平成２２年１２月６日判決言渡　同日原本領収　裁判所書記官

平成２２年（行ケ）第１００８４号　審決取消請求事件

口頭弁論終結日　平成２２年１１月２９日

判　　決

原　　告	シーイエス　エレクトロニカ　インダストリア　エ　コメルスィオ　リミタダ
訴訟代理人弁護士	加　藤　伸　樹
弁理士	小　林　義　孝
被　　告	特　許　庁　長　官
指定代理人	関　谷　隆　一
	小　松　　正
	吉　澤　雅　博
	廣　瀬　文　雄
	田　村　正　明

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。

この判決に対する上告及び上告受理の申立てのための付加期間を３０日と定める。

事　実　及　び　理　由

第１　原告の求めた判決

特許庁が不服２００６－１６４６２号事件について平成２１年１０月２６日にした審決を取り消す。

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について特許庁がした請求不成立審決の取消訴訟である。争点は，容易推考性の存否である。

１　特許庁における手続の経緯

原告は，平成１４年４月１１日，名称を「磁気読み取り装置の磁気ヘッド」（平成１８年２月１６日付けの補正により「磁気カード読み取りシステム」と変更）とする発明について特許出願（特願２００２－１０９０５２号）をしたが，平成１８年２月１６日付けの補正を経た後に拒絶査定を受けたので，不服の審判請求をした。

特許庁は，この請求を不服２００６－１６４６２号事件として審理し，その中で原告は，平成１８年８月２９日付けで特許請求の範囲等を変更する補正をしたところ（甲７の３，請求項の数２，本件補正），特許庁は，平成２１年１０月２６日，「本件審判の請求は，成り立たない。」との審決をし，その謄本は平成２１年１１月１０日原告に送達された。本件補正は審決の理由中で却下された。

２　本件補正の内容

本件補正は，特許請求の範囲の請求項１の記載を補正することなどを内容とするものであるが，本件出願の本件補正前後の請求項１の記載は，次のとおりである（以下，本件補正前の請求項１に記載された発明を「本願発明」といい，本件補正後の請求項１に記載された発明を「本願補正発明」という。）。

(1) 本件補正前（平成１８年２月１６日付け手続補正によるもの）の請求項１

「磁性体を利用して所定のデータを記憶した磁気カードと，前記磁気カードから前記データを読み取る磁気ヘッドを備えた磁気カードリーダと，前記磁気カードリーダにインターフェイスを介して接続されたコンピュータとから形成された磁気カード読み取りシステムにおいて，

前記磁気ヘッドが，前記磁気カードに記憶されたデータをアナログ信号に変換するコイルを備えたコアと，前記コイルに電気的に接続され，前記アナログ信号をデジタル信号に変換するA/D変換チップと，前記A/D変換チップに電気的に接続され，

作成したアルゴリズムに基づいて前記デジタル信号を暗号化する IC とから形成され，前記コアと前記 A/D 変換チップと前記 IC とが，前記磁気ヘッドの外周面を包被するハウジングの内部に収納され，前記 A/D 変換チップと前記 IC とが，前記ハウジングの内部に合成樹脂を介して固定され，

前記コンピュータが，前記 IC に電気的に接続され，前記磁気カードリーダからの前記磁気カードのカード読み取り信号の入力にともなって，前記磁気カードに記憶されたデータを暗号化するための公開鍵と暗号化されたデータを復号化するための秘密鍵とを生成する鍵生成手段と，前記鍵生成手段を介して生成した前記公開鍵を前記磁気ヘッドの IC へ出力する鍵出力手段とを有し，

前記システムでは，前記カード読み取り信号が前記磁気カードリーダから前記コンピュータに入力されると，前記コンピュータが前記公開鍵と前記秘密鍵とを生成かつ出力し，前記デジタル信号が前記 A/D 変換チップから前記 IC に入力されると，前記 IC が前記コンピュータから入力された前記公開鍵を使用してアルゴリズムを作成し，作成したアルゴリズムに基づいて前記デジタル信号を暗号化するとともに，暗号化した前記デジタル信号を前記コンピュータへ出力し，前記コンピュータが前記秘密鍵を使用してアルゴリズムを作成し，作成したアルゴリズムに基づいて暗号化された前記デジタル信号を復号化することを特徴とする前記磁気カード読み取りシステム。」

(2) 本件補正による請求項１（下線部分は補正箇所である。）

「磁性体を利用して所定のデータを記憶した磁気カードと，前記磁気カードから前記データを読み取る磁気ヘッドを備えた磁気カードリーダと，前記磁気カードリーダにインターフェイスを介して接続されたコンピュータとから形成された磁気カード読み取りシステムにおいて，

前記磁気ヘッドが，前記磁気カードに記憶されたデータをアナログ信号に変換するコイルを備えたコアと，前記コイルに電気的に接続され，前記アナログ信号をデジタル信号に変換する A/D 変換チップと，前記 A/D 変換チップに電気的に接続され，

作成したアルゴリズムに基づいて前記デジタル信号を暗号化する IC とから形成され，前記コアと前記 A/D 変換チップと前記 IC とが，前記磁気ヘッドの外周面を包被するハウジングの内部に収納され，前記 A/D 変換チップと前記 IC とが，前記ハウジングの内部に合成樹脂を介して固定され，

前記コンピュータが，前記 IC に電気的に接続され，前記磁気カードリーダから前記磁気カードのカード挿入信号が入力されると，前記磁気カードに記憶されたデータの読み取り開始指令を前記 IC に出力しつつ，前記磁気カードに記憶されたデータを暗号化するための公開鍵と暗号化されたデータを復号化するための秘密鍵とを生成する鍵生成手段と，前記鍵生成手段を介して生成した前記公開鍵を前記磁気ヘッドの IC へ出力する鍵出力手段とを実行し，前記磁気カードリーダから前記磁気カードのカード通過信号が入力されると，前記磁気カードに記憶されたデータの読み取り停止指令を前記 IC に出力し，

前記システムでは，前記カード挿入信号が前記磁気カードリーダから前記コンピュータに入力される度毎に，前記コンピュータが前記公開鍵と前記秘密鍵とを生成かつ出力し，前記デジタル信号が前記 A/D 変換チップから前記 IC に入力されると，前記 IC が前記コンピュータから入力された前記公開鍵を使用してアルゴリズムを作成し，作成したアルゴリズムに基づいて前記デジタル信号を暗号化するとともに，暗号化した前記デジタル信号を前記コンピュータへ出力し，前記コンピュータが前記秘密鍵を使用してアルゴリズムを作成し，作成したアルゴリズムに基づいて暗号化された前記デジタル信号を復号化することを特徴とする前記磁気カード読み取りシステム。」

３　審決の理由の要点

(1)　本願補正発明は，引用例（特開２００１－１４３２１３号公報，甲１）に記載された引用発明，周知技術及び技術常識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って，特許法２９条２項の規定により，特許出願の際独立して特許を受けることができず，したがって，本件補正は，平成１８年法律第５５号

による改正前の特許法１７条の２第５項において準用する特許法１２６条５項の規定に違反するから，平成１４年法律第２４号による改正前の特許法１５９条１項において準用する同改正前の特許法５３条１項の規定により却下すべきものである。

本願発明も，本願補正発明と同様の理由により当業者が容易に発明をすることができたものであり，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。

(2) 審決が認定した引用発明の内容，引用発明と本願補正発明との一致点及び相違点は，次のとおりである。

【引用発明】

「カードに磁気記録されたカードデータを読取る磁気ヘッドと，この磁気ヘッドで読取られたカードデータを用いて各種情報処理を実施する情報処理部とで構成されており，磁気カードリーダが組込まれているカード処理装置において，

磁気ヘッドにおいて，ヘッド容器内に，ヘッド本体，増幅器，A/D 変換器を内蔵する１チップマイクロコンピュータからなる制御部，この制御部に接続された ROM，同じく制御部に接続された RAM が収納され，さらに，このヘッド容器内における各部材相互間には，エポキシ樹脂等からなる不透明の充填材が充填され，

情報処理部内には，マイクロコンピュータからなる本体制御部，この本体制御部に接続された ROM，RAM，表示器，キーボード，及び直流電圧 Vc を出力する電源が組込まれ，

磁気ヘッドと情報処理部との間には，相互に情報交換を行うための信号線が存在し，

カードの磁気ストライプには，デジタルのカードデータに対して，MFM（modified frequency modulation）で磁気記録され，カード磁気記録となり，

カードが移動すると，ヘッド本体がこのカードに磁気記録されたカード磁気記録を読取り，読取信号を増幅器へ送出し，増幅器は読取信号を増幅して，新たな読取信号として制御部の A/D 変換器へ送出し，制御部の A/D 変換器は，増幅器から入力された読取信号をデジタルの読取信号に A/D 変換し，制御部はこの A/D 変換された

読取信号の波形から，デジタル信号（元のカードデータ）に変換し，

制御部に接続された RAM 内には，データ暗号化規格（DES：Data Encryption Standard）に基づく一方向性関数でデジタル信号（カードデータ）を暗号化するためのファンクション（関数）とキー（鍵）が書込まれており，

制御部はこのファンクション（関数）とキー（鍵）とを用いてデジタル信号（カードデータ）を暗号化し，暗号化されたカードデータを信号線を介して情報処理部へ送信し，

制御部に接続された RAM 内に書込まれているキー（鍵）を，１個の暗号化されたカードデータを情報処理部へ送信する毎に，情報処理部から送信されたキー（鍵）に書替（更新）え，

本体制御部は，信号線を介して受信した暗号化されたカードデータを本体制御部に接続された RAM 内に書込まれたキー（鍵）を用いて元のカードデータに復号し，磁気ヘッドから受信した暗号化されたカードデータが正常に復号されると，新たにキー（鍵）を生成して，この生成したキー（鍵）を，信号線を介して磁気ヘッドへ送信し，さらに，磁気ヘッドへ送信したキー（鍵）で本体制御部に接続された RAM に記憶されたキー（鍵）を更新するカード処理装置。」

【一致点】

「磁性体を利用して所定のデータを記憶した磁気カードと，前記磁気カードから前記データを読み取る磁気ヘッドを備えた磁気カードリーダと，前記磁気カードリーダにインターフェイスを介して接続されたコンピュータとから形成された磁気カード読み取りシステムにおいて，

前記磁気ヘッドが，前記磁気カードに記憶されたデータをアナログ信号に変換するコイルを備えたコアと，前記コイルに電気的に接続され，前記アナログ信号をデジタル信号に変換する A/D 変換（器）と，前記 A/D 変換（器）に電気的に接続され，作成したアルゴリズムに基づいて前記デジタル信号を暗号化する IC とから形成され，前記コアと前記 A/D 変換チップと前記 IC とが，前記磁気ヘッドの外周面を包

被するハウジングの内部に収納され，前記 A/D 変換（器）と前記 IC とが，前記ハウジングの内部に合成樹脂を介して固定され，

前記コンピュータが，前記 IC に電気的に接続され，前記磁気カードに記憶されたデータを暗号化するための鍵と暗号化されたデータを復号化するための鍵とを生成する鍵生成手段と，前記鍵生成手段を介して生成した前記（磁気カードに記憶されたデータを暗号化するための）鍵を前記磁気ヘッドの IC へ出力する鍵出力手段とを実行し，

前記システムでは，前記コンピュータが前記（磁気カードに記憶されたデータを暗号化するための）鍵と前記（暗号化されたデータを復号化するための）鍵とを生成かつ出力し，前記デジタル信号が前記 A/D 変換（器）から前記 IC に入力されると，前記 IC が前記コンピュータから入力された前記（磁気カードに記憶されたデータを暗号化するための）鍵を使用してアルゴリズムを作成し，作成したアルゴリズムに基づいて前記デジタル信号を暗号化するとともに，暗号化した前記デジタル信号を前記コンピュータへ出力し，前記コンピュータが前記（暗号化されたデータを復号化するための）鍵を使用してアルゴリズムを作成し，作成したアルゴリズムに基づいて暗号化された前記デジタル信号を復号化する前記磁気カード読み取りシステム。」

【相違点ａ】

「A/D 変換器」について，本願補正発明は，「チップ」であるのに対し，引用発明は，「１チップマイクロコンピュータからなる制御部」に「内蔵」されたものである点。

【相違点ｂ】

「コンピュータ」について，本願補正発明は，「前記磁気カードリーダから前記磁気カードのカード挿入信号が入力されると，前記磁気カードに記憶されたデータの読み取り開始指令を前記 IC に出力し」，「前記磁気カードリーダから前記磁気カードのカード通過信号が入力されると，前記磁気カードに記憶されたデータの読み

取り停止指令を前記 IC に出力」するのに対し，引用発明は，そのようになされていない点。

【相違点ｃ】

「鍵」について，本願補正発明は，「前記磁気カードに記憶されたデータを暗号化するための公開鍵と暗号化されたデータを復号化するための秘密鍵と」を用いるのに対し，引用発明は，「前記磁気カードに記憶されたデータを暗号化するための鍵と暗号化されたデータを復号化するための鍵と」が共通である点。

【相違点ｄ】

「コンピュータ」について，本願補正発明は，「前記カード挿入信号が前記磁気カードリーダから前記コンピュータに入力される度毎に，」「鍵」を「生成かつ出力」するのに対し，引用発明は，「磁気ヘッドから受信した暗号化されたカードデータが正常に復号されると，」「鍵」を「生成かつ出力」する点。

(3)　審決は，各相違点に係る本願補正発明の構成とすることは当業者が容易に想到できたものであり，本願補正発明の効果も，引用例記載の構成，周知技術及び技術常識から予測されるもので格別なものとはいえないとした。そして，本願発明も，前記本願補正発明の一部の構成を削除し，他の一部の構成を上位概念化したものであるから，同様の理由で引用例，周知技術及び技術常識に基づいて当事者が容易に発明できたものであるとした。

第３　原告主張の審決取消事由

１　取消事由１（本願補正発明の認定の誤り）

本願補正発明における「磁気カード読み取りシステム」は，カードリーダからクレジットカード会社等のサーバまで，すなわち，システム全体における通信の安全を達成しようとするものである。

①システムという用語は，複数の要素が関係し合い，まとまって機能する組織や系統のことを意味すること，②本件補正明細書には，「コンピュータ」より先の通

信を示唆する記載が存在しておらず，このような「コンピュータ」は読み取られたカードデータの終点であるといえること，③発明の詳細な説明において，磁気カード読み取りシステム１Ｂの説明（段落【００３２】以降）には「ホストコンピュータ」という記載があること，④「ホストコンピュータ」とは，通信回線で接続したコンピュータと端末装置で構成するコンピュータシステムにおいて，すべての機能を集中的に管理するコンピュータ，あるいは，大規模な計算処理やネットワーク全体の管理，制御処理などを集中的に行うコンピュータをいうことから，本願補正発明の「コンピュータ」が端末機器の本体部分を指しておらず，例えばクレジットカードシステムにおいてすべての端末を集中的に管理するコンピュータを指していることは明らかである。

したがって，本願補正発明にいう「コンピュータ」はクレジット会社等のサーバを指しており，本願補正発明における暗号鍵の生成はサーバで行われることが前提となっている。

審決は，このような本願補正発明の意義を理解せずに相違点の認定・判断を行っており，誤りである。

２　取消事由２（引用発明の認定の誤り）

(1)　審決は，引用発明について，情報処理部に「さらに信用照会実施のための通信回線を接続し」，カードデータを「通信回線を通じて送信（転送）する」構成を認定していない。

この構成は，引用発明がカードリーダに関する発明であることを端的に示している。すなわち，クレジットカード等の磁気カード読み取りシステムは，磁気カードを店舗等に設置されたカードリーダで読み取り，そのカードデータを離れた場所に設置されているカードセンタ等のコンピュータサーバに保存されたデータと照合するものであるが，引用発明は，システムの一部であるカードリーダについてのみ考慮した発明である。つまり，引用発明は一つの機器であるカードリーダの内部（磁気ヘッドとカードリーダ本体間）におけるデータ盗用を防止する目的で考案された

ものにすぎない。

データ盗用のリスクは，引用発明のようなカードリーダ内部の場合，情報の伝達経路が短く情報の発信点と終着点が同じ場所にあるため，盗用された場合の発見が容易であり，対処も素早くできるという点でリスクが比較的小さい。これに対し，本願補正発明のように，カードリーダを出てからサーバまでというカードリーダ外部の経路は長距離にわたり，電話回線やインターネットなど一般回線を通るため，盗用を発見することは極めて困難であり，また，なりすましのリスクも存在することから，リスクが極めて高い。

この点は，当業者が，情報盗用という課題に対してとる思考方法に影響を及ぼすものであり，相違点の判断に影響する。

(2)　審決は，引用発明について，暗号化方式として共通鍵方式の一種である DES 方式を用いることは認定しているが，これ以外にも，この方式と同様の安全性を有し，処理能力が格別高くないチップでも短時間に暗号化が行える共通鍵方式を用いるとされている点を認定していない。

引用例には，DES 方式よりも低い処理能力で実行できる暗号化方式が記載されていること，簡易な暗号化方式を用いた制御部についてことさらに記載している（引用例の請求項６）が，RSA 方式を用いる制御部について記載していないこと，引用例に公開鍵と秘密鍵という用語が一切見られないことから，引用発明は公開鍵方式を適用することを全く念頭に置いていないというべきである。

本願補正発明が採用する公開鍵方式には，鍵の解読防止の問題を克服できるという利点がある一方で，高度な処理能力を要するという制約がある。他方，共通鍵方式は鍵の解読防止に関して重大な問題を抱える一方で，低い処理能力でも採用できるという利点を有する。そして，引用発明は共通鍵方式を前提とした発明であり，DES 方式よりもさらに処理能力を要しない暗号化方式を採用している。このことは，当業者の思考方法に影響を与え，ひいては相違点の判断にも影響を与える。

３　取消事由３（一致点認定の誤り及び相違点の看過）

(1)　審決は，磁気カードリーダに「インターフェイスを介して接続されたコンピュータとから形成された」,「磁気カード読み取りシステム」である点を一致点として認定しているが，上記１，２で主張した内容からして誤りである。また，このような違いを考慮すれば，相違点として，次の２点（ｅ，ｆ）も認定すべきであった。

ｅ「前記制御部について，引用発明においては，制御部はカードリーダの本体内部に設置されており，引用発明は「カードセンタにカードの信用照会を実施するための通信回線が接続されている」「カード処理装置」，すなわち，カードリーダに関する発明であるのに対し，本願補正発明においては，制御部は「コンピュータ」すなわち，システムの終点であるサーバに設置されており，通信回線の接続を予定しておらず,「磁気カード読み取りシステム」に関する発明である点。」

ｆ「暗号化方式について，引用発明は「DES 方式ないしそれと同等の安全性を有し，処理能力が格別高くないチップでも短時間に暗号化が行える暗号化方式」を用いるのに対し，本願補正発明は DES 方式よりも高度な処理能力を要求する暗号化方式を用いている点。」

(2)　引用発明は，カードリーダ内部における情報の盗用を防止するという課題を解決するための発明である。カードリーダ内部における情報盗用のリスクは相対的に小さいから，当業者は，カード処理の高速化及びカードリーダの小型化を志向し，暗号を強化することにそれほど意識を払わない。このため，引用発明は，低い処理能力でも足りる共通鍵方式を採用し，かつ，暗号を DES 方式よりも安全性が低いが処理速度に優れた方法を採用している。つまり，鍵の解読防止の問題について一切注意を払っておらず，高い処理能力を要する暗号化方式を排除しているのである。引用発明にみられる技術思想では，カードリーダ外部の通信の安全は別途考慮されることになり，解決すべき課題に含まれていない。

これに対し，本願補正発明は，カードリーダ外部まで含めた読み取りシステムに関する発明であるから，なりすましのリスク等の情報盗用のリスクは相対的に高く，

高い処理能力を要求されたとしても，暗号の強化が重要となる。とりわけ，鍵の解読防止の問題は重要である。また，本願出願当時，クレジットカード読取りに用いる端末機器である CAT 端末の本体部分を不正に開いて情報を取り出す犯罪（薬品を用いて溶かすなどの方法が存在した。）も発生しており，引用発明のようにカードリーダの本体部分で鍵を生成し，かつ，同カードリーダ内で復号する方法はこのような犯罪に対して無力であった。本願補正発明は，これらの課題に対処するために考案されたものであり，その技術思想の本質は，カードリーダの磁気ヘッドとコンピュータサーバをいわばシームレス（縫い目なし）につなぐことにある。

このように，本願補正発明は，引用発明とは課題が異なり，また，技術思想も異なる。したがって，上記原告主張の相違点ｅ，ｆについて，引用発明から本願補正発明を想到することが容易であるとはいえない。

４　取消事由４（相違点に関する判断の誤り）

(1)　相違点ｃについて

ア　本願補正発明の出願当時，公開鍵方式は，高度な処理能力を要するため，平文（伝達対象である情報）の暗号化ではなく，（平文より短い）平文ではない情報を暗号化・復号化することによる情報発信者の認証が主たる使用法として考えられていた。したがって，当業者は，公開鍵方式を認証機能のために用いるのが通常であるといえる。

引用発明は，カードリーダ内部の課題に対する発明であり，情報を発信する磁気ヘッドと情報を受信するカードリーダ本体は 1 本の有線で接続されているから，認証機能の必要性はない。そのため，引用発明は，あえて，高い処理能力を要する公開鍵方式を採用するメリットがなく，共通鍵方式を採用している。

審決は，引用例（段落【００７１】）の「RSA 暗号化方式…を採用してもよい。」の記載を，相違点ｃに関して公開鍵方式の採用に容易に想到できたことの根拠としている。しかし，この記載により分かるのは，引用発明出願当時から RSA 方式（公開鍵方式）が存在するということのみである。公開鍵方式も広い意味で暗号である

から，DES 方式と置換可能であるが，前述したとおり，当業者は引用発明のようなカードリーダ内部の秘密保持を課題とする発明をみても，公開鍵方式の採用を検討しない。そもそも，RSA 方式の主たる用途は認証機能であるから，引用発明において採用する必要性はない。さらにいえば，引用例（段落【００７３】）の「RSA 暗号化方式…と同等の安全性を有し」という記載からすると，引用発明の考案者は暗号技術についてそれほど知識を有しておらず，ただ，RSA 方式という暗号化方式の存在を知っていたにすぎないのではないかと思われる。

以上から明らかなとおり，引用例（段落【００７３】）の上記記載は，RSA 方式という暗号化方式の存在を示唆するにとどまり，RSA 方式をカードリーダひいてはカード読み取りシステムにおいて採用することを示唆するものではないというべきである。

イ　上記３(2)で主張したとおり，引用発明が高い処理能力を要する暗号化方式を排除していることは，RSA 方式を採用することの阻害要因となる。

(2)　相違点ｂ，ｄについて

審決は，相違点ｂとｄを個別に判断するが，次のとおり適切でない。

引用発明において，通過検知センサが採用されていないのは，磁気ヘッドで暗号化が行われるため，読取りを制御する必要がないからである。つまり，引用発明に通過検知センサを組み合わせる動機を当業者は持たない。このことは，磁気ヘッドで暗号化を行う本願補正発明についてもいえる。

にもかかわらず，本願補正発明が通過検知センサを採用したのは，鍵生成のタイミングを制御するためである。鍵を生成するタイミングが暗号化のタイミングに近ければ近いほど，鍵が保管される時間が短くなる。つまり，鍵の保管期間が短くなれば情報盗用リスクを小さくすることができることから，本願補正発明は，カード読取り時に鍵を生成するように設計されたのである（なお，本願補正発明の構成の場合，鍵生成と暗号化のタイミングはほぼ同時といってよいほど，近接する。）。

したがって，容易想到性の判断は，引用発明を見た当業者が「通過検知センサに

よる読取信号を鍵生成のタイミングとすること」に想到できるかという観点からなされるべきである。審決のように，相違点ｂについて「引用発明に検知システムを組み合わせられるか」をまず検討し，これを肯定した後に，相違点ｄについて，検知システムを組み合わせた引用発明を前提として「読取信号を鍵生成のきっかけとできるか」を検討する方法，すなわち，２段階の検討方法は適当ではない。

そこで，上記観点から検討すると，引用発明には鍵生成のタイミングに配慮する記載はない。したがって，引用発明を見た当業者が鍵生成のタイミングを調整しようとは考えない。また，特許第２６９５４８２号公報（発行日平成９年１２月２４日。甲２）には通過検知センサの読取信号を鍵生成のきっかけとすることを示唆する記載はない。したがって，「通過検知センサによる読取信号を鍵生成のタイミングとすること」を示唆する記載は，引用発明にも特許第２６９５４８２号公報（甲２）にもないというべきである。

(3)　有利な効果の参酌について

引用発明はカードリーダ内部における通信の安全を確保するにとどまるのに対し，本願補正発明はカードリーダ外部も含めたシステム全体における通信の安全を確保できるという格別の効果を有する。具体的にいうと， CAT 端末本体を不正に開くという犯罪に対して，引用発明は対応できないが，本願補正発明は対応できるという格別の効果を有する。カードリーダ内部におけるリスクとカードリーダ外部におけるリスクは全く性質が異なり，また，CAT 端末本体を不正に開くという課題及びこれに対する対応を示唆する記載は引用発明にはないから，当業者が上記効果を引用発明から十分に予測できたということはできない。

したがって，この点も参酌して，本願補正発明の進歩性が肯定されるべきである。

(4)　商業的成功

本願補正発明を実施して原告が製作している磁気カード読み取りシステム（クリプトヘッド）は，世界的なクレジットカード会社である VISA 社との提携の下，チケット管理システムに採用され，また，富士通の関連会社である富士通フロンテッ

ク株式会社でも採用された。以上の商業的成功から，本願補正発明の進歩性を肯定的に推認すべきである。

第４　被告の主張

１　取消事由１に対し

本願補正発明の特許請求の範囲には，「コンピュータ」をクレジット会社等のサーバに限定する旨の記載はない。

また，補正明細書における従来の技術，発明が解決しようとする課題，発明の効果の記載をみても，本願補正発明がカードリーダからクレジットカード会社等のサーバまでにおける通信の安全を達成しようとするものである旨の記載はない。

補正明細書の実施例の記載についても，磁気カード読み取りシステム１Ａの「パーソナルコンピュータ」や，システム１Ｂの「ホストコンピュータ」(「パーソナルコンピュータ」）がクレジット会社等のサーバを指す旨の記載はない。

以上のとおりであるから，原告が主張するように，本願補正発明が，カードリーダからクレジットカード会社等のサーバまでにおける通信の安全を達成しようとするものであり，本願補正発明にいう「コンピュータ」はクレジット会社等のサーバを指しており，本願補正発明における暗号鍵の生成はサーバで行われると解する余地はなく，審決の本願補正発明の認定に誤りはない。

２　取消事由２に対し

(1)　本願補正発明にいう「コンピュータ」をクレジット会社等のサーバに限定して解すべき根拠はないから，本願補正発明と対比すべき引用発明について，情報処理部とカードセンタとの間の構成，動作を認定する必要はない。

(2)　引用例は，段落【００３４】～【００７０】において，第１ないし第３実施形態として，暗号化方式としてデータ暗号化規格（DES）を用いたものを説明している。その上で，段落【００７２】～【０１００】おいて，データ暗号化規格（DES）に代わるものとして，データ暗号化規格（DES）と同様の安全性を有し，処理能力

が格別高くないチップでも短時間に暗号化が行える暗号化方式について説明している。

したがって，暗号化方式としてデータ暗号化規格（DES）を用いたものを一つの独立した技術思想として把握でき，暗号化方式としてデータ暗号化規格（DES）を用いたもののみを引用発明として認定することは十分可能である。データ暗号化規格（DES）と同様の安全性を有し，処理能力が格別高くないチップでも短時間に暗号化が行える暗号化方式を用いるものまでも含めて引用発明を認定する必要はない。

３　取消事由３に対し

取消事由３についての原告の主張は，取消事由１及び２についての原告の主張が相当であることを前提としている。前述したように，取消事由１及び２についての原告の主張は失当であるから，取消事由３についての原告の主張は，その前提を欠き，失当である。

４　取消事由４に対し

(1)　相違点ｃにつき

引用例においては，まず，データ暗号化規格（DES）に代えて，RSA 方式，FEAL 方式等を採用し得ることが記載され，次いで，DES 方式，RSA 方式，FEAL 方式と同様の安全性を有し，処理能力が格別高くないチップでも短時間に暗号化が行える暗号化方式について説明することが記載されている。

したがって，引用例に，DES 方式，RSA 方式，FEAL 方式と同様の安全性を有し，処理能力が格別高くないチップでも短時間に暗号化が行える暗号化方式について説明があることをもって，引用発明において，データ暗号化規格（DES）に代えて RSA 方式を採用することの阻害要因とすることはできない。

(2)　相違点ｂ，ｄにつき

ア　一般的に，磁気カードリーダは，カードの移動に合わせて読取りの開始及び停止を制御する必要があるから，引用発明においても，カードの移動に合わせて読

取りの開始及び停止を制御するために，特許第２６９５４８２号公報（甲２）に記載されたような周知の通過検知センサを組み合わせる動機を当業者が持つことは明らかである。

イ　本願補正発明における「鍵」は「公開鍵」及び「秘密鍵」であるが，公開鍵を使用して暗号化された情報を公開鍵を使用して復号化することはできないから，公開鍵を盗取しても，情報を盗用することはできない。公開鍵を使用して暗号化された情報を不正に復号化するためには，復号化を行う装置に不正にアクセスして保管されている秘密鍵を盗取する必要がある。

しかしながら，仮に，復号化を行う装置に不正にアクセスすることができるならば，保管されている秘密鍵を盗取せずとも，復号化された情報を盗取すれば，情報を盗用することができる。

したがって，「公開鍵」と「秘密鍵」を「鍵」とする本願補正発明の場合には，復号化を行う装置における秘密鍵の保管時間の長短と情報盗用リスクの大小との間に直接的な関係はないから，鍵を生成するタイミングをいつにするかは，当業者が適宜選択し得ることである。

(3)　有利な効果の参酌につき

「カードリーダ外部も含めたシステム全体における通信の安全を確保できるという格別の効果」についての原告の主張は，取消事由１についての原告の主張が相当であることを前提としている。前述したように，取消事由１についての原告の主張は失当であるから，「カードリーダ外部も含めたシステム全体における通信の安全を確保できるという格別の効果」についての原告の主張は，その前提を欠き，失当である。

(4)　商業的成功につき

仮に，原告が制作している磁気カード読み取りシステムが商業的に成功しているとしても，他に本願補正発明の進歩性を根拠付けるに足る事実がない本件においては，そのことから，本願補正発明の進歩性を肯定することはできない。

第５　当裁判所の判断

１　本願補正発明の意義

上記第２，２(2)の請求項１の記載，補正明細書の段落【０００１】～【０００７】,【００１５】～【００１７】,【００２０】,【００２１】,【００２４】,【００２６】～【００３５】等の記載によれば，本願補正発明は，磁気カードに記憶されたデータを読み取る磁気カード読取りシステムに関するものであり，従来技術である磁気ヘッド，A/D コンバータ，制御装置（パーソナルコンピュータを含む。）等から構成される磁気カードリーダにおいては，磁気ヘッドと A/D コンバータとを結ぶインターフェイスケーブル及び A/D コンバータと制御装置とを結ぶインターフェイスケーブルからデータが盗取される場合があることから，そのようなデータの盗取を防ぎ，又は盗取されたとしてもデータを使用することができない磁気カード読取りシステムを提供することを目的とするもので，①磁気カードのデータを読み取るコア，②アナログデータをデジタルデータに変換する A/D コンバータ，③データを暗号化する IC（マイクロプロセッサ），④暗号化されたデータを復号化し，かつデータの暗号化・復号化に用いる公開鍵・秘密鍵を生成するデータ制御部（パーソナルコンピュータを含む。）・ホストコンピュータ等から構成され，①～③を合成樹脂の充填されたハウジング内に収容することで，データを盗取する機器の取付けを防止し，データの盗取を困難にし，また，読み取ったデータを公開鍵暗号化方式により暗号化するので，データが不正に盗取されたとしても，その不正使用を防止することができるなどというものであることが認められる。

２　引用発明

引用例（甲１）の段落【０００１】,【０００２】,【０００４】,【００１１】,【００３５】～【００３７】,【００４５】,【００５０】,【００５１】,【００５７】,【００５８】,【図１】等の記載によれば，引用発明は，カードに記録されたカードデータを読み取る磁気ヘッドに関するものであって，磁気カードリーダで読み取ったカ

ードデータの外部への漏出防止を目的とし，①カードのデータを読み取るヘッド本体，② A/D コンバータを内蔵し，データを暗号化する１チップマイクロコンピュータからなる制御部，③暗号化されたデータを復号化し，かつデータの暗号化・復号化に用いる鍵を生成する本体制御部（マイクロコンピュータを含む。）等から構成され，①及び②をエポキシ樹脂等の充填されたヘッド容器内に収容することや，共通鍵方式により暗号化されたデータを送信することで，データの安全性を確保するものであることが認められる。

３　取消事由１（本願補正発明の認定の誤り）について

原告は，審決における本願補正発明の認定について，本願補正発明の「コンピュータ」はクレジット会社等のサーバを指し，暗号鍵の生成はサーバで行われるもので，「磁気カード読み取りシステム」はカードリーダからクレジットカード会社等のサーバまでのシステム全体を対象とするものであることを理解していない点で誤りがある旨主張する。

しかし，①本件補正による請求項１には，単に「コンピュータ」と特定されているだけで，これがクレジット会社等のサーバを指す旨の記載はなく，②補正明細書の発明の詳細な説明においても，実施例の一つで「ホストコンピュータ」の語が用いられているにとどまり，本願補正発明の「コンピュータ」全体又は他の実施例の「データ制御部」（コンピュータを含む。）がクレジット会社等のサーバを指す旨の記載はなく，③同じく発明の詳細な説明において，磁気ヘッド，A/D コンバータ，制御装置（パーソナルコンピュータを含む。）等から構成される磁気カードリーダを従来技術と位置付け，その中の磁気ヘッドと A/D コンバータとを結ぶインターフェイスケーブル及び A/D コンバータと制御装置とを結ぶインターフェイスケーブルからデータが盗取されることの防止を解決課題としている，すなわち，そのような従来技術たる磁気カードリーダにおけるデータ盗取防止を本願補正発明の解決課題としているのであって，カードリーダとサーバとの間を含むシステム全体におけるデータ盗取防止を発明の目的とする旨の記載はない。

これらの点に照らすと，原告の主張する点を考慮してもなお，原告の上記主張は補正明細書の記載に基づかないものというべきであって，採用することができない。

したがって，取消事由１には理由がない。

４　取消事由２（引用発明の認定の誤り）について

(1)　原告は，審決が，引用発明について，カードリーダが読み取ったデータをカードセンタ等へ送信するための通信回線等の構成を認定していないことが誤りである旨主張する。

原告の上記主張は，取消事由１の主張，すなわち本願補正発明がクレジット会社等のサーバまでのシステム全体を対象とする発明であるという主張を前提として，引用発明においても，クレジット会社等のサーバに相当する「カードセンタ」までの構成を認定すべきというものであるが，上記３で説示したとおり，本願補正発明の認定に関する原告の主張は採用できないから，原告の上記主張はその前提を欠く。そうすると，本願補正発明との対比に当たっては，引用発明についても暗号化されたカードデータが復号化されるまでの構成を認定すれば足りるのであって，復号化された後の構成である通信回線等の構成は対比に不要である。

したがって，審決の認定に誤りはなく，原告の上記主張は理由がない。

(2)　原告は，引用発明について，DES 方式と同様の安全性を有し，処理能力が格別高くないチップでも短時間に暗号化が行える共通鍵方式を用いるとされている点を認定すべきと主張する。

しかし，進歩性の判断に当たっては，公知文献に記載された複数の技術思想・構成をすべて認定する必要はなく，対比に必要な範囲の構成を認定すれば足りる。引用例には，カードデータの暗号化方式として共通鍵方式の一種である DES 方式を用いた構成がひとまとまりの技術思想として記載されているのであって，その範囲で引用発明を認定した審決の判断に誤りはない。

したがって，原告の上記主張も採用することができない。

以上のとおり，取消事由２は理由がない。

５　取消事由３（一致点認定の誤り及び相違点の看過）について

原告は，審決の一致点認定に誤りがあり，また，相違点ｅ，ｆを認定しなかった点も誤りであると主張する。

しかし，原告の上記主張は，取消事由１及び２における主張が認められることを前提とするものであって，上記３及び４のとおり，取消事由１及び２に関する原告の主張は理由がないから，取消事由３に関する原告の主張も，その前提を欠き，理由がない。

６　取消事由４（相違点に関する判断の誤り）について

(1)　相違点ｃについて

公開鍵方式の暗号化方式の一種である RSA 方式は周知技術であるところ，引用例の段落【００７１】には，「…カードデータ…暗号化する手法としてデータ暗号化規格（DES）を用いたが，RSA 暗号化方式…等を採用してもよい。」との記載があり，RSA 方式を適用することの直接的な示唆がある。したがって，このような示唆に基づき，引用発明に周知技術である RSA 方式を適用し，本願補正発明の相違点ｃに係る構成とすることは，当業者が容易になし得たというべきであり，この点に関する審決の判断に誤りはない。

原告は，引用発明は高い処理能力を要する暗号化方式を排除しており，引用例に RSA 方式について記載されていたとしても，その採用は念頭に置かれていなかったなどと主張する。

しかし，引用例においては，まず，暗号化方式として DES 方式を用いた３種の実施例が記載され（段落【００３４】～【００７０】），それ以外にも RSA 方式，FEAL 方式等を採用してもよいとした上（段落【００７１】），これらの DES 方式，RSA 方式，FEAL 方式では，アルゴリズムが非常に複雑なため，制御部の処理能力が低いと問題が生じ得ることから，DES 方式と同様の安全性を有し，処理能力が格別高くないチップでも短時間に暗号化が行える方式を用いた実施例を説明しているのであって（段落【００７２】～【０１００】），処理能力の高いチップの使用を前提とする DES

方式等による構成と，処理能力が格別高くないチップでも短時間に暗号化が行える方式を用いた構成とは別個の構成というべきであるし，引用発明が RSA 方式等の処理能力が高いチップを必要とする構成を排除するものでもないというべきである。このように，引用発明が高い処理能力を要する暗号化方式を排除したものとは認められず，原告の上記主張は採用することができない。

(2)　相違点ｂ，ｄについて

原告は，本願補正発明について，鍵を生成するタイミングを制御し，鍵が保管される時間が短くなるよう通過検知センサを採用したのであるから，相違点ｂとｄを一体として判断すべきと主張する。

しかし，補正明細書によれば，本願補正発明は，秘密鍵を生成・保管するコンピュータにおいてデータの復号化が行われるものであることが認められるところ，コンピュータに侵入するなどして秘密鍵を盗取することが可能であるなら，秘密鍵により復号化された情報を盗取すれば足りることになるから，秘密鍵の生成から使用までの期間を短縮するために通過検知センサを用いても，データの安全性が高まるわけではない。また，暗号化に用いる公開鍵は，技術常識に照らし，そもそも秘密にされる必要はないものであるから，その盗取を防止する必要はなく，そのために保管期間を短くする必要もない。

したがって，秘密鍵，公開鍵のいずれについても鍵の保管期間の長短は問題とはならず，その点から相違点ｂ，ｄを一体として判断すべきとする原告の上記主張は採用することができない。

そして，相違点ｂについて，カードを通過検知センサで検知することによりデータの読取りを制御することは，特許第２６９５４８２号公報（甲２）に記載されたとおり周知技術であり，引用発明は，カードの移動によりカードデータを読み取るものであるから（段落【００４２】），カードの移動を何らかの手段で検出して読取りを行う必要があるものである。したがって，上記周知技術を引用発明に適用して，相違点ｂに係る構成とすることは，当業者であれば容易に想到することができるの

であって，相違点ｂに関する審決の判断に誤りはない。

また，相違点ｄについても，鍵を生成するタイミングは当業者が適宜選択し得ることであるといえる。したがって，引用発明において鍵を生成するタイミングを「１個の暗号化されたカードデータを情報処理部へ送信する前」とし，本願補正発明のように，カード挿入信号がコンピュータに入力されるたびに鍵を生成・出力するようにすることは，当業者が容易に想到し得たというべきであって，相違点ｄに関する審決の判断に誤りはない。

(3)　有利な効果の参酌について

原告の主張する本願補正発明の有利な効果は，取消事由１に関する主張を前提とするものであって，取消事由１に理由がないことは上記３で判示したとおりであるから，原告の上記主張も採用することができない。

(4)　商業的成功について

上記のとおり，本願補正発明は，当業者が容易に想到することができたものであるから，仮に原告の製品が商業的成功を収めていたとしても，上記判断を覆すものではなく，原告の主張は採用することができない。

第６　結論

以上によれば，原告主張の取消事由はいずれも理由がない。よって，原告の請求を棄却することとして，主文のとおり判決する。

知的財産高等裁判所 第２部

裁判長裁判官　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

塩　　月　　秀　　平

裁判官　　清　　水　　節

裁判官　　古　　谷　　健　二　郎