令和７年１月２７日判決言渡

令和５年（行ケ）第１０１０５号　審決取消請求事件

口頭弁論終結日　令和６年１１月７日

判　　決

原　　告　　ＰａｙＰａｙ株式会社

同訴訟代理人弁護士　　塩　月　秀　平

同　　松　山　智　恵

同　　高　梨　義　幸

同　　松　本　　陸

同訴訟代理人弁理士　　澤　井　光　一

同　　吉　田　幸　二

被　　告　　株式会社アイエスアイ

同訴訟代理人弁護士　　千　且　和　也

同訴訟代理人弁理士　　矢　口　太　郎

同　　尾　城　日奈子

主　　文

１　原告の請求を棄却する。

２　訴訟費用は、原告の負担とする。

事　実　及　び　理　由

第１　請求

特許庁が無効２０２２－８０００２８号事件について令和５年８月７日にした審決を取り消す。

第２　事案の概要

１　特許庁における手続の経緯等

⑴　被告は、平成２４年（２０１２年）１０月１１日（優先権主張平成２３年（２０１１年）１０月２５日、日本国）を国際出願日とする特許出願（特願２０１３－５４０７２０号、以下「最初の原出願」という。）の一部を、平成２７年１２月１０日に新たな特許出願とした（特願２０１５－２４０７６３号。以下「第１世代出願」という。）。（甲１３）

⑵　被告は、さらに、第１世代出願の一部を分割し、平成２９年１月１９日、発明の名称を「電子マネー送金方法およびそのシステム」とする新たな特許出願（特願２０１７－７１５０号）をした（以下、この出願を「本件出願」という。本件出願の願書並びに願書に添付した明細書、特許請求の範囲、図面及び要約書は別紙１のとおりであり、このうち明細書及び図面を併せて「本件明細書等」という。本件出願の時点での請求項の数は４０であった。甲１８）。被告は、同年２月２０日、出願審査請求書を提出するとともに、手続補正書を提出し、特許請求の範囲を補正して、請求項の数を１とした。さらに、被告は、同年５月９日、手続補正書を提出し、特許請求の範囲を補正して、請求項の数を５とした（以下、同日の手続補正書による手続補正を「本件補正」という。甲１９）。

⑶　被告は、その後、本件出願について特許査定を受け、平成３０年３月１６日、特許権の設定登録を受けた（特許第６３０６２２７号。以下、この特許を「本件特許」という。請求項の数５。）。

⑷　原告は、令和４年３月３１日、本件特許の請求項２ないし５に係る発明（以下、本件特許の請求項２ないし５に記載された発明を、その請求項の番号に応じてそれぞれ「本件発明２」ないし「本件発明５」といい、これらの発明を併せて「本件各発明」という。）についての特許を無効とすることを求める無効審判請求をした（無効２０２２－８０００２８号事件。以下「本件無効

審判請求」という。)。

⑸　特許庁は、令和５年８月７日、「本件審判の請求は、成り立たない。」との審決（以下「本件審決」という。）をし、その謄本は、同月２１日、原告に送達された。

⑹　原告は、令和５年９月１９日、本件審決の取消しを求めて本件訴えを提起した。

２　特許請求の範囲の記載

本件特許の特許請求の範囲の請求項２ないし５（本件各発明）の記載は、次のとおりである（分説記号は、本件審判請求の審判請求書及び本件審決に記載されたとおりである。)。

⑴　請求項２（本件発明２）

２Ａ　第１ユーザが有する第１ユーザ端末（Ａ）と、第２ユーザが有する第２ユーザ端末（Ｂ）と、前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）と通信回線を介して通信可能であり、前記第１ユーザの電子マネーと前記第２ユーザの電子マネーをそれぞれ記憶する電子マネー管理サーバ（３００）とを用いて、前記第１ユーザから前記第２ユーザへの電子マネーの送金を行う電子マネー送金方法であって、

２Ｂ　前記電子マネー管理サーバ(３００)および前記第１ユーザの端末(Ａ)は、前記第１ユーザの情報および／又は前記第１ユーザ端末（Ａ）の情報と関連付けられた第１の証明情報を格納しているものであると共に、前記電子マネー管理サーバ（３００）および前記第２ユーザ端末（Ｂ）は、前記第２ユーザの情報および／又は前記第２ユーザ端末（Ｂ）の情報と関連付けられた第２の証明情報を格納しているものであり、

２Ｃ　この方法は、

２Ｃ－１　前記送金の際、前記第１ユーザ端末（Ａ）が、前記第２ユーザ端末（Ｂ）が出力した、前記第２の証明情報の少なくとも一部の情報である

第２端末情報と、前記第２ユーザが前記第１ユーザから受取る電子マネーの受取額と、を受信し、前記第１ユーザ端末（Ａ）を介して、前記第２端末情報及び前記電子マネーの受取額が前記電子マネー管理サーバに送信されるようになっており、

２Ｃ－２　前記電子マネー管理サーバ（３００）が、

２Ｃ－２－１　前記第１ユーザ端末（Ａ）から、前記第１ユーザ端末（Ａ）の証明情報の少なくとも一部の情報である第１端末情報と、前記第２端末情報とを受信する工程と、

２Ｃ－２－２　前記第１ユーザ端末（Ａ）から受信した前記第１端末情報が前記電子マネー管理サーバ（３００）に格納されている前記第１の証明情報と対応しているか否かの判断と、前記第２端末情報が前記電子マネー管理サーバ（３００）に格納されている前記第２の証明情報と対応しているか否かの判断とを少なくとも行うことにより、前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）の認証を行う認証工程と、

２Ｃ－２－３　前記第１ユーザ端末（Ａ）から、前記第２ユーザへの電子マネーの送金指示と、前記受取額とを受信する工程と、

２Ｃ－２－４　前記第１ユーザ端末（Ａ）から受信した前記受取額が前記電子マネー管理サーバ（３００）に記憶されている前記第１ユーザの電子マネーの残額内であるか否かを少なくとも判断する決済判断工程と、

２Ｃ－２－５　前記決済判断工程において前記残額内であると判断されると、前記電子マネー管理サーバ（３００）内の前記第１ユーザの電子マネーの残額を前記受取額の分だけ減額すると共に、前記電子マネー管理サーバ（３００）内の前記第２ユーザの電子マネーの残額を前記受取額の分だけ増額する決済工程と

を行う

２Ｄ　ことを特徴とする電子マネー送金方法。

⑵　請求項３（本件発明３）

３Ａ　第１ユーザが有する第１ユーザ端末（Ａ）と、第２ユーザが有する第２ユーザ端末（Ｂ）と、前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）と通信回線を介して通信可能であり、前記第１ユーザの電子マネーと前記第２ユーザの電子マネーをそれぞれ記憶する電子マネー管理サーバ（３００）とを有し、前記第１ユーザから前記第２ユーザへの電子マネーの送金を行う電子マネー送金システムであって、

３Ｂ　前記電子マネー管理サーバ(３００)および前記第１ユーザの端末(Ａ)は、前記第１ユーザの情報および／又は前記第１ユーザ端末（Ａ）の情報と関連付けられた第１の証明情報を格納しているものであると共に、前記電子マネー管理サーバ（３００）および前記第２ユーザ端末（Ｂ）は、前記第２ユーザの情報および／又は前記第２ユーザ端末（Ｂ）の情報と関連付けられた第２の証明情報を格納しているものであり、

３Ｃ　このシステムは、

３Ｃ－１　前記送金の際、前記第１ユーザ端末（Ａ）が、前記第２ユーザ端末（Ｂ）の前記第２の証明情報の少なくとも一部の情報である第２端末情報と、前記第２ユーザが前記第１ユーザから受取る電子マネーの受取額とを受信し、この第１ユーザ端末（Ａ）を介して前記第２端末情報及び前記電子マネーの受取額が前記電子マネー管理サーバ（３００）に送信されるようになっており、

３Ｃ－２　前記電子マネー管理サーバ（３００）が、

３Ｃ－２－１　前記第１ユーザ端末（Ａ）から、前記第１ユーザ端末（Ａ）の証明情報の少なくとも一部の情報である第１端末情報と、前記第２端末情報とを受信する手段と、

３Ｃ－２－２　前記第１ユーザ端末（Ａ）から受信した前記第１端末情報が前記電子マネー管理サーバ（３００）に格納されている前記第１の証明情

報と対応しているか否か、および前記第２端末情報が前記電子マネー管理サーバ（３００）に格納されている前記第２の証明情報と対応しているか否かを少なくとも判断することにより、前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）の認証を行う認証手段と、

３Ｃ－２－３　前記第１ユーザ端末（Ａ）から、前記第２ユーザへの電子マネーの送金指示と、前記受取額とを受信する手段と、

３Ｃ－２－４　前記第１ユーザ端末（Ａ）から受信した前記受取額が前記電子マネー管理サーバ（３００）に記憶されている前記第１ユーザの電子マネーの残額内であるか否かを少なくとも判断する決済判断手段と、

３Ｃ－２－５　前記決済判断手段において前記残額内であると判断されると、前記電子マネー管理サーバ（３００）内の前記第１ユーザの電子マネーの残額を前記受取額の分だけ減額すると共に、前記電子マネー管理サーバ（３００）内の前記第２ユーザの電子マネーの残額を前記受取額の分だけ増額する決済手段と

３Ｄ　を有することを特徴とする電子マネー送金システム。

⑶　請求項４（本件発明４）

４Ａ　第１ユーザが有する第１ユーザ端末（Ａ）と、第２ユーザが有する第２ユーザ端末（Ｂ）と、前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）と通信回線を介して通信可能であり、前記第１ユーザの電子マネーと前記第２ユーザの電子マネーをそれぞれ記憶する電子マネー管理サーバ（３００）とを用いて、前記第１ユーザから前記第２ユーザへの電子マネーの送金を行う電子マネー送金方法であって、

４Ｂ　前記電子マネー管理サーバ(３００)および前記第１ユーザの端末(Ａ)は、前記第１ユーザの情報および／又はその情報と関連付けられた第１の証明情報を格納しているものであると共に、前記電子マネー管理サーバ（３００）および前記第２ユーザ端末（Ｂ）は、前記第２ユーザの情報お

よび／又はその情報と関連付けられた第２の証明情報を格納しているものであり、

４Ｃ　この方法は、

４Ｃ－１　前記送金の際、前記第２ユーザ端末（Ｂ）が、前記第１ユーザ端末（Ａ）から前記第１の証明情報の少なくとも一部を受け取り、前記第２ユーザ端末（Ｂ）を介して前記第１の証明情報の少なくとも一部が前記電子マネー管理サーバに送信されるようになっており、

４Ｃ－２　前記電子マネー管理サーバ（３００）が、

４Ｃ－２－１　前記第１の証明情報の少なくとも一部を受け取った第２のユーザ端末（Ｂ）が前記電子マネー管理サーバ（３００）に格納されている前記第２の証明情報と対応しているか否かの判断と、前記第１のユーザ端末（Ａ）が前記電子マネー管理サーバ（３００）に格納されている前記第１の証明情報と対応しているか否かの判断を少なくとも行うことにより、前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）の認証を行う認証工程と、

４Ｃ－２－２　前記第２ユーザから、前記第１ユーザからの電子マネーの受取指示と、受取額とを受信する第３受信工程と、

４Ｃ－２－３　前記第２ユーザから受信した前記受取額が前記電子マネー管理サーバ（３００）に記憶されている前記第１ユーザの電子マネーの残額内であるか否かの判断を少なくとも行う決済判断工程と、

４Ｃ－２－４　前記決済判断工程において前記残額内であると判断されると、前記電子マネー管理サーバ（３００）内の前記第１ユーザの電子マネーの残額を前記受取額の分だけ減額すると共に、前記電子マネー管理サーバ（３００）内の前記第２ユーザの電子マネーの残額を前記受取額の分だけ増額する決済工程と

を行う

４Ｄ　ことを特徴とする電子マネー送金方法。

⑷　請求項５（本件発明５）

５Ａ　第１ユーザが有する第１ユーザ端末（Ａ）と、第２ユーザが有する第２ユーザ端末（Ｂ）と、前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）と通信回線を介して通信可能であり、前記第１ユーザの電子マネーと前記第２ユーザの電子マネーをそれぞれ記憶する電子マネー管理サーバ（３００）とを用いて、前記第１ユーザから前記第２ユーザへの電子マネーの送金を行う電子マネー送金システムであって、

５Ｂ　前記電子マネー管理サーバ(３００)および前記第１ユーザの端末(Ａ)は、前記第１ユーザの情報および／又はその情報と関連付けられた第１の証明情報を格納しているものであると共に、前記電子マネー管理サーバ（３００）および前記第２ユーザ端末（Ｂ）は、前記第２ユーザの情報および／又はその情報と関連付けられた第２の証明情報を格納しているものであり、

５Ｃ　このシステムは、

５Ｃ－１　前記送金の際、前記第２ユーザ端末（Ｂ）が、前記第１ユーザ端末（Ａ）から前記第１の証明情報の少なくとも一部を受け取り、前記第２ユーザ端末（Ｂ）を介して前記第１の証明情報の少なくとも一部が前記電子マネー管理サーバに送信されるようになっており、

５Ｃ－２　前記電子マネー管理サーバ（３００）が、

５Ｃ－２－１　前記第１の証明情報の少なくとも一部を受け取った第２のユーザ端末（Ｂ）が前記電子マネー管理サーバ（３００）に格納されている前記第２の証明情報と対応しているか否か、および前記第１のユーザ端末（Ａ）が前記電子マネー管理サーバ（３００）に格納されている前記第１の証明情報と対応しているか否かを少なくとも判断することにより、前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）の認証を行う認証

手段と、

５Ｃ－２－２　前記第２ユーザから、前記第１ユーザからの電子マネーの受取指示と、受取額とを受信する第３受信手段と、

５Ｃ－２－３　前記第２ユーザから受信した前記受取額が前記電子マネー管理サーバ（３００）に記憶されている前記第１ユーザの電子マネーの残額内であるか否かの判断を少なくとも行う決済判断手段と、

５Ｃ－２－４　前記決済判断手段において前記残額内であると判断されると、前記電子マネー管理サーバ（３００）内の前記第１ユーザの電子マネーの残額を前記受取額の分だけ減額すると共に、前記電子マネー管理サーバ（３００）内の前記第２ユーザの電子マネーの残額を前記受取額の分だけ増額する決済手段と

５Ｄ　を有することを特徴とする電子マネー送金システム。

３　本件無効審判請求に係る審判手続で主張された無効理由

原告は、本件無効審判請求に係る審判手続において、次の無効理由を主張した。

⑴　無効理由１（甲１（中国特許出願公開第１８５１７６２号明細書）に記載された発明を主引用例とする本件発明２及び３の進歩性欠如）

本件発明２及び３は、いずれも、本件出願の優先日（以下「本件優先日」という。）である平成２３年１０月２５日より前の平成１８年（２００６年）１０月２５日に頒布された甲１に記載された発明及び周知技術に基づいて、本件優先日前に本件発明２及び３の属する技術の分野における通常の知識を有する者（当業者）が容易に発明をすることができたものであるから進歩性を欠き、本件発明２及び３に係る特許は、無効とされるべきものである（特許法２９条２項、１２３条１項２号）。

⑵　無効理由２（甲７（国際公開第２０１１／０６５９７４号）に記載された発明を主引用例とする本件発明４及び５の進歩性欠如）

本件発明４及び５は、いずれも、本件優先日である平成２３年１０月２５日より前の同年６月３日に頒布された甲７に記載された発明及び周知技術に基づいて、本件優先日前に当業者が容易に発明をすることができたものであるから進歩性を欠き、本件発明４及び５に係る特許は、無効とされるべきものである（特許法２９条２項、１２３条１項２号）。

⑶　無効理由３（分割要件違反による新規性又は進歩性欠如）

本件出願は、分割要件を満たさず、本件各発明の新規性及び進歩性の判断は、本件出願の現実の出願日である平成２９年１月１９日を基準になされるべきであり、本件各発明は、本件出願の現実の出願日よりも前に公開された、第１世代出願の公開特許公報（甲１３）に記載された発明（以下「甲１３発明」という。）と同一であるから新規性を欠き、また、仮に相違点があったとしても、甲１３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から進歩性を欠き、本件各発明に係る特許は、無効とされるべきものである（特許法２９条１項３号、同条２項、１２３条１項２号）。

⑷　無効理由４（本件発明４及び５に係る特許のサポート要件違反）

本件発明４及び５は、本件明細書等の発明の詳細な説明に記載されていないから、本件発明４及び５に係る特許は、特許法３６条６項１号に規定する要件を満たしていない特許出願に対してされたものであり、無効とされるべきものである（特許法３６条６項１号、１２３条１項４号）。

⑸　無効理由５（本件補正による新規事項追加）

本件発明４及び５を追加する補正は、願書に最初に添付した明細書、特許請求の範囲又は図面に記載した範囲内においてしたものでないから、本件発明４及び５に係る特許は、特許法１７条の２第３項に規定する要件を満たしていない補正をした特許出願に対してされたものであり、本件特許は、無効とされるべきものである（特許法１７条の２第３項、１２３条１項１号）。

４　本件審決の理由等

本件審決の理由の要旨は以下のとおりである。なお、本件審決は、次の⑴から⑸の順に判断している。

⑴　無効理由１（甲１に記載された発明を主引用例とする本件発明２及び３の進歩性欠如）について

ア　甲１に記載された発明（以下「甲１発明」という。）（本件審決第７の１⑴カ、７２ないし７４頁）

「移動端末とレジサービス端末とネットワーク仲介システムを含み、ネットワーク仲介システムはそれぞれ移動端末及びレジサービス端末と通信接続されるモバイル決済システムにより実行されるモバイル決済取引情報処理方法であって、

ネットワーク仲介システムにおいてモバイル決済を実現する装置は、取引情報の画像解析装置及び前記取引情報を処理するための処理装置を含み、処理装置には、サービスプロバイダ情報と対応する口座番号情報、及び移動端末ユーザのIMSI（International Mobile Subscriber Identity：国際移動ユーザ識別コード）情報と対応する口座番号情報といった取引双方の口座番号情報が予め設定され、画像解析装置は画像から具体的な取引情報を解析して処理装置に送信し、処理装置は対応する口座番号情報に基づいて取引を行うものであり、

モバイル決済取引の際に、レジサービス端末はサービスプロバイダ関連情報及び取引内容情報等の取引情報を画像に生成して、後に取引の相手方である移動端末に提供し、当該取引情報には、取引シリアル番号、取引明細及び取引金額等の情報である取引内容情報と、サービスプロバイダのID情報を含むサービスプロバイダ情報や、レジサービス端末の一意の識別情報及びレジサービス端末の番号情報を含むレジサービス端末情報であるサービスプロバイダに関連する身分情報が含まれ、

移動端末は撮像機能又は図形走査機能を備える携帯電話、PDA又はパー

ムトップコンピュータなどであってもよく、撮像機能又は図形走査機能によりレジサービス端末から前記画像を取得すると、取得された画像情報をネットワーク仲介システムに送信し、

ネットワーク仲介システム側には、レジサービス端末の唯一の識別ID、レジサービス端末の番号、口座番号情報を含むレジサービス端末に関する情報と、移動ユーザの身分情報及び口座番号情報とが予め記憶されており、

ネットワーク仲介システムは、ネットワーク装置MSC（Mobile Switching Center：モバイル交換センター）及び／又はHLR（Home Location Register：ホーム位置レジスタ）から移動端末ユーザの身分情報を画像情報とともに受信し、ここで、移動端末ユーザの身分情報は、移動端末のIMSI、移動端末のESN（Electronic serial number：電子シリアル番号であって、移動端末番号MSISDNに唯一に対応する）、移動端末の番号などの情報のうちいずれか一つ又は任意の組み合わせを含むものであり、

ネットワーク仲介システムは、画像情報を受信した後、画像解析装置において解析を行って、サービスプロバイダの関連情報及び取引内容情報の取引情報を取得して、レジサービス端末の身分情報を解析した取引情報から直接抽出し、解析して得られた取引内容情報に基づいて仮取引記録を作成し、

ネットワーク仲介システムは、取得した、買い手である移動端末ユーザの身分情報と、売り手であるレジサービス端末の身分情報を用いて、取引売買双方の身分の正当性を検証し、

ここで、ネットワーク仲介システムは、レジサービス端末の身分情報の検証として、サービスプロバイダID情報を解析した後、対応するサービスプロバイダ情報が登録されているか否かを検索し、存在すれば、解析されたサービスプロバイダが正当であり、そうでなければ、不正であると判定することにより、サービスプロバイダの身分の正当性を検証するとともに、

ユーザ身分情報の検証として、MSC又はHLRから返信されたIMSI情報に基づいて該移動端末ユーザのIMSIと口座番号情報とが予め登録されているか否かを判定し、存在すれば、移動端末ユーザが正当であり、そうでなければ、不正であると判定することにより、移動端末ユーザの身分の正当性を検証するものであり、双方の身分が正当であれば、双方の身分情報に基づいて予め記憶されたデータベースから双方の口座番号情報を呼び出し、

ネットワーク仲介システムは取引情報に基づいて仮取引記録を作成して、移動端末に取引を確認するために、取引金額、取引シリアル番号又は取引明細などの情報が含まれる確認通知を送信し、

移動端末は受信した取引通知が正しいと確認した場合、取引を実行する命令を返信し、

ネットワーク仲介システムは移動端末の確認を受信した後、支払を実行し、仮取引記録を正式な取引記録として確認し、取引ログを記録し、取引が失敗した場合、取引失敗を移動端末に通知する、

モバイル決済取引情報処理方法。」

イ　本件発明２の「証明情報」の技術的意義（本件審決第７の１⑵、７４ないし８０頁）

本件発明２における「証明情報」は、「前記第１ユーザの情報および／又は前記第１ユーザ端末（Ａ）の情報と関連付けられた第１の証明情報」と「前記第２ユーザの情報および／又は前記第２ユーザ端末（Ｂ）の情報と関連付けられた第２の証明情報」であるが、本件明細書等の段落【００１８】、【００１９】、【００２４】、【００５７】ないし【００６１】、【００６８】ないし【００７４】、【００８１】、【図５】及び【図９】の記載によれば、本件発明２の「第１の証明情報」、「第２の証明情報」は、それぞれ、本件明細書等における「第１の電子証明書」、「第２の電子証明書」に対応

し、端末Ａ又は端末Ｂから電子証明書発行の要求を受けて、管理サーバ３００でデジタル署名、公開鍵等を有するように作成され、端末Ａ又は端末Ｂと紐付けて顧客マスタ格納部３５０に格納されるものであって、「端末Ａの製造ＩＤ」のような「個体情報」や、「ユーザＡのログインＩＤ」、「パスワード」、「電子マネー口座番号」とは異なる情報である。

すなわち、本件発明２における「証明情報」は、ユーザ端末から発行の要求を受けて管理サーバで作成される情報であり、認証のためのデジタル署名や公開鍵等を有する電子証明書のような情報であるという技術的意義を有する。そのため、本件発明２における「証明情報」は、ユーザ端末の認証を行う管理サーバで作成されるものではない、ユーザの情報そのものや、ユーザ端末の情報そのものとは異なる情報である。

ウ　本件発明２と甲１発明の一致点、相違点（本件審決第７の１⑶コ、８９ないし９２頁）

(ｱ) 一致点

「第１ユーザが有する第１ユーザ端末（Ａ）と、第２ユーザが有する第２ユーザ端末（Ｂ）と、前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）と通信回線を介して通信可能である管理サーバとを用いて、前記第１ユーザから前記第２ユーザへのマネーの送金を行うマネー送金方法であって、

前記管理サーバおよび前記第１ユーザの端末（Ａ）は、前記第１ユーザ端末（Ａ）の情報を格納しているものであると共に、前記管理サーバおよび前記第２ユーザ端末（Ｂ）は、前記第２ユーザの情報および／又は前記第２ユーザ端末（Ｂ）の情報を格納しているものであり、

この方法は、

前記送金の際、前記第１ユーザ端末（Ａ）が、前記第２ユーザ端末（Ｂ）が出力した、第２端末情報と、前記第２ユーザが前記第１ユー

ザから受取るマネーの受取額と、を取得し、前記第１ユーザ端末（Ａ）を介して、前記第２端末情報及び前記マネーの受取額が前記管理サーバに送信されるようになっており、

前記管理サーバが、

前記第１ユーザ端末（Ａ）から、前記第２端末情報を受信する工程と、

受信した第１端末情報が前記管理サーバに格納されている前記第１ユーザ端末（Ａ）に関する情報と対応しているか否かの判断と、前記第１ユーザ端末（Ａ）から受信した前記第２端末情報が前記管理サーバに格納されている前記第２ユーザ端末（Ｂ）に関する情報と対応しているか否かの判断とを少なくとも行うことにより、前記第１ユーザおよび前記第２ユーザの認証を行う認証工程と、

前記第１ユーザ端末（Ａ）から、前記第２ユーザへのマネーの送金指示を受信する工程と、

を行う

ことを特徴とするマネー送金方法。」

(ｲ) 相違点１－１

本件発明２は、「第１ユーザ」から「第２ユーザ」へ送金されるマネーが「電子マネー」であって、「第１ユーザ」と「第２ユーザ」の「電子マネー」をそれぞれ記憶する「電子マネー管理サーバ（３００）」が、第１ユーザから第２ユーザへの「電子マネーの送金を行う電子マネー送金方法」に関する発明であるのに対し、甲１発明は、「第１ユーザ」から「第２ユーザ」へ送金されるマネーが「電子マネー」であるか定かではなく、また、甲１発明の「管理サーバ」（ネットワーク仲介システム）は、「第１ユーザ」と「第２ユーザ」の「口座番号情報」をそれぞれ記憶するものの、口座のマネー自体を記憶するものではなく、「管理サーバ」が、第

１ユーザから第２ユーザへの「マネーの送金を行うマネー送金方法」に関する発明である点。

(ｳ) 相違点１－２

「管理サーバ」、「第１ユーザ端末（A)」、「第２ユーザ端末（B)」が格納する情報に関して、本件発明２では、電子マネー管理サーバ（３００）および第１ユーザの端末（A）は、「前記第１ユーザの情報および／又は前記第１ユーザ端末(A)の情報と関連付けられた第１の証明情報」を格納し、電子マネー管理サーバ(３００)および第２ユーザの端末(B)は、「前記第２ユーザの情報および／又は前記第２ユーザ端末（B）の情報と関連付けられた第２の証明情報」を格納するのに対し、甲１発明は、管理サーバおよび第１ユーザの端末(A)は、「前記第１ユーザ端末(A)の情報」を格納し、管理サーバおよび第２ユーザの端末（B）は、「前記第２ユーザの情報および／又は前記第２ユーザ端末（B）の情報」を格納するものの、「第１の証明情報」や「第２の証明情報」を格納するものではない点。

(ｴ) 相違点１－３

送金の際の「第１ユーザ端末（A)」の処理に関し、本件発明２は、「前記第２ユーザ端末（B）が出力した、前記第２の証明情報の少なくとも一部の情報である第２端末情報」を受信して、「前記電子マネー管理サーバに送信」するのに対し、甲１発明は、「前記第２ユーザ端末（B）が出力した、第２端末情報」を取得するものの、当該「第２端末情報」は「第２の証明情報の少なくとも一部の情報」ではなく、そのため、甲１発明の「第１ユーザ端末（A)」は、「前記第２の証明情報の少なくとも一部の情報」を「前記第２ユーザ端末（B)」から受信して「管理サーバ」に送信するものでもなく、さらに、本件発明２の「第１ユーザ端末（A)」は、「第２ユーザ端末（B)」が出力した「第２端末情報」と「受取額」

を「受信」するのに対し、甲１発明の「第１ユーザ端末（A)」は、「第２ユーザ端末（B)」が出力した「第２端末情報」と「受取額」の情報を含む「画像情報」を、撮像機能又は図形走査機能を利用して「取得」するのであって、「第２端末情報」と「受取額」を「受信」するものではない点。

(ｵ) 相違点１－４

「管理サーバ」が受信する「第１端末情報」に関して、本件発明２は、「第１ユーザ端末（A)」から「前記第１ユーザ端末（A）の証明情報の少なくとも一部の情報」として受信するものであるのに対し、甲１発明では、「第１端末情報」に相当する「IMSI情報」は「MSC又はHLRから返信された」ものであって、「第１ユーザ端末（A)」である「移動端末」から受信した情報ではなく、また、当該「IMSI情報」は「前記第１ユーザ端末（A）の証明情報の少なくとも一部の情報」ではない点。

(ｶ) 相違点１－５

「認証工程」の認証処理に関して、本件発明２では「受信した前記第１端末情報が前記電子マネー管理サーバ（３００）に格納されている前記第１の証明情報と対応しているか否かの判断」と、「前記第２端末情報が前記電子マネー管理サーバ（３００）に格納されている前記第２の証明情報と対応しているか否かの判断」を行うものであるのに対し、甲１発明においては、「受信した前記第１端末情報」と対応しているか否かの判断は「格納されている前記第１ユーザ端末（A）に関する情報」と行い、「前記第２端末情報」と対応しているか否かの判断は「格納されている前記第２ユーザ端末（B）に関する情報」と行うものであって、「前記第１の証明情報」や「前記第２の証明情報」と対応しているか否かで判断していない点。

(ｷ) 相違点１－６

「認証工程」において認証を行う対象に関して、本件発明２は「前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）の認証を行う」のに対し、甲１発明は「前記第１ユーザおよび前記第２ユーザの認証を行う」ものである点。

(ｸ) 相違点１－７

「前記第１ユーザ端末（Ａ）から、前記第２ユーザへの電子マネーの送金指示を受信する工程」が、本件発明２では、送金指示とともに「受取額」を受信するのに対し、甲１発明では「受取額」は、「送金指示」とは別に、「前記第１ユーザ端末（Ａ）から、前記第２端末情報を受信する工程」において、「レジサービス端末」の「身分情報」とともに受信される点。

(ｹ) 相違点１－８

本件発明２では、「電子マネー管理サーバ（３００）」が「前記第１ユーザ端末（Ａ）から受信した前記受取額が前記電子マネー管理サーバ（３００）に記憶されている前記第１ユーザの電子マネーの残額内であるか否かを少なくとも判断する決済判断工程」を行い、「前記決済判断工程において前記残額内であると判断される」場合に「決済工程」を行うのに対し、甲１発明では、かかる「決済判断工程」は行われず、そのために「決済工程」にかかる処理も「前記決済判断工程において前記残額内であると判断される」場合に行われるものではない点。

エ　本件発明２と甲１発明の相違点に関する容易想到性の判断（本件審決第７の１⑷、９２ないし９３頁）

事案に鑑み、前記相違点のうち相違点１－２、１－３及び１－５について検討すると、甲１発明の「ネットワーク仲介システム」は、「移動端末」から受信した「画像情報」を解析して「サービスプロバイダのＩＤ情報や、レジサービス端末の一意の識別情報及びレジサービス端末の番号情報で

あるサービスプロバイダに関連する身分情報」を取得した後、「対応するサービスプロバイダ情報が登録されているか否かを検索し」、存在するか否かで、売り手であるサービスプロバイダが正当であるか、不正であるかを判定するものである。

しかし、上記「サービスプロバイダに関連する身分情報」に含まれる「サービスプロバイダのＩＤ情報」、「レジサービス端末の一意の識別情報」、「レジサービス端末の番号情報」は、いずれも「第２ユーザの情報」や「第２ユーザ端末（Ｂ）の情報」そのものであって、ユーザ端末の認証を行う管理サーバで作成されるものではなく、ユーザ端末から発行の要求を受けて、認証のためのデジタル署名や公開鍵等を有するように作成されるものでもなく、本件発明２の「証明情報」の技術的意義を有するものではないから、「前記第２ユーザの情報および／又は前記第２ユーザ端末（Ｂ）の情報と関連付けられた第２の証明情報」であるということはできない。そして、甲１発明の「移動端末」において、そのような「第２の証明情報」を、「レジサービス端末」から受信して「ネットワーク仲介システム」へ送信することが、当業者にとって容易に想到し得たことであるともいえない。

さらに、甲１発明の「サービスプロバイダに関連する身分情報」又は「レジサービス端末の身分情報」を用いて「身分の正当性を検証」する処理は、本件発明２のように「前記第２端末情報が前記電子マネー管理サーバ（３００）に格納されている前記第２の証明情報と対応しているか否かの判断」によって「前記第２ユーザ端末（Ｂ）の認証を行う」ものではないし、甲１発明の「サービスプロバイダに関連する身分情報」又は「レジサービス端末の身分情報」を用いて「身分の正当性を検証」する処理を行う際に、「前記第２ユーザの情報および／又は前記第２ユーザ端末（Ｂ）の情報と関連付けられた第２の証明情報」を用いて対応しているか否かを判断する

ことが、当業者にとって適宜なし得たこととともいえない。

また、請求人（原告）が無効理由１において周知技術とする、甲２の１、甲３ないし６のいずれにおいても、前記相違点１－２、１－３及び１－５に係る構成に関しては記載されていない。

したがって、甲１発明及び周知技術に基づいて、当業者が前記相違点１－２、１－３及び１－５に係る構成を容易に想到し得たとはいえないから、相違点１－１、１－４、１－６ないし１－８について検討するまでもなく、本件発明２は、甲１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ものではない。

オ　本件発明３と甲１発明との対比、相違点に関する容易想到性の判断（本件審決第７の２、９４頁）

本件発明３は、本件発明２の「電子マネー送金方法」の発明を「電子マネー送金システム」として記載した発明であって、本件発明３の「前記第１ユーザ端末（Ａ）から、前記第２ユーザへの電子マネーの送金指示と、前記受取額とを受信する手段」についても、甲１発明は、「送金指示を受信する手段」であるが、「受取額」については、「送金指示」とは別に、「前記第１ユーザ端末（Ａ）から、前記第２端末情報を受信する手段」において、「レジサービス端末」の「身分情報」とともに「取引金額」を画像情報として受信しているから、相違点１－７と同様の相違点を有することになる。

そうすると、本件発明３と甲１発明をシステムの発明として表現した発明とを対比すると、前記相違点１－１ないし１－８と同様の相違点を有すると認められる。

そして、相違点１－２、１－３及び１－５と同様の相違点に係る構成については、前記エのとおり、甲１発明及び周知技術に基づいて当業者が容易に想到し得たとはいえないから、本件発明３は、甲１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ものではない。

カ　無効理由１のまとめ（本件審決第７の３、９４頁）

本件発明２及び３は、甲１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ものではない。

⑵　無効理由２（甲７に記載された発明を主引用例とする本件発明４及び５の進歩性欠如）について

ア　甲７に記載された発明（以下「甲７発明」という。）（本件審決第８の１⑴、９５ないし９６頁）

「支払人端末１０２、決済（受取人）端末１０４、および、決済サーバ１０６を備えるモバイル決済処理システムにより、決済データを処理するための方法であって、（甲７の【請求項７】、段落【００１８】）

受取人端末および決済サーバは、インターネット、無線ネットワーク、専用ネットワーク、または、任意の他の適切な接続で通信できるが、支払人端末は、決済サーバとデータを直接やり取りしないものであり、（【００１９】）

支払人端末および受取人端末は携帯型電子端末であり（【００１８】）、それぞれ、支払人口座番号および受取人口座番号を有し、（【００２４】）

決済サーバは、支払人端末に関連付けられた支払人口座番号および決済パスワードと、受取人端末に関連付けられた受取人口座番号とを予め格納し、（【００２４】）

支払人端末および決済サーバは、支払人端末および決済サーバによってアクセス可能なファイル内に予め格納された暗号化関数およびそれに関連するパラメータの定義をデバイスによってロードして、暗号化関数およびパラメータを設定し（【００２５】）、

受取人端末および支払人端末は、現行の決済処理の開始時に接続を確立し、（【００２７】）

決済サーバは、現行の決済を一意的に特定する決済シリアル番号を受取人端末に提供し、決済シリアル番号を格納し、（【００２９】）

受取人端末は、決済シリアル番号および受取人口座番号を含む受取人情報を支払人端末に送信し、受取人情報は、受取人端末によって確定された支払い金額を任意選択的に含んでもよく、（【００３０】）

支払人端末は、暗号化関数を用いて、支払人口座番号、決済パスワード、受取人口座番号、決済シリアル番号、および、支払い金額を決済要求データに暗号化し、暗号化決済要求データと支払人端末によって入力された支払い金額を受取人端末に送信し、（【００３１】、【００３２】）

受取人端末は支払い金額を検証し、金額が正しい場合、暗号化決済要求データおよび支払い金額を決済サーバに転送し、（【００３３】）

決済サーバは、事前に定義された暗号化関数を用いて決済要求データを復号し、復号された支払人口座番号、決済パスワード、受取人口座番号、決済シリアル番号、および、支払い金額を取得し、（【００３４】）

決済サーバは、格納された支払人口座番号、決済パスワード、受取人口座番号、および、決済シリアル番号を読み出し、読み出した支払人口座番号と復号した支払人口座番号、読み出した決済パスワードと復号した決済パスワード、読み出した受取人口座番号と復号した受取人口座番号、および、読み出した決済シリアル番号と復号化した決済シリアル番号を比較して、復号された全決済データが、格納された決済データと一致するか否かを判定し、比較された読み出しデータおよび復号データのすべてが一致する場合、さらに、復号した支払い金額および受信した支払い金額が一致するか否か比較され、金額が一致した場合、特定された金額の決済が決済サーバによって行われ、支払い金額分が、支払人の口座から差し引かれ、受取人の口座に増額される、（【００３５】～【００３７】）

決済データを処理するための方法。」

イ　本件発明４と甲７発明の一致点、相違点（本件審決第８の１⑵ケ、１０４ないし１０７頁）

(ｱ) 一致点

「第１ユーザが有する第１ユーザ端末（Ａ）と、第２ユーザが有する第２ユーザ端末（Ｂ）と、前記第２ユーザ端末（Ｂ）と通信回線を介して通信可能である管理サーバとを用いて、前記第１ユーザから前記第２ユーザへのマネーの送金を行うマネー送金方法であって、

前記管理サーバおよび前記第１ユーザの端末（Ａ）は、前記第１ユーザの情報および／又はその情報と関連付けられた前記第１ユーザ端末（Ａ）の正当性を検証するための情報を格納しているものであると共に、前記管理サーバおよび前記第２ユーザ端末（Ｂ）は、前記第２ユーザの情報を格納しているものであり、

この方法は、

前記送金の際、前記第２ユーザ端末（Ｂ）が、前記第１ユーザ端末（Ａ）から前記第１ユーザ端末（Ａ）の正当性を検証するための情報を受け取り、前記第２ユーザ端末（Ｂ）を介して前記第１ユーザ端末（Ａ）の正当性を検証するための情報が前記管理サーバに送信されるようになっており、

前記管理サーバが、

前記第１のユーザ端末（Ａ）が前記管理サーバに格納されている前記第１ユーザ端末（Ａ）の正当性を検証するための情報と対応しているか否かの判断を少なくとも行うことにより、前記第１ユーザ端末（Ａ）の認証を行う認証工程と、

を行い、

前記第２ユーザから、前記第１ユーザからのマネーの受取指示と、受取額とを受信するものである

ことを特徴とするマネー送金方法。」

(ｲ) 相違点２－１

本件発明４は、「第１ユーザ」から「第２ユーザ」へ送金されるマネーが「電子マネー」であって、「第１ユーザ」と「第２ユーザ」の「電子マネー」をそれぞれ記憶する「電子マネー管理サーバ（３００）」が、第１ユーザから第２ユーザへの「電子マネーの送金を行う電子マネー送金方法」に関する発明であるのに対し、甲７発明は、「第１ユーザ」から「第２ユーザ」へ送金されるマネーが「電子マネー」であるか定かではなく、また、甲７発明の「管理サーバ」（決済サーバ）は、「第１ユーザ」と「第２ユーザ」の「口座番号」をそれぞれ記憶するものの、口座のマネー自体を記憶するものではなく、「管理サーバ」が、第１ユーザから第２ユーザへの「マネーの送金を行うマネー送金方法」に関する発明である点。

(ｳ) 相違点２－２

本件発明４の「電子マネー管理サーバ（３００）」は、「前記第１ユーザ端末（Ａ）及び前記第２ユーザ端末（Ｂ）と通信回線を介して通信可能」であるのに対し、甲７発明の「決済サーバ」は、「前記第２ユーザ端末（Ｂ）」である「受取人端末」とは通信回線を介して通信可能であるものの、「前記第１のユーザ端末（Ａ）」である「支払人端末」とは直接通信を行うものではない点。

(ｴ) 相違点２－３

「管理サーバ」及び「第２ユーザ端末（Ｂ）」が格納する情報に関して、本件発明４では、「電子マネー管理サーバ（３００）」及び「第２ユーザの端末（Ｂ）」は、「前記第２ユーザの情報および／又はその情報と関連付けられた第２の証明情報」を格納し、特に「電子マネー管理サーバ（３００）」は「その情報と関連付けられた第２の証明情報」を

格納するのに対し、甲７発明では、「管理サーバ」（「決済サーバ」）及び「第２ユーザ端末（Ｂ）」（「受取人端末」）は、「前記第２ユーザの情報」である「受取人口座番号」を格納するものの、「その情報」である「第２ユーザの情報」と関連付けられた「第２の証明情報」を格納するものではない点。

(ｵ) 相違点２－４

「管理サーバ」及び「第１ユーザ端末（Ａ）」が格納する情報に関して、本件発明４では、「電子マネー管理サーバ（３００）」及び「第１ユーザの端末（Ａ）」は、「前記第１ユーザの情報および／又はその情報と関連付けられた第１の証明情報」を格納し、特に「電子マネー管理サーバ（３００）」は「その情報と関連付けられた第１の証明情報」を格納するのに対し、甲７発明では、「管理サーバ」（「決済サーバ」）および「第１ユーザ端末（Ａ）」（「受取人端末」）は、「前記第１ユーザの情報」である「支払人口座番号」を格納し、「管理サーバ」は「その情報」である「第１ユーザの情報」と関連付けられた「前記第１ユーザ端末（Ａ）の正当性を検証するための情報」を格納するものの、「第１の証明情報」を格納するものではない点。

(ｶ) 相違点２－５

「認証工程」に関して、本件発明４は、「電子マネー管理サーバ（３００）」が「前記第１の証明情報の少なくとも一部を受け取った第２のユーザ端末（Ｂ）が前記電子マネー管理サーバ（３００）に格納されている前記第２の証明情報と対応しているか否かの判断」を行うことにより、「前記第２ユーザ端末（Ｂ）の認証を行う」ものであるのに対し、甲７発明は、「管理サーバ」に「第２の証明情報」を格納するものではない（［相違点２－３］）から、「第２ユーザ端末（Ｂ）」（「受取人端末」）と「第２の証明情報」とが対応しているか否かの判断を行うも

のではなく、「第２ユーザ端末（Ｂ）」である「受取人端末」の「認証を行う」ものでもなく、さらに、本件発明４は、「電子マネー管理サーバ（３００）」が「前記第１のユーザ端末（Ａ）が前記電子マネー管理サーバ（３００）に格納されている前記第１の証明情報と対応しているか否かの判断」を行うことにより、「前記第１ユーザ端末（Ａ）」「の認証を行う」ものであるのに対し、甲７発明は、「管理サーバ」に「第１の証明情報」を格納するものではない（［相違点２－４］）から、「前記第１ユーザ端末（Ａ）」の認証を行う際に、「第１ユーザ端末（Ａ）」（「支払人端末」）と「第１の証明情報」とが対応しているか否かの判断を行うものではない点。

(ｷ) 相違点２－６

本件発明４では、「電子マネー管理サーバ（３００）」が「認証工程」の後に「前記第２ユーザから、前記第１ユーザからの電子マネーの受取指示と､受取額とを受信する第３受信工程」を行うものであるのに対し、甲７発明の「管理サーバ」（「決済サーバ」）は、「認証工程」の前に「前記第２ユーザから、前記第１ユーザからのマネーの受取指示と、受取額とを受信する」処理を行うものである点。

(ｸ) 相違点２－７

本件発明４では、「電子マネー管理サーバ（３００）」が「前記第２ユーザから受信した前記受取額が前記電子マネー管理サーバ（３００）に記憶されている前記第１ユーザの電子マネーの残額内であるか否かの判断を少なくとも行う決済判断工程」を行い、「前記決済判断工程において前記残額内であると判断される」場合に「決済工程」を行うのに対し、甲７発明では、かかる「決済判断工程」は行われず、そのために「決済工程」が「前記決済判断工程において前記残額内であると判断される」場合に行われるものではない点。

ウ　本件発明４と甲７発明の相違点に関する容易想到性の判断（本件審決第８の１⑶、１０７ないし１０８頁）

前記相違点のうち、相違点２－３、２－５について検討すると、甲７発明においては、「受取人端末」が「受取人口座番号」を記憶するほか、「決済サーバ」も、受取人端末に関連付けられた「受取人口座番号」を予め格納しており、決済処理においては、「受取人端末」が「支払人端末」に送信した受取人情報に含まれる「受取人口座番号」が、「支払人端末」において「決済要求データ」に含まれて暗号化された後に、「暗号化決済要求データ」が「受取人端末」を介して「決済サーバ」に転送され、当該「決済サーバ」が、「暗号化決済要求データ」を復号して「受取人口座番号」を取得する。

そして、甲７発明の「決済サーバ」は、「読み出した受取人口座番号」と「復号した受取人口座番号」を比較して「一致するか否かを判定」する処理を、「決済サーバ」に予め格納された「受取人端末に関連付けられた受取人口座番号」と「復号した受取人口座番号」とを比較することにより行い、この比較によって、「受取人口座番号」と関連付けられた「受取人端末」を特定するものである。

しかし、甲７発明の「受取人口座番号」は、ユーザ端末から発行の要求を受けて、ユーザ端末の認証を行う管理サーバで作成されるものではなく、認証のためのデジタル署名や公開鍵等を有する電子証明書のような情報でもないから、本件発明４に係る「第２の証明情報」ではないし、甲７発明の「決済サーバ」において、「受取人端末」を特定する際に用いられる「受取人口座番号」に代えて、（「第２ユーザ端末（Ｂ）」である「受取人端末」の認証を行うための）「第２の証明情報」を用いることに関しては、甲７には記載も示唆もされていない。

また、請求人（原告）が無効理由２において周知技術とする、甲２の１、

甲３ないし５、甲８ないし１１のいずれにおいても、前記相違点２－３及び２－５に係る構成に関しては記載されていない。

したがって、甲７発明及び周知技術に基づいて、当業者が前記相違点２－３、２－５に係る構成を容易に想到し得たとはいえないから、相違点２－１、２－２、２－４、２－６、２－７について検討するまでもなく、本件発明４は、甲７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ものではない。

エ　本件発明５と甲７発明との対比、相違点に関する容易想到性の判断（本件審決第８の２、１０８ないし１０９頁）

本件発明５は、本件発明４の「電子マネー送金方法」の発明を「電子マネー送金システム」として記載した発明であって、本件発明４における「認証工程」の処理を行う「認証手段」と、本件発明４における「第３受信工程」の処理を行う「第３受信手段」に関して、これらの処理の順番については特定されないものである。

そうすると、本件発明５と甲７発明をシステムの発明として表現した発明とを対比すると、前記相違点２－１ないし２－５、２－７と同様の相違点を有すると認められる。

そして、相違点２－３、２－５と同様の相違点に係る構成については、上記ウのとおり、甲７発明及び周知技術に基づいて当業者が容易に想到し得たとはいえないから、本件発明５は、甲７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ものではない。

オ　無効理由２のまとめ（本件審決第８の３、１０９頁）

本件発明４及び５は、甲７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ものではない。

⑶　無効理由５（本件補正による新規事項追加）について

ア　本件補正による補正事項（本件審決第９の１、１０９ないし１１１頁）

本件補正は、本件出願の特許請求の範囲を補正することにより、本件発明４及び５に係る請求項４及び５を追加するものである。

イ　当初明細書等の記載（本件審決第９の２、１１１ないし１１９頁）

本件出願の願書に最初に添付した明細書、特許請求の範囲及び図面（以下「本件出願の当初明細書等」という。別紙１。）には、段落【００１８】、【００４４】、【００４９】、【００５０】、【００５７】ないし【００６１】、【００６８】ないし【００７８】、【００９８】ないし【０１００】、【図８】及び【図１３】の記載がある。

ウ　補正事項に関する検討

(ｱ) 請求項４（本件発明４）に関する検討（本件審決第９の３(1)、１１９～１２７頁）

a　請求項４が本件出願の当初明細書等に記載されたものであるかについて

本件出願の当初明細書等の段落【００４４】、【００４９】ないし【００５０】、【００６８】ないし【００７８】の記載によれば、構成要件４Ａの事項は、本件出願の当初明細書等に記載されたものである。

本件出願の当初明細書等の段落【００５７】ないし【００６０】、【００６１】の記載によれば、構成要件４Ｂの事項は、本件出願の当初明細書等に記載されたものである。

本件出願の当初明細書等の段落【００６８】ないし【００７８】、とりわけ【００７０】、【００７１】ないし【００７２】の記載によれば、構成要件４Ｃ－１の事項は、本件出願の当初明細書等に記載されたものである。

本件出願の当初明細書等の段落【００７３】、【００７４】、【００９９】の記載によれば、構成要件４Ｃ－２－１の事項は、本件出願の当初明細書等に記載されたものである。

本件出願の当初明細書等の段落【００７５】、【００７６】の記載によれば、構成要件４Ｃ－２－２の事項は、本件出願の当初明細書等に記載されたものである。

本件出願の当初明細書等の段落【００７７】の記載によれば、構成要件４Ｃ－２－３の事項は、本件出願の当初明細書等に記載されたものである。

本件出願の当初明細書等の段落【００７８】の記載によれば、分説４Ｃ－２－４、４Ｄの事項は、本件出願の当初明細書等に記載されたものである。

ｂ　請求人（原告）の主張について（本件審決第９の３⑴ケ、１２４～１２６頁）

請求人（原告）は、本件出願の当初明細書等に記載された第１実施形態においては、段落【００８０】、【００８１】、【００８４】の記載によれば、端末Ａ（送金側）と端末Ｂ（受金側）とが互いに有する電子証明書の内容を交換して、交換した情報をそれぞれが管理サーバ３００に送ることにより、本件発明４及び５における課題（【００１３】）を解決すること、及び、端末Ａと端末Ｂとが、送金指示及び受取指示それぞれを管理サーバ３００に送ることにより、本件発明４及び５における課題を解決することが明確に記載されており、特に【００８１】の記載によれば、端末Ｂ（受金側）からの伝達プロセスで送金が完結すると不正送金が行われる可能性があることに鑑みて、第１実施形態において、端末Ａ（送金側）からも伝達プロセスを必要とする構成を採用し、これにより不正送金が行われないようにしたことが明確に記載されているから、第１実施形態は、送金側からの電子証明書の情報の送信を必須とするものであって、本件発明４及び５のように、交換した電子証明書の内容を送金側から送信すること、及び、送

金指示を送金側から送信することを必ずしも必要としない形態が、本件発明４及び５における課題を解決することができることは、被請求人（被告）が補正の根拠として掲げる第１実施形態には何ら記載されていない旨を主張する。

そこで、請求人（原告）の上記主張について検討すると、本件発明４の「前記送金の際、前記第２ユーザ端末（Ｂ）が、前記第１ユーザ端末（Ａ）から前記第１の証明情報の少なくとも一部を受け取り、前記第２ユーザ端末（Ｂ）を介して前記第１の証明情報の少なくとも一部が前記電子マネー管理サーバに送信される」（４Ｃ－１）という構成は、本件出願の当初明細書等の段落【００１８】の記載における、「自己の端末の電子証明書の情報が他の端末から電子マネー管理サーバに送られ」、又は「当該他の端末の電子証明書の情報が自己の端末から電子マネー管理サーバに送られる」という事項に相当するものであって、当該段落【００１８】の記載によれば、「この時点で取引を行おうとしている２つの端末が特定され」るものである。

また、本件発明４の「前記第１の証明情報の少なくとも一部を受け取った第２のユーザ端末（Ｂ）が前記電子マネー管理サーバ（３００）に格納されている前記第２の証明情報と対応しているか否かの判断と、前記第１のユーザ端末（Ａ）が前記電子マネー管理サーバ（３００）に格納されている前記第１の証明情報と対応しているか否かの判断を少なくとも行うことにより、前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）の認証を行う認証工程」（４Ｃ－２、４Ｃ－２－２）という構成は、本件出願の当初明細書等の段落【００１８】の記載における、「さらに、それぞれ送信された電子証明書の照合が電子マネー管理サーバによって行われる。」という事項に相当するものであって、「これにより、電子マネー管理サーバは、電子マネーの送受

金を行おうとしている端末を確実に認証することができる。」という効果を奏するものである。

一方、本件補正の根拠とされている第１の実施形態について、本件出願の当初明細書等の段落【００７４】には、「ステップＳ１１１およびＳ１１２」の処理に関して、「（１）復号化された第１の電子証明書のデジタル署名と顧客マスタ格納部３５０に格納されている第１の電子証明書のデジタル署名とが対応しているか否か」（ステップＳ１１１）、「（２）復号化された第２の電子証明書のデジタル署名と顧客マスタ格納部３５０に格納されている第２の電子証明書のデジタル署名とが対応しているか否か」（ステップＳ１１１）、「（３）第２の電子証明書のデジタル署名の送信元が端末Ａ（第１の電子証明書に対応している端末）であるか否か」（ステップＳ１１２）、「（４）第１の電子証明書のデジタル署名の送信元が端末Ｂ（第２の電子証明書に対応してる端末）であるか否か」（ステップ１１２）の４点について判断を行うことが記載され、段落【００７５】の記載によれば、第１実施形態では、上記（１）～（４）の全てについて判断を行い、その全てが「対応していると判断された状態」でユーザＡからユーザＢへの電子マネーの送金を行う例が示されている。

ここで、上記の「ステップＳ１１１およびＳ１１２」の技術的意義について、本件出願の当初明細書等には、「ステップＳ１１１およびステップＳ１１２で取引を行う端末を確実に認証することができる」（【００９９】）と示した上で、「さらに、ステップＳ１１１を省く場合でも、ユーザＡからユーザＢへの電子マネーの送金を行うことは可能である。これは、ステップＳ１１２だけでも取引を行う端末を確定することができるからである。」（【０１００】）と記載されており、上記の段落【００１８】の記載も併せて考慮すると、本件発明４

に係る「認証工程」は、「取引を行おうとしている２つの端末が特定」でき、これら２つの端末について「確実に認証すること」ができれば十分であって、必ずしも段落【００７４】に記載された「ステップＳ１１１およびＳ１１２」における上記（１）～（４）の全てについて判断する必要はないものであるといえる。

そうすると、本件発明４は、「前記第２ユーザ端末（Ｂ）が、前記第１ユーザ端末（Ａ）から前記第１の証明情報の少なくとも一部を受け取り、前記第２ユーザ端末（Ｂ）を介して前記第１の証明情報の少なくとも一部が前記電子マネー管理サーバに送信される」ことにより、「取引を行おうとしている２つの端末が特定」できる上に、「前記第１の証明情報の少なくとも一部を受け取った第２のユーザ端末（Ｂ）が前記電子マネー管理サーバ（３００）に格納されている前記第２の証明情報と対応しているか否かの判断と、前記第１のユーザ端末（Ａ）が前記電子マネー管理サーバ（３００）に格納されている前記第１の証明情報と対応しているか否かの判断を少なくとも行うことにより、前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）の認証を行う認証工程」により、「取引を行う端末を確実に認証することができる」ものであるから、受金側から受け取った電子証明書及び送金指示を送金側から送信しなくても、取引を行おうとしている２つの端末を特定し、これら２つの端末について確実に認証するという効果を奏するものである。

したがって、本件発明４において、交換した電子証明書の内容を送金側から送信すること、及び、送金指示を送金側から送信することを特定していないことは、本件出願の当初明細書等の記載を総合することで導き出される技術的事項との関係において新たな技術的事項を導入するものではないから、請求人（原告）の上記主張は採用できない。

ｃ　本件補正による新規事項追加の有無（本件審決第９の３⑴コ、１２６～１２７頁）

請求項４の各構成要件の事項は、本件出願の当初明細書等に一連の方法として記載されたものであるから、本件補正において、本件発明４に係る請求項４を追加する補正は、本件出願の当初明細書等の記載を総合することで導き出される技術的事項との関係において新たな技術的事項を導入するものではない。

(ｲ) 請求項５（本件発明５）に関する検討（本件審決第９の３⑵、１２７頁）

本件補正において追加された請求項５は、請求項４に係る「電子マネー送金方法」の発明を「電子マネー送金システム」の発明として表現したものであって、上記(ｱ)と同様に、請求項５を追加する補正についても、本件出願の当初明細書等の記載を総合することで導き出される技術的事項との関係において新たな技術的事項を導入するものではない。

エ　無効理由５のまとめ（本件審決第９の４、１２７頁）

本件補正は、本件出願の当初明細書等の記載を総合することで導き出される技術的事項との関係において新たな技術的事項を導入するものではないから、本件特許は、特許法１７条の２第３項に規定する要件を満たしていない補正をした特許出願に対してされたものではなく、無効理由５は理由がない。

⑷　無効理由３（分割要件違反による新規性又は進歩性の欠如）について

ア　分割要件に関する検討（本件審決第１０の１、１２７ないし１２８頁）

請求人（原告）が主張する無効理由３（分割要件違反による新規性又は進歩性の欠如）は、要するに、本件出願が分割要件を満たさないから、本件各発明についての新規性及び進歩性の判断の基準日が現実の出願日であることを前提とし、本件各発明が、本件出願の現実の出願日よりも前に

公開された甲１３発明により、新規性及び進歩性を欠くというものである。そして、分割要件を満たさないとの主張は、本件発明４及び５に係る請求項４及び５が、第１世代出願の出願当初の明細書、特許請求の範囲及び図面（以下「第１世代出願の当初明細書等」という。）に記載された事項の範囲内にないことを主張の根拠とするものである。

しかし、前記⑶の説示のとおり、本件補正により追加された請求項４及び５は、本件出願の当初明細書等の記載を総合することで導き出される技術的事項との関係において新たな技術的事項を導入するものではない。そして、本件出願の当初明細書等の記載は、第１世代出願の当初明細書等の記載と同一であり、また、最初の原出願の願書に最初に添付した明細書、特許請求の範囲及び図面（以下「最初の原出願の当初明細書等」という。）の記載とも同一である。したがって、本件出願は、第１世代出願及び最初の原出願に対して分割要件を満たすものである。

イ　新規性、進歩性についての判断（本件審決第１０の２、１２８頁）

上記アのとおり、本件出願は、第１世代出願及び最初の原出願に対して分割要件を満たし、本件出願の出願日は、最初の原出願の出願日（平成２４年１０月１１日）に遡及するから、本件各発明は、本件出願の現実の出願日ではなく、最初の原出願の出願日に基づいて、新規性及び進歩性の判断をすべきものである。

そうすると、最初の原出願の出願日より後の平成２８年４月１４日に公開された第１世代出願の公開特許公報（甲１３）は、本件特許の出願前に頒布された刊行物とはいえず、本件各発明は、当該第１世代出願の公開特許公報に記載された発明により、新規性及び進歩性を欠くものではない。

ウ　無効理由３のまとめ

したがって、本件出願が分割要件を満たさないことを前提とし、本件各発明が、甲１３発明により新規性及び進歩性を欠くという請求人（原告）

の主張は、その前提に誤りがあるから、無効理由３は理由がない。

⑸　無効理由４（本件発明４及び５に係る特許のサポート要件違反）について（本件審決第１１、１２８ないし１２９頁）

前記⑶ウ(ｱ)のとおり、本件発明４は、本件出願の当初明細書等中の明細書の発明の詳細な説明に記載されたものであるから、本件明細書等中の発明の詳細な説明に記載されたものである。同様に、請求項４に係る「電子マネー送金方法」の発明を「電子マネー送金システム」の発明として表現した本件発明５も、本件明細書等中の発明の詳細な説明に記載されたものである。したがって、本件発明４及び５がサポート要件に違反するものであるとはいえない。

５　原告の主張する取消事由

⑴　取消事由１

無効理由１（甲１発明を主引用例とする本件発明２及び３の進歩性欠如）に関する判断の誤り

⑵　取消事由２

無効理由２（甲７発明を主引用例とする本件発明４及び５の進歩性欠如）に関する判断の誤り

⑶　取消事由３

無効理由５（本件補正による新規事項追加）に関する判断の誤り

⑷　取消事由４

無効理由３（分割要件違反による新規性又は進歩性欠如）に関する判断の誤り

⑸　取消事由５

無効理由４（本件発明４及び５に係る特許のサポート要件違反）に関する判断の誤り

第３　当事者の主張

1　取消事由１（無効理由１（甲１発明を主引用例とする本件発明２及び３の進歩性欠如）に関する判断の誤り）について

〔原告の主張〕

⑴　甲１発明の認定の誤り

ア　甲１の「アカウント情報」は金銭的価値（残高等）に関する情報を含むこと

甲３（米国特許公開公報US2003/0050898）、甲７の記載のとおり、「アカウント」の用語は、残高が含まれる意味で一般的に用いられており、当業者からすれば、「アカウント情報」という用語には、口座番号情報の他、金銭的価値（口座の残高等、口座に紐づく金銭）に関する情報が含まれる意味を示すことは技術常識であるから、甲１の「アカウント情報」（甲１原文の「帳号信息」、「帳戸信息」）は、「口座番号情報」の意味に限定されるものではなく、口座番号情報の他、金銭的価値（口座の残高等）に関する情報を含むと解釈されるべきである。

また、アカウント情報に基づいて取引を実行する、又は支払を実行するという甲１の記載に接した当業者であれば、かかるアカウント情報には、残高に相当する電子マネーに関する情報が含まれていると理解することが自然であり、甲１発明においては、かかる電子マネーを用いて取引又は支払が実行されることを意味すると理解することが自然である。

さらに、甲１には、「ネットワーク仲介システム３はそれぞれ移動端末ユーザ及びサービスプロバイダとサービス協議を締結した運営業者のみであってもよく、銀行が参加してもよく」と記載されており、運営業者のみのネットワーク仲介システムが支払を実行し、取引を完結させるためには、ネットワーク仲介システムがアカウント情報として金銭的価値（口座の残高等）に関する情報を記憶し、管理している必要があることは当業者であれば当然に理解できる。

「帳号信息」及び「帳戸信息」の意味として、「帳号」の一つの意味にすぎない「口座番号」（アカウント番号）を採用し、「アカウント情報」は「口座番号情報」であるとして、「ネットワーク仲介システム」が「金銭的価値（口座の残高等）に関する情報」を記憶、管理せず、「口座番号情報」だけを記憶、管理しているかのような本件審決の引用発明の認定は、甲１の記載、訳文及び技術常識に基づくものではなく、誤りである。

そうすると、甲１の「アカウント情報」は金銭的価値（残高等）に関する情報を含む。

イ　甲１の「ネットワーク仲介システム」は、「移動端末」から出力された「移動端末ユーザの身分情報」を受信するといえること

甲１には、移動端末側で画像解析を行い、取引情報を送信する態様が記載されていることから（別紙２の９）、甲１発明の認定において、移動端末が「移動端末ユーザの身分情報」と「レジサービス端末の身分情報」とを「ネットワーク仲介システム」に送信する態様が看過された点で、本件審決には誤りがある。

また、本件審決では、「ネットワーク仲介システム」は、「移動端末」ではなく「MSC」及び／又は「HLR」から画像情報及び移動端末のユーザ身分情報を受信することが認定されているが、移動端末を用いる全ての通信は、「MSC」を通過して行われる（甲２７）。よって、甲１において、「MSC」及び／又は「HLR」から画像情報及び移動端末のユーザ身分情報を受信することは、かかる情報の送信元である「移動端末」からネットワーク仲介システムが受信することと同義であり、「移動端末」からこれらの情報が受信されると認定されてもよいはずである。

したがって、甲１の「ネットワーク仲介システム」は、「移動端末」から出力された「移動端末ユーザの身分情報」を受信するといえる。

ウ　甲１には取引金額とともに送金指示が送信される態様が記載されている

こと

甲１の１４頁５行ないし８行（別紙２の１０。甲１の頁数及び行数は、甲１本文のものを指す。以下、本判決の本文及び別紙２において同じ。）には、「取引を実行する命令」を送信するトリガとなる「確認通知」を必要としない態様が開示されている。「確認通知」が省略される場合、移動端末からネットワーク仲介システムに取引時に送信されるタイミングは、取引金額（受取額）及びレジサービス端末の身分情報が送信されるタイミングだけであるから、これらの情報を送信することが「送金指示」に対応し、甲１発明においても、ネットワーク仲介システムが、送金指示とともに受取額を受信する態様が開示されている。

このように、甲１には、「取引を実行する命令」を送信するトリガとなる「確認通知」を必要としない態様が開示されており、取引金額とともに送金指示が送信される態様が記載されているから、ネットワーク仲介システムが取引金額とともに送金指示を受信する態様を看過し、「取引金額」と「送金指示」とが別の工程で受信されると認定した本件審決には誤りがある。

⑵　本件発明２の認定の誤り

本件審決は、本件発明２の「証明情報」を、（A）ユーザ端末から発行の要求を受けて電子マネー管理サーバで作成される情報であり、（B）認証のためのデジタル署名や公開鍵等を有する電子証明書のような情報である、という二つの意義を有する情報であると認定した。

しかし、第１に、上記の意義（A）について、請求項２においては「証明情報」がどこで作成されるものであるかを示す記載は何もないうえ、本件明細書等の段落【００５９】には外部の電子証明書発行業者に依頼して作成する態様も記載されていることからすれば、ユーザ端末からの発行の要求は必要なく、また、電子マネー管理サーバで作成される必要もない。

第２に、上記の意義（Ｂ）について、請求項２には「証明情報」について、端末の認証のために用いられる情報であることが記載されているだけであり、本件明細書等には、「証明情報」は、端末とサーバ間でユニークな情報であることが記載されているのみである。また、上記の意義（Ｂ）では、「デジタル署名や公開鍵等を有する電子証明書のような」とされていて、「デジタル署名や公開鍵等を有する電子証明書」は一例として記載されているに過ぎず、その他の情報として何を含むのかが不明であり、結局、「証明情報」が何を意味するのかを特定することができない。

したがって、本件発明２における「証明情報」の技術的意義は、請求項及び本件明細書等の記載に基づけば、「端末の認証のために用いられるものであり、端末とサーバ間でユニークな情報」と認定されるべきであり、本件審決が認定するのと異なり、ユーザ端末からの発行の要求は必要なく、また、電子マネー管理サーバで作成される必要もない。

被告自身、本件特許に基づき原告に対して提起した訴訟（東京地方裁判所令和３年（ワ）第７３２１号、知的財産高等裁判所令和５年（ネ）第１００３９号。以下「別件訴訟」という。）において、「第１の証明情報」は、利用者を特定するためのＩＤ等何らかの情報（ユーザ端末の電話番号やパスワード）であればよく、「第２の証明情報」は、加盟店を特定するためのＩＤ等何らかの情報であればよいとのクレーム解釈をしており、本件審決のような限定的な解釈をしていない。

⑶　本件発明２と甲１発明の相違点の認定の誤り

次のとおり、本件発明２と甲１発明の相違点に関する本件審決の認定には誤りがあり、相違点１－２、１－３及び１－５を含む相違点１－１ないし１－７は相違点とはならない。

ア　本件審決が認定した本件発明２と甲１発明の相違点（前記第２の４⑴ウ(ｲ)ないし(ｹ)）のうち、相違点１－１については、前記⑴アのとおり、甲

１発明における「ネットワーク仲介システム」が「運営業者のみ」で実装される場合、当該「ネットワーク仲介システム」が金銭的価値（電子マネー）を記憶、管理する態様が甲１発明に含まれるから、相違点１－１において「甲１発明の『管理サーバ』（ネットワーク仲介システム）は、・・・口座のマネーを管理するものではなく」と本件審決が認定したことは誤りである。

イ　相違点１－２については、本件発明２における「証明情報」の技術的意義は前記⑵のとおり認定されるべきであり、甲１発明における「IMSI情報」などの移動端末情報及びレジサービス端末の情報は、ユーザ又は端末の正当性検証に用いられ、ネットワーク仲介システムと端末間でユニークな情報であるため、原告主張の「証明情報」の技術的意義と一致する。したがって、相違点１－２は、そもそも相違点とはなり得ない。

ウ　相違点１－３については、本件審決は、「甲１発明は、『前記第２ユーザ端末（Ｂ）が出力した、第２端末情報』を取得するものの、当該『第２端末情報』は『第２の証明情報の少なくとも一部の情報』ではなく」と認定しているが、上記イのとおり、レジサービス端末の情報は本件発明２の「証明情報」の技術的意義と合致しているから、上記の点は相違点とはなり得ない。

また、本件審決は、「甲１発明の『第１ユーザ端末（Ａ)』は、『第２ユーザ端末（Ｂ)』が出力した『第２端末情報』と『受取額』の情報を含む『画像情報』を、撮像機能又は図形走査機能を利用して『取得』するのであって、『第２端末情報』と『受取額』を『受信』するものではない」と認定するが、本件発明２の「受信」は、第１ユーザ端末が、第２ユーザ端末から所定の情報を取得することを意図して用いられている用語にすぎず、本件各発明の課題や当該課題を解決するための手段を踏まえてみても、「受信」につき、本来「受信」の語が有する意味を超えて、情報を取得する方法を

限定して解釈する必要はなく、撮像機能又は図形走査機能を利用して画像情報を取得することは「受信」に該当する。なお、仮に、上記認定のとおりであるとしても、第１ユーザ端末は、第２ユーザ端末が出力した「第２端末情報」と「受取額」とを取得することにより、本件発明２は成立するため、取得手段に係る上記相違点は、実質的相違点とならない。

エ　相違点１－４については、前記⑴イのとおり、「MSC又はHLR」から送信されたことと、「移動端末」から送信されたことは同義であるから、「第１端末情報」は「移動端末」から受信した情報であるといえる。また、「証明情報」について前記⑵のとおり限定的に解釈することを前提とした相違点１－４は、そもそも相違点となり得ない。

オ　相違点１－５については、甲１発明における「IMSI情報」などの移動端末の情報は、ネットワーク仲介システムと端末間でユニークな情報であるため、「証明情報」に当たるから、相違点１－５は相違点とはなり得ない。

カ　相違点１－６については、甲１発明では、移動端末ユーザのIMSI、ESN、移動端末番号などの情報を用いて、及び、レジサービス端末のIDなどを用いて、各ユーザの正当性を検証することは、端末の情報を用いての正当性検証になるため、実質的に各端末の認証を行うことと同義であって、相違点１－６に関する本件審決の判断は上記の点を看過している。

キ　相違点１－７については、本件審決は、本件発明２では送金指示と受取額が同時に受信されることを前提として当該相違点を認定したものと解されるが、本件特許の請求項２には、送金指示と受取額とを同時に受信することは何ら特定されておらず、その他の記載や課題等を踏まえてみても、送金指示と受取額を同時に受信していると解釈する理由はないから、相違点１－７は相違点となり得ない。なお、仮に、本件発明２において送金指示と受取額が同時に受信されるものであると解釈したとしても、前記⑴ウのとおり、甲１発明には、ネットワーク仲介システムが送金指示とともに

受取額を受信する態様が開示されている。

ク　以上のとおり、本件審決が認定した相違点は、相違点１－８を除いて実質的な相違点であるとはいえず、本件発明２と甲１発明の相違点は以下のものに限られる（相違点１－８に相当する。以下「原告主張の相違点１」という。）。

「本件発明２では、受取額が残高内であるかの判断を行い、残高内であるという残高確認が行われた場合に電子マネーの送金が行われるのに対し、甲１発明では、かかる残高の判断及び確認を行うのか否かが必ずしも明らかではない点。」

⑷　本件発明２と甲１発明の相違点に関する容易想到性の判断の誤り

次のとおり、本件発明２と甲１発明の相違点に関する本件審決の判断には誤りがある。

ア　本件審決は、相違点１－２、１－３及び１－５に係る構成を容易に想到し得たとはいえないと判断した。しかし、前記⑶のとおり、これらの相違点を含む相違点１－１ないし１－７は、そもそも相違点とはならない。

イ　原告主張の相違点１に係る構成は、甲１発明及び周知技術に基づいて、当業者が容易に想到し得たものである。

すなわち、原告主張の相違点１に係る構成に関し、電子決済分野において、支払者（買い手）のアカウントに、取引額以上の残高があるかの残高確認を行い、残高が十分にあれば取引を行うことは、本件優先日の前から周知技術であった（甲２の１、甲３～５）。

また、甲１に、「したがって、操作しやすくかつ安全で信頼性が高いモバイル決済システム及び方法をどのように提供するかは早急に解決すべき問題となる。」（別紙２の１）等と記載されていることを踏まえれば、甲１発明において、買い手の残高以上の買い物を許容しないよう、取引金額が買い手の残高内であるかの残高確認を行うという上記周知技術を採用す

ることへの示唆があった。

ウ　相違点１－２、１－３及び１－５につき、仮に、本件審決による「証明情報」の認定を前提に、上記各相違点が存在するとしても、電子決済分野において、取引を行うユーザ又は端末の認証に用いる情報に暗号化技術を用いてセキュリティを向上させることは、甲６の２、甲３０、３１をはじめ多数の文献に開示されている内容であって、当業者にとって周知技術又は技術常識であるといえ、安全で信頼性が高いモバイル決済システムを課題とする甲１発明における移動端末の身分情報及びレジサービス端末の身分情報に、周知技術又は技術常識の暗号化技術を用いることは、当業者にとって容易になし得たことである。そして、これによって、本件発明２の上記の相違点に係る構成を想到することは容易であり、上記の相違点に関する本件審決の判断には誤りがある。

エ　仮に、相違点１－１、１－３、１－４、１－６及び１－７が相違点であるとしても、甲１発明ないし技術常識に鑑みれば、これらの相違点に係る構成は当業者であれば容易に想到し得たことである。

(ｱ) 前記⑴アのとおり、甲１に記載のアカウント情報には金銭的価値が含まれると解され、銀行ではないプリペイド決済会社の装置が電子価値を管理することは、甲６（文献「モバイル電子決済のビジネスモデルと技術的要件」）の図５－２８に記載のとおり技術常識である。したがって、相違点１－１として認定された「甲１発明の『管理サーバ』（ネットワーク仲介システム）は、・・・口座のマネー自体を記憶するものではなく」という点において、アカウント情報を記憶し、支払を実行する甲１発明のネットワーク仲介システムに、アカウント情報に金銭的価値が含まれ、銀行ではない会社の装置が電子価値を管理するという技術常識を適用することは、当業者が容易に想到し得る事項である。

(ｲ) 甲６の図５－２８には、端末同士がローカル通信を用いて電子決済に

関する情報を受信することが開示され、甲３０（特表２０１１－５１３８３９号公表特許公報）には、近接場無線通信チャネルを介して信用情報を受信することが開示されており、これらの開示内容に基づき、電子決済に関する情報を通信により受信することは技術常識である。

これらの技術常識に鑑みれば、相違点１－３として認定された「甲１発明の『第１ユーザ端末（A)』は、『第２ユーザ端末（B)』が出力した『第２端末情報』と『受取額』の情報を含む『画像情報』を、撮像機能又は図形走査機能を利用して『取得』するのであって、『第２端末情報』と『受取額』を『受信』するものではない」という点において、甲１に記載の、電子決済に関する情報を含む「画像情報」を撮像機能又は図形走査機能を利用して「取得」することに替えて、電子決済に関する情報を通信により受信するという技術常識を適用することは、当業者が容易に想到し得る事項である。

(ｳ) 相違点１－４につき、「甲１発明では、『第１端末情報』に相当する『IMSI情報』は『MSC又はHLRから返信された』ものであって、『第１ユーザ端末（A)』である『移動端末』から受信した情報ではなく、また、当該『IMSI情報』は『前記第１ユーザ端末（A）の証明情報の少なくとも一部の情報』ではない」との点は、甲１発明のネットワーク仲介システムが受信する情報の送信元として、ネットワーク通信における中継点とするか、大元の送信元とするか、のいずれにするかは当業者にとって適宜なし得る設計変更にすぎず、かかる相違点１－４は、当業者が容易に想到し得る事項である。

(ｴ) 相違点１－６につき、前記(3)カのとおり、甲１に記載の正当性の検証について、移動端末ユーザの端末情報及びレジサービス端末の端末情報が用いられる点を考慮すれば、甲１においても実質的に端末の認証が行われている。そうすると、相違点１－６として認定された「本件発明２

は『前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）の認証を行う』のに対し、甲１発明は『前記第１ユーザおよび前記第２ユーザの認証を行う』ものである」という点において、端末情報を用いてのユーザ認証に対し、決済前に端末認証を行う技術常識（甲７）を適用し、ユーザ認証ではなく端末認証とすることは、当業者が容易に想到し得る事項である。

(ｵ) 相違点１－７として認定された「甲１発明では『受取額』は、『送金指示』とは別に、『前記第１ユーザ端末（Ａ）から、前記第２端末情報を受信する工程』において、『レジサービス端末』の『身分情報』とともに受信される」という点において、甲１には、「送金指示」に対応する「取引を実行する命令」を送信するトリガとなる「確認通知」を省略し、取引金額（受取額）及びレジサービス端末の身分情報が送信されるタイミングが「送金指示」となることが示唆されていることから、「送金指示」とともに「受取額」を受信することは、当業者が容易に想到し得る事項である。

⑸ 本件発明３と甲１発明の対比、相違点に関する容易想到性の判断の誤り

本件審決は、前記第２の４⑴オのとおり、本件発明３は甲１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ものではないと判断した。

しかし、相違点１－２、１－３及び１－５を含む相違点１－１ないし１－７がそもそも相違点とならないことは、前記⑶のとおりであり、本件審決による相違点の認定には誤りがある。

また、本件審決による「証明情報」の認定を前提として各相違点が存在するとしても、前記⑷ウのとおり、各相違点に係る構成は周知技術又は技術常識に基づき容易想到である。

〔被告の主張〕

⑴　本件各発明は、電子マネー管理サーバ内において「電子マネー」を即時かつ安全に送金するために、まず、送金元である第１ユーザと送金先である第２ユーザを「証明情報」を用いて確実に認証し、その後、送金指示／受金指示を送受信することで、即時の送金を可能にしている。これに対し、甲１発明は、電子マネーではなく、基本的に即時の資金移動が発生しないクレジット決済を対象とするものであり、当該クレジット決済に必要な情報を安全に取得してクレジットカードのアクワイアラー（決済代行会社等）や金融機関等に送信するための発明にすぎないから、即時の送金のための第１ユーザ及び第２ユーザの「証明情報」を用いた確実な「認証工程」を必要としない。

⑵　〔原告の主張〕⑴（甲１発明の認定の誤り）に対し

ア　甲１に記載された解決課題は、専ら、ユーザ移動端末を用いた支払情報（取引情報）の入力に関するものであり、甲１発明は、ユーザがモバイル端末を使ってサービスプロバイダのレジ端末で買い物（取引）をした場合の取引情報の入力方法及び入力された取引情報の検証に関する。したがって、甲１発明は、ユーザに代わって取引情報や支払情報を従前のアクワイアラー（決済代行会社等）に渡すものに過ぎず、その取引情報や支払情報を使用して実際に決済を行う具体的方法については何ら言及していないと解するのが妥当である。甲１発明にいう「ネットワーク仲介システム」における「仲介」の語は、ユーザと、従前ユーザがショートメッセージを用いて取引情報を送信していた先であるアクワイアラーやその他の決済機関との間に入って取引情報の通信を「仲介」するという意味であると解するのが相当であるから、甲１発明のネットワーク仲介システムが電子マネーそのものを管理していると解するのは無理がある。

イ　原告は、「ネットワーク仲介システム」がMSC及び／又はHLRから「画像情報」を受信するという本件審決の認定、及び「取引金額」と「送金指示」が別の工程で受信されるという本件審決の認定に誤りがあると主張す

るが、本件発明２の進歩性の判断にどのように影響するのか明らかでない。

⑶　〔原告の主張〕⑵（本件発明２の認定の誤り）に対し

本件各発明では、電子マネーの送金がサーバ内で即時に実行されてしまうことに鑑み、この送金を行う前に、送金元である第１ユーザと送金先である第２ユーザの認証を確実に行う必要がある。本件各発明の「証明情報」は本件明細書等の第１実施形態に例示された電子証明書に限定されるものではないが、ユーザ自身の情報そのもの（氏名やメールアドレス等）やユーザ端末の情報そのもの（電話番号等）ではなく、電子証明書のような、電子マネー管理サーバ内で照合することで送金元・送金先の正当性を認証し、その認証結果により当該サーバ内での即時送金を担保できるような記号や符号であると解されるべきものである。甲１発明の身分情報、すなわち、移動端末ユーザやサービスプロバイダを特定する情報は、ユーザ自体の情報又は移動端末自体の情報であり、ユーザやユーザ端末を証明する情報にはなり得ない。

本件発明２の「証明情報」の技術的意義で重要なのは、本件審決の「証明情報」の認定のうち、「本件特許発明２における『証明情報』は、ユーザ端末の認証を行う管理サーバで作成されるものではない、ユーザの情報そのものや、ユーザ端末の情報そのものとは異なる情報である。」の部分である。原告の主張は本件審決を誤解又は誤読したものである。

⑷　〔原告の主張〕⑶（本件発明２と甲１発明の相違点の認定の誤り）に対し

ア　相違点１－２、１－３、１－５及び１－６に関する原告の主張は、本件審決の「証明情報」の認定に誤りがあることを前提とするものであるが、前記⑶のとおり、本件審決の上記認定は正当であり、原告の主張は理由がない。

イ　相違点１－１については、甲１発明にいう「ネットワーク仲介システム」における「仲介」の語は、取引情報の通信を「仲介」するという意味であると解するのが相当である。また、甲１には上記ネットワーク仲介システ

ムが電子マネーそのものを管理することは開示も示唆もされていない。

したがって、甲１発明に、「ネットワーク仲介システム」が金銭的価値（電子マネー）を記憶、管理する態様が含まれるとする原告の解釈は誤っており、甲１発明のネットワーク仲介システムが「口座のマネー自体を記憶するものではなく」との本件審決の認定判断は正当である。

ウ　相違点１－４については、「IMSI情報」はユーザの情報又は端末情報そのものであり、本件各発明にいう「証明情報」には当たらない。

エ　相違点１－７については、仮に相違点１－７が甲１発明と本件発明２の相違点でなかったとしても、本件発明２の進歩性を基礎付ける部分は、送金指示とともに受取額が受信される点にはなく、この点は本件発明２の進歩性の判断に影響しない。

⑸　〔原告の主張〕⑷（本件発明２と甲１発明の相違点に関する容易想到性の判断の誤り）に対し

ア　原告主張の相違点については、甲１に開示されたネットワーク仲介システムは、金融機関等の送金や決済処理を行うシステムに相当するものではなく、ユーザが入力するべき取引情報の正確な入力を担保するものにすぎず、残高確認を行う必要がないから、当業者であっても、甲１のネットワーク仲介システムに、甲２ないし５に記載された口座残高確認処理を組み合わせる動機付けはないし、組み合わせたとしても本件発明２又は３にはなり得ない。

イ　相違点１－２、１－３及び１－５の容易想到性に関し、原告は、要するに、甲１発明の「身分情報」に周知の暗号化技術を適用すれば、本件発明２の「証明情報」と同等のものになると主張している。しかし、甲１発明と本件発明２は全く異なる発明であり、甲１発明の「身分情報」は、仮に暗号化したとしても「身分情報」であることには変わりがなく、移動端末やレジサービス端末自身そのものの情報にすぎないから、原告の上記主張

は理由がない。

⑹　〔原告の主張〕⑸（本件発明３と甲１発明の対比、相違点に関する容易想到性の判断の誤り）に対し

原告は、本件発明３についての認定判断は、本件発明２について主張したのと同じ理由によって誤りであるという趣旨の主張をするが、被告が本件発明２について反論したように、原告の主張には理由がない。

２　取消事由２（無効理由２（甲７発明を主引用例とする本件発明４及び５の進歩性欠如）に関する判断の誤り）について

〔原告の主張〕

⑴　甲７発明の認定の誤り

ア　甲７の「決済サーバ」は「支払人端末」と通信をすること

甲７には、「決済サーバは、ネットワークを介して、支払人端末および受取人端末にインストールして用いられる電子決済クライアントソフトウェアを提供する」と記載されており（段落【００１９】）、決済サーバは、ネットワークを介して、電子決済クライアントソフトウェアを支払人端末に送信するものであるから、甲７の「決済サーバ」は「支払人端末」と通信をするものであり、甲７において、「決済サーバ」が「支払人端末」と通信をしないとの本件審決の認定は誤りである。

イ　甲７の「決済サーバ」は電子マネーを記憶、管理すること

甲７には、決済サーバについて、「特定された金額の決済が決済サーバによって行われる。支払金額分が、支払人のアカウントから差し引かれ、受取人のアカウントに増額される。」と記載されており（段落【００３７】）、決済サーバ自身が主体となって、支払人及び受取人の口座から差し引いたり増額させたりすることが可能な金銭的価値を、口座に関連付けて記憶していることが、開示ないし示唆されている。また、甲７には、「決済サーバは、Alipay.comなどの信頼できるサードパーティ決済サービス業者によっ

て提供される」ことが記載されており（段落【００１８】）、甲７の出願人であるアリババ社が提供していたモバイル決済システムAlipayは、そのサーバにチャージされた電子マネーを用いてモバイル決済を行うシステムであることが、甲７の公開当時に周知であった（甲８～１１）ことも考慮すれば、当業者であれば、甲７に記載の決済サーバには電子マネーが管理されていると当然に理解する。そのため、本件優先日当時の技術常識に鑑みれば、決済サーバが、アカウントに含まれる残高（電子マネー）を用いて、支払人（ユーザ）の残高から支払金額を減算し、受取人（店舗）の残高に加算することで、電子マネーの送金を行うことが甲７に記載されていることを、当業者であれば当然に理解することができる。

したがって、「決済サーバ」は電子マネーを記憶、管理するものであると認められ、甲７の記載及び技術常識によれば、「決済サーバ」自体が電子マネーを記憶、管理するものであるとはいえないとの本件審決の認定は誤りである。

⑵　本件発明４の認定の誤り

ア　「証明情報」の技術的意義の認定が誤っていること

前記１〔原告の主張〕⑵のとおり、本件審決における「証明情報」の技術的意義の認定には誤りがある。

イ　「第３受信工程」は「認証工程」を行った後に実行されるものに限定されないこと

請求項４の特許請求の範囲の記載からすれば、端末の認証を規定する構成４Ｃ－２－１の後に、受取額の受信を規定する構成４Ｃ－２－２が記載されているにすぎず、この記載の前後をもって直ちに各構成の順番が規定されているとはいえず、特許請求の範囲の請求項４の記載からは、受取額の受信が端末の認証を行った後に行われるとの限定がされているとはいえない。

さらに、被告は、第１世代出願の審査過程において提出した上申書（甲２３）において、最初の原出願の請求項１からタイミングに関する記載を削除したことで、「認証」のタイミングと「送金指示」や「受取指示」の受信のタイミングの前後を実質的に問わないようにしたと述べている。被告は、本件出願の審査過程において提出した上申書（甲２２）において、本件特許が、第１世代出願に係る特許と実質的に同じであることを自認しているから、本願の要旨に関する被告の上記主張内容からしても、受取額を受信するタイミングは端末の認証を行った後であると解釈されるべきではない。

したがって、本件発明４の「第３受信工程」は「認証工程」を行った後に実行されるものに限定されない。

⑶　本件発明４と甲７発明の相違点の認定の誤り

次のとおり、本件発明４と甲７発明の相違点に関する本件審決の認定には誤りがあり、相違点２－３及び２－５を含む相違点２－１ないし２－６はそもそも相違点とはならない。

ア　審決が認定した甲７発明と本件発明４との相違点（前記第２の４⑵イ(ｲ)ないし(ｸ)）のうち、相違点２－１については、前記⑴イのとおり、甲７発明における決済サーバは、電子マネーを管理するAlipayのような決済運営業者により実装されるため、当該決済サーバが金銭的価値（電子マネー）を記憶、管理する態様が甲７発明に含まれる。したがって、相違点２－１に係る本件審決の認定には誤りがある。

イ　相違点２－２については、前記⑴アのとおり、甲７発明における「決済サーバ」は、電子決済クライアントソフトウェアを、ネットワークを介して支払人端末に送信するものであるから、相違点２－２に係る本件審決の認定には誤りがある。

ウ　相違点２－３については、本件発明４における「証明情報」の技術的意

義は、「端末の認証のために用いられるものであり、端末とサーバ間でユニークな情報」と認定されるべきであるから、甲７発明における「受取人口座番号」は本件発明４の「証明情報」に対応する。また、決済サーバ及び受取人端末は、ユーザＩＤなどのユーザ情報に関連付けて受取人口座番号を格納するものであるから、管理サーバ及び受取人端末が、その情報である「第２ユーザの情報」と関連付けられた「第２の証明情報」を格納するものではないとの本件審決の認定は誤りである。

エ　相違点２－４については、甲７発明の「決済パスワード」は本件発明４の「証明情報」に対応し、決済サーバ及び支払人端末が格納する「支払人口座番号」も原告主張の「証明情報」の技術的意義に一致するから、管理サーバ及び支払人端末が、「第１の証明情報」を格納するものではないとする本件審決の認定は誤りである。

オ　相違点２－５については、本件審決における「証明情報」の技術的意義に関する限定的解釈に基づいて認定された相違点であり、そもそも相違点となり得ない。

カ　相違点２－６については、前記⑵イのとおり、請求項４の特許請求の範囲の記載からは、「認証工程」の後に「第３受信工程」を行うことに直ちに限定されないから、相違点２－６に係る本件審決の認定は誤りである。

キ　以上のとおり、本件審決の甲７発明の認定及び本件発明４の認定には誤りがあり、甲７発明と本件発明４との相違点は以下のものに限られる（相違点２－７に相当する。以下「原告主張の相違点２」という。）。

「本件発明４では、受取額が残高内であるかの判断を行い（構成要件４Ｃ－２－３）、残高内であるという残高確認が行われた場合に電子マネーの送金が行われる（構成要件４Ｃ－２－４）のに対し、甲７発明では、かかる残高の判断及び確認を行うのか否かが必ずしも明らかではない点。」

⑷　本件発明４と甲７発明の相違点に関する容易想到性の判断の誤り

ア　本件審決は、相違点２－３及び２－５に係る構成を容易に想到し得たとはいえないと判断したが、前記⑶のとおり、これらの相違点を含む相違点２－１ないし２－６は、そもそも相違点とはならない。

イ　原告主張の相違点２につき、甲７発明に周知技術を適用して、原告主張の相違点２に係る構成に想到することは、当業者が容易になし得たことである。

前記１〔原告の主張〕⑷イのとおり、電子決済分野において、支払者（買い手）のアカウントに、取引額以上の残高があるかの残高確認を行い、残高が十分にあれば取引を行うことは、本件優先日より前において周知技術であった。

また、甲７には、「・・・決済サーバは、Alipay.comなどの信頼できるサードパーティ決済サービス業者によって提供される。」（【００１８】）と記載されているから、甲７発明において、サードパーティ決済サービス業者が信頼できる業者であるために、サードパーティ決済サービス業者が支払人（買い手）の残高以上の買い物を防止すべく、取引金額が買い手の残高内であるかの残高確認を行うという上記周知技術を採用することへの示唆があるといえる。

ウ　相違点２－３及び２－５につき、仮に、本件審決による「証明情報」の認定を前提に、上記各相違点が存在するとしても、電子決済分野において、取引を行うユーザ又は端末の認証に用いる情報に暗号化技術を用いてセキュリティを向上させることは、前記１〔原告の主張〕⑷ウに示した文献をはじめ多数の文献に開示されている内容であって、本件優先日より前に既に当業者にとって周知技術又は技術常識であったといえるから、甲７発明における「受取人口座番号」、「支払人口座番号」、「決済パスワード」に暗号化技術を用いることは、当業者にとって容易になし得たことである。したがって、これらの相違点に係る本件発明４の構成は、周知技術又は技

術常識に基づき容易想到である。

エ　仮に、本件発明４と甲７発明の相違点として相違点２－１、２－２及び２－６が存在するとしても、甲７発明ないし技術常識に鑑みれば、これらの相違点に係る本件発明４の構成は、当業者であれば容易に想到し得たことである。

(ｱ) 前記⑴イのとおり、甲７の出願人であるアリババ社が提供していたモバイル決済システムAlipayは、そのサーバにチャージされた電子マネーを用いてモバイル決済を行うシステムであることは、甲８ないし１１に記載のとおり技術常識である。したがって、相違点２－１として認定された「甲７発明は、『第１ユーザ』から『第２ユーザ』へ送金されるマネーが『電子マネー』であるか定かではなく、また、甲７発明の『管理サーバ』（決済サーバ）は、・・・口座のマネー自体を記憶するものではなく」との点については、甲７発明の決済サーバに、サーバにチャージされた電子マネーを用いてモバイル決済を行うシステム（Alipay）という技術常識を適用することで、当業者が容易に想到し得る事項である。

(ｲ) 甲７には、「決済サーバは、ネットワークを介して、支払人端末および受取人端末にインストールして用いられる電子決済クライアントソフトウェアを提供する」と記載されているところ（段落【００１９】）、相違点２－２として認定された「『電子マネー管理サーバ（３００）』は、…『支払人端末』とは直接通信を行うものではない」という点において、甲７発明の決済サーバを、決済処理の前後において、必要なソフトウェアやデータを支払人端末に送信するように変更することは、当業者が適宜なし得る事項にすぎない。したがって、仮に相違点２－２が存在するとしても、当該相違点に係る構成は当業者にとって容易に想到し得る事項である。

(ｳ) 仮に相違点２－６が相違点であるとしても、「認証」のタイミングと

「送金指示」や「受取指示」の受信のタイミングについては当業者が適宜選択し得る事項であることにすぎないから、相違点２－６は、当業者が容易に想到し得る事項である。

⑸　本件発明５と甲７発明の対比、相違点に関する容易想到性の判断の誤り

本件審決は、前記第２の４⑵エのとおり、本件発明５は甲７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ものではないと判断した。

しかし、相違点２－３及び２－５を含む相違点２－１ないし２－６がそもそも相違点とならないことは、前記⑶のとおりであり、本件審決による相違点の認定には誤りがある。

また、本件審決による「証明情報」の認定を前提として上記の各相違点が存在するとしても、前記⑷ウのとおり、これらの相違点に係る本件発明５の構成は、周知技術又は技術常識に基づき容易想到である。

〔被告の主張〕

⑴　〔原告の主張〕⑴（甲７発明の認定の誤り）に対し

甲７発明は、「ネットワークを介して、支払人端末および受取人端末にインストールして用いられる電子決済クライアントソフトウェアを提供」し（段落【００１９】）、このソフトウェアを用いることにより、支払人端末及び決済サーバは、受取人端末とは無関係に決済データを暗号化することにより、受取人端末に送信される決済データの安全性及び信頼性を高めるとともに、支払人の個人情報のセキュリティを保証するものである。

すなわち、甲７発明は、支払人端末からの決済データが、受取人端末を経由して決済サーバに送られることを前提とし、その際に、受取人端末に当該決済データの内容が知られないように暗号化を施すものである。したがって、甲７の段落【００１９】に明確に記載されているとおり、「支払人端末は、決済サーバとデータを直接やり取りしない」ものであり、「決済サーバ」が「支

払人端末」と通信をしないとの本件審決の認定に誤りはない。

また、甲７発明の解決課題とそれに対する解決手段という観点で正しく解釈すると、甲７発明は、ユーザからの決済要求データを、途中の受取人端末では解読できないように暗号化データとし、それを決済サーバで復号化して検証するようにした点に特徴があり、その決済要求データを使用して実際に決済を行う方法については従来の電子決済（モバイル決済）から何ら変更していないのであるから、口座番号を含む決済要求データには何ら新しい情報は含まれておらず、従来のクレジットカード決済で用いるのと同じ情報であると解するべきであり、これに電子マネーが含まれているとするのは無理がある。

⑵　〔原告の主張〕⑵（本件発明４の認定の誤り）に対し

ア　本件発明４の「証明情報」の技術的意義は、前記１〔被告の主張〕⑶のとおりであり、甲７発明の「アカウントナンバー」／「口座番号」などは、決済をどのユーザや口座番号（アカウント、カード番号）で行うかを特定する情報に過ぎないから、ユーザやユーザ端末を証明する「証明情報」に当たらない。

イ　電子マネー管理サーバにより送金元と送金先の認証を確実に行い、その後で送金を実行することで、即時に電子マネーの送金を完了できることが本件各発明の要点であり、本件明細書等の第１ないし第４の実施形態では、本件各発明の上記要点がより明確になっている。したがって、「第３受信工程」の実行タイミングについて、本件各発明が、電子マネー管理サーバにて証明情報を用いて第１ユーザ端末（送金元）と第２ユーザ端末（送金先）の認証を確実に行った後、当該認証が成功したことに基づいて当該電子マネー管理サーバ内で送金指示が実行され、電子マネーの送金が完了するものであるとした本件審決の認定は正当である。

⑶　〔原告の主張〕⑶（本件発明４と甲７発明の相違点の認定の誤り）に対し

ア　相違点２－３ないし２－５に関する原告の主張は、本件審決の「証明情報」の認定に誤りがあることを前提とするものであるが、「証明情報」に関する本件審決の認定は正当であり、原告の主張は理由がない。

イ　相違点２－１に関する原告の主張は、Alipayのサーバに電子マネーがチャージされているという点で明らかに誤っている。

ウ　相違点２－２に関する原告の主張については、前記⑴のとおり、甲７の段落【００１９】に「支払人端末は、決済サーバとデータを直接やり取りしない」と明確に記載されている以上、本件審決の認定に誤りはない。

エ　相違点２－６に関する原告の主張については、前記⑵イのとおり、本件発明４の要旨は、電子マネー管理サーバにより送金元と送金先の認証（認証工程の実行）を確実に行い、その後で送金指示を送信（第３受信工程の実行）することで、即時に電子マネーの送金を完了できることであるから、本件審決の認定には誤りはない。

⑷　〔原告の主張〕⑷（本件発明４と甲７発明の相違点に関する容易想到性の判断の誤り）に対し

原告は、相違点２－７に関する容易想到性を主張するが、甲７に開示された決済サーバは、金融機関等の送金や決済処理を行うシステムに相当するものではなく、残高確認を行う必要がないため、甲７の決済サーバに甲２ないし５等に記載された口座残高確認処理を組み合わせる動機付けはないし、組み合わせたとしても本件発明４にはなり得ない。

⑸　〔原告の主張〕⑸（本件発明５と甲７発明の対比、相違点に関する容易想到性の判断の誤り）に対し

原告は、要するに、本件審決の本件発明５についての認定判断は、本件発明４について主張したのと同じ理由により誤りであると主張するが、被告が本件発明４について反論したように、原告の主張には理由がない。

３　取消事由３（無効理由５（本件補正による新規事項追加）に関する判断の誤

り）について

〔原告の主張〕

以下に述べるとおり、本件発明４及び５は、本件出願の当初明細書等の第１実施形態に記載されたものではなく、かつ、その他の実施例等に記載されたものでもないので、無効理由５に関する本件審決の認定及び判断には誤りがある。

⑴　本件出願の当初明細書等の第１実施形態の内容

本件出願の当初明細書等における第１実施形態の内容は以下のとおりである。

管理サーバは、「第１の電子証明書」（デジタル署名を含む。）及び「第２の電子証明書」（デジタル署名を含む。）をそれぞれ作成し、さらに、「第１の電子証明書」に対応する秘密鍵と、「第２の電子証明書」に対応する秘密鍵を作成する。また、管理サーバは、「第１の電子証明書」、「第１の電子証明書」の秘密鍵、及び端末Ａを紐づけて格納し、他方で、「第２の電子証明書」、「第２の電子証明書」の秘密鍵、及び端末Ｂを紐づけて格納する。ここで、作成された「第１の電子証明書」の秘密鍵は、「第１の電子証明書」のデジタル署名を唯一復号化できるものであり、作成された「第２の電子証明書」の秘密鍵は、「第２の電子証明書」のデジタル署名を唯一復号化できるものである（ステップＳ４５ないしＳ５７）。なお、管理サーバに格納されているデジタル署名は、特に暗号化等もされておらず、復号せずともいかなるデジタル署名に対応するものかを把握できるデータである。

その後、端末Ａと端末Ｂは、互いに自己が有するデジタル署名を送信し、自己が有していたデジタル署名を、他の端末から送信されたデジタル署名に置換する。その結果、端末Ａは、「第２の電子証明書のデジタル署名」を有する「第１の電子証明書」（置換した第１の電子証明書）を格納し、端末Ｂは、「第１の電子証明書のデジタル署名」を有する「第２の電子証明書」（置換した第２の電子証明書）を格納することになる。なお、デジタル署名は、そも

そも暗号化されたデータを送信することでセキュアな通信を維持するための技術であるから（甲４６）、第１の実施形態においても、端末間にて「デジタル署名」が送信される場合は、当然ながら暗号化された「デジタル署名」がやり取りされている。

次に、端末Ａは、「第２の電子証明書のデジタル署名」を有する「第１の電子証明書」（置換した第１の電子証明書）を管理サーバに送信し、端末Ｂは、「第１の電子証明書のデジタル署名」を有する「第２の電子証明書」（置換した第２の電子証明書）を管理サーバに送信することになる。この際、「第１の電子証明書のデジタル署名」及び「第２の電子証明書のデジタル署名」は、暗号化された状態で、端末Ａ及び端末Ｂから管理サーバに対して送信される。そして、管理サーバは、端末Ａから受信した「置換した第１の電子証明書」に含まれる「第２の電子証明書のデジタル署名」を、管理サーバに格納されている「第２の電子証明書の秘密鍵」を用いて復号し、端末Ｂから受信した「置換した第２の電子証明書」に含まれる「第１の電子証明書のデジタル署名」を、管理サーバに格納されている「第１の電子証明書の秘密鍵」を用いて復号する。

⑵　本件発明４及び５が本件出願の当初明細書等の第１実施形態に記載されたものでないこと

ア　本件発明４及び５における証明情報等の伝達プロセス

本件発明４及び５は、受金側から管理サーバに対する証明情報の伝達プロセスのみを規定するものである。

イ　本件出願の当初明細書等の段落【００１８】に関する認定の誤り

本件審決は、本件発明４のうち、構成要件４Ｃ－１の「前記送金の際、前記第２ユーザ端末（Ｂ）が、前記第１ユーザ端末（Ａ）から前記第１の証明情報の少なくとも一部を受け取り、前記第２ユーザ端末（Ｂ）を介して前記第１の証明情報の少なくとも一部が前記電子マネー管理サーバに

送信される」との構成は、本件出願の当初明細書等の段落【００１８】の記載における「自己の端末の電子証明書の情報が他の端末から電子マネー管理サーバに送られ」、又は「当該他の端末の電子証明書の情報が自己の端末から電子マネー管理サーバに送られる」という事項に相当するものであって、段落【００１８】の記載によれば、「この時点で取引を行おうとしている２つの端末が特定され」るものである、などと認定する（審決書１２４頁末行ないし１２５頁９行)。

しかし、段落【００１８】には、「自己の端末の電子証明書の情報が他の端末から電子マネー管理サーバに送られ、当該他の端末の電子証明書の情報が自己の端末から電子マネー管理サーバに送られる」と記載されており、「自己の端末の電子証明書の情報が他の端末から電子マネー管理サーバに送られ」と、「当該他の端末の電子証明書の情報が自己の端末から電子マネー管理サーバに送られる」との間に「又は」という用語は存在せず、前後の文脈を考慮すれば、これらの文章は「かつ」で接続されるものと認められるのであって、本件審決の上記認定は誤りである。

また、本件審決は、本件発明４のうち、構成要件４Ｃ－２及び４Ｃ－２－２に係る構成は、「当初明細書等の段落【００１８】の記載における、『さらに、それぞれ送信された電子証明書の照合が電子マネー管理サーバによって行われる。』という事項に相当するものであって、『これにより、電子マネー管理サーバは、電子マネーの送受金を行おうとしている端末を確実に認証することができる。』という効果を奏するものである。」（審決書１２５頁１６ないし２１行）などと認定する。

しかし、本件審決が言及する本件出願の当初明細書等の段落【００１８】の記載は、「それぞれ送信された電子証明書の照合」と記載されていることから明らかなとおり、第１ユーザ端末と第２ユーザ端末が、電子証明書の少なくとも一部を相互に交換した上で、両端末が、それぞれ他の端末の電

子証明書の情報を送信することを前提とした記載である。

そうすると、本件発明４の構成要件４Ｃ－１、４Ｃ－２及び４Ｃ－２－２に係る構成、すなわち受金側からの電子証明書の情報の送信のみで送金を行う形態は本件出願の当初明細書等の段落【００１８】に記載されておらず、本件審決の認定は誤りである。

ウ　本件出願の当初明細書等の段落【００７４】に関する認定の誤り

本件審決は、「『さらに、ステップＳ１１１を省く場合でも、ユーザＡからユーザＢへの電子マネーの送金を行うことは可能である。これは、ステップＳ１１２だけでも取引を行う端末を確定することができるからである。』（【０１００】）と記載されており、本件発明４に係る『認証工程』は、『取引を行おうとしている２つの端末が特定』でき、これら２つの端末について『確実に認証すること』ができれば十分であって、必ずしも段落【００７４】に記載された『ステップＳ１１１およびＳ１１２』における上記（１）～（４）の全てについて判断する必要はないものであるといえる。」（本件審決第９の３⑴ケ、１２６頁６ないし１４行）と述べ、本件出願の当初明細書等の段落【０１００】の記載からすると、第１実施形態においては、段落【００７４】に記載された（１）から（４）までの全てを判断する必要はないとした上で、送金側からの伝達プロセスである（２）及び（３）を省略し、受金側からの伝達プロセスである（１）及び（４）のみを判断すれば足りるという趣旨の認定をしている（本件審決第９の３⑴ケ、１２６頁６ないし２９行）。

しかし、段落【０１００】が述べているのは、仮にステップＳ１１１が省略されたとしても、端末Ａと端末Ｂが、電子証明書の少なくとも一部を相互に交換した上で、両端末が、それぞれ他の端末の電子証明書の情報を送信し、管理サーバが、（３）「第２の電子証明書のデジタル署名」の送信元が端末Ａであるか否か、及び（４）「第１の電子証明書のデジタル署名」

の送信元が端末Ｂであるか否かの両者を判断するため、ステップＳ１１２のみでも取引を行う両端末の特定が可能となり、電子マネーの送金が可能になるということである。したがって、段落【００１００】の記載を根拠として、ステップＳ１１１の対応する二つの判断（１）及び（２）を分断し、かつ、ステップＳ１１２の対応する二つの判断（３）及び（４）を分断し、さらに、判断（２）と判断（３）を組み合わせて省略することを可能とするものであると認定することはできず、段落【００７４】に関する本件審決の上記認定は誤りである。

エ　本件発明４及び５は取引を行う端末の特定及び確実な認証という効果を奏するものでないこと

(ｱ) 本件出願の当初明細書等の記載を前提とすると、本件発明４及び５の構成による場合、受金側の端末から管理サーバに対して送信されるのは、「第２の電子証明書」及びそれに含まれる「第１の電子証明書のデジタル署名」であり、管理サーバは、管理サーバ内に格納されている送金側の端末に対応する秘密鍵を用いて、受領した「第１の電子証明書のデジタル署名」を復号化することになる。しかしながら、受金側の伝達プロセスのみでは、送金側の端末に関する情報は、第１の電子証明書のデジタル署名しか存在せず、管理サーバは、送金側の端末に対応する秘密鍵を特定することができない。

　したがって、受金側からの電子証明書の情報の伝達プロセスのみである本件発明４及び５に係る構成では、取引を行おうとする送金側の端末を特定することができず、かかる態様についてまで、本件出願の当初明細書等の記載から導き出される技術的事項から奏する効果を有するということはできない。

(ｲ) また、本件出願の当初明細書等の段落【００８０】、【００８１】の記載等によれば、本件各発明の効果である「２つの端末について確実に認

証する」とは、正当な送金者と受金者とを認証するという意味であり、電子マネーが不正に入手可能となる端末の認証は「確実な認証」には当たらない。

受金側からの電子証明書の情報の伝達プロセスのみである本件発明４及び５に係る構成の場合には、管理サーバが、受金側から取引両者の証明情報を受信することになるため、受金側が、電子マネーを不正に入手することを目的として、送金側の電子証明書を不正に入手して、当該電子証明書の情報を管理サーバに送信した場合も、送金側の端末について認証されてしまうから、不正送金を防ぐことができず、取引を行う二つの端末を「確実」に認証することはできない。

オ　第１の実施形態は、送金側又は受金側の片方からのみの伝達プロセスをサポートしないこと

本件特許の対応ファミリーであるUS17、408、059の審査過程において、拒絶理由通知が出された。この拒絶理由通知には、送金側の伝達プロセスのみで構成されたクレーム（本件特許の請求項２に対応）に対し、第２実施形態（本件出願の当初明細書等の第１実施形態とほぼ同じ伝達プロセスを有する。）における受金側の伝達プロセスを省略することができない旨の拒絶理由が含まれていたが、被告は、上記クレームは、第２実施形態の図１５にサポートされているのではなく、変形例の図３０にサポートされている旨の応答をしている。すなわち、対応ファミリーの審査において、上記第２実施形態は受金側及び送金側の双方からの伝達プロセスが必要であり、片側の伝達プロセスのみでは発明が成立しない点が指摘され、被告もこの点を認めている。

カ　小括

以上のとおり、本件発明４及び５は、本件出願の当初明細書等の記載のうち、少なくとも第１実施形態に係る記載の事項の範囲内にないため、第

１実施形態の記載を根拠として、本件発明４及び５において、交換した電子証明書の内容を送金側から送信すること、及び送金指示を送金側から送金することを特定していないことが、新規事項の追加に該当しない、とした本件審決の判断は誤りである。

⑶　本件出願の当初明細書等の段落【０１４２】以下の実施例（原告の主張にいう「変形例」）の記載について

本件出願の当初明細書等の段落【０１４２】以下の実施例においては、受金側の端末から送金側の端末に対して、第２の電子証明書のデジタル署名が送信され、送金側の端末から管理サーバに対して、当該デジタル署名が送信される構成が変形例として記載されている。

この変形例による場合、管理サーバは、送金側から取引両者の証明情報を受け付けることになるため、受金側が送金側の電子証明書を不正に入手して何らかの手段で送金側の電子マネーを入手しようとしたとしても、送金側の端末から管理サーバに取引両者の証明情報の送信が行われない限り、送金側から受金側への電子マネーの送金が行われることがないから、受金側のみの行為による不正送金を防止することが可能となる。

これに対し、本件発明４及び５においては、管理サーバが受金側から取引両者の証明情報を受信するため、受金側のみの行為による不正送金を防止することができない。

したがって、本件出願の当初明細書等の変形例に関する記載は、本件発明４及び５とは、受金側のみの行為による不正送金を防止することが可能である点で異なるから、本件発明４及び５が新規事項の追加に該当しないことの根拠とならない。

〔被告の主張〕

⑴　〔原告の主張〕⑵（本件発明４及び５が本件出願の当初明細書等の第１実施形態に記載されたものでないこと）に対し

ア　本件発明４の構成要件４Ｃ－１は、受金側からの伝達プロセスと送金側からの伝達プロセスのうち、受金側からの伝達プロセスに対応するものである。他方、本件出願の当初明細書等の段落【００１８】は、第１実施形態の【図１３】に対応する記載であり、段落【００１８】には、「自己の端末の電子証明書の情報が他の端末から電子マネー管理サーバに送られ、当該他の端末の電子証明書の情報が自己の端末から電子マネー管理サーバに送られる」と、受金側からの伝達プロセスと送金側からの伝達プロセスの双方が記載されている。そのため、本件審決が、段落【００１８】の記載を「自己の端末の電子証明書の情報が他の端末から電子マネー管理サーバに送られ」、又は「当該他の端末の電子証明書の情報が自己の端末から電子マネー管理サーバに送られる」と解釈し、その一方が構成要件４Ｃ－１に該当する旨を述べたことに誤りはない。

イ　本件審決は、本件発明４に係る「『認証工程』は、『取引を行おうとしている２つの端末が特定』でき、これら二つの端末について『確実に認証すること』ができれば十分であって、必ずしも段落【００７４】に記載された『ステップＳ１１１およびＳ１１２』における上記（１）～（４）の全てについて判断する必要はないものである」と認定している（本件審決第９の３⑴ケ、１２６頁１０ないし１４行）。これは、本件各発明の「認証工程」を満たすのに必要な技術事項を、段落【００１８】、【００７４】、【００９９】及び【０１００】の記載を総合し、①ステップＳ１１２から「取引を行おうとしている２つの端末が特定」でき、②ステップＳ１１１から「２つの端末について確実に認証することができ」、③ステップＳ１１２を省略できることから、ステップＳ１１１、１１２の（１）ないし（４）の全てについて判断する必要がない、という三つの点を認定したものである。これらのことからすると、原告の段落【００７４】についての主張は当たらない。

ウ　第１実施形態においては、電子マネー管理サーバは、第１のデジタル署名と、これに関連付けられた第１電子証明書及び第１の秘密鍵を有しているので、第１のデジタル署名を参照することで、それに関連付けられた電子証明書及び秘密鍵を特定できる。

また、本件各発明にいう「確実な認証」の技術的意義は、電子マネー管理サーバにより送金元と送金先の認証を確実に行い、その後で送金を実行することで、即時に電子マネーの送金を完了できることである。原告が指摘する段落【００８１】は、具体的に送金元と送金先からの情報をどのように使用して当該不正を防ぐのかについては一切記載しておらず、単に、第１実施形態のように双方からの情報伝達プロセスを有する場合は不正に強い運用をすることができるという一般論を述べたに過ぎないと解釈するのが相当であるから、本件各発明にいう「確実な認証」の意義が「不正のない認証」であるとする原告の主張は当たらない。

エ　サポート要件に関する特許法上の要件及び審査の基準は国ごとに異なり、国ごとに異なる対応を採るのは当然であるから、他国の特許庁によるサポート要件の認定及び出願人の対応により、我が国の特許庁による審決の認定が誤りであると解すべきことにはならない。

⑵　〔原告の主張〕⑶（本件出願の当初明細書等の段落【０１４２】以下の実施例（原告の主張にいう「変形例」）の記載について）に対し

本件発明４の情報伝達パターンは第１実施形態に開示されているのであり、当初明細書に記載された「変形例」は、第１ないし第４実施形態でカバーされていない送金情報の伝達プロセス、すなわち、受金側であるユーザＢから送金側であるユーザＡに受領額の情報を伝達するプロセスを規定するためにあえて示したものであり、原告が主張したような、特に不正利用の課題を解決するために示したものではない。

４　取消事由４（無効理由３（分割要件違反による新規性又は進歩性欠如）に関

する判断の誤り）について

〔原告の主張〕

本件補正により追加された請求項４及び５は、本件出願の当初明細書等に記載された事項の範囲内にないため、本件出願の当初明細書等と記載が同一である第１世代出願の当初明細書等に記載された事項の範囲内にあるともいえないから、本件出願は、第１世代出願及び最初の原出願に対して分割要件を満たさず、本件各発明の新規性及び進歩性の判断の基準日は、現実の出願日である平成２９年１月１９日であり、平成２８年４月１４日に公開された第１世代出願の公開特許公報（甲１３）に基づき、新規性又は進歩性を欠く。

〔被告の主張〕

本件補正により追加された請求項４及び５は、本件出願の当初明細書等、並びにこれと記載を同一にする第１世代出願及び最初の原出願の当初明細書等に記載された事項の範囲内にあり、本件出願は分割要件を満たしている。

５　取消事由５（無効理由４（本件発明４及び５に係る特許のサポート要件違反）に関する判断の誤り）について

〔原告の主張〕

本件補正により追加された請求項４及び５は、本件出願の当初明細書等に記載された事項の範囲内にないから、本件発明４及び５に係る特許はサポート要件に違反する。

〔被告の主張〕

本件補正により追加された請求項４及び５は、本件出願の当初明細書等と同一の記載である本件明細書等に記載された事項の範囲内にあるから、本件発明４及び５に係る特許にサポート要件違反はない。

第４　当裁判所の判断

１　本件各発明の概要等

本件各発明の特許請求の範囲（前記第２の２）及び本件明細書等の記載（別

紙１）によれば、本件各発明の技術分野、背景技術、発明が解決しようとする課題（後記⑴）、課題を解決するための手段（後記⑵）、効果（後記⑶）、本件明細書等に記載されている実施形態（後記⑷）は、次のとおり認められる。

⑴　技術分野、背景技術、発明が解決しようとする課題

本件各発明は、第１のユーザの端末と第２のユーザの端末とを用いて、第１のユーザが有する電子マネーを第２のユーザに送金する電子マネーの送金方法及びそのシステムに関するものである（段落【０００１】）。

従来のキャッシュレス決済としては、ＩＣチップが埋め込まれたカードや携帯端末を用いる電子マネーを用いる決済と、クレジットカードやデビットカードを用いる決済があった。デビットカードを用いる決済には、カード情報や暗証番号が盗まれて悪用されると、銀行口座にあるはずの現金がなくなり、また、その現金を取り戻すことができない場合もあるので、被害が大きくなる可能性があるところ、ＩＣチップを利用した電子マネー決済の場合には、ＩＣチップが埋め込まれた媒体が盗まれない限りは電子マネーを使用することができないため、デビットカードよりも安全といえた（段落【０００２】～【０００５】、【０００７】～【０００９】）。

しかし、ＩＣチップを利用する電子マネー決済には、①ＩＣチップが埋め込まれたＩＣカードや携帯端末等の媒体が紛失等した場合には、ＩＣカードや携帯端末自体を回収しない限り、そこに格納されている電子マネーを回収することはできないという課題（段落【００１０】）と、②ＩＣチップを利用する決済の場合には、ＩＣチップから決済額相当の電子マネーが減額され、他方で、店舗には現金を支払うための処理が行われることによって利用者から店舗へ支払がされたものとみなされるため、一見電子マネーによる支払がされているように見えるが、実は裏で現金のやりとりがされており、電子マネーが完全に現金の代用として使われているものではないという課題（段落【００１１】、【００１２】）があった。

本件各発明は、上記課題を解決するためになされたもので、電子マネーを現金に極めて近い感覚で取り扱うことを可能とし、しかも電子マネーを操作するための端末の紛失時や盗難時においても電子マネーを失わずに済む電子マネー送金方法及びそのシステムを提供することを目的とする（段落【００１３】）。

⑵　課題を解決するための手段

本件各発明は、第１ユーザが有する第１ユーザ端末と、第２ユーザが有する第２ユーザ端末と、前記第１ユーザ端末および前記第２ユーザ端末と通信回線を介して通信可能であり、前記第１ユーザの電子マネーと前記第２ユーザの電子マネーをそれぞれ記憶する電子マネー管理サーバとを用いて、前記第１ユーザから前記第２ユーザへの電子マネーの送金を行う電子マネー送金方法であって、前記電子マネー管理サーバおよび前記第１ユーザの端末は、前記第１ユーザの情報および／又は前記第１ユーザ端末の情報と関連付けられた第１の電子証明書を格納しているものであると共に、前記電子マネー管理サーバおよび前記第２ユーザ端末は、前記第２ユーザの情報および／又は前記第２ユーザ端末の情報と関連付けられた第２の電子証明書を格納しているものであり、この方法は、前記電子マネー管理サーバが、前記第１ユーザ端末および前記第２ユーザ端末の認証を行う認証工程と、電子マネーに係る受取指示及び金額とを受信する受信工程と、前記金額が前記電子マネー管理サーバに記憶されている前記第１ユーザの電子マネーの残額内であるか否かの判断を少なくとも行う決済判断工程と、前記金額が前記残額内であると判断されると、前記電子マネー管理サーバ内の前記第１ユーザの電子マネーの残額を前記金額の分だけ減額すると共に、前記電子マネー管理サーバ内の前記第２ユーザの電子マネーの残額を前記金額の分だけ増額する決済工程とを行う電子マネー送金方法あるいは電子マネー送金システムである（段落【００１４】～【００３９】）。

段落【００１４】ないし【００１７】に記載された電子マネー送金方法あるいは電子マネー送金システムは、第１受信工程で第１ユーザ端末が第２ユーザ端末から第２の電子証明書の少なくとも一部の情報を受信し、第２受信工程で第２ユーザ端末が第１ユーザ端末から第１の電子証明書の少なくとも一部の情報を受信する。このように第１ユーザ端末と第２ユーザ端末が電子証明書の少なくとも一部を交換した上で、電子マネー管理サーバが、第３受信工程で各ユーザ端末からそれぞれの取引相手の電子証明書の少なくとも一部の情報を受信し、その電子証明書の一部の情報が電子マネー管理サーバに格納されている電子証明書の情報と対応しているか否かを判断する。つまり、自己の端末の電子証明書の情報が他の端末から電子マネー管理サーバに送られ、当該他の端末の電子証明書の情報が自己の端末から電子マネー管理サーバに送られるので、この時点で取引を行おうとしている二つの端末が特定され、さらに、それぞれ送信された電子証明書の照合が電子マネー管理サーバによって行われる。これにより、電子マネー管理サーバは、電子マネーの送受金を行おうとしている端末を確実に認証することができる。第１ユーザ端末が有する第１の電子証明書は第１ユーザ端末と電子マネー管理サーバのみが有するユニーク情報であり、第２ユーザ端末が有する第２の電子証明書は第２ユーザ端末と電子マネー管理サーバのみが有するユニーク情報である。そして、第１の電子証明書の少なくとも一部の情報が第２ユーザ端末によって電子マネー管理サーバに送信され、第２の電子証明書の少なくとも一部の情報が第１ユーザ端末によって電子マネー管理サーバに送信される。そして、電子マネー管理サーバでは第１及び第２ユーザ端末の両方から前記電子証明書の少なくとも一部の情報を受け付けることにより、電子マネーの送受金を行おうとしている端末を認証する。このため、例えば第２ユーザ端末が第１ユーザ端末の電子証明書情報を不正に入手して何らかの手段で第１ユーザの有する電子マネーを入手しようとしても、第１ユーザ端末から電子マネー管

理サーバに自らの電子証明書の情報の送信が行われない限り、第１ユーザから第２ユーザへの電子マネーの送金が行われることがない(段落【００１８】、【００１９】)。

段落【００３０】に記載された電子マネー送金方法は、第１受信工程で第１ユーザ端末が第２ユーザ端末から第２の証明情報の少なくとも一部の情報である第２端末情報を受信し、第２受信工程で第２ユーザ端末が第１ユーザ端末から第１の証明情報の少なくとも一部の情報である第１端末情報を受信する。このように第１ユーザ端末と第２ユーザ端末が互いの証明情報を交換した上で、電子マネー管理サーバが、第３受信工程で各ユーザ端末からそれぞれの取引相手の証明情報を受信し、その証明情報が電子マネー管理サーバに格納されている証明情報と対応しているか否かを判断する。つまり、自己の端末の電子証明書の情報が他の端末から電子マネー管理サーバに送られ、当該他の端末の電子証明書の情報が自己の端末から電子マネー管理サーバに送られるので、この時点で取引を行おうとしている二つの端末が特定され、さらに、それぞれ送信された証明情報の照合が電子マネー管理サーバによって行われる。これにより、電子マネー管理サーバは、電子マネーの送受金を行おうとしている端末を確実に認証することができる（段落【００３１】)。

段落【００３５】に記載された電子マネー送金方法は、第１受信工程で第１ユーザ端末が第２ユーザ端末から第２の証明情報の少なくとも一部の情報である第２端末情報を受信する。このように第１ユーザ端末が第２ユーザ端末から証明情報を受信した上で、電子マネー管理サーバが、第２受信工程で第１ユーザ端末から第２ユーザ端末の証明情報を受信し、第１ユーザ端末から受信した第１ユーザ端末の証明情報と第２ユーザ端末の証明情報が電子マネー管理サーバに格納されている第１及び第２ユーザ端末の証明情報と対応しているか否かを判断する。つまり、第２ユーザ端末の証明情報が第１ユーザ端末から電子マネー管理サーバに送られるので、この時点で取引を行おう

としている二つの端末が特定され、さらに、第１ユーザ端末から送信される取引両者の証明情報の照合が電子マネー管理サーバによって行われる。これにより、電子マネー管理サーバは、電子マネーの送受金を行おうとしている端末を確実に認証することができる。電子マネー管理サーバでは第１ユーザ端末から取引両者の証明情報を受け付けることにより、電子マネーの送受金を行おうとしている端末を認証する。このため、例えば第２ユーザ端末が第１ユーザ端末の電子証明書情報を不正に入手して何らかの手段で第１ユーザの有する電子マネーを入手しようとしても、第１ユーザ端末から電子マネー管理サーバに取引両者の証明情報の送信が行われない限り、第１ユーザから第２ユーザへの電子マネーの送金が行われることがない（段落【００３６】、【００３７】）。

⑶　効果

本件各発明によれば、電子マネーを現金に極めて近い感覚で取り扱うことを可能とし、しかも電子マネーを操作するための端末の紛失時や盗難時においても電子マネーを失わずに済む（段落【００４０】）。

⑷　本件明細書等に記載されている実施形態

本件明細書等には、第１実施形態から第４実施形態が記載されている。

第１実施形態に係る電子マネー送金システムは、例えば買い手であるユーザＡ（第１ユーザ）の有する端末Ａと、売り手としての店舗やその店舗の所有者であるユーザＢ（第２ユーザ）の有する端末Ｂと、各端末Ａ、Ｂとインターネットや移動体通信網等の通信回線を介して通信可能である電子マネー管理サーバ（以下、単に「管理サーバ」という。）３００とを有する（段落【００４４】）。

まず、管理サーバ３００の会員用画面表示処理部３８２によって端末Ａにログイン ＩＤとパスワードを要求する画面が表示され、端末Ａから管理サーバ３００にログイン ＩＤおよびパスワードが送信されると（ステップＳ４１）、

これに応答して会員用画面表示処理部３８２は端末Ａの表示部１３０にログイン後の会員用画面を表示させる（ステップＳ４２）。この会員用画面内には電子証明書の発行要求を行うボタンが配置されており、端末Ａにおいてユーザが電子証明書の発行要求の操作を行うと、端末Ａから管理サーバ３００に電子証明書発行の要求が送信される（ステップＳ４３）。また、この電子証明書発行の要求と共に、又は前記要求の後で、端末Ａから管理サーバ３００に端末Ａの個体情報が送信される（ステップＳ４４）。ここで、ユーザＡは端末Ａにて自己のログインＩＤおよびパスワードを用いて会員用画面にログインし、その状態で電子証明書の発行要求を行っているので、前記個体情報がユーザＡのログインＩＤ、パスワード等と紐付けられて顧客契約マスタ３５１に格納される（図５参照）。また、前記個体情報としては、端末Ａの製造ＩＤを用いることが可能であるが、その他端末Ａに固有の他の情報を用いることも可能である（段落【００５８】）。

続いて、管理サーバ３００は電子証明書発行処理部３８３により、ユーザＡ用に第１の電子証明書を作成し、その第１の電子証明書を端末Ａと紐付けて顧客マスタ格納部３５０に格納する（ステップＳ４５）。ここで、電子証明書発行処理部３８３が作成する第１の電子証明書は、図９に概略を示すように、デジタル署名、公開鍵等を有するものである。また、管理サーバ３００の電子証明書発行処理部３８３は、作成した第１の電子証明書に対応する秘密鍵を同時に作成し、その秘密鍵も第１の電子証明書と紐付けて顧客マスタ格納部３５０に格納する。尚、本実施形態では電子証明書の作成を管理サーバ３００にて行うようにしているが、外部の電子証明書発行業者に依頼して作成することも可能である（段落【００５９】）。

続いて、管理サーバ３００の電子証明書発行処理部３８３は第１の電子証明書を端末Ａに送信し（ステップＳ４６）、端末Ａは受信した第１の電子証明書を端末Ａの証明書格納部１７１に格納する（ステップＳ４７）（段落【００

６０】)。

端末Ｂが管理サーバ３００上における電子マネーの送受金に必要な電子証明書を入手する場合についても、端末Ａについての前述の説明と同等の処理（ステップＳ５１～Ｓ５７）が端末Ｂおよび管理サーバ３００において行われる。また、本実施形態では、端末Ｂ用に第２の電子証明書とその秘密鍵が作成される。なお、第１の電子証明書の秘密鍵は第１の電子証明書のデジタル署名を唯一復号化できるものであり、第２の電子証明書の秘密鍵は第２の電子証明書のデジタル署名を唯一復号化できるものである（段落【００６１】)。

ユーザＡ（買い手）がユーザＢ（店舗などの売り手）から商品を購入し、その代金の支払を電子マネーによって行う場合の処理については、まず、ユーザＡが商品Ｘを購入することを決め、それをユーザＢの端末Ｂ（ＰＯＳ端末）の所に持っていく。端末Ｂにはバーコードリーダ等が付いており、バーコードリーダで商品Ｘに貼付されているバーコードを読み取る。ユーザＡが商品の代金を端末Ｂの表示を見て確認し、支払うことを決めると、端末Ａを使って管理サーバ３００の会員用画面表示処理部３８２が提供する会員用画面にアクセスおよびログインする。そして、表示装置１３０に例えば図１４に示すような支払用画面を表示させ、端末Ａを端末Ｂのリーダライタ２５０に近付けて図１４のＰａｙボタンに指で触れる。これにより、下記のステップＳ１０１ないし１２３が行われ、ユーザＡからユーザＢへの電子マネーの送金が行われる（段落【００６８】、【００６９】)。

まず、端末Ａを端末Ｂのリーダライタ２５０に近付けてＰａｙボタン４１０を指で触れると、端末Ｂは、電子証明書交換処理部２８１により、近距離無線通信を介して第２の電子証明書中のデジタル署名を端末Ａに送信し、端末Ａは、電子証明書交換処理部１８１により、端末Ｂから送信される第２の電子証明書のデジタル署名を受信する（ステップＳ１０１)。そして、端末Ａ

は受信したデジタル署名を証明書格納部や端末Ａのメモリのその他の部分に格納する（ステップＳ１０２）。一方、端末Ａは、電子証明書交換処理部１８１により、近距離無線通信を介して第１の電子証明書中のデジタル署名を端末Ｂに送信し、端末Ｂは、電子証明書交換処理部２８１により、端末Ａから送信される第１の電子証明書のデジタル署名を受信する（ステップＳ１０３）。そして、端末Ｂは受信したデジタル署名を証明書格納部や端末Ｂのメモリのその他の部分に格納する（ステップＳ１０４）。ステップＳ１０１とステップＳ１０３はいずれが先であっても良く、同時であっても良い（段落【００７０】）。

続いて、端末Ａは、電子証明書埋め込み処理部１８２により、自己の有する第１の電子証明書のデジタル署名を前記受信した第２の電子証明書のデジタル署名によって置換することにより、デジタル署名を置換した第１の電子証明書を作成し、それを証明書格納部１７１に格納する（ステップＳ１０５）。一方、端末Ｂでは、自己の有する第２の電子証明書のデジタル署名を前記受信した第１の電子証明書のデジタル署名によって置換することにより、デジタル署名を置換した第２の電子証明書を作成し、それを証明書格納部２７１に格納する（ステップＳ１０６）（段落【００７１】）。

続いて、端末Ａは、デジタル証明書情報送信処理部１８３により、デジタル署名を置換した第１の電子証明書を管理サーバ３００に送信し（ステップＳ１０７）、端末Ｂは、デジタル証明書情報送信処理部２８３により、デジタル署名を置換した第２の電子証明書を管理サーバ３００に送信する（ステップＳ１０８）。この時、端末Ａからの送信データには端末Ａの個体情報が含まれており、端末Ｂからの送信データには端末Ｂの個体情報が含まれている（段落【００７２】）。

次に、管理サーバ３００は、電子証明書情報受付処理部３８５により、端末Ａおよび端末Ｂからデジタル署名を置換した第１および第２の電子証明書

を受信する（ステップＳ１０９）。そして、管理サーバ３００は、電子証明書情報受付処理部３８５により、デジタル署名を置換した第１の電子証明書およびそれに含まれる第２の電子証明書のデジタル署名を、顧客マスタ格納部３５０に格納されている対応している秘密鍵によって復号化すると共に、デジタル署名を置換した第２の電子証明書およびそれに含まれる第１の電子証明書のデジタル署名を、顧客マスタ格納部３５０に格納されている対応している秘密鍵によって復号化する（ステップＳ１１０）（段落【００７３】）。

続いて、管理サーバ３００は、電子証明書情報受付処理部３８５により、（１）復号化された第１の電子証明書のデジタル署名と顧客マスタ格納部３５０に格納されている第１の電子証明書のデジタル署名とが対応しているか否か、および（２）復号化された第２の電子証明書のデジタル署名と顧客マスタ格納部３５０に格納されている第２の電子証明書のデジタル署名とが対応しているか否かを判断する（ステップＳ１１１）。また、管理サーバ３００は、電子証明書情報受付処理部３８５により、（３）第２の電子証明書のデジタル署名の送信元が端末Ａ（第１の電子証明書に対応している端末）であるか否か、及び（４）第１の電子証明書のデジタル署名の送信元が端末Ｂ（第２の電子証明書に対応してる端末）であるか否かを判断する（ステップＳ１１２）。ここで、デジタル署名を置換した第１および第２の電子証明書のデジタル署名以外の部分と、顧客マスタ格納部３５０に格納されている第１および第２の電子証明書のデジタル署名以外の部分との比較により、ステップＳ１１２の判断を行うことができる。または、各端末Ａ、Ｂからの送信データに含まれる個体情報と、顧客マスタ格納部３５０の顧客マスタ３５１に格納されている個体情報とを対比することにより、ステップＳ１１２の判断を行うことが可能である。その他の前記（３）及び（４）を判断できる方法を用いてステップＳ１１２を行うことも可能である。つまり、ステップＳ１１２では、自己の端末（端末Ａ）の電子証明書の情報が他の端末（端末Ｂ）から

管理サーバ３００に送られ、且つ、当該他の端末（端末Ｂ）の電子証明書の情報が自己の端末（端末Ａ）から管理サーバ３００に送られているか否かを判断できれば良い（段落【００７４】）。

次に、上記（１）～（４）が全て対応していると判断されると、電子証明書情報受付処理部３８５により、その判断結果が各端末Ａ、Ｂに送信される（ステップＳ１１３、Ｓ１１４）。続いて、端末Ａからアクセスキー要求処理部１８４によって管理サーバ３００に対してアクセスキーの要求が送信されると（ステップＳ１１５）、管理サーバ３００は、アクセスキー発行処理部３８６により、第１のアクセスキーを端末Ａに送信し（ステップＳ１１６）、端末Ａは第１のアクセスキーをアクセスキー格納部１７２に格納する。アクセスキー発行処理部３８６はアクセスキー発行の要求がある度に毎回異なるユニークなアクセスキーを発行するものである。一方、端末Ｂからアクセスキー要求処理部２８４によって管理サーバ３００に対してアクセスキーの要求が送信されると（ステップＳ１１７）、管理サーバ３００は、アクセスキー発行処理部３８６により、第２のアクセスキーを端末Ｂに送信し（ステップＳ１１８）、端末Ｂは第２のアクセスキーをアクセスキー格納部２７２に格納する。本実施形態では、ステップＳ１１６およびＳ１１８におけるアクセスキーの発行は、ステップＳ１１１およびＳ１１２で上記（１）～（４）が対応していると判断された状態でないと行われない。また、アクセスキー発行処理部３８６は、前記第１のアクセスキーが前記第２のアクセスキーに対応していることが送受金要求受付処理部３８７にて認識されるように、前記第１のアクセスキーと第２のアクセスキーを発行する（段落【００７５】）。

続いて、端末Ａは、送受金要求処理部１８５により、第１のアクセスキーと、端末Ｂの所有者であるユーザＢへの送金指示と、送金を行うべき電子マネー口座の口座番号（表示装置１３０に表示されている電子マネーカードのカード番号）とを管理サーバ３００に送信し（ステップＳ１１９）、管理サー

バ３００は送受金要求受付処理部３８７によりそれらを受信する。一方、端末Ｂは、送受金要求処理部２８５により、第２のアクセスキーと、端末Ａの所有者であるユーザＡからの受取額である３００円と、受取指示とを管理サーバ３００に送信し（ステップＳ１２０）、管理サーバ３００は送受金要求受付処理部３８７によりそれらを受信する（段落【００７６】）。

続いて、管理サーバ３００は、送受金要求受付処理部３８７により、端末Ａから受け取ったアクセスキーと端末Ｂから受け取ったアクセスキーが対応しているか否かを判断する（ステップＳ１２１）。また、管理サーバ３００は、送受金要求受付処理部３８７により、前記受取額が管理サーバ３００の口座データ格納部３６０に格納されているユーザＡの口座残高内であるか否か、より具体的には、端末Ａの表示画面１３０に表示されているカード番号（口座番号）の口座（以下、口座ａと称する）の残高内であるか否かを判断する（ステップＳ１２２）（段落【００７７】）。

続いて、前記ステップＳ１２１でアクセスキーが対応していると共に、前記ステップＳ１２２で残高内であると判断されると、前記管理サーバ３００は、送受金処理部３８８により、口座データ格納部３６０に格納されているユーザＡの口座ａの口座データの残額を前記受取額の分だけ減額すると共に、口座データ格納部３６０に格納されているユーザＢの口座（以下、口座ｂと称する）の口座データの残額を前記受取額の分だけ増額する（ステップＳ１２３）。続いて、管理サーバ３００は、前記第１および第２のアクセスキーを無効化し、これらのアクセスキーによる取引ができないようにする（段落【００７８】）。

このように、第１実施形態では、ステップＳ１０１で第１ユーザ端末としての端末Ａが第２ユーザ端末としての端末Ｂから第２の電子証明書の少なくとも一部の情報を受信し、ステップＳ１０３で端末Ｂが端末Ａから第１の電子証明書の少なくとも一部の情報を受信する。このように端末Ａと端末Ｂが

電子証明書の少なくとも一部を交換した上で、管理サーバ３００が、ステップＳ１０７およびＳ１０８で端末Ａ、Ｂからそれぞれの取引相手の電子証明書の少なくとも１部の情報を受信し、受信した電子証明書の一部の情報が管理サーバ３００に格納されている電子証明書の情報と対応しているか否かを判断する。つまり、自己の端末の電子証明書の情報が他の端末から管理サーバ３００に送られ、当該他の端末の電子証明書の情報が自己の端末から管理サーバ３００に送られるので、この時点で取引を行おうとしている二つの端末が特定され、さらに、それぞれ送信された電子証明書の照合が管理サーバ３００によって行われる。これにより、管理サーバ３００は、電子マネーの送受金を行おうとしている端末Ａ、Ｂを確実に認証することができる（段落【００８０】）。

ここで、端末Ａが有する第１の電子証明書は端末Ａと管理サーバ３００のみが有するユニーク情報であり、端末Ｂが有する第２の電子証明書は端末Ｂと管理サーバ３００のみが有するユニーク情報である。そして、第１の電子証明書の少なくとも一部の情報が端末Ｂによって管理サーバ３００に送信され、第２の電子証明書の少なくとも一部の情報が端末Ａによって管理サーバ３００に送信される。そして、管理サーバ３００では端末Ａ、Ｂの両方から前記電子証明書の少なくとも一部の情報を受け付けることにより、電子マネーの送受金を行おうとしている端末を認証する。このため、例えば端末Ｂが端末Ａの電子証明書情報を不正に入手して何らかの手段でユーザＡの有する電子マネーを入手しようとしても、端末Ａから管理サーバ３００に自らの電子証明書の情報の送信が行われない限り、ユーザＡからユーザＢへの電子マネーの送金が行われることがない（段落【００８１】）。

また、第１実施形態では、前述のように電子マネーの送受金を行おうとしている二つの端末Ａ、Ｂを認証した後、管理サーバ３００が、各端末Ａ、Ｂにアクセスキーを送信し、各端末Ａ、Ｂからアクセスキーと共に送信されて

くる送金指示、電子マネーの受取指示等を受信する。また、管理サーバ３００は、各端末Ａ、Ｂから受信するアクセスキーが対応しているか否かを判断し、その上でユーザＡからユーザＢへの電子マネーの送金を管理サーバ３００内で行う。このようにアクセスキーの発行およびアクセスキーが対応しているか否かの判断も行うので、ユーザＡからユーザＢへの電子マネーの送金をより安全に行うことができる（段落【００８２】）。

また、第１実施形態では、各ユーザＡ、Ｂの電子マネーは管理サーバ３００内に格納されるものであるため、例えば端末Ａを紛失し回収することができない場合でも、その一事をもってユーザＡの電子マネーが減ることはない（段落【００８３】）。

さらに、第１実施形態では、端末Ａと端末Ｂとが互いに有する電子証明書の内容を交換することや、管理サーバ３００から発行されるアクセスキーと共に電子マネーの送金指示および受取指示を送ることで、電子マネーの送金の安全性を確保しつつ、ユーザＡからユーザＢに電子マネーを直接に送ることができる。このため、電子マネーを現金に極めて近い感覚でやりとりすることが可能になる（段落【００８４】）。

第１実施形態では、ステップＳ１１１を省く場合でも、ユーザＡからユーザＢへの電子マネーの送金を行うことは可能である。これは、ステップＳ１１２だけでも取引を行う端末を確定することができるからである（段落【０１００】）。

第２実施形態は、基本的には第１実施形態と同等の構成を有しているが、端末Ｂが端末Ａと同様の携帯電話であり、ユーザＡが送金側、ユーザＢが受金側である。ステップＳ２０１ないし２１８は、第１実施形態のステップＳ１０１ないしＳ１１８と同等の処理が行われる。第２実施形態も第１実施形態と同様の作用効果を奏するものであり、第１実施形態について説明した各種の変更を加えることが可能である（段落【０１０１】～【０１０７】、【図

１５】、【図１６】)。

第３実施形態は、基本的には第２実施形態と同等の構成を有しており、ユーザＡ（送り側）がユーザＢ（受け側）にユーザＡが有する電子マネーカードをギフトとして送る場合について用いることができる。ステップ３０１ないし３１８は、第２実施形態のステップＳ２０１ないし２１８と同等の処理が行われる。第３実施形態も第１実施形態と同様の作用効果を奏するものであり、第１実施形態について説明した各種の変更を加えることができる（段落【０１０８】～【０１１７】、【図１７】～【図２０】)。

第４実施形態は、その基本構成は第１実施形態と同様であり、第４実施形態も第１実施形態と同様の作用効果を奏するものであり、第１実施形態について説明した各種の変更を加えることができる（段落【０１２２】～【０１４１】)。

第１実施形態及び第４実施形態では、端末Ａから端末Ｂに第１の電子証明書のデジタル署名が送信され、それが端末Ｂにおいて第２の電子証明書に埋め込まれ､それが端末Ｂから管理サーバ３００に送信されるものを示した(ステップＳ１０３、１０４、１０６、１０８、４１０、４１１、４１３、４１５等)。これに対し､端末Ａから端末Ｂに第１の電子証明書のデジタル署名が送信されない構成とすることも可能である（段落【０１４２】)。

本実施形態（原告の主張にいう「変形例」）において、端末Ｂは、電子証明書交換処理部２８１により、近距離無線通信を介して第２の電子証明書中のデジタル署名を端末Ａに送信すると共に、ユーザＡからの受取額である３００円を送信し、端末Ａはそれらを受信する（ステップＳ５０１)。そして、端末Ａは受信したデジタル署名を証明書格納部や端末Ａのメモリのその他の部分に格納する（ステップＳ５０２）(段落【０１４４】)。

続いて、端末Ａは、電子証明書埋め込み処理部１８２により、自己の有する第１の電子証明書のデジタル署名を前記受信した第２の電子証明書のデジ

タル署名によって置換することにより、デジタル署名を置換した第１の電子証明書を作成し､それを証明書格納部１７１に格納する(ステップＳ５０３)。次に、端末Ａは、デジタル証明書情報送信処理部１８３により、デジタル署名を置換した第１の電子証明書と前記受取額とを管理サーバ３００に送信する（ステップＳ５０４）(段落【０１４５】)。

次に、管理サーバ３００は、電子証明書情報受付処理部３８５により、端末Ａからデジタル署名を置換した第１の電子証明書を受信する（ステップＳ５０５)。そして、管理サーバ３００は、電子証明書情報受付処理部３８５により、デジタル署名を置換した第１の電子証明書およびそれに含まれる第２の電子証明書のデジタル署名を、顧客マスタ格納部３５０に格納されている対応している秘密鍵によって復号化する（ステップＳ５０６）(段落【０１４６】)。

続いて、管理サーバ３００は、電子証明書情報受付処理部３８５により、（１）復号化された第１の電子証明書と顧客マスタ格納部３５０に格納されている第１の電子証明書とが対応しているか否か、および（２）復号化された第２の電子証明書のデジタル署名と顧客マスタ格納部３５０に格納されている第２の電子証明書のデジタル署名とが対応しているか否かを判断する（ステップＳ５０７)。また、管理サーバ３００は、電子証明書情報受付処理部３８５により、（３）第２の電子証明書のデジタル署名の送信元が端末Ａ（第１の電子証明書に対応している端末）であるか否かを判断する（ステップＳ５０８）(段落【０１４７】)。

本実施形態のように構成した場合でも、端末Ａが端末Ｂから第２の電子証明書の少なくとも一部の情報であるデジタル署名を受信する。このように端末Ａが端末Ｂからデジタル署名を受信した上で、管理サーバ３００が、端末Ａから端末Ｂのデジタル署名を受信し、端末Ａから受信した端末Ａの電子証明書と端末Ｂのデジタル署名が管理サーバ３００に格納されている端末Ａお

よび端末Ｂの電子証明書の情報と対応しているか否かを判断する。つまり、端末Ｂのデジタル署名が端末Ａから管理サーバ３００に送られるので、この時点で取引を行おうとしている二つの端末が特定され、さらに、端末Ａから送信される取引両者の証明情報の照合が管理サーバ３００によって行われる。これにより、管理サーバ３００は、電子マネーの送受金を行おうとしている端末を確実に認証することができる（段落【０１５０】）。

ここで、端末Ａが有する第１の電子証明書は端末Ａと管理サーバ３００のみが有するユニーク情報であり、端末Ｂが有する第２の電子証明書は端末Ｂと管理サーバ３００のみが有するユニーク情報である。そして、第２の電子証明書の少なくとも一部の情報が端末Ａによって管理サーバ３００に送信される。そして、管理サーバ３００では端末Ａから取引両者の証明情報を受け付けることにより､電子マネーの送受金を行おうとしている端末を認証する。このため、例えば端末Ｂが端末Ａの電子証明書を不正に入手して何らかの手段でユーザＡの有する電子マネーを入手しようとしても、端末Ａから管理サーバ３００に取引両者の証明情報の送信が行われない限り、ユーザＡからユーザＢへの電子マネーの送金が行われることがない（段落【０１５１】）。

さらに、本実施形態では、端末Ａに端末Ｂからその証明情報が送信されることや、電子マネーの送金指示および受取指示が送信されることで、電子マネーの送金の安全性を確保しつつ、ユーザＡからユーザＢに電子マネーを直接に送ることができる。このため、電子マネーを現金に極めて近い感覚でやりとりすることが可能になる（段落【０１５３】）。

２　取消事由１（無効理由１（甲１発明を主引用例とする本件発明２及び３の進歩性欠如）に関する判断の誤り）について

⑴　甲１発明の認定について

甲１の記載内容は、別紙２「甲１の記載（翻訳・抜粋)」記載のとおりである（翻訳は、本件審決によるものが相当であると認め、これを用いる。ただ

し、別紙２の１０の部分は、本件審決による翻訳がないため、甲１の訳文として原告が提出したものにある翻訳を用いる。)。

上記のとおりである甲１の記載内容によれば、甲１には本件審決が認定した甲１発明（前記第２の４⑴ア）が記載されていると認められる。

⑵　本件発明２の「証明情報」について

本件発明２における「証明情報」の技術的意義について検討する。

本件発明２における「証明情報」は、「前記第１ユーザの情報および／又は前記第１ユーザ端末（Ａ）の情報と関連付けられた第１の証明情報」（構成要件２Ｂ）と、「前記第２ユーザの情報および／又は前記第２ユーザ端末（Ｂ）の情報と関連付けられた第２の証明情報」（構成要件２Ｂ）である。

本件明細書等の【発明を実施するための形態】（段落【００４３】以下）に記載された第１実施形態ないし第４実施形態では、いずれも、端末Ａが第１の電子証明書を有し、端末Ｂが第２の電子証明書を有し、端末Ａと端末Ｂとの間で電子証明書の少なくとも一部の情報のやり取りがされ、管理サーバ３００が、これらの電子証明書の少なくとも一部の情報を受信する構成となっている（段落【００５７】～【００６１】、【００６８】～【００９０】、【０１０３】、【０１１０】、【０１３６】、【０１４２】、【０１５０】～【０１５３】、【図８】、【図１３】、【図１５】、【図１７】、【図２９】、【図３０】）。これらの実施例において、電子証明書以外の「証明情報」が取り扱われていることを窺わせる記載は存在しない。

また、本件明細書等において、「電子証明書」と「証明情報」の差異に関する記載が存在するとは認められない。むしろ、段落【０１４２】以下の実施形態（原告の主張にいう「変形例」）に関する段落【０１５０】には、「このように端末Ａが端末Ｂからデジタル署名を受信した上で、管理サーバ３００が、端末Ａから端末Ｂのデジタル署名を受信し、端末Ａから受信した端末Ａの電子証明書と端末Ｂのデジタル署名が管理サーバ３００に格納されている

端末Ａ及び端末Ｂの電子証明書の情報と対応しているか否かを判断する。つまり、端末Ｂのデジタル署名が端末Ａから管理サーバ３００に送られるので、この時点で取引を行おうとしている二つの端末が特定され、さらに、端末Ａから送信される取引両者の証明情報の照合が管理サーバ３００によって行われる。」との記載があり、段落【０１５１】には、「ここで、端末Ａが有する第１の電子証明書は端末Ａと管理サーバ３００のみが有するユニーク情報であり、端末Ｂが有する第２の電子証明書は端末Ｂと管理サーバ３００のみが有するユニーク情報である。そして、第２の電子証明書の少なくとも一部の情報が端末Ａによって管理サーバ３００に送信される。そして、管理サーバ３００では端末Ａから取引両者の証明情報を受け付けることにより、電子マネーの送受金を行おうとしている端末を認証する。」との記載がある。上記各記載の内容からすると、これらの段落において、「証明情報」は「電子証明書」を指すものとして用いられていると認められる。

以上によれば、本件発明２の「第１の証明情報」及び「第２の証明情報」は、それぞれ、本件明細書等の「第１の電子証明書」、「第２の電子証明書」に対応すると認められる。

本件明細書等によれば、第１の電子証明書は、端末Ａから電子証明書発行の要求を受けて、管理サーバ３００でデジタル署名、公開鍵等を有するものとして作成され、端末Ａと紐付けて顧客マスタ格納部３５０に格納され、その後端末Ａに送信される（段落【００５８】～【００６０】）。電子証明書は、外部の電子証明書発行業者に依頼して作成することも可能である（段落【００５９】）。第２の電子証明書も、同様に、端末Ｂから電子証明書発行の要求を受けて、管理サーバ３００でデジタル署名、公開鍵等を有するものとして作成され、端末Ｂと紐付けて顧客マスタ格納部３５０に格納されるものである（段落【００６１】）。第１の電子証明書の秘密鍵は第１の電子証明書のデジタル署名を唯一復号化できるものであり、第２の電子証明書の秘密鍵は第

２の電子証明書のデジタル署名を唯一復号化できるものである（段落【００６１】）。

そして、上記各段落の記載及び「証明情報」において「証明」の語が用いられていることを考慮すると、本件発明２の「証明情報」は、利用者及び／又は利用者端末を証明する情報であると解される。

以上を総合すると、本件発明２の「証明情報」は、ユーザ端末から発行の要求を受けて管理サーバで又は電子証明書発行業者へ依頼して作成される情報であり、認証のためのデジタル署名や公開鍵等を有する電子証明書のような利用者及び／又は利用者端末を証明する情報であるという技術的意義を有するものと認められる。

そうすると、「証明情報」は、「端末Ａ（又は端末Ｂ）の製造ＩＤ」のように端末Ａ、端末Ｂに固有の情報である「個体情報」や、「ユーザＡ（又はユーザＢ）のログインＩＤ」、「パスワード」、「メールアドレス」、「電子マネー口座番号」とは異なる情報であるといえる。

⑶　本件発明２と甲１発明の相違点について

本件発明２の「証明情報」が上記⑵のとおり解されることを前提に、本件発明２（前記第２の２⑴）と、甲１発明（前記第２の４⑴ア）とを対比すると、その相違点は、本件審決が認定した相違点（相違点１－１ないし１－８、前記第２の４⑴ウ(ｲ)ないし(ｹ)）のとおりであると認められる。

⑷　本件発明２と甲１発明の相違点に関する容易想到性について

本件発明２と甲１発明の相違点のうち相違点１－２、１－３及び１－５に係る本件発明２の構成の容易想到性について検討する。

甲１発明において管理サーバ及び第１ユーザの端末（Ａ）又は第２ユーザ端末（Ｂ）が格納している「前記第１ユーザ端末（Ａ）の情報」又は「前記第２ユーザの情報および／又は前記第２ユーザ端末（Ｂ）の情報」を、前記⑵のとおりの技術的意義を有する「証明情報」とすることによって、相違点

１－２に係る本件発明２の構成とすることについては、当業者がこのようなことを想到すると認めるべき根拠となる副引例又は技術常識があるとは認められず、当業者が容易に想到するに至る動機付けを有するとも認められないから、当業者が容易に想到できたものであるとは認められない。

同様に、相違点１－３についても、甲１発明において「前記第２ユーザ端末（Ｂ）が出力した、第２端末情報」を取得するとされているものを、前記⑵のとおりの技術的意義を有する「証明情報」の少なくとも一部の情報を取得するものとすることによって、相違点１－３に係る本件発明２の構成とすることについては、当業者がこのようなことを想到すると認めるべき根拠となる副引例又は技術常識があるとは認められず、当業者が容易に想到するに至る動機付けを有するとも認められないから、当業者が容易に想到できたものであるとは認められない。

また、相違点１－５についても、甲１発明において、「受信した前記第１端末情報」と対応しているか否かの判断は「格納されている前記第１ユーザ端末（Ａ）に関する情報」と行い、「前記第２端末情報」と対応しているか否かの判断は「格納されている前記第２ユーザ端末（Ｂ）に関する情報」と行うとされているものを、「前記第１の証明情報」や「前記第２の証明情報」と対応しているか否かで判断するものとすることによって、相違点１－５に係る本件発明２の構成とすることについては、当業者がこのようなことを想到すると認めるべき根拠となる副引例又は技術常識があるとは認められず、当業者が容易に想到するに至る動機付けがあるとも認められないから、当業者が容易に想到できたものであるとは認められない。

したがって、相違点１－１、１－４、１－６ないし１－８について検討するまでもなく、本件発明２は、甲１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ものとは認められない。

⑸　本件発明３と甲１発明の対比、相違点に関する容易想到性について

本件発明３は、本件発明２の「電子マネー送金方法」の発明を「電子マネー送金システム」として記載した発明であって、本件発明３と、甲１発明をシステムの発明として表現した発明とを対比すると、相違点１－１ないし１－８と同様の相違点を有すると認められる。そうすると、相違点１－２、１－３及び相違点１－５と同様の相違点に係る本件発明３の構成については、上記⑷のとおり、甲１発明及び周知技術に基づいて当業者が容易に想到できたものとは認められない。

したがって、相違点１－１、１－４、１－６ないし１－８について検討するまでもなく、本件発明３も、甲１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ものとは認められない。

⑹　原告の主張（前記第３の１〔原告の主張〕）に対する判断

ア　〔原告の主張〕⑴（甲１発明の認定の誤り）について

(ｱ)〔原告の主張〕⑴ア（甲１の「アカウント情報」は金銭的価値（残高等）に関する情報を含むこと）について

原告は、甲１の「アカウント情報」は金銭的価値（残高等）に関する情報を含むと主張する。

しかし、甲１の８頁１５行から９頁１行にかけての記載には、「ネットワーク仲介システム３においてモバイル決済を実現する装置は、取引情報の画像解析装置及び前記取引情報を処理するための処理装置を含み、処理装置には取引双方のアカウント情報が予め設定され、・・・処理装置は対応するアカウント情報に基づいて取引を行う。」との記載があるところ（別紙２の２）、「アカウント情報」が残高等の金銭的価値を含むと解することは、「アカウント情報」が処理装置に「予め設定される」ものであることと整合しない。

また、甲１には、ネットワーク仲介システムが運営業者のみであってもよいとの記載はあるが（別紙２の２）、金銭的価値の記憶及び管理に係

る構成については具体的な記載があるとは認められないから、ネットワーク仲介システムがアカウント情報として金銭的価値を記憶し、管理することが甲１に記載されているとも認められない。

銀行とは異なる運営業者によって管理されているものであって、金銭的価値として電子マネーを記憶、管理するサーバが、本件優先日の前に周知又は公知であったとしても、当該技術自体が甲１に記載されていたと認められることにはならず、甲１の記載から自明な事項ともいえない。

したがって、甲１の「アカウント情報」は金銭的価値（残高等）に関する情報を含むとは認められず、原告の上記主張は、採用することができない。

(ｲ) 〔原告の主張〕⑴イ（甲１の「ネットワーク仲介システム」は「移動端末」から出力された「移動端末ユーザの身分情報」を受信するといえること）について

原告は、甲１の「ネットワーク仲介システム」は「移動端末」から出力された「移動端末ユーザの身分情報」を受信するといえると主張する。

しかし、甲１には、移動端末ユーザの身分情報は、移動端末が取得された画像情報をネットワーク仲介システムに送信する場合、ネットワーク装置MSC及び／又はHLRにより関連身分記述情報を画像情報とともにネットワーク仲介システムに自動的に送信するものであると明示されているから（別紙２の６）、原告の上記主張は、採用することができない。

甲１には上記のように記載されているのに対し、本件発明２では、管理サーバは第１端末情報を第１ユーザ端末から受信すると記載されているのであるから（本件発明２の構成２Ｃ－２、２Ｃ－２－１）、本件審決がこの点を相違点１－４として認定したことが誤りであるとはいえない。

(ｳ) 〔原告の主張〕⑴ウ（甲１には取引金額とともに送金指示が送信される態様が記載されていること）について

原告は、甲１の１４頁５ないし８行の記載を根拠として、甲１には、「取引を実行する命令」を送信するトリガとなる「確認通知」を必要としない態様が開示されているとして、甲１には取引金額とともに送金指示が送信される態様が記載されていると主張する。

甲１には、「ネットワーク仲介システムが移動端末に送信した確認通知には取引金額、取引シリアル番号又は取引明細などの情報が含まれている。Ｓ８：移動端末は取引通知を受信した後に確認を行う。正しいと確認した場合、取引を実行する命令を返信し、問題が見つかった場合、取引をキャンセルする命令を返信する。移動端末が取引を確認する時に、ユーザの利益を保護するために、端末に予め設定されたパスワードを入力することにより確認することができる。」（別紙２の７）と記載されていることから、移動端末は、確認通知を受信した後に確認を行い、正しいと確認した場合、取引を実行する命令を返信することが認められる。

そして、原告の指摘する甲１の１４頁５行ないし８行には、「上記方法によると、売り手と買い手とが一回の取引を完了するには、ユーザが画像を一回走査して送信し、『確認』を一回押し、パスワードを一回入力することだけで済む。実際には、上記実施例において、上記の『『確認』の一回押し』というステップの操作も省略することができ、したがって、該方法は取引における売買双方の入力を大幅に簡略化し、取引の効率を向上させる。」（別紙２の１０）と記載されており、ここには、「『確認』の一回押し」というステップの操作の省略が記載されているのみであって、このステップが省略されたとしても、パスワードの処理の後に移動端末が「取引を実行する命令」（送金指示）を送信することを省略することまでも記載されているとは認められない。

したがって、甲１には、「取引を実行する命令」を送信するトリガとなる「確認通知」を必要としない態様が開示されているとの原告の主張を

採用することはできない。

(ｴ) なお、原告は、前記第３の１〔原告の主張〕⑴のとおり、本件審決の甲１発明の認定に誤りがあると主張するところ、その主張内容からすると、前記第３の１〔原告の主張〕⑴ア（甲１の「アカウント情報」は金銭的価値（残高等）に関する情報を含むこと）の主張は相違点１－１の前提となる甲１発明の認定に関するもの、同イ（甲１の「ネットワーク仲介システム」は「移動端末」から出力された「移動端末ユーザの身分情報」を受信するといえること）の主張は相違点１－４の前提となる甲１発明の認定に関するもの、同ウ（甲１には取引金額とともに送金指示が送信される態様が記載されていること）の主張は相違点１－７の前提となる甲１発明の認定に関するものであると認められる。しかし、前記⑷、⑸のとおり、相違点１－１、１－４及び１－７について検討するまでもなく、本件発明２及び３は、甲１発明及び周知技術に基づいて容易想到であると認められないのであるから、この点からしても、原告の上記各主張は、本件発明２及び３の容易想到性に関する判断を左右しない。

イ 〔原告の主張〕⑵（本件発明２の認定の誤り）について

原告は、本件発明２における「証明情報」の技術的意義は、「端末の認証のために用いられるものであり、端末とサーバ間でユニークな情報」と認定されるべきであり、本件審決が認定するのと異なり、ユーザ端末からの発行の要求は必要なく、また、電子マネー管理サーバで作成される必要もないと主張する。

しかし、本件発明２の「証明情報」の意義は前記⑵のとおりであって、原告の主張は採用することができない。また、別件訴訟において、被告が本件発明２の「証明情報」について主張した内容をもって、本件明細書等から認定できる本件発明２の「証明情報」の技術的意義の内容が左右されることはない。

ウ　〔原告の主張〕⑶（本件発明２と甲１発明の相違点の認定の誤り）について

原告は、本件発明２と甲１発明の相違点に関する本件審決の認定には誤りがあると主張する。

しかし、原告の主張のうち、相違点１－１に関する主張、相違点１－４に関する主張及び相違点１－７に関する主張は、それぞれ、前記第３の１〔原告の主張〕⑴アの主張、同イの主張、同ウの主張を前提とするものであるところ（前記ア(ｴ)）、前記第３の１〔原告の主張〕⑴アないしウの主張を採用することができないことは前記ア(ｱ)ないし(ｳ)のとおりであるから、上記各相違点に関する原告の主張も採用することができない。

相違点１－２、１－３及び１－５に関する原告の主張は、本件発明２の「証明情報」の意義に関する本件審決の認定が誤りであるとの原告の主張を前提とするものであるところ、本件審決の上記認定が誤りと認められないことは上記⑵のとおりであるから、上記各相違点に関する原告の主張も採用することができない。

また、相違点１－３に関して、原告は、甲１発明における撮像機能又は図形走査機能を利用した画像情報の取得は、本件発明２における「受信」に該当すると主張する。しかし、甲１発明における撮像機能又は図形走査機能を利用した画像情報の取得は、甲１中のこれらの文言の用法に照らせば、画像を撮ることあるいは図形を走査することであり、他からの信号を受け取るものではないから、本件発明２における「受信」に該当しないとの本件審決の認定が誤りであるとは認められず、原告の上記主張は採用することができない。

相違点１－６に関して、原告は、甲１発明では、移動端末ユーザのIMSI、ESN、移動端末番号などの情報を用いて、及び、レジサービス端末のIDなどを用いて、各ユーザの正当性を検証することは、端末の情報を用いての

正当性検証になるため、実質的に各端末の認証を行うことと同義であると主張する。しかし、端末の情報を用いて各ユーザを認証することと、端末の情報を用いて各端末を認証することとは、認証の対象が異なり、両者が実質的に同義であるとはいえず、原告の上記主張は採用することができない。

以上のとおり、本件発明２と甲１発明の相違点に関する本件審決の認定に誤りがあるとは認められない。

エ　〔原告の主張〕⑷（本件発明２と甲１発明の相違点に関する容易想到性の判断の誤り）について

原告は、本件発明２と甲１発明の相違点１－２、１－３及び１－５に関し、電子決済分野において暗号化技術を用いてセキュリティを向上させることは周知技術又は技術常識であり、甲１発明の移動端末又はレジサービス端末の身分情報に暗号化技術を用いて、本件発明２の上記の相違点に係る構成を想到することは容易であり、上記の相違点に関する本件審決の判断には誤りがあると主張する（〔原告の主張〕⑷ウ）。

しかし、仮に、電子決済分野において暗号化技術を用いることが周知技術又は技術常識であると認められるとしても、そのことをもって、本件発明２の相違点１－２、１－３及び１－５に係る構成を当業者が容易に想到し得ると認められることにはならず、容易に想到するに至る動機付けが認められることにもならない。

その余の相違点に関する主張については、相違点１－２、１－３及び１－５について容易想到と認められない以上、本件発明２及び３の進歩性に関する判断を左右しない。

⑺　取消事由１に関する結論

以上によれば、無効理由１（本件発明２及び３の甲１発明に対する進歩性欠如）に関する本件審決の判断に誤りはなく、取消事由１には理由がない。

3　取消事由２（無効理由２（甲７発明を主引用例とする本件発明４及び５の進歩性欠如）に関する判断の誤り）について

⑴　甲７発明の認定について

甲７の記載内容は、別紙３「甲７の記載（翻訳・抜粋)」記載のとおりである（翻訳は、本件審決によるものが相当であると認め、これを用いる。)。

上記のとおりである甲７の記載内容によれば、甲７には本件審決が認定した甲７発明（前記第２の４⑵ア）が記載されていると認められる。

⑵　本件発明４と甲７発明の相違点について

本件発明４における「証明情報」の技術的意義について検討する。

本件発明４における「証明情報」は、「前記第１ユーザの情報および／又は前記第１ユーザ端末（Ａ）の情報と関連付けられた第１の証明情報」（構成要件４Ｂ）と、「前記第２ユーザの情報および／又は前記第２ユーザ端末（Ｂ）の情報と関連付けられた第２の証明情報」（構成要件４Ｂ）である。そして、本件発明２における「証明情報」の技術的意義に関して前記２⑵で本件明細書等の記載に基づいて述べたことは、本件発明４における「証明情報」にも当てはまる。したがって、本件発明４の「証明情報」は、本件発明２の「証明情報」と同じく、ユーザ端末から発行の要求を受けて管理サーバで又は電子証明書発行業者へ依頼して作成される情報であり、認証のためのデジタル署名や公開鍵等を有する電子証明書のような利用者及び／又は利用者端末を証明する情報であるという技術的意義を有するもの（前記２⑵）と認められる。

本件発明４の「証明情報」が上記のとおり解されることを前提に、本件発明４（前記第２の２⑶）と、甲７発明（前記第２の４⑵ア）とを対比すると、その相違点は、本件審決が認定した相違点（相違点２－１ないし２－７、前記第２の４⑵イ(ｲ)ないし(ｸ)）のとおりであると認められる。

⑶　本件発明４と甲７発明の相違点に関する容易想到性について

本件発明４と甲７発明の相違点のうち相違点２－３及び２－５に係る本件発明４の構成の容易想到性について検討する。

甲７発明において管理サーバ（決済サーバ）及び第２ユーザの端末（Ｂ）（受取人端末）が格納している「前記第２ユーザの情報」である「受取人口座番号」を、上記⑵のとおりの技術的意義を有する「証明情報」である、「第２ユーザの情報」と関連付けられた「第２の証明情報」とすることによって、相違点２－３に係る本件発明４の構成とすることについては、当業者がこのようなことを想到すると認めるべき根拠となる副引例又は技術常識があるとは認められず、当業者が容易に想到するに至る動機付けがあるとも認められないから、当業者が容易に想到できたものであるとは認められない。

同様に、相違点２－５についても、甲７発明においては、管理サーバに「第２の証明情報」を格納するものではなく、「第２ユーザ端末（Ｂ）」（受取人端末）と「第２の証明情報」とが対応しているか否かの判断を行うものではないところ、これを「第２ユーザ端末（Ｂ）」（受取人端末）に「第２の証明情報」を格納するものとし、「第２ユーザ端末（Ｂ）」（受取人端末）と「第２の証明情報」とが対応しているか否かの判断を行うものとすることによって、相違点２－５に係る本件発明４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るとは認められない。

したがって、相違点２－１、２－２、２－４、２－６及び２－７について検討するまでもなく、本件発明４は、甲７発明及び周知技術に基づいて、当業者が容易に発明することができたものとは認められない。

⑷　本件発明５と甲７発明の対比、相違点に関する容易想到性について

本件発明５は、本件発明４の「電子マネー送金方法」の発明を「電子マネー送金システム」として記載した発明である。ただし、本件発明４では、電子マネー管理サーバ（３００）が認証工程の後に「前記第２ユーザから、前記第１ユーザからの電子マネーの受取指示と、受取額とを受信する第３受信

工程」を行うものであるのに対し、本件発明５は、これらの処理の順番について特定がされているとは認められない。

そのため、本件発明５と、甲７発明をシステムの発明として表現した発明とを対比すると、本件発明４と甲７発明の相違点２－１ないし２－７のうち、本件発明４が認証工程の後に「前記第２ユーザから、前記第１ユーザからの電子マネーの受取指示と、受取額とを受信する第３受信工程」を行うことを前提とする相違点２－６に相当する相違点は存在しない。しかし、相違点２－１ないし２－５及び２－７と同様の相違点を有すると認められる。

そして、相違点２－３及び２－５と同様の相違点に係る本件発明５の構成については、上記⑶のとおり、甲７発明及び周知技術に基づいて当業者が容易に想到できたものとは認められない。

したがって、相違点２－１、２－２、２－４、２－７について検討するまでもなく、本件発明５も、甲７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ものとは認められない。

⑸　原告の主張（前記第３の２〔原告の主張〕）に対する判断

ア　〔原告の主張〕⑴（甲７発明の認定の誤り）について

(ｱ)〔原告の主張〕⑴ア（甲７の「決済サーバ」は「支払人端末」と通信をすること）について

原告は、甲７において「決済サーバ」が「支払人端末」と通信をしないとの本件審決の認定は誤りであると主張する。

しかし、本件審決は、甲７発明に関し、「支払人端末は、決済サーバとデータを直接やり取りしないものであり、」と認定しており、支払人端末が決済サーバとデータを間接的にもやり取りしないとは認定していない。

そして、甲７の段落【００１９】には、「特に、受取人端末および決済サーバは、インターネット、無線ネットワーク、専用ネットワーク、または、任意の他の適切な接続で通信できるが、支払人端末は、決済サー

バとデータを直接やり取りしない。」と明確に記載されており（別紙３の２）、これによれば、本件審決の上記認定に誤りがあるとは認められない。

(ｲ) 〔原告の主張〕⑴イ（甲７の「決済サーバ」は電子マネーを記憶、管理すること）について

原告は、甲７の「決済サーバ」は電子マネーを記憶、管理するものであると主張し、「甲７の記載及び技術常識によれば、『決済サーバ』自体が電子のマネーを記憶、管理するものであるとはいえない」との本件審決の認定は誤りであると主張する。

しかし、甲７には、決済データを処理するための方法について記載され、さらに決済サーバはAlipay.comなどのサードパーティ決済サービス業者によって提供されることは記載されているが（段落【００１８】、別紙３の２）、金銭的価値の記憶及び管理に係る構成について具体的な記載があるとは認められないから、ネットワーク仲介システムがアカウント情報として金銭的価値を記憶し、管理していることが甲７に記載されているとも認められない。電子マネーが管理されるサーバが本件優先日前に周知ないし公知であったとしても、当該事実が甲７自体に記載されていると認めることはできず、甲７の記載から自明な事項であるともいえない。

決済サーバがAlipayなどの業者によって提供されるとの記載が甲７に存在すること、Alipayが甲７に係る特許の出願人であること、Alipayが電子マネーを用いてモバイル決済を行うシステムを有していたことが認められるとしても、これらの事実は、「決済サーバ」自体が電子マネーを記憶、管理するものと認めるに足りるものではない。

(ｳ) なお、原告は、前記第３の２〔原告の主張〕⑴のとおり、本件審決の甲７発明の認定に誤りがあると主張するところ、その主張内容からすると、前記第３の２〔原告の主張〕⑴ア（甲７の「決済サーバ」は「支払

人端末」と通信をすること）の主張は相違点２－２の前提となる甲７発明の認定に関するもの、同イ（甲７の「決済サーバ」は電子マネーを記憶、管理すること）の主張は相違点２－１の前提となる甲７発明の認定に関するものであると認められる。しかし、前記⑶のとおり、相違点２－１及び２－２について検討するまでもなく、本件発明４及び５は、甲７発明及び周知技術に基づいて容易想到であると認められないのであるから、この点からしても、原告の上記各主張は、本件発明４及び５の容易想到性に関する判断を左右しない。

イ　〔原告の主張〕⑵（本件発明４の認定の誤り）について

(ｱ)　〔原告の主張〕⑵ア（「証明情報」の技術的意義の認定が誤っていること）について

原告は、本件審決における「証明情報」の技術的意義の認定に誤りがあると主張する。しかし、「証明情報」の意義は前記２⑵のとおりであり、この意義を前提とすると、本件発明４と甲７発明の相違点に関する本件審決の認定並びに相違点２－３及び２－５の容易想到性に関する本件審決の判断に誤りがあるとは認められない。

(ｲ)　〔原告の主張〕⑵イ（「第３受信工程」は「認証工程」を行った後に実行されるものに限定されないこと）について

原告は、本件発明４の「第３受信工程」は「認証工程」を行った後に実行されるものに限定されないと主張する。

しかし、本件発明４は、電子マネーの送金方法に係る方法の発明であるところ、その構成要件の記載には、認証から決済までの工程が特定されているが、「受取額」を受信する「第３工程」は、「認証工程」の後に記載されており、この記載内容からすれば、工程として「第３工程」が「認証工程」の後に行われるものとして特定されていると認められる。被告が第１世代出願及び本件出願に際して提出した上申書の記載内容を

もって、構成要件の記載から解釈される本件発明４の内容は左右されない。

また、原告の上記主張は、本件発明４の構成要件のうち、本件発明４と甲７発明の相違点２－６の前提となる本件発明４の構成要件に関する主張であるが、前記⑶及び⑷のとおり、相違点２－６について検討するまでもなく、本件発明４及び５は甲７発明及び周知技術に基づいて容易想到であると認められないから、この点からしても、原告の上記主張は本件発明４及び５の容易想到性に関する結論を左右しない。

ウ　〔原告の主張〕⑶（本件発明４と甲７発明の相違点の認定の誤り）について

原告は、本件発明４と甲７発明の相違点に関する本件審決の認定には誤りがあると主張する。

しかし、原告の主張のうち、相違点２－１に関する主張、相違点２－２に関する主張及び相違点２－６に関する主張は、それぞれ、前記第３の２〔原告の主張〕⑴イの主張、同⑴アの主張、同⑵イの主張を前提とするものであるところ（前記ア(ｳ)、イ(ｲ)）、前記第３の２〔原告の主張〕⑴ア及びイ並びに同⑵イの主張を採用することができないことは前記ア(ｱ)及び(ｲ)並びにイ(ｲ)のとおりであるから、上記各相違点に関する原告の主張も採用することができない。

相違点２－３ないし２－５に関する主張は、本件発明４の「証明情報」の意義に関する本件審決の認定が誤りであるとの原告の主張を前提とするものであるところ、「証明情報」の意義に関する原告の主張を採用することができないことは前記⑵のとおりであるから、上記各相違点に関する原告の主張も採用することができない。

エ　〔原告の主張〕⑷（本件発明４と甲７発明の相違点に関する容易想到性の判断の誤り）について

(ｱ) 原告は、本件発明４と甲７発明の相違点２－３及び２－５につき、仮に、本件審決による「証明情報」の認定を前提に、上記各相違点が存在するとしても、電子決済分野において、取引を行うユーザ又は端末の認証に用いる情報に暗号化技術を用いてセキュリティを向上させることは、周知技術又は技術常識であったといえるから、甲７発明における「受取人口座番号」、「支払人口座番号」、「決済パスワード」に暗号化技術を用いることは、当業者にとって容易になし得たことであると主張する（〔原告の主張〕⑷ウ）。

しかし、仮に、電子決済分野において暗号化技術を用いることが周知技術又は技術常識であると認められるとしても、そのことをもって、「電子マネー管理サーバ（３００）」が「第２のユーザ端末（Ｂ）」と関連付けられた「第２の証明情報」を格納するという、相違点２－３に係る本件発明４の構成を当業者が容易に想到し得ると認められることにはならず、そのような構成を容易に想到するに至る動機付けが認められることにもならないし、また、「電子マネー管理サーバ（３００）」が「第２のユーザ端末（Ｂ）が前記電子マネー管理サーバ（３００）に格納されている前記第２の証明情報と対応しているか否かの判断」を行うことにより「前記第２ユーザ端末（Ｂ）の認証を行う」、「前記第１のユーザ端末（Ａ）が前記電子マネー管理サーバ（３００）に格納されている前記第１の証明情報と対応しているか否かの判断」を行うことにより「前記第１ユーザ端末（Ａ）」「の認証を行う」という、相違点２－５に係る本件発明４の構成を当業者が容易に想到し得ると認められることにはならず、容易に想到するに至る動機付けが認められることにもならない。したがって、原告の上記主張を採用することはできない。

(ｲ) 原告は、仮に本件発明４と甲７発明の相違点として相違点２－１、２－２及び２－６が存在するとしても、これらの相違点に係る本件発明４

の構成は当業者が容易に想到し得たことであると主張する（〔原告の主張〕⑷エ）。

しかし、上記(ｱ)のとおり、相違点２－３及び２－５に係る本件発明４の構成が容易想到と認められないから、上記の原告の主張は、本件発明４及び５の進歩性に関する判断を左右しない。

オ　原告の主張⑸（本件発明５と甲７発明の対比、相違点に関する容易想到性の判断の誤りについて）について

原告は、相違点２－３及び２－５を含む相違点２－１ないし２－６が、そもそも本件発明５と甲７発明の相違点ではないこと、これらの相違点が存在するとしても、これらの相違点に係る本件発明５の構成は、周知技術又は技術常識に基づいて容易想到であると主張する。

しかし、前記⑷のとおり、本件発明５と、甲７発明をシステムの発明として表現した発明を対比すると、相違点２－１ないし２－５及び２－７と同様の相違点が存在すると認められ、相違点２－３及び２－５と同様の相違点に係る本件発明５の構成については、甲７発明及び周知技術に基づいて当業者が容易に想到できたものとはいえないから、本件発明５は、甲７発明及び周知技術に基づいて当業者が容易に想到できたものとはいえない。したがって、原告の上記主張を採用することはできない。

⑹　取消事由２に関する結論

以上によれば、無効理由２（甲７発明を主引用例とする本件発明４及び５の進歩性欠如）に関する本件審決の判断に誤りはなく、取消事由２には理由がない。

４　取消事由３（無効理由５（本件補正による新規事項追加）に関する判断の誤り）について

⑴　新規事項追加の判断の枠組み

前記第２の１⑵のとおり、被告は、本件補正によって、特許請求の範囲の

請求項４及び５を追加したが、明細書、特許請求の範囲又は図面について補正をするときは、願書に最初に添付した明細書、特許請求の範囲又は図面に記載した事項の範囲においてしなければならない(特許法１７条の２第３項)。

上記の「最初に添付した明細書、特許請求の範囲又は図面に記載した事項」とは、当業者によって、明細書、特許請求の範囲又は図面の全ての記載を総合することにより導かれる技術的事項を意味し、当該補正が、このようにして導かれる技術的事項との関係において、新たな技術的事項を導入しないものであるときは、当該補正は「明細書、特許請求の範囲又は図面に記載した事項の範囲内において」するものということができる。

そこで、特許請求の範囲に請求項４及び５を加えた本件補正が、本件出願の当初明細書等の全ての記載を総合することにより導かれる技術的事項との関係において､新たな技術的事項を導入しないものであるか否かを検討する。なお、本件補正では明細書の補正はされなかったから、本件出願の当初明細書等の明細書及び図面の記載は本件明細書等の記載（別紙１。前記第２の１⑵）と同一である。

⑵　請求項４（本件発明４）の構成が本件出願の当初明細書等に記載されていたかについて

ア　構成要件４Ａ

本件特許の特許請求の範囲の請求項４は、前記第２の２⑶のとおりであるところ、請求項４の構成要件４Ａは、請求項２の構成要件２Ａと同一であり、請求項４の「電子マネー送金方法」の前提となる全体構成が、管理サーバ、第１ユーザ端末及び第２ユーザ端末からなり、請求項４の電子マネー送金方法が「第１ユーザから第２ユーザに電子マネーの送金を行う電子マネー送金方法」であることを特定したものである。

本件出願の当初明細書等の段落【００４４】には､「第１実施形態に係る電子マネー送金システム」として､「買い手であるユーザＡ（第１ユーザ）

の有する端末Ａと、売り手としての店舗やその店舗の所有者であるユーザＢ（第２ユーザ）の有する端末Ｂと、各端末Ａ、Ｂとインターネットや移動体通信網等の通信回線を介して通信可能である電子マネー管理サーバ（以下、単に管理サーバと称する）３００とを有する」システムが記載されており、「買い手であるユーザＡ（第１ユーザ）の有する端末Ａ」、「売り手としての店舗やその店舗の所有者であるユーザＢ（第２ユーザ）の有する端末Ｂ」は、それぞれ構成要件４Ａの「第１ユーザが有する第１ユーザ端末（Ａ）」、「第２ユーザが有する第２ユーザ端末（Ｂ）」に対応する。

また、本件出願の当初明細書等の段落【００４９】及び【００５０】には、「管理サーバ３００」の「口座データ格納部３６０」に、口座番号ごとに「口座残高や送受金の履歴」などの「電子マネー口座のデータ」を格納することが記載されているから、「各端末Ａ、Ｂとインターネットや移動体通信網等の通信回線を介して通信可能である電子マネー管理サーバ（以下、単に管理サーバと称する）３００」は、構成要件４Ａの「前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）と通信回線を介して通信可能であり、前記第１ユーザの電子マネーと前記第２ユーザの電子マネーをそれぞれ記憶する電子マネー管理サーバ（３００）」に対応する。

そして、本件出願の当初明細書等の段落【００６８】ないし【００７８】には、「端末Ａ、端末Ｂおよび管理サーバ３００が行う処理」として、「ユーザＡ（買い手）がユーザＢ（店舗などの売り手）から商品を購入し、その代金の支払いを電子マネーによって行う場合の処理」（【００６８】）が記載されており、当該処理は、「ユーザＡ（買い手）」から「ユーザＢ（店舗などの売り手）」への「電子マネーの送金」（【００６９】）を行う「電子マネー送金方法」（構成要件４Ａ）に係る処理であることは明らかである。

したがって、構成要件４Ａは、本件出願の当初明細書等に記載された事項であると認められる。

イ　構成要件４Ｂ

構成要件４Ｂは、管理サーバ及び第１ユーザ端末に第１の証明情報が格納され、管理サーバ及び第２ユーザ端末に第２の証明情報が格納されていることを特定したものである。

本件出願の当初明細書等の段落【００５７】ないし【００６０】には、「端末Ａが管理サーバ３００上における電子マネーの送受金に必要な電子証明書を入手する場合の処理」について記載されており、特に段落【００５９】には、管理サーバ３００の電子証明書発行処理部３８３により、ユーザＡ用に「第１の電子証明書」を作成すると、「その第１の電子証明書を端末Ａと紐付けて」、(管理サーバ３００の)「顧客マスタ格納部３５０に格納する」ことが、段落【００６０】には、管理サーバ３００の電子証明書発行処理部３８３が「第１の電子証明書を端末Ａに送信し」、「端末Ａは受信した第１の電子証明書を端末Ａの証明書格納部１７１に格納する」ことが記載されている。

そうすると、本件出願の当初明細書等の「第１の電子証明書」は、構成要件４Ｂの「第１の証明情報」に対応し、当該「第１の証明情報」は「電子マネー管理サーバ(３００)」(構成要件４Ｂ)と「第１ユーザの端末(Ａ)」(構成要件４Ｂ)に格納されるものである。

また、本件出願の当初明細書等の段落【００６１】には、端末Ｂが管理サーバ３００上における電子マネーの送受金に必要な電子証明書を入手する場合についても、端末Ａが電子証明書を入手する場合と同等の処理が行われることが記載され、特に図８には、ステップＳ５５として、「電子マネー管理サーバ」において「第２の電子証明書とその秘密鍵を作成し、顧客マスタ格納部に格納(Ｓ５５)」することが、ステップＳ５７として、「端末Ｂ(売り手)」において「第２の電子証明書を格納(Ｓ５７)」することが、それぞれ記載されている。

そうすると、本件出願の当初明細書等の「第２の電子証明書」は、構成要件４Ｂの「第２の証明情報」に対応し、当該「第２の証明情報」は「電子マネー管理サーバ（３００）」（構成要件４Ｂ）と「第２ユーザの端末（Ｂ）」（構成要件４Ｂ）に格納されるものである。

したがって、構成要件４Ｂは、本件出願の当初明細書等に記載された事項であると認められる。

ウ　構成要件４Ｃ－１

前記アのとおり、本件出願の当初明細書等の段落【００６８】ないし【００７８】に記載された、「ユーザＡ（買い手）がユーザＢ（店舗などの売り手）から商品を購入し、その代金の支払いを電子マネーによって行う場合の処理」は「電子マネー送金方法」に係る処理であって、ステップＳ１０１～Ｓ１２３で示される一連の処理が、ユーザＡが自身の端末Ａを使って支払用画面を表示させ、端末Ａを端末Ｂのリーダライタ２５０に近付けてＰａｙボタンに指で触れることを契機として行われる（【００６９】）。

そして、その一連の処理に関して、本件出願の当初明細書等の段落【００７０】には、ステップＳ１０３で「端末Ｂは、電子証明書交換処理部２８１により、端末Ａから送信される第１の電子証明書のデジタル署名を受信」し、ステップＳ１０４で「端末Ｂは受信したデジタル署名を証明書格納部や端末Ｂのメモリのその他の部分に格納する」ことが、段落【００７１】ないし【００７２】には、ステップＳ１０６で「端末Ｂでは、自己の有する第２の電子証明書のデジタル署名を前記受信した第１の電子証明書のデジタル署名によって置換することにより、デジタル署名を置換した第２の電子証明書を作成し」、ステップＳ１０８で「端末Ｂは、デジタル証明書情報送信処理部２８３により、デジタル署名を置換した第２の電子証明書を管理サーバ３００に送信する」ことが、それぞれ記載されている。ここで、端末Ｂは、自己の有する「第２の電子証明書のデジタル署名」を、

端末Ａから受信した「第１の電子証明書のデジタル署名」に置換して、「デジタル署名を置換した第２の電子証明書」を管理サーバ３００に送信するのであるから、「第１の電子証明書のデジタル署名」は、構成要件４Ｃ－１の「前記第１の証明情報の少なくとも一部」に対応するものであって、「前記第１ユーザ端末（Ａ）から」「前記第２ユーザ端末（Ｂ）を介して」「前記電子マネー管理サーバに送信される」（構成要件４Ｃ－１）ものである。

したがって、構成要件４Ｃ－１は、本件出願の当初明細書等に記載された事項であると認められる。

エ　構成要件４Ｃ－２、４Ｃ－２－１

本件出願の当初明細書等の段落【００７３】には、構成要件４Ｃ－１に対応する処理として上記ウで示したステップＳ１０８に続き、「管理サーバ３００」の処理として、まずステップＳ１０９で「端末Ａおよび端末Ｂからデジタル署名を置換した第１および第２の電子証明書を受信」した後、ステップＳ１１０で「デジタル署名を置換した第２の電子証明書およびそれに含まれる第１の電子証明書のデジタル署名を、顧客マスタ格納部３５０に格納されている対応している秘密鍵によって復号化する」ことが記載されている。

続いて、本件出願の当初明細書等の段落【００７４】には、「管理サーバ３００」の処理として、ステップＳ１１１で「（１）復号化された第１の電子証明書のデジタル署名と顧客マスタ格納部３５０に格納されている第１の電子証明書のデジタル署名とが対応しているか否か」を判断し、ステップＳ１１２で「（４）第１の電子証明書のデジタル署名の送信元が端末Ｂ（第２の電子証明書に対応してる端末）であるか否かを判断する」ことが記載されており、ステップＳ１１２における（４）の判断が、構成要件４Ｃ－２－１の「前記第１の証明情報の少なくとも一部を受け取った第２のユーザ端末（Ｂ）が前記電子マネー管理サーバ（３００）に格納されてい

る前記第２の証明情報と対応しているか否かの判断」に、ステップＳ１１１における（１）の判断が、構成要件４Ｃ－２－１の「前記第１のユーザ端末（Ａ）が前記電子マネー管理サーバ（３００）に格納されている前記第１の証明情報と対応しているか否かの判断」に、それぞれ対応する。

そして、本件出願の当初明細書等の段落【００９９】には、「ステップＳ１１１およびステップＳ１１２で取引を行う端末を確実に認証することができる」との記載があることから、ステップＳ１１１における（１）の判断、及びステップＳ１１２における（４）の判断は、構成要件４Ｃ－２－１の「前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）の認証を行う認証工程」に対応する。

したがって、構成要件４Ｃ－２、４Ｃ－２－１は、本件出願の当初明細書等に記載された事項であると認められる。

オ　構成要件４Ｃ－２－２

本件出願の当初明細書等の段落【００７５】及び図１３には、ステップＳ１１１～Ｓ１１２における（１）～（４）の判断が全て対応していると判断されると、すなわち、上記エで示したステップＳ１１１～Ｓ１１２に続き、ステップＳ１１４でその判断結果が端末Ｂに送信され、ステップＳ１１７で端末Ｂから「管理サーバ３００に対してアクセスキーの要求が送信される」と、「管理サーバ３００」はステップＳ１１８で「第２のアクセスキーを端末Ｂに送信」することが記載されている。

そして、本件出願の当初明細書等の段落【００７６】には、ステップＳ１２０で、「端末Ｂ」が「第２のアクセスキーと、端末Ａの所有者であるユーザＡからの受取額である３００円と、受取指示とを管理サーバ３００に送信し」、「管理サーバ」が「それらを受信する」ことが記載されており、「管理サーバ」が「端末Ｂ」から「端末Ａの所有者であるユーザＡからの受取額である３００円」と「受取指示」を受信する処理が、構成要件４Ｃ

－２－２の「前記第２ユーザから、前記第１ユーザからの電子マネーの受取指示と、受取額とを受信する第３受信工程」に対応する。

したがって、構成要件４Ｃ－２－２は、本件出願の当初明細書等に記載された事項であると認められる。

カ　構成要件４Ｃ－２－３

本件出願の当初明細書等の段落【００７７】には、構成要件４Ｃ－２－２に対応する処理として上記オで示したステップＳ１２０に続き、「管理サーバ３００」が、ステップＳ１２２で「前記受取額が管理サーバ３００の口座データ格納部３６０に格納されているユーザＡの口座残高内であるか否か」を判断することが記載されており、当該ステップＳ１２２の処理が、構成要件４Ｃ－２－３の「前記第２ユーザから受信した前記受取額が前記電子マネー管理サーバ（３００）に記憶されている前記第１ユーザの電子マネーの残額内であるか否かの判断を少なくとも行う決済判断工程」に対応する。

したがって、構成要件４Ｃ－２－３は、本件出願の当初明細書等に記載された事項であると認められる。

キ　構成要件４Ｃ－２－４、構成要件４Ｄ

本件出願の当初明細書等の段落【００７８】には、「前記ステップＳ１２２で残高内であると判断されると」、すなわち、上記カで示したステップＳ１２２に続き、「管理サーバ３００」がステップＳ１２３で「口座データ格納部３６０に格納されているユーザＡの口座ａの口座データの残額を前記受取額の分だけ減額すると共に、口座データ格納部３６０に格納されているユーザＢの口座（以下、口座ｂと称する）の口座データの残額を前記受取額の分だけ増額する」ことが記載されており、当該ステップＳ１２３の処理が、構成要件４Ｃ－２－４の「前記決済判断工程において前記残額内であると判断されると、前記電子マネー管理サーバ（３００）内の前記

第１ユーザの電子マネーの残額を前記受取額の分だけ減額すると共に、前記電子マネー管理サーバ（３００）内の前記第２ユーザの電子マネーの残額を前記受取額の分だけ増額する決済工程」に対応する。

そして、上記ウないしカ及び上記のとおり、構成要件４Ｃ－１、４Ｃ－２、４Ｃ－２－１、４Ｃ－２－２、４Ｃ－２－３、４Ｃ－２－４を充足する方法により、本件出願の当初明細書等の段落【００７０】ないし【００７８】に示されたステップＳ１０１ないしＳ１２３により、「ユーザＡからユーザＢへの電子マネーの送金が行われる」（段落【００６９】）から、本件出願の当初明細書等には、上記の各構成要件に該当する「ことを特徴とする電子マネー送金方法」（構成要件４Ｄ）が記載されている。

したがって、構成要件４Ｃ－２－４、４Ｄは、本件出願の当初明細書等に記載された事項であると認められる。

⑶　請求項４の構成要件４Ｃにつき、証明情報の送信が受金側である第２ユーザ端末のみから行われる構成であることについて

ア　第１実施形態

本件出願の当初明細書等に記載された第１実施形態（段落【００４４】～【０１００】、前記１⑷）は、ユーザＢ（第２ユーザ）の有する端末Ｂが第２の電子証明書中のデジタル署名を端末Ａに送信し、端末Ａがこのデジタル署名を格納し、ユーザＡ（第１ユーザ）の有する端末Ａが第１の電子証明書中のデジタル署名を端末Ｂに送信し、端末Ｂがこのデジタル署名を格納する（ステップＳ１０１～１０４、段落【００７０】）。端末Ａは、自己の有する第１の電子証明書のデジタル署名を受信した第２の電子証明書のデジタル署名によって置換することにより、デジタル署名を置換した第１の電子証明書を作成し、これを管理サーバ３００に送信し、端末Ｂは、自己の有する第２の電子証明書のデジタル署名を受信した第１の電子証明書のデジタル署名によって置換することにより、デジタル署名を置換し

た第２の電子証明書を作成し、これを管理サーバ３００に送信する（ステップＳ１０５～１０８、段落【００７１】、【００７２】）。管理サーバ３００は、受信した電子証明書及びこれに含まれるデジタル署名を秘密鍵によって復号化し、復号化された第１の電子証明書のデジタル署名と格納されている第１の電子証明書のデジタル署名とが対応しているか否か、及び、復号化された第２の電子証明書のデジタル署名と格納されている第２の電子証明書のデジタル署名とが対応しているか否かを確認する（ステップＳ１１１、段落【００７４】）。また、管理サーバ３００は、第２の電子証明書のデジタル署名の送信元が端末Ａであるか否か、及び第１の電子証明書のデジタル署名の送信元が端末Ｂであるか否かを確認する（ステップＳ１１２、段落【００７４】）。

本件出願の当初明細書等は、上記各ステップにより、自己の端末の電子証明書の情報が他の端末から管理サーバ３００に送られ、当該他の端末の電子証明書の情報が自己の端末から管理サーバ３００に送られるため、取引を行おうとしている二つの端末が特定され、それぞれ送信された電子証明書の照合が管理サーバ３００によって行われ、これによって管理サーバ３００は、電子マネーの送受金を行おうとしている端末Ａ、Ｂを確実に認証することができるとしている（段落【００８０】）。

そして、上記各ステップは、第２実施形態ないし第４実施形態でも同様の処理が行われることとされている（段落【０１０３】、【０１１０】、【０１２２】）。

イ　請求項４（本件発明４）の構成要件４Ｃ

これに対し、本件特許の特許請求の範囲の請求項４（本件発明４）の構成要件４Ｃは、第２ユーザ端末が、第１ユーザ端末から第１の証明情報の少なくとも一部を受け取り、第２ユーザ端末を介して第１の証明情報の少なくとも一部が電子マネー管理サーバに送信されるようになっており（構

成要件４Ｃ－１）、電子マネー管理サーバが、第１の証明情報の少なくとも一部を受け取った第２のユーザ端末が電子マネー管理サーバに格納されている第２の証明情報と対応しているか否かの判断と、第１のユーザ端末が電子マネー管理サーバに格納されている第１の証明情報と対応しているか否かの判断を少なくとも行うことにより、第１ユーザ端末と第２ユーザ端末の認証を行うこととされている（構成要件４Ｃ－２－１）。

このように、請求項４の構成要件４Ｃでは、電子マネー管理サーバに対する証明情報の送信が、受金側である第２ユーザ端末のみから行われる構成となっており、この構成は前記アの第１実施形態とは異なる。

ウ　本件出願の当初明細書等の記載

しかし、本件出願の当初明細書等において、発明が解決しようとする課題は、ＩＣチップを利用する電子マネー決済について、①ＩＣチップが埋め込まれたＩＣカードや携帯端末等の媒体が紛失等した場合、ＩＣカードや携帯端末自体を回収しない限り、そこに格納されている電子マネーを回収することはできないという課題（段落【００１０】）と、②ＩＣチップを利用する決済の場合、一見電子マネーによる支払がされているように見えるが、実は裏で現金のやりとりがされており、電子マネーが完全に現金の代用として使われているものではないという課題（段落【００１１】、【００１２】）であるとされ、発明はこれらの課題を解決するためになされたもので、電子マネーを現金に極めて近い感覚で取り扱うことを可能とし、しかも電子マネーを操作するための端末の紛失時や盗難時においても電子マネーを失わずに済む電子マネー送金方法及びそのシステムを提供することを目的とするものである（段落【００１３】）。

そして、本件出願の当初明細書等では、【課題を解決するための手段】（段落【００１４】～【００３９】）において、前記第１実施形態ないし第４実施形態とは異なる複数の構成を記載しているところ、第１ユーザ端末が、

第２ユーザ端末から第２の証明情報の少なくとも一部の情報である第２端末情報を受信し、電子マネー管理サーバは、第１ユーザ端末から第１ユーザ端末の証明情報の少なくとも一部の情報である第１端末情報と、第２端末情報を受信し、第１端末情報が電子マネー管理サーバに格納されている第１の証明情報と対応しているか否かの判断と、第２端末情報が電子マネー管理サーバに格納されている第２の証明情報と対応しているか否かの判断とを少なくとも行うことにより、第１ユーザ端末及び第２ユーザ端末の認証を行う認証工程を実施する構成が記載されている（段落【００３５】）。この構成において、第２ユーザ端末の証明情報が第１ユーザ端末から電子マネー管理サーバに送られるので、この時点で取引を行おうとしている二つの端末が特定され、さらに、第１ユーザ端末から送信される取引両者の証明情報の照合が電子マネー管理サーバによって行われ、これにより、電子マネー管理サーバは電子マネーの送受金を行おうとしている端末を確実に認証することができると記載されている（段落【００３６】）。

また、段落【０１４３】以下に記載された構成（原告の主張にいう「変形例」）も、電子マネー管理サーバに電子証明書を送信するのは端末Ａのみであり、電子マネー管理サーバは端末Ａのみから受信された第１の電子証明書及び第２の電子証明書のデジタル署名が、格納されている情報と対応しているか否かを判断するが（段落【０１４７】）、端末Ｂのデジタル署名が端末Ａから電子マネー管理サーバに送られるので、この時点で取引を行おうとしている二つの端末が特定され、端末Ａから送信される取引両者の証明情報の照合が電子マネー管理サーバによって行われるので、電子マネーの送受金を行おうとしている端末を確実に認証することができると記載されている（段落【０１５０】）。

電子マネー管理サーバに対する情報伝達が送金側から行われないとしても、本件各発明の目的は達成されるし、取引を行おうとしている二つの

端末の確実な認証を行うことができる。

以上によれば、本件出願の当初明細書等には、電子マネーの送受金を行おうとしている二つの端末のうちの一方のみから、電子マネー管理サーバに対して証明情報の一部の情報である端末情報を送信し、電子マネー管理サーバが、二つの端末のうちの一方のみから受信した情報と、電子マネー管理サーバに格納されている証明情報とを照合することによって端末の認証を行う構成が記載されており、当業者は、本件出願の当初明細書等の記載から、このような情報の送信及び認証の方法によっても、電子マネーの送受金を行おうとしている端末を確実に認証することができるとの技術的事項を導くことができると認められる。送金側から電子マネー管理サーバに対する情報伝達が行われる場合は、もちろんこれに含まれるが、本件各発明の目的や当初明細書等の記載に照らして、送金側ではなく受金側のみから電子マネー管理サーバに対する情報伝達が行われる場合についても、電子マネーの送受金を行おうとしている二つの端末の認証を確実に行うことができるから（すなわち、取引を行おうとしている二つの端末の確実な認証において、送金側からの情報伝達が必要不可欠ではない。）、そのような場合も、本件出願の当初明細書等の全ての記載を総合することにより導かれる技術的事項に含まれているものと認められ、そのような場合に係る請求項４（本件発明４）の構成要件４Ｃを本件補正により追加しても、新たな技術的事項を導入するものではないと認められる。

そうすると、請求項４の構成要件４Ｃの内容は、本件出願の当初明細書等から導かれる技術的事項との関係において、新たな技術的事項を導入するものではないと認められる。

エ　新規事項追加の有無

上記イ及びウによれば、本件補正のうち請求項４を加えた部分は、本件出願の当初明細書等に記載された事項の範囲内においてしたものであり、

同当初明細書等から導かれる技術的事項との関係において、新たな技術的事項を導入するものではないから、新規事項に当たらないと認められる。

⑷　請求項５について

本件補正において追加された請求項５は、請求項４の「電子マネー送金方法」の発明を「電子マネー送金システム」の発明として表現したものであるから、請求項４と同様、本件補正のうち請求項５を加えた部分は、本件出願の当初明細書等に記載された事項の範囲内においてしたものであり、同当初明細書等から導かれる技術的事項との関係において、新たな技術的事項を導入するものではないから、新規事項に当たらないと認められる。

⑸　原告の主張（前記第３の３〔原告の主張〕）に対する判断

ア　〔原告の主張〕⑵（本件発明４及び５が本件出願の当初明細書等の第１実施形態に記載されたものでないこと）について

(ｱ)　〔原告の主張〕⑵イ（本件出願の当初明細書等の段落【００１８】に関する認定の誤り）について

a　原告は、本件審決が、本件発明４のうち、構成要件４Ｃ－１の「前記送金の際、前記第２ユーザ端末（Ｂ）が、前記第１ユーザ端末（Ａ）から前記第１の証明情報の少なくとも一部を受け取り、前記第２ユーザ端末（Ｂ）を介して前記第１の証明情報の少なくとも一部が前記電子マネー管理サーバに送信される」との構成は、本件出願の当初明細書等の段落【００１８】の記載における「自己の端末の電子証明書の情報が他の端末から電子マネー管理サーバに送られ」、又は「当該他の端末の電子証明書の情報が自己の端末から電子マネー管理サーバに送られる」という事項に相当するものであって、段落【００１８】の記載によれば、「この時点で取引を行おうとしている２つの端末が特定され」るものであると認定した（本件審決１２４頁末行～１２５頁９行）ことに対して、段落【００１８】には、「自己の端末の電子証明書の情

報が他の端末から電子マネー管理サーバに送られ」と、「当該他の端末の電子証明書の情報が自己の端末から電子マネー管理サーバに送られる」との間に「又は」という用語は存在せず、前後の文脈を考慮すれば、これらの文章は「かつ」で接続されるものと認められるのであって、本件審決の上記認定は誤りであると主張する。

しかし、本件発明４の構成要件４Ｃ－１は、その文言（前記第２の２⑶）からすれば、第２ユーザ端末が、第１ユーザ端末から、第１の証明情報の少なくとも一部を受け取り、第２ユーザ端末を介して上記証明情報が電子マネー管理サーバに送られるとの内容であると認められ、第１ユーザ端末が第２ユーザ端末から証明情報を受け取ること及び当該証明情報が第１ユーザ端末から電子マネー管理サーバに送られることは構成要件４Ｃ－１には開示されていないものというべきである。このように、構成要件４Ｃ－１の構成は、一方のユーザ端末のみが他方のユーザ端末から証明情報を取得して、この証明情報が電子マネー管理サーバに送られるとの内容であるから、構成要件４Ｃ－１は、段落【００１８】の記載における「自己の端末の電子証明書の情報が他の端末から電子マネー管理サーバに送られ、」という事項、又は「当該他の端末の電子証明書の情報が自己の端末から電子マネー管理サーバに送られる」という事項のいずれかに該当すると認められ、これらの双方の事項に同時に該当することはないというべきである。したがって、構成要件４Ｃ－１が段落【００１８】の記載における「自己の端末の電子証明書の情報が他の端末から電子マネー管理サーバに送られ」、又は「当該他の端末の電子証明書の情報が自己の端末から電子マネー管理サーバに送られる」という事項に相当するとの本件審決の認定が誤りであるとは認められない。

ｂ　また、原告は、本件審決が、「本件特許発明４の『前記第１の証明情

報の少なくとも一部を受け取った第２のユーザ端末（Ｂ）が前記電子マネー管理サーバ（３００）に格納されている前記第２の証明情報と対応しているか否かの判断と、前記第１のユーザ端末（Ａ）が前記電子マネー管理サーバ（３００）に格納されている前記第１の証明情報と対応しているか否かの判断を少なくとも行うことにより、前記第１ユーザ端末（Ａ）および前記第２ユーザ端末（Ｂ）の認証を行う認証工程』（４Ｃ－２、４Ｃ－２－２）という構成は、当初明細書等の段落【００１８】の記載における、『さらに、それぞれ送信された電子証明書の照合が電子マネー管理サーバによって行われる。』という事項に相当するものであって、『これにより、電子マネー管理サーバは、電子マネーの送受金を行おうとしている端末を確実に認証することができる。』という効果を奏するものである。」（本件審決第９の３⑴ケ、１２５頁）と述べたことについて、本件審決が言及する本件出願の当初明細書等の段落【００１８】の記載は、第１ユーザ端末と第２ユーザ端末が、電子証明書の少なくとも一部を相互に交換した上で、両端末が、それぞれ他の端末の電子証明書の情報を送信することを前提とした記載であり、本件発明４の構成要件４Ｃ－１、４Ｃ－２及び４Ｃ－２－２に係る構成、すなわち受金側からの電子証明書の情報の送信のみで送金を行う形態は段落【００１８】に記載されておらず、本件審決の上記認定は誤りであると主張する。

しかし、本件審決の上記説示は、段落【００１８】の「それぞれ送信された電子証明書の照合が電子マネー管理サーバによって行われる。これにより、電子マネー管理サーバは、電子マネーの送受金を行おうとしている端末を確実に認証することができる。」という文言どおり、送信された電子証明書を照合し、電子マネーの送受金を行おうとしている端末を認証するという効果を示しているにとどまると認められ、

上記の文言から、その前提として、第１ユーザ端末と第２ユーザ端末が、電子証明書の少なくとも一部を相互に交換した上で、両端末が、それぞれ他の端末の電子証明書の情報を送信することによる効果までを述べているとは解されないし、本件審決は、受金側からの電子証明書の情報の送信のみで送金を行う形態が当初明細書等の段落【００１８】に記載されていると認定しているものでもない。したがって、原告の上記主張は、採用することができない。

(ｲ) 〔原告の主張〕⑵ウ（本件出願の当初明細書等の段落【００７４】に関する認定の誤り）について

原告は、本件審決が、「『さらに、ステップＳ１１１を省く場合でも、ユーザＡからユーザＢへの電子マネーの送金を行うことは可能である。これは、ステップＳ１１２だけでも取引を行う端末を確定することができるからである。』（【０１００】）と記載されており、上記の段落【００１８】の記載も併せて考慮すると、本件特許発明４に係る『認証工程』は、『取引を行おうとしている２つの端末が特定』でき、これら２つの端末について『確実に認証すること』ができれば十分であって、必ずしも段落【００７４】に記載された『ステップＳ１１１およびＳ１１２』における上記（１）～（４）の全てについて判断する必要はないものであるといえる。」（本件審決第９の３⑴ケ、１２６頁）と述べたことについて、本件出願の当初明細書等の段落【０１００】は、段落【００７４】に記載された送金側からの伝達プロセスを省略することができる根拠とならない旨主張する。

しかし、本件審決は、本件出願の当初明細書等の段落【０１００】において、「ステップＳ１１２だけでも『取引を行う端末を確定することができる』ため、ステップＳ１１１を省略することができる」旨記載されていることをもって、同当初明細書等において、取引を行おうとしてい

る二つの端末が特定でき、かつ、これら二つの端末について確実に認証することができればよいと解されることの根拠の一つとしていると認められる。そして、取引を行おうとしている二つの端末の確実な認証において、送金側からの情報伝達が必要不可欠ではないことは、前記⑶ウのとおりである。そうすると、本件審決が、段落【００１００】を根拠の一つとして、段落【００７４】に記載されたように、情報伝達のプロセスを省略することができると判断したことが誤りであるとは解されない。

したがって、原告の上記主張は採用することができない。

(ｳ) 〔原告の主張〕⑵エ（本件発明４及び５は取引を行う端末の特定及び確実な認証という効果を奏するものでないこと）について

ａ　原告は、〔原告の主張〕⑵エ(ｱ)のとおり、受金側の伝達プロセスのみでは、送金側の端末に関する情報は、第１の電子証明書のデジタル署名しか存在せず、管理サーバは、送金側の端末に対応する秘密鍵を特定することができないから、受金側からの電子証明書の情報の伝達プロセスのみである本件発明４及び５に係る構成では、取引を行おうとする送金側の端末を特定することができず、かかる態様についてまで、本件出願の当初明細書等の記載から導き出される技術的事項から奏する効果を有するということはできないと主張する。

しかし、本件出願の当初明細書等の段落【０１４２】以下に記載された実施形態は、送金側である端末Ａのみから管理サーバに情報を送信しており、端末Ａから端末Ｂに第１の電子証明書のデジタル署名を送信しない構成であるが、管理サーバは、端末Ａから受信した端末Ａの電子証明書と端末Ｂのデジタル署名が管理サーバに格納されている端末Ａ及び端末Ｂの電子証明書の情報と対応しているか否かを判断し、これにより二つの端末を特定するとされている（段落【０１５０】）。このように、本件出願の当初明細書等において、送金側からのみ管理

サーバに情報を送信する態様でも、管理サーバは格納されている二つの端末の電子証明書の情報と対比することによって、二つの端末を特定できるとされている。そして、同当初明細書等の他の段落の記載からしても、管理サーバは、デジタル署名以外の部分から取引を行う端末を特定することが可能であると解される。

このことからすれば、受金側からの情報送信のみによっても、送金側の端末を特定することはでき、本件発明４及び５が受金側からの情報送信のみによる構成であることをもって、送金側の端末を特定することができないとはいえない。

したがって、原告の上記主張は採用することができない。

b　原告は、〔原告の主張〕⑵エ(ｲ)のとおり、本件出願の当初明細書等の段落【００８０】、【００８１】の記載等によれば、本件各発明の効果である「２つの端末について確実に認証する」とは、正当な送金者と受金者とを認証するという意味であり、電子マネーが不正に入手可能となる端末の認証は「確実な認証」には当たらないと主張する。

しかし、原告が指摘する段落【００８０】、【００８１】を含め、本件出願の当初明細書等において、「確実な認証」とは、取引を行おうとしている二つの端末が特定され、送信された電子証明書の照合が管理サーバによって行われることを意味している。そして、上記ａのとおり、二つの端末のうち一方からのみ管理サーバに情報が送信される場合でも、管理サーバは二つの端末を特定することができる。また、一方の端末からのみ情報が送信された場合でも、管理サーバは、格納している二つの端末の証明情報と照合を行うことができる。これらにより、二つの端末について確実な認証が行われるものと認められる。

原告が指摘する段落【００８１】は、第１実施形態の構成であれば、受金側の端末Ｂが送金側の端末Ａの電子証明書情報を不正に入手して

何らかの手段でユーザＡの有する電子マネーを入手しようとしても、端末Ａから管理サーバに自らの電子証明書の情報の送信が行われない限り、ユーザＡからユーザＢへの電子マネーの送金が行われないと記載しているが、送金側の端末Ａから管理サーバに情報の送信がされて初めて「確実な認証」が可能となるとは記載していない。

そして、本件各発明が解決しようとする課題は前記⑶ウのとおりであり、受金側の行為によって不正な送金が行われることは課題に挙げられていない。

以上によれば、送金側からの情報の送信がされる実施形態であれば、この情報送信によって受金側の行為に基づく不正な送金の危険性が低下するとしても、当初明細書等の記載内容からすれば、送金側からの情報送信がなければ「確実な認証」ができないと解することはできない。

したがって、原告の上記主張は採用することができない。

(ｴ) 〔原告の主張〕⑵オ（第１の実施形態は、送金側又は受金側の片方からのみの伝達プロセスをサポートしないこと）について

原告は、〔原告の主張〕⑵オのとおり、本件特許の対応ファミリーの米国特許の審査経緯において、受金側及び送金側の双方からの伝達プロセスが必要であり、片側の伝達プロセスのみでは発明が成立しない点が指摘され、被告もこの点を認めているとして、本件審決の認定は誤りであると主張する。

しかし、記載要件に関する特許法上の要件や審査の基準は国ごとに異なるから、本件出願に対応する他国の出願の審査経緯や他国の手続における被告の主張によって、我が国の特許庁による本件審決の認定が誤りであると解すべきことにはならない。

したがって、原告の上記主張は採用することができない。

イ　〔原告の主張〕⑶（本件出願の当初明細書等の段落【０１４２】以下の実施例（原告の主張にいう「変形例」）の記載について）について

原告は、本件出願の当初明細書等の段落【０１４２】以下の実施例（原告の主張にいう「変形例」）の記載は、送金側から取引両者の証明情報を受け付けるため、受金側のみの行為による不正送金を防止することが可能となるのに対し、本件発明４及び５では、管理サーバが受金側から取引両者の証明情報を受信するため、受金側のみの行為による不正送金を防止することができないとして、段落【０１４２】以下の実施例の記載は、本件発明４及び５とは、受金側のみの行為による不正送金を防止することが可能である点で異なるから、本件発明４及び５が新規事項の追加に該当しないことの根拠とならないと主張する。

しかし、前記ア(ｳ)ｂのとおり、二つの端末のうちの一方からのみ管理サーバに情報が送信される場合でも、管理サーバは二つの端末を特定することができるし、また、一方の端末からのみ情報が送信された場合でも、管理サーバは、格納している二つの端末の証明情報と照合を行うことができることが、本件出願の当初明細書等に記載されている。前記⑶ウのとおり、同当初明細書等には、本件各発明の課題を踏まえた目的として、電子マネーを現金に極めて近い感覚で取り扱うことを可能とし、しかも電子マネーを操作するための端末の紛失時や盗難時においても電子マネーを失わずに済む電子マネー送金方法及びそのシステムを提供することが示されているところ、電子マネーの送受金を行おうとしている二つの端末のうちの一方のみから受信した情報と、電子マネー管理サーバに格納されている証明情報とを照合することによって、このような本件各発明の目的は達成されるものである。原告が主張するような、管理サーバが送金側から取引当事者双方の証明情報の送信を受けることにより、受金側のみの行為による不正送金を防ぐことができるという効果は、実施例により奏される効果と

いう余地があるとしても、このような方法による不正送金の防止が本件各発明の課題やそれを踏まえた目的である旨の記載は、本件出願の当初明細書等にはないし、そのような方法により不正送金を防止する発明のみが本件出願の当初明細書等に記載されていると解する根拠もない。そうすると、本件出願の当初明細書等の記載に基づくならば、電子マネー管理サーバに対して二つの端末のうちの一方のみから証明情報の一部の情報である端末情報を送信することを内容とする請求項４及び５（本件発明４及び５）の追加は、本件出願の当初明細書等から導かれる技術的事項との関係において、新たな技術的事項を導入するものとは認められない。

したがって、原告の上記主張は採用することができない。

⑹　取消事由３に関する結論

以上によれば、請求項４及び５を追加した本件補正は、本件出願の当初明細書等に記載された事項の範囲内においてしたものであると認められるから、無効理由５（本件補正による新規事項追加）に関する本件審決の判断に誤りはなく、取消事由３は理由がない。

５　取消事由４（無効理由３（分割要件違反による新規性又は進歩性の欠如）に関する判断の誤り）について

原告は、取消事由４として、無効理由３（分割要件違反による新規性又は進歩性の欠如）について、本件補正により追加された請求項４及び５は、本件出願の当初明細書等に記載された事項の範囲内にないため、当初明細書等と記載が同一である第１世代出願の当初明細書及び図面に記載された事項の範囲内にあるともいえないから、本件出願は、第１世代出願及び最初の原出願に対して分割要件を満たさず、本件各発明の新規性及び進歩性の判断の基準日は、現実の出願日である平成２９年１月１９日であり、平成２８年４月１４日に公開された第１世代出願の公開特許公報（甲１３）に基づき、新規性又は進歩性を欠くと主張し、これと異なる本件審決の判断は誤りであると主張する。

しかし、上記４のとおり、本件補正のうち請求項４及び５を追加した部分は、本件出願の当初明細書等に記載された事項の範囲内においてしたものであると認められる。そして、本件出願の当初明細書等の記載は、第１世代出願の当初明細書及び図面の記載、並びに最初の原出願の当初明細書及び図面の記載と同一である（甲１５、１８、弁論の全趣旨（本件審決は、第１０の１において、本件特許出願の当初明細書等（甲１８）の記載は、第１世代出願の当初明細書等（甲１５）の記載、及び最初の原出願の当初明細書等の記載とも同一である出願の当初明細書等の記載と同一であると認定し、当事者らはこれを争っていない。））から、本件出願は、第１世代出願及び最初の原出願に対しても分割要件を満たすものである。本件出願は、第１世代出願及び最初の原出願に対しても分割要件を満たすものであるから、本件出願の出願日は、最初の原出願の出願日（平成２４年１０月１１日）に遡及し、本件各発明は、同日を基準として新規性及び進歩性の判断をすべきものである。そうすると、本件各発明は、最初の原出願の出願日（平成２４年１０月１１日）より後の平成２８年４月１４日に公開された第１世代出願の公開特許公報（甲１３）に記載された発明により新規性及び進歩性を欠くものではない。したがって、これと同旨の本件審決の判断に誤りはなく、取消事由４は理由がない。

６　取消事由５（無効理由４（本件発明４及び５に係る特許のサポート要件違反）に関する判断の誤り）について

原告は、取消事由５として、無効理由４（本件発明４及び５に係る特許のサポート要件違反）について、本件補正により追加された請求項４及び５は、当初明細書等に記載された事項の範囲内にないから、本件発明４及び５に係る特許はサポート要件に違反すると主張し、これと異なる本件審決の判断は誤りであると主張する。

しかし、前記４と同様の理由により、本件発明４及び５は、本件出願の当初明細書等の記載と同一である本件明細書等の発明の詳細な説明に記載されたも

のであると認められるから、本件発明４及び５に係る特許はサポート要件に違反するものとは認められない。したがって、これと同旨の本件審決の判断に誤りはなく、取消事由５は理由がない。

７　結論

その他、原告が種々主張するところは、いずれも理由がない。

以上のとおりであり、原告が主張する取消事由はいずれも理由がなく、本件審決に、これを取り消すべき違法はないから、原告の請求は棄却されるべきである。

よって、主文のとおり判決する。

知的財産高等裁判所第３部

裁判長裁判官　　中　　平　　健

裁判官　　今　　井　　弘　　晃

裁判官　　水　　野　　正　　則

（別紙１　明細書、特許請求の範囲、図面及び要約書省略）

別紙２

甲１の記載（翻訳・抜粋）

１

「背景技術

日常の消費において、消費者は常に銀行カードを使用して商店の端末でカードをスキャンして買物をし、商店はユーザ情報を取得することができ、かつパスワードを入力する時に商店の端末で操作されるため、一般的に他人を回避することが困難であり、一定の安全上の問題が存在し、かつカードを携帯しなければ高額の買物を行うことができない。現在、携帯電話、PDA 及びパームトップコンピュータなどの様々なモバイル機器が普及し、特に携帯電話はほとんど携帯必需品であり、携帯電話又は他の移動端末を利用してモバイル決済を実現することができれば取引の安全性及び利便性を大幅に向上させることができる。

上記の状況から、業界は移動端末により取引支払を行うサービス、例えば中国移動のショートメッセージに基づく支払案を提供している。該サービスの利用時に利用者は特定の電話番号にショートメッセージを送信し、手動で店舗番号、商品番号、パスワードなどの情報を入力する必要がある。該方法はある程度、銀行端末の配置不足の問題を解決しているが、以下の欠点が存在する。

操作が複雑である。ユーザは特定の電話番号にショートメッセージを送信する必要があり、キーボードにより店舗番号、商品番号、パスワードなどの支払情報を入力する必要があり操作が非常に煩雑である。

信頼性が高くない。ユーザが手動で大量のデジタル情報を入力するため、エラーが発生しやすく、かつエラー検査メカニズムがないため、情報入力エラーにより支払が正常に行われることに影響しやすい。

上記問題に基づいて、ショートメッセージによる決済方法は実際の使用において普遍的ではない。

したがって、操作がしやすく、かつ安全で信頼性が高いモバイル決済システム及び

方法をどのように提供するかが、早急に解決すべき課題となる。」（５頁５～２１行）

２

「図１に示すように、モバイル決済システムの構造概略図であり、移動端末１とレジサービス端末２とネットワーク仲介システム３を含み、ネットワーク仲介システム３はそれぞれ移動端末１及びレジサービス端末２と通信接続され、レジサービス端末２は画像生成モジュールを含み、移動端末ユーザとの具体的な取引を行う場合、取引情報を画像に生成して移動端末１に提供することができる。移動端末１は撮像機能又は図形走査機能を備える携帯電話、PDA 又はパームトップコンピュータなどであってもよく、撮像機能又は図形走査機能を利用してレジサービス端末２により生成された取引情報の画像を取得してネットワーク仲介システム３に送信する。ネットワーク仲介システム３はそれぞれ移動端末ユーザ及びサービスプロバイダとサービス協議を締結した運営業者のみであってもよく、銀行が参加してもよく、ネットワーク仲介システム３においてモバイル決済を実現する装置は、取引情報の画像解析装置及び前記取引情報を処理するための処理装置を含み、処理装置には取引双方のアカウント情報が予め設定され、画像解析装置は画像から具体的な取引情報を解析して処理装置に送信し、処理装置は対応するアカウント情報に基づいて取引を行う。」（８頁１５行～９頁１行）

３

「具体的なモバイル決済取引の情報処理方法は以下のステップを含む。

Ｓ１：レジ端末はサービスプロバイダ関連情報及び取引内容情報等の取引情報を画像に生成して、後に取引の相手方である移動ユーザ端末に提供する。

移動端末ユーザとサービスプロバイダとが具体的な取引を行う場合、取引情報には一般的に２つの方面の内容が含まれている。

１．取引内容情報：取引シリアル番号、取引明細及び取引金額等の情報;

２．サービスプロバイダに関連する身分情報：サービスプロバイダ情報とレジ端末情報があり、そのうち、サービスプロバイダ情報はサービスプロバイダの ID 情

報、サービスタイプ、サービスアプリケーションID、バージョン等の情報を含むことができ、サービスプロバイダの ID 情報のみを含むこともできる。レジ端末情報は、レジ端末の一意の識別情報及びレジ端末の番号情報を含む。ここで、サービスアプリケーション ID は端末がどのようなアプリケーションを起動してユーザが取引を完了することを助けるかを指示することができる。一般的に、汎用的な端末アプリケーションを有してユーザの異なるサービスプロバイダに対する取引処理を満たすべきである。」（９頁２～１３行）

４

「Ｓ２：移動端末は、撮像機能又は図形走査機能によりレジサービス端末から前記画像を取得する；

Ｓ３:移動端末は、取得された画像情報をネットワーク仲介システムに送信する;

例えば、移動端末は、マルチメディアメッセージ（MMS）等の方式で該画像情報をネットワーク仲介システムに伝送することができる。取引の安全のために、移動端末は取得された画像情報を仲介システムに送信する前に、さらにユーザに送信するか否かを確認し、ユーザが送信することを確認した場合、移動端末は送信操作を実行する；ユーザが送信しないと選択すると、移動端末は送信操作を実行しない。該確認は、さらに事前に設定されたパスワードを入力することにより実現することができる。

Ｓ４：ネットワーク仲介システムは、画像情報を受信した後、画像解析装置において解析を行って、サービスプロバイダの関連情報及び取引内容情報の取引情報を取得する。」（９頁１７行～最下行）

５

「画像解析から得られたデータに全ての取引金融情報が含まれていない場合、ネットワーク仲介システムは、さらにレジサービス端末から必要な全ての取引金融情報を取得することができる。

又は、レジサービス端末はただレジサービス端末の情報、すなわち、サービスプ

ロバイダのＩＤ情報、レジサービス端末ＩＤ、レジサービス端末番号等と、取引シリアル番号情報のみを画像に保持しておく。移動端末は該画像情報を取得した後、該画像をネットワーク仲介システムに送信し、ネットワーク仲介システムは画像情報を解析し、かつ解析して得られたレジサービス端末の情報及び取引シリアル番号情報に基づいて仮取引記録を作成した場合、次にレジサービス端末から取引金額及び取引商品リスト等の取引内容情報を取得する。例えば、ネットワーク仲介システムは、レジサービス端末の情報及び取引シリアル番号情報に基づいて、対応するサービス端末から対応する取引金額と取引商品リスト等の情報を取得し、この場合、ネットワーク仲介システムは、対応するサービス端末に取引金額、商品明細を取得するように要求するリクエストを送信する必要があり、リクエストには少なくとも取引シリアル番号が含まれ､対応するサービス端末は該リクエストを受信した場合、対応する取引金額と商品明細をネットワーク仲介システムに送信する。」（１０頁１～１２行）

６

「Ｓ５：ネットワーク仲介システムは、移動端末ユーザの身分情報である買い手情報とレジサービス端末の身分情報である売り手情報を取得し、取引売買双方の身分の正当性を検証する。

移動端末ユーザの身分情報は、移動端末が取得された画像情報をネットワーク仲介システムに送信する場合、ネットワーク装置 MSC（Mobile Switching Center：モバイル交換センター）及び／又は HLR（Home Location Register：ホーム位置レジスタ）により関連身分記述情報を画像情報とともにネットワーク仲介システムに自動的に送信するものである。ここで、移動端末ユーザの身分情報は、移動端末の IMSI（International Mobile Subscriber Identity：国際移動ユーザ識別コード)、移動端末の ESN（Electronic serial number：電子シリアル番号であって、移動端末番号 MSISDN に唯一に対応する)、移動端末の番号などの情報のうちいずれか一つ又は任意の組み合わせを含むことができる。

レジサービス端末の身分情報はネットワーク仲介システムで解析された取引情報から直接抽出されるものである。

次に、双方の身分の正当性を検証し、正当であれば、ステップＳ６を実行し、そうでなければサービス拒否のメッセージを返す。ネットワーク仲介システムによるレジサービス端末の身分情報の検証は、レジサービス端末の ID と対応するサービスプロバイダが実際に存在するか否かを判断することを含む。例えば、ネットワーク仲介システムに該サービスプロバイダの情報と対応するアカウント情報とが予め登録されており、ネットワーク仲介システムはサービスプロバイダ ID 情報を解析した後、対応するサービスプロバイダ情報が登録されているか否かを検索し、存在すれば、解析されたサービスプロバイダが正当であると判定し、そうでなければ、不正であると判定する。ネットワーク仲介システムによるユーザ身分情報の検証は、該対応する移動端末ユーザの IMSI 情報と対応するアカウント情報とが予め登録されており、ネットワーク仲介システムは MSC 又は HLR から返信された IMSI 情報に基づいて該移動端末ユーザの IMSI とアカウント情報とが予め登録されているか否かを判定し、存在すれば、移動端末ユーザが正当であると判定し、そうでなければ、不正であると判定する。

Ｓ６：ネットワーク仲介システムは双方の身分情報に基づいて予め記憶されたデータベースから双方のアカウント情報を呼び出す。」（１０頁１３行～１１頁１０行）

７

「Ｓ７：ネットワーク仲介システムは取引情報に基づいて仮取引記録を作成して移動端末に取引を確認するために送信する。

ネットワーク仲介システムで作成された仮取引記録には、レジ端末情報と、移動端末ユーザの唯一の識別情報とアカウント情報などの移動端末ユーザ関連情報とが記録されており、前記レジサービス端末情報は、レジサービス端末の唯一の識別情報、サービスプロバイダ情報、レジ端末の番号、レジ端末の対応する又はサービスプロバイダの対応するアカウント情報を含むことができる。前記移動端末の唯一の

識別情報はIMSI、電子シリアル番号ESN及び移動端末の番号MSISDNのうちの一つを含むことができ、この三種の情報を同時に含むことが望ましい。例えば、移動端末番号によりHLR（Home Location Register：ホーム位置レジスタ）情報を特定することができ、トラブルが発生するとHLRにより関連運営業者等の責任エンティティを追跡することができる。例えばユーザのウェブジャンプが発生したり、又は携帯電話が紛失したなどの状況が発生する場合、古いIMSIにより移動端末のアカウントなどの情報要素を特定することができないが、この場合、移動端末の番号MSISDNにより移動端末のアカウント情報を特定し、取引記録を紹介することができる。

ネットワーク仲介システムが移動端末に送信した確認通知には取引金額、取引シリアル番号又は取引明細などの情報が含まれている。

Ｓ８：移動端末は取引通知を受信した後に確認を行う。正しいと確認した場合、取引を実行する命令を返信し、問題が見つかった場合、取引をキャンセルする命令を返信する。

移動端末が取引を確認する時に、ユーザの利益を保護するために、端末に予め設定されたパスワードを入力することにより確認することができる。」（１１頁１１行～１２頁２行）

８

「Ｓ９：ネットワーク仲介システムは移動端末の確認を受信した後、支払を実行する、すなわち仮取引記録を正式な取引記録として確認し、取引ログを記録する。

Ｓ１０：ネットワーク仲介システムは実行結果をレジサービス端末に送信し、さらに実行結果を移動端末に送信することができる。

ネットワーク仲介システムが取引を実行した結果は、少なくとも支払実行成功通知と取引実行失敗を含むべきである。

支払が成功した場合、取引双方は後続の取引手続きを履行するが、具体的には、レジサービス端末は支払実行成功通知を受信し、レジサービス端末は直接的に勘定

書を生成し印刷して移動端末ユーザに提供することができ、同時に、ネットワーク仲介システムは取引電子勘定書を記録し、かつ電子勘定書を、電子証明書とし、及び移動端末ユーザの将来の消費情報の統計用として移動端末に記憶させるように移動端末に伝送することができる。実際には、電子勘定書にはさらにレジサービス端末の署名情報も付けるべきである。

取引が失敗した場合、レジサービス端末は電子取引失敗通知を表示する。同時に、ネットワーク仲介システムは取引失敗を移動端末に通知する。

実際には、各取引記録は二つのフラグフィールドを含むことができ、取引双方の端末が取引成功通知を受信したか否かを示すために用いられる。ネットワーク仲介システムの取引が成功し、かつ取引成功通知を移動端末及びレジサービス端末に送信した場合、移動端末及びレジサービス端末は自己が当該取引成功通知を受信したことを知らせるメッセージをネットワーク仲介システムに返信すべきである。よって、ネットワーク仲介システムはユーザが電子商取引により取引を達成したので現金を払う必要がないと認識する。ネットワーク仲介システムは通知を受信すると、対応するフラグ情報を変更する。

当該方法を実現するために、ネットワーク仲介システム側には、レジサービス端末の唯一の識別 ID、レジサービス端末の番号、アカウント情報を含むことができるレジサービス端末に関する情報と、移動ユーザの身分情報及びアカウント情報とが予め記憶されているべきである。」（１２頁３～２５行）

９

「上記の方法と類似し、さらに画像解析モジュールを移動端末に設置することができ、移動端末は該画像を取得した後、画像解析モジュールにより該画像を直接解析し、解析して得られた情報をさらに処理した後にネットワーク仲介システムに送信し、ネットワーク仲介システムは移動端末から送信された取引売り手情報、取引内容、及び移動端末のユーザ情報に基づいて仮取引記録を生成し、後続の取引処理を実行する。このような方法により、移動端末は、画像情報を解析して取得されたサ

ービスタイプ情報とサービスアプリケーション ID とバージョン情報等の情報により、対応するサービスアプリケーションプログラムを起動し、かつ画像を解析して得られた情報を利用して該アプリケーションプログラムを初期化し、ユーザは該アプリケーションプログラムによりネットワーク仲介システムに対応する取引情報を送信するか否かを確認する。」（１３頁２３行～１４頁４行）

１０

「上記方法によると、売り手と買い手とが一回の取引を完了するには、ユーザが画像を一回走査して送信し、『確認』を一回押し、パスワードを一回入力することだけで済む。実際には、上記実施例において、上記の『『確認』の一回押し』というステップの操作も省略することができ、したがって、該方法は取引における売買双方の入力を大幅に簡略化し、取引の効率を向上させる。」（１４頁５行～８行）

１１

図１

以　上

別紙３

甲７の記載（翻訳・抜粋）

１

「【請求項７】

決済データを処理するための方法であって、

受取人端末から送信された暗号化決済要求データおよび第１の支払い金額を受信し、前記暗号化決済要求データは、前記受取人端末から送信された受取人情報の受信後に支払人端末から返された決済要求データに基づいており、支払人情報、前記受取人情報、および、第２の支払い金額を含み、

前記暗号化決済要求データおよび前記第２の支払い金額を検証し、

前記検証の結果に従って決済を実行し、

暗号化決済結果データを前記受取人端末に返送すること、

を備える、方法。」

２

「【００１８】

図１は、モバイル決済処理システムの一実施形態を示すブロック図である。プラットフォーム１００は、支払人端末１０２、決済（受取人）端末１０４、および、決済サーバ１０６を備える。決済サーバは、ネットワークまたは専用ラインを介して銀行と接続されている決済サーバであってよい。いくつかの実施形態において、決済サーバは、Ａｌｉｐａｙ．ｃｏｍなどの信頼できるサードパーティ決済サービス業者によって提供される。支払人端末および受取人端末は、通信機能を有する任意の適切な電子デバイス、特に、携帯電話、携帯情報端末（ＰＤＡ）、ノートブックコンピュータなどの携帯型電子端末であってよい。

【００１９】

図の実施形態において、決済サーバは、ネットワークを介して、支払人端末および受取人端末にインストールして用いられる電子決済クライアントソフトウェアを

提供する。支払人端末において、決済クライアントソフトウェアは、支払いを実行する機能を提供する。受取人端末において、決済クライアントソフトウェアは、支払いを受け取る機能を提供する。特に、受取人端末および決済サーバは、インターネット、無線ネットワーク、専用ネットワーク、または、任意の他の適切な接続で通信できるが、支払人端末は、決済サーバとデータを直接やり取りしない。」

３

「【００２３】

プラットフォーム１００による決済データ処理について、図２Ａ～図２Ｂを参照しつつ説明する。これらの図は、決済データを処理するための手順の一実施形態を示すフローチャートである。処理２００は、決済処理プラットフォーム（１００など）上で実行されてよい。

【００２４】

支払人端末および受取人端末は、それぞれ、支払人口座番号および受取人口座番号を有するよう構成される。工程２０１において、決済サーバは、支払人端末に関連付けられた支払人口座番号および決済パスワードと、受取人端末に関連付けられた受取人口座番号とを予め格納する。

【００２５】

工程２０２において、支払人端末および決済サーバは、暗号化関数およびそれに関連するパラメータを設定する。いくつかの実施形態において、暗号化関数およびパラメータの定義は、支払人端末および決済サーバによってアクセス可能なファイル内に予め格納されており、構成設定中にデバイスによってロードされる。

【００２６】

予め定義された暗号化関数は、支払人端末と決済サーバと間の決済データの伝送の安全性を保証するために、受取人端末には知られていない。換言すると、受取人端末は、暗号化されたデータを復号できない。例えば、いくつかの実施形態では、予め定義された暗号化関数としてＲＳＡ暗号化関数が実装される。ＲＳＡアルゴリ

ズムは、公開鍵を用いてデータを暗号化し、秘密鍵を用いてのみ復号することができる。したがって、決済サーバは、公開されない秘密鍵を持ち、対応する公開鍵を公開する。支払人端末は、公開鍵で決済要求データを暗号化し、暗号化された情報を受取人端末に送信する。決済サーバの秘密鍵は受取人端末または別の第三者に知られていないため、受取人端末は、決済要求データに対して復号、偽造、または、それ以外の改ざんを行うことができない。

【００２７】

この例では、接続ベースのプロトコルが用いられる。工程２０３において、受取人端末および支払人端末は、現行の決済処理の開始時に接続を確立する。支払人端末および受取人端末は、現行の決済の開始時に有線接続を用いて接続されてよい。例えば、携帯電話である支払人端末と、コンピュータである受取人端末が、ミニＵＳＢラインで接続されてよい。あるいは、支払人端末および受取人端末は、Ｂｌｕｅｔｏｏｔｈ、赤外線、ＷＩＦＩなどの無線プロトコルを用いて無線接続されてもよい。」

４

「【００２９】

工程２０４において、決済サーバは、現行の決済を一意的に特定する決済シリアル番号を受取人端末に提供し、決済シリアル番号を格納する。決済シリアル番号は、決済の開始時に受取人端末に対して決済サーバによって割り当てられるランダムな番号、または、決済サーバおよび受取人端末によって同意された所定のアルゴリズムによって生成されるランダムな番号であってよい。例えば、いくつかの実施形態において、アルゴリズムは、決済が成功する度に所定のカウントをインクリメントし、その結果の値をシリアル番号として用いる。

【００３０】

工程２０５において、受取人端末は、決済シリアル番号および受取人口座番号を含む受取人情報を支払人端末に送信する。受取人端末から支払人端末へ送信された

受取人情報は、受取人口座番号と決済サーバによって提供された決済シリアル番号とを含んでおり、受取人端末によって確定された支払い金額を任意選択的に含んでもよい。

【００３１】

工程２０６において、支払人端末は、暗号化関数を用いて、支払人口座番号、決済パスワード、受取人口座番号、決済シリアル番号、および、支払い金額を決済要求データに暗号化し、暗号化された決済要求データを受取人端末に送信する。

【００３２】

工程２０５および２０６において、支払い金額が受取人端末から支払人端末に送信される場合、支払人端末から返された暗号化決済要求データに含まれる支払い金額は、受取人端末からの支払い金額である。あるいは、受取人端末が支払人端末に支払い金額を送信しない場合、支払人端末から返された暗号化決済要求データに含まれる支払い金額は、支払人端末によって入力された支払い金額である。受取人端末は、暗号化決済要求データと支払人端末によって入力された支払い金額とを受信する。

【００３３】

工程２０７において、受取人端末は支払い金額を検証する。金額が正しい場合、受取人端末は、暗号化決済要求データおよび支払い金額を決済サーバに転送する。工程２０５において受取人端末が支払人端末に支払い金額を送信しない場合には、検証が必要であり、支払人端末から返された暗号化決済要求データに含まれる支払い金額は、支払人端末によって入力された支払い金額である。受取人端末は、支払人端末から、暗号化決済要求データと支払人端末によって入力された支払い金額とを受信すると、まず、支払い金額が正しいか検証する。一例では、暗号化された支払い金額が、販売される製品の費用と比較される。金額が正しい場合、受取人端末は、暗号化決済要求データおよび支払い金額を決済サーバに転送する。

【００３４】

工程２０８において、決済サーバは、復号された支払人口座番号、決済パスワード、受取人口座番号、決済シリアル番号、および、支払い金額を取得するために、事前に定義された暗号化関数を用いて決済要求データを復号する。

【００３５】

工程２０９において、決済サーバは、復号された全決済データが、格納された決済データと一致するか否かを判定し、一致する場合、フローは工程２１０に進み、そうでない場合、フローは工程２１６に進む。判定を行うために、決済サーバは、格納された支払人口座番号、決済パスワード、受取人口座番号、および、決済シリアル番号を読み出し、一致するか否かについて以下のデータを比較する。読み出した支払人口座番号と復号した支払人口座番号、読み出した決済パスワードと復号したパスワード、読み出した受取人口座番号と復号した受取人口座番号、および、読み出した決済シリアル番号と復号化した決済シリアル番号。

【００３６】

工程２０９において比較された読み出しデータおよび復号データのすべてが一致すると、さらに、工程２１０において、復号した支払い金額および受信した支払い金額が一致するか否か比較される。金額が一致した場合、フロー制御は工程２１１に進み、そうでない場合、フロー制御は工程２１６に進む。

【００３７】

工程２１１において、特定された金額の決済が決済サーバによって行われる。支払い金額分が、支払人の口座から差し引かれ、受取人の口座に増額される。決済が成功したか否かに応じて、決済処理の成功または失敗を示す決済結果データが生成される。」

５

「【００９６】

図１０は、決済サーバの第２の実施形態を示すブロック図である。

【００９７】

決済サーバは、事前設定ユニット１０１０、格納ユニット１０２０、提供ユニット１０３０、受信ユニット１０４０、検証ユニット１０５０、返送ユニット１０６０、および、削除ユニット１０７０を含む。

【００９８】

特に、事前設定ユニット１０１０は、支払人端末で暗号化関数を予め定義するよう構成されている。

【００９９】

格納ユニット１０２０は、受取人口座番号、支払人口座番号、および、決済パスワードを事前に格納するよう構成されている。

【０１００】

提供ユニット１０３０は、現行の決済を一意的に特定する決済シリアル番号を受取人端末に提供し、決済シリアル番号を格納するよう構成されている。

【０１０１】

受信ユニット１０４０は、受取人端末から送信された暗号化決済要求データおよび支払い金額を受信するよう適合されており、決済要求データは、受取人端末から送信された受取人情報の受信後に支払人端末から返された決済要求データであり、支払人情報、受取人情報、および、支払い金額を含み、支払人端末は、暗号化関数によって決済要求データを暗号化決済要求データに暗号化し、受取人情報は、決済シリアル番号および受取人口座番号を含み、支払人情報は、支払人口座番号および決済パスワードを含む。

【０１０２】

検証ユニット１０５０は、暗号化決済要求データおよび支払い金額を検証し、検証結果に従って決済を実行するよう構成されている。」

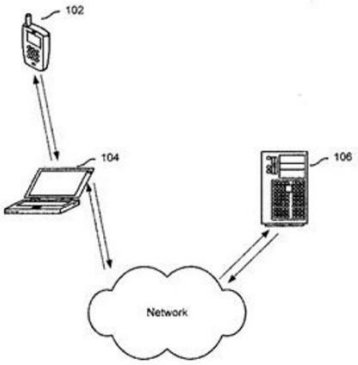
102
104
106
Network

FIG. 1

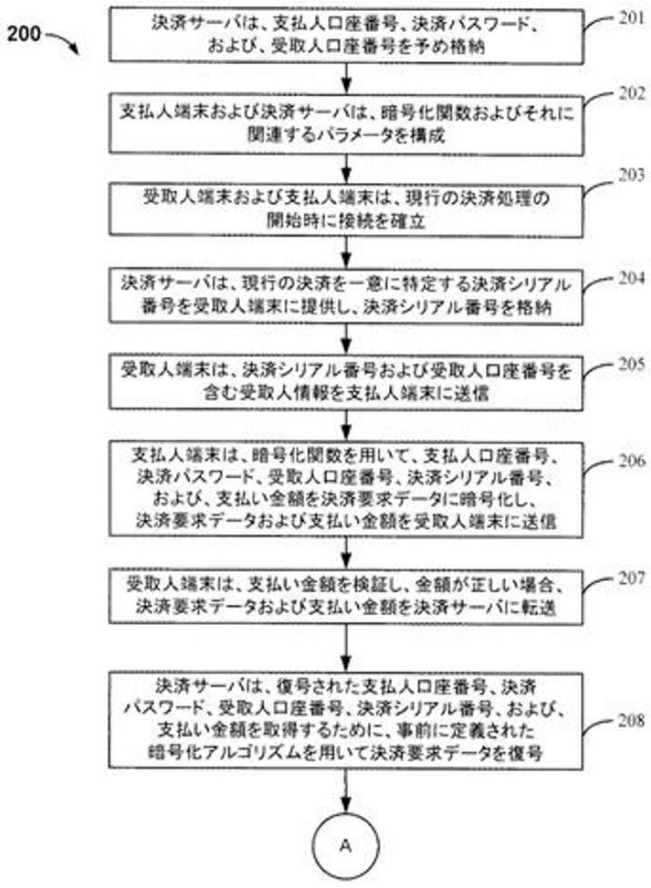
200
決済サーバは、支払人口座番号、決済パスワード、および、受取人口座番号を予め格納
201
支払人端末および決済サーバは、暗号化関数およびそれに関連するパラメータを構成
202
受取人端末および支払人端末は、現行の決済処理の開始時に接続を確立
203
決済サーバは、現行の決済を一意に特定する決済シリアル番号を受取人端末に提供し、決済シリアル番号を格納
204
受取人端末は、決済シリアル番号および受取人口座番号を含む受取人情報を支払人端末に送信
205
支払人端末は、暗号化関数を用いて、支払人口座番号、決済パスワード、受取人口座番号、決済シリアル番号、および、支払い金額を決済要求データに暗号化し、決済要求データおよび支払い金額を受取人端末に送信
206
受取人端末は、支払い金額を検証し、金額が正しい場合、決済要求データおよび支払い金額を決済サーバに転送
207
決済サーバは、復号された支払人口座番号、決済パスワード、受取人口座番号、決済シリアル番号、および、支払い金額を取得するために、事前に定義された暗号化アルゴリズムを用いて決済要求データを復号
208
A

FIG. 2A

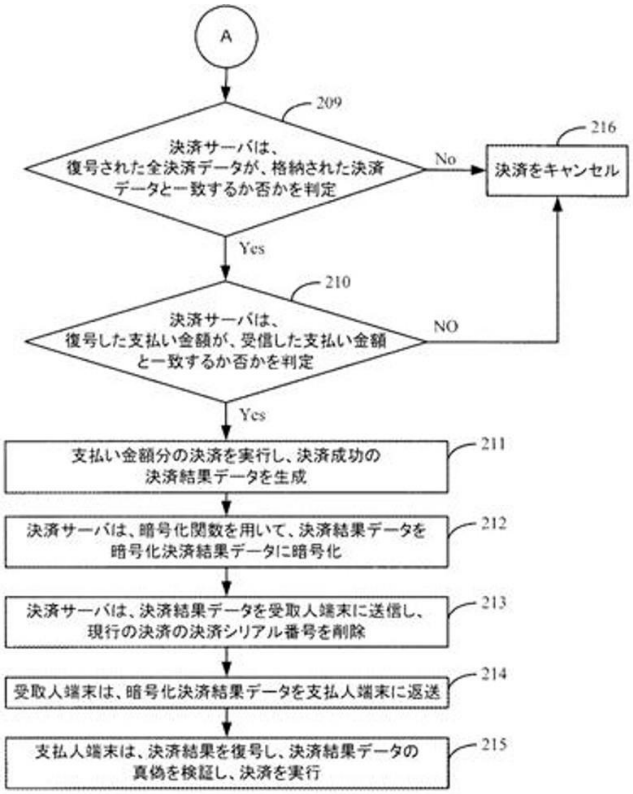
A
209
決済サーバは、
復号された全決済データが、格納された決済
データと一致するか否かを判定
No
216
決済をキャンセル
Yes
210
決済サーバは、
復号した支払い金額が、受信した支払い金額
と一致するか否かを判定
NO
Yes
支払い金額分の決済を実行し、決済成功の
決済結果データを生成
211
決済サーバは、暗号化関数を用いて、決済結果データを
暗号化決済結果データに暗号化
212
決済サーバは、決済結果データを受取人端末に送信し、
現行の決済の決済シリアル番号を削除
213
受取人端末は、暗号化決済結果データを支払人端末に返送
214
支払人端末は、決済結果を復号し、決済結果データの
真偽を検証し、決済を実行
215

FIG. 2B

以　上

5