

審決

不服2015- 20015

アメリカ合衆国 カリフォルニア 92121 サン ディエゴ モアハウス ドライブ 5775
請求人 クアルコム, インコーポレイテッド

東京都千代田区丸の内一丁目9番2号 グラントウキョウサウスタワー 特許業
務法人 志賀国際特許事務所
代理人弁理士 村山 靖彦

東京都千代田区丸の内一丁目9番2号 グラントウキョウサウスタワー 特許業
務法人 志賀国際特許事務所
代理人弁理士 黒田 晋平

特願2014-524051「デバイスにおけるセキュリティ強化のために多要素パスワードまたは動的パスワードを使うための方法および装置」拒絶査定不服審判事件〔平成25年 2月 7日国際公開, WO2013/019880, 平成26年10月 2日国内公表, 特表2014-526105〕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

第1. 手続の経緯

本願は, 2012年8月1日(パリ条約による優先権主張外国庁受理2011年8月2日 アメリカ合衆国)を国際出願日とする出願であって, 平成26年2月21日付けで特許法第184条の4第1項の規定による明細書, 請求の範囲, 及び, 図面(図面の中の説明に限る)の日本語による翻訳文が提出されると共に, 同日付けで審査請求がなされ, 平成27年1月13日付けで審査官により拒絶理由が通知され, これに対して平成27年4月22日付けで意見書が提出されると共に手続補正がなされたが, 平成27年6月25日付けで審査官により拒絶査定がなされ(謄本送達; 平成27年7月6日), これに対して平成27年11月6日付けで審判請求がなされると共に手続補正がなされ, 平成27年12月17日付けで審査官により特許法第164条第3項の規定に基づく報告がなされ, 平成28年4月4日付けで上申書が提出され, 平成29年3月21日付けで当審により拒絶理由が通知され, これに対して平成29年6月27日付けで意見書が提出されると共に手続補正がなされたものである。

第2. 本願発明について

本願の請求項1に係る発明(以下, これを「本願発明」という)は, 平成29年6月27日付けの手続補正により補正された特許請求の範囲の請求項1に記載された, 次のとおりのものである。

「認証を実施する方法であって,
ユーザによって選択された複数の異なる要素を含む多要素パスワードを構成する前記複数の要素すべてについての入力情報を受信するステップと,
前記受信した入力情報に基づいて前記多要素パスワードを判断するステップであって, 前記複数の要素が, 前記ユーザを認証するのに使われる異なるタイプの情報に対応する, 前記多要素パスワードを判断するステップと,
デバイスによって, 前記判断に基づいて前記ユーザを認証するステップと,

を含み、

前記多要素パスワードは、前記複数の要素のそれぞれの認証結果及び該選択された要素の順序に基づき認証され、

前記多要素パスワードを構成する前記複数の要素の順序が前記ユーザによって事前に選択される方法。」

第3. 引用刊行物に記載の事項

1. 当審による平成29年3月21日付けの拒絶理由（以下、これを「当審拒絶理由」という）において、引用刊行物1として引用された、本願の第1国出願前に既に公知である、特開2011-022953号公報（2011年2月3日公開）には、関連する図面と共に、次の事項が記載されている。

A. 「【0028】

利用者は、表示画像を参照し、入力部120を操作して、暗証文字列に対応する数値列を認証情報登録部170bに入力する。利用者は、認証情報として利用する暗証文字列を予め決めておく。ここでは一例として、暗証文字列を「cgi2」とする。

【0029】

利用者は、認証情報「cgi2」に対応する数値列「2579」と、利用者IDとを対応付けて、認証情報登録部170bに入力する。認証情報登録部170bは、利用者IDと数値列とを対応付けて、利用者管理テーブル160aに登録する。」

B. 「【0048】

続いて、認証装置100が、利用者を認証する認証処理について説明する。図9は、認証処理の処理手順を示すフローチャートである。図9に示すように、認証装置100は、利用者IDを取得し（ステップS201）、認証処理部170cが、利用者IDに対応する数値列を利用者管理テーブル160aから検索する（ステップS202）。

【0049】

認証装置100は、生体センサ110から生体情報を取得し（ステップS203）、ハッシュ値生成部170aは、生体情報を基に、ハッシュ値文字列を生成する（ステップS204）。

【0050】

認証処理部170cは、数値列と第1の対応表データとを基にして、数値列に対応する暗証文字列を特定する（ステップS205）。認証処理部170cは、ハッシュ値文字列をランダムに並び替え（ステップS206）、各数値にブロック識別情報を対応付けた表示画像を出力する（ステップS207）。

【0051】

認証処理部170cは、数値列を受け付け（ステップS208）、数値列と第2の対応表データとを比較して、数値列に対応する文字列を特定する（ステップS209）。認証処理部170cは、特定した文字列と暗証文字列とが等しいか否かを判定する（ステップS210）。

【0052】

認証処理部170cは、特定した文字列と暗証文字列とが等しい場合（ステップS211、Yes）、認証成功と判定する（ステップS212）。一方、認証処理部170cは、特定した文字列と暗証文字列とが異なる場合（ステップS211、No）、認証失敗と判定する（ステップS213）。

【0053】

上述してきたように、本実施例2にかかる認証装置100は、生体情報のハッシュ値文字列を並び替えた後に、並び替え文字列と、ダミーの文字列とを混在させた各ブロック識別情報を各数値に対応させて表示画面を出力する。そして、認証装置100は、利用者に入力された数値列に対応する文字列が、暗証文字列と等しいか否かを判定し、判定結果に基づいて本人認証を実行する。表示画面に表示される文字列は毎回順序が変わるので、ユーザが入力する数値列も毎回異なる。したがって、スクリーンショット付きのデータロガーなどにより、入力操作を盗み見された場合でも、認証情報が漏洩することは無い。」

C. 「【0058】

なお、この認証装置100は、既知の情報処理装置に、上述したハッシュ値生成部170a、認証情報登録部170b、認証処理部170cの各機能を搭載することによって実現することもできる。既知の情報処理装置は、例えば、パーソナルコンピュータ、ワークステーション、携帯電話、PHS端末、移動体通信端末またはPDA等に対応する。」

D. 【図2】には、少なくとも、「認証装置」が、「生体センサ」、「入力部」、「出力部」、「入出力制御部」と、「ハッシュ値生成部」、「認証情報登録部」、及び、「認証処理部」から構成される「制御部」、更に、「利用者管理テーブル」を有する「記憶部」から構成されていることが示されている。

2. 平成27年1月13日付けの原審の拒絶理由（以下、これを「原審拒絶理由」という）において引用され、当審拒絶理由において、引用刊行物2として引用された、本願の第1国出願前に既に公知である、特開2011-145906号公報（2011年7月28日公開）には、関連する図面と共に、次の事項が記載されている。

E. 「【0057】

ここでいう認証方式とは、例えば、暗証番号、パスワード、指静脈認証、掌認証、指紋認証、筆跡認証、声紋認証、等である。選択肢として提示される認証方式は、ここで挙げた認証方式以外でも導入可能であり、認証として機能するものであれば、導入しても良いものとする。

【0058】

複数個表示されている枠の中から、どの箇所にもどの認証方式を当て嵌めるか、利用者が予め登録しておき、その組合せ自体も認証として利用する。例えば、認証方式選択枠1にパスワード、認証方式選択枠3に暗証番号、認証方式選択枠7に指静脈認証を選択し、認証方式選択枠と認証方式の種類の組合せ自体もひとつの認証として利用する。」

3. 原審拒絶理由において引用され、当審拒絶理由において、引用刊行物3として引用された、本願の第1国出願前に既に公知である、特開2007-334707号公報（2007年12月27日公開）には、関連する図面と共に、次の事項が記載されている。

F. 「【0007】

本発明の認証システムでは、予め登録された複数の登録生体情報の中から利用者によって選択された少なくとも1つの認証用生体情報に基づいて予め設定された認証手順内容によって本人確認が行われるので、ユーザーが認証に使用する生体情報の数や種類を自由に設定することができる。これにより、たとえば煩雑で高精度の認証と簡易な認証とを取引状況に応じてユーザーが自由に設定できることになる。ここで、「生体情報」は、指紋や声紋、虹彩、音声、体の一部の静脈パターンといった生体的特徴を表す情報を意味する。」

G. 「【0010】

上記生体認証装置において、前記本人確認部は、複数の前記認証用生体情報が選択されている場合には、前記複数の認証用生体情報と、前記複数の認証用生体情報を使用して行われる前記認証の順序である認証順序とに基づいた認証方法で前記本人確認を行うようにしてもよい。」

第4. 引用刊行物に記載の発明

1. 上記Bの「認証装置100は、生体センサ110から生体情報を取得し」という記載、同じく、上記Bの「認証処理部170cは、数値列を受け付け」という記載、及び、同じく、上記Bの「利用者に入力された数値列」という記載と、上記Dにおいて指摘した、【図2】に開示されている事項と、上記Cの「認証装置100は、既知の情報処理装置に、上述したハッシュ値生成部170a、認証情報登録部170b、認証処理部170cの各

機能を搭載することによって実現する」という記載と、同じく、上記Cの「既知の情報処理装置は、例えば、パーソナルコンピュータ、ワークステーション、携帯電話、PHS端末、移動体通信端末またはPDA等に対応する」という記載から、引用刊行物1においては、“認証装置は、携帯電話、PHS端末、移動体通信端末、または、PDA等の、既知の情報処理装置によって実現される”ものであることが読みとれ、これら、「既知の情報処理装置」は、“通信デバイス”、或いは、“携帯デバイス”とも呼称されるもの、即ち、一種の“デバイス”であるから、

引用刊行物1においては、
“デバイスは、生体センサから利用者の生体情報を取得し、デバイスを構成する認証処理部は、デバイスの入力部を介して、利用者によって入力された数値列を受け付ける”ものであることが読みとれ、

2. 上記Bの「数値列と第2の対応表データとを比較して、数値列に対応する文字列を特定する」という記載、及び、同じく、上記Bの「認証処理部170cは、特定した文字列と暗証文字列とが等しいか否かを判定する」という記載と、上記1.において検討した事項から、引用刊行物1においては、

“認証処理部は、対応表データを用いて、受け付けた数値列に対応する文字列を特定し、特定した文字列と暗証文字列が等しいか否かを判定する”ものであることが読みとれる。

3. 上記Bの「認証処理部170cは、特定した文字列と暗証文字列とが等しい場合（ステップS211、Yes）、認証成功と判定する」という記載、及び、同じく、上記Bの「暗証文字列と等しいか否かを判定し、判定結果に基づいて本人認証を実行する」という記載と、上記1.において検討した事項から、引用刊行物1においては、

“デバイスは、判定結果に基づいて本人認証を実行する”ものであることが読みとれる。

4. 上記Aの「入力部120を操作して、暗証文字列に対応する数値列を認証情報登録部170bに入力する。利用者は、認証情報として利用する暗証文字列を予め決めておく」という記載、及び、同じく、上記Aの「利用者は、認証情報「cgi2」に対応する数値列「2579」と、利用者IDとを対応付けて、認証情報登録部170bに入力する。認証情報登録部170bは、利用者IDと数値列とを対応付けて、利用者管理テーブル160aに登録する」という記載と、上記2.、及び、3.において検討した事項から、引用刊行物1においては、

“認証に用いる文字列は、利用者によって予め決定される”ものであることが読みとれる。

5. 以上、1.～4.において検討した事項は、「デバイス」において、「利用者」を「認証」するための方法であることは、明らかであるから、1.～4.において検討した事項から、引用刊行物1には、次の発明（以下、これを「引用発明」という）が記載されているものと認める。

デバイスにおいて、利用者を認証するための方法であって、

前記デバイスは、生体センサから前記利用者の生体情報を取得し、前記デバイスを構成する認証処理部は、デバイスの入力部を介して、利用者によって入力された数値列を受け付け、

前記認証処理部は、対応表データを用いて、受け付けた前記数値列に対応する文字列を特定し、特定した文字列と暗証文字列が等しいか否かを判定し、

前記デバイスは、判定結果に基づいて本人認証を実行するものであって、

前記認証に用いる文字列は、前記利用者によって予め決定される、認証のための方法。

第5. 本願発明と引用発明との対比

1. 引用発明における「デバイスにおいて、利用者を認証するための方法」は、

本願発明における「認証を実施する方法」に相当する。

2. 引用発明においても、認証に必要な「生体情報」と、「利用者」に入力される「数値列」の複数の情報を受信し、そのうち「数値列」は、「利用者」によって決定された「認証に用いる文字列」に関連するものであるから、“ユーザにより選択された要素”といい得るものであって、認証の判断に用いられるものである。

そして、引用発明においては、認証は、「生体センサ」から取得される、「利用者」の「生体情報」と、「利用者」によって入力される「数値列」によって行われるものであるから、「生体情報」と、「数値列」は、「入力情報」であって、引用発明における「パスワード」は、「生体情報」と、「数値列」によって構成されるものであることは明らかである。

そして、「生体情報」と、「数値列」は、「異なる要素」であるから、そうすると、引用発明における「生体情報」、及び、「数値列」が、本願発明における「パスワードを構成する要素」に相当する。

よって、引用発明において、「生体センサから前記利用者の生体情報を取得し、前記デバイスを構成する認証処理部は、デバイスの入力部を介して、利用者によって入力された数値列を受け付け」ることと、

本願発明において、「ユーザによって選択された複数の異なる要素を含む多要素パスワードを構成する前記複数の要素すべてについての入力情報を受信するステップ」とは、

“ユーザによって選択された要素を含むパスワードを構成する複数の要素すべてについての入力情報を受信するステップ”

である点で共通する。

3. 上記2. において検討したとおり、引用発明における「パスワード」は、「生体情報」と、「数値列」により構成されるものであるといえ、入力された「数値列」から得られる「特定した文字列」と「暗証文字列が等しいか判定」することは、「パスワード」の正当性を判断することと同義であり、引用発明における「生体情報」と、「数値列」は、これらの情報から構成される「パスワード」を「認証」するための、「異なるタイプの情報」であることは明らかである。

よって、引用発明における「対応表データを用いて、受け付けた前記数値列に対応する文字列を特定し、特定した文字列と暗証文字列が等しいか否かを判定」することと、

本願発明における「前記受信した入力情報に基づいて前記多要素パスワードを判断するステップであって、前記複数の要素が、前記ユーザを認証するのに使われる異なるタイプの情報に対応する、前記多要素パスワードを判断するステップ」とは、

“受信した入力情報に基づいて前記パスワードを判断するステップであって、前記複数の要素が、前記ユーザを認証するのに使われる異なるタイプの情報に対応する、前記パスワードを判断するステップ”である点で共通する。

4. 引用発明における「デバイスは、判定結果に基づいて本人認証を実行する」が、

本願発明における「デバイスによって、前記判断に基づいて前記ユーザを認証するステップ」に相当する。

5. 引用発明においては、「認証に用いる文字列」が、「利用者によって予め決定される」ものであって、「認証に用いる文字列」は、“認証に必要な情報”であるから、

引用発明における「前記認証に用いる文字列は、前記利用者によって予め決定される」ことと、

本願発明における「前記多要素パスワードを構成する前記複数の要素の順序が前記ユーザによって事前に選択される」こととは、

“認証に必要な情報が、ユーザによって事前に選択されている”点で共通する。

6. 以上、上記1. ～5. において検討した事項から、本願発明と、引用発明との、一致点、及び、相違点は、次のとおりである。

[一致点]

認証を実施する方法であって、ユーザによって選択された要素を含むパスワードを構成する複数の要素すべてについての入力情報を受信するステップと、前記受信した入力情報に基づいて前記パスワードを判断するステップであって、前記複数の要素が、前記ユーザを認証するのに使われる異なるタイプの情報に対応する、前記パスワードを判断するステップと、デバイスによって、前記判断に基づいて前記ユーザを認証するステップと、認証に必要な情報が、前記ユーザによって事前に選択される方法。

[相違点1]

“ユーザによって選択された要素を含むパスワード”に関して、本願発明においては、「ユーザによって選択された複数の異なる要素を含む多要素パスワード」であるのに対して、引用発明においては、「暗証文字列」を予め「利用者」が決めておく点については、言及されているが、「生体情報」の選択については、特に言及されていない点。

[相違点2]

“受信した入力情報に基づいて前記パスワードを判断するステップ”に関して、本願発明においては、「多要素パスワードを判断するステップ」であるのに対して、引用発明においては、「特定した文字列」の判定を行うのみである点。

[相違点3]

本願発明においては、「多要素パスワードは、前記複数の要素のそれぞれの認証結果及び該選択された要素の順序に基づき認証されるものであるのに対して、引用発明においては、「生体情報」の認証に関しては、特に言及されていない点。

[相違点4]

“認証に必要な情報が、前記ユーザによって予め選択される”点に関して、本願発明においては、「複数の要素の順序」が、「ユーザによって選択される」ものであるのに対して、引用発明においては、「生体情報」の取得と、「数値列」の入力の順序は変えられないものである点。

第6. 相違点についての当審の判断

1. [相違点1] について

引用刊行物2の、上記Eに引用した「ここでいう認証方式とは、例えば、暗証番号、パスワード、指静脈認証、掌認証、指紋認証、筆跡認証、声紋認証、等である。選択肢として提示される認証方式は、ここで挙げた認証方式以外でも導入可能であり」という記載内容、同じく、上記Eに引用した「複数個表示されている枠の中から、どの箇所にもどの認証方式を当て嵌めるか、利用者が予め登録しておき、その組合せ自体も認証として利用する。例えば、認証方式選択枠1にパスワード、認証方式選択枠3に暗証番号、認証方式選択枠7に指静脈認証を選択し、認証方式選択枠と認証方式の種類を組合せ自体もひとつの認証として利用する」という記載内容、及び、引用刊行物3の、上記Fに引用した「予め登録された複数の登録生体情報の中から利用者によって選択された少なくとも1つの認証用生体情報に基づいて予め設定された認証手順内容によって本人確認が行われるので、ユーザーが認証に使用する生体情報の数や種類を自由に設定することができる。これにより、たとえば煩雑で高精度の認証と簡易な認証とを取引状況に応じてユーザーが自由に設定できることになる。ここで、「生体情報」は、指紋や声紋、虹彩、音声、体の一部の静脈パターンといった生体的特徴を表す情報を意味する」という記載内容から、複数の「生体情報」から、「利用者」が、いくつかを選択することは、本願の第1国出願前に、当業者には広く知られた技術事項

であった。

したがって、引用発明においても、「認証」に使用する「生体情報」を、「利用者」が複数選択して「多要素パスワード」を構成することは、当業者が、引用発明、引用刊行物2、及び、引用刊行物3に記載の発明に基づいて、容易になし得たものである。

よって、[相違点1]は、格別のものではない。

2. [相違点2]について

引用刊行物3の、上記Gに引用した「前記複数の認証用生体情報と、前記複数の認証用生体情報を使用して行われる前記認証の順序である認証順序とに基づいた認証方法で前記本人確認を行うようにしてもよい」という記載内容から、“入力された複数の生体情報とその順序に基づいて認証を行う”こと、即ち、“入力された複数の生体情報に基づいて認証を行う”ことは、本願の第1国出願前に、当業者には広く知られた技術事項であった。

したがって、引用発明においても、“入力された複数の生体情報に基づいて判断を行う”よう構成することは、当業者が適宜なし得る事項である。

よって、[相違点2]は、格別のものではない。

3. [相違点3]について

上記2.において引用した、引用刊行物3の上記Gの記載内容にもあるとおり、“複数の生体情報の認証の順序に基づいた認証方法を用いて本人認証を行う”点は、本願の第1国出願前に、当業者には広く知られた技術事項であった、そして、“複数の被認証情報を、順に認証していく場合に、前の認証結果に応じて、次の認証を行うか否かを判断すること、即ち、認証の結果に基づいて認証を継続する”ようなことは、当業者が適宜選択し得る事項である。

したがって、引用発明においても、“複数の生体情報を用いて認証を行う際、前段の認証結果、及び、認証の順序に基づいて、全体に認証を行う”よう構成することは、当業者が適宜なし得るものである。

よって、[相違点3]は、格別のものではない。

4. [相違点4]について

上記1.において引用した、引用刊行物2の上記Eの記載内容、或いは、引用刊行物3の上記Fの記載内容にもあるとおり、“認証に用いられる情報を、“利用者、即ちユーザが、予め選択する”よう構成することは、本願の第1国出願前に、当業者には広く知られた技術事項であった。

そして、上記2.、及び、上記3.において検討したとおり、認証の順序に基づいた認証方法を用いて本人認証を行うことも、当業者には広く知られた技術事項であるので、「認証に用いられる情報」として、“複数の認証の順序、及び、複数の要素の順序を含める”ことは、当業者が適宜なし得る事項である。

したがって、引用発明においても、“認証に用いられる情報に複数の要素の順序を含め、当該複数の要素の順序を、ユーザが、予め選択する”よう構成することは、当業者が適宜なし得る事項である。

よって、[相違点4]は、格別のものではない。

5. 以上、上記1.～4.において検討したとおり、[相違点1]～[相違点4]はいずれも格別のものでなく、そして、本願発明の構成によってもたらされる効果も、当業者であれば容易に予測できる程度のものであって、格別なものとは認められない。

第7. むすび

したがって、本願発明は、本願の特許出願前に日本国内又は外国において頒布された刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明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ので、特許法第29条第2項の規定により特許を受けることができない。

よって、結論のとおり審決する。

審判長 特許庁審判官 高木 進
 特許庁審判官 石井 茂和
 特許庁審判官 須田 勝巳

(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。

[審決分類] P 1 8 . 1 2 1 - W Z (G 0 6 F)

出訴期間として90日を附加する。

審判長	特許庁審判官	高木 進	8628
	特許庁審判官	須田 勝巳	8941
	特許庁審判官	石井 茂和	8837