令和４年３月２８日判決言渡

令和３年（行ケ）第１００５５号　審決取消請求事件

口頭弁論終結日　令和４年１月３１日

判　　決

原　　告　　ファーストフェイス　カンパニー
リミテッド

同訴訟代理人弁護士　城　山　康　文
同　後　藤　未　来
同訴訟代理人弁理士　金　山　賢　教
同　市　川　祐　輔

被　　告　　Ａｐｐｌｅ　Ｊａｐａｎ合同会社

同訴訟代理人弁護士　北　原　潤　一
同　米　山　朋　宏
同　梶　並　彰　一　郎

主　　文

１　原告の請求を棄却する。

２　訴訟費用は原告の負担とする。

３　この判決に対する上告及び上告受理の申立てのための付加期

間を３０日と定める。

事　実　及　び　理　由

第１　請求

特許庁が無効２０１９－８００００７号事件について令和２年１２月２４日にした審決中、「特許第６３８６６４６号の請求項１ないし４、７及び８に記載された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（当事者間に争いがない。）

⑴　原告は、２０１２年（平成２４年）１０月１７日を国際出願日とする特許出願（特願２０１４－５３６９８２号。パリ条約による優先権主張外国庁受理２０１１年１０月１９日、韓国。以下、この日付を「本件優先日」という。）の一部を分割して、平成２９年９月２２日、発明の名称を「移動通信端末機の活性化時に、特定動作が行われるようにするための方法、システム及び移動通信端末機」とする特許出願をし（特願２０１７－１８２３９２）、平成３０年８月１７日、特許権の設定登録（特許第６３８６６４６号。請求項の数９。）を受けた（以下、この特許を「本件特許」という。）。

⑵　被告は、平成３１年１月３０日、特許庁に対し、本件特許の請求項１ないし４、７及び８について特許無効審判（無効２０１９－８００００７号）を請求した。

原告は、令和２年５月２０日、請求項１ないし８について訂正する旨の訂正請求（以下「本件訂正請求」という。）をした。

特許庁は、令和２年１２月２４日、本件訂正請求を認めた上で、「特許第６３８６６４６号の請求項１ないし４、７及び８に記載された発明についての特許を無効とする。」との審決（以下「本件審決」という。）をし、その謄本は同年１２月２８日原告に送達された。

⑶　原告は、令和３年４月２６日、本件審決の取消しを求める本件訴訟を提起

した。

２　特許請求の範囲の記載

訂正後の請求項１ないし４、７及び８の特許請求の範囲の記載は、次のとおりである（下線部が本件訂正請求による訂正〔以下「本件訂正」という。〕がされた部分。以下、請求項１に係る発明を「本件発明１」、請求項２に係る発明を「本件発明２」、請求項３に係る発明を「本件発明３」、請求項４に係る発明を「本件発明４」、請求項７に係る発明を「本件発明５」、請求項８に係る発明を「本件発明６」といい、包括して「本件各発明」という。）。

【特許請求の範囲】

【請求項１】

使用者による操作を受け付けるとともに所定の表示を行うタッチスクリーンディスプレイ部と、

外部装置と通信可能な状態であるが前記タッチスクリーンディスプレイ部の表示がオフである非活性状態から前記タッチスクリーンディスプレイ部の表示をオンにしてロック画面が表示された活性状態に切り替えるための活性化ボタンと、

前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて前記非活性状態から前記ロック画面が表示された前記活性状態に切り替えるとともに、前記使用者の操作が第１の操作であった場合には第１動作を、前記使用者の操作が前記第１の操作よりも前記活性化ボタンに対して長い時間継続してなされた第２の操作であった場合には前記第１動作とは異なる第２動作を、前記使用者の操作以外の追加の操作をすることなく、実行するための制御部と、

を含む移動通信端末装置であって、

前記各動作は、カメラ活性化機能、健康情報伝送機能、使用者識別機能、位置情報伝送機能、ハンズフリー機能、または広告表示機能のいずれかを含む、

移動通信端末装置。

【請求項２】

前記第１の操作がなされた場合には、前記非活性状態から前記活性状態に切り替えるとともに、前記タッチスクリーンディスプレイ部へのロック画面の表示と、前記第１動作の実行をし、

前記ロック画面には、現在の時間を表示することができる、請求項１に記載の移動通信端末装置。

【請求項３】

前記第２の操作がなされた場合には、前記非活性状態から前記活性状態に切り替えるとともに、前記タッチスクリーンディスプレイ部へのロック画面の表示し、前記第２動作の実行をする、請求項１又は２に記載の移動通信端末装置。

【請求項４】

前記制御部は、

前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて前記非活性状態から前記ロック画面が表示された前記活性状態に切り替えるとともに、前記使用者の操作が前記第１の操作であった場合には前記第１動作を、前記使用者の操作以外の追加の操作をすることなく、実行し、

前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて前記非活性状態から前記ロック画面が表示された前記活性状態に切り替えるとともに、前記使用者の操作が前記第１の操作よりも前記活性化ボタンに対して長い時間継続してなされた前記第２の操作であった場合には前記第１動作とは異なる前記第２動作を、前記使用者の操作以外の追加の操作をすることなく、実行し、

前記使用者識別機能は、前記使用者があらかじめ登録された使用者であると識別された場合にはロック状態を解除し、前記使用者があらかじめ登録された使用者でないと識別された場合には前記ロック状態を維持する機能である、請

求項１～３のいずれか一項に記載の移動通信端末装置。

【請求項７】

前記使用者識別機能は、指紋認識を利用した機能であり、前記使用者識別機能による認証の結果、前記使用者が正当な使用者と認証されなければ、前記ディスプレイ部にメッセージを表示するよう構成される、請求項１～５のいずれか一項に記載の移動通信端末装置。

【請求項８】

前記使用者識別機能は、顔認識を利用した機能である、請求項１～５のいずれか一項に記載の移動通信端末装置。

３　本件審決の理由の要旨

⑴　本件審決の理由の要旨は、本件各発明は、本件特許出願の優先日前に公然実施されていたｉＯＳ４．２又は４．３を搭載したｉＰｈｏｎｅ４である発明（以下「公然実施発明」という。）、ｉＯＳ４．３を搭載したｉＰｈｏｎｅ４について公然実施された発明（以下「公然実施発明２」という。）及び特表２０１０－５４１０４６号公報（甲３。以下「甲３文献」という。）に記載された２つの発明（以下「甲３発明１」及び「甲３発明２」という。）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から、被告主張の進歩性欠如（特許法２９条２項違反）の無効理由は理由があるというものである。

各論点に関する理由の要旨は、以下のとおりである。

⑵　本件発明１の進歩性について

ア(ア)　公然実施発明の内容について

使用者による操作を受け付けるとともに所定の表示を行うタッチスクリーンディスプレイと、

外部装置と通信可能な状態であるがロックしてタッチスクリーンディスプレイをオフにしたスリープ状態からタッチスクリーンディスプ

レイの表示をオンにしてロック画面が表示されたスリープ解除状態に切り替えるためのホームボタンと、

スリープ状態において、使用者がホームボタンを押すと、スリープ状態からスリープ解除状態に切り替えるとともに、タッチスクリーンディスプレイにロック画面を表示する一方で、使用者がホームボタンを長い時間継続して押した場合には、スリープ状態からスリープ解除状態に切り替えるとともに、タッチスクリーンディスプレイにロック画面を表示し、その後音声コントロールの画面を表示して、音声コントロール機能を、追加の操作をすることなく、実行し、

加えて、パスコードを入力することによる使用者識別機能として、スリープ状態においてホームボタンを押して、ロック画面においてスライダをドラッグした後、４ケタのパスコードを入力したときに、認証を行う制御部と、

を含むスマートフォン。

（イ） 本件発明１と公然実施発明の一致点及び相違点について

＜一致点＞

使用者による操作を受け付けるとともに所定の表示を行うタッチスクリーンディスプレイ部と、

外部装置と通信可能な状態であるが前記タッチスクリーンディスプレイ部の表示がオフである非活性状態から前記タッチスクリーンディスプレイ部の表示をオンにしてロック画面が表示された活性状態に切り替えるための活性化ボタンと、

前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて前記非活性状態から前記ロック画面が表示された前記活性状態に切り替えるとともに、前記使用者の操作が第１の操作よりも前記活性化ボタンに対して長い時間継続してなされた第２の操作で

あった場合には第２動作を、前記使用者の操作以外の追加の操作をすることなく、実行するための制御部と、

を含む移動通信端末装置であって、

前記第２動作は、カメラ活性化機能、健康情報伝送機能、使用者識別機能、位置情報伝送機能、ハンズフリー機能、または広告表示機能のいずれかに含まれるハンズフリー機能である、移動通信端末装置。

＜相違点１＞

使用者の操作が第１の操作であった場合、本件発明１では、「第１動作を」「前記使用者の操作以外の追加の操作をすることなく、実行する」ものであって、「第１動作」は「カメラ活性化機能、健康情報伝送機能、使用者識別機能、位置情報伝送機能、ハンズフリー機能、または広告表示機能のいずれか」の動作であり、かつ、「第２動作」である「カメラ活性化機能、健康情報伝送機能、使用者識別機能、位置情報伝送機能､ハンズフリー機能､または広告表示機能のいずれか」とは異なる動作であるのに対し、公然実施発明では、「カメラ活性化機能、健康情報伝送機能、使用者識別機能、位置情報伝送機能、ハンズフリー機能､または広告表示機能のいずれか」の動作であり､かつ、「第２動作」である「カメラ活性化機能、健康情報伝送機能、使用者識別機能、位置情報伝送機能、ハンズフリー機能、または広告表示機能のいずれか」と異なる動作である「第１動作を」「前記使用者の操作以外の追加の操作をすることなく、実行する」ものではない点。

イ　相違点１の容易想到性について

（ア）　甲３発明１の内容について

ユーザをシームレスに認証するための、ユーザに可視表示を提供するディスプレイ回路とホームボタンとを備える携帯電話であって、

ユーザが押下したことを受信する前記ホームボタンと、

前記ホームボタンの背後に配置されたセンサであって、ユーザが前記ホームボタンを押下したことを受信した時、ユーザからの明示的な入力を要求することなく、ユーザの指紋の特徴を検出するセンサと、

ライブラリに格納された指紋の情報と検出した前記ユーザの指紋の特徴とを比較することで、前記ユーザの指紋の特徴がライブラリに格納された指紋の情報に適合するか、適合しないかが判定され、適合する、すなわち、ユーザが許可されていると判定した場合は、ユーザに制限されたリソースへのアクセスを提供し、適合しない、すなわち、ユーザが許可されていないと判定した場合は、認証を行うようユーザに指示するプロセッサと、

を備えること。

（イ） 公然実施発明のスマートフォンも甲３発明１の携帯電話も携帯通信端末機であるといえる。そして、公然実施発明は、「スリープ状態においてホームボタンを押して、ロック画面においてスライダをドラッグした後、４ケタのパスコードを入力したときに、認証を行う」ものであるところ、公然実施発明の「スリープ状態においてホームボタンを押」すことは、スリープ状態にあるスマートフォンのホームボタンを押して「デバイス機能を有効にする前、または、デバイスリソースにアクセスする前」に「起動する」ことといえ、公然実施発明の「４ケタのパスコードを入力したときに、認証を行う」ことは、甲３発明１が技術課題の前提として例示する「デバイスのホームスクリーンまたはメニューを表示する前に、４つの数字または４つの文字のＰＩＮを入力するよう、ユーザに要求すること」に該当する。

そうすると、甲３文献に接した当業者であれば、公然実施発明には、スリープ状態においてホームボタンを押してから認証を経てデバイスにアクセスできるまでの一連の動作に関して、甲３発明１と共通の技術課

題（デバイスのホームスクリーンまたはメニューを表示する前に、４つの数字または４つの文字のＰＩＮを入力するよう、ユーザに要求することは、パスコードが知られると、制限メカニズムの効果がなくなり、パスワードまたはパスコードを忘れて、許可ユーザがデバイスにアクセスできなくなる場合もある。）が存在することを想起するものといえ、公然実施発明には、許可されていない人物がユーザの個人情報にアクセスし閲覧することを防ぐため、デバイス機能を有効にする前またはデバイスリソースにアクセスする前の起動する時に、デバイスが迅速かつシームレスにユーザを認証することを目的とした甲３発明１を適用する動機付けがある。

（ウ） 甲３発明１は､ユーザがホームボタンを押下したことを受信した時、ユーザによる追加の操作なしに、指紋認識による使用者識別機能が行われる構成を有する。

公然実施発明に甲３発明１を適用する動機付けはあるから、「ユーザがホームボタンを押下したことを受信した時、ユーザによる追加の操作なしに、指紋認識による使用者識別機能が行われる」ために、公然実施発明において、「スリープ状態において、使用者がホームボタンを押」したことを受信した時、「ロック画面においてスライダをドラッグした後、４ケタのパスコードを入力」することなしに、指紋認証による「使用者識別機能」を実行するように構成することは、当業者であれば容易に想到し得る。

（エ） 被請求人（本件原告）は、本件発明１におけるロック画面に関する構成が甲３文献に開示されていないから、公然実施発明に甲３発明１を組み合わせても、相違点１に係る本件発明１の構成を容易に想到することができない旨主張するが、ロック画面について本件各発明の明細書は明確に定義しておらず、本件発明１で特定されるロック画面は、「前記

非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて」「表示され」る画面のことであり、「起動する時に、デバイスが迅速かつシームレスにユーザを認証する」ために「ユーザがホームボタンを押下したことを受信した時、ユーザによる追加の操作なしに、指紋認識による使用者識別機能」を行う甲３発明１は、「ユーザがホームボタンを押下したことを受信した時」に「ロック画面」が表示されているか否かにかかわらず適用できるものである。

⑶　本件発明２の進歩性について

ア　本件発明２と公然実施発明の相違点について

相違点１に加えて、以下の相違点がある。

＜相違点２＞

本件発明２では、「前記ロック画面には、現在の時間を表示することができる」のに対し、公然実施発明ではこの点が特定されていない点。

イ　相違点２の容易想到性について

スマートフォンにおいて、スリープ時にホームボタンが押された際、使用者が設定した背景画面に、現在時間などの非常に簡単な情報だけが表示されている画面は「ロック画面」であるから、公然実施発明において、スリープ状態にあるときに、ユーザがホームボタンを押すと表示されるロック画面に現在の時間が表示できるようにすることは、当業者が適宜になし得る。

⑷　本件発明３の進歩性について

本件発明３と公然実施発明とは、相違点１で相違し、その余の点で一致するところ、本件発明１について検討したのと同様の理由により、公然実施発明及び甲３発明１に基づいて当業者が容易に発明することができた。

⑸　本件発明４の進歩性について

ア　本件発明４と公然実施発明１の相違点について

相違点１に加え、以下の相違点がある。

＜相違点３＞

本件発明４では、「前記使用者識別機能は、前記使用者があらかじめ登録された使用者であると識別された場合にはロック状態を解除し、前記使用者があらかじめ登録された使用者でないと識別された場合には前記ロック状態を維持する機能である」と特定しているのに対し、公然実施発明はこの特定がない点。

イ　相違点３の容易想到性について

甲３発明１の「携帯電話」は、使用者識別機能について、使用者があらかじめ登録された使用者であると識別された場合は、ユーザに制限されたリソースへのアクセスを提供し、使用者があらかじめ登録された使用者でないと識別された場合、使用者に制限されたリソースへのアクセスを提供しない構成、すなわち、相違点３に係る構成を備えるといえる。

したがって、相違点３に係る構成は、公然実施発明において、甲３発明１を採用することに付随して得られる構成であって、格別のものとはいえない。

⑹　本件発明６の進歩性について

ア　本件発明６と公然実施発明の相違点について

＜相違点４＞

相違点１と同じ。

＜相違点５＞

使用者識別機能について、本件発明６では、「顔認識を利用した機能」であるのに対し、公然実施発明では、「パスコードを入力することによる」機能である点。

イ　相違点４及び相違点５の容易想到性について

（ア）　甲３文献には、請求項１５及び１７に記載された発明に関連して、

次の発明（以下「甲３発明２」という。）が記載されている。

ユーザをシームレスに認証するための、ユーザに可視表示を提供するディスプレイ回路とホームボタンとを備える携帯電話であって、

ユーザが押下したことを受信する前記ホームボタンと、

ユーザが電子デバイスリソースに対して閲覧またはアクセスを行うためにディスプレイの方を向いた時に、ユーザの顔の特徴が視野内に位置が合いうるように配置されたセンサであって、ホームボタンをユーザが押下したことを受信した時、ユーザの顔の特徴を検出するセンサと、

前記検出されたユーザの顔の特徴に基づいて、許可ユーザが検出された場合、制限されたコンテンツをディスプレイに表示したり、コンテンツへのアクセスを提供するプロセッサと、

を備えること。

（イ） 甲３発明２は、「ユーザがホームボタンを押下したことを受信した時、ユーザによる追加の操作なしに、顔認識による使用者識別機能が行われる」構成を有するといえる。

本件発明１について判断したところと同様に、公然実施発明に甲３発明２を適用する動機付けはあるから、「ユーザがホームボタンを押下したことを受信した時、ユーザによる追加の操作なしに、顔認識による使用者識別機能」が行われるために、公然実施発明において、「スリープ状態において、使用者がホームボタンを押」したことを受信した時、「ロック画面においてスライダをドラッグした後、４ケタのパスコードを入力」することなしに、「顔認識による使用者識別機能」を実行するように構成することは、当業者であれば容易に想到し得る。

⑺ 本件発明５の進歩性について

ア 公然実施発明２について

使用者による操作を受け付けるとともに所定の表示を行うタッチスク

リーンディスプレイと、

外部装置と通信可能な状態であるがロックしてタッチスクリーンディスプレイをオフにしたスリープ状態からタッチスクリーンディスプレイの表示をオンにしてロック画面が表示されたスリープ解除状態に切り替えるためのホームボタンと、

スリープ状態において、使用者がホームボタンを押すと、スリープ状態からスリープ解除状態に切り替えるとともに、タッチスクリーンディスプレイにロック画面を表示する一方で、使用者がホームボタンを長い時間継続して押した場合には、スリープ状態からスリープ解除状態に切り替えるとともに、タッチスクリーンディスプレイにロック画面を表示し、その後音声コントロールの画面を表示して、音声コントロール機能を、追加の操作をすることなく、実行し、

加えて、パスコードを入力することによる使用者識別機能として、スリープ状態においてホームボタンを押して、ロック画面においてスライダをドラッグした後、４ケタのパスコードを入力したときに、認証を行い、

さらに、パスコードを入力することによる使用者識別機能による認証の結果、使用者が正当な使用者と認証されれば、ロックが解除されて、ホーム画面が表示される一方で、認証されなければ、ロック状態を維持するとともに、ディスプレイに「パスコードが違います　もう一度試してください」というメッセージ（エラーメッセージ）を表示する制御部と、

を含むスマートフォン。

イ　本件発明５と公然実施発明２の一致点及び相違点について

＜一致点＞

使用者による操作を受け付けるとともに所定の表示を行うタッチスクリーンディスプレイ部と、

外部装置と通信可能な状態であるが前記タッチスクリーンディスプレ

イ部の表示がオフである非活性状態から前記タッチスクリーンディスプレイ部の表示をオンにしてロック画面が表示された活性状態に切り替えるための活性化ボタンと、

前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて前記非活性状態から前記ロック画面が表示された前記活性状態に切り替えるとともに、前記使用者の操作が第１の操作よりも前記活性化ボタンに対して長い時間継続してなされた第２の操作であった場合には第２動作を、前記使用者の操作以外の追加の操作をすることなく、実行するための

制御部と、

を含む移動通信端末装置であって、

前記第２動作は、カメラ活性化機能、健康情報伝送機能、使用者識別機能、位置情報伝送機能、ハンズフリー機能、または広告表示機能のいずれかに含まれるハンズフリー機能であり、

前記使用者識別機能は、前記使用者識別機能による認証の結果、前記使用者が正当な使用者と認証されなければ、前記ディスプレイ部にメッセージを表示するように構成される、移動通信端末装置。

＜相違点６＞

相違点１と同じ。

＜相違点７＞

使用者識別機能について、本件発明５では、「指紋認識を利用した機能」であるのに対し、公然実施発明２では、「パスコードを入力することによる」機能である点。

ウ　相違点６及び相違点７の容易想到性について

本件発明１について判断したところと同様に、公然実施発明２に甲３発明１を適用する動機付けはあるから、「ユーザがホームボタンを押下した

ことを受信した時、ユーザによる追加の操作なしに、指紋認識による使用者識別機能」が行われるために、公然実施発明２において、「スリープ状態において、使用者がホームボタンを押」したことを受信した時、「ロック画面においてスライダをドラッグした後、４ケタのパスコードを入力」することなしに、「指紋認識による使用者識別機能」を実行するように構成することは、当業者であれば容易に想到し得る。

第３　当事者の主張

１　取消事由１（本件発明１の進歩性の判断の誤り）

⑴　原告の主張

ア　相違点の認定に誤りがあることについて

（ア）　本件発明１と公然実施発明の相違点は、以下のとおりに認定されるべきである。

「前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて前記非活性状態から前記ロック画面が表示された前記活性状態に切り替えるとともに、前記使用者の操作が第１の操作であった場合には第１動作を、前記使用者の操作が前記第１の操作よりも前記活性化ボタンに対して長い時間継続してなされた第２の操作であった場合には前記第１動作とは異なる第２動作を、前記使用者の操作以外の追加の操作をすることなく、実行する」ものであり、当該各動作は「カメラ活性化機能、健康情報伝送機能、使用者識別機能、位置情報伝送機能、ハンズフリー機能、または広告表示機能のいずれかを含む」という構成

(イ)a　公然実施発明の「ロック画面」は、使用者識別機能（認証）を行うのに先立ち、使用者識別機能を行うのに必要となる「スライダに対するドラッグの操作」を受け付けるという特徴を有する。これによって、公然実施発明では、ユーザ認証におけるユーザの誤操作（意図せざる操作等）による誤動作を防止するという技術的意義がある。

これに対し、本件発明１では、そのようなスライダのドラッグ操作なしに、非活性状態から活性状態に切り替えるための操作入力により使用者識別機能が行われる。

b　また、本件発明１において、第１動作（又は第２動作）が使用者識別機能である場合においては、単なる使用者識別機能ではなく、「前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて前記非活性状態から前記ロック画面が表示された前記活性状態に切り替えるとともに、・・・前記使用者の操作以外の追加の操作をすることなく」実行される「使用者識別機能」である。

c　そのため、相違点１に係る本件発明１の構成は、「前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて前記非活性状態から前記ロック画面が表示された前記活性状態に切り替えるとともに」「前記使用者の操作以外の追加の操作をすることなく」との技術要素を含む形で認定されるべきである。この点を看過した本件審決の認定は誤りである。

イ　相違点の容易想到性の判断に誤りがあることについて

（ア）　甲３文献が、相違点１に係る本件発明１の構成を開示しないことについて

a　甲３文献において、検出した指紋を登録された指紋と照合して適合・不適合を判定する処理について記載しているのは、【００６５】であるが、そこにおいては、当該判定処理を「ユーザからの明示的な入力を要求することなく」行うことについては、何ら開示されていない。

本件審決は、甲３文献の請求項１５に「ユーザをシームレスに認証するための電子デバイス」と記載されていることに依拠して、あたかも相違点１に係る本件発明１の構成が開示されているかのように判断するが、同項の当該記載は具体的な認証処理の方法や手段を開示する

ものではない。

b　指紋認識による使用者識別機能が非活性状態から活性状態に切り替えるための操作入力に応じて行われる点についても、甲３文献には、開示されていない。

この点、本件審決は、一般にスマートフォンを「起動する時」にはスリープ状態からスリープ解除状態に移行する時も含まれるなどと認定している。しかし、甲３文献には、移動通信端末を「起動する」ことが何を意味するのかについて、具体的な記載はない。一般的な用語における「起動」とは、「コンピューターなどの機器の電源を入れて、操作できる状態にすること」を意味するものであり（甲４２）、相違点１に係る本件発明１の構成が規定する、非活性状態（移動通信端末機が通信可能な状態ではあるが、ディスプレイ画面がオフの状態）から、活性状態（移動通信端末機のディスプレイ画面がオンの状態）に切り替える操作とは異なるものである。

（イ）　公然実施発明を改変して本件発明１に想到する動機付けがないことについて

公然実施発明では、使用者識別機能の実行は、ディスプレイが活性化された後、更にディスプレイ上のスライダをドラッグする操作が行われた場合に、パスコードを入力することによって初めて行われるものである。そこにおいては、上記相違点１に係る本件発明１のように、使用者識別機能を、使用者の操作（非活性状態の際になされた活性化ボタンに対する使用者の操作）以外の追加の操作をすることなく、実行するという技術思想は全くない。

また、公然実施発明において、ディスプレイがオンにされた後に、更にディスプレイ上のスライダをドラッグすることで初めて認証を実行することには、ユーザの誤操作（意図せざる操作等）による誤動作を防止

するという意義があることは前記ア(イ)ａのとおりである。これをあえて改変して、本件発明１のように構成しようとすることは、公然実施発明の技術的意義・機能を損なうものといえ、当業者がそのような改変を試みるよう動機付けられることはない。

（ウ） 公然実施発明に甲３発明１を適用したとしても、本件発明１の構成に容易に想到しないことについて

ａ　甲３文献の【００４５】や図６の画面においても、ロックを解除するために画面上のスライダのドラッグ操作を受け付ける構成となっている。したがって、公然実施発明に甲３発明１を組み合わせた場合には、当業者は、公然実施発明と甲３発明１の共通の技術思想をなす上記構成を残しつつ甲３発明１の指紋認証を行うことを想到するものである（別紙３の１図）。そうすると、上記の組み合わせによって得られる構成は、ディスプレイが活性化された後にスライダのドラッグという追加の操作がなされて初めて、使用者識別機能が行われるものであり、これは、使用者による追加の操作なしに指紋認識による使用者識別機能を行う本件発明１の構成とは異なる。

ｂ　仮に、公然実施発明の使用者識別機能に係る手順のうち前記ａのスライダのドラッグ操作を排除することができたと仮定しても、ロック状態の画面の表示だけは残す、という組み合わせを想到することはあり得ない。なぜなら、公然実施発明の構成においては、ロック状態の画面を表示させ、その画面上に表示されるスライダがドラッグされたときに初めて、次のパスコードの入力画面に移行し、パスコードを入力させて認証を行う、という一連の認証操作を行わせるものであるから、認証に先立って表示されるロック画面は、認証画面に移行する前のスライダのドラッグを受け付けるための技術的意義を有するものであり、ロック画面のみが単体で意義を持つものではないからである。

さらに、公然実施発明における上記のような一連の認証操作において、スライダのドラッグ操作は、認証処理の開始のためにユーザの意図した入力を受け付けるインターフェースを提供するという意義・機能をも有するものである。そして、甲３文献においても、その図６に示されるように、ロック状態の画面について開示された構成は、ロック状態の画面上でスライダのドラッグを受け付けて認証を開始するという構成のみである。したがって、仮に公然実施発明に甲３発明１を組み合わせることができたとして、更に公然実施発明のスライダのドラッグ操作を排除する場合においては、公然実施発明のホームボタンの押下というユーザの操作が既に行われた上で認証が開始されているのであるから、更に重ねて認証を開始するためのユーザの意図した入力を受け付ける必要はなく、公然実施発明のロック状態の画面がその意義・機能を発揮する場面は想定され得ないことになり、当業者としては、スライダのドラッグを受け付けるためのロック画面も用いない構成（別紙３の２図）しか容易には想到できないものである。これは、本件発明１の構成（「前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて前記非活性状態から前記ロック画面が表示された前記活性状態に切り替え」）とは異なる。

c　甲３発明１における「シームレス」な認証が、使用者の追加操作なしに使用者識別機能を行うものだと解し得たとしても、公然実施発明のロック画面はパスコードの入力における意図せぬ誤操作を防止する意義・機能及び認証手続きのためのユーザの意図した入力を受け付けるインターフェースを提供し、このようなユーザの意図した入力を保証する意義・機能を有するものであるから、甲３発明１の「シームレス」に使用者識別機能を行う構成とは両立しない。

d　被告は、後記⑵イ（ウ）ｂのとおり、公然実施発明に甲３発明１を組

み合わせることで、公然実施発明のホームボタンの背後にセンサを設け、ホームボタンを押下すると、ロック画面が表示されるとともに、指紋認証を行うという構成を得ることができ（別紙４のＡ図）、この構成において、指紋認証に成功した場合には、認証成功後に直ちにホーム画面に遷移する構成（別紙４のＢ図１）及び認証成功後にスライダのドラッグ操作を経て、ホーム画面に遷移する構成（別紙４のＢ図２）を得ることができる旨主張する。

しかし、被告が主張する認証成功後の構成である別紙４のＢ図１左にはスライダが表示されているところ､指紋認証に成功した場合に｢当該成功後に直ちにホーム画面に遷移する構成」であるとされる以上、スライダをドラッグすることによって次の画面に遷移するという、スライダの機能は利用されない。公然実施発明や甲３発明１において、そのように「利用されないスライダを表示する」という技術思想は何ら開示されておらず、当業者がそのように何ら機能を発揮しないスライダをあえて表示させる構成に容易に想到し得たとはいえない。それを考え付くとすれば、本件発明１を見た上での後知恵である。

また、別紙４のＢ図２のような、「認証の成功後に、更にスライダのドラッグ操作を経て、ホーム画面に遷移する」という構成は、公然実施発明にも、甲３文献にも何ら開示がない。

ウ　小括

以上によれば、本件発明１についての容易想到性に関する本件審決の判断には誤りがある。

⑵　被告の主張

ア　相違点の認定に誤りがあるとの主張について

原告は、前記⑴アのとおり、相違点１に係る本件発明１の構成は、「前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に

基づいて前記非活性状態から前記ロック画面が表示された前記活性状態に切り替えるとともに」「前記使用者の操作以外の追加の操作をすることなく」との技術要素を含む形で認定されるべきである旨主張する。

原告の上記主張が、本件発明１の（使用者識別機能を含む）「第１動作」が、「・・・切り替えるとともに」実行するものである点を強調する趣旨であるとしても、その点は、本件審決の相違点において、「公然実施発明では、・・・「第１動作を」「前記使用者の操作以外の追加の操作をすることなく、実行する」ものではない点」との部分において、実質的に取り込まれていることから、原告の主張は無意味な主張である。

イ　相違点の容易想到性の判断に誤りがあるとの主張について

（ア）　甲３文献が、原告主張の相違点１に係る本件発明１の構成を開示しないとすることについて

ａ　原告は、前記⑴イ（ア）a のとおり、甲３文献には、検出された指紋を記録された指紋と照合して適合・不適合を判定する処理についてまで、ユーザからの明示的な入力を要求することなく行われることは開示されていない旨主張する。

しかし、甲３文献の請求項１５には、ユーザによってホームボタンが押下された時に（ユーザからの入力を受信した時に）、当該ユーザの識別特徴を検出し、当該識別特徴に基づいて、当該ユーザを認証する電子デバイス、つまり、ユーザをシームレスに認証する電子デバイスが開示され、当該検出及び認証は、ホームボタンの押下により、ユーザからの明示的な入力を要求することなく、行われている。

ｂ　原告は、前記⑴イ（ア）ｂのとおり、本件発明１における非活性状態から活性状態に切り替える操作は、甲３文献のいう「起動」には含まれない旨主張する。

しかし、甲３文献の【０００３】は、「デバイスをオンにする」、

「（デバイスを）ロック解除する」及び「（デバイスを）起動する」を並列的に記載していることから、当業者は、「デバイスを起動する」は、「デバイスをオンにする」及び「デバイスをロック解除する」とは異なる意味を含むものであると理解する。そして、スリープ状態にあるスマートフォンをスリープ解除状態に移行する意味で、「起動する」という用語を用いている例は、多数存在する（乙５の１ないし１０）。

（イ） 動機付けについて

原告は、前記⑴イ（イ）のとおり、公然実施発明の技術思想は本件発明１とは大きく異なり、公然実施発明を改変して本件発明１に想到する動機付けがない旨主張する。

しかし、公然実施発明と甲３発明１に基づく本件発明１の容易想到性は、公然実施発明と甲３発明１を組み合わせることができるかの問題であって、当該容易想到性をいうために、本件発明１の技術思想と公然実施発明の技術思想が共通である必要はない。

（ウ） 公然実施発明に甲３発明１を適用したとしても、本件発明１の構成に容易に想到しないとする主張について

ａ 原告主張の第１の構成

原告が前記⑴イ（ウ）ａ で甲３発明１と主張するのは、ディスプレイ内にセンサを設け、スライダのドラッグをすることで指紋認証を行う構成であるのに対し、本件審決が公然実施発明に組み合わせる構成として認定している構成（甲３発明１）は、ホームボタンの背後にセンサを配置し、ユーザが当該ホームボタンを押下した時に、ユーザからの明示的な入力を要求することなく、指紋による認証を行う構成で、これについても甲３文献に開示されたものであり、原告の主張は前提を誤るものである。

b　原告は、前記⑴イ（ウ）ｂのとおり、公然実施発明に甲３発明１を組み合わせた場合に、公然実施発明のロック画面上でのスライダのドラッグ操作を排除しておきながら、ロック画面の表示だけは残す、という組み合わせを想到することはあり得ない旨主張する。

仮に、「スライダのドラッグ操作を排除」したとしても、当該排除によって「ロック画面の表示」を残してはならないということにはならない。公然実施発明における「ロック画面の表示」には、原告が主張する誤操作防止の技術的意義・機能以外にも、例えば、ホーム画面に入らないで日時や電波状態、電池残量を確認することができるといった技術的意義・機能がある。

また、公然実施発明においては、パスコード認証の設定がされない場合があり、その場合でも、ホームボタンの押下により、スリープ状態からスリープ解除状態に切り替わった時に、ロック画面は表示され、スライダのドラッグ操作により、ホーム画面に遷移する。そうすると、公然実施発明に甲３発明１を組み合わせることで、公然実施発明のホームボタンの背後にセンサを設け、ホームボタンを押下すると、ロック画面が表示されるとともに、指紋認証を行うという構成を得ることができる（別紙４のＡ図）。そして、この構成において、指紋認証に成功した場合には、認証成功後に直ちにホーム画面に遷移する構成（別紙４のＢ図１）及び認証成功後にスライダのドラッグ操作を経て、ホーム画面に遷移する構成（別紙４のＢ図２）を得ることができる。

c　原告は、前記⑴イ（ウ）ｃのとおり、公然実施発明のロック画面はパスコードの入力における意図せぬ誤操作を防止する意義・機能があるとした上で、公然実施発明のロック画面の表示と、甲３発明１の「シームレス」に使用者識別機能を行う構成とは両立しない旨主張する。

しかし、公然実施発明への甲３発明１の組み合わせは、原告が主張

する公然実施発明のロック画面の技術的意義・機能（パスコード認証における誤操作の防止）を損なうものではない。

ウ　小括

以上のとおりであって、本件発明１についての容易想到性に関する本件審決の判断に誤りはない。

２　取消事由２（本件発明２ないし４の進歩性の判断の誤り）

⑴　原告の主張

本件発明２ないし４は、本件発明１の構成を含むものであるところ、前記１⑴で論じたとおり、本件発明１の容易想到性に関する審決の判断には誤りがあるから、同様の点において、本件発明２ないし４の容易想到性に関する審決の判断にも誤りがある。

⑵　被告の主張

前記１⑵のとおり、本件発明１についての容易想到性に関する審決の判断には誤りはないから、本件発明２ないし４の容易想到性に関する審決の判断にも誤りはない。

３　取消事由３（本件発明６の進歩性の判断の誤り）

⑴　原告の主張

ア　本件発明６は、本件発明１の構成を含むものであるところ、前記１⑴で論じたとおり、本件発明１の容易想到性に関する審決の判断には誤りがあるから、同様の点において、本件発明６のうち、本件発明１と共通する構成についての容易想到性に関する審決の判断にも誤りがある。

イ　本件発明６は、「前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて」、「前記使用者の操作以外の追加の操作をすることなく」「顔認識を利用した機能である使用者識別機能」を実行する点においても公然実施発明と相違するところ、甲３文献には、顔の特徴を検出するのは、「ユーザの顔がセンサと向かい合うように配置された時」

（【００５６】）との記載しかなく、検出した顔の特徴を用いた使用者識別機能を実行するタイミング（本件発明６のように、非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて、追加の操作なしに、顔認識による使用者識別機能を実行すること）については、何ら開示されていない。

したがって、甲３発明２を、どのように公然実施発明に組み合わせたとしても、本件発明６に容易に想到することはない。

ウ　小括

以上によれば、本件発明６についての容易想到性に関する本件審決の判断には誤りがある。

⑵　被告の主張

ア　前記１⑵のとおり、本件発明１についての容易想到性についての審決の判断には誤りはないから、本件発明６のうち、本件発明１と共通する構成についての容易想到性に関する審決の判断にも誤りはない。

イ　甲３文献の請求項１５、１７及び１８を併せ読むと、ユーザをシームレスに認証するための電子デバイスであって、ホームボタンがユーザからの入力を受信する時、すなわち、ユーザがホームボタンを押下する時に、ユーザの顔の特徴を検出するカメラにより検出された顔の特徴に基づいて、ユーザを認証するプロセッサを備えた電子デバイスが開示されている。

さらに、甲３文献の【要約】【解決手段】に「センサは、生体情報を提供するためのステップを実行するようユーザに要求することなく、ユーザがデバイスを操作した時に、センサが適切な生体情報を検出できるように、デバイスに配置されてよい」と記載されているように、甲３文献には、顔を検出するセンサがデバイスに備えられており、ユーザがデバイスを操作した時に、顔情報を提供するための追加の操作を実行するようユーザに要求することなく、センサが顔情報を検出できる構成が開示されている。

そして、【０００４】に「電子デバイスは、検出した識別情報を、デバイスのライブラリに格納されている識別情報と比較することによって、ユーザを認証してよい。」と記載されているように、センサが検出した顔情報をデバイスのライブラリに格納されている顔情報と比較することによって、ユーザを認証するプロセスである顔認識による使用者識別機能が行われる構成が開示されている。

以上のとおり、甲３文献の記載に触れた当業者は、甲３文献に開示された顔認識による使用者識別機能が、ユーザがホームボタンを押下したことを受信した時に、ユーザによる追加操作なしに行われるものと理解することができる。

ウ　小括

以上のとおりであって、本件発明６についての容易想到性に関する本件審決の判断に誤りはない。

４　取消事由４（本件発明５の進歩性の判断の誤り）

⑴　原告の主張

本件発明５は、本件発明１の構成を含むものであるところ、公然実施発明２と本件発明５の相違点は、公然実施発明と本件発明１の相違点と同様のものであり、前記１⑴で論じたとおり、本件発明１の容易想到性に関する審決の判断には誤りがあるから、同様の点において、本件発明５の容易想到性に関する審決の判断にも誤りがある。

⑵　被告の主張

前記１⑵のとおり、本件発明１についての容易想到性に関する審決の判断には誤りはないから、本件発明５の容易想到性に関する審決の判断にも誤りはない。

第４　当裁判所の判断

１　明細書の記載事項について

⑴　本件各発明の明細書（甲５０。以下「本件明細書」という。）の発明の詳細な説明には、別紙１の記載がある。

⑵　前記⑴の記載事項によれば、本件明細書には、本件発明に関し、次のような開示があることが認められる。

ア　本件各発明は、移動通信端末機の活性化時に、特定動作が行われるようにするための移動通信端末機に関する（【０００１】）。

イ　最近、スマートフォン等、通信機能だけでなく、他の多様な機能を有する各種端末機が普及しているが、該当機能を実行させるためには端末機が活性化状態、すなわち、ディスプレイがオンの状態で常に操作を行わなければならず、ある機能を追加するためには端末機に該当機能を実行するためのインターフェースまたはボタンを更に追加しなければならなかった。また、これらの端末機には、ディスプレイがオフの状態の非活性化状態から活性化状態に切り替えるボタンが備えられているのが一般的であり、使用者は活性化切り替えボタンを意識的または無意識的に数回押す動作を行うことになるが、通常的な端末機では、活性化切り替えボタンが押された際、使用者が設定した背景画面に、現在時間などの非常に簡単な情報だけが表示されるのが一般的であり、使用者は端末機の活性化ボタンを押した場合、いかなる情報及び興味も得ることができずに、端末機は再び非活性化状態に切り替わることとなるという問題があった（【０００２】、【０００３】、【０００５】）。

ウ　本件各発明は、端末機に備えられた活性化ボタンに多様な動作を組み合わせ、習慣的に押していた活性化ボタンを、単純に押す操作だけで有益な機能を活用することとし、簡単な手続だけで保安が強化された使用者認証プロセスを動作させることを目的とする（【０００６】、【０００８】）。

エ　本件各発明の構成を採ることにより、端末機が非活性状態の際に、活性化ボタンを押すだけで、多様な動作が行われるので、端末機使用の興味を

更に向上させることができ、また、簡単に保安が強化された使用者認証プロセスを動作することができるという効果を奏する（【００１４】、【００１６】）。

２　取消事由１（本件発明１の進歩性の判断の誤り）について

⑴　公然実施発明について

証拠（甲６ないし９、１７）によれば、被告は、本件特許の優先日前において、ｉＯＳ４．２又はｉＯＳ４．３を搭載したスマートフォンを販売していたものであるところ、同スマートフォンに係る発明は、日本国内において公然実施をされた発明（特許法２９条１項２号）に当たり、その構成は、本件審決が公然実施発明として認定したとおりのものであると認められる。

⑵　相違点１の認定に誤りがあるとの主張について

ア　本件発明１の構成及び前記⑴認定の公然実施発明の構成によれば、本件発明１と公然実施発明は、公然実施発明が、使用者の操作が第１の操作である場合、「第２動作」である「カメラ活性化機能、健康情報伝送機能、使用者識別機能、位置情報伝送機能、ハンズフリー機能、または広告表示機能のいずれか」と異なる動作である「第１動作を」「前記使用者の操作以外の追加の操作をすることなく、実行する」ものではない点において異なるものであり、本件審決の相違点１の認定に誤りはない。

イ(ア)　原告は、前記第３の１ア(イ)a のとおり、公然実施発明のロック画面は使用者識別機能を行うに先立ち、同機能を行うのに必要となるスライダのドラッグの操作を受け付けるという特徴があるのに対し、本件発明１ではそのような操作なしに使用者識別機能が行われる旨主張し、これは、本件発明１と公然実施発明とでは、ロック画面の技術的意義を異にするという趣旨と解される。しかし、本件発明１のロック画面については、ロックが解除されていない状態を表示する機能以外の特定がなく、この機能において、公然実施発明のロック画面は本件発明１のロック画

面と共通するから、原告が相違点である旨主張する「前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて前記非活性状態から前記ロック画面が表示された前記活性状態に切り替えるとともに」に係る部分は、一致点というべきである。

（イ） 原告は、前記第３の１⑴ア（イ）ｂのとおり、本件発明１では、第１操作（あるいは第２操作）が使用者識別機能である場合においては、単なる使用者識別機能でなく、「前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて前記非活性状態から前記ロック画面が表示された前記活性状態に切り替えるとともに、・・・前記使用者の操作以外の追加の操作をすることなく」実行される「使用者識別機能」であるとして、本件審決の相違点１の認定が誤りである旨主張する。

しかし、本件審決においても、公然実施発明では、「第１動作を」「前記使用者の操作以外の追加の操作をすることなく、実行する」ものではない点が相違点として認定されているから、本件審決に誤りがあるとはいえず、原告の主張は採用できない。

⑶ 相違点の判断に誤りがあるとの主張について

以下、本件審決認定の相違点１を基準として判断する。

ア 甲３発明１について

（ア） 甲３文献には、別紙２の記載がある。

（イ） （ア）によれば、甲３文献には、以下の開示があることが認められる。

ａ 電子デバイス、特に携帯型電子デバイスにおいて、許可されていない人物がユーザの個人情報にアクセスし閲覧することを防ぐため、パスワードまたはパスコードを提供する方法、付属デバイスをデバイスに接続することによって、承認された指紋または網膜を最初に示す方法があるが、前者は、パスワードまたはパスコードを知っている他の

ユーザがいない限りは、効果的であるが、パスワードまたはパスコードを忘れると許可ユーザがデバイスにアクセスできなくなり、後者は、ユーザがデバイスにアクセスできるまでに求めるステップを増やすため時間がかかり、ユーザにとって煩わしい場合があるという課題があった（【０００２】、【０００３】）。

b　そこで、甲３発明１は、携帯電話のホームボタン８１２の背後に、ユーザの指紋の特徴を検出する少なくとも１つのセンサ７２０を配置し、ロック解除する、または、起動する時に指紋によるユーザ認証を行う使用者識別機能を採用した（【０００３】、【００４９】、【００５０】）。

イ　甲３文献が、相違点１に係る本件発明１の構成を開示するかについて

（ア）　指紋認識による使用者識別機能が、非活性状態から活性状態に切り替えるための操作入力に応じて、ユーザからの明示的な入力を要求することなく行われる点について

a　甲３発明１は、指紋による認証を行う上で「ユーザがデバイスにアクセスできるまでに求めるステップを増やすため、時間がかかり、ユーザにとって煩わしい場合があ」ることを課題とするものであり（【０００３】）、この点からすれば、ホームボタンへの操作入力が、指紋の特徴を検出するための使用者識別機能を兼ねることは当然に想定され、その場合には、ホームボタンの背後に配置されたセンサにより検出した指紋を、検出した指紋を登録された指紋と照合して適合・不適合を判定する処理を使用者による追加操作なしで行うことになる。

原告は、前記第３の１⑴イ(ア)a のとおり、甲３文献には、検出した指紋を登録された指紋と照合して適合･不適合を判定する処理を「ユーザからの明示的な入力を要求することなく」行うことについては、開示されていない旨主張するが、上記に説示したところに加え、甲３

文献の請求項１の「前記入力メカニズムに隣接したセンサを用いて、前記入力を受信する時に前記ユーザの識別情報を検出する工程と、前記検出した情報に基づいて前記ユーザを認証する工程」との記載と、請求項７の「請求項１に記載の方法であって、前記識別情報は、指紋、掌紋、・・・の内の少なくとも１つを含む、方法。」との記載を併せ読めば、ホームボタンの操作入力による指紋を検出する工程と認証工程との間に操作は不要であるから、甲３文献には、ホームボタンへの操作入力以外の追加の操作なしで、ユーザが認証されることが開示されているということができる。

ｂ　原告は、前記第３の１⑴イ(ア)ｂのとおり、甲３文献のいう「起動」には、本件発明１が規定する、非活性状態から活性状態に切り替える操作は含まれないから、指紋認識による使用者識別機能が、非活性状態から活性状態に切り替えるための操作入力に応じて行われる点についても、甲３文献には開示されていない旨主張する。

しかし、一般的に「起動する」の意味としては、「コンピューターなどの機器の電源を入れて、操作できる状態にすること」と解されている（甲４２）ものの、甲３文献は、「例えば、ユーザがデバイスをオンにする、ロック解除する、または、起動する時に、」として、デバイスをオンにすること、デバイスをロック解除すること、デバイスを起動することを並列して記載している。そして、この記載に対応する原文（甲１１）には、「ｆｏｒ ｅｘａｍｐｌｅ ａｓ ｔｈｅ ｕｓｅｒ ｔｕｒｎｓ ｏｎ，ｕｎｌｏｃｋｓ ｏｒ ｗａｋｅｓ ｔｈｅ ｄｅｖｉｃｅ.」との記載があり（[０００４]）、「ｔｕｒｎｓ ｏｎ」と「ｗａｋｅｓ」とが別に例示されているところ、ｗａｋｅがｓｌｅｅｐの対義語であることに鑑みると、甲３文献における「起動する（ｗａｋｅｓ）」がスリープ状態であったものを操作できる状態にするこ

とを意味することは明らかであり、甲３文献の「（デバイスを）起動する」との記載は、本件発明１の「非活性状態」から「活性状態」への切り替えを意味するものである。

また、公然実施発明に係る、ｉＰｈｏｎｅユーザガイド（甲１）の１２頁「ｉＰｈｏｎｅのロックを解除する」の「ホームボタン、またはスリープ／スリープ解除のオン／オフボタンを押して、スライダをドラッグします。」との記載や、ｉＰｈｏｎｅパーフェクトガイド（甲２）の２２頁「スリープとロックの解除」の「スリープ時に電源ボタンかホームボタンを押すと、スリープから復帰してロックを解除できるようなる」との記載によれば、甲３文献の図８Ｂに示される一般的なスマートフォンである「携帯電話のホームボタン（図８Ｂのボタン８１２）」も、スリープ時の操作入力によりスリープ状態を解除する機能を有することは明らかである。そして、甲３文献には、スリープ時のホームボタンに対する操作入力に基づく指紋によるユーザ認証を排除する記載はない。

以上によれば、原告の主張はいずれも採用できない。

（イ） まとめ

よって、甲３文献は、相違点１に係る本件発明１の構成を開示するものといえる。

ウ 動機付けについて

（ア） 公然実施発明と甲３発明１は、技術分野や作用機能を共通にし、甲３文献に接した当業者であれば、公然実施発明には、スリープ状態においてホームボタンを押してから認証を経てデバイスにアクセスできるまでの一連の動作に関して、デバイスのホームスクリーン又はメニューを表示する前に、本人認証のためにパスコードの入力を要求することは、パスコードが知られたり、パスワードを忘れたりするという、甲３発明

１と共通の技術課題が存在することを想起するものといえ、公然実施発明において、許可されていない人物がユーザの個人情報にアクセスし、閲覧することを防ぐため、デバイス機能を有効にする前又はデバイスリソースにアクセスする前の起動時に、デバイスが迅速にユーザを認証することを目的とした甲３発明１を適用する動機付けがあるといえる。

（イ） 原告は、前記第３の１⑴イ（イ）のとおり、公然実施発明では、本件発明１のように、使用者識別機能を、使用者の操作以外の追加の操作をすることなく、実行するという技術思想は全くない旨主張するが、前記(ア)のとおり、甲３発明１に接した当業者であれば、公然実施発明が有する技術課題及び甲３発明１の適用を想起するものといえ、原告の主張する当初の技術思想の相違は、その後の技術適用の動機付けの有無と直接関係するものとはいえないから、原告の上記主張は当を得ないというべきである。

また、原告は、公然実施発明において、ディスプレイがオンにされた後に、更にディスプレイ上のスライダをドラッグすることで初めて認証を実行することには、ユーザの誤操作（意図せざる操作等）による誤動作を防止するという意義があるから、これを改変して本件発明１のように構成することは、公然実施発明の技術的意義・機能を損なう旨の主張もするが、甲３発明１の使用者識別機能を採用し、指紋によるユーザ認証をしても、認証に係る誤操作は防止できるから、公然実施発明の技術的意義・機能を損なうことにはならない。なお、仮に、原告がホーム画面の誤作動防止に係る機能をも指摘しているとしても、そもそも本件発明１においては、ロック画面からホーム画面への移行の仕方については何ら規定していないから、操作入力を行った使用者が正当な使用者と認証された場合に、ディスプレイ上のスライダをドラッグすることで初めてホーム画面に移行する構成も本件発明１の構成に含まれることにな

り（現に本件明細書の図１等においてもスライダが表示されているところである。）、スライダを取り除く改変をしなければ本件発明１の構成に至らないわけではないから、原告の主張は前提を誤るものといえる。したがって、原告の主張は、いずれにしても採用できない。

エ　公然実施発明に甲３発明１を適用した場合に、本件発明１の構成に容易に想到するかについて

(ア)　甲３発明１において、指紋による認証の結果を得るには一定の時間を要することは、明らかである。また、公然実施発明に甲３発明１を適用することで、ホームボタンを押下すると、起動によりディスプレイがオンになり、それと同時に指紋認証を行い（別紙４のＡ図右及びＢ図１左)、認証が成功すれば、追加の操作を要することなく、更にホーム画面に移行するという構成を得ることが可能である（別紙４のＢ図１右)。

そして、本件発明１で特定されるロック画面は、「前記非活性状態の際になされた前記活性化ボタンに対する使用者の操作に基づいて」「表示され」るものであって、ロックが解除されていない状態を表示する機能以外は特定されていない。そうすると、公然実施発明に甲３発明１を適用したものにおいて、ホームボタンの押下後、オンになったディスプレイにホーム画面に移行する前に表示される画面も、客観的にロックが解除されていない状態を表示するものであり、これを「ロック画面」ということができる。

したがって、公然実施発明に甲３発明１を適用した場合、使用者による追加の操作なしに、指紋認識による使用者識別機能が、非活性状態からロック画面が表示された活性状態への切り替えのための操作入力により行われるという、本件発明１の構成に容易に想到するということができる。

(イ)　原告は、前記第３の１⑴イ(ウ) a のとおり、甲３発明１においても、

ロックを解除するために画面上のスライダのドラッグ操作を受け付ける構成となっているから、公然実施発明に甲３発明１を組み合わせた場合には、当業者は、公然実施発明と甲３発明１の共通の技術思想をなす上記構成を残しつつ甲３発明１の指紋認証を行うことを想到することになり、ディスプレイが活性化された後にスライダのドラッグという追加の操作を要することになるから、本件発明１の構成とはならない旨主張する。

しかし、前記イ(ア) a のとおり、甲３文献からは、ホームボタンの背後にセンサを配置し、ユーザが当該ホームボタンを押下した時に、ユーザからの明示的な入力を要求することなく、指紋による認証を行う構成も、甲３発明１として認定することができるのであるから、原告の主張は採用できない。

(ウ) 原告は、前記第３の１⑴イ(ウ) b のとおり、公然実施発明の構成においては、ロック状態の画面を表示させ、その画面上に表示されるスライダがドラッグされたときに初めて、次のパスコードの入力画面に移行し、パスコードを入力させて認証を行う、という一連の認証操作を行わせるものであるから、公然実施発明の使用者識別機能に係る手順のうちロック状態の画面上でのスライダをドラッグする処理を排除するのであれば、ロック画面も用いない構成しか想到できない旨主張する。

しかし、前記(ア)のとおり、「ロック画面」自体は、ロックが解除されていない状態を示す画面であり、スライダのドラッグ操作とロック画面の表示を不可分一体のものとして捉えなければならない理由はないから、原告の主張は採用できない。

(エ) 原告は、前記第３の１⑴イ(ウ) c のとおり、公然実施発明のロック画面は、パスコードの入力における意図せぬ誤操作を防止する意義・機能があるとした上で、甲３発明１の「シームレス」に使用者識別機能を

行う構成とは両立しない旨主張する。しかし、公然実施発明において、甲３発明１の使用者識別機能を採用し、ロック解除する時に指紋によるユーザ認証をしても、偶発的な誤操作等は防止できることは前記ウ(イ)のとおりであって、原告の主張は採用できない。

(オ)　原告は、前記第３の１⑴イ(ウ)ｄのとおり、別紙４のＢ図１左にはスライダが表示されているところ、指紋認証に成功した場合に「当該成功後に直ちにホーム画面に遷移する構成」であるとされる以上、スライダの機能は利用されず、当業者がそのように何ら機能を発揮しないスライダをあえて表示させる構成を考え付くとすれば、本件発明１を見た上での後知恵である旨主張する。

原告の主張の真意は判然としないが、そもそも本件発明１においては、ロック画面からホーム画面への移行の仕方については何ら規定していない（したがって、この場面におけるスライダの表示の有無やその利用の有無等についても何も限定はない）ことは前記ウ(イ)において説示したとおりであるところ、被告の主張如何にかかわらず、公然実施発明に甲３発明１を組み合わせた場合に、正当な使用者と認証されたときに、スライダを利用しようとしなかろうと、どちらにしてもロック画面からホーム画面へ移行させることが可能であること自体は明らかであるから、原告の主張は失当というほかない。

⑷　小括

その他原告がるる主張する点は、いずれもその前提に誤りがある、あるいは理由がないものであり、採用できない。

以上によれば、相違点１についての容易想到性を認めた本件審決の判断に誤りはないから、原告主張の取消事由１は理由がない。

３　取消事由２（本件発明２ないし４の進歩性の判断の誤り）について

前記２において判示したとおり、相違点１についての容易想到性に関する本

件審決の判断には誤りはないところ、原告は、この点以外の点について審決取消事由を主張しておらず、また、その判断に誤りがあるとは認められないから、本件発明２ないし４についての容易想到性に関する本件審決の判断についても誤りはない。

４　取消事由３（本件発明６の進歩性の誤り）について

⑴　本件発明６と公然実施発明の相違点について

本件発明６の構成及び前記２⑴認定の公然実施発明の構成によれば、本件発明６と公然実施発明は、相違点４（相違点１と同じ。）のほか、使用者識別機能について、本件発明６では、「顔認識を利用した機能」であるのに対し、公然実施発明では、「パスコードを入力することによる」機能である点（相違点５）において異なるものといえる。

⑵　相違点の容易想到性の判断に誤りがあるとの主張について

ア　甲３発明２について

甲３文献には別紙２のような記載があり、これによれば、甲３文献には、以下の開示があることが認められる。

（ア）　電子デバイス、特に携帯型電子デバイスにおいて、許可されていない人物がユーザの個人情報にアクセスし閲覧することを防ぐため、デバイス機能を有効にする前、または、デバイスリソースにアクセスする前に、パスワード又はパスコードを提供する方法、具体的には、デバイスのホームスクリーン（例えば、スプリングボード）またはメニューを表示する前に、４つの数字または４つの文字のＰＩＮを入力する方法があり、他方、付属デバイスをデバイスに接続することによって、承認された指紋又は網膜を最初に示す方法があるが、前者は、パスワードまたはパスコードを知っている他のユーザがいない限りは、効果的であるが、パスワードまたはパスコードを忘れると許可ユーザがデバイスにアクセスできなくなり、後者は、ユーザがデバイスにアクセスできるまでに

求めるステップを増やすため時間がかかり、ユーザにとって煩わしい場合があるという課題があり、ユーザがデバイスをオンにする、ロック解除する、または、起動する時に、デバイスが迅速かつシームレスにユーザを認証するように、生体認証および他の認証メカニズムを実装した電子デバイスを提供することが望ましい（【０００２】、【０００３】）。

（イ） 甲３発明２は、ユーザ識別機能として、デバイスの検知素子に対して位置合わせするようユーザに案内することなく、前記ユーザが前記検知素子に対して位置合わせされていることを決定する工程と、前記決定工程に応答して、前記検知素子を用いて前記ユーザの顔の特徴を検出する工程と、前記検出工程に応答して、前記ユーザを認証する工程とにより行う顔認証を使用する（請求項１１、１３、【００５６】）。

イ 容易想到性の判断について

（ア） 相違点４（相違点１と同じ。）について

前記２において判示したとおり、相違点１についての容易想到性に関する本件審決の判断には誤りはなく、相違点４の容易想到性に関する本件審決の判断にも誤りはない。

（イ） 相違点５について

ａ 甲３文献には「例えば、認証システムは、ユーザの顔がセンサと向かい合うように配置された時に、ユーザの顔の１または複数の顕著な特徴によって放射または反射される放射線を検出するセンサを備えてよい。」（【００５６】）と記載されているところ、前記ア(ア)のとおり、同文献には、「ユーザがデバイスをオンにする、ロック解除する、または、起動する時に、デバイスが迅速かつシームレスにユーザを認証するように、生体認証および他の認証メカニズムを実装した電子デバイスを提供することが望ましい」との記載があることからすれば、ユーザがホームボタンを押下してデバイスを起動する際、ユーザ

の顔がセンサと向かい合うように配置された時に、顔の特徴を用いた使用者識別機能が作用することも開示されているものということができる。

b　原告は、前記第３の３⑴イのとおり、甲３文献には、顔の特徴を検出するのは、「ユーザの顔がセンサと向かい合うように配置された時」（【００５６】）との記載しかなく、検出した顔の特徴を用いた使用者識別機能を実行するタイミングについては、何ら開示されていない旨主張する。

しかし、甲３の【０００３】の記載を併せて参照すれば、「起動する時」にデバイスが迅速かつシームレスにユーザを認証することが想定されているというべきであるから、原告の主張は採用できない。

⑶　小括

以上によれば、相違点４及び相違点５についての容易想到性を認めた本件審決の判断に誤りはないから、原告主張の取消事由３は理由がない。

５　取消事由４（本件発明５の進歩性の判断の誤り）について

⑴　公然実施発明２について

証拠（甲６ないし９、１６、１７）によれば、被告は、本件特許の優先日前において、ｉＯＳ４．２又はｉＯＳ４．３を搭載したスマートフォンを販売していたものであるところ、同スマートフォンに係る発明は、日本国内において公然実施をされた発明（特許法２９条１項２号）に当たり、その構成は、本件審決が公然実施発明２として認定したとおりのものであると認められる。

⑵　容易想到性の判断について

本件審決が認定したとおり、相違点６は相違点１と同じであり、相違点７は、使用者識別機能について，本件発明５では，「指紋認識を利用した機能」であるのに対し，公然実施発明２では、「パスコードを入力することによる」

機能である点である。

当業者がこのような相違点について容易に想到することができたことは、相違点１の容易想到性について、前記２において説示したとおりである。

⑶　小括

以上によれば、相違点６及び相違点７についての容易想到性を認めた本件審決の判断に誤りはないから、原告主張の取消事由４は理由がない。

６　結論

以上のとおり、原告主張の取消事由はいずれも理由がないから、本件審決を取り消すべき違法は認められない。

したがって、原告の請求を棄却することとして、主文のとおり判決する。

知的財産高等裁判所第４部

裁判長裁判官　菅　野　雅　之

裁判官　本　吉　弘　行

裁判官

岡　　山　　忠　　広

（別紙１）

【技術分野】

【０００１】

本発明は、移動通信端末機の活性化時に、特定動作が行われるようにするための方法、システム及び移動通信端末機に関し、より詳細には、非活性化状態から活性化状態に切り替えるボタンの押す回数及び時間に応じて多様な機能が実行されるようにするための方法、システム及び移動通信端末機に関する。

【背景技術】

【０００２】

最近、通信機能だけでなく、他の多様な機能を有する各種端末機、例えば、スマートフォン、携帯電話、ＰＤＡ、及びウェブパッドなどの端末機が多く普及されている。このような端末機は、いつどこでもデスクトップパソコンと同一または類似の環境を実現させるだけでなく電話機能も有していて、急速に普遍化される実情である。

【０００３】

このような端末機には、各種機能が含まれているが、現在は、該当機能を実行させるためには端末機が活性化状態、すなわち、ディスプレイがオンの状態で常に操作を行わなければならなかった。また、ある機能を追加するためには端末機に該当機能を実行するためのインターフェースまたはボタンをさらに追加しなければならなかった。例えば、緊急状況に対処するための非常ボタンを別途に追加し、該当ボタンを押すことで、非常状況を知らせて救助信号を伝送することができた。

【０００５】

具体的に、端末機には、ディスプレイがオフの状態の非活性化状態からディスプレイがオン状態の活性化状態に切り替えるボタンが備えられているのが一般的であるが、現在多くの使用者はこのような活性化切り替えボタンを意識的または無意識的に数回押す動作を行う。通常的な端末機では、活性化切り替えボタンが押された

際、使用者が設定した背景画面に、現在時間などの非常に簡単な情報だけが表示されるのが一般的であった。よって、使用者は端末機の活性化ボタンを押した場合、いかなる情報及び興味も得ることができずに、端末機は再び非活性化状態に切り替わることとなる。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

本発明の目的は、端末機に備えられた活性化ボタンに多様な動作を組み合わせ、習慣的に押していた活性化ボタンを、単純に押す操作だけで有益な機能を活用することにある。

【０００８】

本発明のさらに他の目的は、簡単な手続きだけで保安が強化された使用者認証プロセスを動作させることにある。

【００１１】

本発明の一実施形態によれば、ディスプレイ部と、前記ディスプレイ部がオフ状態の非活性化状態から前記ディスプレイ部がオン状態の活性化状態に切り替える活性化ボタンとを含み、前記活性化ボタンが押されることで、前記活性化状態に切り替えるとともに、所定の動作が行われる移動通信端末機が提供される。

【００１２】

本発明の他の実施形態によれば、移動通信端末機の活性化時に、特定動作が行われるようにするための方法であって、ディスプレイ部がオフ状態の非活性化状態から前記ディスプレイ部がオン状態の活性化状態に切り替える活性化ボタンが押されることを感知する段階と、前記非活性化状態において前記活性化ボタンが押されたことが感知されると、前記活性化状態に切り替えるとともに前記移動通信端末機内で所定の動作が行われるようにする段階とを含む方法が提供される。

【００１４】

本発明によれば、端末機が非活性状態の際に、活性化ボタンを押すだけで多様な動作が行われるので、端末機をより有益に活用することができ、端末機使用の興味をさらに向上させることができる。

【００１６】

本発明によれば、簡単な手続きだけで保安が強化された使用者認証プロセスを動作することができる。

【００２３】

本明細書において、「非活性状態」とは、移動通信端末機が通信可能な状態ではあるが、ディスプレイ画面がオフ（ｏｆｆ）の状態を意味する。ディスプレイ画面がオフの状態であっても、所定の機能（例えば、音楽再生機能など）は動作し得る。このように、本明細書において「非活性状態」という用語は移動通信端末機が所定の動作をしているか否かを問わず、ディスプレイ画面がオフの状態を包括する概念である。しかし、移動通信端末機が完全にオフされた状態を除く。

【００２４】

本明細書において、「活性状態」とは、移動通信端末機のディスプレイ画面がオン（ｏｎ）状態の場合を意味する。「非活性状態」から「活性状態」への転換とは、ディスプレイ画面がオフの状態からディスプレイ画面をオン状態に切り替えることを意味することであって、オン状態のディスプレイ画面にどのような情報が表示されるかは問わない。例えば、単にロック画面だけが表示される場合であっても、これは移動通信端末機の「活性状態」といえる。

【００２９】

活性化ボタン１２０は移動通信端末機１００の非活性状態を活性状態に切り替えるようにする手段である。すなわち、移動通信端末機１００が非活性状態の際に、使用者が活性化ボタン１２０を押すと活性状態に切り替わる。図１は、移動通信端末機１００が非活性状態の際に、活性化ボタン１２０を押すことで、ディスプレイ部１１０にロック画面が表示された状態を例示する。しかし、活性化ボタン１２０

は、これとは異なる動作のための手段（例えば、ディスプレイ部１１０にある動作状態が表示される間に待機画面に移動するための手段、現在動作中のプログラムリストを表示する手段）として機能することができる。

３．使用者識別機能

移動通信端末機１００が非活性状態の際に活性化ボタン１２０を押すことで保安のための使用者認証プロセスが進行される。

【００４９】

図４Ａ及び図４Ｂは、このような機能を説明するための移動通信端末機１００のブロック図を示す。図４Ａを参照すると、活性化感知部４１０、使用者識別部４２０を含むことができる。

【００５０】

活性化感知部４１０は、移動通信端末機１００が非活性状態の際に、活性化ボタン１２０が使用者によって押されたか否かを感知する。

【００５１】

使用者識別部４２０は活性化感知部４１０によって活性化ボタン１２０が押されたものと感知した場合に動作を行い、多様な方法で使用者を識別する機能を実行する。

【００５２】

図４Ｂは、使用者識別部４２０の一例を示すブロック図である。図４Ｂを参照すると、使用者識別部４２０は、カメラ活性部４２１、虹彩検出部４２２、使用者識別部４２３を含むことができる。

【００５３】

カメラ活性部４２１は、移動通信端末機１００に備えられたカメラ１３０を活性化させる。カメラ１３０の活性化によってディスプレイ部１１０にはカメラ１３０によって現在照らされた映像が表示される。使用者が自分の目または顔をカメラ１３０に照らすと、虹彩検出部４２２は使用者の眼球のうちの虹彩を認識し、これを

抽出する機能を実行する。虹彩を認識するためには通常的な虹彩検出アルゴリズムを用いることができる。使用者識別部４２３は、虹彩検出部４２２を介して検出された虹彩と既に保存されている使用者の虹彩情報を比較して、マッチングされた場合に現在使用者を正当な使用者として認証する機能を実行する。そのために、使用者識別部４２３はデータベース（図示せず）に保存されている使用者の虹彩情報を利用することができる。使用者の虹彩情報は、最初にカメラ１３０を用いて撮影した正当な使用者の映像を利用して虹彩検出部４２２により検出される虹彩に対する情報登録によって保存されることができる。登録された本当な使用者の虹彩情報変更のためには所定の識別情報（例えば、ＩＤ、パスワード、住民登録番号など）が入力されないとならない。使用者識別部４２３により本当な使用者であると認証されると、移動通信端末機１００のロック状態が解除されてすべての機能を使用することができる状態となり、本当な使用者であると認証されないと、警告メッセージ表示とともにロック状態が持続される。

【００５４】

上記説明した動作、すなわち、虹彩検出及び使用者識別、認証などの機能は所定のアプリケーションのインストールによって可能となる。すなわち、該当のアプリケーションには、虹彩検出アルゴリズム、虹彩比較を介する認証アルゴリズムなどが含まれていて、移動通信端末機１００にインストールされることで、上記のような動作を行うことができる。このようなアプリケーションは、使用者によってダウンロードされた後に移動通信端末機１００にインストールされることができる。使用者は、設定メニューを介して活性化ボタン１２０が移動通信端末機１００の非活性状態で押された場合、該当のアプリケーションが直ちに動作されるように設定することで、上記のような機能を利用することができる。

【００５５】

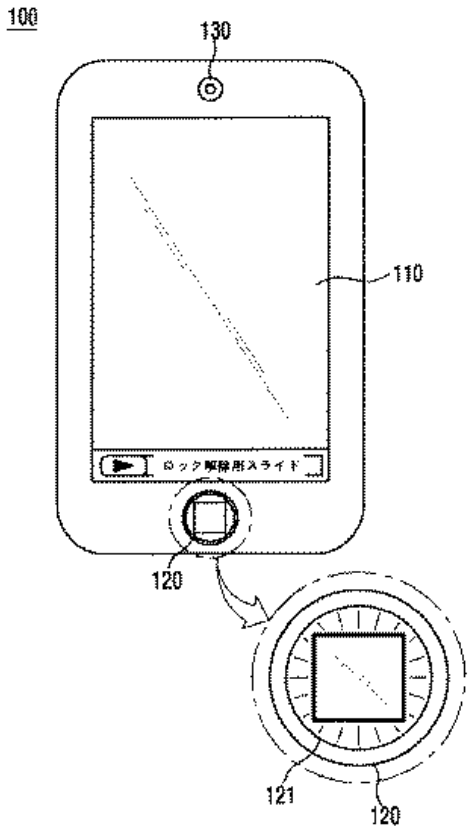
これによれば、保安に脆弱な地域において、移動通信端末機１００を使用する際には、別途の設定、すなわち、活性化ボタン１２０を押し、前記使用者認証プロセ

スが進行されるようにする設定をすることで、効率的に保安危険性を低減させることができる。

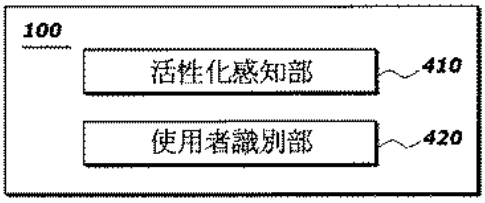
【００５６】

上記説明では虹彩認識を介する認証方法について例として説明したが、これとは異なる方式の認証方法、例えば、認識キーマッチング方法、パスワードマッチング方法、顔面認識方法、指紋認識方法などが用いられる。すなわち、活性化ボタン１２０を押すことで、多様な使用者認証方法のうちのいずれか１つ、または複数の認証方法のうちの任意の方法が行われる。

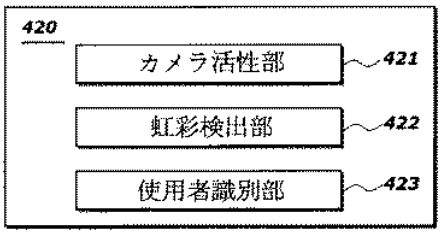
【図１】



【図４Ａ】


100
活性化感知部
410
使用者識別部
420

【図４Ｂ】


420
カメラ活性部
421
虹彩検出部
422
使用者識別部
423

（別紙２）

【要約】

【解決手段】本発明は、デバイスリソースへのアクセスを制限するための内蔵認証システムを備えた電子デバイスに関する。認証システムは、ユーザの生体情報を検出する１または複数のセンサを備えてよい。センサは、生体情報を提供するためのステップを実行するようユーザに要求することなく、ユーザがデバイスを操作した時に、センサが適切な生体情報を検出できるように、デバイスに配置されてよい（例えば、デバイス筐体の別個の部分に指紋センサを設けるのではなく、入力メカニズム内に指紋センサを組み込む）。一部の実施形態において、認証システムは、ユーザを認証するために視覚的または時間的な入力パターンを検出するよう動作してよい。認証に応答して、ユーザは、制限されたファイル、アプリケーション（例えば、ユーザが購入したアプリケーション）、または、設定（例えば、連絡先または保存したゲームプロファイルなどのアプリケーション設定）にアクセスできるようになる。

【特許請求の範囲】

【請求項１】

電子デバイスのユーザをシームレスに認証するための方法であって、

前記電子デバイスの入力メカニズムを用いて、ユーザからの入力を受信する工程と、

前記入力メカニズムに隣接したセンサを用いて、前記入力を受信する時に前記ユーザの識別情報を検出する工程と

前記検出した情報に基づいて前記ユーザを認証する工程と、

を備える、方法。

【請求項７】

請求項１に記載の方法であって、前記識別情報は、

指紋、掌紋、手紋、指関節紋、血管パターン、網膜パターン、虹彩パターン、外

耳道パターン、および、ＤＮＡ配列の内の少なくとも１つを含む、方法。

【請求項１１】

電子デバイスのユーザを認証するための方法であって、

前記デバイスの検知素子に対して位置合わせするよう前記ユーザに案内することなく、前記ユーザが前記検知素子に対して位置合わせされていることを決定する工程と、

前記決定工程に応答して、前記検知素子を用いて前記ユーザの生体属性を検出する工程と、

前記検出工程に応答して、前記ユーザを認証する工程と、

を備える、方法。

【請求項１３】

請求項１１に記載の方法であって、前記検出工程は、さらに、前記ユーザの顔の特徴および前記ユーザの眼の特徴の内の少なくとも１つを検出する工程を備える、方法。

【請求項１５】

ユーザをシームレスに認証するための電子デバイスであって、

ユーザから入力を受信する入力メカニズムと、

前記入力が受信される時に、前記ユーザの識別特徴を検出する検知素子と、

前記検出された識別特徴に基づいて、前記ユーザを認証するプロセッサと、

を備える、電子デバイス。

【請求項１６】

請求項１５に記載の電子デバイスであって、前記検知素子は、前記入力メカニズムに内蔵されている、電子デバイス。

【請求項１７】

請求項１５に記載の電子デバイスであって、前記検知素子は、前記検知素子の視野が、前記入力メカニズムに入力を提供するユーザの少なくとも１つの識別特徴を

捉えるよう配置される、電子デバイス。

【請求項１８】

請求項１５に記載の電子デバイスであって、前記入力メカニズムは、キーボードと、ボタンと、マウスと、タッチパッドと、タッチスクリーンと、スクロールホイールと、の内の少なくとも１つを備える、電子デバイス。

【請求項１９】

請求項１５に記載の電子デバイスであって、前記検知素子は、前記ユーザの皮膚の特徴およびユーザの皮下の特徴の少なくとも一方を検出する、電子デバイス。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、内蔵認証システムを備えた電子デバイスに関する。

【背景技術】

【０００２】

電子デバイス、特に携帯型電子デバイスは、個人情報を格納するために用いられる。例えば、ユーザは、ユーザが用いる連絡先、電子メール、カレンダー情報、文書、および、その他の情報を格納するために、携帯電話、ＰＤＡ、スマートフォン、または、その他の電子デバイスを用いてよい。この情報は、必ずしも秘密にしなくてもよいが、ユーザは、情報の少なくとも一部を他人に利用できなくするよう望んでもよい。許可されていない人物がユーザの個人情報にアクセスし閲覧することを防ぐ方法の１つとして、デバイス機能を有効にする前、または、デバイスリソースにアクセスする前に、パスワードまたはパスコードの提供を電子デバイスのユーザに要求する方法が挙げられる。例えば、電子デバイスは、デバイスのホームスクリーン（例えば、スプリングボード）またはメニューを表示する前に、４つの数字または４つの文字のＰＩＮを入力するよう、ユーザに要求してよい。別の例として、ユーザの指紋を検出するためまたはユーザの網膜を走査するための付属デバイスを

デバイスに接続することによって、ユーザが、デバイスへのアクセス権を受ける前に、承認された指紋または網膜を最初に示さなければいけないようにしてもよい。

【０００３】

これらの方法は両方とも有効でありうるが、パスワードまたはパスコードに基づくアクセス制限は、パスワードまたはパスコードを知っている他のユーザがいない限りは、効果的である。パスワードまたはパスコードが知られると、制限メカニズムは、効果がなくなりうる。また、パスワードまたはパスコードを忘れて、許可ユーザがデバイスにアクセスできなくなる場合もある。さらに、ユーザに指紋を提供するまたは網膜スキャンを受けるよう要求することは、ユーザがデバイスにアクセスできるまでに求めるステップを増やすため、時間がかかり、ユーザにとって煩わしい場合がある。この方法は、パスワードまたはパスコードの入力よりも安全であるが、ハードウェア（例えば、必要なスキャナ、検出器、または、リーダ）のコストと時間がかかる。したがって、例えば、ユーザがデバイスをオンにする、ロック解除する、または、起動する時に、デバイスが迅速かつシームレスにユーザを認証するように、生体認証および他の認証メカニズムを実装した電子デバイスを提供することが望ましい。

【発明の概要】

【０００４】

電子デバイスのユーザを認証するための方法、電子デバイス、および、コンピュータ読み取り可能な媒体が提供されている。一部の実施形態において、電子デバイスは、ユーザをシームレスに認証しうる。電子デバイスは、ユーザから入力を受信してよく、その入力は、電子デバイスの入力メカニズムによって提供される。電子デバイスは、ユーザが、入力メカニズムの中またはその近傍に組み込まれた１または複数のセンサから入力を提供する時に、識別情報を検出してよい。電子デバイスは、検出した識別情報を、デバイスのライブラリに格納されている識別情報と比較することによって、ユーザを認証してよい。例えば、センサは、ユーザの皮膚の特

長、または、ユーザの皮下の特長を検出するためのセンサを含んでよい。センサは、タッチスクリーン、ボタン（例えば、キーボードまたはマウスのボタン）、入力メカニズム近傍のデバイスの筐体（例えば、キーボードの近くのラップトップ筐体）、または、任意の他の適切な位置の少なくとも一カ所に組み込まれてよい。

【０００５】

一部の実施形態において、電子デバイスは、デバイスの検知素子に対して位置合わせするようユーザに指示することなく、ユーザが検知素子に対して位置合わせされていることを決定してよい。例えば、検知素子は、センサの検知領域が、電子デバイスを操作する際に予期されるユーザの位置を含むように配置されてよい。センサは、検知素子を用いて、ユーザの１または複数の生体属性（例えば、顔または眼の特長）を検出してよい。例えば、センサは、デバイスのディスプレイに隣接したカメラまたは光学センサを備えてよい。次いで、ユーザは、検出された生体属性を、電子デバイスに格納された、または、電子デバイスがアクセスできる生体属性のライブラリと比較することによって認証されてよい。

【発明を実施するための形態】

【００３２】

ディスプレイスクリーン４００は、デバイスリソースにアクセスする前に、認証を受けるようユーザに指示する通知４２０を含んでよい（例えば、情報およびアプリケーションを起動するホームスクリーン）。通知４２０は、例えば、ポップアップ、オーバーレイ、新たなディスプレイスクリーン、または、ユーザに指示を提供するための任意の他の適切なタイプのディスプレイなど、任意の適切なタイプの通知を含みうる。電子デバイスは、例えば、ユーザがデバイスのスイッチを入れた時（例えば、その後ディスプレイスクリーン４００を見る時）、第１の認証なしにユーザがデバイスリソースへのアクセスを試みたことに応じて（例えば、エラーメッセージとして）、ユーザによるヘルプの要求に応じて、または、任意のその他の適切な時点など、任意の適切な時に通知４２０を表示してよい。通知４２０は、例え

ば、ユーザが認証を行う方法、許可ユーザのリスト、または、任意のその他の適切な情報など、任意の適切な指示を含んでよい。

【００４５】

センサは、電子デバイス内の任意の適切な位置に配置されてよい。一部の実施形態において、センサは、ユーザが電子デバイスを操作する時または操作し始める時に、ユーザの皮膚の適切な部分を検出するよう動作できるように配置されてよい。センサの位置は、検出すべきユーザの皮膚の部分（例えば、指、手、または、掌）によって異なってよい。図６は、本発明の一実施形態に従って、ユーザの指紋を検出するための電子デバイスのディスプレイの一例を示す概略図である。ディスプレイ６００は、電子デバイスのロックを解除するようユーザに指示するスクリーン６０２を備えてよい。例えば、スクリーン６０２は、ブロック６１０に指を置いてトラック６１２に沿って指をドラッグすることによって、トラック６１２に沿ってブロック６１０をスライドさせて電子デバイスのロックを解除するよう、ユーザに指示する矢印を有するブロック６１０を備えてよい。

【００４９】

リソースへの安全なアクセスを提供するために、電子デバイス７００は、ユーザを特定するためにユーザの指紋の特徴を検出する少なくとも１つのセンサ７２０を備えてよい。シームレスなユーザ体験を提供するために、センサ７２０は、入力メカニズム７１０および７１２の少なくとも一方の中または下に組み込まれてよい。一部の実施形態において、入力メカニズム７１０は、ユーザが電子デバイス７００に入力を提供するために押下しうる複数の別個のキーを備えうるため、１または複数のキーに内蔵されたセンサ７２０を備えてよい。例えば、光学または容量センサは、ユーザが指をキーに置いた（例えば、ユーザの人差し指を「Ｆ」または「Ｊ」キーに置いた）時に、センサがユーザを認証するためにユーザの指先の特徴を検出できるように、キーの上面に配置されてよい。ユーザの指がキーの上に置かれている間にユーザを認証するために、二次元すなわち移動センサが、用いられ得る。

【００５０】

センサ７２０は、電子デバイスにおいてユーザが押下しうる任意のボタンまたはその他の物理的入力の中、近傍、または、裏側に配置されてもよい。例えば、センサ７２０は、携帯型メディアプレーヤまたは携帯電話のホームボタン（例えば、図８Ｂのボタン８１２）の背後に配置されてよい。センサ７２０は、外部のカバーまたは表面（例えば、ガラスまたはプラスチック表面）と、スイッチまたは電子回路に作用する機械的構成要素との間に配置されてよい。例えば、指紋検知メカニズムが、透明な表面の下に組み込まれてよく、そうすれば、検知メカニズムは、その表面を介して、ユーザの指紋の隆線および谷線を検出することができる。一部の実施形態においては、透明な表面を追加しなくてもよい（例えば、検知メカニズムが、ユーザが指を置くことのできる表面を備える場合）。

【００５６】

一部の実施形態において、認証システムは、代替的または追加的に、ユーザの顔の特徴を検出するセンサを備えてもよい。例えば、認証システムは、ユーザの顔がセンサと向かい合うように配置された時に、ユーザの顔の１または複数の顕著な特徴によって放射または反射される放射線を検出するセンサを備えてよい。センサは、任意の適切な種類の放射線を検出するよう動作してよい。例えば、センサは、光センサ（例えば、カメラ）、赤外線センサ、紫外線センサ、スキャニングレーザ、超音波センサ（例えば、ソナー）、または、所望の放射線（例えば、特定の範囲の放射線周波数または周期を持つもの）を検出する任意の他の適切なセンサを含みうる。

【００６５】

電子デバイスは、任意の適切な方法を用いて、許可ユーザを反映する生体情報を取得してよい。例えば、ユーザが特定のデバイスリソースに対して用いるよう認証システムを選択すると、電子デバイスは、ライブラリに格納すべき生体情報（例えば、指紋、眼の走査結果、または、ＤＮＡ配列）を提供するようユーザに指示してよい。電子デバイスは、例えば、視覚的な合図、聴覚的な合図を用いる方法、およ

び、認証システムのセンサの位置を強調または特定する方法など、任意の適切な方法を用いて、生体情報入力を提供するようユーザに指示してよい。取得されてライブラリに格納された生体情報は、ユーザが認証を試みる時に取り出され、ユーザによって提供された生体情報と比較されてよい。提供された生体認証情報がライブラリに格納された情報（例えば、要求されたリソースに関連づけられた情報）と適合する場合、電子デバイスは、制限されたリソースへのアクセスを提供してよい。一部の実施形態において、同様の方法を用いて、非生体認証情報を受信してもよい。

【００７８】

図１５は、本発明の一実施形態に従って、ユーザを認証するための方法の一例を示すフローチャートである。処理１５００は工程１５０２で始まる。工程１５０４で、電子デバイスは、デバイスのユーザを特定してよい。例えば、電子デバイスは、ユーザに関連づけられたユーザ名またはパスワードを受信してよい。別の例として、電子デバイスは、認証システムを用いて認証情報を受信し、受信した認証システムからユーザを特定してもよい。電子デバイスは、例えば、ユーザがデバイスを操作する時に認証情報をシームレスに取得できるように認証システムのセンサを配置することによって、ユーザからの明示的な入力を要求することなく、認証情報を自動的に受信しうる。別の例として、センサは、ユーザがセンサの視野すなわち検知領域内に入るとすぐに、ユーザの属性の特徴を検出するよう動作してもよい。一部の実施形態において、処理１５００は、工程１５０２から工程１５０６に直接移行してもよい。

【００７９】

工程１５０６で、電子デバイスは、制限されたリソースへのアクセス要求が受信されたか否かを判定してよい。例えば、電子デバイスは、ユーザが、特定のユーザに関連づけられたデータ（例えば、連絡先リストまたは他の個人情報）にアクセスするための命令を提供したか否かを判定してよい。別の例として、電子デバイスは、ユーザが、制限されたアプリケーション（例えば、管理者などの特定の階層のユー

ザに制限されたアプリケーション、または、特定のユーザが購入したアプリケーション）にアクセスするための命令を提供したか否かを判定してもよい。制限されたリソースにアクセスするための命令を受信していないと、電子デバイスが判定した場合、処理１５００は、工程１５０６に戻って、ユーザから受ける入力を監視し続けてよい。

【００８０】

一方、工程１５０６で、制限されたリソースにアクセスするための命令を受信したと、電子デバイスが判定した場合、処理１５００は、工程１５０８に進んでよい。工程１５０８で、電子デバイスは、特定されたユーザがリソースへのアクセスを許可されているか否かを判定してよい。例えば、電子デバイスは、ユーザが、制限されたリソースにアクセスするのに適切な認証情報を提供したか否かを判定してよい。電子デバイスは、例えば、通常の使用中に認証情報を取得できるように、デバイスに認証センサを内蔵することによって、ユーザの知るところなく、適切な認証情報を取得してよい。特定されたユーザが許可されていないと、電子デバイスが判定した場合、処理１５００は、工程１５１０に進んでよい。工程１５１０で、電子デバイスは、認証を行うようユーザに指示してよい。例えば、電子デバイスは、認証システム（例えば、上述の認証システムのいずれか）に認証情報を提供するようユーザに指示してよい。一部の実施形態において、電子デバイスは、ユーザによる複数の入力を検出し、それらの入力が、許可ユーザに関連づけられたパターンを有しているか否か、または、許可ユーザに関連づけられた属性を共有しているか否かを判定してよい（例えば、ユーザが、許可ユーザの属性またはパターンに対応する適切な入力を提供したか否かを判定する、または、入力の属性またはパターンが、許可ユーザに関連づけられた属性またはパターンと適合するか否かを判定する）。次いで、処理１５００は、ユーザが適切な認証情報を提供したか否かを判定する工程１５０８に戻ってよい。

【００８１】

一方、工程１５０８で、ユーザが許可されていると、電子デバイスが判定した場合、処理１５００は、工程１５１２に進んでよい。工程１５１２で、電子デバイスは、要求された制限されたリソースへのアクセスをユーザに提供してよい。例えば、電子デバイスは、個人データへのアクセスまたはユーザに固有のアプリケーションへのアクセスをユーザに提供してよい。次いで、処理１５００は、工程１５１４で終了してよい。

【図６】

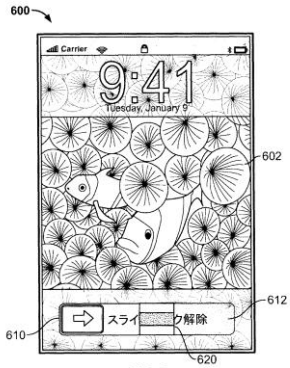


FIG. 6

【図８Ｂ】

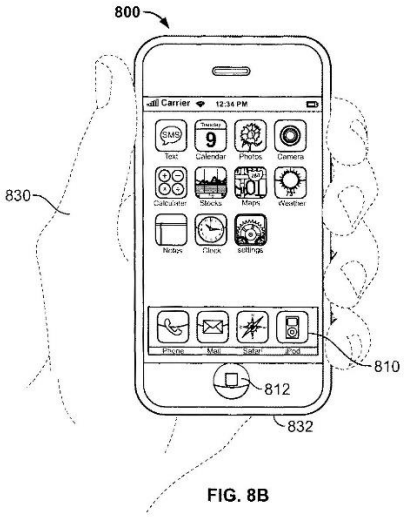


FIG. 8B

【図１５】

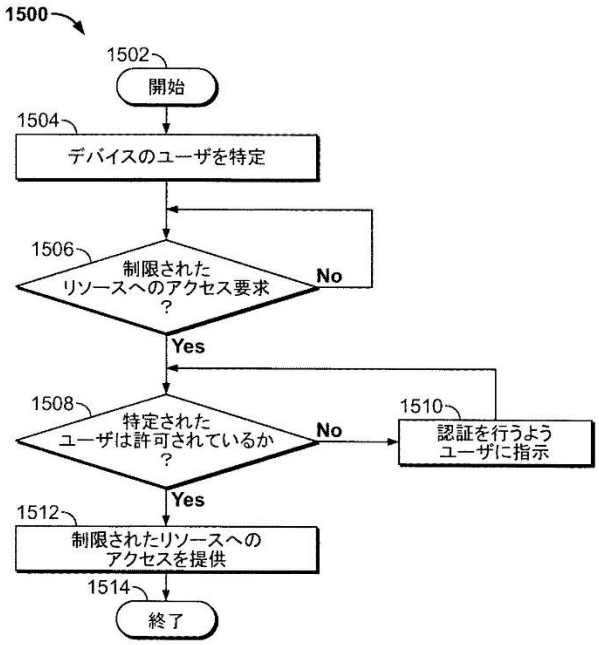
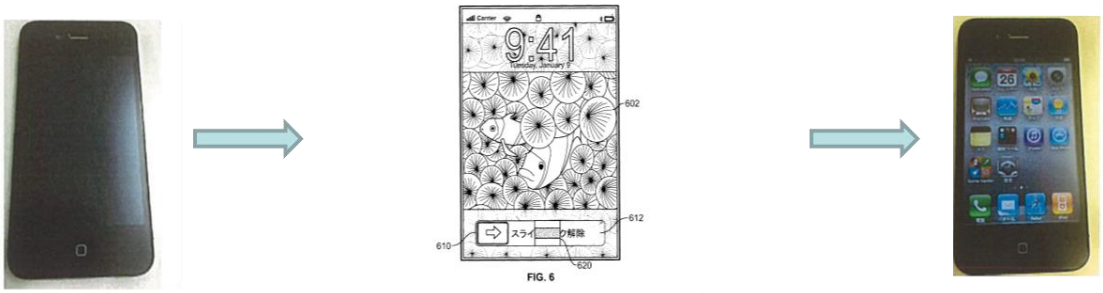

1500
1502
開始
1504
デバイスのユーザを特定
1506
制限された
リソースへのアクセス要求
？
No
Yes
1508
特定された
ユーザは許可されているか
？
No
1510
認証を行うよう
ユーザに指示
Yes
1512
制限されたリソースへの
アクセスを提供
1514
終了

FIG. 15

（別紙３）

１図



<第1段階>
ホームボタンに対
する操作入力

<第2段階>
スライダに対するドラッグ
の操作入力と認証

２図

＜第１段階＞
ホームボタンに
対する操作入力

＜第２段階＞
指紋認識による
使用者識別機能

（別紙４）

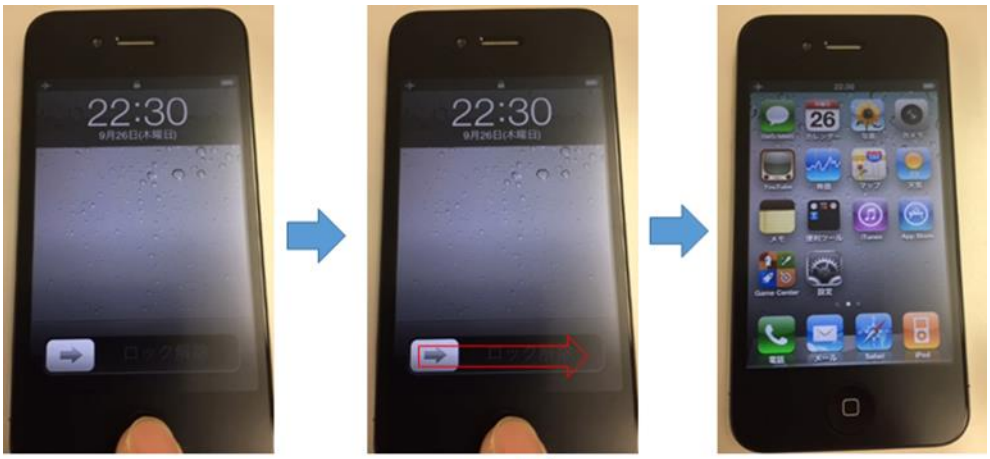
Ａ図


22:30
ホームボタン
の背後にセン
サを設ける。
ホームボタンを押下す
ると、ロック画面が表示
されるとともに、指紋認
証を行う。

Ｂ図１


22:30
直ちに
認証成功
ホーム画面

B図２



5