場合，端末装置１のユーザは，初期登録時に登録した座標（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）に配置されているランダムパスワード，すなわち『４』，『８』，『３』，『０』を順次入力する。認証サーバ４２は，ユーザによって入力されたパスワードの位置と初期登録時に登録された位置とを照合して，同一位置であれば，ユーザ本人と判断する。以上により，ワンタイムパスワードを用いた認証が行われる（ステップ１０３）。」との記載によれば，ユーザ認証を行う時点においては，ユーザによって入力されたランダムパスワードの複数の位置情報と初期登録時に登録された位置の位置情報とが，同一位置であるかどうかで判断して，ユーザ認証しているから，甲１には，

「認証サーバは，ユーザによって入力されたランダムパスワードの複数の位置情報と初期登録時に登録された複数の位置情報とを照合して，同一位置であれば，ユーザ本人と判断する」こと

が記載されているものと認められる。

(3) 以上を総合すれば，甲１には，次の発明が記載されているものと認められる（下線部が審決の認定と異なる部分である。以下，かかる発明をもって「甲

１発明」という。）。

「サービス提供システムにおける携帯電話機等の端末装置でユーザ認証を行うためのワンタイムパスワード発行の方法であって，

初期登録時点において，認証サーバは，ウエブサーバを介してアクセス元の端末装置に初期ワンタイムパスワード情報登録ＵＲＬを通知する電子メールを送信し，

前記端末装置は，前記初期ワンタイムパスワード情報登録ＵＲＬを用いて，前記認証サーバのウエブページの（Ａ，１）から（Ｄ，１２）までの座標が付与された縦４個×横１２個の数字からなるランダムパスワードを，４個の数字群と数字群の間に所定の記号を挿入して表示するとともに，『パスワード』と表示された箇所にユーザによって選択された複数の数字からなるランダムパスワードの入力を可能とし，

前記ユーザは，前記端末装置に表示されているランダムパスワードに基づき，登録したい位置のランダムパスワードを入力し，

前記端末装置は，前記認証サーバから送信される２回目のランダムパスワードを表示するとともに，前記ユーザによって選択される２回目のランダムパスワードの入力を可能とし，

前記ユーザは，前記端末装置に表示されている２回目のランダムパスワードに基づき，前記登録したい位置のランダムパスワードを入力し，

前記認証サーバは，前記端末装置からの２回の入力により，前記ユーザによって選択されたランダムパスワードの複数の位置情報を確定し，確定した前記位置情報をワンタイムパスワードとしてデータベースに登録し，

ユーザ認証を行う時点においては，前記端末装置は，縦４個×横１２個の数字からなるランダムパスワードに，４個の数字群と数字群の間に所定の記号を挿入して，初期登録時とランダムパスワードの配置が異なるように表示するとともに，『パスワード』と表示された箇所にユーザによって選択され

た複数の数字からなるランダムパスワードの入力を可能とし，

前記認証サーバは，ユーザによって入力されたランダムパスワードの複数の位置情報と初期登録時に登録された複数の位置情報とを照合して，同一位置であれば，ユーザ本人と判断する，方法。」

3　第１事件の取消事由１（発明の同一性の認定の誤り）について

(1) 原告は，本件発明８及び９は，先願の甲１発明と同一であり，この点に関する審決の認定判断に誤りがあると主張するので，以下検討する。

(2) 本件発明８について

ア　本件発明８の構成は，前記第２の２の【請求項８】のとおりであり，甲１発明の構成は，前記２(3)のとおりである。

イ　上記各構成を対比すると，以下のとおりとなる。

(ｱ) 甲１発明の「ワンタイムパスワード」は，「サービス提供システムにおける携帯電話機等の端末装置でユーザ認証を行う」ためのものであって，「認証サーバは，前記端末装置からの２回の入力により，前記ユーザによって選択されたランダムパスワードの複数の位置情報を確定し，確定した前記位置情報をワンタイムパスワードとしてデータベースに登録」することから，「ワンタイムパスワード」は「ユーザによって選択されたランダムパスワードの複数の位置情報」に基づき決定されるものである。

一方，本件発明８の「パスワード」は，ユーザ認証に用いられるものであって，「パスワード導出パターン」によって導出され，「パスワード導出パターン」は，「入力されたキャラクタに基づいて特定され」るから，甲１発明の「ワンタイムパスワード」及び「ユーザによって選択されたランダムパスワードの複数の位置情報」は，それぞれ，本件発明１の「パスワード」及び「パスワード導出パターン」に相当する。

また，甲１発明の「サービス提供システム」は，「携帯電話機等の端

末装置」と「認証サーバ」とを含み，「携帯電話機等の端末装置」と「認証サーバ」とは，通信回線を介して接続されていることは明らかである。

そうすると，甲１発明の「携帯電話機等の端末装置」と「認証サーバ」とを含む「サービス提供システム」において，「端末装置でユーザ認証を行うためのワンタイムパスワード発行」を行い，「初期登録時点において，」「確定した位置情報」を「データベースに登録」する「サービス提供システム」は，本件発明８の構成要件Ｅ，すなわち，「端末装置と，前記端末装置と通信回線を介して接続されたサーバとを含む，ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録システム」に相当する。

(ｲ) 甲１発明において，「携帯電話機等の端末装置」は，「前記初期ワンタイムパスワード情報登録ＵＲＬを用いて，前記認証サーバのウエブページの（Ａ，１）から（Ｄ，１２）までの座標が付与された縦４個×横１２個の数字からなるランダムパスワードを，４個の数字群と数字群の間に所定の記号を挿入して表示する」から，「ランダムパスワード」は，（Ａ，１）から（Ｄ，１２）までの座標を有する縦４個×横１２個で構成されるマトリックスの要素のそれぞれに数字を割り当てたマトリックスを表示したものであるといえる。

よって，甲１発明の「数字」，「『（Ａ，１）から（Ｄ，１２）までの座標を有する縦４個×横１２個』で構成されるマトリックス」及び「縦４個×横１２個の数字からなるランダムパスワード」は，それぞれ，本件発明８の「キャラクタ」，「所定のパターン」及び「提示用パターン」に相当する。

また，甲１発明は，「『パスワード』と表示された箇所にユーザによって選択された複数の数字からなるランダムパスワードの入力を可能と」するものであり，ユーザは，「縦４個×横１２個の数字からなるランダ

ムパスワード」の中から，特定の「座標」の「ランダムパスワード」に割り当てられた「数字」を選択して入力することは明らかである。

そうすると，甲１発明の「前記端末装置は，前記初期ワンタイムパスワード情報登録ＵＲＬを用いて，前記認証サーバのウエブページの（Ａ，１）から（Ｄ，１２）までの座標が付与された縦４個×横１２個の数字からなるランダムパスワードを，４個の数字群と数字群の間に所定の記号を挿入して表示するとともに，『パスワード』と表示された箇所にユーザによって選択された複数の数字からなるランダムパスワードの入力を可能と」することは，本件発明８の構成要件Ｆ，すなわち，「前記端末装置は，複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを無線端末装置が表示し，これにより，前記提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す手段」を有することに相当する。

(ｳ) 甲１発明において，「ユーザは，前記端末装置に表示されているランダムパスワードに基づき，登録したい位置のランダムパスワードを入力」すると，「前記端末装置は，前記認証サーバから送信される２回目のランダムパスワードを表示」し，「認証サーバは，前記端末装置からの２回の入力により，前記ユーザによって選択されたランダムパスワードの複数の位置情報を確定」するものであり，ここで，「端末装置」は「ユーザによって選択されたランダムパスワードの複数の位置情報」が確定されるまで，２回繰り返して「縦４個×横１２個の数字からなるランダムパスワード」を表示することは明らかであるから，甲１発明では，入力された「数字」に基づいて「ユーザによって選択されたランダムパスワードの複数の位置情報」が特定されるまで，新たな「縦４個×横１２個の数字からなるランダムパスワード」を「端末装置」が表示する処理を繰り返し行うといえる。

また，甲１発明は，「『パスワード』と表示された箇所にユーザによって選択された複数の数字からなるランダムパスワードの入力を可能とし」，ランダムパスワードの入力をした後に，「端末装置は，前記認証サーバから送信される２回目のランダムパスワードを表示するとともに，前記ユーザによって選択される２回目のランダムパスワードの入力を可能と」するものであり，ここで，２回繰り返して「縦４個×横１２個の数字からなるランダムパスワード」を表示し，ユーザに登録したい位置の「数字」の入力を促すことは明らかであるから，甲１発明では，「縦４個×横１２個の数字からなるランダムパスワード」の中から，特定の「座標」の「ランダムパスワード」に割り当てられた「数字」の入力を促す処理を繰り返すといえる。

そうすると，甲１発明の「ユーザは，前記端末装置に表示されているランダムパスワードに基づき，登録したい位置のランダムパスワードを入力し，前記端末装置は，前記認証サーバから送信される２回目のランダムパスワードを表示するとともに，前記ユーザによって選択される２回目のランダムパスワードの入力を可能とし，前記ユーザは，前記端末装置に表示されている２回目のランダムパスワードに基づき，前記登録したい位置のランダムパスワードを入力」することは，本件発明８の構成要件Ｇ，すなわち，「前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，新たな提示用パターンを表示する処理を繰り返し，これにより，前記新たな提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す処理を繰り返す手段」を有することに相当する。

(ｴ) 甲１発明は，「認証サーバは，前記端末装置からの２回の入力により，前記ユーザによって選択されたランダムパスワードの複数の位置情報を確定し，確定した前記位置情報をワンタイムパスワードとしてデータベ

ースに登録」するものであり，上記(ｱ)から，甲１発明の「ユーザによって選択されたランダムパスワードの複数の位置情報」，「携帯電話等の端末装置」及び「認証サーバ」は，それぞれ，本件発明８の「パスワード導出パターン」，「端末装置」及び「サーバ」に相当する。

そして，甲１発明では，「端末装置」と通信回線を介して接続され，ユーザにより入力された「数字」に基づいて特定された「ユーザによって選択されたランダムパスワードの複数の位置情報」を「データベース」に登録するが，当該「複数の位置情報」を「データベース」に登録するに当たり，ユーザによる“パスワード導出パターン”の登録確認を行うことについては特定されていない。

一方，本件発明８は，ユーザによる「パスワード導出パターン」の確認のための構成として，「前記パスワード導出パターンが特定されたとき，前記特定されたパスワード導出パターンを含む登録確認画面を前記無線端末装置が表示して，これにより，前記パスワード導出パターンを登録するか又は前記表示及び入力を最初からやり直すかの選択を促す手段」が特定され，さらに，「前記パスワード導出パターンが特定され」ると，「前記端末装置と通信回線を介して接続されたサーバは，前記登録が選択されたとき，前記特定されたパスワード導出パターンを登録させるための手段を備える」ことが特定されている。

そうすると，甲１発明の「認証サーバは，前記端末装置からの２回の入力により，前記ユーザによって選択されたランダムパスワードの複数の位置情報を確定し，確定した前記位置情報をワンタイムパスワードとしてデータベースに登録」することと，本件発明８の構成要件Ｈ，すなわち，「前記パスワード導出パターンが特定されたとき，前記特定されたパスワード導出パターンを含む登録確認画面を前記無線端末装置が表示して，これにより，前記パスワード導出パターンを登録するか又は前

記表示及び入力を最初からやり直すかの選択を促す手段」と，構成要件Ｉ，すなわち，「前記端末装置と通信回線を介して接続されたサーバは，前記登録が選択されたとき，前記特定されたパスワード導出パターンを登録させるための手段を備える」こととは，後記の相違点があるものの，「前記端末装置と通信回線を介して接続されたサーバは，前記パスワード導出パターンが特定されると，前記特定されたパスワード導出パターンを登録させるための手段」を有する点で一致する。

ウ　以上の対比によれば，本件発明８と甲１発明の間には，次の一致点及び相違点が認められる。

(ｱ) 一致点

「端末装置と，前記端末装置と通信回線を介して接続されたサーバとを含む，ユーザ認証に用いられるパスワードを導出するためのパスワード導出パターンの登録システムであって，

前記端末装置は，複数の要素から構成される所定のパターンの要素のそれぞれに所定のキャラクタを割り当てた提示用パターンを表示し，これにより，前記提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促すための手段と，

前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，新たな提示用パターンを表示する処理を繰り返し，これにより，前記新たな提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す処理を繰り返す手段と，

を有し，

前記端末装置と通信回線を介して接続されたサーバは，

前記パスワード導出パターンが特定されると，前記特定されたパスワード導出パターンを登録させるための手段を備える，

パスワード導出パターンの登録システム。」

(ｲ) 相違点

本件発明８は，「前記パスワード導出パターンが特定されたとき，前記特定されたパスワード導出パターンを含む登録確認画面を前記無線端末装置が表示して，これにより，前記パスワード導出パターンを登録するか又は前記表示及び入力を最初からやり直すかの選択を促す手段」(構成要件H）を備え，「前記端末装置と通信回線を介して接続されたサーバは，前記登録が選択されたとき，前記特定されたパスワード導出パターンを登録させる」（構成要件Ｉ）のに対して，甲１発明では，「サーバ」（認証サーバ）は，「特定されたパスワード導出パターンを登録させるための手段」を有するものの，「特定されたパスワード導出パターン」（ユーザによって選択された複数の位置とその選択順序の情報）を含む登録確認画面を無線端末装置に表示して，前記パスワード導出パターンを登録するか又は前記表示及び入力を最初からやり直すかの選択を促す手段，及び，前記登録が選択されたとき，前記特定されたパスワード導出パターンを登録させる手段を備えていない点。

エ　相違点についての検討

(ｱ) 上記相違点について検討すると，甲１発明では，ユーザにより入力された「数字」に基づいて「特定されたパスワード導出パターン」，すなわち，「ユーザによって選択された複数の位置情報」を「データベース」に登録するものであり，当該「複数の位置情報」を「データベース」に登録するに当たり，「特定されたパスワード導出パターン」である「複数の位置とその選択順序の情報」を「端末装置」に表示し，ユーザによる確認を行うことについて開示も示唆もない。

(ｲ) また，以下に検討するとおり，当該技術が当該技術分野において周知慣用技術であったともいえない。

すなわち，原告が周知慣用技術であることの裏付けとして提出した関

係各証拠について検討すると，まず，甲７３（特開平９－６０２９６号公報）は，鉄骨建入れ検査システムにおける計測データの入力の確認，甲７４（特開２０００－３２２６４６号公報）は，インターネットを利用した商品の販売方法における利用者のユーザ情報登録の確認，甲７５（特開２０００－３１１２００号公報）及び甲７６（特開２０００－２４２７１１号公報）は，ネットワークを介した贈り物を仲介する技術における商品の登録の確認，甲７７（特開２０００－５７２１３号公報）及び甲７８（特開平１０－２３２８９３号公報）は，インターネットを介した求人求職情報交換システムに関し，求職会員が入力した情報内容の確認に関するものであり，いずれも，パスワードの登録の確認に関する技術ではない。

また，甲１５（特開平９－２３１１７２号公報）は，コンピュータの提案したパスワードをユーザが承認して，仮パスワードとして決定するものであり，コンピュータがパスワードを提示するものであって，ユーザが入力したパスワードを確認するために表示するものではない。

甲１６（特開平１０－４９５９６号公報）及び甲１７（特開平１１－２２７２６７号公報）は，ユーザが入力したパスワードをそのまま表示し，確認して登録するものである。

甲１８（特開２０００－３５３１６４号公報）には，入力したパスワードが入力枠に表示されることは記載されておらず，２回のパスワードの入力が一致した場合にパスワードを登録するものであって，表示により登録確認をするものではない。

甲１９（特開２００１－９２７８５号公報）には，パスワード認証装置及びパスワード認証方法に関し，画面上を升目状に分割したグリッドをグリッドプレーンに配置し，認証用画像とグリッドプレーンを合成したパスワード入力映像を表示し，グリッドの選択順序をパスワードとし

て設定するパスワード認証方法（【００３０】ないし【００３６】）が記載され，パスワード登録画面には，パスワードの登録時に，グリッドを選択すると，選択されたグリッドが表示され，「パスワード入力終了」ボタンを押すと，終了する（図３）ことが記載されている。しかし，甲１９は，パスワードとしてグリッドの位置を登録する際に，登録するグリッドの位置を表示して確認するものではあるが，それ自体は公知技術にすぎず，甲１９のみをもって，パスワード導出パターンを，ユーザによって選択された複数の位置とその選択順序を確認できるように表示することが周知技術であるとはいえない。そして，このような周知技術とはいえない単なる公知技術に基づいて，甲１の記載を補充して，特許法２９条の２の先願発明との同一性を判断することは相当でない。

甲２（平成１９年３月８日付けQの宣誓供述書）の添付資料６（平成１３年１１月１日付けモバイルコネクトサービス操作説明書）及び甲７（日経インターネットテクノロジー平成１３年１２月号）には，ＮＴＴコム社による甲１発明の実施においては，「Ｇｏ！」，「やり直し」という，「パスワード導出パターンを登録するか，最初からやり直すか」を選択するためのボタンが示されている。

しかしながら，ＮＴＴコム社において公然実施された「Ｇｏ！」ボタン，「やり直し」ボタンは，本件特許の出願前の公然実施発明であり周知技術とはいえず，このような周知技術とはいえない単なる公知技術に基づいて先願明細書等の記載を補充して，特許法２９条の２の先願発明との同一性の判断することは相当でない。

(ｳ) 以上のとおり，原告が提出した証拠のうち，パスワードの登録に関し，入力されたパスワードの確認表示を行う周知技術についての文献は，甲１６及び１７のみであるところ，これらは，いずれもパスワードの登録に関して，入力されたパスワードの数字をそのまま表示して確認をする

ことが周知技術であることを示すものである。これを本件発明８に関していえば，「キャラクタの入力」を表示確認することが周知技術であることを示すものであり，具体的には，本件明細書の図１９（ａ），（ｂ），（ｃ）の４桁の数字（キャラクタ）を入力し，入力した数字（キャラクタ）を画面に表示し，確認して「ＯＫ」ボタンを押すことが周知技術であることを示す文献である。

しかし，ユーザが入力したキャラクタ等を表示することと，ユーザが入力したキャラクタに基づいて特定されたパスワード導出パターンを表示することとは異なるから，これらの文献に記載された周知技術を参酌しても，本件発明８の構成要件である，「パスワード導出パターンが特定されるまで」「キャラクタの入力」を繰り返し，「入力されたキャラクタに基づいて」，「前記パスワード導出パターンが特定されたとき，前記特定されたパスワード導出パターンを含む登録確認画面を前記無線端末装置が表示」することが甲１に記載されているに等しい事項とすることはできない。

また，甲７３ないし７８，甲１５ないし１９の各文献には，パスワードの登録確認画面において，「前記表示及び入力を最初からやり直す」かの選択を促す手段については，開示も示唆もされていない。

(ｴ) そうすると，甲１には，「特定されたパスワード導出パターン」を，ユーザによって選択された複数の位置とその選択順序を確認できるように表示することについて開示も示唆もなく，当該技術は，当該技術分野における周知慣用技術とは認められないから，上記相違点は周知慣用技術の付加などではなく，甲１発明と本件発明８は，実質同一であるとはいえない。

(3) 本件発明９について

本件発明９の構成は，前記第２の２の【請求項９】のとおりであるところ，

本件発明９は本件発明８に従属するものであり，上記のとおり，甲１発明と本件発明８は実質同一ではないから，甲１発明と本件発明９も実質同一とはいえない。

(4) 以上のとおり，本件発明８及び９は，いずれも甲１発明と同一とはいえないから，この点に関する審決の認定判断に誤りがあるとはいえない。

よって，原告が主張する取消事由１は理由がない。

４　第１事件の取消事由２（特許法１３１条の２第２項の裁量権の逸脱・濫用の有無）について

原告は，種々理由を述べて，本件審判手続において，原告が無効理由を追加すべく本件補正の許可を求めたのに対し，審判長がこれを認めなかったことには，特許法１３１条の２第２項において認められた裁量権を逸脱・濫用した違法がある，と主張する。

しかしながら，原告が許可を求めた本件補正が要旨変更に当たることについては原告自身も争っていないところ，同項に基づいて審判長が行う請求の理由の補正の許否の判断は，たとえ不許可の決定がされたとしても，審判請求人はいつでも同一の理由に基づいて別途無効審判を請求できることから，不服を申し立てることができないものとされており（同条の２第４項），これによれば，その許否の判断の当否については，そもそも審決の取消事由に当たらないというべきである。

さらにいえば，平成２９年９月４日付け審判請求弁駁書（甲７０）における本件無効審判の請求の理由の補正は，特許法３８条の共同出願要件違反を無効理由として追加するものであるが，そもそも，かかる無効理由に基づく特許無効審判は，特許を受ける権利を有する者に限り請求できるものとされている（特許法１２３条２項括弧書）ことからすると，これに当たらない原告（原告が本件発明に係る特許を受ける権利を有する者でないことは明らかである。）が本件審判手続においてかかる無効理由を主張することが許されないこともまた明

らかというべきである。したがって，その意味においても，本件補正を認めなかった審判合議体の判断に誤りはない。

なお，原告は，上記弁駁書において，本件特許は特許法の平成２３年改正前に出願されたものであるから，同法１２３条２項ただし書（括弧書の誤りと認める。）の適用はないとも主張しているが，本件無効審判の請求日は，平成２７年１１月２７日であるところ，同年４月１日以降の無効審判の請求については，全て同項の適用がある（平成２６年法律第３６号による改正附則２条１７項参照）のであるから，上記主張は誤解に基づくというべきである。

以上の次第であるから，原告が主張する無効理由２は理由がない。

５　第２事件の取消事由１（甲１発明の認定の誤り）について

(1) 被告は，甲１発明は，端末装置からの２回の入力によっては，ユーザによって選択された４個のランダムパスワードの位置情報を確定することができないのであるから，審決が，甲１発明について，認証サーバは，端末装置からの２回の入力により，ユーザによって選択されたランダムパスワードの複数の位置情報を確定し，確定した前記位置情報をワンタイムパスワードとしてデータベースに登録するものと認定したのは誤っている，と主張する。

(2) そこで検討するに，甲１の【００２０】には，「端末装置１のユーザは，例えば座標（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）を位置登録したい場合，これらの各座標位置に配置されているランダムパスワード，すなわち『６』，『３』，『４』，『１』を入力する。次に，認証サーバ４２からは図４（ｂ）に示すような２回目のランダムパスワードが送られる。端末装置１のユーザは，図４（ｂ）のランダムパスワードの配置を見て，前述の座標位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）に配置されているランダムパスワード，すなわち『３』，『２』，『０』，『２』を入力する。認証サーバ４２は，２回の入力により，ユーザによって選択されたランダムパスワードの位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）を

確定し，確定した位置情報を前記ユーザ情報としてデータベース４５に登録する。」と記載されている。

他方で，図４（ａ）（ｂ）に示されるランダムパスワードに対し，上記【００２０】に記載された，１回目に「６」，「３」，「４」，「１」を入力し，２回目に「３」，「２」，「０」，「２」を入力すると，ランダムパスワードの位置は，（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）以外に，（Ａ，１０），（Ｃ，６）にも該当するから，２回の入力では位置登録したい（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）には確定しない。

しかしながら，前記２(2)及び(3)のとおり，甲１の記載全体を総合すれば，甲１には，「２回の入力により，ユーザによって選択されたランダムパスワードの位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）を確定」すること，すなわち，２回の入力（４つの数字の入力）によって，ランダムパスワードの４つの位置が確定することが記載されていると認めるのが相当であり，被告が指摘する明細書の記載と図面との不整合は，甲１の出願時，明細書及び図面を作成する際に，図４（ａ）（ｂ）の座標位置（Ａ，３），（Ｂ，７），（Ｃ，４），（Ｄ，９）については，明細書の記載と整合するように作成されたが，それ以外の座標位置については，適当に数字を割り当てて作成されたため，誤った記載となったもの，すなわち，明細書及び図面を作成する際の不注意による誤りであると理解することが可能である（そうでなければ，２回の入力によっても位置が確定しない場合のことについて，何らかの記載があってしかるべきであるが，甲１にそのような記載はない。）。

そうすると，審決が，甲１の【００２０】の記載等に基づいて，「前記認証サーバは，前記端末装置からの２回の入力により，前記ユーザによって選択されたランダムパスワードの複数の位置情報を確定し，確定した前記位置情報をワンタイムパスワードとしてデータベースに登録し」と，甲１発明を認定した点に誤りはないというべきであり，これに反する被告の主張は採用

できない。

(3) 以上の次第であるから，被告が主張する取消事由１は理由がない。

６　第２事件の取消事由２（一致点及び相違点の認定の誤り）及び取消事由３（発明の同一性の認定の誤り）について

(1) 被告は，取消事由１で主張したとおり審決が甲１発明の認定を誤ったことを前提に，①審決は，かかる甲１発明の認定誤りに起因して本件発明と甲１発明との一致点及び相違点の認定を誤り，その結果，本件発明１と甲１発明との同一性の判断を誤った，②本件発明１（請求項１）を直接又は間接に引用する本件発明２ないし７（請求項２ないし７）についても，審決は，同じように本件発明との一致点及び相違点の認定を誤り，甲１発明との同一性の判断を誤った，などと主張する。

しかしながら，被告が主張する取消事由１に理由がないことは上記５のとおりであるから，これを前提とする上記主張も理由がないは明らかである。

(2) 本件発明４固有の認定誤りを主張する点について

被告は，要するに，本件発明４は，同発明の数式（当該数式）の左辺の方が右辺よりも大きくなる場合を排除することにより，従来型のパスワードより安全性が低くなるマトリックスを排除することとし，その前提として，パスワード導出パターンの利用に際してユーザは同じ位置の要素を選択しないという傾向が見られることに鑑みて，従来型のパスワードの数字の組合せの総数とマトリックスの大きさに基づく順列の総数との関係を規定するものであるのに対し，甲１のどこにもそのような記載はない（甲１発明は，縦４個×横１２個のランダムパスワードの中から例えば４つを選択すること以上のことを開示していない）ことなど，技術的思想の違いを種々指摘して，審決が，甲１発明の「縦４個×横１２個の数字からなるランダムパスワード」と本件発明４の「提示用パターン」とに実質的な違いはないとして，両発明の同一性を認めたのは誤りである，と主張する。

しかしながら，甲１の【００１９】の記載に鑑みれば，甲１には，縦４個×横１２個のランダムパスワードの中から４つのパスワード（数字）を任意に選択する構成が開示されており，「４つ」選択するものとされている以上は，それぞれ別の場所を選択するのが通常であるから，本件発明４と同様に，ユーザは同じ位置の要素を選択しないことが前提とされているということができるし，現に，本件発明４の数式（当該数式）を充足する実施例が甲１に記載されていること，すなわち，甲１に記載がある，縦４個×横１２個のランダムパスワードの中から４つを選択する場合（Ｋ＝４，Ｌ＝ｌ２，Ｊ＝４の場合）に，本件発明４の数式（当該数式）を充足する結果となることそれ自体は，被告も積極的に争ってはいない。

そうである以上，上記審決の認定判断に誤りはないというべきであり，この点に関する被告の主張はいずれにしても理由がない。

(3) 以上の次第であるから，被告が主張する取消事由２及び３は，いずれも理由がない。

7　第２事件の取消事由４（発明者同一の認定の誤り）について

(1) 被告の主張は，要するに，先願である甲１発明の発明者が後願である本件発明の発明者（被告代表者であるＰ）と同一であるとの被告主張を認めず，特許法２９条の２本文括弧書（発明者同一）の適用を認めなかった審決の認定判断に誤りがある，とするものである。

そこで検討するに，上記括弧書は，先後願の発明者が同一である場合には拡大先願（特許法２９条の２本文）の適用外とする例外規定であって，その性格は，ただし書が規定する出願人同一の場合と何ら変わらないといえること，本件の場合，願書上，本件発明の発明者はＰとされている一方で，先願である甲１発明の発明者はＮＴＴコム社のＱとされており（甲１，８），少なくとも願書上先後願の発明者が同一とはいえないことは明らかであるのに，被告において，あえてこれと異なる主張を行うものであることからすれば，

まずは，例外規定である上記括弧書の適用を求めて，先願である甲１発明の発明者につき上記願書の記載とは異なる主張を行う被告において，甲１発明の真の発明者が後願である本件発明の発明者と同じＰであるという点について具体的に主張立証を行う必要があるというべきである。

この点，甲１発明の従来技術に対する課題は，携帯電話機のように画面が小さく，入力方法に制限があっても，簡単にパスワード導出パターンを登録できるようにすることにあり，同発明の特徴的部分は，主として，①携帯電話（ｉモード）の限られた画面で操作できるように，マトリックスを４×１６から４×１２とした点，②マトリックス表の個々の升目に表示される数字を１桁とした点，及び③１回の入力ではワンタイムパスワードを確定できないことから，２回の入力により，ユーザが選択したランダムパスワードの複数の位置情報を確定するものとした点にあると認められるところ（甲１０，２３ないし２５等），ベース社のＲの陳述書（甲１０）によれば，少なくとも，上記①及び②の点に関しては，同人の積極的な関与（具体的な提案等）が認められるというべきであるし，上記③の点に関しても，同陳述書に「私の方からパスワード導出パターンについて数字の入力を２回繰り返すことで登録することが可能か，セキュアプロバイダ社に打診した」とあることからすると，やはり同人の関与がうかがわれる（少なくとも，これらの関与が事実に反するとして完全に否定できるだけの証拠はない。）。

また，甲１発明は，そもそも，ＮＴＴコム社のサービスであるモバイルコネクトサービスのユーザ認証システムの開発プロジェクトにおいて着想及び具体化されたものであるところ，同社のＱにおいて，携帯電話（ｉモード）の画面でも一見してパスワードの位置が記憶しやすいものとする，簡単で分かりやすい操作で登録できるようにするとの要件定義をし，これが同社のプロジェクトチームのメンバーからベース社及びセキュア社（被告）に対して提示された上で，個々の検討が進められていたものと認められる（甲３５，

弁論の全趣旨）。

以上によれば，甲１発明に関しては，ＮＴＴコム社のＱによる上記要件定義の下，ベース社のＲや被告のＰを含む上記プロジェクトチームのメンバーが互いに知恵を出し合い，協力し合って開発に当たっていたことが容易に推察できる一方で，同発明がＰの単独発明であること（上記①ないし③の提案等，発明の着想及び具体化を行ったのが同人のみであって，プロジェクトチームの他のメンバーが実質的に関与していないこと）を認めるに足りる的確な証拠（客観的かつ具体的な証拠）は存在しない。

したがって，甲１発明の発明者がＰである（甲１発明の着想及び具体化を行ったのがＰのみである）と認めるには足りないというべきであり，これと同旨をいう審決の認定判断に誤りがあるものとは認められない。

(2) 被告の主張について

ア　これに対し，被告は，Ｐがパスワード導出パターンの登録方法について，それまでに発案していたもの，あるいは構想していた複数のパスワード登録方法をｉモードに適するように具現化し，平成１２年１２月，方式Ｃを含む「ｉモードでのＯＦＦＩＣ利用開始手順案」（甲２２）にまとめあげて，これをセキュア社の担当者から，ＮＴＴコム社の担当者に対し，電子メールにて送信した，などと主張する。

しかしながら，甲２２の方式Ｃの説明文書が，いつ，どのような形で作成され，プロジェクトチームの他のメンバーに伝達されたかは争いがある上に，そもそも，そこに記載されている方式Ｃの手順がプロジェクトチームでの議論を反映することなく，専ら被告（Ｐ）によって着想及び具体化されたという事実自体を認めるに足る的確な証拠がない。

したがって，被告の上記主張は採用できない。

イ　被告は，ほかにも，①Ｐ以外の者の方式Ｃの特徴的部分への関与がないとか，②ＮＴＴコム社が被告からワンタイムパスワード認証特許のライセ

ンスを得ているなどと主張するが，①の主張が証拠から認められる事実関係に必ずしも合致しないことは上記(1)のとおりであるし，②の主張についても，ワンタイムパスワード認証特許自体は被告が所有するものであり，ＮＴＴコム社としては，自社の提供するサービスに同認証技術を使用する以上，被告からライセンスを得ることは当然であって，そのことと，携帯電話による初期登録に係る甲１発明がＰ単独によるものであるか否かは全く関係がないというべきである。

また，被告は，審決が４桁の数字群と数字群の間に何か記号等を入れることを取り込んで甲１発明を認定しているのは不当であるとも指摘するが，審決はかかる認定のみに基づいて発明者の同一性を判断しているわけではないから，失当である。

ウ　その他被告がるる主張する点は，いずれも上記(1)の認定判断を覆すには足りないものであり，審決の取消事由として採用することはできない。

(3) 以上の次第であるから，被告が主張する取消事由４は理由がない。

８　結論

以上のとおり，原告が主張する取消事由１及び２並びに被告が主張する取消事由１ないし４はいずれも理由がなく，審決に取り消されるべき違法はない。

よって，原告の第１事件に係る請求及び被告の第２事件に係る請求をいずれも棄却することとし，主文のとおり判決する。

知的財産高等裁判所第３部

裁判長裁判官

鶴　　岡　　稔　　彦

裁判官

寺　　田　　利　　彦

裁判官

間　　明　　宏　　充

（別紙）訂正請求の内容

本件訂正の内容は，平成２９年６月１２日提出の訂正請求書に添付の訂正特許請求の範囲に記載された以下のとおりのものである。

１　請求項１ないし７からなる一群の請求項に係る訂正

（訂正事項１）

特許請求の範囲の請求項１に「前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，新たな提示用パターンを前記無線端末装置が表示する処理を繰り返し行い，」とあるのを，「前記入力されたキャラクタに基づいて，前記入力されたキャラクタの数に等しい数の要素からなるパスワード導出パターンが２回で特定されるように，新たな提示用パターンを前記無線端末装置が表示する処理を繰り返し行い，」に訂正する。

（訂正事項２）

特許請求の範囲の請求項４に「前記所定のパターンは，マトリックスであり，」とあるのを，「前記所定のパターンは，Ｋ行Ｌ列のマトリックスであり，」に訂正する。

（訂正事項３）

特許請求の範囲の請求項４に「前記提示用パターンは，マトリックスの各要素に０～９までの整数を割り当てたものである，」とあるのを，「前記提示用パターンは，前記Ｋ行Ｌ列のマトリックスの各要素に０～９までの整数を割り当てたものであり，」に訂正する。

（訂正事項４）

特許請求の範囲の請求項４に「前記提示用パターンは，マトリックスの各要素に０～９までの整数を割り当てたものである，」とあるのを，その記載の直後に，「前記Ｋ行Ｌ列のマトリックスは，前記所定のキャラクタの数字列がＪ桁のとき，

以下の数式：

１０＾Ｊ＜（Ｋ＊Ｌ）＊（Ｋ＊Ｌ－１）・・（Ｋ＊Ｌ－Ｊ＋１）

に従って，構成される，」との記載を追加する。

２　請求項８及び９からなる一群の請求項に係る訂正

（訂正事項５）

特許請求の範囲の請求項８に「前記入力されたキャラクタに基づいてパスワード導出パターンが特定されるまで，新たな提示用パターンを表示する処理を繰り返し，これにより，前記新たな提示用パターンについての特定の要素に割り当てられたキャラクタの入力を促す処理を繰り返す手段と，」とあるのを，その記載の直後に，「前記パスワード導出パターンが特定されたとき，前記特定されたパスワード導出パターンを含む登録確認画面を前記無線端末装置が表示して，これにより，前記パスワード導出パターンを登録するか又は前記表示及び入力を最初からやり直すかの選択を促す手段と，」との記載を追加する。

（訂正事項６）

特許請求の範囲の請求項８に「前記特定されたパスワード導出パターンを登録させるための手段を備える，」とあるのを，「前記登録が選択されたとき，前記特定されたパスワード導出パターンを登録させるための手段を備える，」に訂正する。

（訂正事項７）

特許請求の範囲の請求項９に「前記所定のパターンは，マトリックスであり，」とあるのを，「前記所定のパターンは，Ｋ行Ｌ列のマトリックスであり，」に訂正する。

（訂正事項８）

特許請求の範囲の請求項９に「前記提示用パターンは，マトリックスの各要素に０～９までの整数を割り当てたものである，」とあるのを，「前記提示用パタ

ーンは，前記Ｋ行Ｌ列のマトリックスの各要素に０～９までの整数を割り当てたものであり，」に訂正する。

（訂正事項９）

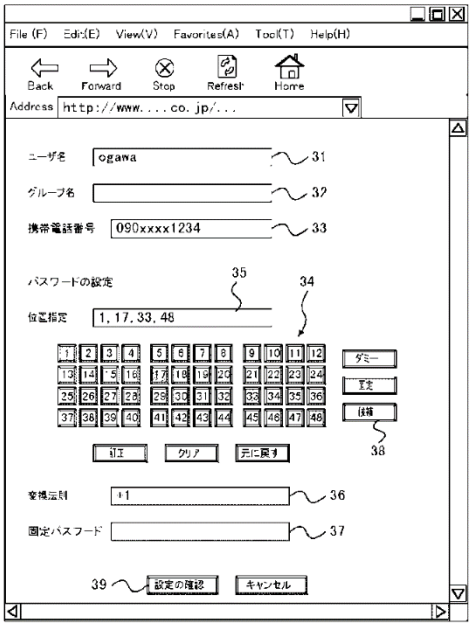
特許請求の範囲の請求項９に「前記提示用パターンは，マトリックスの各要素に０～９までの整数を割り当てたものである，」とあるのを，その記載の直後に，「前記Ｋ行Ｌ列のマトリックスは，前記所定のキャラクタの数字列がＪ桁のとき，以下の数式：

１０＾Ｊ＜（Ｋ＊Ｌ）＊（Ｋ＊Ｌ－１）・・（Ｋ＊Ｌ－Ｊ＋１）

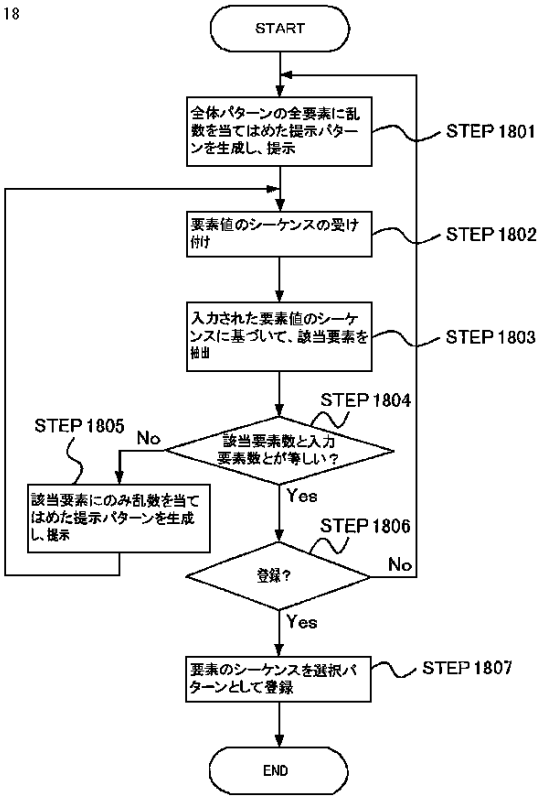
に従って，構成される，」との記載を追加する。

（別紙）本件明細書の図

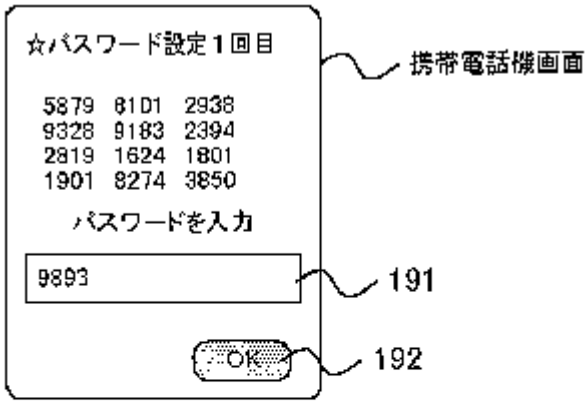
【図３】
Fig. 3



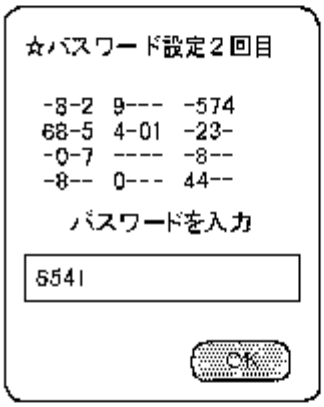

【図１８】
Fig.18



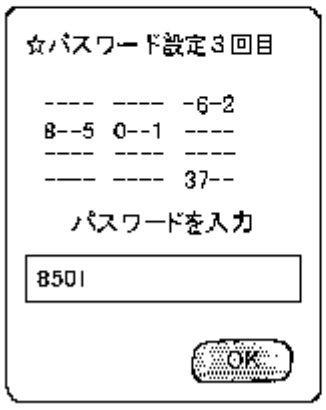
【図19】




(a)



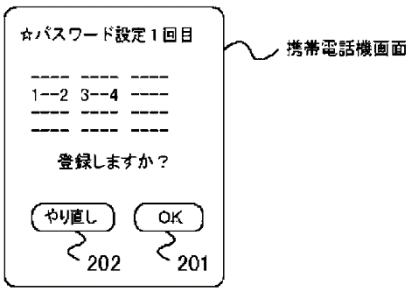

(b)




(c)

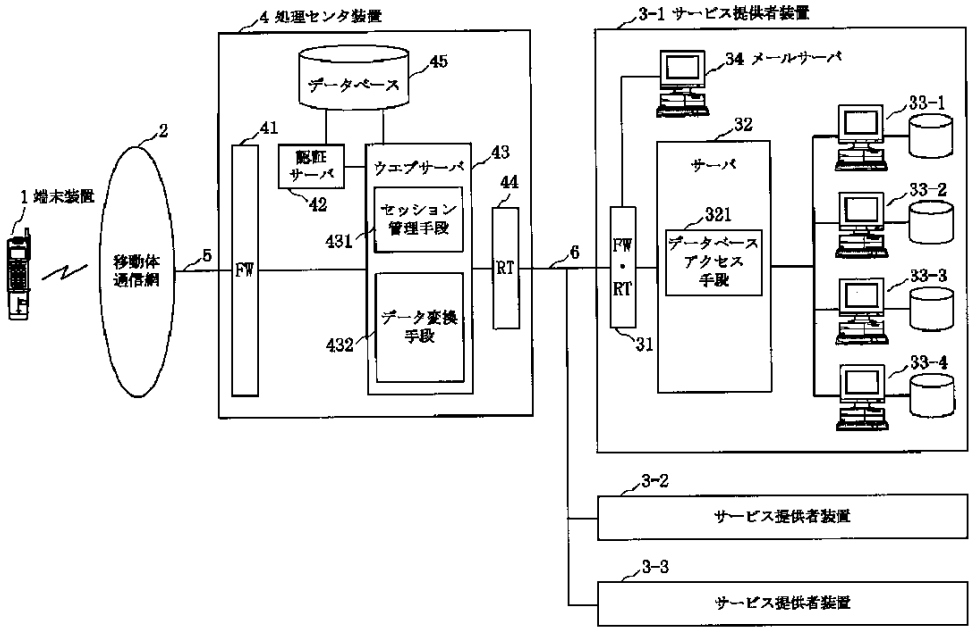
【図２０】

Fig. 20

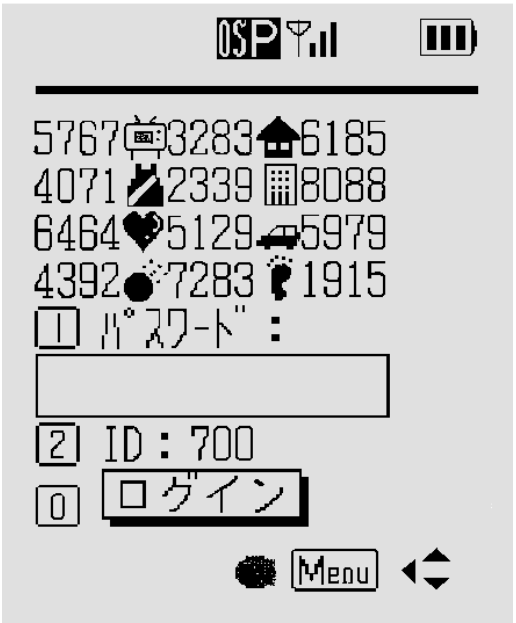


（別紙）甲１の図

【図１】

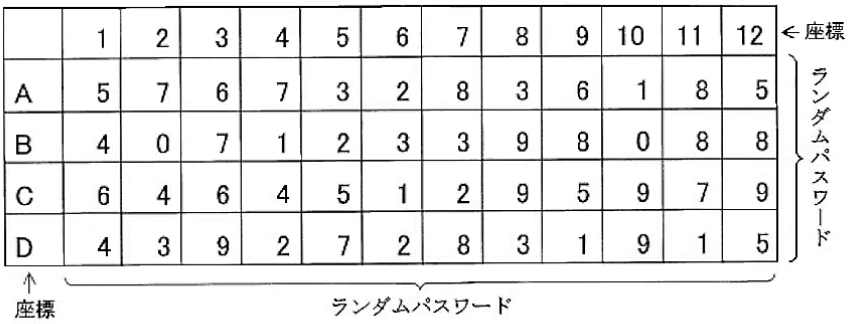

4 処理センタ装置
3-1 サービス提供者装置
データベース
45
34 メールサーバ
33-1
41
32
2
1 端末装置
脆弱性サーバ
42
ウエブサーバ
43
44
サーバ
33-2
セッション管理手段
431
321
移動体通信網
5
FW
RT
6
FW・RT
データベースアクセス手段
33-3
データ変換手段
432
31
33-4
3-2
サービス提供者装置
3-3
サービス提供者装置

【図３】


5767 3283 6185
4071 2339 8088
6464 5129 5979
4392 7283 1915
1 パスワード：
2 ID：700
0 ログイン
Menu

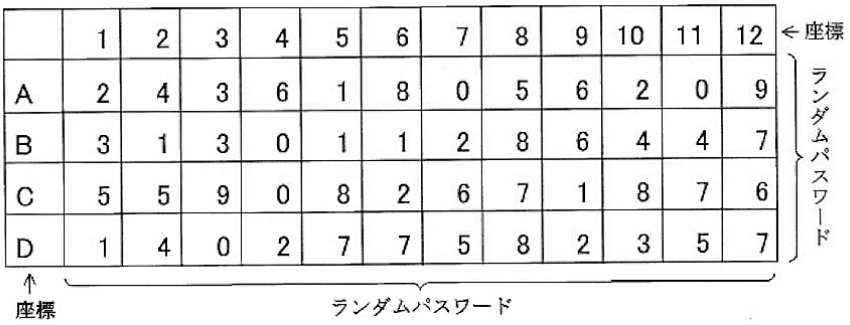
【図４】

（ａ）



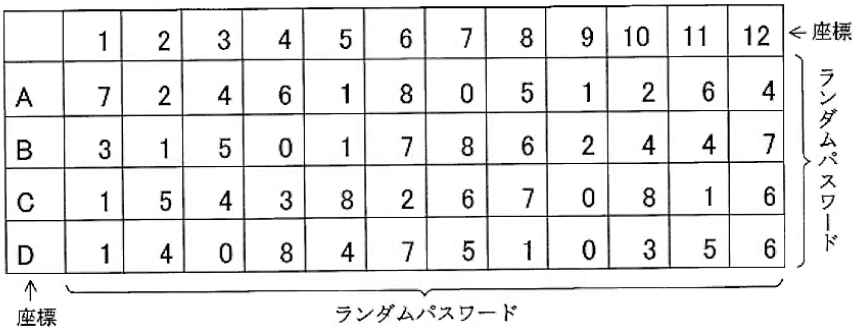

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | 5 | 7 | 6 | 7 | 3 | 2 | 8 | 3 | 6 | 1 | 8 | 5 |
| B | 4 | 0 | 7 | 1 | 2 | 3 | 3 | 9 | 8 | 0 | 8 | 8 |
| C | 6 | 4 | 6 | 4 | 5 | 1 | 2 | 9 | 5 | 9 | 7 | 9 |
| D | 4 | 3 | 9 | 2 | 7 | 2 | 8 | 3 | 1 | 9 | 1 | 5 |

（ｂ）




| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | 2 | 4 | 3 | 6 | 1 | 8 | 0 | 5 | 6 | 2 | 0 | 9 |
| B | 3 | 1 | 3 | 0 | 1 | 1 | 2 | 8 | 6 | 4 | 4 | 7 |
| C | 5 | 5 | 9 | 0 | 8 | 2 | 6 | 7 | 1 | 8 | 7 | 6 |
| D | 1 | 4 | 0 | 2 | 7 | 7 | 5 | 8 | 2 | 3 | 5 | 7 |

【図５】




| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | 7 | 2 | 4 | 6 | 1 | 8 | 0 | 5 | 1 | 2 | 6 | 4 |
| B | 3 | 1 | 5 | 0 | 1 | 7 | 8 | 6 | 2 | 4 | 4 | 7 |
| C | 1 | 5 | 4 | 3 | 8 | 2 | 6 | 7 | 0 | 8 | 1 | 6 |
| D | 1 | 4 | 0 | 8 | 4 | 7 | 5 | 1 | 0 | 3 | 5 | 6 |