

平成13年（行ケ）第177号 審決取消請求事件（平成14年1月30日口頭弁論終結）

原告	被告	判決	
エヌ・ヴィー	コーニンクレッカ	フィリップス	エレク
トロニクス	生田哲郎	山田基司	上田浩及
	特許庁長官	山本春樹	武井袈彦
	小宮林川	宮文信久	成
訴訟代理人弁護士			
同被指定代理人			
同			
同			

主  
原告の請求を棄却する。  
訴訟費用は原告の負担とする。  
この判決に対する上告及び上告受理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 当事者の求めた裁判

1 原告  
特許庁が平成11年審判第6298号事件について平成12年12月1日に  
した審決を取り消す。  
訴訟費用は被告の負担とする。

2 被告  
主文と同旨

#### 第2 当事者間に争いのない事実

1 特許庁における手続の経緯

原告は、昭和60年3月25日（優先権主張日1984年（昭和59年）3  
月24日・西ドイツ国）の特許出願に係る特願昭60-60508号出願の一部を  
新たな特許出願として、平成8年3月27日、名称を「移動無線局」とする発明に  
つき特許出願をした（特願平8-99331号）が、平成11年1月21日に拒絶  
査定を受けたので、同年4月21日、これに対する不服の審判の請求をし、同年5  
月21日、その特許請求の範囲の補正（以下、補正後の特許請求の範囲の請求項1  
に係る発明を「本願発明」という。）をした。

特許庁は、同請求を平成11年審判第6298号事件として審理した上、平  
成12年12月1日に「本件審判の請求は、成り立たない。」との審決をし、その  
謄本は、平成13年1月22日、原告に送達された。

2 本願発明の要旨  
移動無線局に割当てられた識別コードの不正使用を検出する形態の移動無線  
システムに適用され、ランダム値が移動無線局へ送信され、送信された当該値から  
導かれる暗号値が当該移動無線局から返送され、そして前記移動無線システムにお  
いて当該暗号値と前記ランダム値に係る暗号との比較を実施して前記不正使用を検  
出する移動無線局であって、  
前記システムから受信した前記ランダム値及び当該移動無線局に設けられた  
格納手段に格納された識別コードとを基に新たな暗号値を導く手段と、  
前記システムに向けて当該新たな暗号値を送信する手段とを有することを特  
徴とする移動無線局。

#### 3 審決の理由

審決は、別添審決謄本写し記載のとおり、本願発明が、特開昭54-148  
402号公報（甲第4号証、以下「引用文献」という。）に記載された発明（以下  
「引用発明」という。）及び周知技術に基づいて当業者が容易に発明をすることが  
できたものと認められるから、特許法29条2項の規定により特許を受けることが  
できないとした。

#### 第3 原告主張の審決取消事由

審決の理由中、本願発明の要旨の認定、引用文献の記載を摘記した部分（審  
決謄本2頁2行目～31行目）の認定、本願発明と引用発明との一致点及び相違点  
1～4の各認定は認める。

審決は、本願発明と引用発明との相違点１～４についての判断を誤った（取消事由１～３）結果、本願発明が引用発明及び周知技術に基づいて当業者が容易に発明をすることができたとの誤った結論に至ったものであるから、違法として取り消されるべきである。

１ 取消事由１（相違点１及び同２についての判断の誤り）

(1) 審決は、本願発明と引用発明との相違点１として認定した「『伝送位置にある装置』及び『システム』が、本願発明では、各々、『移動無線局』及び『移動無線システム（前記システム）』と具体的に記載されているのに対し、引用発明に関して、引用文献には、『移動無線局』及び『移動無線システム』についての言及はない」（審決謄本３頁２０行目～２３行目）点、及び相違点２として認定した「『識別コード』が、本願発明では、伝送位置にある装置である『移動無線局』に割当てられているのに対し、引用発明では、伝送位置にある装置を利用する『ユーザ』である」（同頁２５行目～２７行目）点につき、「引用文献には、引用発明を、データ伝送に関したものではありませんものの、無線システムに適用できる旨記載されており（引用文献第１１頁左上欄第１１～１６行の摘記事項参照。）、また、移動無線システムにおいて、移動無線局に割当てられた識別コードの不正使用を検出するために、認証技術が必要なことは・・・周知であるから、引用発明を、移動無線システムに適用することは、当業者が当然想起することであり、その際、『伝送位置にある装置』を『移動無線局』とし、受け取り位置にある装置を含む『システム』を『移動無線システム』とすること、及び、識別コードを移動無線局に割り当てることは、当業者が容易になし得ることと認められる」（同４頁２行目～１２行目）との判断をし、上記周知技術に係る周知例として特開昭５６－１０９０５１号公報（甲第５号証、以下「周知例１」という。）及び特開昭５６－６０１２６号公報（甲第６号証、以下「周知例２」という。）を挙げた。

しかしながら、以下のとおり、審決の相違点１、２に対する上記判断は誤りである。

(2) 移動無線システムでは、ユーザーは専用の端末（移動無線局）を使用し、端末とユーザーとは一対一で対応するから、中央（基地局）が認証の対象とするのは端末（すなわち、装置）であり、この場合を「端末認証」という。端末認証システムでは、端末ごとに識別コード（端末識別コード）を割り当てるから、端末内に端末識別コードを格納しておくことが可能である。

これに対し、銀行の現金預払機等のように、同じ端末を複数のユーザーが利用するシステムでは、認証の対象は端末ではなく、ユーザー（すなわち、個人）であり、この場合をユーザー認証という。ユーザー認証システムでは、ユーザーが識別コード（ユーザー識別コード）を管理し、同システムを使用するたびにユーザー自身がキーボード等により入力する必要があるから、端末内に識別コードを格納しておくことはできない。

このように、端末認証とユーザー認証とは、一見類似するが、全く異なる概念である。そして、本願発明は端末認証システムに属し、引用発明はユーザー認証システムに属するものである。

(3) 相違点１に関し、審決は、引用文献には、引用発明を無線システムに適用できる旨が記載されていると認定したが、審決が指摘する引用文献（甲第４号証）の「本発明の実施例の合成システムは、伝送されたデータ又は権限のあるユーザーの識別符号と関連した秘密保持を損うことなく・・・無線等の普通のデータ伝送によって、符号化されたデータを伝達するのを可能にする」（１１頁左上欄１１行目～１６行目）との記載は、引用文献に記載された認証技術の伝送方法として「無線」を採用してもよいという趣旨であり、引用発明を移動無線システムにも適用できるという意味ではない。移動無線システムは、少数の基地局と多数の移動無線局との通信を行うというその性質上、素早い認証を必要とする等の特殊性を有する。したがって、引用文献の上記「無線等の普通のデータ伝送」との文言から、引用発明が用いている認証技術を移動無線システムに適用することまで、当然に想起するということはできない。

また、審決は、移動無線システムにおいて、移動無線局に割り当てられた識別コードの不正使用を検出するために認証技術が必要なことは周知であるとして、周知例１（甲第５号証）及び同２（甲第６号証）を挙げるが、これらの周知例に記載された移動無線システムは、いずれも、移動無線局に割り当てられた移動機番号（電話番号）と識別コード（キー番号又は暗証番号）とを移動無線局から基地局に送出することにより、移動機番号の不正使用を検出する単純なものにすぎず、

識別コードの不正使用まで検出するものではない。したがって、これらの周知例は、移動無線システムにおける端末認証の必要性は開示するものの、識別コードに対し暗号化等の不正窃取防止処理を施す技術思想まで開示するものではないから、移動無線局に割り当てられた識別コードに対して認証技術が必要であることは周知とはいえない。

さらに、引用発明は、上記のとおりユーザー認証システムであり、かつ、識別コードに対して暗号化処理を施すものである。他方、周知例 1、2 に記載されたシステムは、いずれも端末認証システムであり、しかも、識別コードに対して暗号化処理を施す技術思想はない。したがって、引用発明と周知例 1、2 に記載されたシステムとでは、「識別コードを用いた認証」という限度では関連するとしても、認証の対象が異なるほか、認証方法に関する技術思想も異なるものであるから、周知例 1、2 に開示された技術を引用発明に適用することは困難である。

(4) 相違点 2 に関し、審決は、「識別コードを移動無線局に割り当てることは、当業者が容易になし得る」とする根拠を示していない。

上記のとおり、引用発明はユーザー認証システムであり、端末認証システムである本願発明とは技術的背景が異なるものである。相違点 2 は、認証対象の差異に起因する本質的な相異点であり、したがって、引用発明の「PIN」（ユーザー識別コード）を本願発明の「移動無線局に割り当てられた識別コード」（端末識別コード）とすることを容易に想起することができるものではない。

## 2 取消事由 2（相違点 3 についての判断の誤り）

(1) 審決は、本願発明と引用発明との相違点 3 として認定した「『ランダム値』が、本願発明では、伝送位置にある装置である『移動無線局』へ送信されているのに対し、引用発明では、受け取り位置にある装置へ送信されている。また、『ランダム値から導かれる暗号値が伝送位置にある装置から送信』される点について、本願発明では、『送信』が『返信』に記載変更されている」（審決謄本 3 頁 29 行目～33 行目）点につき、「認証技術において、ランダム値の送信（源）を認証する側にするか、認証される側にするかは、システムの規模、システムの構成、使い勝手等によって決められる周知の単なる設計的事項・・・である。してみると、相違点 1、2 についての變更に伴って、物理的制約の多い移動無線局でなく、制約の少ない移動無線システムを選択するのは当然の設計的事項であって、同じ内容を単に表現変更した相違点 3 に、格別の創意工夫を認めることはできない」（同 4 頁 14 行目～26 行目）と判断し、上記周知事項に係る周知例として、引用発明のほか、昭和 55 年共立出版発行のコンピュータ・サイエンス 149～173 頁所収「暗号化と安全な計算機ネットワーク」（甲第 7 号証、以下「周知例 3」という。）及び特開昭 59-769 号公報（甲第 8 号証、以下「周知例 4」という。）を挙げた。

しかしながら、以下のとおり、審決の上記判断は誤りである。

(2) 引用発明は、端末局においてメッセージを暗号化（符号化、エンコーディング）して伝送し、基地局（中央局）において解読（復号化、デコーディング）する従来のシステムにおいて、エンコーディングキーが符号化のみならず復号化も可能な可逆キーである場合には、ひとたびエンコーディングキーが窃取されると、暗号が解読されて秘密を保持することができなくなるとの問題点を、不可逆なランダムキーを端末局及び基地局の双方で用いることにより解決しようとするものである。具体的には、端末局において、ランダム数発生器によって発生したランダム値を用いて PIN 値（識別コード）を不可逆アルゴリズムモジュールにおいて符号化し、この暗号化された PIN 値とランダム値とを基地局に送信し、基地局は、その保持するユーザーの PIN 値を、送信されたランダム値を用いて不可逆アルゴリズムモジュールにおいて符号化し、この値を、端末局より送信された暗号化された PIN 値と比較するものであって、復号化という手順のない構成を採用するものである。

すなわち、引用発明は、ランダム値と暗号化された PIN 値の双方が窃取されたとしても、暗号化された PIN 値が復元されなければ不正使用防止の目的は達成されるから、ランダム数発生器を端末局に設置しても問題はないとの認識に立つものであり、そこで想定されている危険は、あくまで PIN 値が解読されること、すなわち、窃取した PIN 値（識別コード）を有するユーザーになりすますことであって、窃取したランダム値と暗号化された PIN 値とを基地局に送って端末局になりすますという事態は想定されていない。この場合には、ランダム数を基地局で生成して端末局に送り、端末局がさらに返信することは、むしろ煩雑で通信負

担が増すため、ランダム値を基地局で生成することは、そのことに何らかの利点がない限り発想し得ないのである。また、引用発明の端末局は現金預払機のようなある程度の大きさの装置を想定しており、ランダム数発生器を内蔵したとしても負担はない。

このように、認証技術を適用する分野、防止すべき不正使用の態様等に対応してランダム値送信源の設置位置はそれぞれ異なるのであり、単なる設計的事項ではない。引用発明においては、ランダム数発生器の設置位置を端末局から基地局に変更する必要性を欠いており、そのような変更をすることを発想することができない。

(3) また、審決は、周知例3（甲第7号証）では、「ランダム値に対応する『無作為で一意的データ項目』を、認証する側（受信側）で発生させて」（審決謄本4頁20行目～21行目）いるとする。

しかしながら、周知例3に記載された技術は、認証側が被認証側に本願発明のランダム値に対応する「平文」を送信し、被認証側が送信された「平文」を暗号化して返送し、認証側が返送された「暗号文」を被認証側の暗号化キーに対応する復号化キーにより復号化することにより認証を行うものである。したがって、この場合には、ランダム値に対応する「平文」自体を暗号化しており、ランダム値によって識別コードを暗号化するものではない。また、暗号化キーに対応する復号化キーによって復号化するものであるから、使用される暗号化キーは可逆的であって復号化を伴う認証技術である。さらに、そもそも、周知例3は、コンピュータネットワーク等における使用者間同士の認証に関するものであって、端末局や基地局という概念がなく、識別コードを用いるシステムでもない。結局、周知例3に記載された技術は、引用発明と全く技術分野が異なり、引用発明に適用できるものではない。

審決は、さらに、周知例4（甲第8号証）にも、ランダム値を認証する側（受信側）で発生させる構成があるとする。

しかしながら、周知例4に記載された技術は、小売業者、銀行、コンピュータ端末等におけるユーザー認証システムであり、ランダム値から暗号値を導くものではなく、しかも、暗号化のアルゴリズムは可逆的であって復号化を伴う認証技術である。したがって、周知例4に記載された技術も、引用発明と全く技術分野が異なり、引用発明に適用できるものではない。

(4) 移動通信システムにおいては、ランダム値により暗号化された識別コードとランダム値とを、共に端末局（移動無線局）から基地局に送信することとする。と、共に送信されるこれらを双方ともに窃取することは比較的容易であるので、窃取した者が他の端末を改造するなどして、これらを基地局に送信することにより、窃取された識別コードを有する端末局になりすますことが可能となる。すなわち、端末局でランダム値を発生させ、それによって識別コードの暗号化を行い、暗号化された識別コードとランダム値とを共に基地局へ送信するという方法では、不正使用を十分に防止することができないのである。

本願発明において、基地局から端末局（移動無線局）へ通話の度にランダム値を送信し、端末局は受信したランダム値により暗号化した識別コードを送信する構成としたのは、このためである。このようにすることにより、識別コードとランダム値とは送信の方向が逆（双方向）となるから窃取が困難となるし、仮に、ある通話の際に、ランダム値と暗号化した識別コードが窃取されたとしても、次の通話の際に、基地局から発信されるランダム値はそれと異なるから、窃取したデータを利用して不正な通話をすることはできない。

本願発明の要旨は、「ランダム値から導かれる暗号値が伝送位置にある装置から送信」される点を「返送され」と規定し、ランダム値を基地局から端末局（移動無線局）に「送信」し、暗号値を端末局から基地局に「送り返す」という本願発明の構成を明確に示しているものであり、「返送」は本願発明の技術思想を表す重要な文言であるから、これを「送信」という文言と同一にとらえることができないことは明らかである。

### 3 取消事由3（相違点4についての判断の誤り）

審決は、本願発明と引用発明との相違点4として認定した「本願発明では、『移動無線局に識別コードの格納手段を設け』、格納された識別コードを基に新たな暗号値を導いているが、引用発明に関して、引用文献には、『格納手段』との明記はない」（審決謄本3頁35行目～37行目）点につき、「伝送位置（移動無線局）自体に『識別コード』を割当てて必要がある以上、何らかの形で識別コードの

格納手段を設けなくてはならないから、上記相違点 4 も単なる設計的事項にすぎない」(同 4 頁 3 1 行目～3 3 行目)と判断した。

しかしながら、ユーザー認証システムである引用発明は、ユーザー自身がユーザー識別コードを管理し、使用時に入力するものであるから、端末にユーザー識別コードをあらかじめ格納しておくことができないことは当然であり、したがって、端末に識別コードの格納手段を設けることが単なる設計的事項でないことは明白である。

#### 第 4 被告の反論

審決の認定及び判断は正当であり、原告主張の審決取消事由は理由がない。

##### 1 取消事由 1 (相違点 1 及び同 2 についての判断の誤り) について

(1) 原告は、審決が指摘する引用文献(甲第 4 号証)の「本発明の実施例の合成システムは、伝送されたデータ又は権限のあるユーザーの識別符号と関連した秘密保持を損うことなく、郵便、電話による音声伝達、無線等の普通のデータ伝送によって、符号化されたデータを伝達するのを可能にする」(11 頁左上欄 11 行目～16 行目)との記載は、引用文献に記載された認証技術の伝送方法として「無線」を採用してもよいという趣旨であり、引用発明を移動無線システムにも適用できるという意味ではない旨主張する。

しかしながら、引用文献の上記記載中には、無線システムのほか電話システムの利用も記載されており、したがって、無線による電話システムの利用も想定されているところ、周知例 1 (甲第 5 号証) 又は同 2 (甲第 6 号証) によれば、無線による電話システムの中には、自動車電話など移動無線電話が含まれることが明らかであるから、結局、引用文献には移動無線システムの利用も開示されていることができる。

仮に、引用文献に、移動無線システムへの適用につき直接的記載又は示唆がないとしても、後記(2)のとおり、移動無線システムに認証技術が必要であることは周知の事項であるから、引用発明を移動無線システムに適用することは容易にし得ることである。

(2) 原告は、周知例 1 (甲第 5 号証) 及び同 2 (甲第 6 号証) に記載された移動無線システムが、移動機番号の不正使用を検出するものであって、識別コード(キー番号又は暗証番号)に対し暗号化等の不正窃取防止処理を施す技術思想まで開示するものではないから、移動無線局に割り当てられた識別コードに対して認証技術が必要であることは周知とはいえない旨主張する。

しかしながら、審決の「移動無線システムにおいて、移動無線局に割り当てられた識別コードの不正使用を検出するために、認証技術が必要なことは、上記拒絶理由通知で引用した引用文献 B、C (注、周知例 1、2)・・・から明らかなように周知である」(審決謄本 4 頁 4 行目～8 行目)との認定における「識別コード」とは、周知例 1 の「移動機番号」及び周知例 2 の「移動端末番号」を指すものであり、周知例 1 の「キー番号」及び周知例 2 の「暗証番号」を指すものではない。審決の上記認定は、周知例 1、2 に、移動無線局に割り当てられた識別コード(移動機番号又は移動端末番号)を第三者によって不正使用されることがあり、その防止のため、より防止効果の大きい認証技術(周知例 1 ではキー番号を用いること、周知例 2 では暗証番号を用いること)が開示されているから、移動無線局の識別コードの不正使用を検出するために、認証技術が必要であることは周知であるという趣旨である。原告の主張は、審決の説示を誤解するものであって、前提を欠く。

(3) 原告は、引用発明は、ユーザー認証システムであり、識別コードに対して暗号化処理を施すものであるのに対し、周知例 1、2 に記載されたシステムは、いずれも端末認証システムであり、識別コードに対して暗号化処理を施す技術思想はないから、周知例 1、2 に開示された技術を引用発明に適用することは困難である旨主張する。

しかしながら、引用発明と周知例 1、2 に開示された周知技術とは、識別コードを用いた認証技術との限度で技術分野を同じくし、かつ、識別コードの不正利用防止という技術課題においても共通するものである(周知例 1、2 においても、識別コードの不正利用防止のため認証技術を用いていることは上記のとおりである。)

そうとすれば、引用発明を周知例 1、2 に開示された移動無線局の認証手段に適用することが妨げられるものではなく、これら技術分野及び技術課題の共通性を無視して、認証手段が相違するからといって、あるいはユーザー認証と端末認

証という認証対象が異なるからといって、上記適用が容易ではないとする原告の主張は誤りである。

(4) 審決の「その際、『伝送位置にある装置』を『移動無線局』とし、受け取り位置にある装置を含む『システム』を『移動無線システム』とすること、及び、識別コードを移動無線局に割り当てることは、当業者が容易になし得ることと認められる」（審決謄本4頁9行目～12行目）との判断は、このように引用発明を周知例1、2に開示された移動無線局の認証手段に適用することの結果として、引用発明の「伝送位置にある装置」を「移動無線局」とすること、その「受け取り位置にある装置を含むシステム」を「移動無線システム」とすること、及び識別コードを移動無線局に割り当てること、半ば自動的に導かれると判断したものであり、この判断に誤りはない。

## 2 取消事由2（相違点3についての判断の誤り）について

(1) 原告は、周知例3（甲第7号証）及び同4（甲第8号証）に記載された技術は、引用発明と技術分野が異なるから、引用発明に適用できるものではない旨主張する。

周知例3に記載された認証の具体的手法が原告主張のとおりであることは認めるが、審決が周知例3から引用したのは、暗号化技術を用いた認証において、認証側から被認証側にランダム値を送信する点であって、認証側及び被認証側における具体的な認証の手法を引用したものではない。すなわち、認証手続において、ランダム値の送信源を認証側又は被認証側のいずれに設置するのかは設計的事項であることを立証するために周知例3を引用したのであり、このことは、周知例4についても同様である。

そして、周知例3、4に記載されたものも、引用発明も、ランダム値に基礎を置く認証技術の分野に属しており、技術分野が異なるとの主張は誤りである。

認証技術において、ランダム値の送信源を認証側にするか、被認証側にするかは、二者択一であって、システムの規模、システムの構成、使い勝手等によって決められる単なる設計的事項にすぎず、この点についての審決の判断に誤りはない。

(2) 原告は、本願発明において、基地局から端末局（移動無線局）へ通話の度にランダム値を送信し、端末局は受信したランダム値により暗号化した識別コードを送信することによる効果を主張するが、その点も、設計的事項としての「ランダム値が移動無線局へ送信されること」による当然生ずる自明の効果でしかない。

また、原告は、本願発明の要旨における「返送」との規定が、本願発明の技術思想を表す重要な文言であるとも主張するが、「返送」と「送信」は、ランダム値送信源の設置位置を認証側に変更することに伴って当然に生ずる表現の相違であるにすぎず、これを「同じ内容を単に表現変更した相違点3に、格別の創意工夫を認めることはできない」（審決謄本4頁25行目～26行目）とした審決の判断に誤りはない。

## 3 取消事由3（相違点4についての判断の誤り）について

原告は、ユーザー認証システムである引用発明は、ユーザー自身がユーザー識別コードを管理し、使用時に入力するもので、端末にユーザー識別コードをあらかじめ格納しておくことはできないことは当然であるから、端末に識別コードの格納手段を設けることは設計的事項でない旨主張する。

しかしながら、移動無線局（端末）自体を識別コードで識別することは周知であるから、この識別コードの格納手段を移動無線局に設けることは、当然の事項である。審決が「伝送位置（移動無線局）自体に『識別コード』を割り当てる必要がある以上、何らかの形で識別コードの格納手段を設けなくてはならないから、上記相違点4も単なる設計的事項にすぎない」（審決謄本4頁31行目～33行目）としたのはその趣旨であり、上記判断に誤りはない。

## 第5 当裁判所の判断

### 1 取消事由1（相違点1及び同2についての判断の誤り）について

(1) 相違点1につき、審決は、「引用文献には、引用発明を、データ伝送に関したものであるものの、無線システムに適用できる旨記載されており」（審決謄本4頁2行目～3行目）とした上、引用文献（甲第4号証）の「本発明の実施例の合成システムは、伝送されたデータ又は権限のあるユーザーの識別符号と関連した秘密保持を損うことなく、郵便、電話による音声伝達、無線等の普通のデータ伝送によって、符号化されたデータを伝達するのを可能にする」（11頁左上欄11行目～16行目）との記載を引用し、さらに、被告は、引用文献の上記記載中には、



無線システムのほか電話システムの利用も記載されており、これには自動車電話など移動無線電話のシステムも含まれるから、結局、引用文献には移動無線システムの利用も開示されている旨主張するが、引用文献の上記記載は、引用文献に記載されたシステムにおいて符号化されたデータを伝達するための手段として、「電話による音声」、「無線」等を採用することができるとの趣旨であることは明らかであって、引用文献記載のシステム自体を移動無線システムに適用することを明示的に記載したものではないから、審決の上記認定及び被告の上記主張は誤りであるといわざるを得ない。

(2) しかしながら、引用文献(甲第4号証)に、「この装置は、伝送位置23に、ランダム数発生器13、不可逆アルゴリズムモジュール(L.A.M)・・・15を備え・・・受け取り位置25に、記憶ファイル17別の不可逆アルゴリズムモジュール19、及び比較器21を備えている。ユーザーにより入力されたPINデータに応答して、かつランダム数発生器13により発生したランダム数(RN)に응答して、アルゴリズムモジュール15は、伝送されて、受け取り位置の比較器21に印加することができるユーザー識別コード(ID)を発生する。ランダム数発生器13によって発生したRNはまた、受け取り位置25でのL.A.M19に伝送される。所定の本物のPIN(記憶ファイル17の選択されたレジスタ内に予め記憶される)は呼び出されて、新たなユーザー識別コード(ID')を発生するために、受け取ったRNと共にアルゴリズムモジュール19に印加することができる。アルゴリズムモジュール19は、モジュール15と同じ方法で、そこに印加された信号を暗号化し又は符号化する。先に発生したユーザー識別コードIDは、それから比較器21によって新たに発生したユーザー識別コード(ID')と比較される。もし一致するならば(すなわち、もしIDとID'が同じであることがわかったならば)業務・・・を進めるべきであるということを示す出力データ値が発生する・・・もし一致しないならば、比較器21は、業務を進めるべきではないということを示す出力値を発生する」(審決謄本2頁5行目～23行目)との記載があることは当事者間に争いがなく、また、上記記載に先立って、「可変キーがデコーディング処理において使用することができるようにそれを伝送することは、権限のないユーザーがキーの伝送中にそのキーに近づくことが考えられるので、その動作の秘密保持を危くする。それ故、このようなデータ伝送動作(特に、データの秘密伝送だけでなく、ユーザーの正確な識別を必要とする銀行業務動作等)の秘密保持を改善するとき、一致エンコーディングデコーディングキー又はユーザー識別情報の伝送を必要とすることなく、データの秘密伝送をする技術を使用することが望ましい」(甲第4号証10頁左下欄16行目～右下欄7行目)、「PIN(銀行預金又は引き出し業務のような業務を開始するためにユーザーによりこの装置に入力される個人識別番号)」(同11頁左上欄3行目～5行目)との各記載がある。

これらの記載によれば、引用文献には、引用発明につき、端末局(伝送位置)において、ユーザーにより入力されたユーザー識別コードであるPINデータを、端末局で発生したランダム数で暗号化して基地局(受け取り位置)に伝送することにより、伝送中におけるPIN値の不正窃取を防止するとともに、ランダム数も同時に基地局に伝送し、基地局において、登録されているPIN値を伝送されてきたランダム数で暗号化し、端末局から伝送されてきた暗号化入力PINと、基地局で生成された暗号化登録PINとを比較することにより、入力されたPINが業務を許可すべき正当なPINであるか否かを認証すること、すなわち、PIN値の不正使用を検出することが記載されているものと認められる。そして、引用文献の上記「データの秘密伝送だけでなく、ユーザーの正確な識別を必要とする銀行業務動作等」との記載によれば、引用文献には、引用発明が「銀行業務」以外の「ユーザーの正確な識別を必要とする」業務全般に適用が可能であることが記載されていると認められるのみならず、引用文献(甲第4号証)中に、引用発明を移動無線システムに適用することを妨げるような記載は見当たらない。

なお、この点につき、原告は、移動無線システムは、少数の基地局と多数の移動無線局との通信を行うというその性質上、素早い認証を必要とする等の特殊性を有する旨主張するが、そうであるとしても、当該移動無線システムの性質に引用発明が適合せず、これを移動無線システムに適用することが阻害されるとする根拠は見いだせない。

(3) 他方、周知例1(甲第5号証)には、「本発明は例えば自動車電話等の移動機が正規の加入者以外の人によつて不正に使用されることを防止する移動機的不正使用防止方式に関するものである」(1頁左下欄12行目～15行目)、「接続

する移動機はこのサービスに登録されている移動機に限定するのは勿論である。登録されているか否かはその移動機の移動機番号で識別する」（2頁左上欄4行目～7行目）、「移動機番号はその移動加入者のダイヤル番号に対応する」（同頁右上欄16行目～18行目）、「登録されていない移動機は接続しないようになされていても、悪意ある人が移動機番号を書きかえるか又は何らかの方法で移動機又はこれと等価（注、「等価」の誤記と認める。）な働きをする装置を入手し、移動機番号を適当に設定した場合でこの移動機番号が実際に登録されているもののうちの1つに合致した場合には不正使用は防げない」（同頁左上欄15行目～20行目）、「本発明は・・・移動機番号に対応するキー番号をあらかじめ決めておき、このキー番号が接続しようとしている移動機の中に記憶してあるキー番号と合致した場合のみ接続をすることにより、移動機が正規の加入者以外の人によつて不正に使用されることを防止し得る移動機的不正使用防止方式を提供することを目的とする」（同頁右上欄末行～左下欄7行目）、「移動機が発呼する場合には従来の発呼識別信号と移動機番号に加えてキー番号を送出する。このキー番号は移動機番号に対応して決められた値とする。基地局では移動機番号が登録されているか否かと、キー番号がその移動機番号に対応したものであるか否かをチェックし、イエス（YES）であれば・・・接続するが、ノウ（NO）であれば接続しない」（同頁左下欄11行目～19行目）、「本発明におけるキー番号は加入者自身はこれを知る必要はない」（3頁右上欄4行目～5行目）との各記載がある。

これらの記載によれば、周知例1には、移動無線システムに関して、端末（移動機）に記憶されているダイヤル番号に対応した移動機番号は不正に使用されるおそれがあることから、移動機番号に加え、さらに正当な加入者であっても知らないキー番号を端末に割り当てて記憶させ、接続の際には、端末から移動機番号とキー番号とを基地局に送り、基地局において、移動機番号とキー番号とをセットにして、送られてきた移動機番号及びキー番号とあらかじめ登録された移動機番号及びキー番号とを比較することにより、その移動機番号により接続しようとする端末が正当な端末であるか否かを認証すること、すなわち、移動機番号の不正使用を防止するために、その不正使用を検出することが記載されていると認められる。なお、周知例1には、移動機番号の不正使用に関し、適当に書き換えた値が登録済みの移動機番号に合致した例を挙げてあるが、他人の端末の移動機番号を不正に窃取して、その番号に書き換える事態も容易に想定されるところである。

そうすると、周知例1により、移動無線システムに関して、移動無線局である端末に割り当てられた識別コード（移動機番号）の不正使用を検出するため、識別コードに対して認証の手段を講ずる必要があることは周知であったものと認められる。そして、このような周知事項を併せ考えれば、上記のとおり、識別コード（PIN値）の不正使用を検出するための識別コードに対する認証の方法を内容とするものであって、かつ、ユーザーの正確な識別を必要とする業務全般に適用が可能であることが引用文献に記載されており、しかも、移動無線システムに適用することを妨げるような事由も格別見当たらない引用発明を、周知例1に示されたような、識別コードが移動無線局に割り当てられた移動無線システムに適用することは容易にし得たものというのが相当である。

(4) 原告は、周知例1に記載されたシステムについて、識別コードに当たるものがキー番号であるとの前提の下に、上記システムは、移動機番号の不正使用を検出するものであって、識別コード（キー番号）に対し暗号化等の不正窃取防止処理を施す技術思想まで開示するものではないから、移動無線局に割り当てられた識別コードに対して認証技術が必要であることは周知とはいえない旨主張する。

しかしながら、上記(3)で認定した周知例1の記載に照らし、そこに記載されたシステムにおいて、移動機番号が個々の移動機を識別するために割り当てられた番号であることは明白であり、したがって、移動機番号は移動機の「識別コード」であるということが出来る。そして、上記システムにおいて、識別コード（移動機番号）の不正使用を検出するため、キー番号を用いた認証の手段を採用していることも上記(3)で認定したとおりである。

審決の「移動無線システムにおいて、移動無線局に割り当てられた識別コードの不正使用を検出するために、認証技術が必要なことは、上記拒絶理由通知で引用した引用文献B（注、周知例1）、C（注、周知例2）・・・から明らかなように周知である」（審決謄本4頁4行目～8行目）との認定は、周知例1については、その「識別コード」が「移動機番号」を意味するものと認められる上、移動無線局（移動機）に割り当てられた識別コードの不正使用を検出するために、認証技



術が必要であることを認定したにとどまり、当該認証技術が、識別コードに対し暗号化等の不正窃取防止処理を施すものであることまで含めて周知であることを周知例１に基づいて認定したものではない。そうすると、審決の上記認定は、周知例２（甲第６号証）を引用した点が、同周知例に記載された発明は、識別コード（移動機番号）の不正使用を検出することを課題とするものではなく、端末自体の不正使用の防止を目的とするものである（１頁右下欄７行目～１４行目）から、必ずしも適切とはいえないものの、結論に影響を及ぼす誤りはない。

（５）原告は、引用発明がユーザー認証システムであり、識別コードに対して暗号化処理を施すものであるのに対し、周知例１に記載されたシステムが端末認証システムであり、識別コードに対して暗号化処理を施す技術思想はないから、引用発明と周知例１に記載されたシステムとは、認証の対象及び認証方法に関する技術思想が異なり、周知例１に開示された技術を引用発明に適用することは困難である旨主張する。

しかしながら、まず、認証の対象（ユーザー認証システムと端末認証システム）の点について検討するに、確かに、周知例１に記載されたシステムは、直接には端末局（移動機）自体が偽造されたものであるか否かを検出するものであるから、引用発明がユーザー認証システムであるのに対し、周知例１に記載されたシステムは端末認証システムであるといえないことはない。しかしながら、上記（２）及び（３）の認定事実によれば、周知例１に記載されたシステムにおける認証は、ユーザーからの接続要求が正当な権限を有する者の要求として許可すべきものであるかどうかに係るものであり、その点では、引用発明における認証が、ユーザーからの「業務の開始」の要求が正当な権限を有する者の要求として許可すべきものであるかどうかに係るものであることと変わりがない。のみならず、上記（２）のとおり、引用発明は、基地局において、端末局から伝送されてきた暗号化入力PINと、基地局で生成された暗号化登録PINとを比較することにより、入力されたPINが業務を許可すべき正当なPINであるか否かを認証するものであり、他方、上記（３）のとおり、周知例１に記載されたシステムは、基地局において、移動機番号とキー番号とをセットにして、端末局（移動機）から送られてきた移動機番号及びキー番号と予め登録された移動機番号及びキー番号とを比較することにより、接続しようとする端末が正当な端末であるか否かを認証するものであるから、引用発明と周知例１に記載されたシステムとは、いずれも、識別コード（PIN値及び移動機番号）を用いて、上記のとおり、ユーザーの権限を認証するものであって、実質的に認証対象に異なるところはないというべきである。したがって、認証対象について、引用発明を移動無線システムに適用することについて妨げとなる差異があるということとはできない。

また、認証の方法については、上記（３）のとおり、周知例１に記載されたシステムは、移動機番号とキー番号とをセットにして、送られてきた移動機番号及びキー番号と予め登録された移動機番号及びキー番号とを比較することにより、接続しようとする端末が正当な端末であるか否かを認証するものであって、識別コード（移動機番号）に対して暗号化処理を施すことは周知例１に記載されていない。しかしながら、例えば、後記のとおり、周知例４（甲第８号証）には、端末局と基地局（ホスト）間でパスワードを暗号化して端末局から基地局に送ることが記載されているが、このような記載を待つまでもなく、識別コード等のメッセージの不正使用を防止するため、そのメッセージについての認証の手段としてメッセージに対して暗号化処理を施すこと自体も周知の技術であったことは明らかである。そして、そうとすれば、上記（３）のとおり、周知例１に基づき、移動無線システムに関して、移動無線局である端末に割り当てられた識別コードの不正使用を検出するため、識別コードに対して認証の手段を講ずる必要があることは周知であったものと認められる場合に、周知例１自体には、識別コードに対して暗号化処理を施すことは記載されていないとしても、そのことが、識別コードの不正使用を防止するため、識別コードに対する認証の手段として暗号化処理をした識別コード（PIN値）を用いる引用発明を移動無線システムに適用することについて妨げとなるものということもできない。

したがって、原告の上記主張は採用することができない。

（６）原告は、相違点２に関し、審決は「識別コードを移動無線局に割り当てることは、当業者が容易になし得る」とする根拠を示していないとした上、引用発明はユーザー認証システムであり、端末認証システムである本願発明とは技術的背景が異なるものであるから、引用発明のユーザー識別コード（PIN値）を本願発明

の「移動無線局に割当てられた識別コード」（端末識別コード）とすることを容易に想起することができるものではない旨主張する。

しかしながら、引用発明を、周知例 1 に示されたような、識別コードが移動無線局に割り当てられた移動無線システムに適用することが容易にし得たものと認められることは上記 (3) のとおりであり、そうとすれば、識別コードを移動無線局に割り当てることが格別の判断をせずとも自動的に導かれることは明白であるから、審決の上記判断に誤りがあるということとはできない。

なお、原告の主張するユーザー認証システムと端末認証システムとの相違が、引用発明を移動無線システムに適用することの妨げとならないことは、上記 (5) のとおりである。

(7) そうすると、審決の相違点 1 及び同 2 についての判断は、上記のとおり、瑕疵がないわけではないが、当該瑕疵は審決の結論に影響を及ぼすものではなく、その判断に原告主張の誤りはない。

## 2 取消事由 2（相違点 3 についての判断の誤り）

(1) 周知例 4（甲第 8 号証）には、「この発明は小売業者、銀行、コンピュータアクセス端末等において、個人識別番号等を記憶した ID カードと、使用者がキーボード等に入力するパスワードとによつてその使用者が、正当な使用者であるかどうかを調べる識別システムに関するものである」（2 頁左上欄 1 行目～6 行目）、「この発明は端末とホスト間でタッピング等により、盗み聞きすることにより ID ナンバー、パスワードを容易に知られることを防ぐために、ID ナンバー、パスワードを暗号化して端末からホストに送り、かつパスワードを暗号化する暗号化キーは毎回ホストで発生し、その暗号化キーを暗号化してホストから端末に送る構成とすることにより、ホストで送られてきた ID ナンバー、パスワードの正当性を確認するシステムを提供する」（同頁左下欄 19 行目～右下欄 7 行目）、「この発明によれば入力装置から入力されるパスワードで個人識別番号を暗号化してカードに記憶されており、このカードを読出して暗号化された個人識別番号を入力装置より送出すると共に、入力装置では中央処理ユニットから送られる暗号化された暗号化キーを、予め記憶してあるキー暗号化キーで復号化し、その復号された暗号化キーにより上記入力されたパスワードを暗号化して送出する。」（同頁右下欄 8 行～16 行目）、「端末とホストとの間の通信を設定して認証システムの動作を開始させるため、使用者は ID カード 103 をカード読取装置 102 に挿入し、次いでパスワードをキーボード 101 から入力する・・・キーボード 101 からキーインされるとホスト側の認証システムを作動させるため、入力装置 100 から適当な信号 300 により起動が開始される。ランダムワード発生器 201 から適当なランダムワード RN<sub>i</sub> が作り出され、これがキーイン入力したパスワードを暗号化する暗号化キーとなる・・・ランダムワード発生器 201 で発生したランダムワード RN<sub>i</sub> は・・・暗号化され、端末へ転送される。すなわち、E<sub>KM</sub>(RN<sub>i</sub>) となる。端末側の入力装置 100 では E<sub>KM</sub>(RN<sub>i</sub>) を受信し・・・復号化される・・・先程キーボード 101 よりキーインしたパスワード PW<sub>i</sub> を・・・復号化した RN<sub>i</sub> をキーとして暗号化する、すなわち E<sub>RN<sub>i</sub></sub>(PW<sub>i</sub>) となる。この暗号化されたパスワードがホストに転送される。ホスト側では送られてきた E<sub>RN<sub>i</sub></sub>(PW<sub>i</sub>) に対して復号化ブロック 203 で、ランダムワード発生器 201 で発生したランダムワード (RN<sub>i</sub>) をキーとして復号化を行う・・・次にカード読取装置 101 により読取られた ID カードのデータ・・・はホスト側に転送され・・・ID カードのデータを、復号化ブロック 203 で復号化した結果をキーとして復号化する」（3 頁左下欄 6 行目～4 頁右上欄 6 行目）、「パスワードの解読がなされると ID 番号も推察可能となるため、パスワードの暗号化には毎回違ったキーで暗号化することによりパスワードの解読をより困難にしている」（同頁左下欄 16 行目～18 行目）との各記載がある。

これらの記載によれば、周知例 4 には、認証システムにおいて、パスワードを端末局から基地局（ホスト）に送るに当たり、基地局でランダム値（ランダムワード）を毎回発生して端末局に送信し、端末局で送信されたランダム値によりパスワードを暗号化し、その暗号化されたパスワードを基地局に送信することにより、通信回線におけるパスワードの解読を防止すること（不正窃取の防止）が記載されているものと認められる。

そして、この記載と上記 1 の (2) の引用文献の記載とによれば、端末局において、ユーザーにより入力されたメッセージ（識別コード、パスワード）をランダム値で暗号化して基地局に送信する認証技術に関し、そのランダム値の送信源、すなわち、ランダム数発生器の設置位置を、端末局とすることも、基地局とすること

も、いずれも周知であるものと認められる。このことに、このような認証システムにおいて、ランダム数発生器の設置位置は、技術常識上、端末局と基地局との二者択一となることを併せ考えれば、ランダム数発生器の設置位置を端末局とするか、基地局とするかは、システムの規模、システムの構成、使い勝手等を考慮して適宜決定することができる単なる設計的事項にすぎないものというのが相当である。なお、原告は、周知例4に記載された技術は、ランダム値から暗号値を導くものではなく、しかも、暗号化のアルゴリズムは可逆的であって復号化を伴う認証技術であるから、引用発明と全く技術分野が異なり、引用発明に適用できない旨主張する。

しかしながら、上記のとおり、周知例4に記載されたシステムにおいて、パスワードを暗号化する暗号化キーは、基地局（ホスト）のランダムワード発生器で発生し、端末局に送信されたランダムワードであるから、ランダム値から暗号値を導くものであることは明らかである。また、上記パスワードの暗号化のアルゴリズムは可逆的であって、基地局における復号化が伴っていることは原告主張のとおりであるが、端末局においてユーザーにより入力されたメッセージをランダム値で暗号化して基地局に送信する認証技術に関し、そのランダム値に係るランダム数発生器の設置位置を端末局とするか、基地局とするかという問題と、当該暗号化のアルゴリズムを可逆的にするか、不可逆的にするかという問題とが、技術的に直接関連しないこと、すなわち、ランダム数発生器の設置位置がいずれであっても、技術的には、暗号化のアルゴリズムを可逆的にすることもできるし、不可逆的にすることもできることは明白である。したがって、周知例4に基づき、上記認証技術に関しランダム数発生器の設置位置を基地局とすることが周知であることを認定するに当たって、周知例4に記載されたシステムが、暗号化のアルゴリズムが可逆的である点で引用発明と異なることがその妨げとなるものではない。

(2) 原告は、引用発明が想定する危険はPIN値が解読されることであり、ランダム値と暗号化されたPIN値の双方が窃取されたとしても、暗号化されたPIN値が復元されなければ不正使用防止の目的は達成されるから、ランダム数発生器を端末局に設置しても問題はないとの認識の下に、ランダム値を用いてPIN値を不可逆的に符号化し、復号化という手順のない構成を採用したものであること、ランダム数を基地局で生成して端末局に送り、端末局がさらに返信することは煩雑で通信負担が増すこと、引用発明の端末局はある程度の大きさの装置を想定しており、ランダム数発生器を内蔵したとしても負担はないことを挙げて、認証技術を適用する分野、防止すべき不正使用の態様等に対応してランダム値送信源の設置位置はそれぞれ異なり、単なる設計的事項ではないから、引用発明においては、ランダム数発生器の設置位置を端末局から基地局に変更する必要性を欠いており、そのような変更をすることを発想することができない旨主張する。

しかしながら、復号化という手順のない構成を採用したこと及び端末局がランダム数発生器を内蔵したとしても負担がないことは、いずれも、端末局にランダム数発生器を設置することによる利点というわけではなく、まして、基地局にランダム数発生器を設置することを困難にする事由ではない。そうすると、結局、ランダム数を基地局で生成して端末局に送り、端末局がさらに返信することによる煩雑さと通信負担の増加を避けることが、端末局にランダム数発生器を設置することによる利点と認められるが、この程度のことは、端末局にランダム数発生器を設置することによる効果として当然に予測されることであるばかりでなく、ランダム数発生器を基地局に設置することを困難にするほどの事由であるともいえないから、ランダム数発生器の設置位置が、システムの規模、システムの構成、使い勝手等を考慮して適宜決めることができる設計的事項であるとの上記認定を左右するに足りない。

のみならず、上記1のとおり、相違点1、2についての審決の判断に誤りではなく、引用発明を移動無線システムに適用することは、当業者が容易にし得たものと認められるのであるから、ランダム数発生器の設置位置を端末局から基地局に変更する動機付けの有無は、上記適用に伴って変更された引用発明を基準として考慮すべきであり、その場合には、端末局（移動無線局）と基地局との物理的制約の差異に照らして、ランダム数発生器の設置位置として基地局を選択する動機付けが存在することは明白である。

したがって、原告の上記主張は採用することができない。

(3) 「『ランダム値から導かれる暗号値が伝送位置にある装置から送信』される点について、本願発明では、『送信』が『返信』に記載変更されている」（審決

膳本3頁31行目～33行目）点につき、原告は、本願発明において、基地局から端末局（移動無線局）へ通話の度にランダム値を送信し、端末局は受信したランダム値により暗号化した識別コードを送信する構成としたのが、そうすることにより、識別コードとランダム値との送信の方向が逆となって窃取が困難となり、また、仮に、ランダム値と暗号化した識別コードが窃取されたとしても、次の通話の際のランダム値はそれと異なるから、窃取したデータを利用して不正な通話をすることができなくなるためであるとした上で、本願発明の要旨の「返送され」との規定が、このような本願発明の構成を明確に示しており、「返送」は本願発明の技術思想を表す重要な文言であるから、これを「送信」という文言と同一にとらえることができない旨主張する。

しかしながら、原告の上記主張に係る、識別コード（暗号化したメッセージ）とランダム値との送信の方向が逆となって窃取が困難となるとか、ランダム値と暗号化した識別コード（メッセージ）が窃取されたとしても、そのデータを利用して不正な通話（メッセージの不正使用）をすることができない等の効果は、端末局においてユーザーにより入力されたメッセージをランダム値で暗号化して基地局に送信する認証技術において、そのランダム値に係るランダム数発生器の設置位置を基地局としたこと、あるいはメッセージをランダム値で暗号化すること自体に伴って当然に予測される効果にすぎない。のみならず、そもそも、ランダム値によって暗号化された識別コードが端末局から基地局に送信される点において、本願発明と引用発明とで異なる点ではなく、その送信を「返送」と表現したところで、技術的内容に相違が生ずるものではない。本願発明の要旨が、この送信を「返送され」と規定したのは、ランダム値の移動無線システム（基地局）から移動無線局（端末）への送信を基地局側から見て「送信され」と規定したことに合わせて基地局側から見た表現を採用したにすぎないものと解するのが相当である。

したがって、原告の上記主張は採用することができない。

（4） そうすると、相違点3についての審決の判断は、周知例3（甲第7号証）を引用した点は必ずしも適切ではないが、その瑕疵は審決の結論に影響を及ぼすものではなく、その判断に原告主張の誤りはない。

3 取消事由3（相違点4についての判断の誤り）について

審決の相違点4についての「伝送位置（移動無線局）自体に『識別コード』を割り当てる必要がある以上、何らかの形で識別コードの格納手段を設けなくてはならないから、上記相違点4も単なる設計的事項にすぎない」（審決膳本4頁31行目～33行目）との判断につき、原告は、ユーザー認証システムである引用発明において、端末にユーザー識別コードをあらかじめ格納しておくことができないことは当然であるから、端末に識別コードの格納手段を設けることは設計的事項でない旨主張する。

確かに、審決の上記「設計的事項」との文言は適切を欠くものではあるが、相違点2で認定されたとおり、本願発明が、移動無線局（端末）自体に識別コードを割り当てるものである以上、移動無線局に識別コードの格納手段を設けることは、いわば自動的に導かれる事項であって、このような構成を採用することの容易推考性を改めて検討するまでもないことである。審決の上記説示は、この趣旨を述べたものであることが明白であり、したがって、その判断に誤りはない。

4 以上のとおり、原告主張の審決取消事由は理由がなく、他に審決を取り消すべき瑕疵は見当たらないから、原告の請求を棄却することとし、訴訟費用の負担並びに上告及び上告受理申立てのための付加期間の指定につき行政事件訴訟法7条、民事訴訟法61条、96条2項を適用して、主文のとおり判決する。

東京高等裁判所第13民事部

裁判長裁判官 篠 原 勝 美

裁判官 石 原 直 樹

裁判官 宮 坂 昌 利