審決

不服２０１８－１０２７０

（省略）
請求人　ソニー株式会社

（省略）
代理人弁理士　特許業務法人酒井国際特許事務所

特願２０１７－８６９５１「電子決済システム、情報処理装置、および電子決済管理装置」拒絶査定不服審判事件〔平成２９年７月２０日出願公開、特開２０１７－１２６３８６〕について、次のとおり審決する。

結論
本件審判の請求は、成り立たない。

理由
第１ 手続の経緯
本願は、
平成１３年５月９日（優先権主張 平成１２年５月１０日、平成１３年２月２３日）に特願２００１－１３９１６４号を出願し、
その一部を、平成２３年５月９日に特願２０１１－１０４３２６号として新たに出願し、
その一部を、平成２５年５月２４日に特願２０１３－１０９５５６号として新たに出願し、
その一部を、平成２５年１１月２９日に特願２０１３－２４７６４９号として新たに出願し、
その一部を、平成２７年６月１０日に特願２０１５－１１７４３２号として新たに出願し、
その一部を、平成２９年４月２６日に特願２０１７－０８６９５１号として新たにしたものであって、以降の手続は次のとおりである。
平成３０年１月３０日付け：拒絶理由通知
平成３０年４月　４日　　：意見書、手続補正書の提出
平成３０年５月　９日付け：拒絶査定
平成３０年７月２７日　　：審判請求書、手続補正書の提出
令和　元年７月１２日付け：当審拒絶理由通知
令和　元年９月１３日　　：意見書、手続補正書の提出

第２ 本願発明
令和元年９月１３日付けの手続補正書により補正された特許請求の範囲の請求項１～４には、以下の事項が記載されている（以下、「本願発明１」、

「本願発明２」・・・「本願発明４」、総じて「本願発明」という。）。
「【請求項１】
　情報処理装置と、
　電子決済管理装置と、
　を有し、
　前記情報処理装置は、
　ユーザからの入力に基づいて、クレジットカードによる支払、デビットカードによる支払、または電子マネーによる支払を含む複数の支払い方法の中から、一つの支払い方法を決定する決定部と、
　前記電子マネーによる支払が決定された場合、前記電子マネーによる支払の決定に応じて、金額に関する情報を含む決済要求情報を前記電子決済管理装置に送信する送信部と、
　前記電子決済管理装置から受信した残高読み出し要求を含む決済情報に応じた処理によって、データ記憶装置が当該データ記憶装置内の耐タンパ性メモリから読み出した残高情報を含む決済情報を当該データ記憶装置から取得し、取得した決済情報を前記電子決済管理装置に送信する処理部と、
　を備え、
　前記電子決済管理装置は、
　前記決済要求情報を受信する受信部と、
　前記決済要求情報に基づいて、残高読み出し要求を含む決済情報を生成する生成部と、
　前記残高読み出し要求を含む決済情報を前記情報処理装置に送信する送信部と、
　を備える、電子決済システム。
【請求項２】
　前記電子決済管理装置は、
　前記情報処理装置から受信した残高情報を含む決済情報から生成したログ情報を前記データ記憶装置に書き込むためのログ書き込み情報と、当該残高情報が示す金額から請求額を減算するための減算情報とを含む決済処理要求を生成し、生成した決済処理要求をセッション鍵により暗号化し、暗号化した決済処理要求に対して秘密鍵に基づく署名を付して情報処理装置に送信し、
　前記情報処理装置において、前記秘密鍵に対応する公開鍵を用いて、前記決済要求情報に付与された署名の正当性が検証され、検証結果が正当である場合、データ記憶装置に記憶される残高情報が更新される、請求項１に記載の電子決済システム。
【請求項３】
　前記検証結果が正当である場合、前記データ記憶装置において、共通鍵により前記決済要求情報が復号化され、復号化された前記決済要求情報に含まれる減算情報に基づいて、前記データ記憶装置に記憶された残高情報が更新される、請求項２に記載の電子決済システム。
【請求項４】
　ユーザからの入力に基づいて、クレジットカードによる支払、デビットカー

ドによる支払、または電子マネーによる支払を含む複数の支払い方法の中から、一つの支払い方法を決定する決定部と、
　前記電子マネーによる支払が決定された場合、前記電子マネーによる支払の決定に応じて、金額に関する情報を含む決済要求情報を電子決済管理装置に送信する送信部と、
　前記電子決済管理装置から受信した残高読み出し要求を含む決済情報に応じた処理によって、データ記憶装置が当該データ記憶装置内の耐タンパ性メモリから読み出した残高情報を含む決済情報を当該データ記憶装置から取得し、取得した決済情報を前記電子決済管理装置に送信する処理部と
　を備える、情報処理装置。」

第３　当審の拒絶理由通知書の概要
　当審の拒絶の理由である、令和元年７月１２日付け拒絶理由通知の理由は、概略、次のとおりのものである。
　この出願は、特許請求の範囲の記載が下記の点で、特許法第３６条第６項第１号に規定する要件を満たしていない。

記

１．特許請求の範囲に記載された発明が、発明の詳細な説明に記載された発明であるか否かについて
　（略）

２．特許請求の範囲に記載された発明が、発明の詳細な説明の記載により当業者が当該発明の課題を解決できる範囲のものであるか否か（また、発明の詳細な説明に記載や示唆がなくとも当業者が優先基準日当時の技術常識に照らし当該発明の課題を解決できると認識できる範囲のものであるか否か）について
　本願明細書の発明の詳細な説明には、本願発明に関する技術分野、背景技術及び発明が解決しようとする課題について、【０００１】～【００１０】に鑑みると、当該発明の課題は、共通鍵を保持したＩＣカードなどのデータ記憶装置を用いて、ネットワークを介した電子商取引を安全に行うことができるようにすることであると認められる。
　当該発明の課題を解決するためには、決済管理装置３のセキュリティサーバ３１及びＩＣカードなどのデータ記憶装置２０において、共通鍵KC からセッション鍵KSES が生成され、該セッション鍵KSES を用いて、決済管理装置３と情報処理装置２２との間で送受信される情報、例えば、残高読み出し要求ＢＲＣを含む決済情報や残高情報ＢＩを決済情報が、暗号・復号処理される事項を含むことが必要であると認められる。
　これに対して、特許請求の範囲に記載された発明である、請求項１乃至５に係る発明は、上記技術事項を含んでいないとともに、請求項１乃至５に係る発明により、当該発明の課題を解決できると当業者が認識できるとの技術常識があるとは認められないことから、上記当該発明の課題を解決するための手段が

反映されているとは認められない。
　また、本願明細書の発明の詳細な説明には、上記事項以外に当該発明の課題は記載されておらず、また、優先基準日当時の技術常識に照らしても、本願明細書の発明の詳細な説明の記載から、当該発明により解決される課題を認識できるとは認められない。
　してみると、特許請求の範囲に記載された発明が、発明の詳細な説明の記載により当業者が当該発明の課題を解決できる範囲のもの、或いは、発明の詳細な説明に記載や示唆がなくとも当業者が優先基準日当時の技術常識に照らし当該発明の課題を解決できると認識できる範囲のものであるとは認められない。
　よって、請求項１～５に係る発明は、発明の詳細な説明に記載したものでない。

第４ 本願の発明の詳細な説明の記載
　本願の発明の詳細な説明の記載には、以下の記載がある。
（１）「【技術分野】
　【０００１】
　本発明は、共通鍵を保持したＩＣカードなどのデータ記憶装置を用いて、ネットワークなどを用いた決済処理を安全に行うことができる電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカードなどのデータ記憶装置、コンピュータプログラムおよび記憶媒体に関する。
【背景技術】
　【０００２】
　インターネットなどのオープンネットワークを介した電子商取引を安全に行うために、従来、ＰＫＩ（Ｐｕｂｌｉｃ Ｋｅｙ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ：公開鍵インフラ）プロトコルが採用されている。
　【０００３】
　ＰＫＩプロトコルでは、送信元で秘密鍵を用いて署名情報を作成し、送信元から送信先に、当該署名情報を伝送情報と共に送信する。そして、送信先において、当該秘密鍵に対応する公開鍵を用いて当該署名情報の検証を行うことで、受信した伝送情報が正当な送信元で作成されたものであるか否かを判断する。
　【０００４】
　ところで、近年、ＩＣ（Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）カードを用いて、ネットワークを介した電子商取引を行う試みがある。ここで、通常、ＩＣカードなどのデータ記憶装置は、共通鍵を保持しており、共通鍵暗号方式を用いて秘匿性のある情報の入出力を行う。このようなＩＣカードなどのデータ記憶装置は、共通鍵が署名情報を作成するための鍵とはなり得ないため、ＩＣカードなどのデータ記憶装置を紛失した場合でも、被害を小さくできるという利点がある。
【発明の概要】
【発明が解決しようとする課題】
　【０００５】
　しかしながら、ネットワークを介した電子商取引を安全に行うためには、秘

密鍵を用いて署名情報を作成する必要があるが、従来の手法では、ＩＣカードなどのデータ記憶装置が秘密鍵を保持（記憶）していないため、署名情報の作成ができないという問題がある。この場合に、ＩＣカードなどのデータ記憶装置に秘密鍵を保持する方法も考えられるが、前述したように、秘密鍵は署名情報を作成できるため印鑑照明と同様の効力があり、ＩＣカードなどのデータ記憶装置を紛失して悪用されたときの被害が大きすぎるという問題がある。

【０００６】

また、上述したようなＩＣカードなどのデータ記憶装置が採用する共通鍵暗号方式のみを用いて、ネットワークを介した電子商取引を行うと、取り引きを行う多数の相手先のサーバ装置などが共通鍵を持つことになり、共通鍵が盗まれたり、悪用される可能性が高くなるという問題もある。

【０００７】

電子決済においては、ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ）やＳＥＴ（Ｓｅｃｕｒｅ Ｅｌｅｃｔｒｏｎｉｃ Ｔｒａｎｓａｃｔｉｏｎ）が多く採用されている。しかし、ＳＳＬでは、クライアント装置と店舗装置間の通信路に対する安全性は保証されるが、店舗側の不正を検出できないという問題がある。

【０００８】

また、ＳＥＴでは、ＳＳＬの利点とクライアント装置、店舗装置、決済管理装置で改ざんができないという利点とを併せ持つが、各装置がＰＫＩの証明書を持たなければならないため、煩雑であり費用がかかり、さらに署名および署名検証を何度も行わなければならず冗長であるという問題がある。

【０００９】

さらに、電子商取引システムにおいては、ユーザがクライアント装置上で確認した価値情報が、実際にＩＣカードなどのデータ記憶装置に書き込まれる価値情報と同じであるかどうかを確認する手段を持っていなかった。

【００１０】

本発明は上述した問題点に鑑みてなされ、共通鍵を保持したＩＣカードなどのデータ記憶装置を用いて、ネットワークを介した電子商取引を安全に行うことができる電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカードなどのデータ記憶装置、コンピュータプログラムおよび記憶媒体を提供することを目的とする。」

（２）「【００５８】

「電子決済システム」は、インターネットなどのオンライン通信系を介して商品やサービスの販売を行った場合に、代金決済を電子的にオンライン通信系を介して行うシステムである。オンライン通信系を介して決済を行う方法としては、クレジットカードやキャッシュカードやデビットカードによる支払い、プリペイドカードなどの電子マネーによる支払いが可能である。」

（３）「【００８５】

ＩＣカードなどのデータ記憶装置２０は、例えば、プラスチックなどのカー

ドにＩＣチップが埋め込まれているものである。ＩＣカードなどのデータ記憶装置２０は、図２（Ａ）に示すように耐タンパ性のＩＣモジュール５０を有し、図２（Ｂ）に示すように当該ＩＣモジュール５０内に処理回路５１およびメモリ５２を内蔵している。」

（４）「【０１１４】
「決済情報」は、決済管理装置３が店舗装置４から決済管理装置３に送信された決済要求情報に基づいて作成するもので、決済管理装置３からクライアント装置であるパーソナルコンピュータ２２およびリーダライタ２１を介してＩＣカードなどのデータ記憶装置２０に記憶された価値情報を増減することにより決済を行うための各種情報が含まれる。この決済情報のセキュリティは、決済管理装置３とＩＣカードなどのデータ記憶装置２０との間で共用される共通鍵により確保される。さらに、決済情報の正当性は、決済管理装置３の秘密鍵を用いて作成された第２署名を付し、クライアント装置であるパーソナルコンピュータ２２がその第２署名を決済管理装置３の秘密鍵に対応する公開鍵を用いて検証することにより確保される。」

（５）「【０１３６】
次に、図９～図１１を参照しながら、共通鍵、公開鍵、および電子署名を用いたセキュリティの高い本実施の形態にかかる電子決済システムおける商品情報伝送シーケンスおよび価値情報伝送シーケンスについて、詳細に説明する。
（中略）
【０１４１】
ステップＳＴ１：
パーソナルコンピュータ２２とネットワークサーバ４０との間でＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ）を用いたサーバ認証または相互認証を行い、セキュアな通信路を確立する。
【０１４２】
ステップＳＴ２：
ユーザ２が、図１２に示すような商品選択画面において、パーソナルコンピュータ２２のキーボードやマウスなどを操作して購入を希望する商品を決定すると、それに応じた商品決定情報がパーソナルコンピュータ２２からネットワークサーバ４０に送信される。
【０１４３】
ステップＳＴ３：
ネットワークサーバ４０は、パーソナルコンピュータ２２から商品決定情報を受けると、その見積もり情報をパーソナルコンピュータ２２に送信する。
【０１４４】
ステップＳＴ４：
パーソナルコンピュータ２２は、図１３に示すように、ネットワークサーバ４０から受けた見積もり情報をディスプレイに表示する。ユーザ２は、当該見積もりに同意した場合には、図１４に示す画面において、支払い方法を選択す

る。ユーザ２が、パーソナルコンピュータ２２のキーボードなどを操作して電子マネーを利用した決済を選択すると、請求額要求がネットワークサーバ４０に送信される。

【０１４５】

ステップＳＴ５：

ネットワークサーバ４０は、パーソナルコンピュータ２２から請求額要求を受けると、店舗装置４がユーザ２に請求する金額を示す決済要求情報と、当該決済要求情報に対して店舗装置４の秘密鍵ＫSHOP,S を用いて作成した第１署名情報ＳＩＧ１と、インタフェースプログラム２４とをパーソナルコンピュータ２２に送信する。

【０１４６】

ステップＳＴ６：

パーソナルコンピュータ２２は、図１５に示すように、ステップＳＴ５でネットワークサーバ４０から受信した決済要求情報が示す金額をディスプレイに表示する。

【０１４７】

ステップＳＴ７：

ステップＳＴ６でディスプレイに表示された金額に同意したユーザ２がパーソナルコンピュータ２２のキーボードなどを用いて所定の指示を出すと、ステップＳＴ５でネットワークサーバ４０から受信したインタフェースプログラム２４が起動される。

【０１４８】

そして、図１６に示すような画面表示にしたがって、ユーザ２がＩＣカードなどのデータ記憶装置２０をリーダライタ２１にかざすと、パーソナルコンピュータ２２は、起動されたインタフェースプログラム２４を用いて、決済管理装置３のアプリケーションサーバ３０との間でＳＳＬを用いたサーバ認証または相互認証を行い、セキュアな通信路を確立する。

【０１４９】

本実施の形態にかかる決済システムにおいて決済処理が行われている間は、パーソナルコンピュータ２２のディスプレイには、図１７に示すように、ユーザに待機を促すような画面が表示される。

【０１５０】

ステップＳＴ８：

パーソナルコンピュータ２２は、ステップＳＴ５で店舗装置４のネットワークサーバ４０から受信した決済要求情報と、当該決済要求情報に対する第１署名情報ＳＩＧ１とを含む決済要求情報を決済管理装置３のアプリケーションサーバ３０に送信する。

【０１５１】

ステップＳＴ９：

アプリケーションサーバ３０は、例えば、情報管理サーバ３２から読み出した店舗装置４の秘密鍵に対応する公開鍵ＫSHOP,P を用いて、ステップＳＴ８で受信した第１署名情報ＳＩＧ１を検証し、当該第１署名情報ＳＩＧ１が店舗

装置４のネットワークサーバ４０において付された正当なものであると判断すると、ステップＳＴ１０の処理を行う。

【０１５２】

なお、アプリケーションサーバ３０は、第１署名情報ＳＩＧ１が不正なものであると判断した場合には、例えば、パーソナルコンピュータ２２に対してのその旨を通知した後、処理を終了する。

【０１５３】

ステップＳＴ１０：

次いで、決済管理装置３のアプリケーションサーバ３０は、例えば、決済要求情報をセキュリティサーバ３１に送信する。

【０１５４】

ステップＳＴ１１：

セキュリティサーバ３１は、ＩＣカードなどのデータ記憶装置２０から決済要求情報を受けると、アプリケーションサーバ３０との間で相互認証を行い、ＩＣカードなどのデータ記憶装置２０との間で用いる共通鍵KC からセッション鍵KSES を生成する。ＩＣカードなどのデータ記憶装置２０でも、同様に、共通鍵KC からセッション鍵KSES を生成する。

【０１５５】

ステップＳＴ１２：

セキュリティサーバ３１は、決済情報を生成し、これをセッション鍵KSESで暗号処理を施してアプリケーションサーバ３０に出力する。その際に、セキュリティサーバ３１は、決済管理装置の秘密鍵を用いて作成した第２署名を付す。

【０１５６】

アプリケーションサーバ３０は、セキュリティサーバ３１から入力した残高読み出し要求（ＢＲＣ）を含む決済情報をパーソナルコンピュータ２２に送信する。

【０１５７】

パーソナルコンピュータ２２は、アプリケーションサーバ３０から受信した残高読み出し要求ＢＲＣを含む決済情報をリーダライタ２１を介してＩＣカードなどのデータ記憶装置２０に出力する。

【０１５８】

ステップＳＴ１３：

ＩＣカードなどのデータ記憶装置２０は、パーソナルコンピュータ２２からの残高読み出し要求ＢＲＣを含む決済情報が入力されると、これをステップＳＴ１１で生成したセッション鍵KSES を用いて復号する。

【０１５９】

そして、ＩＣカードなどのデータ記憶装置２０は、残高読み出し要求ＢＲＣを含む決済情報に応じた処理回路５１の処理によって、ＩＣカードなどのデータ記憶装置２０内の耐タンパ性のメモリ５２から残高情報ＢＩを含む決済情報を読み出し、これをセッション鍵KSES を用いて暗号処理を施した後に、パーソナルコンピュータ２２に出力する。

【０１６０】
パーソナルコンピュータ２２は、ＩＣカードなどのデータ記憶装置２０からの残高情報ＢＩを含む決済情報をアプリケーションサーバ３０に送信する。
【０１６１】
アプリケーションサーバ３０は、パーソナルコンピュータ２２から受信した残高情報ＢＩを決済情報をセキュリティサーバ３１に出力する。
【０１６２】
セキュリティサーバ３１は、アプリケーションサーバ３０から入力した残高情報ＢＩを含む決済情報をセッション鍵KSES を用いて復号し、ログ情報を生成する。」

第５ 判断
上記第４（１）に摘記した事項によれば、本願発明は、
技術分野を、「共通鍵を保持したＩＣカードなどのデータ記憶装置を用いて、ネットワークなどを用いた決済処理を安全に行うことができる電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカードなどのデータ記憶装置、コンピュータプログラムおよび記憶媒体に関する」ことにし、
発明が解決しようとする課題を、
（ア）「従来の手法では、ＩＣカードなどのデータ記憶装置が秘密鍵を保持（記憶）していないため、署名情報の作成ができないという問題」、
（イ）「ＩＣカードなどのデータ記憶装置に秘密鍵を保持する方法」では「秘密鍵は署名情報を作成できるため印鑑照明と同様の効力があり、ＩＣカードなどのデータ記憶装置を紛失して悪用されたときの被害が大きすぎるという問題」、
（ウ）「ＩＣカードなどのデータ記憶装置が採用する共通鍵暗号方式のみを用いて、ネットワークを介した電子商取引を行うと、取り引きを行う多数の相手先のサーバ装置などが共通鍵を持つことになり、共通鍵が盗まれたり、悪用される可能性が高くなるという問題」、
（エ）電子決済の多くで採用されるＳＳＬでは、「店舗側の不正を検出できないという問題」、
（オ）電子決済の多くで採用されるＳＥＴでは、「各装置がＰＫＩの証明書を持たなければならないため、煩雑であり費用がかかり、さらに署名および署名検証を何度も行わなければならず冗長であるという問題」及び
（カ）「電子商取引システムにおいては、ユーザがクライアント装置上で確認した価値情報が、実際にＩＣカードなどのデータ記憶装置に書き込まれる価値情報と同じであるかどうかを確認する手段を持っていなかった」ことにし、
この問題点に鑑みて、発明の目的を、「共通鍵を保持したＩＣカードなどのデータ記憶装置を用いて、ネットワークを介した電子商取引を安全に行うことができる電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカードなどのデータ記憶装置、コンピュータプログラムおよび記憶媒体を提供すること」にしている。
ここで、本願における発明の目的である「共通鍵を保持したＩＣカードなど

のデータ記憶装置を用いて、ネットワークを介した電子商取引を安全に行うことができる電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカードなどのデータ記憶装置、コンピュータプログラムおよび記憶媒体を提供すること」について、「ネットワークを介した電子商取引を安全に行うことができる電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカードなどのデータ記憶装置、コンピュータプログラムおよび記憶媒体を提供する」ために、「共通鍵を保持したＩＣカードなどのデータ記憶装置を用い」ることを目的しているとの解釈と、「共通鍵を保持したＩＣカードなどのデータ記憶装置を用い」ることを前提として、「ネットワークを介した電子商取引を安全に行うことができる電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカードなどのデータ記憶装置、コンピュータプログラムおよび記憶媒体を提供すること」を目的としているとの解釈が文言上は可能である。

しかしながら、上記（イ）では、「共通鍵を保持したＩＣカードなどのデータ記憶装置を用い」ても、「ネットワークを介した電子商取引を安全に行うことができる電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカードなどのデータ記憶装置、コンピュータプログラムおよび記憶媒体を提供する」上で問題点があることを示していることから、前者の解釈は成り立たず、本願発明では、「共通鍵を保持したＩＣカードなどのデータ記憶装置を用い」ることを前提として、「ネットワークを介した電子商取引を安全に行うことができる電子決済システム、決済管理装置、店舗装置、クライアント装置、ＩＣカードなどのデータ記憶装置、コンピュータプログラムおよび記憶媒体を提供すること」を目的としている解釈するのが妥当である。

そして、上記の課題や目的に対応する事項として、発明の詳細な説明には、上記第４（５）に摘記したように、

ア　パーソナルコンピュータ２２と決済管理装置３との間で、ＳＳＬを用いたサーバ認証または相互認証によるセキュアな通信路が確立されること、

イ　「パーソナルコンピュータ２２は」、「決済要求情報と、当該決済要求情報に対する第１署名情報ＳＩＧ１とを含む決済要求情報を決済管理装置３」に送信すること、

ウ　「決済管理装置」は、「ＩＣカードなどのデータ記憶装置２０との間で用いる共通鍵KC から」生成した「セッション鍵KSES で暗号処理を施し」、「決済管理装置の秘密鍵を用いて作成した第２署名を付」した「残高読み出し要求（ＢＲＣ）を含む決済情報をパーソナルコンピュータ２２に送信」すること、

エ　「パーソナルコンピュータ２２」は、「残高読み出し要求ＢＲＣを含む決済情報」を「セッション鍵KSES を用いて復号」し、「残高読み出し要求ＢＲＣを含む決済情報に応じた処理回路５１の処理によって、ＩＣカードなどのデータ記憶装置２０内の耐タンパ性のメモリ５２から残高情報ＢＩを含む決済情報を読み出」すこと、

オ　「パーソナルコンピュータ２２」は、ＩＣカードなどのデータ記憶装置２

０内の耐タンパ性のメモリ５２から読み出した「残高情報ＢＩを含む決済情報」をセッション鍵ＫSES を用いて暗号処理を施し」て、「残高情報ＢＩを含む決済情報を」決済管理装置に送信すること
が記載されている。

これに対して、本願発明では、上記第２に摘記した事項からみて、「残高読み出し要求を含む決済情報に応じた処理によって、データ記憶装置が当該データ記憶装置内の耐タンパ性メモリから読み出した残高情報を含む決済情報を当該データ記憶装置から取得し、取得した決済情報を前記電子決済管理装置に送信する」こと、すなわち、発明の詳細な説明に記載された上記エについては特定されているものの、その他の上記ア～ウ、オについては特定されていない。
そして、内部に秘密鍵や共通鍵を保持したメモリは「耐タンパ性のメモリ」であることに鑑みると、上記エの事項は本願発明が問題とする従来技術に相当し、上記（イ）及び（ウ）の問題を内在するものであるから、上記エの事項により本願発明の課題が解決されるとは認められない。

さらに、本願明細書の発明の詳細な説明には、上記した課題以外に当該発明の課題は記載されておらず、出願基準日当時の技術常識に照らしても、本願明細書の発明の詳細な説明の記載から、当該発明により解決される課題を認識できるとは認められない。

してみると、本願発明が、発明の詳細な説明の記載により当業者が当該発明の課題を解決できる範囲のもの、或いは、発明の詳細な説明に記載や示唆がなくとも当業者が出願基準日当時の技術常識に照らし当該発明の課題を解決できると認識できる範囲のものであるとは認められない。
よって、本願発明は、発明の詳細な説明において、発明の課題が解決できることを当業者が認識できるように記載された範囲を超えるものであって、特許法３６条６項１号の規定を満たしていない。

第６　審判請求人の主張の検討
１　審判請求人の主張
審判請求人は、令和元年９月１３日の意見書において、
「〔４〕拒絶理由に対する意見
（中略）
また、上記補正により、本願発明は、発明の詳細な説明の記載により、少なくとも、「複数の支払い方法の中から選択できる（段落００５８）」ことによりユーザの利便性を向上させるという効果を期待できるとともに、「耐タンパ性のＩＣモジュール５０を利用することによりセキュリティが向上する（段落００８５）」という効果を期待でき、ユーザ利便性及びセキュリティの面における課題を解決できるものと思料致します。」と主張している。

２　検討

本願明細書の段落【００５８】及び【００８５】に記載された事項は、上記第４（２）及び同（３）に摘記された事項であって、「オンライン通信系を介して決済を行う方法としては、クレジットカードやキャッシュカードやデビットカードによる支払い、プリペイドカードなどの電子マネーによる支払いが可能である」こと、及び、「ＩＣカードなどのデータ記憶装置２０は、図２（Ａ）に示すように耐タンパ性のＩＣモジュール５０を有」することは記載されている。

しかしながら、本願明細書には、従来の電子決済システムに「ユーザ利便性」の面で課題を有していること、或いは、電子決済システムに用いるＩＣカードに「セキュリティ」の面で課題を有していることは記載されていないとともに、本願発明において、「クレジットカードやキャッシュカードやデビットカードによる支払い、プリペイドカードなどの電子マネーによる支払い」を可能したことでユーザ利便性を向上させ、「耐タンパ性のＩＣモジュール５０を有」するＩＣカードを用いたことでセキュリティを向上させることができたという効果を奏したことは記載されていない。

してみると、審判請求人の上記主張は、本願発明及び本願明細書の記載に基づいた主張ではないことから、該主張を認めることはできない。

第７ むすび

以上のとおり、この出願は、特許請求の範囲の記載が特許法３６条６項１号に規定する要件を満たしていない。

よって、結論のとおり審決する。

令和１年１０月２９日

審判長　特許庁審判官　渡邊 聡
特許庁審判官　佐藤 聡史
特許庁審判官　石川 正二

（行政事件訴訟法第４６条に基づく教示）

この審決に対する訴えは、この審決の謄本の送達があった日から３０日（附加期間がある場合は、その日数を附加します。）以内に、特許庁長官を被告として、提起することができます。

〔審決分類〕Ｐ１８．５３７－ＷＺ（Ｇ０６Ｑ）

審判長　特許庁審判官渡邊　聡　8622
特許庁審判官　石川　正二　8524

特許庁審判官　佐藤　聡史　8943