平成２８年１２月２６日判決言渡

平成２８年（行ケ）第１００４０号　審決取消請求事件

口頭弁論終結日　平成２８年１２月１２日

判　　決

原　　告	コーニンクレッカ　フィリップス　エヌ　ヴェ	
訴訟代理人弁理士	津　　軽	進
	笛　　田　秀	仙
	矢　ヶ　部　喜	行
被　　告	特　許　庁　長　官	
指定代理人	石　　井　茂	和
	高　　木	進
	相　　崎　裕	恒
	田　　中　敬	規

主　　文

１　特許庁が不服２０１４－５２３３号事件について平成２７年９月３０日にした審決を取り消す。

２　訴訟費用は被告の負担とする。

事 実 及 び 理 由

第１　原告の求めた裁判

主文同旨

第２　事案の概要

本件は，特許出願拒絶査定に対する不服審判請求を不成立とした審決の取消訴訟である。争点は，①手続違背の有無，②進歩性の有無（一致点の認定の誤り，相違点についての判断の誤り）である。

１　特許庁における手続の経緯

原告は，名称を「安全な認証型距離測定法」とする発明につき，平成１５年（２００３年）６月２７日を国際出願日とする特許出願（パリ条約による優先権主張　平成１４年（２００２年）７月２６日（本願優先日）・欧州特許庁。特願２００４－５２５６００号。原出願。）の分割出願として，平成２２年（２０１０年）４月２８日，特許出願（甲６。特願２０１０－１０３０７２号，請求項の数１３。本願。）をし，平成２４年１２月２１日に手続補正をした（乙１）が，平成２５年１１月１３日付けで拒絶査定を受けた（甲１０）ので，平成２６年３月１９日，拒絶査定不服審判請求をするとともに（甲７。不服２０１４－５２３３号。），平成２７年４月２１日に手続補正をした（乙２。請求項の数１４。本願補正。）。

特許庁は，平成２７年９月３０日，「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，同年１０月１３日，原告に送達された。

２　本願発明の要旨

本願補正後の請求項１に係る発明（以下「本願発明」という。）は，本願補正書（乙２）に記載された以下のとおりのものである（なお，本願の願書に最初に添付された明細書及び図面（甲６）を併せて「本願明細書」という。）。

【請求項１】

「　第１通信装置に記憶されたマルチメディアデータが第２通信装置によってアク

セスされるべきかを決定する方法であって，当該方法は，前記第１通信装置と前記第２通信装置との間の距離測定を実行し，測定された距離が事前に規定された距離間隔の範囲にある場合に，前記第２通信装置による前記マルチメディアデータへのアクセスを許可し，前記距離測定は，

第１時間ｔ１において第１信号を前記第１通信装置から前記第２通信装置へ伝送するステップであって，前記第２通信装置が，前記第１信号を受信し，前記第１通信装置及び前記第２通信装置が共有する共通秘密に従い前記受信された第１信号を修正することにより第２信号を生成し，前記第２信号を前記第１通信装置へ伝送するように構成された，ステップと，

第２時間ｔ２において前記第２信号を受信するステップと，

前記第２信号が前記共通秘密に従い修正されたかを確認するステップと，

前記第１通信装置と前記第２通信装置との間の距離をｔ１とｔ２との間の時間差に従い決定するステップと，

に従い実行され，

前記第１通信装置と前記第２通信装置との間で前記共通秘密を鍵管理プロトコルに従って安全に伝送することによって共有する方法。」

３　審決の理由の要旨

(1)　引用発明の認定

甲１（特開平９－１７０３６４号公報）には，次の発明（甲１発明）が記載されていると認められる。

「　車両側無線装置が，携帯型無線装置からの応答信号に基づいて，ドアの解錠指令の送出を決定する方法であって，

前記車両側無線装置から，前記携帯型無線装置までの距離Ｒの算定が行われ，

前記車両側無線装置と，前記携帯型無線装置との距離Ｒが所定値Ｒｏ未満であればドアの解錠指令の送出を決定し，

前記携帯型無線端末までの距離Ｒの算定は，

前記車両側無線装置と前記携帯型無線装置の双方に予め同一の関数Ｆ（ｘ）を登録させておき，

前記車両側無線装置が，乱数ｚを呼出し信号に含ませて送出すると共に，この乱数を登録中の関数Ｆ（ｘ）に代入することにより関数値Ｆ（ｚ）を算定し，

前記携帯型無線装置は，受信した呼出し信号から乱数ｚを抽出し，これを登録中の関数Ｆ（ｘ）に代入することにより，関数値Ｆ（ｚ）を生成し，これを応答信号に含ませて送信し，

前記車両側無線装置は，受信した応答信号から関数値Ｆ（ｚ）を抽出し，これを予め算定しておいた関数値Ｆ（ｚ）と照合し，照合一致の場合には前記応答信号が正当であると判定し，

前記応答信号が正当であると判定された場合に，前記車両側無線装置が，前記呼出し信号を送信してから前記応答信号を受信するまでの所要時間Ｔを算定し，前記Ｔから，前記呼出し信号と前記応答信号の伝播所要時間ｔを算定し，これを電波の伝播速度Ｃで除算することにより，前記距離Ｒを算定する，方法。」

⑵　本願発明と引用発明との一致点及び相違点

ア　一致点

「　第１信号送信装置が，第２信号送信装置に対して所定のサービスを実行すべきかを決定する方法であって，当該方法は，第１信号送信装置と第２信号送信装置との間の距離測定を実行し，

測定された距離が事前に規定された距離間隔の範囲にある場合に，前記第２信号送信装置への所定のサービスの実行を許可し，

前記距離測定は，

第１時間ｔ１において第１信号を前記第１信号送信装置から前記第２信号送信装置へ伝送するステップであって，前記第２信号送信装置が，前記第１信号を受信し，前記第１信号送信装置及び前記第２信号送信装置が共有する共通秘密に従い前記受

信された第１信号を修正することにより第２信号を生成し，前記第２信号を前記第１信号送信装置へ伝送するように構成された，ステップと，

第２時間ｔ２において前記第２信号を受信するステップと，

前記第２信号が前記共通秘密に従い修正されたかを確認するステップと，

前記第１信号送信装置と，前記第２信号送信装置との間の距離をｔ１とｔ２との間の時間差に従い決定するステップと，

とに従い実行される，方法。」

イ　相違点

(ｱ)　相違点１

「　“第１信号送信装置が，第２信号送信装置に対して所定のサービスを実行すべきかを決定する”ことに関して，

本願発明における『所定のサービスを実行すべきかを決定する』ことが，“第１通信装置に記憶されたマルチメディアデータへの，第２通信装置によるアクセスの許可の決定”であって，『第１通信装置』が，『マルチメディアデータ』を記憶する装置であり，『第２通信装置』が，当該『マルチメディアデータ』のアクセスを要求する装置であるのに対して，

引用発明においては，“車両側無線装置が搭載された車のドアの解錠の決定”であって，『マルチメディアデータ』との関係については，特に，言及されていない点。」

(ｲ)　相違点２

「　本願発明においては，『前記第１通信装置と前記第２通信装置との間で前記共通秘密を鍵管理プロトコルに従って安全に伝送することによって共有する』ものであるのに対して，

引用発明においては，どのようにして，『車両側無線装置と携帯型無線装置の双方に予め同一の関数Ｆ（ｘ）を登録させておく』のか，特に，言及されていない点。」

(3)　判断

ア　相違点１について

甲１発明において，“車両側無線装置と，携帯型無線装置との距離Ｒが所定値Ｒｏ未満であるかを判定する”処理と，“ドアの解錠指令の送出を決定する”処理との間に一体不可分の関係は存在しておらず，前記“判定する”処理の結果として，許可される処理として，「ドアの解錠指令の送出」以外を設定することは，当業者が適宜なし得る事項である。

そして，“２つの装置が，所定の距離範囲内に存在するか否かを判定し，存在する場合に，所定のプログラムや，データ，或いは装置へのアクセスを許可する”ようなことは，本願の原出願の第１国出願前に，当業者には周知の技術事項である（甲３（特開２００２－１８９９６６号公報），４（国際公開特許公報ＷＯ９９／４９３７８号，４の２（特表２００３―５２６８２６号公報））から，甲１発明において，“車両側無線装置と，携帯型無線装置との距離Ｒが所定値Ｒｏ未満であるかを判定”した後，“距離Ｒが所定値Ｒｏ未満であった場合”に，“車両のドアの解錠を行う”ことに換えて，“車両内の記憶手段に記憶されているマルチメディアデータ等の資源へのアクセスを，携帯型無線装置に許可する”といった構成を採用することは，当業者が適宜なし得る事項である。

したがって，相違点１は，格別のものではない。

イ　相違点２について

ＩＳＯ９７９８に記載のプロトコル等に従って「秘密」を共有することは，本願の原出願の第１国出願前に，当業者には周知技術にすぎない（甲２（特開２００１－２４９８９９号公報））。

また，甲１発明において，「車両側無線装置と携帯型無線装置の双方に予め同一の関数Ｆ（ｘ）を登録させておく」ことに関して，キーレス・エントリーシステムにおいて，“自動車側の施錠装置”と，“無線装置”間で，鍵の配送等をセキュアに行うことは，当業者にとって周知の技術事項である（甲５（特開平１１－１０１０３５号公報））から，甲１発明においても，「関数Ｆ（ｘ）」を更新する構成を採用し，当該更新の手法として，甲２に開示されている「鍵管理プロトコル」を採用するこ

とは，当業者が適宜なし得る事項である。

したがって，相違点２は，格別のものではない。

ウ　結論

よって，本願発明は，本願の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２９条２項の規定により特許を受けることができない。

第３　原告主張の審決取消事由

１　取消事由１（手続違背の存在）

甲３～５を引用した拒絶の理由を通知することなく行われた審決には，特許法１５９条２項が準用する同法５０条の規定に違反する手続違背がある。

(1)　マルチメディアデータの情報セキュリティの分野において，マルチメディアデータのアクセスに関与する両装置間の距離に応じてアクセスを許可するか否かを決定すること，及び，キーレス・エントリーシステムにおいて秘密鍵を無線装置間で配送することが周知・慣用技術であるかについて，審査及び審判段階のいずれの拒絶理由通知・拒絶査定においても言及されていない。

拒絶理由通知で慣用（又は周知）技術として議論されているのは，（距離測定との関係が不明な）何らかの認証によってマルチメディアデータへのアクセスを許可する技術であり，被告が，審決において新たに引用した甲３及び４によって示した「２つの装置が，所定の距離範囲内に存在するか否かを判定し，存在する場合に，所定のプログラムや，データ，或いは装置へのアクセスを許可する」技術ではない。

(2)　これらの点は，審判段階の拒絶理由通知（甲１１）に対する原告の意見書（甲１２）における主要な争点であるところ，甲３～５は，周知文献ではなく引用文献として評価されるべきものであり，当該引用文献を引用した拒絶の理由は，査定の理由と異なる拒絶の理由であって，本件審決前に通知されていない拒絶理由で

ある。

被告が拒絶理由通知において慣用技術であると主張していなかった「２つの装置が，所定の距離範囲内に存在するか否かを判定し，存在する場合に，所定のプログラムや，データ，或いは装置へのアクセスを許可する」ことが慣用技術であることを立証するための文献を，審決において初めて引用することは，原告にとって不意打ちとなり過酷である。

被告は，手続保障の観点から，それらの文献について意見書を提出する機会を与える必要があったというべきであり，そのような機会を与えることなく行われた審決には手続違背がある。

２　取消事由２（進歩性の存在）

本願発明は，甲１及び甲２に記載された発明並びに甲３～５に記載された事項に基づいて容易に発明をすることができたものではない。

(1)　一致点の認定の誤り

審決は，本願発明と甲１発明とは，第１信号送信装置と第２信号送信装置との間の測定された距離が事前に規定された距離間隔の範囲にある場合に，「第２信号送信装置へ」の「所定のサービスの実行」を許可する点で，一致すると判断するが，前記判断は誤りである。

本願発明と甲１発明とは，距離測定の結果に基づいて実行される処理の内容が異なり，当該処理が，本願発明では第１信号送信装置と第２信号送信装置との間で実行される処理であるのに対し，甲１発明では第１信号送信装置の側で実行される処理である点において相違する。

ア(ア)　本願発明では，第１通信装置は，映画のライセンス保持者の認証物件として機能するマルチメディアデータを記憶するＰＣ等やＤＶＤ再生装置などに対応し，第２通信装置は，当該マルチメディアデータを表示するためのテレビなどに対応し，第１通信装置に記憶されたマルチメディアデータは，第２通信装置に転送

又は複製される（第２通信装置が受信する。）。

したがって，本願発明の「第１通信装置に記憶されたマルチメディアデータが第２通信装置によってアクセスされる」及び「第２通信装置によるマルチメディアデータへのアクセス」は，第１通信装置との間で距離測定がされる第２通信装置への転送や複製を介したアクセスである。

(ｲ)　ＤＶＤに記録された映画を隣人宅のテレビで再生する場合，ＤＶＤ再生装置と認証物件との間の距離測定は，ＤＶＤ再生装置とテレビ・スクリーン間の距離が不明であるから，当該認証物件を所持する者がテレビ・スクリーンの近くにいるといえる場合か否かの判定の役に立たないのであって，本願発明の課題を解決することができない。

したがって，この場合は，本願発明の態様に含まれない。

(ｳ)　以上によれば，前記(ｲ)の場合が本願発明の態様に含まれることを前提に，「アクセス」は第２通信装置への転送や複製を介在したアクセスには限定されていないとする後記第４の２(1)ア記載の被告の主張は，失当である。

イ(ｱ)　甲１発明は，車両側に存在するドア用キーシリンダーの施解錠に関するキーレス・エントリーシステムに関するものであり，甲１発明の一般化を試みたとしても，車両のドア以外のドアの施解錠に限られ，「所定のサービスの実行」まで拡張することはできない。

(ｲ)ａ　甲１発明における「解錠指令」の「送出」は，ドアの解錠に特有ではない処理であるとする，後記第４の２(1)イ記載の被告の主張は，意味不明である。

仮に，前記主張が，甲１発明において，「車両側無線装置と携帯型無線装置との間の距離測定から独立して」，すなわち，「そのような距離測定とは無関係に」送光部３４から送信される何らかの信号がドアの施解錠以外に利用可能であるとの主張であるとしても，２装置間の距離測定の結果に基づいて送光部３４から送信される信号が何であるかが問題となり，甲１発明では，前記信号は，ドアの施解錠に特有のもののみである。

b　進歩性の判断に当たっては，特許出願に係る発明が，公知文献に記載された発明に基づいて容易に発明することができたか否かが問題なのであって，公知文献において排除されていない発明に基づいて容易に発明をすることができたかどうかが判断されるのではない。

仮に，公知文献において排除されていなければ当該文献に記載されていると解釈できるのであれば，公知文献に開示された発明を無制限に拡張することが可能となり，不合理である。

⑵　相違点１の判断の誤り

審決は，甲１発明において，「“車両側無線装置と，携帯型無線装置との距離Ｒが所定値Ｒｏ未満であるかを判定する”処理と，“ドアの解錠指令の送出を決定する”処理との間に一体不可分の関係は存在しておらず，前記“判定する”処理の結果として，許可される処理として，『ドアの解錠指令の送出』以外を設定することは，当業者が適宜なし得る事項である。」と判断するが，車両側無線装置と携帯型無線装置との間の距離の判定処理の結果として許可される処理として，「ドアの解錠指令の送出」以外を設定することは，当業者が適宜なし得る事項ではない。

ア(ｱ)ａ　甲１発明において，車両側無線装置と携帯型無線装置との距離Ｒが所定値Ｒｏ未満である場合にドアを解錠する理由は，携帯型無線装置を所持するユーザ（ドライバー等）が車両から遠く離れている場合にドアの解錠が行われてしまうとセキュリティ上の問題が生じてしまうから，そのような事態を防止するためである。

したがって，「車両側無線装置と，携帯型無線装置との距離Ｒが所定値Ｒｏ未満であるかを判定する」処理と，「ドアの解錠指令の送出を決定する」処理との間には，一体不可分の関係が存在する。

b　この点，被告は，後記第４の２⑵ア(ｱ)ｂのとおり，「ポリシー」と「メカニズム」は独立に検討され得るものであると主張する。

しかしながら，「ポリシー」は，システムにおけるセキュリティの目的，達成すべ

き目標，満たすべき条件などを定めるものであり，「メカニズム」は，ポリシーを実現する技術的手段である（乙３）。また，ポリシーの表現態様も，メカニズムの１つである。

甲１発明における「ポリシー」は，「車両側無線装置と携帯型無線装置との間の測定された距離Ｒが所定値Ｒｏ未満である場合にドアの解錠指令を送出する」であり，「メカニズム」は，乱数ｚ，関数Ｆ（ｘ）を用いて，呼び出し信号と応答信号の伝播所要時間ｔと電波の伝播速度Ｃなどから距離Ｒを計算することである。

前記ポリシーによって，アクセス制御のセキュリティ上の目的のうち，少なくとも，機密保持の一態様としての車両自体又は車両内に存在する物品の盗難などの防止という目的を達成することができる。

被告が甲１発明におけるアクセス制御の「ポリシー」であると主張する，「車とユーザ（携帯型無線装置）との間の距離Ｒが所定値Ｒｏ未満である場合を正当なものとする」ことのみでは，アクセス制御の目的である①機密保持，②データ，システムの完全性，及び③システムの可用性のいずれの目的も達成することができない。アクセスが「正当なもの」であった場合に「何を許可するのか」までを定義して，初めて何らかのアクセス制御の目的を達成することができる。

したがって，甲１発明において，「車両側無線装置と携帯型無線装置との間の測定された距離Ｒが所定値Ｒｏ未満である」ことと「ドアの解錠指令を送出する」ことは１つのポリシーとして一体に定められるものであって，互いに一体不可分の関係にある。

(ｲ)　前記⑴イ(ｱ)のとおり，甲１発明を，ドアの施解錠処理以外の「所定のサービスの実行」にまで拡張することはできない。

イ　仮に，甲１発明において，距離判定の結果として許可される処理として「ドアの解錠指令の送出」以外を設定したとしても，当該処理は，車両側無線装置（第１信号送信装置）の側において実行されるにすぎず，車両側無線装置（第１信号送信装置）と携帯型無線装置（第２信号送信装置）との間で実行される処理が

許可される発明にはならない。

甲１発明は，車両側無線装置（第１信号送信装置）が距離測定の結果に基づいて解錠処理を実行するのは，当該車両側無線装置が搭載された車両の側に存在する施解錠実行部１０又はドア用キーシリンダーに対してであって，携帯型無線装置（第２信号送信装置）に対してではない。

ウ　甲１発明に，甲３及び甲４に記載された技術を組み合わせたとしても，本願発明のように，距離測定の対象である第１通信装置（第１信号送信装置）及び第２通信装置（第２信号送信装置）のうち，第１通信装置に記憶されたマルチメディアデータへのアクセスを，第２通信装置に許可する発明にはなり得ない。

(ｱ)　甲３に記載された技術は，電子情報担体１（例えばクレジットカード）と，当該電子情報担体１の識別情報で特定される携帯通信端末６（例えば携帯電話やＰＨＳ）との間の距離が正当な使用範囲内である場合に，当該電子情報担体の使用を許可するものであって，距離測定の対象である電子情報担体及び携帯通信端末のうちの一方の装置に記録されたプログラムやデータへのアクセスを，他方の装置に許可する技術ではない。

(ｲ)　甲４に記載された技術は，ワークステーションとユーザが所持するトークンとの間の距離が所定の最大距離以内である場合に，「ユーザ」によるワークステーションへのアクセスを許可するものであって，距離測定の対象であるワークステーション及びトークンのうちの一方の装置に記録されたプログラムやデータのアクセスを，他方の装置に許可する技術ではない。

エ　また，甲１発明に，乙８又は乙９に記載された周知技術を組み合わせて本願発明を容易に発明することはできない。

前記ア(ｱ)のとおり，甲１発明において，「車両側無線装置と，携帯型無線装置との距離Ｒが所定値Ｒｏ未満であるかを判定する」処理と，「ドアの解錠指令の送出を決定する」処理との間には，一体不可分の関係があるから，両装置間の距離判定に基づいて，ドアの解錠処理以外の処理を行うことを，当業者が容易に想到することは，

あり得ない。

キーレス・エントリーシステムに関してユーザが車から離れている場合に許可すべきでないのはドアの解錠のみであり，乙８及び乙９には，車載装置側のデータへの携帯装置のアクセスや携帯装置側のデータへの車載装置のアクセスの許可に，ユーザと車との間の距離を考慮することは，開示も示唆もされていない。

(3) 相違点２の判断の誤り

審決は，「キーレス・エントリーシステムにおいて，“自動車側の施錠装置”と，“無線装置”間で，鍵の配送等をセキュアに行うことは，当業者にとって周知の技術事項であるから，甲１発明においても，「関数Ｆ（ｘ）」を更新する構成を採用し，当該更新の手法として，甲２に開示されている「鍵管理プロトコル」を採用することは，当業者が適宜なし得る事項である。」と判断するが，甲５において採用されている暗号方式は，公開鍵暗号方式であり，装置＃Ａから装置＃Ｄに配送されているのは，公開鍵であり，装置＃Ａと装置＃Ｄとの間の秘密ではないから，当業者が，甲５の開示内容に基づいて，甲１発明のＦ（ｘ）を車両側無線装置と携帯型無線装置との間で配送する構成を採用することは，あり得ない。

ア　甲１発明は，同一の関数Ｆ(ｘ)を共通秘密として，２装置間の認証を行うものであるから，共通鍵暗号方式に基づくものであり，両装置にあらかじめ同一の関数Ｆ（ｘ）を登録させておくことが選択されており，両装置の間で関数Ｆ（ｘ）を伝送することを否定している（甲１の【００２７】，【００２８】）。

共通鍵の秘匿性が高度に求められる共通鍵暗号方式と，公開鍵自体は公開されている公開鍵暗号方式とは，思想を異にし，公開鍵方式では，両装置間で保持する秘密は，共通ではなく，異なるものである。

したがって，甲２によって，「セッション鍵」という「秘密」を伝送して共有することが周知技術であるとしても，当業者が当該周知技術を甲１発明に付加することはあり得ない。

イ　甲５において公開されている公開鍵が装置Ａ＃と装置Ｄ＃との間で伝送

により共有されていることは，共通鍵方式の甲１発明に甲２の周知技術を付加する動機付けとはなり得ない。

被告は，後記第４の２(3)イのとおり，甲５においては，装置＃Ｄを装置＃Ａが認証して初めて装置＃Ｄに暗号化されて送信された「使用回数／期限付きで消滅するプログラムを内包させた＃Ａ公開暗号キー」がこれらの間の暗号化通信に用いられるのであり，これが両装置間の「秘密」であると解してよいと主張する。

しかしながら，「装置＃Ｄを装置＃Ａが認証して初めて」が，甲５のどの記載に対応するものであるのか不明である。

また，暗号化通信に用いられるのは，「＃Ａ公開暗号キー」であって，この公開暗号キーが公開されているという事実には変わりがない。

ウ　甲１発明のキーレスエントリーの技術分野における当業者にとって，甲３の電子情報担体の不正使用防止技術及び甲４のマルチユーザコンピュータ環境におけるアクセス技術は，周知・慣用技術ではない。

第４　被告の反論

１　取消事由１について

拒絶理由通知と審決を全体としてみれば，審決は，拒絶理由通知において示したものと異なる理由を示したものではなく，手続違背はない。

(1)　平成２７年４月２１日付け手続補正書（乙２）による本願補正により特許請求の範囲が補正されていることから，審決における一致点，相違点１，相違点２は，平成２６年１０月１５日付け拒絶理由通知（甲１１）における一致点，相違点１，相違点２と，文言上同じではないが，それぞれが内容的に対応している。

(2)　審決の相違点判断は，前記拒絶理由通知における相違点判断と文言上同じではないが，甲３～５は，相違点の判断に当たって，当業者の「通常の知識」を補足説明するために示したものにすぎない。とりわけ，甲５は，原告が意見書において主張した阻害事由が存在しないことを示すためのものであり，キーレス・エン

トリーシステムにおいて秘密鍵を無線装置間で配送すること自体を副引用発明として示すためのものではない。

２　取消事由２について

(1)　一致点の認定の誤りについて

本願発明と甲１発明とは，第１通信装置が認証により第２通信装置によるサービスの実行を許可する点において一致している。

ア　本願発明における「アクセス」とは，アクセス要求と，それに対し，何らかの利便を与える行為の総称をいい，「第２通信装置による」「アクセス」とは，「第２通信装置」を用いた「アクセス」を総称したものであって，「第１通信装置」との間で「距離測定」がされる「第２通信装置」への転送や複製を介在したアクセスには限定されていない。

「第２通信装置」による「アクセス」であれば，「第１通信装置」の側で実行される処理であってもかまわないから，甲１発明が「第１通信装置の側で実行される処理」であることは，本願発明との相違点にならない。

(ｱ)　ＤＶＤに記録された映画を隣人宅のテレビで再生する場合，ＤＶＤ再生装置と認証物件との間で距離測定がされるとき，ＤＶＤ再生機器が「第１通信装置」，認証物件が「第２通信装置」となる。また，インターネットで流通してＰＣ等に記録された映画を隣人宅のテレビで再生する場合，認証物件であるＰＣ等とテレビとの間で距離測定がされるとき，認証物件として機能するＰＣ等が「第１通信装置」となり，テレビが「第２通信装置」となる。

仮に，「第２通信装置」による「アクセス」を，「第２通信装置」への転送や複製を介在したアクセスの趣旨と限定解釈すると，前者は，本願発明の実施態様に含まれない。

しかし，本願発明が考慮しているマルチメディアデータには，ＤＶＤに記録されたものが含まれており，一方が認証物件であるとともに，一方にマルチメディアデ

ータが記憶されているという要件を満たすにもかかわらず，前者の場合を技術的に区別する理由は見当たらない。

(ｲ)　前者の場合，映画を記録した媒体の貸与や無断持出しに対する再生制限となるが，後者の場合，そのような再生制限となっていないから，それのみで課題解決手段とならない場合が想定される。ＰＣ等とテレビとのインタフェースが近距離無線の場合には，所定範囲内に機器が置かれていなければそもそも再生がされないが，後者の距離測定により実現されることは，これと変わらない。

(ｳ)　このように，「第２通信装置」による「アクセス」を，「第１通信装置」との間で「距離測定」がされる「第２通信装置」への転送や複製を介在したアクセスの趣旨と限定する解釈は，技術的に合理的な区別によるものではない上，本願発明を明細書に記載された課題を解決できない態様へと限定して解釈するものであって，このような解釈に合理性はない。

イ　審決において，甲１発明は，必ずしもドアの解錠に特有ではない処理を捉えて認定されており，甲１発明は，解錠以外のサービスにおいても用いることが可能な内容を示している。

(ｱ)　甲１には，２つの実施例（図１に係るものと，図３に係るもの）が記載されている。これらは，ドアの解錠をアクチュエータを起動して行う構成については共通しているものの，図１に係る実施例は，認証の結果として所定のサービスを実行するという，ドアの解錠以外の処理にも応用可能な処理を行うものである。

(ｲ)　甲１には，解錠以外のサービスについては明示されていないが，エンジンやエアコンの始動（乙６，７）や照明の制御（乙７），自動車のオーディオやカーナビゲーションシステムの制御（乙７）が想定され，これらは既にキーレス・エントリーシステムに係る制御の態様とされているものである。

⑵　相違点１の判断の誤りについて

ア(ｱ)ａ　２の装置間の距離が所定範囲内であることを判定することによ

り，所定のプログラム若しくはデータ又は装置へのアクセスを許可すること（すなわち，装置間の距離が所定範囲内であることによって許可されるアクセスを，所定のプログラム若しくはデータ又は装置へのアクセスとすること）は，周知技術である（甲３，４）し，自動車に「オーディオ」や「カーナビゲーションシステム」のように「マルチメディアデータ」を用いたサービスが用意されている場合が多いことにも照らせば，「データ」を「マルチメディアデータ」を含むものとすることは，文献を示すまでもない事項である。

前記⑴イのとおり，甲１発明の処理の中には，オーディオやカーナビゲーションシステムの動作も含まれ得るから，甲１発明において，「ドアの解錠指令の送出」以外を設定し，その際，「第１通信装置」である車両内に記憶されたマルチメディアデータへのアクセスを許可するように構成することは，当業者が適宜なし得ることである。

ｂ　認証を用いたアクセス制御において，どのようなアクセスが「正当」であるかの定義である「ポリシー」は，このポリシーを実現するための「メカニズム」と独立に検討され得る（乙３）。

甲１発明において，車とユーザ（携帯無線装置）との間の距離Ｒが所定値Ｒｏ未満である場合を正当なものとする「ポリシー」と，ドアの解錠が要求された場合にこの「ポリシー」に従ってドアの解錠指令の送出を決定する「メカニズム」とは，独立に検討され得るのであり，必ずしも一体不可分なものとして検討される必要はない。

ドライバーが車から離れている場合に解錠されることによって問題が生じないようにする必要があることは，甲１発明において，「解錠指令の送出」を用いない他の「メカニズム」を採用できない理由にならない。

(ｲ)　前記(1)アのとおり，「第２通信装置」による「アクセス」とは，「第２通信装置」を用いたアクセスを総称したものであって，本願発明において「許可」されるのは，必ずしも，互いの間の距離測定がなされる「第１通信装置」と

「第２通信装置」との間で実行される処理ではない。

イ　仮に，これが，互いの間の距離測定がされる「第１通信装置」と「第２通信装置」との間で実行される処理であるという前提に立つとしても，キーレス・エントリーシステムにおいて，「車載装置（第１通信装置）」と「携帯装置（第２通信装置）」との間でデータを送受信し，車載装置側のデータに携帯装置がアクセスしたり，携帯装置側のデータに車載装置がアクセスすることは，周知技術である（乙８，９）。

甲１発明とこの周知技術とは，いずれもキーレス・エントリーシステムに係るものであり，このようなキーレス・エントリーシステムでは，ユーザ（携帯無線装置）が車から離れている場合の車へのアクセスを許可すべきでないのであるから，甲１発明とこの周知技術を組み合わせて，装置間の距離が所定範囲内であることによって車載装置側のデータに携帯装置がアクセスしたり，携帯装置側のデータに車載装置がアクセスすることを許可するように構成することは，当業者が適宜なし得ることであり，相違点１は容易想到である。

(3)　相違点２の判断の誤りについて

ＩＳＯ９７９８に記載のプロトコル等に従って「秘密を共有すること」は，周知技術であり，甲１発明においてこのような周知技術を採用することは，適宜なし得る事項であり，格別のものではない。

ア　「ＩＳＯ９７９８の相互認証手続」として「公開鍵暗号方式を用いた相互認証方法」によって，共通鍵暗号による通信に使用される「セッション鍵」という「秘密」をＡ，Ｂ間で共有することは，ＩＳＯ９７９８が国際規格であることからしても，周知技術である（甲２）。

甲１発明においては，何らかの形で「秘密」であるＦ（ｘ）を共有する必要があり，このために周知技術を単に付加することは，当業者が適宜なし得ることである。

イ　甲５においては，装置＃Ｄを装置＃Ａが認証して初めて装置＃Ｄに暗号

化されて送信された「使用回数／期限付きで消滅するプログラムを内包させた＃Ａ公開暗号キー」が，これらの間の暗号化通信に用いられるのであり，これが両装置間の「秘密」であると解してよい。

ウ　審決は，甲１発明において甲５に開示された構成を採用することが容易想到であると説示したわけではないのであり，甲１と甲５が「思想を異にする」としても審決の論旨が成り立たなくなるものではない。

第５　当裁判所の判断

１　本願発明と引用発明について

(1) 本願発明について

本願明細書（甲６）には，以下の記載がある。

【技術分野】

【０００１】

本発明は，第１通信装置と第２通信装置との間の認証型距離測定を実行する第１通信装置のための方法に関する。本発明は，第１通信装置に記憶されたデータが，第２通信装置によってアクセスされるべきかを決定する方法にも関する。更に，本発明は，第２通信装置への認証型距離測定を実行するための通信装置に関する。本発明は，通信装置を有する，マルチメディア・コンテンツを再生するための機器にも関する。

【背景技術】

【０００５】

デジタル・データの形のコンテンツを保護する一つの手段は，コンテンツが，

－受信装置が，準拠した装置であるとして認証された場合と，

－コンテンツの使用者が，このコンテンツを他の装置に転送（移動，複製）する権利を有する場合と，

にのみ転送されるということを保証することである。

【０００６】

コンテンツの転送が許可される場合，この転送は，コンテンツが有用な形式で違法に取り込まれ得ないことを確実にする暗号化手段で一般的に実行される。

【０００７】

装置認証及び暗号化コンテンツ転送を実行する技術は，利用可能であり，セキュア認証済チャンネル（ＳＡＣ）と呼ばれる。ＳＡＣ上に渡ってコンテンツを複製することを可能にされ得るが，コンテンツ業界は，インターネット上でのコンテンツ流通に関しかたくなである。これにより，インターネットすなわちイーサネット（登録商標）とうまく整合するインターフェース上でのコンテンツの転送に関し，コンテンツ業界の意見の不一致が生じる。

【０００８】

また，隣人を訪ねている使用者が，彼が所有する映画を隣人の大きなテレビ・スクリーンで鑑賞することは，可能であるべきである。一般的にコンテンツ所有者は，このことを許可しないであろうが，この映画のライセンス保持者（又はこのライセンス保持者が所有する装置）が，このテレビ・スクリーンの近くにあると証明され得る場合，容認され得る。

【０００９】

したがって，コンテンツが他の装置によってアクセスされる又は複製されるべきかを判断する場合に，認証型距離測定を含むことが可能であることは興味深い。

【発明が解決しようとする課題】

【００１１】

本発明の目的は，有限距離におけるコンテンツの安全な転送を実行する課題に対する解決法を得ることである。

【課題を解決するための手段】

【００１２】

このことは，第１通信装置が前記第１通信装置と第２通信装置との間の認証型距離測定を実行する方法によって達成され，前記第１通信装置及び前記第２通信装置は，共通秘密を共有し，前記共通秘密は，第１及び第２通信装置との間の距離測定を実行するのに用いられる。

【００１３】

前記共通秘密は距離測定を実行するために使用されているので，第１通信装置から第２通信装置への距離を測定する場合，測定されているのは正しい装置間の距離であることを保証され得る。

【００１５】

特定の実施例において，当該認証型距離測定は，次の，

－第１時間ｔ１において第１信号を前記第１通信装置から前記第２通信装置へ伝送するステップであって，前記第２通信装置が，前記第１信号を受信し，前記受信された第１信号を前記共通秘密に従い修正することにより第２信号を生成し，前記第２信号を前記第１装置へ伝送するように構成されたステップと，

－第２時間ｔ２において前記第２信号を受信するステップと，

－前記第２信号が，前記共通秘密に従い修正されたかを確認するステップと，

－前記第１と前記第２通信装置との間の距離をｔ１とｔ２との間の時間差に従い決定するステップと，

に従い実行される。

【００１６】

信号の伝送と受信との間の時間差を測定し，帰還信号が第２通信装置から実際に生じたかを決定するための，第１及び第２通信装置の間で共有された秘密を使用することによって距離を測定する場合に，（前記秘密を知らない）第３通信装置へこの距離が測定されないことを保証する安全な認証された手段で，この距離は測定される。信号を修正する共通秘密を使用することは，セキュアな認証型距離測定を実行する簡便な手段である。

【００２１】

共通秘密が距離測定を実行する前に共有されている実施例において，この共有ステップは，

－第２通信装置が一群の事前規定された準拠規則に準拠するかを確認することによって，第１通信装置からの第２通信装置に関する認証確認を実行するステップと，

－第２通信装置が準拠する場合，前記秘密を第２通信装置へ伝送することによって前記共通秘

密を共有するステップと，

によって実行される。

【００２２】

これは，秘密の共有を実施するのに安全な手段であり，準拠規則に準拠する装置のみが秘密を受信することが可能であることを保証する。更に，共有された秘密は，当該２つの装置の間においてＳＡＣチャンネルを生成するためにその後用いられ得る。当該秘密は，例えばＩＳＯ１１７７０－３に記載の鍵配送機構（key transport mechanisms）を用いて共有され得る。代わりとして，鍵共有プロトコル(key agreement protocol)が用いられ得，例えば，このプロトコルも，ＩＳＯ １１７７０－３に記載されている。

【００２４】

本発明は，第１通信装置に記憶されたデータが第２通信装置によってアクセスされるべきかを決定する方法に関し，当該方法は，第１通信装置と第２通信装置との間の距離測定を実施し，前記測定された距離が既定の距離区間の範囲内であるかを確認するステップを有し，ここでは，距離測定は，上記に従う認証型距離測定である。装置間におけるデータの共有に関連する認証型距離測定を用いることにより，コンテンツの不正配布は，低減され得る。

【００２５】

特定の実施例において，第１装置に記憶されたデータが第２装置によってアクセスされるべきであると決定される場合，第１装置に記憶されたデータは，第２装置に送信される。

【発明を実施するための形態】

【００３５】

図２（省略）において，流れ図は，認証型距離測定を実行する通信装置を各々有する２つの装置２０１と２０３との間の認証型距離測定を実行する概略的な考え方を示す。この例において，第１装置２０１は，第２装置２０３が要求したコンテンツを有する。この認証型距離測定は，次のように行われる。ステップ２０５において，第１装置２０１は，第２装置２０３を認証する。このステップは，第２装置２０３が，準拠する装置であるかを確認するステップを有し得，第２装置２０３が確かに第１装置２０１へ特定された装置であるかを確認するステップ

も有し得る。その後ステップ２０７において，第１装置２０１は，秘密を第２装置２０３と交換し，このステップは，例えば，ランダムに生成されたビットワードを装置２０３へ伝送することによって実行され得る。当該秘密は，例えば，ＩＳＯ　１１７７０等に記載の何らかの鍵管理プロトコルに従い安全に共有されなければならない。

【００３６】

その後ステップ２０９において，距離測定のための信号は，第２装置２０３へ伝送され，当該第２装置は，受信された信号を前記秘密に従い修正し，この修正された信号を第１装置へ再返送する。第１装置２０１は，出発信号と帰還信号との間の往復時間を測定し，帰還信号が前記交換された秘密に従い修正されたかを確認する。何らかの秘密に従う帰還信号の修正は，伝送システム及び距離測定に用いられる信号に最も依存しやすく，すなわち（１３９４，イーサネット（登録商標），ブルートゥース及びIEEE 802.11等のような）各々の通信システム関して特有である。

【００３９】

認証２０５及び秘密の交換２０７は，いくつかの既知であるISO国際標準規格の，ＩＳＯ　９７９８及びＩＳＯ　１１７７０に記載のプロトコルを用いて実行され得る。例えば，第１装置２０１は，次の通信シナリオに従い第２装置２０３を認証することができる。・・・

【００４１】

この場合，第２装置２０３が鍵を決定し（すなわち鍵制御を有し），これは，鍵配送プロトコルとも呼ばれるが，鍵共有プロトコルも用いられ得る。これは，第１装置が鍵を決定するような，反転され得る場合には望ましくないこともあり得る。ここで，秘密鍵は，図２におけるステップ２０７に従い交換された。再び，秘密鍵は，例えば，鍵配送プロトコル又は鍵共有プロトコルによって交換され得る。

【００４２】

距離が上述のような安全な認証手順で測定された後で，データは，ステップ２１１において第１装置及び第２装置の間で送信され得る。

【００４３】

図３（省略）は，認証型距離測定を実行するステップを更に詳細に示す。上述されるように，第１装置３０１及び第２装置３０２は，鍵を交換してあり，当該鍵は，第１装置のメモリ３０５及び第２装置のメモリ３０７に記憶される。距離測定を実行するために，信号は，伝送器３０９を介して第２装置へ伝送される。第２装置は，受信器３１１を介して該信号を受信し，３１３は，該信号をローカルに記憶された秘密を用いることにより修正を行う。前記信号は，第１装置３０１によって既知の規則に従い修正され，伝送器３１５を介して第１装置３０１へ返送される。第１装置３０１は，受信器３１７を介して前記修正された信号を受信し，３１９において，当該受信された修正信号は，ローカルに修正されていた信号と比較される。ローカルでの修正は，伝送器３０９で第２装置へ伝送される信号を用い，第２装置によって用いられる修正規則と同一のローカルに記憶された秘密を用いて信号を修正することにより，３２１において実行される。受信された修正信号とローカルに修正された信号とが同一である場合，受信された信号は，認証され，第１装置と第２装置との間の距離を決定するのに用いられ得る。この２つの信号が同一でない場合，受信された信号は，認証され得ず，したがって３２５で示されるように距離を測定するのに用いられることができない。３２３において，第１装置と第２装置との間の距離が計算される。このステップは，例えば，信号が第１装置から第２装置へ伝送器３０９によって伝送される時，及び受信器３１７が前記信号を第２装置から受信する時に，時間を測定することにより実行される。したがって，伝送時間と受信時間との間の時間差は，第１装置と第２装置との間の物理的距離を決定するのに用いられ得る。

【００４４】

図４（省略）において，認証型距離測定を実行するための通信装置が示される。装置４０１は，受信器４０３及び伝送器４１１を有する。当該装置は，通信バスを介してメモリ４１７に接続されるマイクロプロセッサ４１３を用いてソフトウェアを実行することによって実現され得る，上述のステップを実行する手段を更に有する。当該通信装置は，保護されたコンテンツにアクセスするために，DVD，計算機，CD，CD レコーダ，テレビ及びその他の装置のような装置の内部において配置され得る。

(2)　甲１発明について

甲１発明は，前記第２の３(1)記載のとおりであり，甲１には，次の記載がある。

【０００１】

【発明の属する技術分野】本発明は，自動車などのドアを遠隔から施錠したり解錠したりするのに利用されるキーレス・エントリーシステムに関するものである。

【０００５】

【発明が解決しようとする課題】上記特開平 3－148352 号や特開平 63－40073 号公報に開示された距離式のキーレス・エントリーシステムは，距離に応じて自動的に施錠や解錠を実行したり，あるいは，施錠や解錠の待ち状態への移行が行われるため，リモコン式に比較して便利であるという利点がある。しかし，特開平 3－148352 号公報の距離検出式のキーレス・エントリーシステムでは，携帯型の送信器から送信されて車両側で受信されたマイクロ波の伝播時間から距離を測定する構成であるから，ＧＰＳシステムなどと同様に，携帯型の送信器からは送信時刻を付加した電波を放射し，受信側ではこの電波の受信時刻を測定して送信時刻と受信時刻の差から電波の伝播時間を測定することが必要になる。

【０００６】しかしながら，そのようなキーレス・エントリーシステムでは，ＧＰＳにおける電波の伝播時間が数十ｍｓの程度であるのに対して，数十ｎsec 程度と桁違いに短くなる。このため，送信器と受信器との間で数十ｎsec 程度の極めて高精度で時間合わせ（同期）を行わなければならず，送受双方に極めて高精度の時計が必要になり，実現が困難になる。

【０００７】また，特開平 63－40073 号公報に開示された距離式のキーレス・エントリーシステムでは，電波の受信強度に基づいて距離を検出している。しかし，電波の強度は，駐車場などに生じる定在波やフェーディングなどの影響で空間的にも時間的にも大きく変動するため，受信電波の強度に基づいて距離を検出するのは困難になるという問題がある。従って，本発明の一つの目的は，電波の伝播時間の測定が容易なキーレス・エントリーシステムを提供することにある。

【０００８】また，特開平 2－164988 号公報などに開示されたリモコン式のキーレス・エント

リーシステムを，上述の距離検出式のキーレス・エントリーシステムに変更しようとすれば，解錠や施錠を行う制御部までをも含めてシステムの構成要素一式を交換しなければならず，費用がかさむという問題がある。従って，本発明の他の目的は，リモコン式のキーレス・エントリーシステムを安価な費用で距離検出式のキーレス・エントリーシステムに変更可能な新たなキーレス・エントリーシステムを提供することにある。

【０００９】

【課題を解決するための手段】本発明のキーレス・エントリーシステムは，応答信号の送信を要求する呼出し信号を空中に送信し，その後に空中から受信した応答信号の正当性をこれに含まれる識別子に基づき検査し，前記呼出し信号の送信から前記応答信号の受信までの時間差に基づきこの応答信号の送信元との距離を検出し，応答信号が正当の場合には前記検出した距離が所定値未満であるか否かに応じて車両などのドアの解錠と施錠とを実行するドア側無線装置と，前記呼出し信号を受信して前記識別子を含む応答信号を空中に送信する携帯型無線装置とを備えている。このように，呼出し信号と応答信号の電波の伝播所要時間をドア側無線装置内の時計のみを使用して計測した送信から受信までの時間差に基づき検出できるので，実用的な時計の安定度の範囲内で距離の測定が可能になる。

【００１０】

【発明の実施の態様】本発明の実施の態様によれば，上記ドア側無線装置は，呼出し信号の送信の後に受信した応答信号が正当の場合には検出した距離が所定値未満であるか否かに応じて車両などのドアの解錠と施錠とに関する指令で変調した電波，光線又は超音波を送出するというリモコン式の施解錠部に対する中継ないしは変換機能を果たす。

【００１１】

【実施例】図１（省略）は，本発明の一実施例の車両のドアを施解錠の対象とするキーレス・エントリーシステムの構成を示すブロック図であり，１０は車両内の適宜な箇所に設置された施解錠実行部，２０は車両のイグニッションキー上に搭載された携帯型無線装置，３０は車両内の適宜な箇所に設置された車両側無線装置である。

【００１２】施解錠実行部１０は，ＣＰＵ１１，受光部１２及びアクチュエータ１３を備えて

いる。携帯型無線装置２０は，ＣＰＵ２１，送受信部２２，アンテナ２３及び電池２４を備えている。車両側無線装置３０は，ＣＰＵ３１，送受信部３２，アンテナ３３及び送光部３４を備えている。車両側無線装置３０は，施解錠部１０を含むリモコン式のキーレス・エントリーシステムと，携帯型無線装置２０を含む距離式キーレス・エントリーシステムとの中継ないしは変換の機能を果たす。

【００１７】すなわち，ＣＰＵ３１は，上記内蔵のカウンタのカウント値に基づき，まず，呼出し信号を送信してから応答信号を受信するまでの所要時間Ｔを算定する。次に，ＣＰＵ３１は，この所要時間Ｔから予め定められている自装置内の応答遅延時間δτ１と，携帯型無線装置２０内における応答遅延時間δτ２とを引き算すした（原文ママ）のち半分にすることにより，呼出し信号と応答信号の伝播所要時間ｔを算定し，これを電波の伝播速度Ｃで除算（原文ママ）することにより，距離ＲをＲ＝（Ｔ－δτ１－δτ２）／（２Ｃ）（原文ママ）と算定する。

【００１８】ＣＰＵ３１は，算定した携帯型無線装置２０までの距離Ｒが解錠最遠距離として定められた所定値Ｒｏ未満であるか否かを判定し（ステップＳ９），そうであれば，フラグＦがドアの施錠状態を示す「１」であるか否かを判定する。ＣＰＵ３１は，距離Ｒが解錠最遠距離Ｒｏ未満でしかもドアが施錠状態にあれば，フラグＦを「１」から「０」に反転させ（ステップＳ１１），引き続き，送光部３４からドアの解錠指令を送出させる。

【００１９】送光部３４から送出された解錠指令による変調を受けた光線は，施解錠実行部１０内の受光部１２に受光される。ＣＰＵ１１は，受光信号に含まれる解錠指令を解読しアクチュエータ１３を起動する。起動されたアクチュエータ１３はドアの解錠を行う。

【００２０】ＣＰＵ３１は，ステップＳ８で算定した距離Ｒが施錠最近距離として定められた所定値Ｒｏ以上であることをステップＳ９で判定すると，今度は，この算定済みの距離Ｒが施錠最近距離（Ｒｏ＋ΔＲ）よりも大きいか否かを判定する（ステップＳ１３）。ＣＰＵ３１は，距離Ｒが施錠最近距離（Ｒｏ＋ΔＲ）よりも大きければ，フラグＦがドアの解錠状態を示す「０」であるか否かを判定する（ステップＳ１４）。ＣＰＵ３１は，距離Ｒが（Ｒｏ＋ΔＲ）よりも大きくしかもドアが解錠状態にあれば，フラグＦを「１」から「０」に反転させ（原文ママ）（ステップＳ１５），引き続き，送光部３４からドアの解錠（原文ママ）指令を送出させる。

【００２１】送光部３４から送出された施錠指令による変調を受けた光線は，施解錠実行部１０内の受光部１２に受光される。ＣＰＵ１１は，受光信号に含まれる施錠指令を解読し，アクチュエータ１３を起動する。起動されたアクチュエータ１３はドアの施錠を行う。

【００２２】なお，ＣＰＵ３１は，ステップＳ１３において，Ｒｏ≦Ｒ≦（Ｒｏ＋ΔＲ）であると判定すると，ドアが施錠状態にあるか解錠状態にあるかに関係なく，何らの処理を行うことなくステップＳ２に復帰することにより，施錠や解錠に関するドアの状態を現状のものに保つ。このように，距離の測定誤差などによりドアの状態が施錠状態と解錠状態との間を頻繁に交番するバタツキを防止するために，ΔＲのヒステリシスが賦与されている。

【００２３】また，ＣＰＵ３１は，算定距離Ｒが解錠最遠距離Ｒｏ未満の場合であってもドアが既に解錠状態（Ｆ＝０）にあれば，ドアを改めて解錠状態にすることなく，ステップＳ１０からステップＳ２に復帰する。同様に，ＣＰＵ３１は，算定距離Ｒが解錠最近距離（Ｒｏ＋ΔＲ）よりも大きい場合であってもドアが既に施錠状態（Ｆ＝１）にあれば，ドアを改めて施錠状態にすることなく，ステップＳ１４からステップＳ２に復帰する。

【００２５】図３（省略）は，本発明の他の実施例のキーレス・エントリーシステムの構成を示すブロック図であり，２０はイグニッションキー上に搭載された携帯型無線装置，４０は車両内の適宜な箇所に設置された車両側無線装置である。携帯型無線装置２０は，図１に関して既に説明した実施例で使用した携帯型無線装置と同一の装置であり，このため同一の参照符号が付されている。この実施例の車両側無線装置４０は，ＣＰＵ４１，送受信部４２，アンテナ４３及びアクチュエータ４４を備えている。

【００２６】本実施例のキーレス・エントリーシステムと，図１に示したキーレス・エントリーシステムとの相違点は，車両側無線装置４０がアクチュエータ４４を備えており，このアクチュエータ４４が車両のドアの施錠や解錠を直接実行する点である。従って，車両側無線装置４０内のＣＰＵ４１の動作は，図２のフローチャートを参照しながら説明したものとほぼ同一であり，異なる点は，ステップＳ１２とＳ１６のそれぞれにおいて，解錠指令や施錠指令を別途設置されていた施解錠部１０に光線で送出させる代わりに，直接アクチュエータ４４に実行させるという点である。・・・

【００２７】本出願人が先に出願した特願平７－231024 号に開示されているように，車両の窃盗を企てる者が，車両側無線装置と携帯型無線装置との間の通信を傍受して記録することなどによって識別子を盗み出したり，可能性のある多数の識別子を高速で自動的に発生させて多数回にわたって応答信号を反復して送信するなどの問題が考えられる。

【００２８】上記の問題点を解決するために，必要に応じて，上記先願のキーレス・エントリーシステムに開示したと同様，以下の方法が採用される。すなわち，車両側無線装置と携帯型無線装置の双方に予め同一の関数Ｆ（ｘ）を登録させておく。車両側無線装置は，呼出し信号を送信しようとするたびに乱数ｚを発生させ，この乱数ｚを呼出し信号に含ませて送出すると共に，この乱数を登録中の関数Ｆ（ｘ）に代入することにより関数値Ｆ（ｚ）を算定しておく。

【００２９】携帯型無線装置は，受信した呼出し信号から乱数ｚを抽出し，これを登録中の関数Ｆ（ｘ）に代入することにより，関数値Ｆ（ｚ）を生成し，これを応答信号に含ませて送信する。車両側無線装置は，受信した応答信号から関数値Ｆ（ｚ）を抽出し，これを予め算定しておいた関数値Ｆ（ｚ）と照合し，照合一致の場合には応答信号が正当であると判定する。勿論，この乱数の関数値に加えて，装置固有の識別子の照合を行う構成とすることもできる。

【００３２】さらに，施錠／解錠対象のドアが車両のドアである場合について，本発明の一実施例のキーレス・エントリーシステムを説明した。しかしながら，施解錠対象のドアは車両のドアに限らず，倉庫や家屋のドアなど他の適宜なものであってもよい。

【００３３】

【発明の効果】以上詳細に説明したように，本発明のキーレス・エントリーシステムは，車両側から呼出し信号を送信し，これに対する応答信号を受信し，この間の所要時間から電波の伝播時間と携帯型無線装置までの距離を測定する構成であるから，距離の測定が容易に実現できる。例えば，上記実施例で解錠最遠距離Ｒｏを 10 メートルに設定した場合，電波の伝播所要時間は往復で 66 nsec であるから，周波数が 100 MHz 程度のクロック信号(周期 10 nsec) を使用する簡便なカウンタを用いて距離を容易に測定できる。この際，解錠と施錠に関する距離に対してヒステリシスを設定することなどにより，数 nsec 程度の誤差は十分に許容できる。

【００３４】また，本発明の一つによれば，図１に示したように，リモコン式と距離検出式と

の変換を行う変換ないしは中継機能を備えた車両側無線装置を車両内などに設置する構成であるから，既に車両に設置してあるリモコン式の施解錠実行部をそのまま利用する形式で，距離検出式のキーレス・エントリーシステムに変更できるという効果が奏される。

２　取消事由２（進歩性の存在）について

事案に鑑み，まず取消事由２から判断する。

⑴　一致点の認定の誤りについて

ア　審決は，「引用発明において，『車両側無線装置が，携帯型無線装置からの応答信号に基づいて，ドアの解錠指令の送出を決定する』とは，“車両側無線装置が，携帯型無線装置からの応答信号に基づいて，所定のサービスの実行を許可する”ことに他ならない」（７頁２１～２４行）として，「第１信号送信装置が，第２信号送信装置に対して『所定のサービス』を実行すべきかを決定する方法」である点，「測定された距離が事前に規定された距離間隔の範囲にある場合に，前記第２信号送信装置への『所定のサービス』の実行を許可」する点を，本願発明と甲１発明の一致点と認定する。

しかしながら，本願発明と甲１発明の一致点として，「所定のサービス」の実行を許可する点を認定するのは，次のとおり，誤りである。

㋐　甲１発明は，「ドアの解錠指令の送出を決定する」ことを構成要素とするものであり，「『所定のサービスの実行を許可』する」ことという抽象化され，上位概念化された動作が甲１発明の構成要素であると評価することはできない。

ａ　甲１には，「本発明は，自動車などのドアを遠隔から施錠したり解錠したりするのに利用されるキーレス・エントリーシステムに関するものである。」（【０００１】），「施解錠対象のドアは車両のドアに限らず，倉庫や家屋のドアなど他の適宜なものであってもよい。」（【００３２】）との記載があり，甲１発明は，車両のドアに限定されないものの，ドアの施解錠に限定されたものであるといえる。また，甲１には，「本発明の他の目的は，リモコン式のキーレス・エントリーシステ

ムを安価な費用で距離検出式のキーレス・エントリーシステムに変更可能な新たなキーレス・エントリーシステムを提供することにある。」（【０００８】），「本発明の実施の態様によれば，上記ドア側無線装置は，呼出し信号の送信の後に受信した応答信号が正当の場合には検出した距離が所定値未満であるか否かに応じて車両などのドアの解錠と施錠とに関する指令で変調した電波，光線又は超音波を送出するというリモコン式の施解錠部に対する中継ないしは変換機能を果たす。」（【００１０】）との記載があるから，甲１発明において，ドアの解錠指令を送出する車両側無線装置は，リモコン式の施解錠部に対する中継又は変換機能を果たすものであって，その動作は，リモコン式のドアの施解錠に特有の処理というべきである。

甲１には，「サービス」という文言自体記載されていない上，ドアの解錠指令の送出がドアの解錠に特有でない処理であって，より一般化された処理であることを示す記載は，存在しない。前記の甲１の【００３２】の記載は，ドアの種類を一般化しているにすぎず，施解錠処理以外の処理を示唆するものではなく，これを根拠に，甲１発明が「所定のサービスの実行を許可する」という動作を構成要素とするものと，上位概念化して評価することは許されない。

ｂ　被告は，前記の「サービス」とは，「サービス要求と，それに対し，何らかの利便を提供する行為の総称」であると主張する。

前記の定義は，その文言上，①第１の主体が，第２の主体に対し，何らかのサービスを要求する行為，②第２の主体が，第１の主体からの何らかのサービスの要求に対し，第１の主体又は第３の主体に対し，何らかの利便を提供する行為という，2 種類の行為を含んでいる。

「サービス」は，「①奉仕，②給仕。接待。③商売で値引きしたり，客の便宜を図ったりすること。④物質的生産過程以外で機能する労働。用益。用務。⑤（競技用語）サーブに同じ。」（広辞苑第６版）と解されているのであって，前記の行為のうち，「第２の主体が，」「第１の主体又は第３の主体に対し，何らかの利便を提供する行為」は，「サービス」と表現され得るが，「第１の主体が，第２の主体に対し，何

らかのサービスを要求する行為」は，「サービス」と表現され得るとは考えられず，「サービス」を，前記の２種類の行為を一個の概念に包括する総称と定義することには，無理がある。

(ｲ) 仮に，被告の主張する「サービス」の定義を前提としても，甲１発明において，車両側無線装置が，携帯型無線装置からの応答信号に基づいて，「ドアの解錠指令の送出を決定」することが，「第２信号送信装置への『所定のサービスの実行を許可』する」ことには該当しない。

甲１発明において，車両側無線装置が行うのは，①ドアの解錠指令の送出を決定し，②ドアの解錠指令を送出して，③これを受光した車両の施解錠実行部をして，車両のドア用キーシリンダーを解錠させることである（甲１）。このうち，①ドアの解錠指令の送出の決定は，車両側無線装置が他の装置に対して行う動作とは評価できない。また，②ドアの解錠指令の送出は，施解錠実行部に対して行われるものであると評価でき，車両側無線装置が携帯型無線装置に対して行う動作とは認められない。さらに，③ドア用キーシリンダーの解錠は，施解錠実行部を介してドア用キーシリンダーに対して行われるものであると評価でき，いずれも，車両側無線装置（本願発明の第１通信装置）が携帯型無線装置（本願発明の第２通信装置）に対して行う動作とは認められない。

そうすると，これらの動作が「サービス要求」であるにしろ，「それに対し，何らかの利便を提供する行為」であるにしろ，「第２信号送信装置への」行為には該当しない。

以上によれば，甲１発明において，車両側無線装置が，携帯型無線装置からの応答信号に基づいて，「ドアの解錠指令の送出を決定」することをもって，「第２信号送信装置への」「所定のサービスの実行」を許可するものとは評価できない。

イ(ｱ) 被告は，「本願発明と甲１発明とは，第１通信装置が認証により第２通信装置によるサービスの実行を許可する点において一致している。」と主張する。

審決は，「第１信号送信装置が，第２信号送信装置に対して所定のサービスを実行

すべきかを決定する方法」であって，一定の場合に，「前記第２信号送信装置への所定のサービスの実行を許可」する点を，本願発明と甲１発明の一致点と認定しているのであって，被告のいう「第２通信装置によるサービスの実行」の許可と，審決のいう「第２信号送信装置へのサービスの実行」の許可では，その文言上，前者は，第２通信装置が他の装置又は他者に対してサービスを実行することを第１通信装置が許可すること，後者は，第１信号送信装置が第２信号送信装置に対するサービスを実行することを許可すること，を意味すると解される点で違いがあるから，両者は一致するものではない。

しかも，前記のとおり，車両側無線装置（本願発明の第１通信装置）に対する信号を送信後特段の動作を行わない携帯型無線装置（本願発明の第２通信装置）が，所定のサービスを実行したと評価することはできない。

したがって，被告の前記主張は，採用できない。

(ｲ)ａ　被告は，審決において，相違点１とされている，本願発明においては，「所定のサービスを実行すべきかを決定する」ことが，「第１通信装置に記憶されたマルチメディアデータへの，第２通信装置によるアクセスの許可の決定」である点につき，この「アクセス」は，「アクセス要求と，それに対し，何らかの利便を与える行為の総称」であるとして，「第２通信装置による」「アクセス」とは，第２通信装置を用いた「アクセス」を総称したものであって，「第２通信装置」への転送や複製を介在したアクセスには限定されておらず，「第２通信装置」による「アクセス」は，「第１通信装置」の側で実行される処理であってもかまわないから，甲１発明が「第１通信装置」の側で実行される処理であることは，本願発明との相違点にならない旨主張する。

ところで，「アクセス」とは，「①情報に対する操作の総称。特にコンピュータで，記憶装置や周辺装置にデータの読み出しや書き込みをすること。②交通手段の連絡」（広辞苑第６版）と解されているのであって，情報を保管する記憶媒体を有する装置に対し，情報を送って記憶させることや，その記憶媒体に保管された情報の送信

を受けることを意味するものと解される。

そして，本願発明における「アクセス」の主体と客体は，本願明細書に「第１通信装置に記憶されたデータが第２通信装置によってアクセスされるべきかを決定」する旨の記載がある（【００２４】，【００２５】）ことから，主体が第２通信装置，客体が「第１通信装置に記憶された」マルチメディア「データ」であると解される。第２通信装置が，第１通信装置に対し，第１通信装置が記憶するマルチメディアデータの読み出しを命令し，第１通信装置がこれに応じて第２通信装置に前記データを送信するという一連の動作において，前記データを記憶している装置である第１通信装置が「アクセス」の客体，読み出しを求める側である第２通信装置が「アクセス」の主体とされるのは，前記の「アクセス」の文言上の解釈に沿う用法である。そうすると，第２通信装置が主体であり，第１通信装置が客体である「第２通信装置による」「アクセス」を，第２通信装置以外の主体が存在することを前提とする「第２通信装置を用いた」「アクセス」を総称したものと読み替えることはできないし，「第１通信装置」の側のみで行われる処理を，「アクセス」と呼ぶことも不適当である。

また，本願明細書（甲６）には，「デジタル・データの形のコンテンツを保護する一つの手段は，コンテンツが，受信装置が，準拠した装置であるとして認証された場合と，コンテンツの使用者が，このコンテンツを他の装置に転送（移動，複製）する権利を有する場合と，にのみ転送されるということを保証することである。」（【０００５】），「隣人を訪ねている使用者が，彼が所有する映画を隣人の大きなテレビ・スクリーンで鑑賞することは，可能であるべきである。・・・この映画のライセンス保持者（又はこのライセンス保持者が所有する装置）が，このテレビ・スクリーンの近くにあると証明され得る場合，容認され得る。」（【０００８】）との記載があり，これを前提に，前記のとおり，「第１通信装置に記憶されたデータが第２通信装置によってアクセスされるべきかを決定」する旨の記載がある（【００２４】，【００２５】）のであるから，ここでいう「アクセス」は，「映画のライセンス保持

者が所有する装置」から「テレビ・スクリーン」への映画の送信を意味しているとしか解釈できない。そして，本願発明にいう「アクセス」が，第１通信装置から第２通信装置へのコンテンツの送信に限定されず，第１通信装置が第２通信装置に向けて実行するものではない処理も含む，より一般化された概念であることを示す記載は，本願明細書中に存在しない。

以上によれば，「アクセス」の解釈についての被告の前記主張を採用することはできず，これを前提とする，「第２通信装置」による「アクセス」は，「第１通信装置」の側で実行される処理であってもかまわないから，甲１発明が「第１通信装置」の側で実行される処理であることは，本願発明との相違点にならない旨の主張も，採用できない。

ｂ(a)　被告は，この点に関し，ＤＶＤに記録された映画を隣人宅のテレビで再生する場合，ＤＶＤ再生装置と認証物件との間で距離測定がされるとき，認証物件が第２通信装置であるから，「アクセス」を「第２通信装置」への転送や複製を介在したアクセスの趣旨と解すると，これは，本願発明の実施態様に含まれないが，これをインターネットからＰＣ等に記録された映画を隣人宅のテレビで再生するときと技術的に区別する理由は見当たらない旨主張する。

(b)　被告の前記主張を検討するに，本願明細書(甲６)には，「隣人を訪ねている使用者が，彼が所有する映画を隣人の大きなテレビ・スクリーンで鑑賞することは，可能であるべきである。一般的にコンテンツ所有者は，このことを許可しないであろうが，この映画のライセンス保持者（又はこのライセンス保持者が所有する装置）が，このテレビ・スクリーンの近くにあると証明され得る場合，容認され得る。」（【０００８】），「本発明は，第１通信装置に記憶されたデータが第２通信装置によってアクセスされるべきかを決定する方法に関し，当該方法は，第１通信装置と第２通信装置との間の距離測定を実施し，前記測定された距離が既定の距離区間の範囲内であるかを確認するステップを有し，ここでは，距離測定は，上記に従う認証型距離測定である。」（【００２４】），「特定の実施例において，第１装置

に記憶されたデータが第２装置によってアクセスされるべきであると決定される場合，第１装置に記憶されたデータは，第２装置に送信される。」（【００２５】），「本発明は，第１通信装置に記憶されたデータが第２通信装置によってアクセスされるべきかを決定する方法に関し，当該方法は，第３通信装置と第２通信装置との間のおける距離測定を実施し，前記測定された距離が既定の距離区間の範囲内であるかを確認するステップを有し，ここでは，距離測定は，上記に従う認証型距離測定である。この実施例において，距離は，第２通信装置とデータが記憶される第１通信装置との間の距離は測定されない。代わりに，距離は，第３通信装置がコンテンツの所有者の私的なものであり得るような，第３通信装置と第２通信装置との間において測定される。」（【００２６】），「データが記憶される計算機とその他の装置の間の距離が測定される必要のないような特定の例において，当該その他の装置は，第３装置，すなわち事前規定の距離の範囲内にあるコンテンツの所有者の私的なものである装置でもあり得る。（【００３４】）との記載がある。

また，甲６には，【請求項１０】として，「第１通信装置に記憶されたデータが第２通信装置によってアクセスされるべきかを決定する方法であって，当該方法は，第３通信装置と前記第２通信との間の距離測定を実行し，当該測定された距離が事前規定された距離間隔の範囲内にあるかを確認するステップを有し，前記距離測定が請求項１に記載の認証型距離測定である方法。」との記載があり，前記の第３通信装置についての記載は，これを前提にしたものであると解される。

以上によれば，本願明細書には，第１通信装置に記憶されたデータが第２通信装置によってアクセスされるべきであるかを決定する方法として，①第１通信装置と第２通信装置との間の距離測定が行われ，その結果が所定の距離の範囲内であれば，第１通信装置から第２通信装置へとデータが送信される場合，及び，②第１通信装置と第２通信装置との間の距離測定は行われず，第３通信装置と，第２通信装置との間の距離測定が行われ，その結果が所定の距離の範囲内であれば，第１通信装置から第２通信装置へとデータが送信される場合があることが記載されているといえ

る。

(c) しかしながら，前記の本願明細書の記載は，出願の当初の請求項を前提にしたものであり，本願補正後の請求項は，いずれも，第１通信装置及び第２通信装置の存在のみを前提としており，第３通信装置が存在し，第３通信装置と第２通信装置との間の距離測定が行われることを前提としていない（乙２）。

したがって，本願補正後の請求項は，前記①の場合のみを前提とするものであり，前記②の場合を前提とするものではない。

被告の前記主張は，「ＤＶＤに記録された映画を隣人宅のテレビで再生する場合」に，ＤＶＤ再生装置が第１通信装置であることを前提としているところ，「ＤＶＤに記録された映画を隣人宅のテレビで再生する場合」，ＤＶＤ再生装置が第１通信装置であるならば，テレビが第２通信装置である。この場合において，ＤＶＤ再生装置及びテレビのほかに，認証物件が存在すると想定すると，本願補正後の請求項の記載と合致しなくなる。

したがって，被告の前記主張は，前提を欠き，採用できない。

(ｳ) 被告は，甲１発明は，解錠以外のサービスにおいても用いることが可能な内容を示していると主張するが，前記ア(ｱ)ａ及びｂのとおりであって，甲１発明は，飽くまで，キーレス・エントリーシステムに関する発明であり，そのような抽象化され，上位概念化された内容の発明が記載されていると評価することは許されず，被告の前記主張は，採用できない。

ウ 以上のとおり，審決における一致点の認定には誤りがあり，取消事由２にはその限度で理由があるが，上記一致点の誤認に関連する相違点１についての判断も，以下，念のため検討することとする。

(2) 相違点１の判断の誤りについて

ア 審決は，「所定のサービスを実行すべきかを決定する」ことが，本願発明においては，第１通信装置に記憶されたマルチメディアデータへの，第２通信装置によるアクセスの許可の決定であるのに対し，甲１発明においては，車両側無線装

置が搭載された車のドアの解錠の決定であるとして，①距離判定の処理と，ドアの解錠指令の送出を決定する処理との間に一体不可分の関係は存在しておらず，距離判定の処理の結果として許可される処理として，ドアの解錠指令の送出以外を設定することは，当業者が適宜なし得る事項である，②２つの装置が，所定の距離の範囲内に存在するか否かを判定し，存在する場合に，所定のプログラム等へのアクセスを許可するようなことは，周知技術である（甲３，４）から，甲１発明において，距離判定の結果に基づき，車両のドアの解錠を行うことに換えて，車両内の記憶手段に記憶されているマルチメディアデータ等の資源へのアクセスを携帯型無線装置に許可するといった構成を採用することは，当業者が適宜なし得る事項であるから，相違点１は格別のものではないと判断する。

しかしながら，前記⑴に判示した結果によれば，距離判定の処理に基づいて行われる動作は，本願発明においては，マルチメディアデータが，第１通信装置から第２通信装置に送信されるのに対し，甲１発明においては，ドアの解錠指令が，車両側無線装置から，携帯型無線装置ではなく，車両にある施解錠実行部に対して送出される（甲１）点が，本願発明と甲１発明の相違点として認定されるべきであるから，この点の容易想到性について，以下，判断する。

イ㈠ａ　甲３には，次の記載がある。

【０００１】

【発明の属する技術分野】この発明は，例えばクレジットカードなどのような所有者の電子化された情報を取り引きする電子情報担体の不正使用防止システム及び不正使用防止方法に関するものである。

【００１０】

【発明が解決しようとする課題】従来の電子情報担体の不正使用防止システムは以上のように構成されているので，端末位置検出手段１２０が測位する端末装置１００の現在位置が，予め登録しておいた取引許可エリア内にあるか否かに基づいてその使用の正当性をサーバ装置２０

０が判定することから，クレジットカードなどのように世界中の地域（広範囲な領域）においても使用される可能性のある電子情報担体に適用することが困難であるという課題があった。

【００１１】上記課題を具体的に説明すると，クレジットカードなどのような電子情報担体を使用するための端末装置１００は，広範囲な地域に存在するのが一般的である。このような端末装置１００の全てに対して取引許可エリアを設定するのは，かなりの労力を要する作業である。また，複数の端末装置１００が近接した位置にあり，複数の取引許可エリアが重なってしまうような場合では，端末装置１００の正確な位置確認を行うことが困難である。これにより，クレジットカードなどのような電子情報担体に対して上記従来のシステムを適用すると，認証の信頼性が低下してしまう。

【００１２】この発明は上記のような課題を解決するためになされたもので，自己の位置を測定する手段を設けた電子情報担体と，この電子情報担体の識別情報で特定される携帯通信端末との位置関係情報から電子情報担体の使用が正当であるか否かを判定することで，クレジットカードなどのような電子情報担体に対しても有効に不正使用を防ぐことができる電子情報担体の不正使用防止システム及び不正使用防止方法を得ることを目的とする。

【００１７】この発明に係る電子情報担体の不正使用防止システムは，位置関係算出手段が電子情報担体及び携帯通信端末から取得した各現在位置の測位情報を用いて，両者の位置関係情報として現在の２点間距離を算出し，使用許可判定手段が，電子情報担体及び携帯通信端末の各現在位置の測位情報から電子情報担体の使用を許可すべき２点間距離を算出し，これと位置関係算出手段が算出した現在の２点間距離とを比較して，電子情報担体の使用許可を判定するものである。

【００２８】端末装置５はカード１のカード番号とカード１の現在位置の測位情報とを取得すると，通信装置１３が通信回線９を介してこれらの情報をカード会社のセンターに設置されているホストコンピュータ８に送信する（ステップＳＴ３）。・・・

【００２９】ホストコンピュータ８内の通信装置１２は，送信されてきたカード番号を受信すると，直ちに制御装置１１に送信する。制御装置１１は上記カード番号からデータベース１０を検索し，このカード番号で一意に対応する携帯通信端末６の電話番号を取得する（ステップ

ＳＴ４）。

【００３０】制御装置１１は，ステップＳＴ４にて携帯通信端末６の電話番号を取得すると，通信装置１２を用いてその電話番号をコールし，該携帯通信端末６に対して接続要求を行う（ステップＳＴ５）。

【００３２】ステップＳＴ７において，通信装置１２が使用禁止要求を受信しなかった場合，制御装置１１が通信装置１２を用いて携帯通信端末６の現在位置の測位情報を送信するよう要求する。これにより，携帯通信端末６は，自己のＧＰＳ機能を使用して現在位置を測定し，得られた測位情報をホストコンピュータ８に送信する（ステップＳＴ８）。・・・

【００３３】このあと，ホストコンピュータ８の位置関係算出手段１１ａは，ステップＳＴ３にて取得したカード１の現在位置の測位情報と，ステップＳＴ８にて取得した携帯通信端末６の現在位置の測位情報とから，現在の位置関係情報としてカード１と携帯通信端末６との２点間距離を算出する（ステップＳＴ９，位置関係算出ステップ)。

【００３４】使用許可判定手段１１ｂは，ステップＳＴ３，８にて取得したカード１及び携帯通信端末６の現在位置の測位情報からカード１や携帯通信端末６の使用場所から誤差の大きさなどを考慮して正当な使用範囲（カード１の使用を許可すべき２点間距離）を決定し，位置関係算出手段１１ａが算出した２点間距離がその範囲以内かどうかにより正当な使用か否かを判別する（ステップＳＴ９，使用許可判定ステップ)。上記正当な使用範囲としては，例えば２点間距離がおよそ１m以内であるものとする。

【００３５】使用許可判定手段１１ｂは，位置関係算出手段１１ａが算出した２点間距離からカード１の使用が正当であると判定した場合，通信装置１２を用いて通信回線９を介してカード１の使用を許可する旨の信号を端末装置５に送信する。これによって，カード１の使用が可能になる（ステップＳＴ１０，使用許可判定ステップ)。

【００４０】以上のように，この実施の形態１によれば，自己の位置を測定する手段を有するカード１から現在位置の測位情報とその識別情報であるカード番号とを取得し，このカード番号で特定されて，自己の位置を測定する手段を有する携帯通信端末６から現在位置の測位情報を取得して，各測位情報から両者の現在の位置関係情報を算出し，さらに，各測位情報から電

子情報担体の使用を許可すべき位置関係情報を算出し，これと現在の両者の位置関係情報とを比較して電子情報担体の使用許可を判定するので，暗証番号などの重要情報を通信回線を通して授受することによる危険性をできるだけ最小限に押さえることができるとともに，不正な利用者による「成りすまし」を排除することができる。また，Ｗｅｂにおける電子商取引きなどにおいて，今後，益々利用されることが多くなるカード決済の安全性を強化することができる。

ｂ　甲４及び甲４の２には，次の記載がある（なお，甲４の２は，甲４の訳文であり，【】書きの番号は，甲４の２の記載部分を示す。）。

【０００１】

【発明の属する技術分野】

本発明は，多端末環境にあるコンピュータ端末装置を経由したコンピュータシステムへの無許可アクセスを防止する方法に関する。

【０００４】

この問題に対する改良された解決法は，ユーザ（トークン）がコンピュータサイトを離れたかどうかを自動的に検出し，総ての，または選ばれたコンピュータ資源へのどのようなアクセスも自動的に不能にする近接センサに基づいている。近接センサは，ＲＦ，ＩＲ，音，超音波などの無接触の通信技術を使用する。近接センサを使用する従来技術のシステムはユーザにとっては便利であるが，特に，それらのシステムは複製することができるから，無許可アクセスに対して高度なセキュリティを提供しないので，さらにシステムがユーザ（トークン）と所定のワークステーションとを対にし適応性が低いために，深刻な欠点がある。・・・

【０００５】

しかし，従来技術は，現在の作業環境にある実際的な問題を解決することができなかった。この問題は，作業環境に複数のユーザが存在し，そのユーザの全部または一部の者が異なるアクセス権を持つ可能性があり，さらにユーザがお互いに影響を及ぼす可能性があることから生じている。そのような状況を図１（省略）に模式図で示す。いくつかの分離したワークステー

ションを含む標準的な作業域を図に示す。「トークン」（・・・）で示される複数のユーザは，その環境内を移動する。この例示的な図で，いくつかの異なる状況が見られる。すなわち，ａ）作業域に入ったり出たりするユーザ，ｂ）単一ユーザの存在を検出する２台のワークステーション，ｃ）１つのワークステーションから他のワークステーションに移動する一人のユーザ，及び，ｄ）１つのワークステーションのそばにいる二人のユーザである。毎日の生活でよくあるその他のもっと複雑な状況がもちろん考えられるが，図１の例示的な例から，マルチユーザ環境の状況は，隔離された単一ユーザ環境と実質的に異なり，はるかに複雑であることが理解できる。

【００１１】

「存在信号」は，正当なトークンがワークステーションの近くにまだいること，すなわち，システムのセットアップで許された最大距離内に未だいることをシステムに表示する信号を示す意図である。

【００２０】

また，本発明は，複数のユーザが１つまたは複数のワークステーションへのアクセス権を独立に得る必要があるマルチユーザシステムにあるワークステーションへのユーザによる連続したアクセスであって，ユーザがアクセス権を得たワークステーションから所定の最大距離にユーザがいることを条件とする連続したアクセスを提供するシステムであって，

Ａ　データ受取り手段及びデータ伝送手段をそれぞれ備える複数のアクセストークンと，

Ｂ　データ列を含む所定の信号を生成し，かつ，前記データ伝送手段を経由して予め設定された時間間隔で前記所定の信号を伝送する手段と，

Ｃ　各トークンに備えられる各トークンに固有の個人識別データと，

Ｄ　前記ワークステーションから予め設定された最大距離内にあるトークンによって伝送された信号を受け取るために，各ワークステーションに結合されたデータ伝送感知手段と，

Ｅ　トークンの識別情報と，１つまたは複数のワークステーションへのトークンの近接とを表すデータを受け取り格納するために，前記データ伝送感知手段に接続されたマッピング手段と，

Ｆ　トークン識別データと特定のワークステーションに固有で特徴的な同期信号とを含む信号

を伝送するために，各ワークステーションに結合されたデータ伝送手段と，

Ｇ　前記トークン識別データをも含む信号に含まれた同期信号のみを格納するために，各トークンに設けられた論理手段と，

Ｈ　前記トークンが受け取った上記ステップ（Ｆ）の条件を満たす信号ごとに，前記特定のワークステーションの同期信号により変調された前記トークン識別番号からなる存在信号を前記トークンから伝送する手段と，

Ｉ　前記同期信号が参照するワークステーションの前記データ伝送感知手段により前記存在信号が受け取られたときに，任意にパスワードまたはＰＩＮをさらに入力することにより，前記ワークステーションへのユーザのアクセスを可能にする手段と，

Ｊ　前記ワークステーションにより前記存在信号が受け取られることを周期的に検査する手段と，

Ｋ　所定の期間の後に前記存在信号が受け取られない場合は，前記ワークステーション及び／またはその選ばれた資源へのアクセスを禁ずる手段と，

を備えているシステムに向けられる。

(ｲ)ａ　前記(ｱ)ａによれば，甲３には，電子情報担体の不正使用防止システムとして（【０００１】），電子情報担体（カード）及び携帯通信端末の２点間距離を算出し，電子情報担体（カード）の使用を許可すべき２点間距離と比較して，電子情報担体（カード）の使用許可を判定するものが記載されているといえる(【００１７】)。

前記システムにおいては，端末装置５は，カード１のカード番号とカード１の現在位置の測位情報とを取得すると，通信装置１３が通信回線９を介してこれらの情報をカード会社のセンターに設置されているホストコンピュータ８に送信し（【００２８】），ホストコンピュータ８内の制御装置１１は，前記カード番号からデータベース１０を検索し，このカード番号で一意に対応する携帯通信端末６の電話番号を取得し（【００２９】），制御装置１１は，通信装置１２を用いてその電話番号をコ

ールし，該携帯通信端末６に対して接続要求を行い（【００３０】），制御装置１１が通信装置１２を用いて携帯通信端末６の現在位置の測位情報を送信するよう要求し，携帯通信端末６は，自己のＧＰＳ機能を使用して現在位置を測定し，得られた測位情報をホストコンピュータ８に送信し（【００３２】），ホストコンピュータ８の位置関係算出手段１１ａは，カード１の現在位置の測位情報と，携帯通信端末６の現在位置の測位情報とから，カード１と携帯通信端末６との２点間距離を算出し（【００３３】），ホストコンピュータ８の使用許可判定手段１１ｂは，誤差の大きさなどを考慮して正当な使用範囲を決定し，位置関係算出手段１１ａが算出した２点間距離がその範囲以内かどうかにより正当な使用か否かを判別し（【００３４】），使用許可判定手段１１ｂは，２点間距離からカード１の使用が正当であると判定した場合，通信装置１２を用いてカード１の使用を許可する旨の信号を端末装置５に送信し，これによって，カード１の使用が可能になる（【００３５】）。

ｂ　前記(ｱ)ｂによれば，甲４には，多端末環境にあるコンピュータ端末装置を経由したコンピュータシステムへの無許可アクセスを防止する方法として（【０００１】），トークンを用いてワークステーションへのユーザのアクセスの可否を判断することが記載されているといえる（【００２０】。トークンの位置は，ユーザの位置と同一視されるものである（【０００４】，【０００５】）。甲４には，マルチユーザシステムにおけるワークステーションに対し，アクセス権を得たユーザに，連続したアクセスを提供するために，ユーザ（トークン）がワークステーションから所定の距離以内に居続けることを要するシステムとして，各ワークステーションから，トークン識別データと当該ワークステーションに固有で特徴的な同期信号とを含む信号が送信され，当該信号を受信したトークンは，前記ワークステーションの同期信号により変調された前記トークン識別番号からなる存在信号を送信し，前記存在信号は，正当なトークンが前記ワークステーションの近くにまだ居ることをシステムに示す信号であって，前記ワークステーションのデータ伝送感知手段が前記存在信号を受信したかを周期的に検査し，前記同期信号が参照するワークステー

ションのデータ伝送感知手段により前記存在信号が受け取られたときに，前記ワークステーションへのユーザのアクセスを可能にし，所定の期間の後に前記存在信号が受け取られない場合は，前記ワークステーション又はそのワークステーションの資源へのアクセスを禁ずるものであり，前記データ伝送感知手段は，前記ワークステーションからあらかじめ設定された最大距離内にあるトークンによって伝送された信号を受け取るためのものである（【００２０】）。

(ｳ) a　前記(ｲ) a によれば，甲３には，カードと携帯通信端末の間の距離を測定し，その距離が所定の範囲内の場合に，ホストコンピュータが，カードの使用を許可することが記載されているといえ，カードの使用が許可された場合に，カードに記憶されているマルチメディアデータを携帯通信端末に送信したり，携帯通信端末に記憶されているマルチメディアデータをカードに送信することは，記載されていない。

b　前記(ｲ) b によれば，甲４には，トークンが発する信号をワークステーションが受信できる場合に，トークンがワークステーションのデータ伝送感知手段で受信できる距離の範囲内にあるとして，ユーザ（トークン）にワークステーションへのアクセスを許可することが記載されているといえ，トークンに記憶されているマルチメディアデータをワークステーションに送信したり，ワークステーションに記憶されているマルチメディアデータをトークンに送信することは，記載されていない。

c　前記 a 及び b によれば，コンピュータシステムの不正使用防止の技術分野において，装置Ａの記憶媒体に記憶されている情報を，特定の者に利用させる場合につき，当該特定の者が装置Ｂを携行することを前提に，装置Ａと装置Ｂとの間の距離測定を行い，その距離が所定の範囲内であるときに限り，装置Ｂの所持者に当該情報を利用させることは，本願優先日には周知技術であったと認められる。

ウ(ｱ)　甲１発明は，前記(1)のとおり，車両側無線装置と携帯型無線装置との間の距離を測定し，所定の間隔の範囲内である場合に，車両側無線装置が車両の施

解錠実行部に解錠指令を送出するキーレス・エントリーシステムである。

一方，甲３は，前記イ(ｳ)ａのとおり，携帯通信端末とカードとの距離に応じてカードの使用を許可するシステムであって，ここでのカードの使用とは，クレジットカードの情報を用いる電子商取引，すなわち，情報処理である。また，甲４は，同ｂのとおり，多端末環境でのユーザのワークステーションへのアクセスを許可するシステムであり，ここでのワークステーションへのアクセスは，当然に情報処理を目的としている。つまり，甲３及び４に記載された技術は，情報処理システムに対する不正使用防止の技術であるのに対し，甲１発明は，ドアの解錠システムという，情報処理システムではないシステムに対する不正使用防止の技術であって，両者は，その前提とするシステムが相違しており，技術分野が異なる。

(ｲ) しかも，装置Ａの記憶媒体に記憶されている情報を，特定の者に利用させる場合につき，当該特定の者に装置Ｂを携行させ，装置Ａと装置Ｂとの間の距離測定を行い，その距離が所定の範囲内であるときに限り，装置Ｂの所持者に当該情報を利用させるという周知技術を，甲１発明に適用したとしても，距離測定後に，距離測定の対象である装置の一方から他方へ，当該一方の装置が記憶しているマルチメディアデータを，他方の装置に送信するという構成に至るものではない。

(ｳ) したがって，当業者が，甲１発明と甲３又は４に記載された周知技術を組み合わせることは，容易とはいえず，仮に組み合わせたとしても，本願発明を発明することができたとはいえない。

エ(ｱ)ａ　被告は，２つの装置間の距離が所定範囲内であることを判定することにより，所定のプログラム若しくはデータ又は装置へのアクセスを許可することは，周知技術であり（甲３，４），「データ」を「マルチメディアデータ」を含むものとすることは文献を示すまでもない事項であり，甲１発明には，解錠以外のサービスは明記されていないが，自動車のオーディオやカーナビゲーションシステムの動作も含まれ得る（乙７）から，甲１発明において，ドアの解錠指令の送出に換えて，車両内に記憶されたマルチメディアデータへのアクセスを許可するように構成

することは，当業者が適宜なし得ることである旨主張する。

しかしながら，前記⑴ア(ア)ａのとおり，甲１には，甲１に記載されたキーレス・エントリーシステムを，ドアの施解錠以外に適用することについての記載はなく，示唆もない。また，甲１には，距離測定後に，車両側無線装置が，その記憶しているマルチメディアデータを,携帯型無線装置に送信することについて,記載がなく，示唆もない。

そうすると，当業者は，上記の乙７を参照したとしても，車両側無線装置が，携帯型無線装置からの応答信号に基づいて装置間の距離を測定し，事前に規定された距離間隔の範囲内にある場合に解錠指令を送出する引用発明において，距離の測定等を前提としないオーディオの操作等の動作が含まれるものと解することは困難であるし，まして，通常，ドアの施解錠とは無関係のマルチメディアデータへのアクセスという動作を，容易に想到できるとは到底いえない。

なお，乙７には，携帯機と，制御対象を含む物に搭載，付設，又は，接続され，前記携帯機との間で無線通信を行って，所定の携帯機であることを照合確認した上で，制御対象の所定の動作を実現するための制御処理を実行する本体機とを有する制御装置（【０００５】）につき，車両などの乗物のほか，機械，機器，建造物又は設備を制御対象とすること，制御対象の所定の動作として，車両ドアの施解錠動作のほか，乗り物の搭載物や付帯物の動作や起動又は起動の許可設定などがあり得ること，乗物の搭載物や付帯物としては，エンジンやモータ等の駆動源，トランスミッションなどの駆動機構，エアコン，オーディオ，ナビゲーションシステム，照明等があり得ること（【０００７】）が記載されている。

しかしながら，乙７には,「消費電力が少なく，防犯性が高く，使用者の利便性も高い制御装置を提供すること」が課題であって（【０００４】），本体機は，リクエスト信号を常時又は間欠的に無線送信し，携帯機は，本体機から無線送信されるリクエストを受信すると，当該携帯機にあらかじめ登録された制御用認証コードを含むアンサー信号を無線送信し，当該本体機は，前記アンサー信号を受信すると，それ

に含まれる制御用認証コードが，当該本体機にあらかじめ登録された制御用認証コードに対応しているか否かを判定し，この判定結果が肯定的であれば，制御対象の所定の動作が行われること（【０００５】，【０００７】），使用者が車両近くに行き乗り込むまでに，車両又は車両搭載物の盗難の危険性があることにつき，通信可能範囲を狭くして抑制することは，遠隔操作の利便性が悪化する弊害があり，解決にならないこと（【０００４】）が記載されているのであって，携帯機と本体機との間の距離測定により，両装置の距離が所定範囲内であることを判定して，制御対象の所定の動作が行われるようにすることについては，示唆はない。

したがって，被告の前記主張は，採用できない。

ｂ　被告は，この点，車とユーザ（携帯無線装置）との間の距離が一定の数値未満である場合を正当なものとする「ポリシー」と，ドアの解錠指令の送出を決定する「メカニズム」は，必ずしも一体不可分なものとして検討される必要はなく，ドライバーが車から離れている場合に解錠されることによって問題が生じないようにする必要があることは，甲１発明において，「解錠指令の送出」に換えて他の「メカニズム」を採用できない理由にならない旨主張する。

しかしながら，前記ウ(ｲ)のとおり，仮に，甲１発明と甲３又は４に記載された周知技術を組み合わせても，距離測定後，距離測定の対象である装置の一方が記憶しているマルチメディアデータを他方の装置に送信するという構成，すなわち，本願発明の構成にはならないのであって，このことは，被告の主張する「ポリシー」と「メカニズム」を一体不可分なものとして検討するか否かによって，結論を異にするものではない。

したがって，被告の前記主張は，採用できない。

(ｲ)ａ　なお，被告は，キーレス・エントリーシステムにおいて，車載装置と携帯装置との間でデータを送受信し，車載装置側のデータに携帯装置がアクセスしたり，携帯装置側のデータに車載装置がアクセスすることは，周知技術であり（乙８，９），甲１発明と，この周知技術を組み合わせて，装置間の距離が所定範囲内で

あることによって，車載装置側のデータに携帯装置がアクセスしたり，携帯装置側のデータに車載装置がアクセスすることを許可するように構成することは，当業者が適宜なし得ることであるとも主張する。

b(a)　乙８には，次の記載がある。

【０００１】

【発明の属する技術分野】本発明は，車両のキーレスエントリー装置に関する。

【０００４】本発明は，前記従来の問題点に鑑みてなされたもので，情報を書き込み読み出しが可能な車両キーレスエントリー装置を提供することを課題とする。

【００１２】図１（省略）は，本発明の第１実施形態にかかる車両キーレスエントリー装置を示す。この車両キーレスエントリー装置は，リモートユニット１と車両側ユニット２とからなる。リモートユニット１は，第１コイルアンテナ３，第１制御回路４，電池５，送信機６，第１送受信回路７および第１メモリ８を有する。

【００１４】図１に示すように，前記車両側ユニット２は，第２コイルアンテナ９，該第２コイルアンテナ９に電力を供給しリモートユニット１起動用電磁波を送信させる給電回路１０，受信機１１，第２制御回路１２，車両のドアを施解錠するドアロック装置を駆動するドアロック装置駆動回路１３，車内人体検知センサ１４，自動施錠タイマ１５，タイマ１６，第２送受信回路１７および第２メモリ１８を有する。

【００１５】前記第２コイルアンテナ９は，図２（省略）に示すように，ドアハンドルモジュール内に設けられ，前記給電回路１０により電力を供給されＬＦ（１２５ｋｈｚ）の磁界を発生する。この磁界の到達距離は，約１～１．５ｍである。前記受信機１１は，前記送信機６からのＩＤコード信号を受信するものであり，公知のイモビライザ機能を有するキーエスエントリーシステムに用いられ，車両のイグニッションスイッチモジュール（不図示）に設けられる一般的な受信機１１である。前記車内人体検知センサ１４は，運転席への着座を検知する一般的なシートスイッチやシートベルトの着脱を検知するシートベルトスイッチ，赤外線の反射を利用した一般的な人体検知センサであればよい。前記第２メモリ１８は，通信制御回路１９に接続され，ナビゲーションシステム２０や各種コントロールユニットに対する情報を記憶するようになっている。

【００１８】リモートユニット１１に設けられる前記第１制御回路４は，図４（省略）のフロ

ーチャートに示すように，ステップ１０１において，リモートユニット１内の第１コイルアンテナ３において第１，第２起動用電磁波を受信したか否かを判断する。これらの起動用電磁波を受信したと判断したならば，ステップ１０２において，マイコン動作を開始し，ステップ１０３において，送信機６を介してＩＤコードを送信させる。送信が終了すると，ステップ１０４において，マイコン動作を停止する。

【００１９】車両側に設けられる前記第２制御回路１２は，図５（省略）のフローチャートに示すように，ステップ２０１において，車両のドアが閉状態にあるか否かを判断する。閉状態でないならば，リターンする。閉状態であるならば，ステップ２０２において，車両のドアのロックが施錠状態にあるか否かを判断する。施錠状態であるならば，ステップ２０３において，車両側に設けられた給電回路１０により電力を供給された第２コイルアンテナ９からＬＦ（１２５ｋｈｚ）の磁界（磁界範囲は，第２コイルアンテナ９から約１～１．５ｍ）を発生させ，第１起動用電磁波を送信し，ステップ２０４において，その第１起動用電磁波送信を停止する。

【００２１】そして，ステップ２０５において，ＩＤコードを受信したと判断したならば，ステップ２０７において，受信したＩＤコードと車両側にあらかじめ登録されている登録ＩＤコードとが一致しているか否かを判断する。一致していないと判断すれば，リターンする。一致していると判断すれば，ステップ２０８において，車両のドアロックを解錠し，ステップ２０９において，自動施錠タイマ１５を作動させ，リターンする。

【００２６】これにより，図３（Ａ）（省略）に示すように，リモートユニット１を所持した運転者が，車両に近づき，車両側ユニット２の第２コイルアンテナ９から約１～１．５ｍ内の前記磁界の範囲に入ると，リモートユニット１の第１コイルアンテナ３において電磁誘導が発生し，第１制御回路４に電流が流れる。第１制御回路４は，これに基づき，第１コイルアンテナ３からの電流を第１制御回路４が起動する起動信号として受け，これを受けて初めて送信機６を作動させる。送信機６の作動後，リモートユニット１の電池５は，第１制御回路４が第１コイルアンテナ３からの電流を受けることを待機するのに必要な待機電力だけに使用されるので，電池５の消耗を低減できる。また，図３（Ｂ）（省略）に示すように，運転者がリモートユニット１を所持して降車し車両から離れるときや，車両のドアを開けたが乗車せずに車両のドアを閉め車両から離れるなどのときには，リモートユニット１が車両から一定距離離れかつ車両の

ドアが解錠されてから所定の時間が経過した場合のみに，ドアのロック装置を施錠するようにしたので，ロック装置の無駄な動作を低減できる。また，第１コイルアンテナ３が第２コイルアンテナ９に対して一定距離にあるときに，送信機６を作動し所定の信号を送信させ常時は信号を送信していないため，所定の信号をコピーされ難くセキュリティー性が高く，盗難防止を図れるものである。

【００２７】以上のようなキーレスエントリー動作に加え，本実施形態のキーレスエントリー装置は，次の付加機能を有する。すなわち，車両の故障箇所やエンジンオイルの内容量，バッテリーの交換時期などの各種コントロールユニットからの情報を，通信制御回路１９を介して車両内において第２メモリ１８に記憶し，その記憶された情報を第２送受信回路１７から第１送受信回路７に送信し，第１メモリ８に記憶させることができる。このためユーザは，リモートユニット１を車両から持ち出し，家庭やディーラなどの車両以外の場所において，リモートユニット１を読み出し装置（不図示）に接続し，第１メモリ８に記憶されている情報をパソコンなどで情報処理し，どの部品が交換必要か等の情報を得ることができる。

【００２８】また，家庭などの場所において，ナビゲーションシステムの目的地またはルート情報などを，リモートユニット１の第１メモリ８に記憶し，ユーザが車両に乗車したとき第１メモリ８に記憶された情報を第１送受信回路７から第２送受信回路１７に送信し，その情報を第２メモリ１８に記憶した後，通信制御回路１９を介して車両内のナビゲーションシステム２０で自動的に目的地の設定やルート設定などをすることができる。

(b)　乙９には，次の記載がある。

【０００１】

【発明の属する技術分野】本発明は，自動車等の車両に対するロック・アンロックを，キーシリンダに対するキー操作無しで行うことが可能なキーレスエントリ装置及びその情報通信方法及びキーレスエントリ用携帯機及びキーレスエントリ用車載機に関する。

【０００７】即ち，携帯機に設けられた送受信機と，車載機に設けられた送受信機とにより構

成される第１通信ライン（無線または赤外線）を介して所定の制御情報を送受信することにより，該車載機がドアロック機構のロック・アンロック動作を制御するキーレスエントリ装置であって，前記携帯機と前記車載機とは，前記所定の制御情報とは異なる任意の情報（例えば，音楽データ等）を，前記第１通信ラインを介して送受信する情報通信制御手段をそれぞれ備えることを特徴とする。

【００２８】上記のシステム構成を有する本実施形態に係るキーレスエントリ装置において，携帯機１と車載機２とは，無線信号または赤外線信号を用いて第１通信ラインを確立し，その第１通信ラインによってドアロック動作を実現する制御情報と，音楽データや地図データ等の任意情報とを送受信する。

【００２９】また，携帯機１と車載機２とは，第１通信ラインによる情報通信ができないとき，或いは携帯機１の操作者が操作スイッチ（後述する第２データ送信スイッチ１２４）によって選択したときに，数十m程度の範囲内の通信に採用して好適な所定の近距離無線通信方式（例えば，Bluetooth 等）に基づく無線信号を用いて第２通信ラインを確立し，その第２通信ラインによって少なくとも上記の任意情報を送受信する。

【００３０】携帯機１が車載機２に伝送する任意情報は，情報機器４から無線信号によって入手した情報であり，車載機２が携帯機１に伝送する任意情報は，ナビゲーションユニット２８，オーディオユニット２９，或いは故障診断ユニット３０から受信した情報である。

【００４５】ここで，本実施形態の主な特徴を概説する。携帯機１に設けられたキーレス送受信機１５と，車載機２に設けられたキーレス送受信機２２とは，無線または赤外線を用いて構成される第１通信ラインを介して所定のロック制御情報を送受信することにより，車載機２がドアロック機構のロック・アンロック動作を制御すると共に，当該所定のロック制御情報が送受信されていない期間を利用して，そのロック制御情報とは異なる任意情報（音楽データや地図データ等）を，当該第１通信ラインを介して，携帯機１から車載機２に，または車載機２から携帯機１に転送する。また，少なくとも当該任意情報の送信に使用する通信ラインに関しては，携帯機１に設けられた第１または第２データ送信スイッチ１２３，１２４の操作者による選択，または後述する制御処理による自動的な切り替えにより，第１または第２通信ラインの

何れかが選択される。

【００４６】尚、本実施形態において、携帯機１と車載機２とによって実現されるドアロック制御動作は、携帯機１を操作する操作者が、アンロックスイッチ１２１またはロックスイッチ１２２を操作するのに応じて、車載機２のドアロックアクチュエータ２７が作動すると共に、所定時間周期毎に車載機１から自動的に送出されるアンロック要求信号を車載機２にて受信したときにその受信電界強度が所定の電界強度Ｌ１より大きいときに、車載機２のドアロックアクチュエータ２７が自動的に作動する構成を採用するが、この構成に限られるものではなく、例えば、アンロック信号の受信電界強度に応じた自動的なロック・アンロック動作は備えない装置構成であっても良い。

【００９０】尚，送受信する任意情報が著作権保護の観点から問題ない情報である場合に限られるが，上述した所定のドアロック制御信号が携帯機１と車載機２との間で送受信されるときにその制御信号に含まれるべき固体識別情報（セキュリティ情報）は，上述した携帯機データ通信処理（図７（省略））及び車載機データ通信処理（図８（省略））においては一致しなくても，携帯機１と車載機２との間の任意情報の送受信は許容することにより，任意情報の情報伝送を，効率（使い勝手）良く行うことができ，携帯機１と同じ装置構造を備える端末を複数用意すれば，それら複数の携帯機１同士で，任意情報の共有を容易に行うことができる。

ｃ(a)　前記ｂ(a)によれば，乙８には，キーレスエントリー装置につき（【０００１】），車両側ユニット２は第２コイルアンテナ９から磁界範囲１～１．５ｍの磁界を発生させて第１起動用電磁波を送信し，リモートユニット１を所持した運転者が前記磁界の範囲に入るとリモートユニット１の第１コイルアンテナ３において電磁誘導が発生し，これに基づき，リモートユニット１の送信機６が作動し（【００１２】，【００１４】，【００１５】，【００１９】，【００２６】），送信機６を介してＩＤコードを送信し（【００１８】），車両側ユニット２の受信機１１が前記ＩＤコードを受信したならば，前記ＩＤコードと登録ＩＤコードとが一致しているか否かを判断し，一致している場合には，車両のドアロックを解錠する（【００１５】，【００

２１】）ように構成されたキーレスエントリー装置において（【０００１】），付加機能として，車両の故障箇所やエンジンオイルの内容量，バッテリーの交換時期などの各種コントロールユニットからの情報を，車両側ユニット２の第２送受信回路１７からリモートユニット１の第１送受信回路７に送信してリモートユニット１の第１メモリ８に記憶させ，リモートユニット１を車両から持ち出し，家庭やディーラなどの車両以外の場所において，リモートユニット１を読み出し装置に接続し，前記の記憶された情報をパソコンなどで情報処理すること(【００１２】,【００１４】,【００２７】)，また，家庭などの場所において，ナビゲーションシステムの目的地又はルート情報などを，リモートユニット１の第１メモリ８に記憶し，ユーザが車両に乗車したとき，第１メモリ８に記憶された情報を，第１送受信回路７から車両側ユニット２の第２送受信回路１７に送信し，その情報を車両側ユニット２の第２メモリ１８に記憶させ，通信制御回路１９を介して車両内のナビゲーションシステム２０で自動的に目的地の設定やルート設定などをすること（【００１４】,【００２８】）が記載されている。

(b)　前記ｂ(b)によれば，乙９には，携帯機１と車載機２とが，無線信号又は赤外線信号を用いて第１通信ラインを確立し，その第１通信ラインを介して所定の制御情報を送受信することにより，車載機がドアロック動作を実現するキーレスエントリ装置において（【０００１】,【０００７】），前記第１通信ラインによって，携帯機１から車載機２に，又は，車載機２からが携帯機１に，音楽データや，地図データ等（車載機２から携帯機１への伝送のときは，ナビゲーションユニット２８，オーディオユニット２９，又は故障診断ユニット３０から受信した情報）を伝送し，第１通信ラインによる情報通信ができないとき，又は，携帯機１の操作者が操作スイッチによって選択したときに，数十m程度の範囲内の通信に採用して好適な所定の近距離無線通信方式（例えば，Bluetooth 等）に基づく無線信号を用いて第２通信ラインを確立し，その第２通信ラインによって，少なくとも上記のナビゲーションユニット，オーディオユニット，又は，故障診断ユニットから受信した情

報を送受信すること（【０００７】,【００２８】～【００３０】），前記の情報が著作権保護の観点から問題ない情報である場合には，ドアロック制御信号が携帯機１と車載機２との間で送受信されるときにその制御信号に含まれるべき固体識別情報（セキュリティ情報）が一致しなくても，携帯機１と車載機２との間の前記の情報の送受信を許容することができること（【００９０】）が記載されている。

ｄ(a)　前記ｃ(a)によれば，乙８には，車両のキーレスエントリー装置の付加機能として，車両の故障箇所やエンジンオイルの内容量，バッテリーの交換時期などの各種コントロールユニットからの情報を，車両側ユニット２からリモートユニット１に送信し，車両からリモートユニット１を持ち出して，それを読み出し装置に接続して読み出すこと，車両から持ち出したリモートユニット１にナビゲーションシステムに読み込むべき情報を記憶させ，これをユーザが車両に乗車したときに車両側ユニット２に送信して記憶させ，車両内のナビゲーションシステムに読み込むことが記載されているところ，乙８には，車両側ユニットとリモートユニットとの間の情報の送信が，車両側ユニットとリモートユニットとの間の距離測定に基づいて行われることにつき，記載も，示唆もない。

確かに，前記のとおり，前記送信が行われるのは，リモートユニットが車両にあるとき，又は，ユーザが車両に乗車したときと記載されているが，これは，車両側ユニットの第２コイルアンテナの磁界の到達距離が，約１～１．５メートルであり（乙８【００１４】,【００１５】），リモートユニットが前記磁界の範囲に入ると，リモートユニットの第１制御回路が起動し，送信機が作動する（同【００２６】）ことから，必然的に，前記磁界の範囲内にリモートユニットがないと，リモートユニットは起動用電磁波を受信したと判断できず，リモートユニットからのＩＤコードの送信もできず，解錠もできず（同【００１８】,【００２１】），各種コントロールユニットからの情報等の送受信もできないことによるものである。

しかも，乙８には，車両の故障箇所やエンジンオイルの内容量，バッテリーの交換時期などの各種コントロールユニットからの情報及びナビゲーションシステムに

読み込むべき情報の送信が記載されているのであって，映画を含むマルチメディアデータの送信についての記載はない。

(b) 前記ｃ(b)のとおり，乙９には，車両のキーレスエントリ装置において，ドアロックの制御情報を送受信する無線信号又は赤外線信号を用いて確立される第１通信ライン，又は，数十m程度の範囲内の通信に好適な所定の近距離無線通信方式に基づく無線信号を用いて確立される第２通信ラインによって，携帯機１から車載機２に，又は，車載機２から携帯機１に，音楽データや地図データ等を伝送することが記載されているところ，乙９には，車載機と携帯機との間の情報の送信が，車載機と携帯機との間の距離測定に基づいて行われることにつき，記載も，示唆もない。

乙９には，第２通信ラインについて，数十m程度の範囲内の通信に好適な近距離無線通信方式を用いるとの記載がある（【００２９】）ものの，これは，車載機と携帯機との距離が数十mの範囲内であることを測定し，認証することを記載したものではなく，近距離無線通信方式の持つ性質を述べたものにすぎない。

しかも，乙９には，車両におけるキーレス・エントリーシステムの付加機能としてのナビゲーションユニット，オーディオユニット，又は，故障診断ユニットからの情報と，これらのユニットに読み込むべき情報の送信について記載されているのであって，送信の対象に音楽データ等が含まれるとしても，映画を含むマルチメディアデータについて記載はない。

(c) 以上によれば，乙８及び９は，甲１発明と同様のキーレス・エントリーシステムに関するものであり，車両側無線装置と携帯型無線装置との間で，車両に関する情報や音楽データ等を送受信する技術を周知のものとして開示していると認められるが，車両側無線装置と携帯型無線装置との間の距離測定を行い，前記距離が所定範囲内である場合に，車両側無線装置から携帯型無線装置へマルチメディアデータを送信することは開示されておらず，したがって，距離判定の処理に基づいて行われる動作として，車両側無線装置から携帯型無線装置へマルチメディ

アデータを送信することが，周知技術であるとも認められない。

そうすると，甲１発明について，乙８及び９に記載の周知技術を適用したとしても，前記ア記載の本願発明との相違点に係る構成に至るものではない。

(ｳ) したがって，前記被告の主張は，いずれも採用できない。

オ まとめ

以上のとおり，甲１発明において，距離判定の結果に基づき，車両のドアの解錠を行う構成に換えて，マルチメディアデータの転送を行う構成を採用することは，当業者が容易になし得ることではなく，相違点１は格別のものではないと判断した審決には，誤りがあるから，取消事由２には，理由がある。

第６ 結論

以上の次第で，審決は，進歩性の有無の判断に誤りがある（取消事由２）から，その余の取消事由２及び取消事由１について判断するまでもなく，原告の請求を認容することとして，主文のとおり判決する。

知的財産高等裁判所第２部

裁判長裁判官 清 水 節

裁判官　　中　　村　　　　恭

裁判官　　森　　岡　　礼　　子