平成２２年６月１６日判決言渡　同日原本領収　裁判所書記官

平成２１年（行ケ）第１０３１０号　審決取消請求事件

口頭弁論終結日　平成２２年６月２日

判　　決

原　　告		株式会社野村総合研究所
同訴訟代理人弁護士		横　井　康　真
同　　弁理士		森　下　賢　樹
		三　木　友　由
		宗　田　悟　志
被　　告		株式会社セフティーアングル
同訴訟代理人弁護士		栄　枝　明　典
同　　弁理士		伊　丹　　勝
		田　村　和　彦
		千　且　和　也

主　　文

原告の請求を棄却する。

訴訟費用は原告の負担とする。

事実及び理由

第１　請求

特許庁が無効２００８－８００２６５号事件について平成２１年８月２４日にした審決を取り消す。

第２　事案の概要

本件は，原告が，下記１のとおりの手続において，被告の下記２の本件発明に係る特許に対する原告の特許無効審判の請求について，特許庁が同請求は成り立たないとした別紙審決書（写し）の本件審決（その理由の要旨は下記３のとおり）には，下記４のとおりの取消事由があると主張して，その取消しを求める事案である。

１　特許庁における手続の経緯

（１）　被告は，平成１４年４月２６日，発明の名称を「個人認証方法及びシステム」とする特許出願（特願２００２－１２６９３３号）をし，平成１７年5月２０日，設定の登録（特許第３６７８４１７号。以下，この特許を「本件特許」といい，本件特許に係る明細書（甲５）を「本件明細書」という。）を受けた。

（２）　原告は，平成２０年１１月２６日，全１６項からなる請求項のうち，請求項１，２，５，６，９ないし１４に係る発明（以下，請求項の番号に従い，請求項１記載の発明を「本件発明１」などといい，これらを併せて「本件発明」という。）に係る特許について，特許無効審判を請求し，無効２００８－８００２６５号事件として係属した。

（３）　特許庁は，平成２１年８月２４日，「本件審判の請求は，成り立たない。」旨の本件審決をし，同年９月３日，その謄本が原告に送達された。

２　本件発明の要旨

本件発明の要旨は，本件明細書における特許請求の範囲の請求項１，２，５，６，９ないし１４に記載された次のとおりのものである。なお，文中の「／」は原文の改行部分を示す。

【請求項１】ユーザの第１と第２の認証キーのうちの前記第１の認証キーと，前記ユーザの管理マスタＩＤとを第１のシステムで記憶するステップと，／前記ユーザの第１と第２の認証キーのうちの前記第２の認証キーと，前記ユーザの管理マスタＩＤとを，前記第１のシステムと通信可能な第２のシステムで記憶するステップと，／前記第１のシステムにて，前記ユーザから第１の認証キーの入力を受けて，入力された第１の認証キーと，記憶されている前記ユーザの第１の認証キーとを照合することで，第１段階の個人認証を行なうステップと，／前記第１段階の個人認証が成功した場合，前記第１のシステムから前記ユーザに対して，ワンタイムＩＤを発行するステップと，／前記第１のシステムから前記第２のシステムに対し，前記ユーザに発行した前記ワンタイムＩＤと，前記第１段階の個人認証でマッチしたユー

ザの管理マスタＩＤとを通知するステップと，／前記第１のシステムから通知された前記ワンタイムＩＤを，通知された前記管理マスタＩＤに該当するユーザのワンタイムＩＤとして，前記第２のシステムで記憶するステップと，／前記第２のシステムにて，第２の認証キー及びワンタイムＩＤの入力を受けて，入力された第２の認証キー及びワンタイムＩＤを，記憶されている前記ユーザの第２の認証キー及びワンタイムＩＤと照合することで，第２段階の個人認証を行なうステップと，／前記第２段階の個人認証の結果に応じて，前記ユーザへのサービスの提供を制御するステップと／を有する個人認証方法。

【請求項２】前記ユーザの携帯通信端末の識別番号を前記第１のシステムで記憶するステップを，さらに有し，／前記第１段階の個人認証を行なうステップでは，携帯通信端末を通じて前記ユーザから第１の認証キーの入力を受けて，入力された第１の認証キー及び前記入力に使用された携帯通信端末の識別番号を，記憶されている前記ユーザの第１の認証キー及び通信端末の識別番号と照合することで，前記ユーザに関する前記第１段階の個人認証を行なう，請求項１記載の個人認証方法。

【請求項５】ユーザの第１と第２の認証キーのうちの前記第１の認証キーと，前記ユーザの管理マスタＩＤとを記憶した第１のシステムと，／前記ユーザの第１と第２の認証キーのうちの前記第２の認証キーと，前記ユーザの管理マスタＩＤとを記憶した，前記第１のシステムと通信可能な第２のシステムと，／を備え，

（１）　前記第１のシステムは，

（１－１）前記ユーザから第１の認証キーの入力を受けて，入力された第１の認証キーを，記憶されている前記ユーザの第１の認証キーと照合することで，第１段階の個人認証を行なう手段と，

（１－２）前記第１段階の個人認証が成功した場合，前記ユーザに対して，ワンタイムＩＤを発行する手段と，

（１－３）前記ユーザに発行した前記ワンタイムＩＤと，前記第１段階の個人認証でマッチしたユーザの管理マスタＩＤとを，前記第２のシステムに通知する手段

と，／を有し，

（２）　前記第２のシステムは，

（２－１）前記第１のシステムから通知された前記ワンタイムＩＤを，通知された前記管理マスタＩＤに該当するユーザのワンタイムＩＤとして，記憶する手段と，

（２－２）第２の認証キー及びワンタイムＩＤの入力を受けて，入力された第２の認証キー及びワンタイムＩＤを，記憶されている前記ユーザの第２の認証キー及びワンタイムＩＤと照合することで，第２段階の個人認証を行なうステップと，／を有し，／前記第２段階の個人認証の結果に応じてユーザへのサービスの提供を制御可能な個人認証システム。

【請求項６】前記第１のシステムは，／（１－４）前記ユーザの携帯通信端末の識別番号を記憶する手段を，さらに有し，／前記第１のシステムの前記第１段階の個人認証を行なう手段（１－１）は，携帯通信端末を通じて前記ユーザから第１の認証キーの入力を受けて，入力された第１の認証キー及び前記入力に使用された携帯通信端末の識別番号を，記憶されている前記ユーザの第１の認証キー及び通信端末の識別番号と照合することで，前記第１段階の個人認証を行なう，請求項５記載の個人認証システム。

【請求項９】ユーザの第１と第２の認証キーのうちの第２の認証キーと，前記ユーザの管理マスタＩＤとを記憶して前記ユーザの個人認証を行なう認証システムに対して，個人認証の支援を行なうための，前記認証システムと通信可能な個人認証支援システムにより行われる方法において，／ユーザの第１と第２の認証キーのうちの前記第１の認証キーと，前記ユーザの管理マスタＩＤとを記憶するステップと，／記憶されている前記ユーザの第１の認証キーを用いて，予備的な個人認証を行なうステップと，／前記予備的な個人認証が成功した場合，前記ユーザに対して，ワンタイムＩＤを発行するステップと，／前記第２のシステムに対し，前記ユーザに発行した前記ワンタイムＩＤと，前記予備的な個人認証でマッチしたユーザの管理マスタＩＤとを通知するステップと，／を有し，それにより，前記認証システムを

して，前記第１のシステムから通知された前記第１のワンタイムＩＤを，通知された前記管理マスタＩＤに該当するユーザのワンタイムＩＤとして記憶した上で，記憶している前記第２の認証キー及びワンタイムＩＤを用いて前記ユーザの個人認証を行なうことを可能にならしめる個人認証支援方法。

【請求項１０】前記ユーザの携帯通信端末の識別番号を記憶するステップを，さらに有し，／前記予備的な個人認証を行なうステップでは，携帯通信端末を通じて前記ユーザと通信を行なって，前記第１の認証キーとともに，前記通信に使用された携帯通信端末の識別番号も用いて，前記予備的な個人認証を行なう，請求項９記載の個人認証支援方法。

【請求項１１】ユーザの第１と第２の認証キーのうちの前記第２の認証キーと，前記ユーザの管理マスタＩＤと記憶して，前記第２の認証キーを用いて前記ユーザの認証を行なう認証システムに対して，個人認証の支援を行なうための，前記認証システムと通信可能な個人認証支援システムにおいて，／ユーザの第１と第２の認証キーのうちの前記第１の認証キーと，前記ユーザの管理マスタＩＤとを記憶する手段と，／記憶されている前記ユーザの第１の認証キーを用いて，予備的な個人認証を行なう手段と，／前記予備的な個人認証が成功した場合，前記ユーザに対して，ワンタイムＩＤを発行する手段と，／前記第２のシステムに対し，前記ユーザに発行した前記ワンタイムＩＤと，前記予備的な個人認証でマッチしたユーザの管理マスタＩＤとを通知する手段と，／を備え，それにより，前記認証システムをして，前記第１のシステムから通知された前記ワンタイムＩＤを，通知された前記管理マスタＩＤに該当するユーザのワンタイムＩＤとして記憶した上で，記憶されている前記ユーザの第２の認証キー及びワンタイムＩＤを用いて，前記ユーザの個人認証を行なうことを可能にならしめる認証支援システム。

【請求項１２】前記ユーザの携帯通信端末の識別番号を記憶する手段を，さらに備え，／前記予備的な個人認証を行なう手段は，携帯通信端末を通じて前記ユーザと通信を行なって，前記第１の認証キーとともに，前記通信に使用された携帯通信端

末の識別番号も用いて，前記予備的な個人認証を行なう，請求項１１記載の個人認証支援システム。

【請求項１３】ユーザの第１と第２の認証キーのうちの前記第１の認証キーと，前記ユーザの管理マスタＩＤとを記憶して，前記第１の認証キーを用いて前記ユーザの予備的な個人認証を行ない，前記予備的な個人認証が成功した場合には前記ユーザに対してワンタイムＩＤ発行する認証支援システムの支援の下で，前記ユーザの個人認証を行なうための，前記認証支援システムと通信可能な個人認証システムにより行われる方法において，／前記ユーザの第１と第２の認証キーのうちの前記第２の認証キーと，前記ユーザの管理マスタＩＤとを記憶するステップと，／前記認証支援システムでの前記予備的な個人認証が成功した場合，前記ユーザに対して発行されたワンタイムＩＤと，前記予備的な個人認証でマッチしたユーザの管理マスタＩＤとを，前記認証支援システムから通知されるステップと，／前記認証支援システムから通知された前記ワンタイムＩＤを，通知された前記管理マスタＩＤに該当するユーザのワンタイムＩＤとして，記憶するステップと，／記憶されている前記ユーザの第２の認証キー及びワンタイムＩＤを用いて，前記ユーザの第２段階の個人認証を行なうステップと，／を有する個人認証方法。

【請求項１４】ユーザの第１と第２の認証キーのうちの前記第１の認証キーと，前記ユーザの管理マスタＩＤとを記憶して，前記第１の認証キーを用いて前記ユーザの予備的な個人認証を行ない，前記予備的な個人認証が成功した場合には前記ユーザに対してワンタイムＩＤ発行する認証支援システムの支援の下で，前記ユーザの個人認証を行なうための，前記認証支援システムと通信可能な個人認証システムにおいて，／前記ユーザの第１と第２の認証キーのうちの前記第２の認証キーと，前記ユーザの管理マスタＩＤとを記憶する手段と，／前記認証支援システムでの前記予備的な個人認証が成功した場合，前記ユーザに対して発行されたワンタイムＩＤと，前記予備的な個人認証でマッチしたユーザの管理マスタＩＤとを，前記認証支援システムから通知される手段と，／前記認証支援システムから通知された前記ワ

ンタイムＩＤを，通知された前記管理マスタＩＤに該当するユーザのワンタイムＩＤとして，記憶する手段と，／記憶されている前記ユーザの第２の認証キー及びワンタイムＩＤを用いて，前記ユーザの第２段階の個人認証を行なう手段と，／を備えた個人認証システム。

３　本件審決の理由の要旨

本件審決の理由は，要するに，①本件発明１，５，９，１１及び１３は，下記の引用例１記載の発明（以下「引用発明１」という。）と同一ではない，②本件発明１，５，９，１１及び１３は，引用発明１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はない，③本件発明２，６，１０及び１２は，引用発明１及び下記の引用例２記載の発明（以下「引用発明２」という。）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とはいえない，などとしたものである。

（１）引用例１：特開２００２－８２９１０号公報（甲１）

（２）引用例２：特開２００１－１８４３１０号公報（甲２）

４　取消事由

（１）　本件発明の新規性についての判断の誤り（取消事由１）

（２）　本件発明の進歩性についての判断の誤り（取消事由２）

第３　当事者の主張

１　取消事由１（本件発明の新規性についての判断の誤り）について

〔原告の主張〕

（１）　本件発明１の認定の誤り

ア　本件審決は，本件発明１の「管理マスタＩＤ」がユーザごとに設定されていること，すなわち管理マスタＩＤがユーザごとに複数存在することを前提としている。しかしながら，以下のとおり，本件発明１は，管理マスタＩＤがユーザごとに複数存在するものに限られるものではない。

イ　本件発明１は，特許請求の範囲の記載に，いずれの「ユーザ」という記載の前後にも「各」や「ごと」等の複数のユーザの存在を前提とした記載がなく，複数

のユーザの個人認証に限定されるものではないから，「管理マスタＩＤ」についても，ユーザごとに複数存在するものに限定されない。

本件発明１における「管理マスタＩＤ」は，①第１のシステムで記憶されている，②第２のシステムで記憶されている，③第１のシステムから第２のシステムに対して通知される，④第２のシステムでワンタイムＩＤを記憶する際に利用される，と記載され，その技術的意義は明らかであり，リパーゼ判決にいう「特段の事情」があるとはいえない。そのため，本件発明１は，第１，第２のシステムが複数ユーザの管理マスタＩＤを記憶している発明を含むが，当然に，１人のユーザの管理マスタＩＤのみを記憶している発明も含むのであり，第１，第２のシステムが複数ユーザの管理マスタＩＤを記憶していることを前提とした本件発明１の技術的範囲の特定には誤りがある。

ウ　本件発明１を文言どおり正しく認定すれば，本件発明１の「管理マスタＩＤ」は，同一ユーザの第１の認証キーと第２の認証キーをシステム間で関連付けるものであり，ユーザごとに異なるものであるとして，「管理マスタＩＤ」がユーザごとに複数存在するものと限定する本件審決の認定は，誤りである。

（２）　引用発明１の認定の誤り

ア　「ホームサーバアクセス用識別コードＩＤ」の認定の誤り

（ア）　本件審決は，引用例１の【００２１】の記載を根拠に，ホームサーバアクセス用識別コードＩＤは，携帯端末装置を介してユーザにパスワードを発行したホームサーバを識別するコードと解した上，ホームサーバアクセス用識別コードＩＤというのは，ホームサーバをアクセスしようとする者に関する識別コードではなく，アクセスされるホームサーバに関する識別コードであると認定した。

（イ）　引用例１の【００２１】の記載は，Ｗｅｂページが，ホームサーバアクセス用の識別コードＩＤ及びパスワードの入力を要求して，入力された識別コードＩＤ及びパスワードによってユーザを認証するためのページであることを明示しているのであって，まさに，ホームサーバアクセス用識別コードＩＤが，ユーザ認証

のために入力されることを特定しているのであり，引用例１の【請求項３】にも記載するように，識別コードＩＤがユーザを識別するコードであることに疑いはない。

（ウ）　したがって，引用発明１の「ホームサーバアクセス用識別コードＩＤ」は，ホームサーバをアクセスしようとする者に関する識別コードではなく，アクセスされるホームサーバに関する識別コードであるとする本件審決の認定は，誤りである。

イ　「ＵＲＬ」の認定の誤り

（ア）　上記のとおり，本件発明１は，複数ユーザの個人認証に限定されるものではなく，したがって，引用発明１における「ＵＲＬ」が複数のユーザごとに管理されているか否かにかかわらず，当該「ＵＲＬ」は本件発明１の「管理マスタＩＤ」に相当するものである。仮に，本件発明１が複数ユーザについての個人認証に限定されるとしても，引用発明１における「ＵＲＬ」も複数ユーザごとに管理されているものである。

（イ）　引用例１の【０００２】には，通常のユーザ認証の手法として，「予め定められたユーザ識別コード及びパスワードがユーザごとに記憶されており，アクセスがあったときに端末装置に入力されたユーザ識別コード及びパスワードが予め定められたユーザ識別コード及びパスワードと一致することが判定される」ことが示され，【０００３】には，引用発明１の課題として，不正ユーザのアクセスを確実に排除するために，簡単でかつ確実なユーザ認証が望まれていることが示される。

この課題を解決するべく，引用発明１は，「携帯端末装置１１とホームサーバ１との間の通信可能がパスワードの新規発行要求となって，ホームサーバ１は，新たなパスワードを作成し（ステップＳ１４），作成したパスワードを携帯端末装置１１に対して送信する（ステップＳ１５）。ステップＳ１４においてパスワードはホームサーバアクセス用のパスワードであり，例えば，乱数に基づいて生成される。」（【００２９】）などの処理を実行する。すなわち，【０００３】でいうところの「比較的簡単でかつ確実なユーザ認証」とは，予め定められたパスワードを

用いるのではなく，ホームサーバが新たに作成したパスワードを携帯端末装置に送信し，新規パスワードを用いて，その後のユーザ認証が行われることを意味するのである。

（ウ）　引用例１の【０００２】ないし【０００４】には，①通常，ユーザ認証は，ユーザごとに予め定められたユーザ識別コードとパスワードを利用して行われること，②しかしながら，予め定められたパスワードを使用するのでは，不正ユーザがアクセスする可能性もあること，③そこで，不正ユーザによるサーバへのアクセスを確実に排除できるユーザ認証システムを提供することが記載されている。この記載から，不正ユーザによるサーバへのアクセスを排除するためには，個々人を区別する個人認証をしないでよいなどとは，到底読み取ることはできない。

また，そもそも，引用発明１では，ユーザの携帯端末装置の電話番号を用いて，第１段階のユーザ認証が行われている。複数のユーザが存在する場合，それぞれのユーザの携帯端末装置の電話番号は異なるのであり，したがって電話交換局装置は，携帯端末装置の電話番号をもとに，それぞれのユーザを認証するのである。引用発明１のユーザ認証システムでは，このようにユーザの個人認証が行われているのであって，個々人がすでに区別されていることは明らかである。

したがって，引用発明１においても，各ユーザの区別はなされているのであり，その結果，当然に「ＵＲＬ」についても，ユーザごとに管理されているのである。

（エ）　引用例１の【００２５】【００２３】の記載からは，回線接続が許可される特定の電話番号が複数存在する中に携帯端末装置１１の電話番号も含まれるということが理解され，これは引用発明１において複数のユーザが存在することの証左でもある。また，「回線接続要求には少なくとも発信元の電話番号及び着信先の電話番号が含まれる」ことから，複数のユーザがそれぞれ別個の電話番号を用いた場合においても，ホームサーバ１側では回線接続要求において通知されている電話番号により各ユーザを特定できるのであり，単に接続するか否かの２分をしているわけではない。

引用発明１においては，複数のユーザが利用することが前提とされており，かかる

複数ユーザをホームサーバでも区別すべく，それぞれの電話番号が通知されているのであるから，個別のユーザごとにＵＲＬが用意されているのは当然である。

（オ）　以上のとおり，引用発明１の「ＵＲＬ」がユーザごとに管理されていないとする本件審決の認定は，明らかに誤りである。

〔被告の主張〕

（１）　本件発明１の認定について

ア　本件審決は，「管理マスタＩＤ」が，「同一ユーザの第１の認証キーと第２の認証キーをシステム間で関連付けるものであり，ユーザごとに異なるものである」と認定しているところ，これは「管理マスタＩＤ」の性質を認定しているのであって，「ユーザごとに複数存在する」ことを認定しているのではない。

イ　本件発明１は，特許請求の範囲記載のとおり，「管理マスタＩＤ」は「ユーザの管理マスタＩＤ」であってユーザに固有のものであり，「ユーザ」ごとに異なるものでなければ，「管理マスタＩＤに該当するユーザ」を特定することはできないから，「ユーザごとに異なる」ことは明らかである。

ウ　本件発明１は，「ユーザの第１と第２の認証キーのうち前記第１の認証キーと，前記ユーザの管理マスタＩＤとを第１のシステムで記憶」し，「前記ユーザの第１と第２の認証キーのうちの前記第２の認証キーと，前記ユーザの管理マスタＩＤとを，前記第１のシステムと通信可能な第２のシステムで記憶する」ものであり，「第１と第２の認証キーを，異なるシステムが分離して記憶する。また，第１と第２のシステムは，ユーザを識別するための管理マスタＩＤを記憶している。」（本件明細書【０００８】）というものであるから，「管理マスタＩＤ」は，「同一ユーザの第１の認証キーと第２の認証キーをシステム間で関連付けるもの」であることは明らかである。

エ　よって，「管理マスタＩＤ」は，「同一ユーザの第１の認証キーと第２の認証キーをシステム間で関連付けるものであり，ユーザごとに異なるものである」とした本件審決の認定に何ら誤りはない。

（２）　引用発明１の認定について

ア　「ホームサーバアクセス用識別コードＩＤ」の認定

（ア）　原告の主張は，引用発明１が，ユーザごとに識別されるものであることを前提とした主張であって，その前提自体に誤りがある。

引用発明１において個々のユーザを識別する必然性は，その目的及び電話交換局装置の動作からみても存在しない。したがって，引用例１から，「ホームサーバアクセス用識別コードＩＤ」が個々のユーザを識別する機能を持つものであると読み取ることはできない。むしろ，特定のユーザのみがホームサーバにアクセスするために入力するものであり，その名称のとおり，「ホームサーバアクセス用識別コードＩＤ」は，アクセスされるホームサーバに関する識別コードと解すべきである。

（イ）　また，引用例１の【００１９】【００２１】の記載からも明らかなように，「ユーザＰ」と「ホームサーバ１」とは，一体であって，「ユーザ」を識別するということは，「ホームサーバ」を識別することにほかならない。よって，この点からも本件審決の認定に誤りはない。

イ　「ＵＲＬ」の認定

（ア）　引用例１にはWWWサーバが複数のユーザに対応してユーザ対応に複数のＵＲＬを有する構成について直接的な記載がない点については原告も認めるところであるから，原告の主張は，引用例１の記載から「WWWサーバが複数のユーザに対応してユーザ対応に複数のＵＲＬを有する構成」が当業者であれば読み取れるという主張に絞られる。

（イ）　引用例１の【０００２】ないし【０００４】の記載によれば，引用発明１は，【０００２】で述べた従来の手法とは異なる新たな「ユーザ認証システム及びユーザ認証方法を提供する」ものであることは明らかであり，【０００２】で述べた「従来のユーザ認証の手法をそのまま適用するものではない」とした本件審決の認定に誤りはないことは明らかである。

（ウ）　また，引用例１の【００２５】の記載によれば，「交換局装置３ａ」が，

特定の電話番号を持つ携帯端末装置１１のみをモデム２に回線接続することしか開示されておらず，たとえ複数のユーザがホームサーバ１を利用するとしても，「交換局装置３ａ」は，ホームサーバ１へ接続するかどうかの機能しか開示されていないのであるから，「電話交換局装置は，発信元電話番号により携帯端末装置のユーザを特定の人か特定の人以外かに２分しているだけであり」との本件審決の認定に誤りはない。逆に，上記記載をもって，「電話交換局装置は，携帯端末装置番号をもとに，それぞれのユーザを認証する」との原告の主張には，何ら根拠がない。

（エ）　さらに，引用例１の【００３２】の記載のとおり，WWWサーバのＵＲＬを指定するのは，ホームサーバ１であるのに対し，回線接続選択を行うのは，電話交換局装置３ａであって，ホームサーバ１ではない。したがって，「電話交換局装置」が回線接続選択機能を実行することをもって，「ホームサーバ」が管理する「ＵＲＬ」について，「その結果，当然に「ＵＲＬ」についてもユーザごとに管理されている」との結論を導き出す根拠は全く存在しない。

（オ）　以上のとおり，引用発明１の「ＵＲＬ」がユーザごとに設定されているとみることはできないから，引用発明１の「ＵＲＬ」は本件発明１の「管理マスタＩＤ」に相当するものではないとした本件審決の認定に誤りはない。

２　取消事由２（本件発明の進歩性についての判断の誤り）について

〔原告の主張〕

（１）　仮に，別々のユーザが近接した時間に連続してホームサーバ１にアクセスする状況が特殊であったとしても，ユーザ認証システムを設計する当業者の常識からして，特殊な状況でも機能不全とならないようにシステムは構築されなければならない。そのためには，携帯端末装置番号ごとのユーザ認証を行う引用発明１において，ＵＲＬがユーザごとに異なっていればよいのであって，このことは当業者にとってみれば当然のことである。引用発明１のユーザ認証システムでは，ユーザ個人を認証するために，もともとユーザごとの携帯端末装置番号が管理されているのであり，したがって，ユーザごとにＵＲＬを割り当てることは自然のことである。

本件審決は，この点に関し，あえて，「認証用Ｗｅｂページを表示するためのＵＲＬに関連してユーザごとのデータを記録すれば足りる」などと述べるが，その場合には，ＵＲＬで指定される記憶領域に，ユーザごとのホームサーバアクセス用識別コードＩＤとパスワードとが記録されることになるため，Ｗｅｂページで入力された識別コードＩＤ及びパスワードは，記憶領域内のそれぞれの識別コードＩＤ及びパスワードと比較されることとなり，認証処理は複雑となる。一方，ＵＲＬをユーザごとに割り当てれば，認証処理は，単純に１つの識別コードＩＤ及びパスワードと比較するだけですむ。このように，ＵＲＬをユーザごとに割り当てる方が処理が簡潔になることは，当業者に自明の事項であるから，ユーザごとにＵＲＬを割り当てることは自然である。

（２）　以上のように，仮に引用発明１においてＵＲＬがユーザごとに設定されていると直接的にいえないとしても，引用発明１においてＵＲＬをユーザごとに設定し，割り当てることは当業者にとっては当然の設計的事項といい得るものである。また，仮に，引用例１にＵＲＬがユーザごとに設定されていることが記載されていないとしても，引用発明１のユーザ認証システムは，もともとユーザ個人を認証するために，ユーザごとの携帯端末装置の電話番号が管理されているのであるから，ユーザごとにＵＲＬを割り当てることは自然なことである。

よって，本件発明１は，引用発明１に基づき容易に発明できるものである。

（３）　被告の主張について

引用例１の【００６４】の記載によると，引用発明１においても，別々のユーザが近接した時間に連続してホームサーバ１にアクセスする事態は十分にあり得ることである。かかる事態における対処としては，ユーザごとにＵＲＬを設定しておくのが最も簡便な方法であり，仮に引用発明１において「ＵＲＬをユーザごとに設ける」ことが記載されていないとしても，それは当業者における単なる設計的事項といえるものにすぎない。

（４）　よって，本件発明１は引用発明１に基づき容易に発明することができた

ものではないとする本件審決の判断には誤りがある。

〔被告の主張〕

（１）　引用例１には，ユーザＡとユーザＢとが連続してホームサーバにアクセスすることを想定する記載も示唆もなく，また，そもそも引用発明１は，複数のユーザＡ，Ｂが連続してホームサーバにアクセスできるように構成されたものではない。

（２）　引用発明１が，複数のユーザＡ，Ｂが連続してホームサーバにアクセスできるように構成されたものでないことは，引用例１の図２及び【００２７】ないし【００３３】の記載から明らかである。

すなわち，ホームサーバ１は，ユーザＰの携帯端末装置１１からの回線接続要求に基づいて，パスワードを携帯端末装置１１に発行した後，携帯端末装置１１との回線を遮断し（ステップＳ１８），インターネット１０にダイアルアップ接続することにより，ＩＰアドレスを取得する（ステップＳ２５）。このＩＰアドレスがアクセス先データとしてWWWサーバ５の所定ＵＲＬで指定される記憶領域内に新たなアクセス先データとして記憶され（ステップＳ２９），以後，ホームサーバ１は，WWWサーバ５を通じてユーザＰがホームサーバ１にアクセスして来るのをインターネット１０に接続した状態で待機することになる。

したがって，引用発明１の技術思想には，そもそも複数のユーザＡ，Ｂがホームサーバ１に連続してアクセスすることを想定しておらず，仮にユーザＡとユーザＢとが連続してアクセスしたとしても，ユーザＡの回線接続要求によってインターネット１０にダイアルアップしたホームサーバ１は，ユーザＡからのインターネット１０を経由したアクセス待ち状態であるから，ユーザＢの携帯端末装置１１は，ホームサーバ１とは接続できないのである。したがって，引用例１の開示内容から，複数ユーザの同時連続的なアクセスを想定することはできない以上，そのようなケースを前提とした原告の主張は，そもそも前提が誤りである。

仮に，引用例１の開示内容から複数ユーザの利用を想定できるとすれば，せいぜ

いユーザＡのホームサーバ１へのアクセスが終了し，ホームサーバ１がインターネットから切断された後に，別のユーザＢがホームサーバ１にアクセスして再度インターネットにダイアルアップ接続するというケースである。このように，１人のユーザが，ホームサーバへの回線接続からインターネット終了まで回線を占有していることは，引用例１の図２及び【００２７】ないし【００３８】に明示されている。このようなケースでは，ホームサーバに同時アクセス可能なユーザは必ず１人であるから，ユーザごとに「ＵＲＬ」を割り当てる必要はない。すなわち，ホームサーバに１つの「ＵＲＬ」が割り当てられていれば足りる。したがって，引用例１の開示内容から，仮に複数ユーザの利用を想定したとしても，「ＵＲＬ」がユーザごとに設けられなくてはならない必然性は存在しない。

（３）　なお，「電話交換局装置」の回線接続選択機能をもって，「ユーザごとにＵＲＬを割り当てることは自然」とはいえないから，原告の上記主張は失当である。

「ＵＲＬ」がユーザごとに割り当てられるためには，ホームサーバに，ユーザの「電話番号」と「ＵＲＬ」とを対応させる手段を設け，回線接続時にこれを参照することが必要であるが，引用例１には，予め定められた携帯端末装置以外の回線接続を交換局装置で遮断することは開示されていても，それ以上のことは何ら開示されていないのであり，原告の上記主張は，引用発明１を拡大解釈にしたにすぎない。

（４）　よって，本件発明１は引用発明１に基づいて容易に発明することができたものということはできないとした本件審決の認定に誤りはない。

第４　当裁判所の判断

１　取消事由１（本件発明の新規性についての判断の誤り）について

（１）　本件発明１の認定

ア　本件明細書の記載（甲５）

本件明細書の【発明が属する技術分野】（【０００１】），【従来の技術】（【０００４】），【発明が解決しようとする課題】（【０００７】～【００１

０】），【発明の実施の形態】（【００１７】～【００２４】，【００２７】～【００３３】）の記載によると，本件発明１は，ワンタイムＩＤを利用した個人認証方法において，ユーザの個人認証の信頼性や安全性を向上させることを課題とし（【０００４】，【０００７】），ワンタイムＩＤを発行する認証支援システム(第１のシステム)と，ユーザがサービスを利用するための個人認証を行なう認証システム(第２のシステム)とが，ユーザに固有の会員ＩＤ（第１の認証キー）とパスワード（第２の認証キー）とを分離して管理するとともに（【０００８】，【００１７】～【００２４】），ユーザの管理マスタＩＤを共通に登録しておき（【０００８】【００２９】），認証支援システム(第１のシステム)が，発行したワンタイムＩＤを認証システム(第２のシステム)に通知するとき，管理マスタＩＤを一緒に通知し，認証システム(第２のシステム)が，ワンタイムＩＤがどのユーザに対して発行されたものかを認識できる構成（【０００９】，【００２７】～【００３３】）としたものであると解される。

イ　「管理マスタＩＤ」の技術的意義

本件発明１の「管理マスタＩＤ」は，認証支援システム（第１のシステム）と認証システム（第２のシステム）に共通に登録された識別コードであって，本件明細書の【００２９】の記載を参照すれば，「管理マスタＩＤ」について，「各会員のデータとして，上記の携帯電話番号や会員ＩＤのほかに，認証システム６がその会員を識別するためにその会員にユニークに割り当てたＩＤ」であることから，会員ＩＤ（第１の認証キー）及びパスワード（第２の認証キー）と同様に，ユーザごとに設定された，ユーザ固有の識別コードということができる。

また，「管理マスタＩＤ」は，認証支援システム（第１のシステム）がユーザに発行したワンタイムＩＤを認証システム（第２のシステム）に通知する際，ワンタイムＩＤと一緒に通知することにより，認証システム（第２のシステム）において，通知されたワンタイムＩＤがどのユーザに対して発行されたものかを認識できるようにする機能を有するものであるから，複数のユーザが存在することを前提に，第

１のシステムのユーザと第２のシステムのユーザとを関連付け，システム間でユーザを識別し同定するために設定されたものということができる。

ウ　原告の主張について

原告は，本件発明１には，いずれの「ユーザ」という記載の前後にも「各」や「ごと」等の複数のユーザの存在を前提とした記載がなく，複数のユーザの個人認証に限定されるものではないから，「管理マスタＩＤ」についても，ユーザごとに複数存在するものに限定されず，単一のユーザの「管理マスタＩＤ」のみを記憶している発明も含まれると主張する。

しかし，上記イのとおり，認証システム（第２のシステム）は，「管理マスタＩＤ」がワンタイムＩＤと一緒に通知されることによって，通知されたワンタイムＩＤが，複数のユーザのうち，どのユーザに対して発行されたものかを認識できるのであって，原告の主張するように単一のユーザを想定するとすれば，「管理マスタＩＤ」を通知するまでもなく，ワンタイムＩＤに対応するユーザは当該単一のユーザにおのずと特定されるものであるから，そもそも「管理マスタＩＤ」を通知する意義が存しないこととなるのである。

また，本件発明１に係る特許請求の範囲の記載によると，ユーザが単一である場合を含むか否か一義的に明確とはいえないところ，本件明細書の発明の詳細な説明の「ユーザを識別するための管理マスタＩＤ」（【０００８】），「その会員を識別するためにその会員にユニークに割り当てたＩＤ」（【００２９】），「全ての会員の各々について，管理マスタＩＤ…が予め登録」（【００２９】），「既にデータベース７に格納されている様々な会員のワンタイムＩＤとパスワードのセットの中から…マッチするものを探す」（【００３２】）等の記載を参酌すれば，ユーザが単一の場合を含まないものと解される。

したがって，本件発明１において，文言上，複数のユーザが存在することや，「管理マスタＩＤ」がユーザごとに複数存在することが記載されていないとしても，ワンタイムＩＤと一緒に「管理マスタＩＤ」を通知することが特定されている以上，

複数のユーザが存在することを前提とした発明であって，「管理マスタＩＤ」は，その複数のユーザを識別するために，ユーザごとに複数設定されるものというべきである。

よって，原告の上記主張は理由がない。

（２）　引用発明１の認定

ア　引用例１の記載（甲１）

引用例１の【発明が属する技術分野】（【０００１】），【従来の技術】（【０００２】）【発明が解決しようとする課題】（【０００３】【０００４】），【発明の実施の形態】（【００１９】，【００２１】～【００３７】），【発明の効果】（【００６５】）の記載によると，引用発明１は，端末装置からインターネット等のネットワーク回線に接続されたホームサーバにアクセスする際のユーザ認証方法において，比較的簡単な構成で，特定のユーザ以外の不正ユーザによる端末装置からのホームサーバへのアクセスを確実に排除することを課題とし（【０００１】【０００４】），その解決手段として，次の構成を備えたものであるということができる。

固定端末装置からホームサーバにアクセスしようとするユーザは，まず新たなホームサーバアクセス用のパスワードを取得するために，携帯端末装置から公衆電話回線網を介してホームサーバと通信する。ユーザが携帯端末装置から回線接続要求すると，電話交換局装置は，携帯端末装置の電話番号が特定の電話番号に含まれる場合，回線接続を実行する（【００２５】～【００２８】）。携帯端末装置とホームサーバとの間の通信が可能になると，ホームサーバは，新たなホームサーバアクセス用のパスワードを作成し，作成したパスワードを携帯端末装置に送信するとともに（【００２９】【００３０】），インターネットに接続してWWWサーバにアクセスし，所定のＵＲＬで指定される記憶領域内のホームサーバアクセス用のパスワードデータとホームサーバへのアクセス先データ（ＩＰアドレス）を，それぞれ新たなパスワードとＤＨＣＰサーバから取得したＩＰアドレスに更新する（【００

３１】～【００３３】）。ユーザが固定端末装置を用いてホームサーバにアクセスするためにWWWサーバにアクセスすると（【００３３】），WWWサーバは，ユーザが所定のＵＲＬで指定される記憶領域に保存した，ホームサーバアクセス用の識別コードＩＤ及びホームサーバアクセス用のパスワードの入力を要求するＷｅｂページの表示データを，固定端末装置に送信する（【００３４】）。ユーザが識別コードＩＤ及びパスワードを入力し送信すると（【００３５】），WWWサーバは，受信した識別コードＩＤ及びパスワードが記憶領域内の識別コードＩＤ及びパスワードと一致するか否を判別し（ユーザ認証動作），認証が完了すると，所定のＵＲＬで指定される記憶領域に保存されているホームサーバへのアクセス先データ（ＩＰアドレス）を固定端末装置に送信する（【００３６】）。この結果，固定端末装置は，ホームサーバのＩＰアドレスにアクセスし，ホームサーバと通信することができるようになる（【００３７】）。

すなわち，ユーザは，特定の電話番号の携帯端末装置から電話交換局装置を介してホームサーバと通信して新たなホームサーバアクセス用のパスワードを取得した後，固定端末装置からWWWサーバにアクセスし，所定のＵＲＬで指定される記憶領域のＷｅｂページから，ホームサーバアクセス用の識別コードＩＤと取得した新たなホームサーバアクセス用のパスワードとを入力し，ユーザ認証を受けることにより，固定端末装置からホームサーバにアクセスできる構成としたものである。

イ　「ホームサーバアクセス用の識別コードＩＤ」の技術的意義

（ア）　引用例１の【００２１】には，「ユーザＰはＷｅｂページを形成する表示データをWWWサーバ５の所定のＵＲＬ（ユニホームリソースロケータ）で指定される記憶領域に保存させている。そのＷｅｂページはホームサーバ１へのアクセスを許可するためにホームサーバアクセス用の識別コードＩＤ及びパスワードの入力を要求して入力された識別コードＩＤ及びパスワードによってユーザを認証するページである。」と記載されている。よって，ホームサーバアクセス用の識別コードＩＤ及びホームサーバアクセス用のパスワードは，特定のホームサーバにアクセ

スするための識別コードＩＤ及びパスワードであって，WWWサーバは，前記のとおり，ホームサーバアクセス用の識別コードＩＤ及びホームサーバアクセス用のパスワードが，所定のＵＲＬで指定される記憶領域に保存された識別コードＩＤ及びパスワードと一致するか否を判別することによって，固定端末装置から特定のホームサーバにアクセスしようとするユーザを認証し，特定のユーザ以外の不正ユーザが特定のホームサーバにアクセスすることを排除しており，「ホームサーバアクセス用の識別コードＩＤ」は，ホームサーバアクセス用のパスワードとともに使用されることによって，特定のホームサーバにアクセスできる特定のユーザを識別する機能を有する識別コードということができる。

（イ）　これに対し，本件審決は，ホームサーバアクセス用識別コードＩＤというのは，ホームサーバをアクセスしようとする者に関する識別コードではなく，アクセスされるホームサーバに関する識別コードであると認定した。

被告は，引用発明１には，個々のユーザを識別する必然性はなく，「ホームサーバアクセス用の識別コードＩＤ」が個々のユーザを識別する機能を持つものと解釈することはできないから，アクセスされるホームサーバに関する識別コードと解すべきであると主張する。引用発明１の課題は，特定のユーザ以外の不正ユーザによる端末装置からのホームサーバへのアクセスを排除することであるから，ユーザ認証において個々のユーザを識別する必要性はなく，また，「ホームサーバアクセス用の識別コードＩＤ」は，ホームサーバアクセス用のパスワードとともに使用されることによって，特定のユーザを識別する機能を達成できるのであるから，それ自体が個々のユーザを識別する機能を有するということはできない。しかし，「ホームサーバアクセス用の識別コードＩＤ」は，個々のユーザを識別する機能を有しないとしても，特定のホームサーバにアクセスできる特定のユーザを識別するユーザ認証において使用されるものである以上，ホームサーバをアクセスしようとする者に関する識別コードではないということはできない。「ホームサーバアクセス用の識別コードＩＤ」は，アクセスされるホームサーバに関する識別コードであるとと

もに，ホームサーバにアクセスしようとするユーザ認証に関する識別コードと解される。

したがって，本件審決の上記認定は，ユーザ認証に関する識別コードであることを否定する趣旨であるとすれば，是認することができない。

ウ　「ＵＲＬ」の技術的意義

（ア）　引用発明１における「所定のＵＲＬ」（以下「ＵＲＬ」という。）は，引用例１の【００２１】の記載によると，Ｗｅｂページを表示するデータ，ホームサーバアクセス用の識別コードＩＤ，ホームサーバアクセス用のパスワードデータ及びホームサーバへのアクセス先データ（ＩＰアドレス）を保存するWWWサーバの記憶領域を指定するものであり，WWWサーバには，「ＵＲＬ」が記憶されているということができる。

Ｗｅｂページは，ユーザがWWWサーバにアクセスすると，ユーザの固定端末装置に送信され，ユーザに識別コードＩＤとパスワードの入力を要求し，入力された識別コードＩＤとパスワードによってユーザを認証するページであり，ユーザが保存させたものである（【００２１】）。また，ホームサーバアクセス用のパスワードデータ及びホームサーバへのアクセス先データ（ＩＰアドレス）は，ユーザが携帯端末装置からホームサーバに回線接続要求をし，通信可能になったとき，ホームサーバによって作成されたデータ及びＤＨＣＰサーバから割り当てられたＩＰアドレスであり，ホームサーバの指示により更新されるものである（【００３２】）。

また，ホームサーバは，新たなホームサーバアクセス用のパスワードを作成すると，WWWサーバにアクセスし，「ＵＲＬ」で指定される記憶領域内のホームサーバアクセス用のパスワードデータとホームサーバへのアクセス先データ（ＩＰアドレス）を更新することから，ホームサーバには，「ＵＲＬ」が記憶されているということができる。

（イ）　本件発明１の「管理マスタＩＤ」は，前記（１）イのとおり，複数のユーザが存在することを前提に，第１のシステムのユーザと第２のシステムのユーザ

とを関連付けるために，ユーザごとに設定されたユーザ固有の識別コードといえるから，引用発明１における「ＵＲＬ」が本件発明１の「管理マスタＩＤ」に相当するというためには，少なくとも，引用発明１が，複数のユーザが存在することを前提とした発明であり，「ＵＲＬ」が，ユーザごとに設定されたユーザ固有のものであることが必要である。

しかし，引用例１には，「この実施例では説明を簡単にするために携帯端末装置１１だけを示しているが，これに限らず，複数の携帯端末装置があっても良い。」（【００２３】）との記載があり，ホームサーバと通信できる携帯端末装置が複数存在することは示唆されているものの，ホームサーバにアクセスできる複数のユーザが存在すること及び「ＵＲＬ」がユーザごとに設定されていることは，明示されていない。

また，引用発明１は，前記イのとおり，特定のユーザ以外の不正ユーザによる端末装置からのホームサーバへのアクセスを排除することを課題とした発明であり，特定のユーザが，少なくとも１人いれば実施できるものであるから，引用発明１が，複数のユーザが存在することを前提としているということはできない。

さらに，引用発明１において，「ＵＲＬ」によって指定される記憶領域に記憶されたホームサーバアクセス用のパスワード及びホームサーバへのアクセス先データ（ＩＰアドレス）は，特定のユーザが特定の電話番号の携帯端末装置からホームサーバと通信するたびに更新されるのであり，また，ホームサーバアクセス用の識別コードＩＤも，個々のユーザを識別する機能を有するものではないから，単一の「ＵＲＬ」によって指定される記憶領域を複数の特定のユーザが共用することを妨げるものではない。そして，仮に複数の特定のユーザが存在しているとしても，それぞれの特定のユーザは，携帯端末装置からホームサーバと通信し，ホームサーバアクセス用のパスワードデータを入手した後，WWWサーバにアクセスすれば，所定の「ＵＲＬ」で指定される記憶領域に保存したＷｅｂページの表示データを受信することができ，ホームサーバアクセス用の識別コードＩＤとホームサーバアクセ

ス用のパスワードデータを入力することによってユーザ認証を受けることができるのであるから，「ＵＲＬ」が，ユーザごとに設定されるユーザ固有のものであるとはいえない。

（ウ）　以上のとおり，引用発明１は，ホームサーバにアクセスするユーザが複数存在することを前提とした発明であるとはいえないし，「ＵＲＬ」が，ユーザごとに設定されるユーザ固有のものであるともいえないから，引用発明１の「ＵＲＬ」が，本件発明１の「管理マスタＩＤ」に相当するということはできない。

エ　原告の主張について

（ア）　原告は，本件発明１は複数ユーザの個人認証に限定されるものではないから，引用発明１における「ＵＲＬ」は，本件発明１の「管理マスタＩＤ」に相当すると主張する。

しかし，上記（１）イ，ウのとおり，本件発明１の「管理マスタＩＤ」は，複数のユーザが存在することを前提に，第１のシステムのユーザと第２のシステムのユーザとを関連付けるために，ユーザごとに設定されたユーザ固有の識別コードであるのに対し，引用発明１の「ＵＲＬ」は，複数のユーザが存在することを前提としているともいえないし，ユーザごとに設定されたユーザ固有のものともいえないから，引用発明１における「ＵＲＬ」が，本件発明１の「管理マスタＩＤ」に相当するということはできない。

（イ）　原告は，仮に本件発明１が複数ユーザについての個人認証に限定されるとしても，引用発明１は，ホームサーバが新たに作成したパスワードを用いてユーザ認証を行うものであり，「ユーザ認証」とは，その文言から，ユーザ個人を認証する意味であるから，個人を区別する個人認証をしないでよいと解釈することはできず，引用発明１における「ＵＲＬ」も複数のユーザごとに管理されていると主張する。

しかし，引用例１の記載において，ユーザ個人を識別する個人認証が排除されていないからといって，必然的に「ＵＲＬ」が複数のユーザごとに管理されていると

いうことはできない。また，ホームサーバにアクセスできる特定のユーザが複数存在するとしても，上記ウのとおり，引用発明１は，単一の「ＵＲＬ」を複数の特定のユーザが利用することを妨げるものではないから，「ＵＲＬ」が複数のユーザごとに管理されているということもできない。

（ウ）　また，原告は，引用発明１では，ユーザの携帯端末装置の電話番号を用いて第１段階のユーザ認証が行われているから，電話番号により各ユーザの区別がなされており，当然に「ＵＲＬ」についてもユーザごとに管理されていると主張する。

引用例１の【００２５】には，「モデム２に接続される上記の交換局装置３ａは，特定の電話番号によるモデム２への回線接続要求以外の回線接続要求に対してはモデム２との回線確立を行わず，遮断処理する。特定の電話番号には携帯端末装置１１に割り当てられた電話番号が含まれるので，携帯端末装置１１からのモデム２へ至る電話回線への回線接続要求に対しては交換局装置３ａは回線接続を行う。これにより，予め定められた携帯端末装置以外からモデム２を介してホームサーバ１と通信することはできない。」と記載されており，電話交換局装置は，携帯端末装置の電話番号が特定の電話番号に含まれるか否かによって，携帯端末装置をモデムに回線接続するか遮断するかを判断しているから，携帯端末装置の電話番号に基づいてユーザ認証を行っているということができる。しかし，電話交換局装置におけるユーザ認証は，特定の電話番号の携帯端末装置以外からのモデムへの通信を遮断することを目的としたものであり，ホームサーバは，携帯端末装置とホームサーバとの間の通信が可能になると，新たなホームサーバアクセス用のパスワードを作成するのであるから，ホームサーバにおいて，ユーザ個人が区別されて管理されている必然性はない。

したがって，引用発明１は，電話交換局装置において，電話番号により個別のユーザを識別することが可能であるとしても，「ＵＲＬ」がユーザごとに個別に用意されているのが当然ということはできない。

（３）　本件発明１の新規性

以上のとおり，引用発明１の「ＵＲＬ」は，本件発明１の「管理マスタＩＤ」に相当するものではない。よって，結局，本件発明１は，引用発明１と同一であるということはできない。

（４）　本件発明５，９，１１，１３及び１４の新規性

また，同様の理由により，本件発明５，９，１１，１３及び１４が引用発明１と同一であるということもできない。

（５）　小括

よって，取消事由１は理由がない。

２　取消事由２（本件発明の進歩性についての判断の誤り）について

（１）　本件発明１と引用発明１との相違点

前記１のとおり，本件発明１は，複数のユーザが存在することを前提に，第１のシステムのユーザと第２のシステムのユーザとを関連付けるために設定された，ユーザ固有の「管理マスタＩＤ」を有するのに対し，引用発明１は，ホームサーバにアクセスするユーザが複数存在することを前提とした発明であるとはいえないし，「ＵＲＬ」がユーザごとに設定されるユーザ固有のものであるともいえない。よって，引用発明１の「ＵＲＬ」は，本件発明１の「管理マスタＩＤ」に相当するものではなく，引用発明１は本件発明１と，少なくともこの点において相違する。

（２）　本件発明１と引用発明１との技術分野及び課題の共通性

本件発明１は，前記１（１）のとおり，ワンタイムＩＤを利用した個人認証方法において，ユーザの個人認証の信頼性や安全性を向上させることを課題とした発明であり，一方，引用発明１は，前記１（２）のとおり，端末装置からホームサーバにアクセスする際のユーザ認証方法において，特定のユーザ以外の不正ユーザによる端末装置からのホームサーバへのアクセスを排除することを課題とした発明である。よって，両者は，いずれも，広い意味で「認証」に関する技術分野に属する発明ということができる。

しかし，本件発明１における課題は，前記１（１）のとおり，ユーザ個人を認証する「個人認証」であるのに対し，引用発明１は，前記１（２）のとおり，特定のホームサーバにアクセスしようとする者が特定のユーザか不正ユーザかを識別するものであって，ユーザ個人を識別する必要はない。よって，両者は，解決すべき課題が，前提において相違する。

さらに，本件発明１の「管理マスタＩＤ」は，前記１（１）のとおり，第１のシステムのユーザと第２のシステムのユーザとを関連付けるために用いられるユーザ固有の識別コードであるのに対し，引用発明１の「ＵＲＬ」は，前記１（２）のとおり，複数の特定のユーザが共用することを妨げるものではない。そうすると，引用発明１において，複数のユーザが存在するとしても，複数の「ＵＲＬ」を設定し，ユーザごとに割り当てる動機付けも存在しないというべきである。

したがって，本件発明１は，引用発明１に基づいて容易に発明することができたものということはできない。

（３）　原告の主張について

原告は，引用発明１において，別々のユーザが近接した時間に連続してホームサーバ１にアクセスする状況に対処するためには，ＵＲＬがユーザごとに異なっていればよく，ＵＲＬで指定される記憶領域にユーザごとのホームサーバアクセス用識別コードＩＤとパスワードとを記録するよりも，ＵＲＬをユーザごとに割り当てる方が処理が簡潔になることは，当業者に自明の事項であり，もともとユーザごとの携帯端末装置番号が管理されているから，ユーザごとにＵＲＬを割り当てることは当業者にとって当然の設計事項であり，自然なことであると主張する。

しかし，引用発明１は，前記１（２）のとおり，単一のユーザによっても実施することができるものであり，また，引用例１には，別々のユーザが近接した時間に連続してホームサーバにアクセスする状況があることは，記載も示唆もされていない。また，前記１（２）のとおり，電話交換局装置において，携帯端末装置の電話番号に基づいてユーザ認証が行われているとしても，ホームサーバにおいてユーザ

個人が区別されて管理されているとはいえない。よって，引用例１に記載された事項から，ＵＲＬをユーザごとに設定するという構成を採用することを，想起する契機も動機付けもないというべきである。したがって，引用発明１において，ユーザ個人を認証するために，ユーザごとにＵＲＬを割り当てることが，当業者にとって当然の設計的事項であるということも，自然なことであるということもできない。

（４）　本件発明１の進歩性

以上のとおり，本件発明１は引用発明１に基づいて容易に発明をすることができたものということはできない。

（５）　本件発明２，５，６，９ないし１４の進歩性

また，同様の理由により，本件発明５，９，１１，１３及び１４が引用発明１に基づいて容易に発明をすることができたものということはできないし，本件発明２，６，１０及び１２が引用発明１及び引用発明２に基づいて容易に発明をすることができたものということもできない。

（６）　小括

よって，取消事由２は理由がない。

３　結論

以上の次第であるから，原告の請求は棄却されるべきものである。

知的財産高等裁判所第４部

裁判長裁判官　　滝　　澤　　孝　　臣

裁判官　　高　　部　　眞　規　子

裁判官　　井　　上　　泰　　人