令和５年２月２４日判決言渡　同日原本交付　裁判所書記官

令和３年（ワ）第７３２１号　損害賠償等請求事件

口頭弁論終結日　令和４年１２月２３日

判　　決

原　　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

同補佐人弁理士　尾　城　日　奈　子

被　　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　髙　梨　義　幸

同　松　本　　陸

同補佐人弁理士　澤　井　光　一

同　吉　田　幸　二

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

被告は、原告に対し、１００万円及びこれに対する令和３年４月３日から支払済みまで年５分の割合による金員を支払え。

第２　事案の概要等

１　事案の概要

本件は、発明の名称を「電子マネー送金方法及びそのシステム」とする２つの特許権（特許第６３０６２２７号、特許第６７１０８２０号）を有する原告が、被告が提供している電子決済サービスが同特許権に係る発明の技術的範囲に属するとして、主位的に特許法１０２条３項及び民法７０９条に基づき、予備的に不当利得に基づき、損害又は利得の一部として１００万円及びこれに対する令和３年４月３日（訴状送達の日の翌日）から支払済みまで平成２９年法律第４４号による改正前の民法所定の年５分の割合による遅延損害金又は利息を請求する事案である。

２　前提事実（当事者間に争いがないか、後掲各証拠及び弁論の全趣旨によって容易に認められる事実）

⑴ア　原告は、電子決済サービスのコンサルティング等を業とする株式会社である。（争いなし）

イ　被告は、電子決済サービスの提供等を業とする株式会社である。（争いなし）

⑵　原告は、以下の特許権（以下、アの特許権を「本件特許権１」、本件特許権１に係る特許を「本件特許１」、イの特許権を「本件特許権２」、本件特許権２に係る特許を「本件特許２」といい、本件特許権１、２を併せて「本件各特許権」、本件特許１、２を併せて「本件各特許」という。また、本件特許１及び本件特許２に係る明細書は同一であり、以下、「本件明細書」という。）を有している。（甲１～４）

ア　特許番号　　特許第６３０６２２７号

発明の名称　電子マネー送金方法及びそのシステム

優先日　　平成２３年１０月２５日

出願日　　平成２９年１月１９日

登録日　　平成３０年３月１６日

イ　特許番号　　特許第６７１０８２０号

発明の名称　電子マネー送金方法及びそのシステム

優先日　　平成２３年１０月２５日

出願日　　令和２年４月８日

登録日　　令和２年５月２９日

(3)　本件特許１の特許請求の範囲の請求項２、４、本件特許２の特許請求の範囲の請求項１の記載は以下のとおりである（以下、本件特許１の請求項２に記載された発明を「本件発明１」、同請求項４に記載された発明を「本件発明２」、本件特許２の請求項１に記載された発明を「本件発明３」といい、これらの発明を併せて「本件各発明」という。）。

ア　本件発明１

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、

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、

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、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、

前記電子マネー管理サーバ（３００）が、

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、

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、

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、

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、

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

ことを特徴とする電子マネー送金方法。

イ　本件発明２

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、

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、

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の証明情報の少なくとも一部（電子署名、個体情報）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、

前記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（ステップＳ１１１、１１２）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、

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、

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、

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

ことを特徴とする電子マネー送金方法。

ウ　本件発明３

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、少なくとも前記第１ユーザの電子マネーを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／決済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（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、

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）

が出力した前記第２の証明情報の少なくとも一部の情報を受けとり、この前記第１ユーザ端末（Ａ）を介して前記電子マネー管理サーバ（３００）に送信、及び／又は、前記第２ユーザ端末（Ｂ）が、前記第１ユーザ端末（Ａ）が出力した前記第１の証明情報の少なくとも一部の情報を受けとり、この第２ユーザ端末（Ｂ）を介して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、

前記電子マネー管理サーバ（３００）は、

前記第１ユーザ端末（Ａ）から受信した前記第２の証明情報の少なくとも一部の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及び前記第２の証明情報の送信元である前記第１ユーザ端末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、並びに／又は、 前記第２ユーザ端末（Ｂ）から受信した前記第１の証明情報の少なくとも一部の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及び前記第１の証明情報の送信元である前記第２ユーザ端末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）の認証を行う認証工程と、

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及び／又は前記第２ユーザ端末（Ｂ）から前記第１ユーザからの電子マネーの受取指示を受信し、さらに前記第１ユーザ端末（Ａ）から前記第２ユーザへの送金額の受信又は前記第２ユーザ端末（Ｂ）から前記第１ユーザからの受取額の受信を行う送金指示受信工程と、

前記第１ユーザ端末（Ａ）から受信した前記送金額又は前記第２ユーザ端末（Ｂ）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、

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、前記受信した前記送金額／受取額の電子マネーを、前記第１ユーザから前記第２ユーザへ送金する決済処理を行う決済工程と

を行う

ことを特徴とする電子マネー送金方法。

⑷ 本件各発明は、次のとおり分説することができる（以下、本件各発明におけるそれぞれの構成について、冒頭の符号に従い、「構成要件Ａ」等という。）。

ア　本件発明１

Ａ　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、

Ｂ　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、

Ｃ　この方法は、

Ｃ－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、

Ｃ－２　前記電子マネー管理サーバ（３００）が、

Ｃ－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、

Ｃ－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、

Ｃ－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、

Ｃ－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、

Ｃ－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

Ｄ　ことを特徴とする電子マネー送金方法。

イ　本件発明２

Ａ　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、

Ｂ　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（顧客マスタ及び／若しくは顧客マスタ中の端末を認証できる証明情報）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、

Ｅ　この方法は、

Ｅ－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、

Ｅ－２　前記電子マネー管理サーバ（３００）が、

Ｅ－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（ステップＳ１１１、１１２）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、

Ｅ－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、

Ｅ－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、

Ｅ－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

Ｄ　ことを特徴とする電子マネー送金方法。

ウ　本件発明３

Ｆ　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、少なくとも前記第１ユーザの電子マネーを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／決済を行う電子マネー送金方法であって、

Ｇ　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、

Ｈ　この方法は、

Ｈ－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を受けとり、この前記第１ユーザ端末（Ａ）を介して前記電子マネー管理サーバ(３００)に送信､及び／又は､前記第２ユーザ端末(Ｂ)が、前記第１ユーザ端末（Ａ）が出力した前記第１の証明情報の少なくとも一部の情報を受けとり、この第２ユーザ端末（Ｂ）を介して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、

Ｈ－２　前記電子マネー管理サーバ（３００）は、

Ｈ－２－１　前記第１ユーザ端末（Ａ）から受信した前記第２の証明情報の少なくとも一部の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及び前記第２の証明情報の送信元である前記第１ユーザ端末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､並びに／又は、 前記第２ユーザ端末（Ｂ）から受信した前記第１の証明情報の少なくとも一部の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及び前記第１の証明情報の送信元である前記第２ユーザ端末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）の認証を行う認証工程と、

Ｈ－２－２　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及び／又は前記第２ユーザ端末（Ｂ）から前記第１ユーザからの電子マネーの受取指示を受信し、さらに前記第１ユーザ端末（Ａ）から前記第２ユーザへの送金額の受信又は前記第２ユーザ端末（Ｂ）から前記第１ユーザからの受取額の受信を行う送金指示受信工程と、

Ｈ－２－３　前記第１ユーザ端末（Ａ）から受信した前記送金額又は前記第２ユーザ端末（Ｂ）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、

Ｈ－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、前記受信した前記送金額／受取額の電子マネーを、前記第１ユーザから前記第２ユーザへ送金する決済処理を行う決済工程と

を行う

Ｉ　ことを特徴とする電子マネー送金方法。

(5) 被告は、次の内容の電子決済サービス（以下「被告サービス」という。）を提供している。（弁論の全趣旨）

被告サービスは、現金等による代金等の支払に代えて行われる電子決済である。利用者（以下、被告サービスにおいて商品を購入したり、サービスの提供を受けたりする者を「利用者」という。）は、被告サービスを用いて決済すると、利用者があらかじめ被告に金銭を支払う等して被告のシステム（以下、「ＰａｙＰａｙシステム」といい、ＰａｙＰａｙシステムに用いる被告のサーバを「ＰａｙＰａｙサーバ」という。）上で仮想的に保有しているＰａｙＰａｙ残

高（１単位１円相当。）が減少する。他方で、利用者に商品の購入やサービスの提供をすることによって利用者と決済することになった相手方（以下「加盟店」という。）は、利用者について減少したＰａｙＰａｙ残高に対応する額が「売上金額」としてＰａｙＰａｙシステム上で記録される。被告サービスを利用した決済が行われるごとに当該加盟店の「売上金額」は加算されていき、後日、加盟店には、被告から「売上金額」の合計額に応じた清算金（後記のとおり、「返金処理」がされている場合には、その分、清算金が減少する。）が支払われる。

⑹　ＰａｙＰａｙシステムでは、加盟店又は利用者が提示するＱＲコード等のコードを加盟店又は利用者が読み取ることによって決済するが、コードを提示する主体、コードを提示する方法には次の種類がある（以下、冒頭の名称に従って、「被告方法１」などといい、これらの方法を併せて「各被告方法」という。）。

（弁論の全趣旨）

被告方法１　加盟店がコードを提示し、利用者が、自身の端末（以下、利用者が決済時に用いる端末を「利用者端末」という。）でコードを読み取って決済する。

被告方法１－１　利用者が決済金額を利用者端末に入力することによってＰａｙＰａｙシステムに対して当該決済に係る決済金額を指定する。

被告方法１－１－①　加盟店が、決済の時、加盟店が保有する端末（以下、加盟店が決済時に決済の場で用いる端末を「加盟店端末」という。）にコードを表示させて利用者に提示する。（加盟店は、あらかじめＩＤとパスワードを用いてＰａｙＰａｙサーバにログインし、必要なコード取得、表示させる。）

被告方法１－１－②　加盟店が、ＰａｙＰａｙサーバと通信してあらかじめ決済に必要なコード取得、印刷しておき（以下、加

盟店がＰａｙＰａｙサーバと通信してあらかじめコードを取得してこれを印刷する端末を「本件印刷端末」という。）、決済時にこれを利用者に呈示する。（加盟店は、あらかじめＩＤとパスワードを用いてＰａｙＰａｙサーバにログインし、必要なコード取得、表示させる。）

被告方法１－１－③　加盟店が、あらかじめ被告が作成した決済に必要なコードの印刷物を受領しておき、決済時にこれを利用者に提示する。

被告方法１－２　加盟店が決済金額を加盟店端末に入力することによって、ＰａｙＰａｙシステムに対して当該決済に係る決済金額を指定する。（ただし、加盟店端末が PayPay for Business アプリによってＰａｙＰａｙシステムを用いた決済に係る通信を行うものに限る。なお、同アプリを用いる場合には、当該端末は、決済につき直接被告のサーバと通信する。）

被告方法１－２－①　加盟店が、決済の時に加盟店端末に当該決済に必要なコードを表示させて利用者に提示する。

被告方法１－２－②　加盟店が、あらかじめ自身で特定の決済金額に係るコードを印刷しておき、決済時にこれを利用者に提示する。（被告方法１－１－②と同様、加盟店は、本件印刷端末を用いてＰａｙＰａｙサーバと通信して必要なコードを取得し、これを印刷する。）

被告方法１－３　加盟店が決済金額を加盟店端末に入力することによって、ＰａｙＰａｙシステムに対して当該決済に係る決済金額を指定する。（ただし、被告以外の者が開発した PayPay for Developers を用いて開発したアプリがインストールされた

加盟店端末を用いてＰａｙＰａｙシステムを用いた決済に係る通信を行うものに限る。なお、同アプリを用いる場合には、加盟店端末と被告サーバが直接通信をするものと、加盟店端末が加盟店のサーバと通信し、加盟店のサーバが被告のサーバと通信するものがあり得る。）

被告方法１－３－①　加盟店が、決済の時に自身の端末に特定の決済金額に係るコードを表示させて利用者に提示する。

被告方法１－３－②　加盟店が、あらかじめ自身で特定の決済金額に係るコードを印刷しておき、決済時にこれを利用者に提示する。（被告方法１－１－②と同様、加盟店は、本件印刷端末を用いてＰａｙＰａｙサーバと通信して必要なコードを取得し、これを印刷する。）

被告方法２　利用者がコードを提示し、加盟店が、加盟店端末でコードを読み取って決済する。

被告方法２－１　PayPay for Business が導入された加盟店の端末でコードを読み取るもの。（加盟店端末は、ＰａｙＰａｙサーバと直接通信する。）

被告方法２－２　PayPay for Developers を用いて被告以外の者が開発したアプリが導入された加盟店端末でコードを読み取り、決済代行業者のサーバを介してＰａｙＰａｙサーバと通信するもの。（加盟店端末は、①決済代行業者のサーバと通信し、決済代行業者のサーバがＰａｙＰａｙサーバと通信するものと、加盟店端末が直接ＰａｙＰａｙサーバと通信するものがある。）

(7)　各被告方法に係る決済の方式の概略は次のとおりである。

ア　被告方法１－１

●（省略）●その後、利用者は、利用者端末を用いて加盟店に提示されたコード（加盟店がコードを作成する方法は、前記のとおり３種類ある。）を読み取る。当該コードには、当該加盟店にひもづくＵＲＬ情報が記載されている。利用者端末は、同ＵＲＬを基にＰａｙＰａｙサーバと通信し、ＰａｙＰａｙサーバから加盟店の情報（加盟店名やロゴ等）を受信し、これが利用者端末に表示される。利用者は、同情報に基づいて決済相手に間違いがないことを確認し、利用者端末に決済金額を入力し、ＰａｙＰａｙサーバと通信する。●（省略）●

ＰａｙＰａｙサーバは、●（省略）●また、当該決済金額がＰａｙＰａｙサーバに記録されている利用者が保有するＰａｙＰａｙ残高の範囲内であるかを確認する。ＰａｙＰａｙ残高の範囲内である場合には、決済が実行され、ＰａｙＰａｙサーバで記録されている当該利用者に係るＰａｙＰａｙ残高の額を決済額分だけ減少させ、対応する加盟店に係る「売上金額」を決済金額分だけ増額する。

イ　被告方法１－２

●（省略）●その後、加盟店は、加盟店の端末に取引金額を入力し、●（省略）●ＰａｙＰａｙサーバは、加盟店ＩＤと取引金額とをひもづけたＵＲＬを作成し、同ＵＲＬが記載されたコードを加盟店の端末に送信する。加盟店は、ＰａｙＰａｙサーバから受信したＵＲＬに係るコードを利用者に提示する（提示の方法は前記のとおり２種類ある。）。●（省略）●ＰａｙＰａｙサーバは、利用者端末に対して当該加盟店情報（店舗名、ロゴ等）及び取引金額を送信する。●（省略）●決済金額が利用者のＰａｙＰａｙ残高未満であれば、決済を実行し、利用者のＰａｙＰａｙ残高の額を決済金額分だけ減少させ、対応する加盟店に係る「売上金額」を決済額分だけ増額する。

エ　被告方法１－３

加盟店は、取引金額を確定し、加盟店が PayPay for Developers を用いて

開発したアプリがインストールされた加盟店端末を用いてＰａｙＰａｙサーバに対して当該取引金額及び加盟店ＩＤを送信して利用者に提示するコードのＵＲＬの作成を依頼する。このとき、加盟店端末が直接ＰａｙＰａｙサーバと通信する場合と、加盟店のサーバを介してＰａｙＰａｙサーバと通信する場合があり得る。ＰａｙＰａｙサーバは、直接通信する相手となる加盟店端末又はサーバと認証情報のやり取りをして通信する端末またはサーバがアクセス権限を有することを確認するが、間接的に通信する対象となる端末を認証することはない。利用者に提示するコードが作成された後は、被告方法１－２と同じである。

オ　被告方法２－１

●（省略）●利用者端末は、同ワンタイムコードに対応するコードを利用者端末に表示させる。●（省略）●その後、同端末で利用者に提示されたワンタイムコードを読み取ることによって同ワンタイムコードを取得する。●（省略）●また、ＰａｙＰａｙサーバは、当該決済金額がＰａｙＰａｙサーバに記録されている利用者が保有しているＰａｙＰａｙ残高の範囲内であるかを確認する。決済金額がＰａｙＰａｙ残高の範囲内である場合には、決済が実行され、ＰａｙＰａｙサーバで記録されている当該利用者に係るＰａｙＰａｙ残高の額を決済金額分だけ減少し、ＰａｙＰａｙサーバが受信した加盟店ＩＤに対応する加盟店に係る「売上金額」を決済額分だけ増額する。

カ　被告方法２－２

利用者がワンタイムコードを加盟店に提示するまでは、被告方法２－１と同じ。加盟店端末は、PayPay for Developers を用いて加盟店が開発したアプリを導入した端末でワンタイムコードを読み取る。加盟店端末が同アプリを用いて直接ＰａｙＰａｙサーバと通信する場合には、あらかじめＰａｙＰａｙサーバから発行を受けていた認証情報を利用し、以降の仕組みは、被告方法２－１と同じ。同アプリを用いて中間決済業者を介して通信する場合に

は、中間決済事業者に対して同ワンタイムコード、加盟店ＩＤ、決済金額を送信する。中間決済業者は、ＰａｙＰａｙサーバに対して同情報及び中間決済事業者の認証情報を送信する。ＰａｙＰａｙサーバは、受信した認証情報を照合し、また、受信したワンタイムコードが利用者の情報と対応しているかを確認する。また、ＰａｙＰａｙサーバは、当該決済金額がＰａｙＰａｙサーバに記録されている利用者が保有しているＰａｙＰａｙ残高の範囲内であるかを確認する。確認後の仕組みは、被告方法２－１と同じである。

３　争点

⑴　各被告方法が本件各発明の技術的範囲に属するか

原告は、被告方法１が本件発明１、３の技術的範囲に属し（被告方法１－１－③については均等侵害)、被告方法２が本件発明２、３の技術的範囲に属すると主張している。構成要件に即した各被告方法に関する各当事者の主張の詳細は、別紙各被告方法に関する主張整理表のとおり（下線部が相違点である。）であり、争点は次のとおりである。

ア　各被告方法について

㋐　各被告方法は、「電子マネーの送金」を行っているといえるか（構成要件Ａ、Ｆ）（争点１－１－１）

㋑　各被告方法で、「第１ユーザ端末」及び「第２ユーザ端末」の認証を行っているか（構成要件Ｃ－２－２、Ｅ－２－１、Ｈ－２－１）（争点１－１－２）

イ　被告方法１について

㋐　被告方法１－１－②、１－２－②における本件印刷端末が「第２ユーザ端末」に当たるか（構成要件Ａ、Ｂ、Ｃ－１、Ｃ－２－２、Ｆ、Ｇ、Ｈ－１、Ｈ－２－１、Ｈ－２－２、Ｈ２－３）（争点１－２－１）

㋑　被告方法１で、「第１端末情報」及び「第２端末情報」の送受信をしているか（構成要件Ｃ－１、Ｃ－２－１、Ｃ－２－２）（争点１－２－２）

㈢　被告方法１で、「第２ユーザ端末」が「出力」した受取額を「第１ユーザ端末」が「受信」しているか（構成要件Ｃ－１）（争点１－２－３）

㈣　被告方法１－２で、第２ユーザ端末が「受取額」を出力し、第１ユーザ端末が「受取額」を受信しているか（構成要件Ｃ－１）（争点１－２－４）

㈤　被告方法１で、加盟店端末が第２の証明情報の少なくとも一部の情報を「出力」しているか（構成要件Ｈ－１）（争点１－２－５）

ウ　被告方法２について

被告方法２で、ユーザ端末が第１の証明情報の少なくとも一部の情報を「出力」しているか（構成要件Ｈ－１）（争点１－３）

⑵　被告方法１－１－③について、本件発明１、３に係る特許請求の範囲に記載された構成と均等なものとして、本件発明１、３の技術的範囲に属するか（争点２）

⑶　損害又は利得（争点３）

⑷　本件各特許に特許無効審判により無効とされるべき事由があるか

ア　分割要件違反に起因する新規性、進歩性欠如の有無（争点４－１）

イ　本件発明１に係る特許について

特許出願公開明細書公開番号第１８５１７６２号(以下「乙１３公報」という。)に記載された発明（以下「乙１３発明」という。）に基づく本件発明１の進歩性欠如の有無（争点４－２）

ウ　本件発明２に係る特許について

㈠　国際公開第ＷＯ２０１１／０６５９７４号(以下「乙１８公報」という。)に記載された発明（以下「乙１８発明」という。）に基づく本件発明２の進歩性欠如の有無（争点４－３－１）

㈡　サポート要件違反があるか（争点４－３－２）

㈢　補正要件違反があるか（争点４－３－３）

エ　本件発明３に係る特許について

㈠　乙１３発明、乙１８発明に基づく本件発明３の進歩性欠如の有無（争点４－４－１）

㈡　サポート要件違反があるか（争点４－４－２）

㈢　補正要件違反があるか（争点４－４－３）

４　争点に対する当事者の主張

⑴　各被告方法は、「電子マネーの送金」を行っているといえるか（構成要件Ａ、Ｆ）（争点１－１－１）

（原告の主張）

ア　電子マネーとは「貨幣価値をデジタル - データとしてＩＣカードやソフトウェアに記録し、貨幣価値の授受を電子的に行う仕組み」、すなわち貨幣価値を表すデジタルデータを使った決済の仕組みであるので、被告のＰａｙＰａｙ残高が電子マネーに該当することは明らかである。このような電子マネーに関する解釈は、電子マネーの取扱いを規制する「資金決済に関する法律」（資金決済法）の規定にも合致する。被告は、被告自身のホームページ及び被告のプライバシーポリシーで、ＰａｙＰａｙ残高は、上記と同意義の「電子マネー」の一種であると自認している。

本件各発明における「電子マネーの送金」とは、貨幣的価値としてのデジタルデータが、決済工程に従って電子マネー管理サーバ上で第１ユーザの残高から減額され、その分、第２ユーザの残高の増額として記録される決済処理のことをいう。

本件各発明は、各ユーザ下にある携帯端末やＩＣ媒体が電子マネーを記憶するのではなく、これらのユーザの情報を格納した電子マネー管理サーバが集中的に電子マネーを管理するようにしたこと電子マネーを格納したＩＣカードや携帯端末を紛失若しくは盗難されてしまうと、ＩＣチップに格納された電子マネーを取り戻すことは不可能であったという従来技術における問題点を解決したものである。さらに、本件各発明では、上記電子マネー管

理サーバにおいて各ユーザの端末を確実に認証できるようにしたことで、ユーザ間での電子マネーの送金を行うことができるようにした。このような本件特許の意義からしても、本件各発明における「電子マネーの送金」とは、電子マネー管理サーバ上での電子マネーそのものであるデジタルデータの流れ、すなわち電子マネーを用いたユーザ間での決済のことをいうものと解釈するのが自然である。

また、各被告方法では、加盟店は、加盟店アプリ上で返金処理を行なうことができる。返金処理されると、加盟店アプリには、取引ごとにそのことが表示され、サービス利用者のＰａｙＰａｙアプリには、その減額された取引金額のＰａｙＰａｙ残高が増額されて表示される。

ここで、加盟店の未入金の取引金額が利用者に返金したい額に満たない場合には、上記利用者へのＰａｙＰａｙ残高への返金は行えず、返金額を上回る取引金額の新規取引が発生した時点でＰａｙＰａｙ残高への返金を行なうことができる。加盟店の取引残高がＰａｙＰａｙ残高として返金したい金額以上ない場合には返金が行えないことから、当該加盟店の取引残高は、現金ではなく、データとしてＰａｙＰａｙ残高に相当することは明らかである。このように加盟店の取引残高は電子マネーとしての代替性を備えることが明らかである。

イ　被告は、裏で現金のやり取りをしていることを根拠に電子マネーの送金に当たらないと主張するが、一般的な電子マネーの取引においては、電子マネーそのものであるデジタルデータの流れ（電子マネーの送金）とは別に、現金等の流れがある。本件発明１は、電子マネー管理サーバ上での電子マネーであるデジタルデータの処理のみを規定しているにもかかわらず、被告の主張は、デジタルデータの他に現金の流れも「電子マネーの送金」に含めて議論しており、失当である。

また、被告は、規約等に基づき被告方法が電子マネーの送金に当たらない

と主張するが、本件発明１などで規定しているのは電子マネーを使った商品対価データの流れまでであり、加盟店における現金清算までは規定していない。被告の規約に基づく説明は、特許請求の範囲において規定した「電子マネーの送金」であるデジタルデータの流れとは乖離した現実の取引に基づく説明であって、特許請求の範囲の該当性判断に対する反論としては当を得ていない。

（被告の主張）

ア　本件各発明は、特許請求の範囲及び本件明細書（【０００１】）にも記載されているとおり、電子マネーの送金方法に関する発明である。本件明細書には決済が行われた後に、電子マネーの発行会社から店舗に対して実際の金銭が支払われる内容の先行技術が記載されている。本件明細書では、このような「電子マネーによる支払いは、一見電子マネーによる支払いがなされているように見えるが、実は裏で現金のやり取りがされており、電子マネーが完全に現金の代用として使われるものではない。」（【００１２】）とした上で、「本発明は、このような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およびそのシステムを提供することを目的とする」（【００１２】）としている。

他方で、各被告方法で決済に用いられるのは、ＰａｙＰａｙ残高であるが、被告の定める利用規約上も、ＰａｙＰａｙ残高は、サービス利用者のみが保有又は利用することを前提としており、加盟店がＰａｙＰａｙ残高を保有又は利用することは想定されていない。また、加盟店に適用される被告の定めたＰａｙＰａｙ残高加盟店規約においても、被告サービスにおいては、対象商品等の代価については加盟店ではなく被告が受領することとされており、加盟店が直接受領するわけではない。また、被告が加盟店に対して支払う精

算金は、あくまで現金である。したがって、被告サービスにおいては、ＰａｙＰａｙ残高がサービス利用者から加盟店に対して送金されるわけではなく、加盟店は、被告から精算金という形で現金を受け取っているにすぎない。被告サービスは、本件明細書で従来技術として記載されている、裏で現金のやり取りが行われているものである。よって、被告サービスにおいて用いられるＰａｙＰａｙ残高による支払は、本件各発明における「電子マネーの送金」には該当せず、また、ＰａｙＰａｙ残高は、本件各発明における「電子マネー」に該当しない。

イ　原告は、被告サービスにおける返金処理をもってＰａｙＰａｙ残高の「電子マネー」該当性を主張する。しかし、被告サービスにおける返金処理は、①被告から加盟店に対する、取消の対象となる取引に係る精算金（現金）の支払を中止する手続又は②被告が加盟店に対して既に支払った、取消の対象となる取引に係る取引金額分を、将来加盟店に対して支払われることが予定されている精算金（現金）の金額から減額することで、加盟店に対して支払われる現金の額につき調整を図っているものにすぎない。したがって、加盟店からサービス利用者に対してＰａｙＰａｙ残高を送金し返しているような処理は何ら行われていない。

(2)　各被告方法で、「第１ユーザ端末」及び「第２ユーザ端末」の認証を行っているか（争点１－１－２）（構成要件Ｃ－２－２、Ｅ－２－１、Ｈ－２－１）

（原告の主張）

第１ユーザ端末の認証と第２ユーザ端末の認証について規定している構成要件Ｃ－２－２、Ｅ－２－１、Ｈ－２－１の冒頭には、具体的な認証プロセスが記載されており、そこで行われるのは、管理サーバに格納されている「第１の証明情報」、「第２の証明情報」との照合であり、端末の情報ではなく、その端末を保有するユーザや加盟店を証明する情報を用いて照合することもできるとされている。

●（省略）●第２ユーザ端末に対応する加盟店端末又は本件印刷端末については加盟店情報にひもづくＵＲＬを利用して認証されており、「第１ユーザ端末」及び「第２ユーザ端末」の認証を行っているといえる。被告方法２では、第１ユーザ端末については、ワンタイムコードを利用して認証され、第２ユーザ端末については、加盟店ＩＤを利用して認証されている。

（被告の主張）

本件各発明で規定されているのは、「第１ユーザ端末」及び「第２ユーザ端末」の認証であって、その文言上、認証対象は端末に限られると解すべきである。

●（省略）●

加盟店についても、ＱＲコードに規定されているのは加盟店に関する情報であり、加盟店が利用する端末の情報は何ら含まれていないから、加盟店端末の認証は行われておらず、第２ユーザ端末の認証が行われているとはいえない。

また、被告方法１－３のうち、加盟店のサーバを介して通信するもの、被告方法２－２のうち決済代行業者のサーバを介して通信するものについては、ＰａｙＰａｙサーバが認証するのは、これらのサーバに係る認証情報であるから、加盟店の端末を認証しないことは明白である。

⑶　被告方法１－１－②、１－２－②における本件印刷端末が「第２ユーザ端末」に当たるか（構成要件Ａ、Ｂ、Ｃ－１、Ｃ－２－２、Ｆ、Ｇ、Ｈ－１、Ｈ－２－１、Ｈ－２－２、Ｈ２－３）（争点１－２－１）

（原告の主張）

被告方法１－１－②、１－２－②では、加盟店が本件印刷端末を用いて加盟店ＱＲコードを決済の前にあらかじめプリントアウトしておくが、ＰａｙＰａｙサーバから同コードを取得するにあたっては、コードを取得するタイミングを除いて、被告方法１－１－①、１－２－①と同じプロセスを経る。

被告方法１－１－②、１－２－②では、加盟店の端末はユーザとの決済に先立ってＰａｙＰａｙサーバとコード取得のために必要な通信を行ってこれを出力し、決済の時に加盟店の端末は必ずしもログイン状態にあるとは限らないが、そもそも、構成要件Ｃ－２－２記載の認証工程は、もっぱら電子マネー管理サーバのみで実行されるものであり、決済の場に第２ユーザの端末が存在するか否か、同端末が動作しているか否かは無関係である。

よって、本件印刷端末は「第２ユーザ端末」に当たる。

（被告の主張）

被告方法１－１－②、１－２－②では、あらかじめプリントアウトしておいた加盟店ＱＲコードを店内に設置しておき、ユーザが当該加盟店ＱＲコードを読み取るものであり、ユーザによる支払のときに、加盟店はＰａｙＰａｙサーバと通信可能な端末を用いておらず、認証工程において認証の対象になる端末も存在しない。よって、被告方法１－１－②、１－２－②では、第２ユーザ端末に相当するものが存在しない。

⑷　被告方法１で、「第１端末情報」及び「第２端末情報」の送受信をしているか（構成要件Ｃ－１、Ｃ－２－１、Ｃ－２－２）（争点１－２－２）

（原告の主張）

特許請求の範囲で定義されているとおり「第２端末情報」は、第２ユーザの情報又は第２端末の情報に関連付けられた情報の少なくとも一部の情報であればよく、「第１端末情報」も同様である。本件明細書でも、電子証明書中のデジタル署名が第２端末情報として記載されているが、被告が主張するような端末に関する情報ではない。

第２端末情報は、電子マネー管理サーバにおいてユーザ又は端末に関連付けられてさえすれば、いかなる情報、すなわち、どのような数字、記号の組み合わせからなる情報であってもよい。ＰａｙＰａｙシステム上のデータベース等によってユーザもしくは端末に関連付けられてさえいれば、システムとして端

末やユーザの認証を行えるのであり、実際、この実施例によれば、第２端末情報であるデジタル署名を用いることによって、ユーザ及び端末の認証を行っている。

●（省略）●

（被告の主張）

「第２端末情報」とは、その文言どおり、第２ユーザ端末に関する情報であり、また、本件各発明が通信回線を介して通信可能な第１ユーザ端末と第２ユーザ端末との間の電子マネーの送金方法に関するものであることを踏まえると、「第２端末情報」とは、「第２ユーザが有する通信可能な端末に関する情報」を意味すると解すべきである。

また、「第１端末情報」も同様に、「第１ユーザが有する通信可能な端末に関する情報」を意味すると解すべきである。

ＰａｙＰａｙサーバにおいては、端末単位ではなく、店舗単位で加盟店情報が管理されており、「ＰａｙＰａｙサーバ内において管理されている加盟店情報にひもづくＵＲＬ」には、加盟店の端末の情報は含まれていない。よって、ＰａｙＰａｙサーバとの間で、第２端末情報の送受信は行われていない。

●（省略）●よって、ＰａｙＰａｙサーバとの間で第１端末情報の送受信は行われていない。

(5) 被告方法１で、第２ユーザ端末が「出力」した受取額を「第１ユーザ端末」が「受信」しているか（構成要件Ｃ－１）（争点１－２－３）

（原告の主張）

本件明細書の記載によれば、ＰＯＳ端末に決済金額が表示されるものは「出力」に当たる。「出力」の態様は被告が主張するものに限定されない。

被告方法１でＰａｙＰａｙサービスに対応するＰＯＳレジスター等を用いている場合には、ＰＯＳ端末に商品の代金が表示されるから、これが第２ユーザ端末による受取金額の「出力」に当たる。被告方法１－２では、加盟店の端

末にPayPay for Businessが導入されているところ、ＱＲコードと共に取引金額が表示される構成になっているから、取引金額の「出力」に当たる。被告方法１－３でも同様の仕様になっているものは「出力」に当たる。また、被告方法１－２、１－３では、加盟店が設定した取引金額をＰａｙＰａｙサーバに送信する処理が行われるから、これも「出力」に当たる。

「受信」の方法も何ら限定されていないから、どんな方法であれ、出力された受領金額が入力されれば「受信」に当たる。したがって、ユーザが端末に直接入力することも、取引金額を取得可能なＵＲＬを受信して当該ＵＲＬから取引金額を受信することも「受信」に当たる。

（被告の主張）

本件発明１においては、第２ユーザ端末が「出力」した、第２端末情報と受取額を、第１ユーザ端末が「受信」することが規定されている。文言及び本件明細書の記載から、本件発明１における「出力」とは、第２ユーザ端末が第１ユーザ端末に対して、電信・電波を送ることであり、「受信」とは、第１ユーザ端末が第２ユーザ端末から電信・電波を受けることであると解すべきである。

被告方法１－１においては、ユーザが、加盟店側から何らかの方法で伝えられた取引金額を、自らユーザ端末に入力するのであって、加盟店端末は、受取額を「出力」しておらず、また、ユーザ端末も、受取額を「受信」しいていない。

また、被告方法１－２、１－３でも、支払時に加盟店からＱＲコードが提示され、ユーザもこれをカメラの読み取り機能を用いて読み取っているにすぎないから、ユーザ端末が電信・電波を受けるわけではない。したがって、加盟店端末は、受取額を「出力」していないし、また、ユーザ端末も受取額を「受信」などしていない。

(6) 被告方法１－２で、第２ユーザ端末が「受取額」を出力し、第１ユーザ端末が「受取額」を受信しているか（構成要件Ｃ－１）（争点１－２－４）

（原告の主張）

前記⑸で主張したとおり、出力、受信の方式は限定されるものではなく、被告方法１－２では、ＰａｙＰａｙサーバを介して「受取額」の情報をやり取りしているから、第２ユーザ端末が「受取額」を出力し、第１ユーザ端末が「受取額」を受信しているといえる。

（被告の主張）

被告方法１－２で利用されるＱＲコードに含まれているのは、ＰａｙＰａｙサーバ内において管理されている取引金額にひもづくＵＲＬにすぎず、取引金額それ自体の情報は含まれていない。ユーザは、当該ＵＲＬを基にＰａｙＰａｙサーバ上において取引金額を取得することで初めて取引金額を把握することができる。よって、第２ユーザ端末が「受取額」を出力することも、第１ユーザ端末が「受取額」を受信することもない。

⑺　被告方法１で、加盟店端末が第２の証明情報の少なくとも一部の情報を「出力」しているか（構成要件Ｈ－１）（争点１－２－５）

（原告の主張）

前記⑸で主張したとおり、本件各発明の「出力」の方法は限定されていない。被告方法１では加盟店端末又は本件印刷端末がＱＲコードを作成、提示することによって「出力」している。

（被告の主張）

本件発明３では、第２ユーザ端末が、第２の証明情報の少なくとも一部を「出力」することが規定されている。前記⑸で主張したとおり、本件各発明の「出力」とは、電子・電波を送ることを意味しており、被告方法１はいずれもこれに当たらない。

⑻　被告方法２で、ユーザ端末が第１の証明情報の少なくとも一部の情報を「出力」しているか（構成要件Ｈ－１）（争点１－３）

（原告の主張）

前記⑸で主張したとおり、本件各発明の「出力」の方法は限定されていない。被告方法２では利用者端末がコードを表示させることによって「出力」している。

（被告の主張）

前記⑸で主張したのと同様の理由により、加盟店端末は第１の証明情報の少なくとも一部の情報を「出力」していない。

⑼　被告方法１－１－③について、本件発明１、３に係る特許請求の範囲に記載された構成と均等なものとして、本件発明１、３の技術的範囲に属するか（争点２）

（原告の主張）

被告方法１－１－③については、「第２ユーザ」に対応する加盟店ではなく、被告が出力したＱＲコードを用いるため、「第２ユーザ端末」が「出力した」（構成要件Ｃ－１、Ｈ－１）の要件を満たさないものの、次のとおり、本件発明１、３に係る特許請求の範囲に記載された構成と均等なものとして、本件発明１、３の技術的範囲に属する

ア　第１要件（特許発明の本質的部分）について

本件各発明の第１の特徴は、各ユーザ下にある携帯端末やＩＣ媒体が電子マネーを記憶するのではなく、これらのユーザの情報を格納した電子マネー管理サーバが集中的に電子マネーを管理するようにしたことである。本件各発明の第２の特徴は、上記電子マネー管理サーバにおいて各ユーザの端末を確実に認証できるようにしたことである。したがって、これら２つの特徴が本件各発明の本質的部分に該当する。

この点、本件各発明の構成要件Ｃ－１、Ｈ－１には、「第２ユーザ端末」が「出力した」との限定が含まれている。しかし、本件各発明の課題を解決するための重要な部分は、ユーザの情報を格納した電子マネー管理サーバが集中的に電子マネーを管理すること、及び、上記電子マネー管理サーバにおい

て各ユーザの端末を確実に認証できるようにしたことであるから、このことが実現できればよいのであり、「第２ユーザ端末」が「出力した」については、第２ユーザが自己の端末を用いて出力するか、第三者、例えば外部の印刷業者や被告が印刷出力したＱＲコードの供給を受けてそれをユーザに読み取らせるように構成しても、本件各発明の課題は解決できる。

したがって、「第２ユーザ端末」が「出力した」との構成は、少なくとも本件各発明を特徴付けるほどの重要な部分ではない。

イ　第２要件（置換可能性）について

被告方法１－１－①、１－１－②、１－１－③で出力されるＱＲコードは全て同一であり、同一の加盟店証明情報（加盟店の証明情報）が含まれている。

そして、被告方法１－１－②のＱＲコードが本件各発明の作用効果を奏することからすると、被告方法１－１－③のＱＲコードは、加盟店自身がプリンター等で印刷出力するものよりも高品質な印刷を提供することにより加盟店における顧客体験を向上させることが専らの目的であり、そのような目的を有する以外は、ＱＲコード自体は被告方法１－１－①、１－１－②により出力されるものと全く同じものなのであるから、結果的に本件各発明の作用効果と同一の作用効果を奏する。

ウ　第３要件（容易想到性）について

被告方法１－１においては、同一のＱＲコードを被告方法１－１－①、１－１－②、１－１－③の全てで出力可能であり、各出力形態で出力されたＱＲコードの使い分けは専らＱＲコードの使用目的による。

例えば、被告方法１－１－③のＱＲコードは、高品質な印刷により提供されるものであるから加盟店における顧客体験を向上させたい箇所に使用されることが想定でき、そうでない箇所に使用する場合には被告方法１－１－②により加盟店自身が汎用プリンター等で印刷出力する方法によりＱＲコ

ードの印刷を実施する。被告方法１－１においては、ＱＲコードのダウンロードが行えるから、これを自らが備える汎用プリンターで印刷するのに変え、ＱＲコードを第三者の印刷業者に印刷を依頼して高品質なＱＲコードを得ることは容易である。

そして、被告のように加盟店に対して決済サービスを提供する業者であれば、本件特許の成立当時において、上記のような加盟店のニーズに応える形で、加盟店の要求の有無にかかわらずあらかじめ被告方法１－１－③によって高品質な印刷で出力したＱＲコードを郵送するサービスを提供することは容易に想到可能である。

エ　第４要件（公知技術容易推考でないこと）について

本件各発明の課題を解決するための重要な部分、すなわち、ユーザの情報を格納した電子マネー管理サーバが集中的に電子マネーを管理すること、及び、上記電子マネー管理サーバにおいて各ユーザの端末を確実に認証できるようにしたことに新規性及び進歩性が認められる以上、当業者が容易に推考できたものではない。

オ　第５要件（意識的除外にあたらないこと）について

原告は、ＱＲコードが第２ユーザ以外の被告を含む第三者によって出力されることを意識的に除外していない。

（被告の主張）

ア　第１要件について

本件特許の優先日当時の従来技術からすれば、原告も主張する本件明細書に記載された課題は、本件特許の優先日当時において既に解決されている課題であった。よって、本件各発明は、「従来技術と比較して特許発明の貢献の程度がそれ程大きくないと評価される場合」に該当し、本件各発明の本質的部分は、特許請求の範囲の記載とほぼ同義のものとして認定されることとなる。

被告方法１－１－③においては「第２ユーザ端末」が「第２端末情報」と「受取額」を出力していないため、構成要件１（Ｃ―１）を充足しない。また、前記のとおり、そもそも被告方法１は、本件発明１、３のすべての構成要件を充足しない。

したがって、被告方法１－１－③が本件各発明の本質的部分を備えておらず、本件各発明と被告方法１－１－③とは本質的部分において相違することは明らかである。よって、被告方法１－１－③は均等の第１要件を充足しない。

イ　第２要件について

本件各発明は、第１ユーザ端末と第２ユーザ端末が互いに有する電子証明書の情報を交換した上で、両者が他方の電子証明書に関する情報を電子マネー管理サーバに送信することで、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されているところ（【００１８】等）、「第２端末情報」が「第２ユーザ端末」により出力されたものであることにより、「電子マネー管理サーバ」が、「第２ユーザ端末」を確実に認証することができる。これに対して、被告方法１－１－③では、「第２ユーザ端末」が「第２端末情報」と「受取額」を出力しておらず、本件各発明と同一の作用効果を奏するとはいえない。よって、均等の第２要件も満たさない。

ウ　第３要件について

否認ないし争う。

エ　第４要件について

被告方法１－１－③は、本件明細書に記載された従来技術や、乙１３公報等の公知文献と同一又は当業者がこれから出願時に容易に推考できたものであるから、均等の第４要件を充足しない。

⑽　損害又は利得（争点３）

（原告の主張）

ア　被告は、平成３０年１０月５日より、各被告方法を使用して、電子決済サービスを提供しており、令和２年５月９日までの累計決済回数は、１０億回以上である。

また、各被告方法によるＱＲコード決済における１回の平均決済額は、約１０００円である。そうすると、上記期間中の決済総額は、１兆円を下らない。決済手数料を３％とすると、各被告方法の提供に基づき被告が得るべき決済手数料は上記決済総額の３％である３００億円を下らない。

そして、本件各発明のライセンス料は、少なくとも決算手数料の３％であるので、特許法１０２条３項に基づいて算定された原告の損害額は、少なくとも９億円である。

この損害は、被告の不法行為に起因するものであるので、被告は、原告の弁護士費用として、上記損害額の１割である９０００万円の損害賠償義務を負う。

よって、原告は、主位的に９億９０００万円の損害賠償請求権の一部として１００万円を請求する。

イ　また、被告は、原告に対して、上記本件各発明のライセンス料として、少なくとも９億円の支払を免れているので、原告は、被告に対して、少なくとも９億円の不当利得返還請求権を有する。

よって、原告は、被告に対して、予備的に９億円の不当利得返還請求権の一部として、１００万円の支払を求める。

（被告の主張）

否認ないし争う。

⑾　分割要件違反に起因する新規性、進歩性欠如の有無（争点４－１）

（被告の主張）

本件特許１に係る特許出願（以下「第２世代出願」という。）は、特願２０１３－５４０７２０号（以下「親出願」という。）の分割出願である特願２０１５

－２４０７６３号（以下「第１世代出願」という。）を原出願とする特許出願である。本件特許２は、第２世代出願の分割出願の分割出願の分割出願（第５世代出願）である。

本件発明２では、サーバに対する①第１ユーザの認証に用いる情報送信、②受取指示及び③受取額の指定をいずれも第２ユーザ側が行うこととされているが、第１世代出願に係る明細書にはこの事項が開示されていない。

また、本件発明２では、①第１ユーザの認証に用いる情報の送信、及び②受取指示の指定をいずれも第２ユーザ側からの伝達プロセスにより送金処理が完結することが規定されているが、第１世代出願に係る明細書には、この事項が開示されていない。

よって、分割出願の明細書、特許請求の範囲又は図面に記載された事項が、原出願の出願当初の明細書、特許請求の範囲又は図面に記載された事項の範囲内であるとはいえないから、本件特許１は分割要件を満たさない。本件特許１が分割要件を満たさないため、これの分割出願の分割出願の分割出願である本件特許２も分割要件を満たさない。

そして、このように分割要件を満たさないから、本件発明１、２の新規性、進歩性の判断は、本件特許１の現実の出願日である平成２９年１月１９日を基準とし、本件発明３の新規性、進歩性の判断は、早くても同日を基準としてされる。本件各発明は、いずれも第１世代出願に係る明細書（特開２０１６－５３９９１号）に記載された発明であるから新規性を欠き、本件発明２、３については少なくとも進歩性を欠く。

（原告の主張）

被告の主張は争う。本件発明２の構成要件は第１世代出願の実施形態１に開示されており、かつ、本件発明２の構成により本件各発明の課題が達成できるから分割要件を満たす。

⑿　乙１３発明に基づく本件発明１の進歩性欠如の有無（争点４－２）

（被告の主張）

ア　乙１３公報には、以下の各構成を含む乙１３発明が記載されている。

乙１３ａ　移動端末ユーザが有する移動端末と、サービスプロバイダが有するレジサービス端末と、移動端末及びレジサービス端末と通信接続され、レジサービス端末及び移動端末ユーザの身分情報及びそのアカウント情報を予め記憶しているネットワーク仲介システムとを用いて、移動端末ユーザからサービスプロバイダへの支払を実行するモバイル決済を行うモバイル決済方法であって、

乙１３ｂ　ネットワーク仲介システム及び移動端末は、移動端末ユーザのアカウント情報に関連付けられた移動端末ユーザの身分情報（移動端末の IMSI、移動端末の ESN、移動端末の番号などの情報のうちのいずれか一つ又は任意の組み合わせを含む）を記憶し、ネットワーク仲介システム及びレジサービス端末は、サービスプロバイダのアカウント情報又はサービスプロバイダ情報に関連付けられたレジサービス端末の身分情報（レジ端末情報（レジ端末の唯一の識別情報とレジ端末の番号情報を含む））を記憶し、

乙１３ｃ　モバイル決済方法は、

乙１３ｃ－１　モバイル決済の際、移動端末が、レジサービス端末が出力した、取引金額とレジサービス端末の身分情報に含まれるレジ端末情報とを含む画像を取得又は走査し、移動端末を介して、画像に含まれる、又は、画像から解析されたレジ端末情報及び取引金額がネットワーク仲介システムに送信されるようになっており、

乙１３ｃ－２　ネットワーク仲介システムが、

乙１３ｃ－２－１　移動端末から、移動端末の身分情報に含まれる移動端末の識別情報（移動端末の IMSI、移動端末の ESN、移動端末の番号などの情報のうちのいずれか一つ又は任意の組み合わせを含

む）と、レジ端末情報とを受信する工程と、

乙１３ｃ－２－２　移動端末から受信した移動端末の識別情報が、ネットワーク仲介システムに記憶されている移動端末の識別情報と対応しているか否かの判断と、レジ端末情報が、ネットワーク仲介システムに記憶されているレジ端末情報と対応しているか否かの判断とを行うことにより、移動端末ユーザ及びサービスプロバイダの身分の正当性を検証する工程と、

乙１３ｃ－２－３　移動端末から、取引金額を含む取引情報を受信する工程と、

乙１３ｃ－２－５　ネットワーク仲介システムに記憶される移動端末ユーザのアカウント情報とサービスプロバイダのアカウント情報に基づいて、移動端末ユーザからサービスプロバイダへの支払を実行するモバイル決済を行う工程とを行う、

乙１３ｄ　現金を支払う必要がないモバイル決済方法。

イ　本件発明１と乙１３発明とは、構成要件Ｃ－２－４及び構成要件Ｃ－２－５における以下の相違点を除き、一致する。

［相違点］

電子マネーの送金に関わるサーバの処理について、本件発明１では、受取額が残高内であるかの判断を行い（構成要件Ｃ－２－４）、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Ｃ－２－５）のに対し、乙１３発明では、このような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。

ウ　電子決済分野において、支払者（買手）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、本件特許の優先日より前において周知技術であった。そして、乙１３公報に「モバイル消費の様々なスーパーマーケットでの応用を加速することができる」

との記載があることも踏まえると、信頼性が高いモバイル決済を提供するという乙１３発明の課題を解決するために、乙１３発明において、買手の残高以上の買い物を許容しないよう、取引金額が買手の残高内であるかの残高確認を行うという周知技術を採用することへの示唆があるといえる。

（原告の主張）

被告の主張は否認ないし争う。乙１３発明は、その解決課題に基づけば、ネットワーク仲介システムにおいて、ユーザからの取引情報を仲介する取引情報の処理に関する発明であって、実際の支払処理までは開示していない。乙１３発明のネットワーク仲介システムにおけるアカウント情報に基づいた身分情報の正当性の判断も、決済のために行っているのではなく、専らユーザが送信する取引情報の正確な入力を担保するために行っている。

被告は、乙１３発明のネットワーク仲介システムが保持する「アカウント情報」には、金銭的価値すなわち電子マネーが含まれると主張するが、乙１３発明の技術思想に基づいて解釈すれば、そのように解釈する余地はない。

これらによれば、乙１３発明と本件発明１は、発明の構成要件として一致するものは存在せず、全く異なる発明である。あえて、被告が摘示した箇所に基づいて本件発明１の構成要件になぞらえて比較しても本件発明１と乙１３発明には次の相違点がある。

〔相違点１〕

本件発明１の電子マネー管理サーバは電子マネーを集中的に格納するのに対して、乙１３発明のネットワーク仲介システムでは、その点が必ずしも明らかでない点。

〔相違点２〕

本件発明１は、電子マネーの送金を行うに際して第１ユーザの電子マネー残高を確認するのに対して、乙１３発明は単に取引情報に含まれるべきユーザとサービスプロバイダの身分情報を確認しているにすぎない点。

〔相違点３〕

本件発明１は、第１ユーザと第２ユーザの認証を行い、これに基づいて電子マネー管理サーバに格納した第１ユーザの電子マネーを減額しかつ第２ユーザの電子マネー残高を増額することによって電子マネー送金を即座に完了するのに対して、乙１３発明は、そのような処理が記載されておらず単に支払又は取引情報を処理する点。

⑬　乙１８発明に基づく本件発明２の進歩性欠如の有無（争点４－３－１）

（被告の主張）

ア　乙１８公報には、以下の各構成を含む乙１８発明が記載されている。

乙１８ａ　支払人が有する支払人端末と、受取人が有する受取人端末と、支払人端末及び受取人端末とネットワークを介して接続され、支払人のアカウントナンバー及び受取人のアカウントナンバーをそれぞれ記憶する決済サーバとを用いて、支払人から受取人へ電子マネーに相当する金銭的価値の送金を行う決済データ処理方法であって、

乙１８ｂ　決済サーバ及び支払人端末は、支払人端末に関連付けられた支払人アカウントナンバーおよび決済パスワードを格納し、決済サーバ及び受取端末は、受取人端末に関連付けられた受取人アカウントナンバーを格納し、

乙１８ｅ　決済データ処理方法は、

乙１３ｅ－１　決済の際、受取人端末は、支払人端末から暗号化された暗号化決済要求データに含まれる支払人アカウントナンバー、決済パスワードを受け取り、受取人端末を介して、暗号化された暗号化決済要求データに含まれる支払人アカウントナンバー、決済パスワードが決済サーバに送信され、

乙１３ｅ－２　決済サーバが、

乙１３ｅ－２－１　支払人端末に関連付けられる支払人アカウントナンバーを受信した受取人端末により送信された、受取人端末に関連付けられた受取人アカウントナンバーが、決済サーバに格納されている受取人アカウントナンバーと一致しているかの比較と、受取人端末から受信した支払人端末に関連付けられた支払人アカウントナンバーが、決済サーバに格納されている支払人アカウントナンバーと一致しているか否かの比較とを行うことにより、支払人端末及び受取人端末の認証を行う工程と、

乙１３ｅ－２－２　受取人端末から、支払人端末からの支払金額を含む暗号化決済要求データを受信する工程と、

乙１３ｅ－２－４　決済サーバ内の支払人のアカウントから支払金額分が差し引かれ、決済サーバ内の受取人のアカウントに支払金額分が増額される工程とを行う、

乙１３ｄ　決済データ処理方法。

イ　本件発明２と乙１８発明とは、構成要件Ｅ－２－３及び構成要件Ｅ－２－４における以下の相違点を除き、一致する。

［相違点］

電子マネーの送金に関わるサーバの処理について、本件発明２では、受取額が残高内であるかの判断を行い（構成要件Ｅ－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Ｅ－２－４）のに対し、乙１８発明では、このような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。

ウ　電子決済分野において、支払者のアカウントに、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が周知技術であったことは、前記⑾ウで主張したとおりである。そして、乙１８公報には、乙１８発明のようなモバイル決済において、「・・・決済処理デバイスを店頭

に導入すること」との記載や、「[００１８]・・・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事業者によって提供される。」との記載がある。これらを考慮すると、サードパーティ決済サービス事業者が信頼できる事業者であるために、乙１８発明において、サードパーティ決済サービス事業者が支払人（買手）の残高以上の買い物を防止すべるために、支払金額が支払人の残高内であるかの残高確認を行うという周知技術を採用することへの示唆がある。

（原告の主張）

解決課題とそれに対する解決手段という観点からすると、乙１８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。このことは、乙１８発明を定義する請求項の記載でも「アカウントナンバー」を含む詳細な決済要求データの中身が特定されていないことからも明らかである。

したがって、アカウントナンバーを含む決済要求データには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べきであり、これには電子マネーは含まれていない。むしろ、乙１８発明におけるアカウントナンバーは、乙１３発明における「アカウント情報」と同様、決済要求データに含まれる支払人情報と受取人情報の正当性の判断を行うのに十分な情報であればよい。

これらによれば、被告が主張する乙１８発明と本件発明２の一致点及び相違点は認められず、乙１８発明に、上記の誤った相違点に関して被告が主張する周知技術を適用したとしても本件発明２の進歩性は否定できない。

⑭　サポート要件違反があるか（争点４－３－２）

（被告の主張）

本件特許１に係る本件明細書は、第１世代出願に係る明細書と同一である。前記⑾で主張したのと同じ理由で、本件発明２にはサポート要件違反がある。

（原告の主張）

被告の主張は争う。前記⑾と同様の理由により、サポート要件違反はない。

⑮　補正要件違反があるか（争点４－３－３）

（被告の主張）

本件明細書は、第１世代出願に係る明細書と同一である。そして、本件発明２に係る請求項４は、平成２９年５月９日付け手続補正書により追加されたものであるところ、上記補正は、前記⑾で主張したのと同様の理由により、新規事項を追加するものである。

（原告の主張）

被告の主張は争う。前記⑾で主張したのと同様の理由により、新規事項の追加はない。

⑯　乙１３発明、乙１８発明に基づく本件発明３の進歩性欠如の有無（争点４－４－１）

（被告の主張）

ア　本件発明３の構成要件Ｈ－１、Ｈ－２－１からＨ－２－４には、「及び／又は」、「並びに／又は」、「又は」、「／（「又は」を示すものと思われる）」と記載されていて、本件発明３の内容は不明確であるが、原告は、被告方法１、２のいずれもが本件発明３の技術的範囲に属すると主張するので、本件発明３には、少なくとも次の本件発明３－１、３－２の２つの発明が含まれている。

㋐　本件発明３－１

３－１（Ｆ）　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、少な

くとも前記第１ユーザの電子マネーを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／決済を行う電子マネー送金方法であって、

３－１（G）　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、

３－１（H）　この方法は、

３－１（H－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を受けとり、この前記第１ユーザ端末（A）を介して前記電子マネー管理サーバ（３００）に送信、及び／又は、・・・されるようになっており、

３－１（H－２）　前記電子マネー管理サーバ（３００）は、

３－１（H－２－１）　前記第１ユーザ端末（A）から受信した前記第２の証明情報の少なくとも一部の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及び前記第２の証明情報の送信元である前記第１ユーザ端末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、並びに／又は、・・・を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）の認証を行う認証工程と、

３－１（H－２－２）　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及び／又は・・・を行う送金指示受信

工程と、

３－１（Ｈ－２－３）　前記第１ユーザ端末（Ａ）から受信した前記送金額又は・・・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、

３－１（Ｈ－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、前記受信した前記送金額／・・・の電子マネーを、前記第１ユーザから前記第２ユーザへ送金する決済処理を行う決済工程とを行う

３－１（Ｉ）　ことを特徴とする電子マネー送金方法。

㈠　本件発明３－２

３－２（Ｆ）　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、少なくとも前記第１ユーザの電子マネーを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／決済を行う電子マネー送金方法であって、

３－２（Ｇ）　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、

３－２（Ｈ）　この方法は、

３－２（Ｈ－１）　前記送金の際、・・・及び／又は、前記第２ユーザ端末（Ｂ）が、前記第１ユーザ端末（Ａ）が出力した前記第１の証明情報

の少なくとも一部の情報を受けとり、この第２ユーザ端末（Ｂ）を介して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、

３－２（Ｈ－２）　前記電子マネー管理サーバ（３００）は、

３－２（Ｈ－２－１）　・・・並びに／又は、前記第２ユーザ端末（Ｂ）から受信した前記第１の証明情報の少なくとも一部の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及び前記第１の証明情報の送信元である前記第２ユーザ端末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）の認証を行う認証工程と、

３－２（Ｈ－２－２）　・・・及び／又は前記第２ユーザ端末（Ｂ）から前記第１ユーザからの電子マネーの受取指示を受信し、さらに・・・又は前記第２ユーザ端末（Ｂ）から前記第１ユーザからの受取額の受信を行う送金指示受信工程と、

３－２（Ｈ－２－３）　・・・又は前記第２ユーザ端末（Ｂ）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、

３－２（Ｈ－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、前記受信した前記・・・／受取額の電子マネーを、前記第１ユーザから前記第２ユーザへ送金する決済処理を行う決済工程とを行う

３－２（Ｉ）　ことを特徴とする電子マネー送金方法。

イ　本件発明３－１について

本件発明３－１は、乙１３発明に基づけば進歩性が欠如している。乙１３発明の内容は前記⑿で主張したとおりである。本件発明３－１と乙１３発明は、構成要件３－１（Ｈ－２－３）及び構成要件３－１（Ｈ－２－４）における以下の相違点を除き、一致する。そして、以下の相違点は、前記⑿における本件発明１における相違点と同じであるため、前記⑿において主張したのと同様の理由により、決済時における残高の判断及び確認は周知技術であり、相違点に係る構成は、乙１３発明に基づいて当業者が容易に想到できた。

［相違点］

電子マネーの送金に関わるサーバの処理について、本件発明３－１では、受取額が残高内であるかの判断を行い（構成要件３－１（Ｈ－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３－１（Ｈ－２－４））のに対し、乙１３発明では、このような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。

ウ　本件発明３－２は、乙１８発明に基づけば進歩性が欠如している。乙１８発明の内容は前記⒀で主張したとおりである。本件発明３－２と乙１８発明とは、次の相違点を除き、一致する。そして、本件発明３－２における相違点は、前記⒀における本件発明２における相違点と同じであるため、前記⒀で主張したのと同様の理由により、決済時における残高の判断及び確認は周知技術であり、相違点に係る構成は、乙１８発明に基づいて当業者が容易に想到できた。

［相違点］

電子マネーの送金に関わるサーバの処理について、本件発明３－２では、受取額が残高内であるかの判断を行い（構成要件３－２（Ｈ－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３－２（Ｈ－２－４））のに対し、乙１８発明では、このような残高確認を行うのか否かが必ずしも明らかではない点。

（原告の主張）

被告の主張は否認ないし争う。被告が主張する乙１３発明と乙１８発明の解釈に誤りがあることは前記⑿、⒀で主張したとおりである。

⒄　サポート要件違反があるか（争点４－４－２）

（被告の主張）

本件特許２に係る明細書は本件特許１に係る明細書と同一である。前記⑾で主張したのと同様の理由により本件発明３にはサポート要件違反がある。

（原告の主張）

被告の主張は争う。前記⑾と同様の理由により、サポート要件違反はない。

⒅　補正要件違反があるか（争点４－４－３）

（被告の主張）

本件特許２に係る本件明細書は、第１世代出願に係る明細書と同一である。そして、本件発明３（請求項１）は、令和２年４月９日付け手続補正書により手続補正されたものであり、その補正された電子マネーの送金方法には、サーバに対する①ユーザの認証に用いる情報の送信、及び②受取指示の指定をいずれも受金側からの伝達プロセスにより送金処理が完結するものが含まれる。上記補正は、前記⑾で主張したのと同様の理由により、新規事項を追加するものである。

（原告の主張）

被告の主張は争う。前記⑾で主張したのと同様の理由により、新規事項の追加はない。

第３　当裁判所の判断

１　本件各発明について

⑴　本件明細書の記載

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、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およびそのシステムに関する。

【背景技術】

【０００２】

近年では、ＩＣチップが埋め込まれた非接触型のＩＣカードやＩＣチップが埋め込まれた携帯端末などが普及してきている。ＩＣチップが埋め込まれた非接触型のＩＣカードの例としては、鉄道バスの乗降時に改札や乗降口で使われるものがあり、このＩＣカードのＩＣチップには予め電子マネーが記憶されている。このＩＣカードを改札や乗降口で専用のリーダライタに近付けると、前記リーダライタからの電磁波によってＩＣカードのＩＣチップに電力が供給されると共に、前記リーダライタから例えば乗車賃分の金銭の支払いを要求する信号がＩＣカードのＩＣチップに送信される。一方、ＩＣチップは前記供給される電力によって動作して前記リーダライタからの信号を受信し、前記乗車賃分の金額をＩＣチップに記憶されている電子マネーの残額から減額すると共に、前記乗車賃分の支払いを行うための信号を前記リーダライタに送信する。そして、ＩＣカードからの信号を受信したリーダライタはこのＩＣカードの電子マネーを管理しているセンター等と通信をして前記乗車賃の決済を完了させる。この決済を完了させるステップでは、電子マネーの発行会社から鉄道会社やバス会社に実際の現金が振り込まれることになる。このように、ＩＣカードのＩＣチップは予め電子マネーが記憶されており、ＩＣチップ自体が電子マネー（金銭的価値）を保持しているものである。

【０００３】

一方、ＩＣチップが埋め込まれた携帯端末でも、ＩＣチップに電子マネーを予め記憶させるようになっているので、ＩＣカードの場合と同様に前述のリー

ダライタを介して鉄道やバスの乗降時に乗車賃の支払いを行うことができる。

【０００４】

また、ＩＣチップが埋め込まれた携帯端末の場合は、携帯端末のアプリケーションからＩＣチップにアクセスし、そのアプリケーションを介してインターネットショッピング等を行うことも可能である。携帯端末のアプリケーションを用いたインターネットショッピングを行う場合の処理の例としては、先ず、この携帯端末のＩＣチップにＥｄｙ（登録商標）の電子マネーが格納されている状態で、前記アプリケーションがこの電子マネーを使用できるインターネットショッピングサイトにアクセスし、当該電子マネーを用いた決済の申込をする。すると、決済の申込を受け付けたショッピングサイトはその申込に関する実際の決済の要求をＥｄｙセンター（前記電子マネーを管理している所）に送信する。Ｅｄｙセンターでは前記実際の決済の要求に基づいた決済確認メールを前記携帯電話のアプリケーションに表示させ、決済の可否についての入力を要求する。前記携帯端末において決済可であると入力されると、前記アプリケーションによってこの携帯端末のＩＣチップから前記決済に係る金額の電子マネーが減額され、決済可であることがＥｄｙセンターに送信される。そして、Ｅｄｙセンターが決済可の信号を前記携帯電話から受信すると、前記ショッピングサイトに対して銀行等を介して実際の金銭の支払いの処理を行うと共に、前記ショッピングサイトおよび前記携帯端末に決済が完了したことを通知する。また、前記ショッピングサイトでも前記携帯端末のアプリケーションに決済が完了したことを表示させる等する。このように、ＩＣチップが埋め込まれた携帯端末を用いてインターネットショッピングを行う場合でも、ＩＣチップ自体が電子マネー（金銭的価値）を保持していることが前提となる。

【０００５】

一方、電子マネーを用いない決済としては、クレジットカードを用いた決済やデビットカード（デビットカード付きの銀行キャッシュカード）を用いた決

済もある。例えばデビットカードを用いてデビットカードを使用できる店舗で決済を行う場合は、先ず、デビットカードを店舗の定員に渡し、店舗の定員がそのデビッドカードをＰＯＳ端末に接続されている専用の読取装置に読み取らせる。また、デビットカードの持ち主はＰＯＳ端末に接続されている専用の機器に暗証番号を入力する。ＰＯＳ端末は、読取装置で読み取ったカード情報と、決済に係る金額と、暗証番号とをそのカードを発行した銀行のサーバに送信する。銀行のサーバにおいてカード情報の照会結果がＯＫの判断となり、そのカード情報に対応した口座に前記決済に係る金額が格納されていると判断されると、その口座から即時に前記決済に係る金額が引き落とされ、その金額を前記銀行から前記店舗に送金するための処理が行われる。また、前記店舗に前記口座からの引き落としが完了したこと等が通知され、デビットカードによる決済が完了する。

【０００６】

前記ＩＣカード、ＩＣチップ付き携帯端末、およびデビットカードによる決済方法については、特開２００９－１５１７３７号公報、特開２００６－０４８３６０号公報、特開２００８－２６４５２９号公報等の特許文献に参考となる記載がある。

【０００７】

ところで、前記デビットカードは実際の現金を取り扱うのに対し、前記ＩＣカードやＩＣチップ付き携帯端末は電子マネーを取り扱うものである。

【０００８】

ここで、デビットカードは実際の現金を取り扱うものであり、且つ、銀行の口座から直接現金を引き落として使われるものであるため、前記カード情報や暗証番号が盗まれ悪用されると、銀行口座にあるはずの現金が無くなることにより他の引き落としに影響が出る場合もあり、悪用された現金を取り戻すことが出来ない場合もあるので、その被害が大きくなる可能性がある。

【０００９】

一方、前記ＩＣカードやＩＣチップ付き携帯端末は電子マネーを取り扱うものであるため、例えＩＣカードや携帯端末を盗まれて悪用されたとしても、その電子マネーの被害額に限度があるため、デビットカードよりは安全であると言える。また、前記ＩＣカードやＩＣチップ付き携帯端末はそのＩＣチップ自体に電子マネー（金銭的価値）が格納されているので、ＩＣカードや携帯端末自体を盗まない限りはその電子マネーを使用することができないので、その点でもデビットカードよりは安全であると言える。

【００１０】

しかしながら、前記ＩＣカードやＩＣチップ付き携帯端末は、そのＩＣカードや携帯端末を紛失し又は盗まれることは、ＩＣチップに入っている電子マネーごと紛失又は盗まれることを意味する。このため、前記ＩＣカードや携帯端末を紛失し又は盗まれた際は、ＩＣカードの発行会社等に連絡することによりその使用に制限をかけることはできるが、ＩＣカードや携帯端末自体を回収できない限り、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。

【００１１】

一方、ＩＣチップ付き携帯端末を用いて店舗で電子マネーの支払いを行うことができるか否かは、主に店舗のＰＯＳ端末がリーダライタを備えていると共にその電子マネーによる決済システムを導入しているか否かによる。また、ＩＣチップ付き携帯端末を用いて店舗のＰＯＳ端末で電子マネーの支払いをする場合は、携帯端末のＩＣチップから代金分の電子マネーが減額され、その電子マネーの情報と、ＩＣチップの格納するユニーク情報と、ＰＯＳ端末が有するユニーク情報等が電子マネーを管理しているセンターに送信される。そして、センターにおいてその決済が問題無いことが確認されると、センターから前記店舗に実際の現金を支払うための処理が行われ、これにより携帯端末の持ち主から店舗への支払いが行われたものとみなされる。

【００１２】

このように、前記ＩＣカードや前記ＩＣチップ付き携帯端末による電子マネーによる支払いは、一見電子マネーによる支払いがな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。

【発明の概要】

【発明が解決しようとする課題】

【００１３】

本発明は、このような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およびそのシステムを提供することを目的とする。

【課題を解決するための手段】

【００１８】

このように、本発明では、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２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。

【００１９】

ここで、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。

【００２０】

また、本発明では、前述のように電子マネーの送受金を行おうとしている２つの端末を認証した後、電子マネー管理サーバが、各端末にアクセスキーを送信し、各端末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、電子マネー管理サーバは、各端末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、その上で第１ユーザから第２ユーザへの電子マネーの送金を電子マネー管理サーバ内で行う。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、第１ユーザから第２ユーザへの電子マネーの送金をより安全に行うことができる。

【００２１】

また、本発明では、各ユーザの電子マネーは電子マネー管理サーバ内に格納されるものであるため、例えば第１ユーザ端末を紛失し回収することができない場合でも、その一事をもって第１ユーザの電子マネーが減ることはない。

【００２２】

さらに、本発明では、第１ユーザ端末と第２ユーザ端末とが互いに有する電子証明書の内容を交換することや、電子マネー管理サーバ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、第１ユーザから第２ユーザ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。

【００３１】

このように、本発明では、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、自己の端末の証明情報が他の端末から電子マネー管理サーバに送られ、当該他の端末の証明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２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。

【００３２】

ここで、第１ユーザ端末が有する第１の証明情報は第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の証明情報は第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の証明情報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の証明情報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ユーザ端末の証明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。

【００３３】

また、本発明では、各ユーザの電子マネーは電子マネー管理サーバ内に格納されるものであるため、例えば第１ユーザ端末を紛失し回収することができない場合でも、その一事をもって第１ユーザの電子マネーが減ることはない。

【００３４】

さらに、本発明では、第１ユーザ端末と第２ユーザ端末とが互いに有する証明情報の内容を交換することや、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、第１ユーザから第２ユーザ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。

【００３５】

また、この本発明のさらに他の主要な観点によれば、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の証明情報を格納しているものであり、この方法は、前記第１ユーザ端末が、近距離無線通信又は前記通信回線を介して前記第２ユーザ端末から前記第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ユーザ端末のメモリに格納する第１受信工程を行い、前記電子マネー管理サーバが、前記第１受信工程の後に、前記第１ユーザ端末から前記第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、前記第２端末情報と、前記第１ユーザ端末から前記第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第２受信工程と、前記第１ユーザ端末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ユーザ端末および前記第２ユーザ端末の認証を行う認証工程と、前記認証工程の後、前記受取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を少なくとも判断する決済判断工程と、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ことを特徴とする電子マネー送金方法が提供される。

【００３６】

このように、本発明では、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および第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２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。

【００３７】

ここで、第１ユーザ端末が有する第１の証明情報は第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の証明情報は第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２の証明情報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ユーザ端末の証明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。

【００３８】

また、本発明では、各ユーザの電子マネーは電子マネー管理サーバ内に格納されるものであるため、例えば第１ユーザ端末を紛失し回収することができない場合でも、その一事をもって第１ユーザの電子マネーが減ることはない。

【００３９】

さらに、本発明では、第１ユーザ端末に第２ユーザ端末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、第１ユーザから第２ユーザ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。

【発明の効果】

【００４０】

本発明によれば、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。

【発明を実施するための形態】

【００４３】

以下、本発明の実施形態に係る電子マネー送金システムを図面に基づき説明する。

【００４４】

図１は本発明の第１実施形態に係る電子マネー送金システムの概略構成を示す図である。このシステムは、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

管理サーバと称する）３００とを有する。端末Ａ，Ｂは携帯情報端末（ＰＤＡ）やパーソナルコンピュータ（ＰＣ）と同等の機能を備えた携帯電話であっても良く、デスクトップ型やラップトップ型のＰＣであっても良く、ＰＯＳ端末等のコンピュータ装置であっても良く、他の公知のコンピュータ装置であっても良い。本実施形態では端末ＡはＰＣと同等の機能を備えた携帯電話であり、端末ＢはＰＯＳ端末である。なお、ファイアウォール、Ｗｅｂサーバ等の周知の構成は図示および説明を省略している。

【００５２】

先ず、端末Ａおよび管理サーバ３００が行う処理の一例（図７参照）に沿って、端末Ａを有するユーザＡが管理サーバ３００上における電子マネーの購入や電子マネーの送受金に必要な会員登録をする場合の処理について説明する。なお、ユーザＡは個人であっても良く、団体であっても良い。

【００５３】

先ず、端末Ａから管理サーバ３００に電子マネー取引用のアプリケーションのダウンロードを要求すると（ステップＳ１）、これに応答して管理サーバ３００から端末Ａにアプリケーションがダウンロードされる（ステップＳ２）。そして、端末Ａで前記アプリケーションを起動すると、表示装置１３０に会員登録の意思を確認する画面が表示される。端末Ａにおいてユーザ Ａが会員登録の意思を示す操作を行うと、端末Ａから管理サーバ３００に会員登録の要求が送信され（ステップＳ３）、これに応じて管理サーバ３００の会員登録処理部３８１により端末Ａの表示装置１３０に会員登録用の画面が表示される（ステップＳ４）。この最初に表示される会員登録用の画面ではユーザＡの有するメールアドレスの入力が要求される。続いて、ユーザＡが前記会員登録用の画面にメールアドレスを入力してその送信を行うと（ステップＳ５）、これに応答して管理サーバ３００の会員登録処理部３８１がユーザＡのメールアドレスに本登録用画面のＵＲＬを送信する（ステップＳ６）。尚、ステップＳ４およびＳ５でメ

ールアドレスの代わりに端末Ａ（携帯電話）の電話番号を送信するように構成することも可能である。

【００５４】

続いて、ユーザＡが端末Ａを操作することにより端末Ａから前記ＵＲＬの画面の表示要求が送信されると（ステップＳ７）、管理サーバ３００の会員登録処理部３８１により端末Ａの表示装置１３０に本登録画面が表示される（ステップＳ８）。続いて、ユーザＡが前記本登録画面にニックネームや氏名や名称、パスワード、秘密の質問の答え等を入力してその送信を行うと（ステップＳ９）、これに応答して管理サーバ３００の会員登録処理部３８１がユーザＡのメールアドレスにログインＩＤを送信する（ステップＳ１０）。前記ログインＩＤ、パスワード等を用いることにより、会員用画面表示処理部３８２によって表示される会員用画面にユーザＡがログインできるようになる。

【００５５】

前述のようにユーザＡの会員登録をする過程で、管理サーバ３００はその顧客マスタ格納部３５０の顧客マスタ３５１にユーザＡの情報を格納する（ステップＳ１１）（図５参照）。

【００５６】

また、端末Ｂを有するユーザＢが管理サーバ３００上における電子マネーの購入や電子マネーの送受金に必要な会員登録をする場合についても、図７に示すように、ユーザＡについての前述の説明と同等の処理（ステップＳ２１～Ｓ３１）が端末Ｂおよび管理サーバ３００において行われる。

【００５７】

続いて、端末Ａおよび管理サーバ３００が行う処理の一例（図８参照）に沿って、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説明する。

【００５８】

先ず、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。

【００５９】

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。

【００６０】

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）。

【００６１】

また、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、図８に示すように、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。

【００６２】

続いて、端末Ａおよび管理サーバ３００が行う処理の一例（図１０参照）に沿って、端末Ａを使ってユーザＡが電子マネーカードを購入する場合の処理について説明する。尚、この処理は端末Ｂでも行うことができる。

【００６３】

先ず、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Ｓ６１）、これに応答して管理サーバ３００の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Ｓ６２）。この会員用画面内には電子マネーカードの購入を行うためのボタンが配置されており、端末Ａにおいてユーザ Ａが電子マネーカードの購入を要求する操作を行うと、端末Ａから管理サーバ３００に電子マネーカードを購入要求が送信される（ステップＳ６３）。続いて、管理サーバ３００は電子マネーカード発行処理部３８

４により、端末Ａの表示装置１３０に電子マネーカードの購入画面（図１１参照）を表示させる（ステップＳ６４）。図１１のようにユーザＡが各項目に入力し購入ボタンを押すと、そのカード購入情報が端末Ａから管理サーバ３００に送信される（ステップＳ６５）。本実施形態の場合、図１１で選択されたカードの図柄（デザイン）は、ユーザが自分の好きな画像をカードの図柄として設定できるものである。この場合、ユーザＡはカードの図柄として使いたい画像を端末Ａの中等から選択し、その図柄がステップＳ６５において管理サーバ３００に送信される。この後、必要に応じて管理サーバ３００の電子マネーカード発行処理部３８４が必要な画面を端末Ａの表示装置１３０に表示させ、購入した電子マネーカードの料金の支払いや全ての情報の入力が完了すると、電子マネーカードが購入されたことになる。

【００６４】

続いて、管理サーバ３００の電子マネーカード発行処理部３８４は、ユーザＡが購入した電子マネーカードに対応する電子マネー口座の口座番号（カード番号)、セキュリティー番号等を設定し（ステップＳ６６)、その電子マネー口座の口座データを口座データ格納部３６０に格納すると共に（ステップＳ６７)、その口座番号を図５に示すように顧客マスタに格納する（ステップＳ６８)。本実施形態では、口座番号とカード番号に同じ番号を用いている。前記口座データは例えば図６に示すようなもので、送受金の履歴、残額等が格納されるようになっている。尚、各ユーザはそれぞれ管理サーバ３００内に複数の電子マネー口座を作成することが可能であり、この場合は各電子マネー口座それぞれに口座番号（カード番号）が設定される。つまり、各ユーザはそれぞれ複数の電子マネーカードを保有することができ、管理サーバ３００は各電子マネーカードをそれぞれ口座番号（カード番号）に紐付けて管理する。

【００６５】

また、管理サーバ３００は、電子マネーカード発行処理部３８４により、前

記カードの図柄、前記購入したカードの金額、口座番号（カード番号）等のカード情報を端末Ａに送信する（ステップＳ６９）。一方、端末Ａでは、受信したカード情報をカード情報格納部１７３に格納する（ステップＳ７０）。

【００６６】

端末Ａでは、前記アプリケーションによって図１２に示すようにカードの図柄、その口座番号（カード番号）に対応した残額、口座番号（カード番号)、およびセキュリティーコードを表示装置１３０に表示することができる。また、カード番号の一部とセキュリティーコードの一部にマスキング４００が表示され、マスキング４００によってカード番号の一部とセキュリティーコードの一部が隠れるようになっている。そして、指で表示画面１３０のマスキング４００に対応した位置を触れると、マスキング４００が消えることにより隠れていたカード番号の一部やセキュリティーコードの一部を見ることができるようになる。尚、端末ＡがＰＣやＰＯＳ端末の場合は、ポインタの位置をマスキング４００に合わせた時にマスキング４００が消えるように構成することも可能である。

【００６７】

ユーザＢも端末Ｂを用いてユーザＡが端末Ａで購入するのと同様の方法で電子マネーカードを購入することが可能である。

【００６８】

続いて、端末Ａ、端末Ｂおよび管理サーバ３００が行う処理の一例（図１３参照）に沿って、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について説明する。

【００６９】

先ず、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。これにより、ＰＯＳ端末の表示装置２３０に商品Ｘの代金である３００円が表示される。ユーザＡがその代金を端末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、以下のステップＳ１０１～Ｓ１２３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。

【００７０】

具体的には、先ず、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、第２の電子証明書中のデジタル署名を近距離無線通信を介して端末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、第１の電子証明書中のデジタル署名を近距離無線通信を介して端末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は何れが先であっても良く、同時であっても良い。また、前記近距離無線通信は端末Ａの近距離無線通信部１５０と端末Ｂのリーダライタ２５０とを介して行われる。また、近距離無線通信部１５０とリーダライタ２５０は互いの距離が数ｃｍ～十数ｃｍの距離になった時に近距離無線通信が可能と

なるものであり、それ以上の距離では通信できないものである。このような近距離無線通信の技術の例としてはＩＳＯ／ＩＥＣ１４４４３のＴｙｐｅＡ、Ｂ、又はＩＳＯ／ＩＥＣ１８０９２のＦｅｌｉｃａ（登録商標）等が挙げられる。尚、本実施形態ではこのような近距離無線通信を用いているが、前記距離以上で通信する近距離無線通信を用いることも勿論可能である。

【００７１】

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）。

【００７２】

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。

【００７３】

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）。

【００７４】

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、および（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）および（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。

【００７５】

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。

【００７６】

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。

【００７７】

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）。

【００７８】

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。

【００７９】

ここで、ステップＳ１０１～Ｓ１２３を行う際に、管理サーバ３００内にユーザＢの電子マネー口座が１つも設定されていない場合がある。この場合は適

切なタイミングでユーザＢに電子マネー口座の作成を促せば良い。例えば、ステップＳ１２１およびＳ１２２でアクセスキーが対応し且つ残額内であると判断された際に、ユーザＢの端末Ｂに電子マネー口座を作成することを促すことができる。具体的には、図１１においてカードの種類とカードの名称だけを選択させる画面を端末Ｂに表示させると共に、残金が０円の電子マネーカードを設定するか否かを確認するメッセージをユーザＢの端末Ｂに表示させる。ユーザＢがこのような処理に沿って電子マネーカードを作成することにより、前記ステップＳ１２３で前記受取額を振り込む電子マネー口座が管理サーバ３００内に設定される。

【００８０】

このように、本実施形態では、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２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。

【００８１】

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。

【００８２】

また、本実施形態では、前述のように電子マネーの送受金を行おうとしている２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。

【００８３】

また、本実施形態では、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。

【００８４】

さらに、本実施形態では、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。

【００８５】

尚、本実施形態では、端末Ａと端末Ｂの間で互いの電子証明書の一部を交換しているが、前記ステップＳ１０３で端末Ａから端末Ｂに第１の電子証明書そのものを送信し、前記ステップＳ１０１で端末Ｂから端末Ａに第２の電子証明書そのものを送信することもできる。

【００８６】

ここで、例えば取引を行う２つの携帯端末にＩＣチップを埋め込むと共に、各携帯端末のＩＣチップに所定の認証機関によって認証されたセキュリティーモジュールを持たせ、取引を行う２つの端末の認証を各端末のセキュリティーモジュールの内容に基づき行うことも考えられる。しかしながら、この場合、２つの端末のセキュリティーモジュールの仕様が異なると各端末が互いのセキュリティーモジュールの解読ができず、これにより取引が行えないなどの不都合が発生し易い。これに対し、本実施形態では、管理サーバ３００が各端末Ａ，Ｂに電子証明書を発行すると共に、発行した電子証明書およびその秘密鍵を管理サーバ３００が所有するシンプルな構成であるにも拘わらず、前述のように安全な取引を実現できるものであるから、セキュリティーモジュールを用いる場合に比べて実社会における有用性が高い。

【００８７】

また、本実施形態では、ステップＳ１１５およびＳ１１７において端末Ａと端末Ｂの両方からアクセスキーの要求があった後に、各端末Ａ，Ｂにそれぞれ

アクセスキーが発行される。このように、各端末Ａ，Ｂの何れか一方だけでは取引ができないようになっており、電子マネーの送金の安全性を確保する上で極めて有利である。

【００８８】

また、本実施形態では、管理サーバ３００のみが第１および第２の電子証明書の秘密鍵を有している。このため、端末Ａが端末Ｂから第２の電子証明書の一部を受信しても、端末Ａにおいてその電子証明書の一部を復号化することができない。また、端末Ｂも端末Ａから第１の電子証明書の一部を受信しても、端末Ｂにおいてその電子証明書の一部を復号化することができない。このため、電子マネーの送金の安全性が確保される。尚、本実施形態では、管理サーバ３００は第１および第２の電子証明書と紐付けて秘密鍵を有しているが、管理サーバ３００の有する第１および第２の電子証明書の中に秘密鍵を含めることも可能である。

【００８９】

また、本実施形態では、管理サーバ３００はユーザＡの電子マネーを複数の電子マネー口座番号に対応させて記憶可能である。また、ステップＳ１１９では、端末Ａは送金を行うべき電子マネー口座の口座番号を管理サーバ３００に送信する。このように、ユーザＡは複数の電子マネー口座を所有することが可能であり、送金の時に何れの電子マネー口座から送金するかを選択することができる。このため、ユーザＡが各電子マネー口座の用途をそれぞれ決定し、その用途に従って送金を行うことができる。

【００９０】

また、本実施形態では、ステップＳ１１２において、（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、および（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している。ここで、

ステップＳ１０５において、端末Ａが自己の有する第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し、ステップＳ１０６において、端末Ｂが自己の有する第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している。このため、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に比較により、ステップＳ１１２の判断を行うことができ、効率的であると共に、電子マネーの送金の安全性を確保する上で極めて有利な構成である。

【００９１】

また、ステップＳ１２３の後に、管理サーバ３００が前記第１および第２のアクセスキーを無効化し、これにより前記第１および第２のアクセスキーによる取引をさらに行うことはできなくなる。このように、本実施形態は、電子マネーの送金の安全性を確保する上で極めて有利な構成を有する。

【００９２】

また、本実施形態では、近距離無線通信部１５０とリーダライタ２５０は互いの距離が数ｃｍ～十数ｃｍの距離になった時に近距離無線通信が可能となるものであり、それ以上の距離では通信できないものである。このため、端末Ａと端末Ｂとが取引を行おうとする際に、他の端末との間で電子証明書の交換等を行うエラーが発生し難く、取引の安全性を確保する上で極めて有利である。

【００９３】

尚、本実施形態では、端末ＢがＰＯＳ端末であるものを示したが、端末Ｂも端末Ａと同様の携帯電話とすることが可能である。この場合、端末Ｂのリーダライタ２５０は近距離無線通信部となり、入力装置２６０もタッチパネル式入力装置となる。このように端末Ｂが携帯電話として構成されている場合でも、前記ステップＳ１０１～Ｓ１２３の処理を用いて商品Ｘの売買をすることも

可能である。しかも、端末Ａおよび端末Ｂが携帯電話として構成されている場合、ユーザＡとユーザＢはいつでもどこでも商品Ｘの売買をすることが可能になる。例えば、商品Ｘがユーザの有する農園で取れる果実である場合や、ユーザＡとユーザＢが道でばったり会った時に物品Ｙの売買をしたいと思った時でも、ユーザＡからユーザＢへの電子マネーの支払いを行うことができる。

【００９４】

例えば、管理サーバ３００や前記アプリケーションがユーザＢの端末Ｂの表示装置２３０に商品Ｘや物品Ｙの販売金額（ユーザＡから受け取りたい金額）を入力できるように構成することにより、端末Ｂが前記ＰＯＳ端末としての端末Ｂと同様の働きをする。そして、端末Ａの近距離無線通信部１５０と端末Ｂの近距離無線通信部２５０とを近付けて、ユーザＡが図１４のＰａｙボタンを押すことにより、前記ステップＳ１０１～Ｓ１２３の処理が行われる。

【００９５】

さらに、商品Ｘや物品Ｙの売買だけではなく、ユーザＢがユーザＡから電子マネーを受け取りたいと考えた場合でも、ユーザＢの端末Ｂの表示装置２３０にユーザＡから受け取りたい金額を入力できるように構成することにより、前記ステップＳ１０１～Ｓ１２３の処理によりユーザＢは電子マネーを受け取ることが可能である。

【００９６】

尚、本実施形態では、管理サーバ３００はユーザＡおよびユーザＢの電子マネーを電子マネーカードに紐付けられたものとして記憶している。これに対し、管理サーバ３００内にユーザＡおよびユーザＢの電子マネー口座として電子マネー財布や電子マネーフォルダのようなものを設定する場合、管理サーバ３００はユーザＡおよびユーザＢの電子マネーを前記電子マネー財布や電子マネーフォルダに紐付けて記憶することが可能である。

【００９７】

尚、本実施形態では、端末Ａの表示装置１３０に表示されるＰａｙボタンの操作により、前記ステップＳ１０１が開始される。これに対し、端末Ａの近距離無線通信部１５０と端末Ｂのリーダライタ２５０とを数ｃｍや十数ｃｍよりも近付けると自動的にステップＳ１０１が開始されるように構成することも可能であり、その他のきっかけによってステップＳ１０１が開始されるように構成することも可能である。

【００９８】

尚、本実施形態では、前記ステップＳ１０１およびＳ１０３において、近距離無線通信を介して端末Ａ，Ｂの間で互いの電子証明書の一部を交換している。これに対し、前記ステップＳ１０１およびＳ１０３において、移動体通信網やインターネット網を介して端末Ａ，Ｂの間で互いの電子証明書の一部を交換することも可能である。

【００９９】

尚、本実施形態では、ステップＳ１１１およびＳ１１２で前記（１）～（４）が全て対応していると判断された後、ステップＳ１１３～Ｓ１２１でアクセスキーを用いて取引をより安全にしている。これに対し、ステップＳ１１３～Ｓ１１８を省き、ステップＳ１１９およびＳ１２０でアクセスキーの送信を省き、ステップＳ１２１の判断を省いても、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。つまり、アクセスキーは取引をより安全にするために用いられているので、簡易な取引などの場合は省くことが可能となってくる。そして、アクセスキーを用いない場合でも、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ので、ユーザＡからユーザＢに安全に電子マネーを送金することができる。

【０１００】

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。

【０１０１】

以下、本発明の第２実施形態に係る電子マネー送金システムを説明する。このシステムは基本的には第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る。これにより、端末Ｂのリーダライタ２５０は近距離無線通信部となっており、入力装置２６０もタッチパネル式入力装置となっている。

【０１０２】

このシステムにおいて、ユーザＡ（送金側）がユーザＢ（受金側）に電子マネーの送金を行う場合について、端末Ａ、端末Ｂおよび管理サーバ３００が行う処理の一例（図１５参照）に沿って説明する。ユーザＡ（送金側）がユーザＢ（受金側）に電子マネーの送金を行う場合とは、ユーザＡがユーザＢにこずかいを渡す場合や電子マネーを貸す場合等が考えられる。以下では、ユーザＡがユーザＢに３００円を貸す場合について説明する。また、本実施形態の場合、管理サーバ３００や前記アプリケーションによりユーザＡの端末Ａの表示装置１３０に図１６に示すような画面が表示され、この画面でユーザＡが送金したい金額を入力できるように構成されている。以下はその金額が既に入力されているものとして説明する。

【０１０３】

先ず、端末Ａと端末Ｂの近距離無線通信部１５０および２５０を互いに近付けて、例えば図１６のＳｅｎｄボタン４２０を指で触れると、図１５のステップＳ２０１～Ｓ２２３が行われる。ここで、ステップＳ２０１～Ｓ２１８迄は第１実施形態のステップＳ１０１～Ｓ１１８と同等の処理が行われるので、その説明は割愛する。

【０１０４】

ステップ２１８の後、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、３００円である送金額とを管理サーバ３００に送信し（ステップＳ２１９）、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、受取指示とを管理サーバ３００に送信し（ステップＳ２２０）、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。ここで、端末Ｂは送金されたお金が入金されるべき電子マネー口座の口座番号を管理サーバ３００に送信することも可能である。

【０１０５】

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Ｓ２２１）。また、管理サーバ３００は、送受金要求受付処理部３８７により、前記送金額が管理サーバ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Ｓ２２２）。

【０１０６】

続いて、前記ステップＳ２２１でアクセスキーが対応していると共に、前記ステップＳ２２２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送金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送金額の分だけ増額する（ステップＳ２２３）。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。

【０１０７】

このような構成により、本実施形態も第１実施形態で説明したの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前述の各種の変更を加えることも可能である。

【０１０８】

以下、本発明の第３実施形態に係る電子マネー送金システムを説明する。このシステムは基本的には第２実施形態と同等の構成を有している。

【０１０９】

このシステムにおいて、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、端末Ａ、端末Ｂおよび管理サーバ３００が行う処理の一例（図１７参照）に沿って説明する。以下では、ユーザＡがユーザＢに３０００円の電子マネーカードを送る場合について説明する。また、本実施形態の場合、管理サーバ３００や前記アプリケーションがユーザＡの端末Ａの表示装置１３０に図１８に示すような画面が表示され、この画面でユーザＡが表示されている電子マネーカードの送信を指示できるように構成されている。

【０１１０】

先ず、端末Ａと端末Ｂの近距離無線通信部１５０および２５０を互いに近付けて、例えば図１８のＳｅｎｄボタン４３０を指で触れると、管理サーバ３００や前記アプリケーションが端末Ｂの表示装置２３０に、端末Ａに表示されている電子マネーカードの金額情報や、受け取るか受け取らないかの選択ができるボタンを表示させる（図１９参照）。この状態で、端末Ｂの表示装置２３０のＹｅｓボタン４３１を指で触れると、図１７のステップＳ３０１～Ｓ３２４が行われる。ここで、ステップＳ３０１～Ｓ３１８は第２実施形態のステップＳ２０１～Ｓ２１８と同等の処理が行われるので、その説明は割愛する。

【０１１１】

ステップＳ３１８の後、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、その電子マネーカードの全残額である送金額とを管理サーバ３００に送信し（ステップＳ３１９）、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。尚、ステップＳ３１９において、対象となっている電子マネーカードを端末Ｂに送ることを端末Ａから管理サーバ３００に指示することは、前述のように送金を行うべき電子マネー口座の口座番号と、その電子マネーカードの全残額とを管理サーバ３００に送信していることになる。

【０１１２】

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、受取指示とを管理サーバ３００に送信し（ステップＳ３２０）、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。

【０１１３】

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Ｓ３２１）。また、管理サーバ３００は、送受金要求受付処理部３８７により、前記送金額が管理サーバ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）の全残額であるか否かを判断する（ステップＳ３２２）。

【０１１４】

続いて、前記ステップＳ３２１でアクセスキーが対応していると共に、前記

ステップＳ３２２で全残額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送金額の分だけ減額すると共に、口座データ格納部３６０にユーザＢ用の新たな電子マネー口座（以下、口座ｂと称する）を設定し、その口座データの残額を前記送金額の分だけ増額する（ステップＳ３２３）。本実施形態では、ステップＳ３２２の後に口座データ格納部３６０から口座ａを抹消し、ステップＳ３２３で新たに設定するユーザＢ用の口座番号を抹消した口座ａの口座番号とする。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。

【０１１５】

続いて、端末Ａは近距離無線通信や移動体通信網を介して、口座ａの電子マネーカードの図柄を端末Ｂに送信する（ステップＳ３２４）。この後、管理サーバ３００や前記アプリケーションにより、端末Ｂの表示装置２３０に図２０に示すような画面が表示される。

【０１１６】

このような構成により、本実施形態も第１実施形態で説明したの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前述の各種の変更を加えることも可能である。

【０１１７】

また、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に電子マネーカードを直接に送ることができる。このため、電子マネーカードを現実のカードの受け渡しに極めて近い感覚でやりとりすることができる。

【０１１８】

尚、前記各実施形態で示した電子マネーカードは、通常のインターネットショッピングでも使用できるものである。例えば、ユーザＡがＰＣを使って当該電子マネーを使えるインターネットショッピングサイトを訪れ、欲しい商品の支払いをする時に、自己の有する電子マネーカードのカード番号やキュリティーコードをクレジットカードでの支払いの場合と同様に入力することにより、その商品を購入することが可能である。この決済を行う際、インターネットショッピングのサイト経営者から管理サーバ３００に問い合わせが行き、管理サーバ３００でそのカード番号の残額等を判断する処理が行われることになる。

【０１１９】

さらに、ユーザＡが端末Ａでログインしており、前記アプリケーション等によって端末Ａの表示装置１３０にログイン後の会員用画面が表示されている状態で、前記アプリケーションを介してインターネットショッピングを表示させ、その中の商品を電子マネーカードを使って購入することも可能である。この場合、当該インターネットショッピングで支払いを行う際に、前記アプリケーションや管理サーバ３００によって端末Ａの表示装置１３０に図２１に示すような画面が表示される。前述のように、図２１でも、電子マネーカードのカード番号やキュリティーコードを入力する画面となっている。

【０１２０】

しかし、ユーザＡは端末Ａで既にログインＩＤやパスワードを用いてログインしているので、この状態での当該電子マネーカードの不正使用の可能性が低くなっている。また、電子マネーカードはプリペイド式なので被害額に限度がある。そこで、図２１では右下に当該電子マネーカードの情報をあらわすボタン４４０を表示させ、電子マネーカードのカード番号やキュリティーコードを入力せずに前記ボタンの位置を指で触れることにより、表示装置１３０に図２２の画面および図２３の画面が表示されるようになっている。図２２の画面で

は、ユーザＡが入力すべきだったカード番号やセキュリティーコード等が入力された状態になっている。つまり、電子マネーカードのカード番号やキュリティーコードを入力しなくても決済を行うことができる。

【０１２１】

尚、前記第１実施形態では、端末Ｂが直接に管理サーバ３００とやりとりするものを示した。これに対し、ＪＣＢ（登録商標）やＶＩＳＡ（登録商標）等のカード会社のシステムを経由して端末Ｂが管理サーバ３００とやりとりをし、前記ステップＳ１０１～Ｓ１２３等を行うことも可能である。この場合、カード会社のシステムが端末Ｂと管理サーバ３００との間のデータのやりとりを中継するだけの場合もあり、ステップＳ１０１～Ｓ１２３のうち何れかのステップで管理サーバ３００や端末Ｂの代わりに機能する場合もある。さらに、カード会社のシステムと前記管理サーバ３００とを実質的に一体のシステムとして機能させることも可能である。このように、カード会社のシステムを介するようにするか、カード会社のシステムと実質的に一体のものとして機能すると、前記電子マネーカードを前記カード会社の加盟店で使用することが可能になる。

【０１２２】

以下、本発明の第４実施形態に係る電子マネー送金システムを説明する。このシステムの基本構成は第１実施形態と同様であり、端末Ａと管理サーバ３００が図２４および図２５のように構成されているものである。

【０１２３】

この実施形態の端末Ａは、第１ユーザ情報格納部１７５と、ＧＰＳ１７６とを有すると共に、プログラム格納部１８０に、それぞれ端末Ａに所定の動作を行わせる特典情報表示部１８７と、享受意思受付部１８８と、位置情報検出部１８９と、位置情報送信部１９０と、口座情報表示部１９１とを有する。

【０１２４】

第１ユーザ情報格納部１７５は第１ユーザ情報を格納しているものであり、この第１ユーザ端末固有情報は、ユーザＡ（第１ユーザ）の電子マネー口座の口座番号、又は当該口座番号に紐付けられたユーザＡの名前や生年月日等の固有情報、若しくはユーザＡの端末Ａの個体情報等の端末Ａ（第１ユーザの端末）に固有の第１ユーザ端末固有情報を少なくとも有するものである。

【０１２５】

特典情報表示部１８７は、後述する選択特典内容送信部３９０によって送信される特典情報を端末Ａの表示装置１３０に表示させるものである。例えば、図２６に示すように、表示装置１３０に特典情報を表示させる。表示する特典情報は１つでも複数でも良く、ユーザＢが顧客に提供する特典の情報だけであっても良く、ユーザＢが顧客に提供する特典の情報と他のユーザが顧客に提供する特典の情報を同時に表示しても良い。図２６では、ユーザＢが顧客に提供する特典の情報と他のユーザが顧客に提供する特典の情報を同時に表示している。

【０１２６】

享受意思受付部１８８は、例えば図２６に表示される「この特典を享受する」ボタン４５０をユーザが操作すると、その操作をタッチパネル式入力装置１６０を介して受け付け、受付けたユーザの意思を管理サーバ３００に送信するものである。また、場合によって、享受意思受付部１８８は第１ユーザ情報格納部１７５に格納されている第１ユーザ情報の一部又は全部を管理サーバ３００に送信するものである。

【０１２７】

位置情報検出部１８９は地図情報と連動しており、ＧＰＳ１７６により検知される端末Ａの位置情報に基づき、前記地図情報上における端末Ａの位置を特定するものである。また、位置情報送信部１９０は、位置情報検出部１８９で特定された前記地図情報上における端末Ａの位置情報を管理サーバ３００に

送信するものである。

【０１２８】

口座情報表示部１９１は、後述する口座情報送信部３９４によって送信される口座情報を端末Ａの表示装置１３０に表示させるものである。例えば、図２７に示すように、表示装置１３０にユーザＡの電子マネーの口座情報を表示させる。

【０１２９】

この実施形態の管理サーバ３００は、前記第１ユーザ情報格納部１７５と同じ第１ユーザ情報を格納している第１ユーザ情報格納部３７１と、ユーザＢ（第２ユーザ）や他のユーザが顧客に提供する特典の内容と特典の付与条件とを格納している特典格納部３７２とを有すると共に、プログラム格納部３８０は、それぞれ管理サーバ３００に所定の動作を行わせる特典内容選択部３８９と、選択特典内容送信部３９０と、前記享受意思受付部１８８によって送信されるユーザの意思を受信する享受意思受信部３９１と、付与判断部３９２と、特典付与部３９３と、口座情報送信部３９４とを有する。

【０１３０】

特典格納部３７２は、例えば図２８に示すように、ユーザＢや他のユーザが顧客に提供する特典の内容とその付与条件とを格納しているものである。図２８において、ユーザＢの特典は、ユーザＢの店舗での支払額に応じてキャッシュバックする特典であり、ユーザＣの特典は、ユーザＣの店舗での支払額に応じて、キャッシュバックを行うか、ユーザＣ以外の組織によって運営されている駐車場の割引を行う特典であり、ユーザＤの特典は、ユーザＤの店舗での支払額に応じて次回の飲食代を割引する特典である。また、図２８に示すように、各特典には配信条件も設定されており、例えば、ユーザＢの特典は、年齢と過去ユーザＢの店舗を利用した回数と地域の条件が設定されている。

【０１３１】

特典内容選択部３８９は、前記享受意思受付部１８８によって送信される第１ユーザ情報の一部や位置情報送信部１９０によって送信される位置情報に基づき、当該ユーザに適した特典内容を選択するものである。例えば、ユーザＡが百貨店ａや駅ｂの近傍にいることが位置情報送信部１９０によって送信され、前記享受意思受付部１８８によってユーザＡの第１ユーザ情報の一部である口座番号が送信され、サーバ３００内の第１ユーザ情報格納部で前記口座番号に対応して記憶格納されているユーザＡの年齢性別が２８歳男である場合は、図２８中に示されている５つの特典の配信条件に適合するので、５つの特典が選択される。なお、特典を選択する際に、対象となる店舗の利用回数を条件にすることも可能であり、図２８中のユーザＢの特典のように、ユーザＢの店舗を３回以上利用したユーザに特典を提供するように構成することも可能である。さらに、図２８中に記憶格納されている各特典にそれぞれプライオリティレートを付与し、特典を提供するユーザが管理サーバ３００を管理している企業に支払った特典付与サービス利用料に応じてプライオリティレートを変動させ、プライオリティレートに応じて選択の優先順位変更することも可能であり、下記選択特典内容送信部３９０により送信される際の優先送信順位を変更することも可能であり、上記特典情報表示部１８７によって表示する際の優先表示順位や表示位置を変更することも可能である。

【０１３２】

選択特典内容送信部３９０は、前記特典内容選択部３８９で選択された特典の内容に関する特典情報が端末Ａに送信される。

【０１３３】

付与判断部３９２、特典付与部３９３、および口座情報送信部３９４の動作については、端末Ａ、端末Ｂ、管理サーバ３００が行う処理の例（図２９参照）に沿って後述する。図２９は、第１実施形態と同様に、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を説明するものである。

【０１３４】

先ず、ユーザＡがユーザＢの店舗を訪れる前の段階で、端末Ａが位置情報検出部１８９により端末Ａの検出を行い（ステップＳ４０１）、特定された位置情報を端末Ａが管理サーバ３００に送信する（ステップＳ４０２）。管理サーバ３００は端末Ａの位置情報を受信すると、特典内容選択部３８９によってユーザＡに適した特典内容を特典格納部３７２に記憶格納されている特典テーブルから選択し（ステップＳ４０３）、選択特典内容送信部３９０によって端末Ａに選択された特典内容に関する特典情報を送信する（ステップＳ４０４）。この送信は端末Ａのブラウザーで表示するための表示データの送信であっても良く、メール送信であっても良い。

【０１３５】

ステップＳ４０４で送信される情報を受信した端末Ａは、図２６に示すように、例えばメールによって送信された情報を特典情報表示部１８７によって表示装置１３０に表示させ（ステップＳ４０５）。また、例えば図２６に表示される「この特典を享受する」ボタン４５０をユーザＡが操作すると、享受意思受付部１８８が前記操作をタッチパネル式入力装置１６０を介して受け付け（ステップＳ４０６）、受付けたユーザＡの意思を管理サーバ３００に送信する（ステップＳ４０７）、管理サーバ３００が享受意思受信部３９１によって送信されたユーザの意思を受信しメモリに格納する。ここでは、ユーザＡによって図２６中のユーザＢの特典が選択されるものとする。

【０１３６】

その後、第１実施形態と同様に、ユーザＡがユーザＢの店舗で商品Ｘを購入することを決め、ステップＳ４０８～Ｓ４３１が第１実施形態のステップＳ１０１～１２３と同様に行われる。なお、本実施形態では、ステップＳ４２６において、端末Ａがユーザ Ａについての前記第１ユーザ情報としてユーザＡの口

座番号を送信し、当該第１ユーザ情報を管理サーバ３００がメモリに記憶格納する。

【０１３７】

続いて、管理サーバ３００は付与判断部３９２によって、ステップ４２８で受信する受取額と、前記ステップＳ４１４、Ｓ４１５、Ｓ４１８、Ｓ４１９、Ｓ４２６、Ｓ４２８、Ｓ４２９、Ｓ４３０若しくはＳ４３１と、ステップＳ４３１における電子マネーの増減額のうち少なくとも１つとユーザＡが選択した特典の付与条件とを比較することにより、付与条件が満たされているか否かを判断する（ステップＳ４３２）。

【０１３８】

続いて、ステップＳ４０７で送信されるユーザＡによりユーザＢの特典を利用する意思が管理サーバ３００により受信されており、前記ステップＳ４３２で付与条件が満たされていると判断されると、管理サーバ３００は特典付与部３９３により、前記特典内容に基づいてユーザＡの電子マネー口座に特典を付与する（ステップＳ４３３）。例えば、図２７に示されているユーザＡの口座情報に示されているように、２０１２年９月１０日のユーザＢの店舗での２５００円の支払に対し、２００円のキャッシュバックを行う。ここで、ステップＳ４０７で端末Ａから管理サーバ３００にユーザＡについての前記第１ユーザ情報としてユーザＡの口座番号が送信されるようにし、ステップＳ４３２でその口座番号がステップＳ４２６で送信される口座番号に対応しているか否かも判断し、そこで対応していると判断された時に前記ステップＳ４３３を行うようにすることも可能である。この場合、特典の付与がより正確に行われるようになる。

【０１３９】

続いて、管理サーバ３００は口座情報送信部３９４により、ユーザＡの電子マネー口座の口座情報を、前記ステップＳ４３３で付与された付与特典情報と

共に端末Ａに送信し（ステップＳ４３４）、端末Ａは口座情報表示部１９１により、例えば図２７に示すようにユーザＡの口座の口座情報と共に前記付与特典情報を表示する（ステップＳ４３５）。

【０１４０】

このように、本実施形態によれば、ユーザＡの属性（年齢性別）や、ユーザＡの有する端末Ａの位置情報に基づいて、ユーザＡの端末に特典情報が表示されるので、ユーザＡにとっては自分に関連した特典情報を探す手間や時間を省くことができ、ユーザＢにとっては顧客に効果的に特典情報を知らせることができる。また、ステップＳ４０６でユーザＡが特典を享受するか否かの意思を受付け、ユーザＡが特典を使う意思を示した後に例えばユーザＢの店舗で特典の付与条件を満たす支払が行われた際に、ユーザＡの口座に特典が付与されるように構成したので、例えばユーザＡがどのような特典が付与されるのか意識せずに特典が自動的に付与される場合と比較し、ユーザＡの口座に特典が付与されたことやその内容が印象に残り易い。これは、ユーザＡの購買意欲を向上させることや、ユーザＡに例えばユーザＢの店舗を強く印象付けることに寄与し得るものである。また、ユーザＡの表示装置１３０にユーザＡの口座の口座データと共に付与された特典の情報が表示されるので、ユーザＡの口座に特典が付与されたことやその内容がより印象に残り易い。

【０１４１】

尚、本実施形態も第１実施形態で説明したの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前述の各種の変更を加えることも可能である。

【０１４２】

また、第１および第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、Ｓ１０４、Ｓ１０６、Ｓ１０８、Ｓ４１０、Ｓ４１１、Ｓ４１３、Ｓ４１５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。

【０１４３】

具体的には、図３０に示すように処理を行う。第１実施形態と同様に、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）の所に持っていく場合を想定して説明する。

【０１４４】

先ず、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、第２の電子証明書中のデジタル署名を近距離無線通信を介して端末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)。

【０１４５】

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)。

【０１４６】

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）。

【０１４７】

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）。

【０１４８】

続いて、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Ｓ５０９）。

【０１４９】

続いて、前記ステップＳ５０９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Ｓ５１０）。

【０１５０】

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２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。

【０１５１】

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。

【０１５２】

また、本実施形態では、各ユーザ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。

【０１５３】

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。

【０１５４】

尚、この発明は上記一実施形態に限定されるものではなく、発明の要旨を変更しない範囲で種々変形可能である。

【０１５５】

その他、本発明は、さまざまに変形可能であることは言うまでもなく、上述した一実施形態に限定されず、発明の要旨を変更しない範囲で種々変形可能である。

(2) 本件各発明の意義

本件明細書に記載された本件各発明の意義は次のとおりである。

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（【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カードや携帯端等の媒体が紛失等した場合には、発行会社等に連絡

することにより、使用に制限をかけることはできるが、「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」（【００１０】）という課題（以下、この課題を「課題①」ということがある。）があり、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」（【００１１】、【００１２】）といった課題（以下、この課題を「課題②」ということがある。）があった。

本件各発明は、これらの課題の解決を目的とする電子マネーの送金方法及びそのシステムの提供を目的とするものであり（【００１３】）、本件各発明の構成をとることによって、課題①について、送金に係る各ユーザの電子マネーをＩＣチップではなく電子マネー管理サーバ内に格納することによって、送金に利用する端末を紛失等して回収できなくなった場合であっても、そのことのみではユーザが保有する電子マネーが減少することがなくなり（【００２１】、【００３３】、【００３８】）、課題②について、各ユーザ端末が互いに有する電子証明書の内容を交換することや電子マネー管理サーバ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及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、各ユーザに電子マネーを直接送ることができるため、電子マネーを現金に極めて近い感覚でやり取りすることが可能になる（【００２２】、【００３４】、【００３９】）。

２　争点１－１（被告方法は、「電子マネーの送金」を行っているといえるか（構成要件Ａ、Ｆ）について

(1)　「電子マネーの送金」、「電子マネー送金方法」の意義

ア　本件各発明は、「電子マネーの送金」を行う「電子マネー送金方法」である

（構成要件Ａ、Ｆ）。これらからは、本件各発明は「電子マネー」を送金する方法であると理解できるが、記載特許請求の範囲には、本件各発明における「電子マネーの送金」、「電子マネーの送金方法」自体を定義する記載はない。

イ　「電子マネー」について、一般に、「貨幣価値をデジタルデータとしてＩＣカードやインターネットに接続されたサーバに記録し、貨幣価値の授受を電子的に行う仕組み。」（広辞苑第７版）という説明がされるなどし、また、貨幣とは「①商品交換の媒介物で、価値尺度・流通手段・価値貯蔵手段の３つの機能を持つもの。本来はそれ自身が交換されるものと等価な商品で、昔は貝殻・獣皮・宝石・布・農産物など、のち貨幣商品として最も適した金・銀のような貴金属が漸次用いられようになった。②広義には、本位貨幣のほか、法律によって強制通用力を認められた信用貨幣および預金通貨をも含めていう。」（広辞苑第７版）という説明がされる。

ウ　「電子マネーの送金」を行う「電子マネーの送金方法」である本件各発明の技術的意義は前記１(2)のとおりである。

そのうち、前記１(2)の課題②は、従来技術について、ＩＣチップが埋め込まれたＩＣカードやＩＣチップがあり、ＩＣチップ自体が電子マネー（金銭的価値）を保持しているところ（【０００２】、【０００４】）、ＩＣ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（【００１１】、【００１２】）ことを課題としている。そして、本件各発明は、この課題について、各ユーザ端末が互いに有する電子証明書の内容を交換することや電子マネー管理サーバ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及

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、各ユーザに電子マネーを直接送ることができるため、電子マネーを現金に極めて近い感覚でやり取りすることが可能になる（【００２２】、【００３４】、【００３９】）ことによって解決したとしている。これらによれば、利用者が利用するＩＣチップから決済相当額の電子マネーが減額されるが、その利用を行った店舗に対して現金の支払がされるものは、本件各発明とは異なる従来技術であり、本件各発明は、そのような従来技術の課題を解決した「電子マネーを直接送る」ものである。したがって、本件各発明の「電子マネーの送金」とは、利用者が電子マネーを利用してその後に利用先の店舗等に対する現金の支払等がされるようなものではない。そして、「電子マネーを直接送る」という文言は、送金元のユーザが保有している電子マネーの数額が減少すると同時に、送金先のユーザにおいて、電子マネーの数額を同額だけ増加させ、その数額について送金元のユーザと同様に利用できることと整合的である。このような解釈は電子マネーが電子マネーとして流通するものであるともいえるところ、電子マネーや貨幣については、上記イのような説明がされ、貨幣には流通手段としての側面があるとされる。本件各発明は、課題②との関係では、従前のＩＣチップ等の技術とは異なり、電子マネーが利用された場合にその利用先においてもそれを電子マネーとして利用できるという貨幣の流通手段の側面についても着目してされたものと解することができる。そして、本件明細書には、本件各発明の「電子マネーの送金」について、上記のような意味で電子マネーの数額の増減がされていることと矛盾する記載もない。

エ　これらによれば、本件各発明の「電子マネーの送金」は、その文言や、本件明細書に記載された従来技術と比較した本件各発明の技術的意義等に照らして、送金元の電子マネーの数額に係るデジタルデータが、送金額分だけ減少した数額に係るデジタルデータに置き換わり、送金先において、送金元

と同じ電子マネーについて、その数額に係るデジタルデータが、送金額分だけ増加した値に置き換わることを意味するものと解され、そのような送金に係る方法が本件各発明の「電子マネー送金方法」といえる。

本件各発明は、課題①について、送金に係る各ユーザの電子マネーをＩＣチップではなく電子マネー管理サーバ内に格納することにより解決し、また、「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」といった課題②を解決するため、本件各発明において各ユーザ端末が互いに有する電子証明書の内容を交換することや電子マネー管理サーバ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及び受取指示を送るなどの構成をとり（前記１(2)）、このような各ユーザ端末等に関係する構成により、「電子マネーの安全性」を確保しながらも、上記のとおり、送金元のユーザが保有している電子マネーの数額に係るデジタルデータが減少した値に置き換わるのと同時に、送金先において、送金元と同じ電子マネーについて、その数額に係るデジタルデータが、送金額分だけ増加した値に置き換わり、送金先のユーザにおいてその増加した数額分を電子マネーとして利用できることとして「電子マネーの送金」をすることを実現したものと解される。

(2) 各被告方法は、前記第２の２(5)ないし(7)のとおりであり、これらに関係する規約等について、証拠及び弁論の全趣旨によれば、次の事実が認められる。

ア　ＰａｙＰａｙ残高利用規約（以下「利用規約」という。）の記載（乙１）

被告と利用者の間で適用されるＰａｙＰａｙ残高利用規約には、次の記載がある。

第１編　総則

第２条　定義

本規約において、以下の用語は、以下に定める意味を有するものとしま

す。

⑸　「ＰａｙＰａｙ残高」とは、ＰａｙＰａｙマネー、ＰａｙＰａｙマネーライト、ＰａｙＰａｙボーナスおよびＰａｙＰａｙボーナスライトの総称をいいます。

⑹　「ＰａｙＰａｙ残高アカウント」とは、ＰａｙＰａｙ残高を電磁的に記録し、保管するために必要な口座をいいます。

第３条

１　利用者は、ＰａｙＰａｙ残高を、１単位１円として加盟店における対象商品等の購入に際しての代価の決済に利用することができます。・・・

２　利用者は、対象商品等を購入するときにＰａｙＰａｙ残高での決済を希望する場合には、当社所定の方法でＰａｙＰａｙ残高による支払いを指定するものとします。対象商品等の代金の金額が利用者のＰａｙＰａｙ残高アカウントに記録されたＰａｙＰａｙ残高の範囲内である場合、当社は、当該残高から対象商品等の代金に相当する額のＰａｙＰａｙ残高を、次項に定める方法により、当該利用者のＰａｙＰａｙ残高アカウントから減算します。当該減算がなされた時点で、利用者は、加盟店に対する対象商品等の代金の支払義務を免れるものとします。

４　利用者は、ＰａｙＰａｙ残高で決済した取引に関し、加盟店（当社を除きます。以下、本項において同じものとします。）との間で対象商品等の瑕疵、債務不履行その他の事由に基づき問題が生じた場合、利用者と当該加盟店との間で解決するものとします。この場合、利用者と加盟店との間で決済を取り消す必要が生じたときでも、加盟店は利用者に対して対象商品等の代金を直接返金せず、対象商品等の代金に相当するＰａｙＰａｙ残高をＰａｙＰａｙ残高アカウントに加算する方法により返金がなされることに利用者は同意するものとします。

イ　ＰａｙＰａｙ残高加盟店規約の記載（乙２）

被告と加盟店の間に適用されるＰａｙＰａｙ残高加盟店規約（以下「加盟店規約」という。）には次の記載がある。

第１条　総則

本規約は、商品等（第２条第５項に定義）の販売または提供（以下「販売等」といいます。）をする者がその販売等の代価を決済するにあたり、ＰａｙＰａｙ株式会社（以下「当社」といいます。）が発行するＰａｙＰａｙ残高（第２条第１項に定義）による決済を可能にすることを希望する場合に適用される条件を定めるものです。

第２条　定義

１　「ＰａｙＰａｙ残高」とは、以下の⑴および⑵の総称をいいます。

⑴　商品等の代価の弁済の為に使用することができ、また譲渡することができる電磁的方法により記録される前払式支払手段であって、当社がＰａｙＰａｙマネーライトという名称で発行するもの

⑵　商品等の代価の弁済のために使用することができ、また譲渡及び出金することができる電磁的記録であって、当社がＰａｙＰａｙマネーという名称で発行するもの。

２　「ＰａｙＰａｙ残高アカウント」とは、ＰａｙＰａｙ残高を電磁的に記録し、保管するために必要な口座をいいます。

３　「利用者」とは、別途当社が定めるＰａｙＰａｙ残高利用規約に従って、ＰａｙＰａｙ残高を利用する者または利用を希望する者をいいます。

４　「加盟店」とは、本規約に同意のうえ、ＰａｙＰａｙ残高による商品等の販売等の代価の決済を可能にすることを当社に申し込み、当社がこれを承認した者をいいます。

５　「商品等」とは、加盟店によって販売または提供される商品、役務および権利をいいます。

第５条　ＰａｙＰａｙ残高取引

1　本サービスの利用にあたり、加盟店は、当社に対し、対象商品等の代価（税金、送料等を含みます。以下同じ。）の代理受領権限を授与するものとします。

2　利用者が加盟店との間での対象商品等の取引に係る決済について、当社所定の方法でＰａｙＰａｙ残高による支払を選択した場合であって、当該対象商品等の代価が、当該利用者が保有するＰａｙＰａｙ残高の範囲内である場合、当社は、対象商品等の代価に相当するＰａｙＰａｙ残高を利用者のＰａｙＰａｙ残高アカウントから減算します。当該減算が完了したときに、加盟店の利用者に対する対象商品等の代価に係る債権は消滅するものとし、当社は、本契約に従い、当該対象商品等の代価を加盟店に支払うものとします。

第６条　商品の引渡し等

1　加盟店は、ＰａｙＰａｙ残高取引を受け付けた場合、遅滞なく利用者に対し対象商品等を引渡しまたは提供するものとします。・・・

第８条　返品等の取扱い

1　加盟店は、利用者との間に生じた対象商品等の瑕疵、欠陥その他ＰａｙＰａｙ残高取引上の一切の問題については、自己の責任において加盟店と利用者との間で当該問題を解決するものとします。ただし、加盟店は、利用者に対して対象商品等の代金を直接返還してはならないものとします。

2　加盟店は、利用者とのＰａｙＰａｙ残高取引を取消す必要が生じた場合、当社に通知し、当社の指示に従うものとします。

第１２条

1　当社は、当社所定の期間に係る決済額の合計金額から、当該期間に係る決済システム利用料およびこれに対する消費税を控除した残額を当社所定の時期までに加盟店が届け出た振込指定金融機関口座に振り込む方法により支払うものとします（以下ここで支払う金銭を「精算金」といいます。）。

ただし、当該支払日が銀行休業日に該当するときは、翌銀行営業日を支払日とするものとします。

2　当社が加盟店に対し決済システム利用料に係る支払請求権以外の債権（本契約に基づく債権に限りません。）を有している場合、当社は、前項に定める支払を行う際に、当該債権に係る代金についても控除したうえで支払うことができるものとします。

3　加盟店が決済額に係る請求額以外に当社に対する支払債権を有している場合、当社は、第１項に定める支払を行う際に、当該債権に係る債務をあわせて支払うことができるものとします。

(3)ア　本件各発明は、「電子マネーの送金」を行う「電子マネー送金方法」である（構成要件Ａ、Ｆ）とされている。そして、本件各発明の「電子マネーの送金」とは、送金元の電子マネーの数額に係るデジタルデータが、送金額分だけ減少した数額に係るデジタルデータに置き換わり、送金先において、送金元と同じ電子マネーについて、その数額に係るデジタルデータが、送金額分だけ増加した値に置き換わることを意味し（前記(1)エ）、本件各発明は、そのような「電子マネーの送金」についての方法である。そして、前記(1)で述べたところによれば、仮に送金元と送金先で増減する対象が別の性質を有するものであれば、送金先で取得できるものは送金元が保有していたものとは別のものなのであるから、送金先では同一条件でこれを利用することはできず、流通性が確保されていないことになってしまい、本件各発明の趣旨に反するものであるといえる。

イ　各被告方法が、前記(1)のとおりの「電子マネーの送金」を行っているか否かについて検討すると、原告は、各被告方法で用いられているＰａｙＰａｙ残高が電子マネーに当たり、各被告方法ではＰａｙＰａｙ残高の送金が行われていると主張する。

各被告方法には、いずれも利用規約及び加盟店規約が適用されるところ、

各被告方法はいずれもＰａｙＰａｙ残高を用いた加盟店からの商品、役務、権利の販売、提供に関する代金の決済に係る方法である（加盟店規約１条参照）。利用者は、決済に先立ち、ＰａｙＰａｙ残高を保有しておき、ＰａｙＰａｙ残高は、ＰａｙＰａｙ残高アカウントにおいて、電磁的に記録、保管される（利用規約２条１項(6)）。利用者は、代金の額がＰａｙＰａｙ残高（１単位１円相当）の範囲内であれば、各被告方法を用いてＰａｙＰａｙ残高を用いた決済をすることができ、このとき、利用者のＰａｙＰａｙ残高アカウントで電磁的に記録されていたＰａｙＰａｙ残高が代金分だけ減算され、利用者は加盟店に対する代金の支払義務を免れる（利用規約３条１項、２項、３項）。他方で、加盟店は、あらかじめ被告に対して代金の代理受領権限を授与しており（加盟店規約５条１項）、利用者によるＰａｙＰａｙ残高を用いた決済が実行されると、後日、被告から代金の支払を受けることになる（加盟店規約５条２項）。加盟店は、被告から、所定の期間に係るＰａｙＰａｙ残高を用いた決済の合計金額から、決済システム利用料及びこれに対する消費税を控除した残額（清算金）を、金融機関に対する振込みの方法で受領する（加盟店規約１２条１項）。

ＰａｙＰａｙシステムについての以上の仕組みを前提にすると、ＰａｙＰａｙ残高は、ＰａｙＰａｙ残高アカウントにより、記録されているデジタルデータであり、利用者が決済に利用する場合には、１単位１円相当でその数額が減少し、代わりに同額分だけ代金の支払を免れることができる。そうすると、ＰａｙＰａｙ残高は貨幣価値がデジタルデータとして対応するサーバ（ＰａｙＰａｙサーバ）に記録されているものであるといえる。しかし、各被告方法を用いた決済の場合には、利用者のＰａｙＰａｙ残高アカウントに記録されたＰａｙＰａｙ残高は決済額分だけ減算されるものの、決済の相手方である加盟店は、後に同額から支払手数料等を控除した残金（清算金）の支払を受け取ることとされており、加盟店のＰａｙＰａｙ残高アカウントに

記録されたＰａｙＰａｙ残高が代金額分だけ増加するという処理が行われることとはされていない。

加盟店に対しては、ＰａｙＰａｙ残高を用いた決済の合計額から決済手数料等を控除した残金が支払われるため、ＰａｙＰａｙサーバまたはその他の記録媒体では、当該加盟店に係る決済額またはその累計額を電磁的に記録していることが推認できる。しかし、前記のとおり、加盟店は同額に対応するＰａｙＰａｙ残高を取得するものとされていないのであるから、同累計額をもってＰａｙＰａｙ残高による決済が可能な他の加盟店との取引で利用することができるとは認められない。そうすると、各被告方法によって、利用者については、そのＰａｙＰａｙ残高の数額に係るデジタルデータは決済額分だけ減額されたものに置き換わるものの、加盟店については、仮に決済額分だけ何らかのデジタルデータ上の数額が増加したとしても、これはＰａｙＰａｙ残高とは別の価値、機能を有するものに係る数額であり、各被告方法により利用者に係る電子マネーの数額が減算された分だけ、加盟店に係る同一の価値・機能を有する電子マネーの数額が増加したと評価することはできない。

よって、原告が上記で主張する各被告方法においては、ＰａｙＰａｙ残高について、本件各発明にいう「電子マネーの送金」がされているとはいえず、他に、各被告方法が「電子マネーの送金」に当たると認めるに足りる証拠はない。

ウ　原告は、ＰａｙＰａｙシステムを用いた取引において、返金処理をした場合には、利用者のＰａｙＰａｙ残高がその分増加し、加盟店の清算金がその分減少すること、清算金の額が返金額に満たない場合には返金が実行できないことをも根拠に、各被告方法が「電子マネーの送金」に当たると主張する。

返金処理に基づく清算金の減額は、加盟店規約１２条２項に基づくものであると解される。そして、利用規約第３条４項によって、利用者にはＰａｙ

Ｐａｙ残高の加算によって返金がされ、これに対応して被告が加盟店に金銭債権を取得し、同金額が加盟店規約１２条２項に基づいて清算金が控除されるものと解される。ここで、前記のとおり、加盟店はＰａｙＰａｙ残高を用いた決済が実行されても、同代金に対応する金額分をもって、ＰａｙＰａｙ残高を用いた決済が可能な他の加盟店との間で決済が可能になるといったことはないのであるから、仮にＰａｙＰａｙ残高を用いた決済によって同決済に関係する何らかのデジタルデータ上の数額の増加があったとしても、それは、清算金請求債権または返金にのみ用いることができるものであり、利用者が保有していた電子マネー（ＰａｙＰａｙ残高）とは別の性質を有するのであるから、各被告方法による決済が前記で認定した本件各発明の「電子マネーの送金」に当たるとはいえない。

その他、原告は、一般的な電子マネーや電子マネー取引の意義、本件各発明の意義なども挙げて各被告方法が「電子マネーの送金方法」に当たることなどを主張する。しかし、本件各発明においては、前記⑴に述べたとおり、ＩＣチップを用いるなどした電子マネーが従来技術としてあったところ、それら従来技術とは異なるものとして、本件各発明の「電子マネーの送金方法」が定められている。その内容は前記⑴に述べたとおりのものであって、各被告方法がそれに該当しないことは前記イのとおりである。原告の主張は採用できない。

第４　結論

以上のとおりであって、各被告方法において、「電子マネーの送金」が行われているとは認められず、各被告方法が構成要件Ａ、Ｆを充足するとはいえないから、各被告方法が本件各発明の技術的範囲に属するとはいえない。よって、その余の争点について判断するまでもなく、原告の請求には理由がないから、主文のとおり判決する。

東京地方裁判所民事第４６部

裁判長裁判官　　柴　　田　　義　　明

裁判官　　佐　　伯　　良　　子

裁判官　　仲　　田　　憲　　史