(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6748667号
(P6748667)
(45)発行日　令和2年9月2日(2020.9.2)　(24)登録日　令和2年8月12日(2020.8.12)

(51)Int.Cl.　　F I
G06F 21/33 (2013.01)　G06F 21/33
G06Q 20/40 (2012.01)　G06Q 20/40
G06Q 20/38 (2012.01)　G06Q 20/38

請求項の数 10　(全 26 頁)

(21)出願番号　特願2018-52047(P2018-52047)
(22)出願日　平成30年3月20日(2018.3.20)
(65)公開番号　特開2019-164590(P2019-164590A)
(43)公開日　令和1年9月26日(2019.9.26)
審査請求日　平成30年12月18日(2018.12.18)

(73)特許権者　510247995
楽天銀行株式会社
東京都世田谷区玉川一丁目１４番１号
(74)代理人　110000154
特許業務法人はるか国際特許事務所
(72)発明者　井上　俊博
東京都世田谷区玉川一丁目１４番１号　楽天銀行株式会社内

審査官　松平　英

最終頁に続く

(54)【発明の名称】ＡＰＩ提供システム、認証サーバ、ＡＰＩ提供方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
仲介システムを介して複数のＡＰＩを提供するＡＰＩ提供システムであって、
ユーザ端末から前記仲介システムに第１のＡＰＩの利用要求が送信された場合に、当該利用要求に基づくリダイレクトを受けて、前記ユーザ端末との間で第１の認証を行う第１認証手段と、
前記第１の認証が成功した場合に、前記ユーザ端末にユーザ認証情報を発行し、前記仲介システムに、前記第１のＡＰＩを利用するための第１の認証情報を発行する第１発行手段と、
前記仲介システムから受信した前記第１の認証情報に基づいて、前記第１のＡＰＩを提供する第１提供手段と、
前記ユーザ端末から前記仲介システムに第２のＡＰＩの利用要求が送信された場合に、当該利用要求に基づくリダイレクトを受けて、前記ユーザ端末との間で、前記第１発行手段により発行された前記ユーザ認証情報に基づく第２の認証を行う第２認証手段と、
前記第２の認証が成功した場合に、前記仲介システムに、前記第２のＡＰＩを利用するための第２の認証情報を発行する第２発行手段と、
前記仲介システムから受信した前記第２の認証情報に基づいて、前記第２のＡＰＩを提供する第２提供手段と、
を含み、
前記第１認証手段は、前記第２の認証が失敗した場合に、前記ユーザ端末との間で再度

の前記第１の認証を行い、
前記第１発行手段は、前記再度の第１の認証が成功した場合に、前記ユーザ端末に新たなユーザ認証情報と、前記仲介システムに新たな前記第１の認証情報と、を発行し、
前記第１提供手段は、前記仲介システムから受信した前記新たな第１の認証情報に基づいて、前記第１のＡＰＩを提供し、
前記第２認証手段は、前記新たなユーザ認証情報に基づく再度の前記第２の認証を行う、
ことを特徴とするＡＰＩ提供システム。
【請求項２】
前記第１発行手段は、前記第１の認証情報に有効期限を設定し、
前記第１発行手段は、前記再度の第１の認証が成功した場合に、前記新たな第１の認証情報に新たな有効期限を設定する、
ことを特徴とする請求項１に記載のＡＰＩ提供システム。
【請求項３】
前記ＡＰＩ提供システムは、前記第２の認証が成功した場合に、前記ユーザ端末との間で第３の認証を行う第３認証手段を更に含み、
前記第２発行手段は、前記第２の認証が成功し、かつ、前記第３の認証が成功した場合に、前記第２の認証情報を発行する、
ことを特徴とする請求項１又は２に記載のＡＰＩ提供システム。
【請求項４】
前記第３認証手段は、前記第３の認証が行われる場合に、前記第２のＡＰＩの利用要求の内容を前記ユーザ端末に表示させる、
ことを特徴とする請求項３に記載のＡＰＩ提供システム。
【請求項５】
前記第１発行手段は、前記ユーザ認証情報に有効期限を設定し、
前記第２認証手段は、前記ユーザ認証情報に設定された有効期限に基づいて、前記第２の認証を行う、
ことを特徴とする請求項１～４の何れかに記載のＡＰＩ提供システム。
【請求項６】
前記第１発行手段は、前記第１の認証情報に有効期限を設定し、
前記第１提供手段は、前記第１の認証情報に設定された有効期限に基づいて、前記第１のＡＰＩを提供し、
前記第２発行手段は、前記第２の認証情報に、前記第１の認証情報よりも短い有効期限を設定し、
前記第２提供手段は、前記第２の認証情報に設定された、前記第１の認証情報よりも短い有効期限に基づいて、前記第２のＡＰＩを提供する、
ことを特徴とする請求項１～５の何れかに記載のＡＰＩ提供システム。
【請求項７】
前記第２発行手段は、前記第２の認証情報に基づく前記第２のＡＰＩの提供回数又は利用期間が所定回数又は所定期間未満となるように、前記第２の認証情報を発行する、
ことを特徴とする請求項１～６の何れかに記載のＡＰＩ提供システム。
【請求項８】
仲介システムを介して複数のＡＰＩを提供するための認証サーバであって、
ユーザ端末から前記仲介システムに第１のＡＰＩの利用要求が送信された場合に、当該利用要求に基づくリダイレクトを受けて、前記ユーザ端末との間で第１の認証を行う第１認証手段と、
前記第１の認証が成功した場合に、前記ユーザ端末にユーザ認証情報を発行し、前記仲介システムに、前記第１のＡＰＩを利用するための第１の認証情報を発行する第１発行手段と、
前記ユーザ端末から前記仲介システムに第２のＡＰＩの利用要求が送信された場合に、

当該利用要求に基づくリダイレクトを受けて、前記ユーザ端末との間で、前記ユーザ認証情報に基づく第２の認証を行う第２認証手段と、
前記第２の認証が成功した場合に、前記仲介システムに、前記第２のＡＰＩを利用するための第２の認証情報を発行する第２発行手段と、
を含み、
前記第１認証手段は、前記第２の認証が失敗した場合に、前記ユーザ端末との間で再度の前記第１の認証を行い、
前記第１発行手段は、前記再度の第１の認証が成功した場合に、前記ユーザ端末に新たなユーザ認証情報と、前記仲介システムに新たな前記第１の認証情報と、を発行し、
前記第２認証手段は、前記新たなユーザ認証情報に基づく再度の前記第２の認証を行う、
ことを特徴とする認証サーバ。
【請求項９】
仲介システムを介して複数のＡＰＩを提供するＡＰＩ提供方法であって、
ユーザ端末から前記仲介システムに第１のＡＰＩの利用要求が送信された場合に、当該利用要求に基づくリダイレクトを受けて、前記ユーザ端末との間で第１の認証を行う第１認証ステップと、
前記第１の認証が成功した場合に、前記ユーザ端末にユーザ認証情報を発行し、前記仲介システムに、前記第１のＡＰＩを利用するための第１の認証情報を発行する第１発行ステップと、
前記仲介システムから受信した前記第１の認証情報に基づいて、前記第１のＡＰＩを提供する第１提供ステップと、
前記ユーザ端末から前記仲介システムに第２のＡＰＩの利用要求が送信された場合に、当該利用要求に基づくリダイレクトを受けて、前記ユーザ端末との間で、前記ユーザ認証情報に基づく第２の認証を行う第２認証ステップと、
前記第２の認証が成功した場合に、前記仲介システムに、前記第２のＡＰＩを利用するための第２の認証情報を発行する第２発行ステップと、
前記仲介システムから受信した前記第２の認証情報に基づいて、前記第２のＡＰＩを提供する第２提供ステップと、
を含み、
前記第１認証ステップは、前記第２の認証が失敗した場合に、前記ユーザ端末との間で再度の前記第１の認証を行い、
前記第１発行ステップは、前記再度の第１の認証が成功した場合に、前記ユーザ端末に新たなユーザ認証情報と、前記仲介システムに新たな前記第１の認証情報と、を発行し、
前記第１提供ステップは、前記仲介システムから受信した前記新たな第１の認証情報に基づいて、前記第１のＡＰＩを提供し、
前記第２認証ステップは、前記新たなユーザ認証情報に基づく再度の前記第２の認証を行う、
ことを特徴とするＡＰＩ提供方法。
【請求項１０】
ユーザ端末から仲介システムに第１のＡＰＩの利用要求が送信された場合に、当該利用要求に基づくリダイレクトを受けて、前記ユーザ端末との間で第１の認証を行う第１認証手段、
前記第１の認証が成功した場合に、前記ユーザ端末にユーザ認証情報を発行し、前記仲介システムに、前記第１のＡＰＩを利用するための第１の認証情報を発行する第１発行手段、
前記ユーザ端末から前記仲介システムに第２のＡＰＩの利用要求が送信された場合に、当該利用要求に基づくリダイレクトを受けて、前記ユーザ端末との間で、前記ユーザ認証情報に基づく第２の認証を行う第２認証手段、
前記第２の認証が成功した場合に、前記仲介システムに、前記第２のＡＰＩを利用する

ための第２の認証情報を発行する第２発行手段、
としてコンピュータを機能させ、
前記第１認証手段は、前記第２の認証が失敗した場合に、前記ユーザ端末との間で再度の前記第１の認証を行い、
前記第１発行手段は、前記再度の第１の認証が成功した場合に、前記ユーザ端末に新たなユーザ認証情報と、前記仲介システムに新たな前記第１の認証情報と、を発行し、
前記第２認証手段は、前記新たなユーザ認証情報に基づく再度の前記第２の認証を行う、
プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ＡＰＩ提供システム、認証サーバ、ＡＰＩ提供方法、及びプログラムに関する。

【背景技術】

【０００２】

従来、ＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍｍｉｎｇ　Ｉｎｔｅｒｆａｃｅ）を利用して各種サービスを提供する技術が知られている。例えば、特許文献１には、認証装置と、ＡＰＩを利用したサービスを提供するサービス提供装置と、サービスの提供を仲介するサービス仲介装置と、を含むシステムにおいて、認証装置によるユーザの認証が成功した場合に、サービスを利用するためのトークンを発行し、サービス仲介装置に送信することが記載されている。サービス仲介装置は、サービス提供装置に認証情報を送信し、サービス提供装置からのサービスの仲介を行う。

【０００３】

また例えば、特許文献２には、電子商取引システムを通じて銀行システム内のＡＰＩを利用する場合に、銀行システムが電子商取引システムに対してトークンを発行し、電子商取引システムが保有するトークンを利用してＡＰＩを提供するシステムが記載されている。このシステムでは、トークン発行時の認証だけでなく、決済の際に電子商取引システムで暗証番号を入力させることによって、二段階の認証が行われる。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特許特５４５８８８８号公報
【特許文献２】特許特６２５５０７０号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

上記のような技術では、ＡＰＩの利用を仲介する仲介システムに認証情報が管理されるため、仲介システムは、悪意のある第三者の攻撃対象になりがちである。この点、複数のＡＰＩを提供する場合に、これら複数のＡＰＩで共通のトークンを発行したとすると、第三者にトークンが漏えいすると全てのＡＰＩが悪用される可能性があり、セキュリティ性を高めることはできない。

【０００６】

本発明の目的は、仲介システムを介して複数のＡＰＩを提供する場合のセキュリティを高めることが可能なＡＰＩ提供システム、認証サーバ、ＡＰＩ提供方法、及びプログラムを提供することである。

【課題を解決するための手段】

【０００７】

上記課題を解決するために、本発明に係るＡＰＩ提供システムは、仲介システムを介して複数のＡＰＩを提供するＡＰＩ提供システムであって、ユーザ端末から前記仲介システ

ムに第１のＡＰＩの利用要求が送信された場合に、当該利用要求に基づくリダイレクトを受けて、前記ユーザ端末との間で第１の認証を行う第１認証手段と、前記第１の認証が成功した場合に、前記ユーザ端末にユーザ認証情報を発行し、前記仲介システムに、前記第１のＡＰＩを利用するための第１の認証情報を発行する第１発行手段と、前記仲介システムから受信した前記第１の認証情報に基づいて、前記第１のＡＰＩを提供する第１提供手段と、前記ユーザ端末から前記仲介システムに第２のＡＰＩの利用要求が送信された場合に、当該利用要求に基づくリダイレクトを受けて、前記ユーザ端末との間で、前記第１発行手段により発行された前記ユーザ認証情報に基づく第２の認証を行う第２認証手段と、前記第２の認証が成功した場合に、前記仲介システムに、前記第２のＡＰＩを利用するための第２の認証情報を発行する第２発行手段と、前記仲介システムから受信した前記第２の認証情報に基づいて、前記第２のＡＰＩを提供する第２提供手段と、を含むことを特徴とする。

【図面の簡単な説明】

【０００８】

【図１】実施形態に係るＡＰＩ提供システムの一例を示す図である。

【図２】ユーザが仲介システム２のサービスを利用する様子を示す画面遷移図である。

【図３】更新系ＡＰＩが利用される場合の画面遷移図である。

【図４】本実施形態において実現される機能を示す機能ブロック図である。

【図５】ユーザデータベースの一例を示す図である。

【図６】口座データベースの一例を示す図である。

【図７】本実施形態において実行される処理のフロー図である。

【図８】本実施形態において実行される処理のフロー図である。

【図９】本実施形態において実行される処理のフロー図である。

【図１０】本実施形態において実行される処理のフロー図である。

【発明を実施するための形態】

【０００９】

［１．ＡＰＩ提供システムの全体構成］

以下、本発明に係る実施形態の例について図面に基づき詳細に説明する。図１は、実施形態に係るＡＰＩ提供システムの一例を示す図である。図１に示すように、例えば、ＡＰＩ提供システム１は、インターネットなどのネットワークＮを介し、仲介システム２及びユーザ端末３０の各々とデータ送受信可能である。

【００１０】

ＡＰＩ提供システム１は、複数のＡＰＩを提供するシステムであり、少なくとも１つのコンピュータを含む。各ＡＰＩは、仲介システム２に公開されている。このため、ＡＰＩ提供システム１と仲介システム２とは連携可能であり、各ＡＰＩに係る機能は、仲介システム２を介してユーザに間接的に提供される。ＡＰＩの機能としては、任意の内容であってよく、例えば、金融サービス、電子商取引、保険サービス、旅行予約サービス、又はＳＮＳ（Ｓｏｃｉａｌ　Ｎｅｔｗｏｒｋｉｎｇ　Ｓｅｒｖｉｃｅ）に係る機能がＡＰＩを利用してユーザに提供されるようにしてもよい。

【００１１】

本実施形態では、金融機関がＡＰＩ提供システム１を管理し、ＡＰＩを利用して金融サービスを提供する場合を一例として説明する。金融機関は、金融取引に関する業務を営む組織であり、例えば、銀行や信用金庫といった預貯金取扱金融機関だけでなく、証券会社であってもよい。本実施形態では、金融機関が銀行であり、ユーザは、銀行の口座を開設済みであるものとする。なお、ユーザは、法人であってもよいし、個人（個人事業主を含む）であってもよい。

【００１２】

例えば、ＡＰＩ提供システム１は、サーバコンピュータであるＡＰＩ提供サーバ１０を含む。ＡＰＩ提供サーバ１０は、制御部１１、記憶部１２、及び通信部１３を含む。制御部１１は、例えば、少なくとも１つのマイクロプロセッサを含む。記憶部１２は、例えば

、ＲＡＭ等の主記憶部やハードディスク等の補助記憶部を含む。制御部１１は、記憶部１２に記憶されたプログラムやデータに従って処理を実行する。通信部１３は、有線通信又は無線通信用の通信インタフェースを含む。通信部１３は、インターネットやＬＡＮなどのネットワークを介して外部機器とのデータ送受信が可能である。

【００１３】

仲介システム２は、ＡＰＩ提供システム１と連携するシステムであり、少なくとも１つのコンピュータを含む。例えば、仲介システム２は、ＡＰＩ提供システム１が公開するＡＰＩを利用し、ユーザの業務を支援するサービスを提供する。本実施形態では、ＡＰＩを利用して金融サービスが提供される場合を説明するので、仲介システム２は、経費精算や給与振込などの会計業務を支援するシステム（例えば、いわゆるクラウド会計システム）である場合を一例として説明する。

【００１４】

例えば、仲介システム２は、サーバコンピュータである仲介サーバ２０を含む。仲介サーバ２０は、制御部２１、記憶部２２、及び通信部２３を含む。制御部２１、記憶部２２、及び通信部２３のハードウェア構成は、それぞれ制御部１１、記憶部１２、及び通信部１３と同様であってよい。

【００１５】

ユーザ端末３０は、ユーザが操作するコンピュータであり、例えば、パーソナルコンピュータ、携帯電話（スマートフォンを含む）、又は携帯情報端末（タブレット型端末を含む）である。ユーザ端末３０は、制御部３１、記憶部３２、通信部３３、操作部３４、及び表示部３５を含む。制御部３１、記憶部３２、及び通信部３３のハードウェア構成は、それぞれ制御部１１、記憶部１２、及び通信部１３と同様であってよい。操作部３４は、入力デバイスであり、例えば、タッチパネルやマウスなどのポインティングデバイス又はキーボードである。表示部３５は、例えば、液晶ディスプレイ又は有機ＥＬディスプレイである。

【００１６】

なお、記憶部１２，２２，３２に記憶されるものとして説明するプログラムやデータは、コンピュータ読み取り可能な情報記憶媒体（例えば、ＵＳＢメモリ又はＳＤカード）に記憶されたものが各コンピュータに供給されるようにしてもよいし、ネットワークを介して各コンピュータに供給されるようにしてもよい。また、上記説明した各コンピュータのハードウェア構成は、上記の例に限られず、例えば、情報記憶媒体を読み取る読取部（例えば、ＳＤカードスロット）、又は、外部機器と直接的に通信するための入出力部（例えば、ＵＳＢ端子）が備えられていてもよい。

【００１７】

［２．ＡＰＩ提供システムが実行する処理の概要］

ＡＰＩ提供システム１は、仲介システム２を介して複数のＡＰＩを提供する。ここでは、ＡＰＩの一例として、口座情報を参照するためのＡＰＩ（以降、参照系ＡＰＩと記載する。）と、口座情報を更新するためのＡＰＩ（以降、更新系ＡＰＩと記載する。）と、を説明する。なお、ＡＰＩ提供システム１が提供するＡＰＩは３つ以上であってもよい。

【００１８】

参照系ＡＰＩは、口座情報を参照する機能が関連付けられている。例えば、ユーザが、仲介システム２のサービスを利用して、入出金明細や口座残高を参照する場合に、参照系ＡＰＩが利用される。更新系ＡＰＩは、口座情報を更新する機能が関連付けられている。例えば、ユーザが、仲介システム２のサービスを利用して、振込、入金、又は出金をする場合に、更新系ＡＰＩが利用される。

【００１９】

図２は、ユーザが仲介システム２のサービスを利用する様子を示す画面遷移図である。図２に示すように、ユーザがユーザ端末３０を操作して仲介システム２にアクセスすると、仲介システム２のログイン画面Ｇ１が表示部３５に表示される。仲介システム２のユーザアカウントとパスワードがログイン画面Ｇ１から入力され、仲介システム２において正

当性が確認されると、ユーザは仲介システム２にログインする。

【００２０】

ユーザが仲介システム２にログインすると、仲介システム２が提供する種々のサービスを利用するためのメニュー画面Ｇ２が表示部３５に表示される。例えば、ユーザは、メニュー画面Ｇ２から、経費申請、経費承認、入出金明細照会、経費や給与などの振込処理、残高照会、及び入出金処理といったサービスを利用することができる。例えば、ユーザが、メニュー画面Ｇ２から入出金明細参照の項目を選択すると、ＡＰＩ提供システム１に移動する旨のメッセージが表示され、ユーザが同意すると、ＡＰＩ提供システム１へのリダイレクトが実行される。

【００２１】

リダイレクトが実行されると、ＡＰＩ提供システム１のログイン画面Ｇ３が表示部３５に表示される。ＡＰＩ提供システム１のユーザアカウントとパスワードがログイン画面Ｇ３から入力され、ユーザの正当性が確認されると、例えば、ＡＰＩ提供システム１は、Ｃｏｏｋｉｅを発行してユーザ端末３０に送信し、ＯＡｕｔｈ２．０に基づくトークンを発行して仲介システム２に送信する。

【００２２】

Ｃｏｏｋｉｅは、ウェブブラウザで用いられるユーザの識別情報である。本実施形態では、参照系ＡＰＩを利用するための認証でＣｏｏｋｉｅが発行されるので、Ｃｏｏｋｉｅは、当該認証を受けたユーザであることを証明する情報ということもできる。Ｃｏｏｋｉｅは、仲介システム２ではなく、ユーザ端末３０に保持される。

【００２３】

ＯＡｕｔｈ２．０は、認証プロトコルの一種であり、例えば、管理主体の異なる複数のシステム間で連携する場合に利用される。トークンは、ＡＰＩの利用が認可されたことを証明する情報である。本実施形態では、ユーザは仲介システム２を介してＡＰＩを間接的に利用するので、仲介システム２が、ユーザの代わりにＡＰＩに対してリクエストを送信するために、トークンが用いられる。このため、トークンは、ユーザ端末３０ではなく、仲介システム２に保持される。

【００２４】

本実施形態では、複数のＡＰＩで共通のトークンが用いられるのでなく、ＡＰＩごとに異なるトークンが発行される。以降、参照系ＡＰＩで使用されるトークンを参照系トークンと記載し、更新系ＡＰＩで使用されるトークンを更新系トークンと記載する。図２の例では、参照系ＡＰＩが利用されるので、参照系トークンが発行されることになる。

【００２５】

仲介システム２は、ＡＰＩ提供システム１から受信した参照系トークンを利用し、参照系ＡＰＩにリクエストを送信する。ＡＰＩ提供システム１は、仲介システム２から受信した参照系トークンの正当性を確認すると、参照系ＡＰＩの応答として、ユーザの入出金明細を取得して仲介システム２に送信する。仲介システム２は、受信した入出金明細に基づいて、ユーザ端末３０に入出金明細画面Ｇ４を表示させる。

【００２６】

図３は、更新系ＡＰＩが利用される場合の画面遷移図である。図３に示すように、ユーザが、メニュー画面Ｇ２から振込処理の項目を選択すると、振込内容を入力するための振込内容入力画面Ｇ５が表示部３５に表示される。ユーザが振込内容入力画面Ｇ５から振込先や振込金額等を入力して所定の振込指示をすると、ＡＰＩ提供システム１に移動する旨のメッセージが表示され、ユーザが同意すると、ＡＰＩ提供システム１へのリダイレクトが実行される。

【００２７】

リダイレクトが実行されると、ユーザ端末３０に記憶されていたＣｏｏｋｉｅ（参照系ＡＰＩの利用時に発行されたＣｏｏｋｉｅ）がＡＰＩ提供システム１に送信される。ＡＰＩ提供システム１は、受信したＣｏｏｋｉｅの正当性を確認すると、口座の暗証番号を入力するための暗証番号入力画面Ｇ６をユーザ端末３０に表示させる。ユーザが、口座（こ

こでは、ユーザが勤務する会社の口座）の暗証番号を入力し、正当性が確認されると、ＡＰＩ提供システム１は、更新系トークンを発行し、仲介システム２に送信する。

【００２８】

仲介システム２は、ＡＰＩ提供システム１から受信した更新系トークンを利用し、更新系ＡＰＩにリクエストを送信する。ＡＰＩ提供システム１は、仲介システム２から受信した更新系トークンの正当性を確認すると、更新系ＡＰＩの応答として、振込処理を実行して実行結果を仲介システム２に送信する。仲介システム２は、受信した振込の実行結果に基づいて、ユーザ端末３０に振込完了画面Ｇ７を表示させる。

【００２９】

以上のように、本実施形態のＡＰＩ提供システム１は、参照系ＡＰＩの利用時にＣｏｏｋｉｅを発行してユーザ端末３０に送信し、更新系ＡＰＩの利用要求（詳細後述）が送信された場合に、ユーザが有効なＣｏｏｋｉｅを保有するか否かを確認する。ＡＰＩ提供システム１は、Ｃｏｏｋｉｅの正当性を確認したうえで暗証番号を入力させることで、参照系ＡＰＩを利用するユーザと、更新系ＡＰＩを利用するユーザと、の同一性を確認し、セキュリティを高めるようにしている。以降、ＡＰＩ提供システム１の構成の詳細について説明する。

【００３０】

［３．本実施形態において実現される機能］

図４は、本実施形態において実現される機能を示す機能ブロック図である。図４に示すように、ここでは、主にＡＰＩ提供システム１で実現される機能を説明する。例えば、ＡＰＩ提供システム１では、参照系ＡＰＩ１００、更新系ＡＰＩ１０１、データ記憶部１０２、第１認証部１０３、第１発行部１０４、第１提供部１０５、第２認証部１０６、第３認証部１０７、第２発行部１０８、及び第２提供部１０９が実現される。データ記憶部１０２は記憶部１２を主として実現され、他の各機能は制御部１１を主として実現される。

【００３１】

［参照系ＡＰＩ］

参照系ＡＰＩ１００は、本発明に係る第１のＡＰＩの一例である。このため、本実施形態で参照系ＡＰＩ１００と記載した箇所は、第１のＡＰＩと読み替えることができる。第１のＡＰＩは、ＡＰＩ提供システム１が提供する複数のＡＰＩのうちの何れかであればよく、参照系ＡＰＩ１００及び更新系ＡＰＩ１０１以外の他のＡＰＩ（例えば、ユーザの基本情報を参照するためのＡＰＩや住所などの登録情報を変更するためのＡＰＩなど）を提供する場合には、当該他のＡＰＩが第１のＡＰＩに相当してもよい。先述したように、参照系ＡＰＩ１００は、口座情報を参照する機能が関連付けられており、本実施形態では、後述する口座データベースを参照する。

【００３２】

［更新系ＡＰＩ］

更新系ＡＰＩ１０１は、本発明に係る第２のＡＰＩの一例である。このため、本実施形態で更新系ＡＰＩ１０１と記載した箇所は、第２のＡＰＩと読み替えることができる。第２のＡＰＩは、ＡＰＩ提供システム１が提供する複数のＡＰＩのうち、第１のＡＰＩとは異なるＡＰＩであればよい。本実施形態では、セキュリティレベルが互いに異なる複数のＡＰＩが存在し、第２のＡＰＩは、第１のＡＰＩよりもセキュリティレベルが高いものとする。このため、第２のＡＰＩは、第１のＡＰＩよりも複雑な認証が必要であり、本実施形態では、第２のＡＰＩは、第１のＡＰＩよりも利用時に必要な認証回数が多いものとする。先述したように、更新系ＡＰＩ１０１は、口座情報を更新する機能が関連付けられており、本実施形態では、後述する口座データベースを更新する。

【００３３】

［データ記憶部］

データ記憶部１０２は、ＡＰＩを提供するために必要なデータを記憶する。ここでは、データ記憶部１０２が記憶するデータの一例として、ユーザに関する各種情報を格納するためのユーザデータベースと、口座に関する各種情報を格納するための口座データベース

と、を説明する。

【００３４】

図５は、ユーザデータベースの一例を示す図である。図５に示すように、ユーザデータベースには、ユーザアカウント、ユーザ名、パスワード、Ｃｏｏｋｉｅ、参照系トークン、更新系トークン、及び口座識別情報が格納される。ユーザデータベースに格納されるユーザアカウントとパスワードは、ＡＰＩ提供システム１にログインするための認証情報である。ユーザアカウントは、ユーザがＡＰＩ提供システム１に利用登録した際に発行され、パスワードは、利用登録後に任意のものを設定可能である。

【００３５】

Ｃｏｏｋｉｅは、参照系トークン発行時に生成されたＣｏｏｋｉｅである。参照系トークンが発行されていないユーザについては、ユーザデータベースにＣｏｏｋｉｅは格納されない。Ｃｏｏｋｉｅは、特に有効期限が存在しなくてもよいが、本実施形態では、Ｃｏｏｋｉｅは、有効期限が設定されている。有効期限を示す情報は、Ｃｏｏｋｉｅの内部に組み込まれていてもよいし、Ｃｏｏｋｉｅとは別の情報として管理されていてもよい。

【００３６】

参照系トークンは、参照系ＡＰＩ１００の利用が認可されたことを証明する情報である。参照系トークンは、本発明に係る第１の認証情報に相当する。このため、本実施形態で参照系トークンと記載した箇所は、第１の認証情報と読み替えることができる。参照系トークンは、公知の認証プロトコルを利用して発行されるようにすればよく、本実施形態では、ＯＡｕｔｈ２．０を利用する場合を説明する。

【００３７】

例えば、参照系トークンは、アクセストークンと、リフレッシュトークンと、を含む。アクセストークンとリフレッシュトークンとは、それぞれ有効期限が設定されており、リフレッシュトークンの有効期限は、アクセストークンの有効期限よりも長い。通常のリクエストでは、リフレッシュトークンは送信されずアクセストークンだけが送信され、リフレッシュトークンは、アクセストークンを再発行する場合に送信される。

【００３８】

更新系トークンは、更新系ＡＰＩ１００の利用が認可されたことを証明する情報である。更新系トークンは、本発明に係る第２の認証情報に相当する。このため、本実施形態で更新系トークンと記載した箇所は、第２の認証情報と読み替えることができる。更新系トークンは、公知のプロトコルを利用して発行されるようにすればよく、本実施形態では、ＯＡｕｔｈ２．０を利用する場合を説明する。

【００３９】

更新系トークンは、参照系トークンと同様、アクセストークンとリフレッシュトークンとを含んでもよいが、本実施形態では、アクセストークンだけが発行されるものとする。詳細は後述するが、更新系トークンの有効期限は、参照系トークンの有効期限よりも短く、ワンタイム化されているものとする。なお、口座識別情報は、口座を識別するための情報であればよく、例えば、支店名、口座番号、及び口座名義人である。

【００４０】

図６は、口座データベースの一例を示す図である。図６に示すように、口座データベースには、銀行の支店名、口座を識別する口座番号、口座名義人、残高情報、暗証番号、及び入出金明細情報が格納される。暗証番号は、口座の暗証番号であり、口座開設時等に指定された暗証番号である。入出金明細情報は、口座の入出金の履歴を示す情報であり、例えば、日付、入出金額、及び入出金者といった情報が格納される。例えば、口座データベースに格納された各情報は、参照系ＡＰＩ１００によって参照される。また例えば、口座データベースに格納された残高情報及び入出金明細情報は、更新系ＡＰＩ１０１によって更新される。

【００４１】

［第１認証部］

第１認証部１０３は、ユーザ端末３０から仲介システム２に参照系ＡＰＩ１００の利用

要求が送信された場合に、当該利用要求に基づくリダイレクトを受けて、ユーザ端末３０との間でログイン認証を行う。

【００４２】

利用要求は、利用対象となるＡＰＩを識別するための情報を含み、所定形式のデータが送信されることで利用要求が行われるようにすればよい。利用要求は、ユーザ端末３０から仲介システム２に対してなされる要求のうち、ＡＰＩ提供システム１が提供するＡＰＩの利用が必要なもの（又は、ＡＰＩの利用を予定しているもの）である。本実施形態では、参照系ＡＰＩ１００又は更新系ＡＰＩ１０１の何れかが利用されるので、利用要求には、これらの何れを利用するかを識別するための情報（例えば、メニュー画面Ｇ２のどの項目が選択されたかを示す情報等）が含まれているものとする。

【００４３】

なお、ユーザ端末３０から受信する要求の中には、ＡＰＩ提供システム１が提供するＡＰＩを利用しないもの（例えば、メニュー画面Ｇ２における経費申請等）もあるので、仲介システム２は、ＡＰＩ提供システム１が提供するＡＰＩを利用する要求がどれであるかを特定可能となっている。例えば、仲介システム２は、メニュー画面Ｇ２の入出金明細照会の項目が選択された旨の通知を受信した場合には、参照系ＡＰＩの利用要求であると判定し、メニュー画面Ｇ２の振込処理の項目が選択された旨の通知を受信した場合には、更新系ＡＰＩの利用要求であると判定する。

【００４４】

参照系ＡＰＩ１００の利用要求は、ユーザが操作部３４から所定の操作を行った場合に、ユーザ端末３０から仲介システム２に送信される。本実施形態では、メニュー画面Ｇ２において入出金明細参照の項目を選択する操作を一例として説明するので、ユーザ端末３０から仲介システム２に対し、入出金明細参照の項目が選択された旨の通知が送信されることが、参照系ＡＰＩ１００の利用要求が送信されることに相当する。仲介システム２において、当該通知が受信された場合に、参照系ＡＰＩ１００にリクエストを送信するようになっている。なお、入出金明細参照以外にも、残高照会の項目をするための操作が行われた場合に、参照系ＡＰＩ１００の利用要求が送信されてもよい。

【００４５】

なお、リダイレクトは、公知の方法で実行されるようにすればよく、仲介システム２側で実行されてもよいし、ユーザ端末３０側で実行されてもよい。例えば、Ａｐａｃｈｅで．ｈｔａｃｃｅｓｓファイルに所定のルールを記載しておくことによって、仲介システム２側でリダイレクトが実行されてもよいし、ＪａｖａＳｃｒｉｐｔ（登録商標）を利用してユーザ端末３０側でリダイレクトが実行されてもよい。

【００４６】

ログイン認証は、本発明に係る第１の認証の一例である。このため、本実施形態でログイン認証と記載した箇所は、第１の認証と読み替えることができる。第１の認証は、ＡＰＩ提供システム１とユーザ端末３０との間で行われる認証であればよい。本実施形態のように、ログイン画面Ｇ３から入力されたユーザアカウントとパスワードを利用したログイン認証以外にも、第１の認証は、種々の認証方法を利用可能である。例えば、顔認証や指紋認証などの生体認証であってもよいし、物理トークンや携帯機器ＰＩＮを利用した認証であってもよい。他にも例えば、ＩＣカードを利用した認証であってもよいし、二次元コード等のコード情報を利用した認証であってもよい。

【００４７】

例えば、第１認証部１０３は、ユーザ端末３０から受信した認証情報（ユーザが入力した認証情報）と、ユーザデータベースに格納された認証情報と、に基づいて、ログイン認証を実行する。本実施形態のように、ユーザアカウントとパスワードの組み合わせを利用する場合には、第１認証部１０３は、ユーザ端末３０から受信したユーザアカウントとパスワードの組み合わせと、ユーザデータベースに格納されたユーザアカウントとパスワードの組み合わせと、が一致するか否かを判定する。第１認証部１０３は、これらが一致する場合には認証成功と判定し、これらが一致しない場合には認証失敗と判定する。なお、

認証成功と判定されるためには、必ずしも認証情報が一致しなければならないわけではなく、例えば、生体認証を利用する場合には、顔認証又は指紋認証における画像の一致度が１００％でなくても、閾値以上であれば認証成功と判定してもよい。

【００４８】

［第１発行部］

第１発行部１０４は、ログイン認証が成功した場合に、ユーザ端末３０にＣｏｏｋｉｅを発行し、仲介システム２に、参照系ＡＰＩ１００を利用するための参照系トークンを発行する。

【００４９】

Ｃｏｏｋｉｅは、本発明に係るユーザ認証情報の一例である。このため、本実施形態でＣｏｏｋｉｅと記載した箇所は、ユーザ認証情報と読み替えることができる。ユーザ認証情報は、第１の認証が成功したユーザ（又はユーザ端末３０）を識別する情報である。本実施形態では、参照系ＡＰＩ１００を利用する場合のログイン認証が第１の認証に相当するので、Ｃｏｏｋｉｅは、当該ログイン認証が成功したユーザを識別する情報といえる。なお、ユーザ認証情報は、Ｃｏｏｋｉｅに限られず、例えば、電子証明書、暗号キー、又はパスコードといった情報であってもよい。

【００５０】

なお、ユーザ認証情報の発行方法自体は、公知の種々の手法を適用可能であり、ユーザ認証情報の内容に応じたアルゴリズムを用意しておき、第１発行部１０４は、当該アルゴリズムに基づいて、ユーザ認証情報を発行すればよい。本実施形態のように、Ｃｏｏｋｉｅをユーザ認証情報として利用する場合には、例えば、第１発行部１０４は、ＰＨＰ（Ｈｙｐｅｒｔｅｘｔ　Ｐｒｅｐｒｏｃｅｓｓｏｒ）におけるｓｅｔｃｏｏｋｉｅ関数に基づいて、Ｃｏｏｋｉｅを発行してもよい。

【００５１】

例えば、Ｃｏｏｋｉｅには、特に有効期限が設定されていなくてもよいが、本実施形態では、第１発行部１０４は、Ｃｏｏｋｉｅに有効期限を設定する。Ｃｏｏｋｉｅの有効期限は、任意の長さであればよく、例えば、１０分～１時間程度であってもよいし、それ以下又はそれ以上であってもよい。Ｃｏｏｋｉｅの有効期限は、ユーザ端末３０がＡＰＩ提供システム１にアクセスした場合に延長されるようにしてもよい。

【００５２】

参照系トークンは、本発明に係る第１の認証情報の一例である。このため、本実施形態で参照系トークンと記載した箇所は、第１の認証情報と読み替えることができる。第１の認証情報は、第１のＡＰＩの利用が認証されたユーザを識別する情報である。なお、第１の認証情報は、トークンに限られず、例えば、電子証明書、暗号キー、又はパスコードといった情報であってもよい。ただし、第１の認証情報は、ユーザ認証情報とは異なる情報であるものとする。第１の認証情報の発行方法自体は、公知の種々の手法を適用可能であり、第１の認証情報の内容に応じたアルゴリズムを用意しておき、第１発行部１０４は、当該アルゴリズムに基づいて、第１の認証情報を発行すればよい。本実施形態のように、トークンを第１の認証情報として利用する場合には、例えば、ＯＡｕｔｈ２．０で実装されているトークン生成方法を利用すればよい。

【００５３】

例えば、参照系トークンには、特に有効期限が設定されていなくてもよいが、本実施形態では、第１発行部１０４は、参照系トークンに有効期限を設定する。参照系トークンの有効期限は、任意の長さであればよく、例えば、参照系トークンのアクセストークン（以降、単に参照系アクセストークンと記載する。）については１０分～１時間程度とし、参照系トークンのリフレッシュトークン（以降、単に参照系リフレッシュトークンと記載する。）については、数時間程度としてもよい。

【００５４】

なお、本実施形態では、Ｃｏｏｋｉｅの有効期限と、参照系アクセストークンの有効期限と、を同じ長さにして、参照系アクセストークンの有効期限が切れた場合に、Ｃｏｏｋ

ｉｅも無効とする場合を説明するが、これらの長さは異なってもよい。例えば、Ｃｏｏｋｉｅの有効期限を参照系アクセストークンの有効期限よりも短く設定することで、後述するＣｏｏｋｉｅ認証のセキュリティレベルを上げるようにしてもよい。

【００５５】

［第１提供部］

第１提供部１０５は、仲介システム２から受信した参照系トークンに基づいて、参照系ＡＰＩ１００を提供する。例えば、第１提供部１０５は、仲介システム２から参照系トークンを受信し、当該参照系トークンの正当性を確認する。第１提供部１０５は、仲介システム２から受信した参照系トークンと、ユーザデータベースに格納された参照系トークンと、が一致するか否かを判定する。第１提供部１０５は、これらが一致しない場合には、参照系ＡＰＩ１００を提供せず、これらが一致する場合に、参照系ＡＰＩ１００を提供する。

【００５６】

なお、ＡＰＩを提供するとは、ＡＰＩが有する機能を提供することであり、ＡＰＩに関連付けられたプログラムを実行して処理結果を返すことを意味する。参照系ＡＰＩ１００であれば、口座データベースを参照する機能が関連付けられているので、第１提供部１０５は、口座データベースに格納された支店名、口座番号、口座残高、及び入出金明細情報の少なくとも１つを送信することによって、参照系ＡＰＩ１００を提供する。例えば、第１提供部１０５は、入出金明細情報を送信することによって、入出金明細を参照させ、口座残高の数値を送信することによって、口座残高を参照させる。

【００５７】

本実施形態では、参照系トークンに有効期限が設定されているので、第１提供部１０５は、参照系トークンに設定された有効期限に基づいて、参照系ＡＰＩ１００を提供する。第１提供部１０５は、リアルタイムクロック等を利用して現在日時を取得し、参照系トークンに設定された有効期限が経過しているか否かを判定する。本実施形態では、第１提供部１０５は、参照系アクセストークンに設定された有効期限が経過しているか否かを判定することになる。第１提供部１０５は、有効期限が経過していると判定した場合は参照系ＡＰＩ１００を提供せず、有効期限が経過していないと判定された場合は参照系ＡＰＩ１００を提供する。

【００５８】

［第２認証部］

第２認証部１０６は、ユーザ端末３０から仲介システム２に更新系ＡＰＩ１０１の利用要求が送信された場合に、当該利用要求に基づくリダイレクトを受けて、ユーザ端末３０との間で、第１発行部１０４により発行されたＣｏｏｋｉｅに基づくＣｏｏｋｉｅ認証を行う。なお、リダイレクト処理自体は、参照系ＡＰＩの利用要求が送信された場合と同様の処理で実行されてよい。

【００５９】

更新系ＡＰＩ１０１の利用要求は、ユーザが操作部３４から所定の操作を行った場合に、ユーザ端末３０から仲介システム２に送信される。本実施形態では、メニュー画面Ｇ２において振込処理が選択され、その後に振込内容入力画面Ｇ５から振込内容を入力する操作を一例として説明するが、利用要求は、予め定められた操作が行われた場合に送信されるようにすればよく、例えば、経費申請を承認する操作であってもよい。

【００６０】

Ｃｏｏｋｉｅ認証は、本発明に係る第２の認証の一例である。このため、本実施形態でＣｏｏｋｉｅ認証と記載した箇所は、第２の認証と読み替えることができる。第２の認証は、第１の認証を実行したユーザとの同一性を確認するための認証であり、第２の認証は、第１の認証が成功した際にユーザ端末３０に送信されたユーザ認証情報を利用して行われる。本実施形態では、Ｃｏｏｋｉｅがユーザ認証情報に相当する場合を説明するので、Ｃｏｏｋｉｅ認証を例に挙げるが、ユーザ認証情報が電子証明書、暗号キー、又はパスコードであれば、これらの正当性を確認することが第２の認証であってもよい。即ち、第２

の認証は、第１の認証が成功したユーザしか知りえない（第１の認証が成功したユーザのユーザ端末３０でしか記憶しえない）情報の有無を確認するための認証といえる。

【００６１】

例えば、第２認証部１０６は、ユーザ端末３０に対してＣｏｏｋｉｅを要求し、ユーザ端末３０から受信したＣｏｏｋｉｅと、ユーザデータベースに格納されたＣｏｏｋｉｅと、に基づいて、Ｃｏｏｋｉｅ認証を実行する。第２認証部１０６は、これらが一致するか否かを判定する。第２認証部１０６は、これらが一致する場合には認証成功と判定し、これらが一致しない場合には認証失敗と判定する。別の言い方をすれば、第２認証部１０６は、ユーザ端末３０から受信したＣｏｏｋｉｅがユーザデータベースに存在するか否かを判定する。第２認証部１０６は、ユーザ端末３０から受信したＣｏｏｋｉｅがユーザデータベースに存在する場合には認証成功と判定し、存在しない場合には認証失敗と判定する。

【００６２】

本実施形態では、Ｃｏｏｋｉｅに有効期限が設定されているので、第２認証部１０６は、Ｃｏｏｋｉｅに設定された有効期限に基づいて、Ｃｏｏｋｉｅ認証を行う。第２認証部１０６は、リアルタイムクロック等を利用して現在日時を取得し、Ｃｏｏｋｉｅに設定された有効期限が経過しているか否かを判定する。第２認証部１０６は、有効期限が経過していると判定した場合は認証失敗とし、有効期限が経過していない場合は認証成功とする。

【００６３】

なお、Ｃｏｏｋｉｅの有効期限が経過しているか否かは、ユーザ端末３０において判定されてもよい。この場合、第２認証部１０６は、ユーザ端末３０から当該判定結果だけを受信するようにしてもよい。例えば、第２認証部１０６は、Ｃｏｏｋｉｅの有効期限が経過していない旨の判定結果を受信した場合は認証失敗とし、Ｃｏｏｋｉｅの有効期限が経過している旨の判定結果を受信した場合は認証成功としてもよい。また、第２認証部１０６によりＣｏｏｋｉｅ認証が失敗したと判定された場合は、第１認証部１０３によるログイン認証が再び実行され、Ｃｏｏｋｉｅの再発行と、参照系トークンの再発行と、が実行されてもよい。

【００６４】

［第３認証部］

第３認証部１０７は、第２の認証が成功した場合に、ユーザ端末３０との間で暗証番号認証を行う。

【００６５】

暗証番号認証は、本発明に係る第３の認証の一例である。このため、本実施形態で暗証番号認証と記載した箇所は、第３の認証と読み替えることができる。第３の認証は、第２の認証とは異なる認証方法であればよい。本実施形態では、第２の認証は、第１の認証時に発行されたユーザ認証情報が用いられる認証なので、第３の認証は、第１の認証前からユーザとＡＰＩ提供システム１とが互いに保有している認証情報を利用して実行される。また例えば、第１の認証、第２の認証、及び第３の認証の各々で用いられる認証情報は、異なるデータベースで別管理することによってセキュリティ性を高めてもよい。

【００６６】

例えば、本実施形態では、第２の認証でＣｏｏｋｉｅが利用され、第３の認証で暗証番号が利用される場合を説明するが、第３の認証では、第２の認証で用いられるＣｏｏｋｉｅ以外の情報が用いられるようにすればよく、暗証番号以外にも、電子証明書、暗号キー、又はパスコードが利用されてもよい。また例えば、第３の認証は、第１の認証と同じ認証方法（例えば、ログイン認証等）であってもよいが、本実施形態では、よりセキュリティ性を高めるために、第３の認証が第１の認証と異なる認証方法とし、暗証番号認証が用いられる場合を説明する。

【００６７】

例えば、第３認証部１０７は、暗証番号認証が行われる場合に、更新系ＡＰＩ１０１の

利用要求の内容をユーザ端末３０に表示させてもよい。利用要求の内容とは、更新系ＡＰＩ１０１に対する命令内容であり、更新系ＡＰＩ１０１のプログラムの引数となりうる情報である。例えば、更新系ＡＰＩ１０１によって振込処理が実行される場合には、振込先の口座情報や振込金額といった情報である。また例えば、更新系ＡＰＩ１０１によって入出金処理が実行される場合には、入出金額や入出金者といった情報である。

【００６８】

例えば、第３認証部１０７は、Ｃｏｏｋｉｅ認証が成功した場合に、図３に示す暗証番号入力画面Ｇ６をユーザ端末３０に表示させる。第３認証部１０７は、仲介システム２から受信した利用要求に含まれる情報を参照し、更新系ＡＰＩ１０１の利用要求の内容を取得する。第３認証部１０７は、当該取得した内容に基づいて、暗証番号入力画面Ｇ６の表示内容を決定し、ユーザ端末３０に表示させる。

【００６９】

なお、更新系ＡＰＩ１０１の利用要求の内容は、暗証番号が入力される前に表示されるようにすればよく、必ずしも暗証番号を入力する画面と同じ画面で表示させなくてもよい。例えば、更新系ＡＰＩ１０１の利用要求の内容は、暗証番号入力画面Ｇ６を表示させる前の画面で表示させてもよいし、暗証番号入力画面Ｇ６のポップアップとして表示されてもよい。

【００７０】

［第２発行部］

第２発行部１０８は、Ｃｏｏｋｉｅ認証が成功した場合に、仲介システム２に、更新系ＡＰＩ１０１を利用するための更新系トークンを発行する。

【００７１】

更新系トークンは、本発明に係る第２の認証情報の一例である。このため、本実施形態で更新系トークンと記載した箇所は、第２の認証情報と読み替えることができる。第２の認証情報は、第２のＡＰＩの利用が認証されたユーザを識別する情報である。なお、第２の認証情報は、トークンに限られず、例えば、電子証明書、暗号キー、又はパスコードといった情報であってもよい。ただし、第２の認証情報は、ユーザ認証情報及び第１の認証情報とは異なる情報であるものとする。第２の認証情報の発行方法自体は、公知の種々の手法を適用可能であり、第２の認証情報の内容に応じたアルゴリズムを用意しておき、第２発行部１０８は、当該アルゴリズムに基づいて、第２の認証情報を発行すればよい。本実施形態のように、トークンを第２の認証情報として利用する場合には、例えば、ＯＡｕｔｈ２．０で実装されているトークン生成方法を利用すればよい。

【００７２】

本実施形態では、更新系ＡＰＩ１０１の利用要求を受信した場合に、Ｃｏｏｋｉｅ認証と暗証番号認証が実行されるので、第２発行部１０８は、Ｃｏｏｋｉｅ認証が成功し、かつ、暗証番号認証が成功した場合に、更新系トークンを発行する。第２発行部１０８は、Ｃｏｏｋｉｅ認証又は暗証番号認証の何れか一方でも失敗した場合には、更新系トークンを発行せず、Ｃｏｏｋｉｅ認証と暗証番号認証の両方が成功した場合に、更新系トークンを発行する。

【００７３】

例えば、更新系トークンには、特に有効期限が設定されていなくてもよいが、本実施形態では、第２発行部１０８は、更新系トークンに有効期限を設定する。更新系トークンの有効期限は、任意の長さであればよく、参照系トークンと同じ長さとしてもよいが、本実施形態では、第２発行部１０８は、Ｃｏｏｋｉｅに、参照系トークンよりも短い有効期限を設定する場合を説明する。例えば、参照系トークンの有効期限を１０分～１時間程度とする場合、更新系トークンの有効期限は数十秒～数分程度であってもよい。

【００７４】

なお、本実施形態では、第２発行部１０８は、更新系トークンのアクセストークン（以降、単に更新系アクセストークンと記載する。）だけを発行し、更新系トークンのリフレッシュトークン（以降、単に更新系リフレッシュトークンと記載する。）は発行しないも

のとして説明するが、更新系リフレッシュトークンを発行してもよい。ただし、この場合も、更新系リフレッシュトークンの有効期限は、参照系リフレッシュトークンの有効期限よりも短いものとする。

【００７５】

また例えば、第２発行部１０８は、更新系トークンに基づく更新系ＡＰＩ１０１の利用期間が所定期間未満となるように、更新系トークンを発行してもよい。当該所定期間は、任意の長さを設定すればよいが、例えば、更新系トークンのアクセストークン（以降、単に更新系アクセストークンと記載する。）については数十秒～数分程度とし、更新系トークンを実質的にワンタイム化してもよい。例えば、第２発行部１０８は、利用期間が１分未満の更新系トークンを発行する。

【００７６】

なお、第２発行部１０８は、更新系トークンに基づく更新系ＡＰＩ１０１の提供回数（利用回数）が所定回数未満となるように、更新系トークンを発行してもよい。即ち、有効期限ではなく、更新系トークンの使用回数に上限値を設けるようにしてもよい。例えば、上限値としては、１回に限られず、２回又は３回以上であってもよいが、上限値を少なく設定した方がセキュリティを高くすることができる。この場合、更新系ＡＰＩ１０１の提供回数を示す情報は、ユーザデータベース等に格納しておけばよい。後述する第２提供部１０９は、更新系ＡＰＩ１０１の提供回数が上限値に達したか否かを判定し、更新系トークンの有効性を判断してもよい。

【００７７】

なお、上記では、Ｃｏｏｋｉｅ認証が成功した場合に、第２発行部１０８が更新系トークンを発行する処理を説明したが、Ｃｏｏｋｉｅ認証が失敗した場合には、第１認証部１０３は、ユーザ端末３０との間で再度のログイン認証を行うようにしてもよい。再度のログイン認証は、１回目と全く同じ方法であってもよいし、１回目とは異なる認証方法であってもよい。例えば、１回目のログイン認証は、ユーザアカウントパスワードの組み合わせを利用して、再度のログイン認証は、当該組み合わせに追加して他の情報を利用してもよい。

【００７８】

第１発行部１０４は、再度のログイン認証が成功した場合に、ユーザ端末３０に新たなＣｏｏｋｉｅを発行する。Ｃｏｏｋｉｅの発行方法自体は、先述した通りである。この場合に、第２認証部１０６は、新たなＣｏｏｋｉｅに基づく再度のＣｏｏｋｉｅ認証を行うようにしてもよい。Ｃｏｏｋｉｅ認証の認証方法自体も、先述した通りである。再度のＣｏｏｋｉｅ認証が成功した場合には、暗証番号認証に進むようにすればよい。

【００７９】

［第２提供部］

第２提供部１０９は、仲介システム２から受信した更新系トークンに基づいて、更新系ＡＰＩ１０１を提供する。例えば、第２提供部１０９は、仲介システム２から更新系トークンを受信し、当該更新系トークンの正当性を確認する。第２提供部１０９は、仲介システム２から受信した更新系トークンと、ユーザデータベースに格納された更新系トークンと、が一致するか否かを判定する。第２提供部１０９は、これらが一致しない場合には、更新系ＡＰＩ１０１を提供せず、これらが一致する場合に、更新系ＡＰＩ１０１を提供する。

【００８０】

なお、ＡＰＩを提供するという言葉の意味は、第１提供部１０５で説明した通りである。更新系ＡＰＩ１０１であれば、口座データベースに格納された口座情報を更新する機能が関連付けられているので、第２提供部１０９は、口座データベースに格納された口座情報に基づいて振込処理を実行したり入出金処理を実行したりすることによって、更新系ＡＰＩ１０１を提供する。なお、口座情報を更新とは、口座情報の内容を変更することであり、例えば、口座残高の数値を変更したり、入出金明細情報に情報を追加したりすることである。

【００８１】
例えば、第２提供部１０９は、振込処理によって振り込まれた金額に基づいて、口座残高を減少させ、振込内容に基づいて、入出金明細情報を更新する。また例えば、第２提供部１０９は、入金処理によって入金された金額に基づいて、口座残高を増加させ、入金内容に基づいて、入出金明細情報を更新する。また例えば、第２提供部１０９は、出金処理によって出金された金額に基づいて、口座残高を減少させ、出金内容に基づいて、入出金明細情報を更新する。
【００８２】
本実施形態では、参照系トークンよりも短い有効期限が更新系トークンに設定されているので、第２提供部１０９は、更新系トークンに設定された、参照系トークンよりも短い有効期限に基づいて、第２のＡＰＩを提供することになる。第２提供部１０９は、リアルタイムクロック等を利用して現在日時を取得し、更新系トークンに設定された有効期限が経過しているか否かを判定する。第２提供部１０９は、有効期限が経過していると判定した場合は更新系ＡＰＩ１０１を提供せず、有効期限が経過していないと判定された場合は更新系ＡＰＩ１０１を提供する。
【００８３】
［仲介システムとユーザ端末で実現される機能］
仲介システム２では、例えば、仲介サーバ２０の記憶部２２は、仲介システム２のユーザアカウントとパスワードなどのデータベースを記憶する。ユーザによる仲介システム２へのログインは、当該データベースに基づいて実行される。また例えば、記憶部２２は、ユーザアカウントに関連付けて、第１発行部１０４が発行した参照系トークンと、第２発行部１０８が発行した更新系トークンと、を記憶する。また例えば、ＡＰＩ提供システム１のユーザアカウントと、仲介システム２のユーザアカウントと、が連携されてもよく、これらの対応関係が記憶部２２に記憶されてもよい。同様の対応関係は、ＡＰＩ提供システム１のデータ記憶部１０２に記憶されてもよい。
【００８４】
ユーザ端末３０では、例えば、記憶部３２は、第１発行部１０４が発行したＣｏｏｋｉｅを記憶する。また例えば、制御部３１は、操作部３４が受け付けた操作内容を、通信部３３を介してＡＰＩ提供システム１又は仲介システム２に送信する。また例えば、制御部３１は、通信部３３を介してＡＰＩ提供システム１又は仲介システム２から受信したデータに基づいて、図２及び図３で説明した各種画面を表示部３５に表示させる。
【００８５】
［４．本実施形態において実行される処理］
図７－図１０は、本実施形態において実行される処理のフロー図である。図７－図１０に示す処理は、制御部１１が記憶部１２に記憶されたプログラムに従って動作し、制御部２１が記憶部２２に記憶されたプログラムに従って動作し、制御部３１が記憶部３２に記憶されたプログラムに従って動作することによって実行される。これらの処理は、各機能ブロックが実行する処理の一例である。
【００８６】
図７に示すように、まず、ユーザ端末３０において、仲介システム２が提供するサービスのアプリケーションが起動したり、仲介システム２のウェブサイトのＵＲＬが入力されたりすると、制御部３１は、仲介システム２にアクセスする（Ｓ１）。仲介システム２においては、アクセスを受け付けると、仲介サーバ２０の制御部２１は、ユーザ端末３０に対し、ログイン画面Ｇ１の表示データを送信する（Ｓ２）。表示データは、ユーザ端末３０に画面を表示させるためのデータであればよく、例えば、ＨＴＭＬデータであってもよいし、アプリ内の画面フレームにはめ込む画像やテキストであってもよい。
【００８７】
ユーザ端末３０においては、表示データを受信すると、制御部３１は、ログイン画面Ｇ１を表示部３５に表示させる（Ｓ３）。ログイン画面Ｇ１から入力されたユーザアカウントとパスワードが仲介システム２に送信され、仲介サーバ２０の制御部２１は、ログイン

認証を実行する（Ｓ４）。Ｓ３においては、ユーザ端末３０は、ユーザがログイン画面Ｇ１で入力したユーザアカウントとパスワードの組み合わせを送信し、Ｓ４においては、仲介システム２は、記憶部２２に記憶された当該組み合わせと一致するか否かを判定する。

【００８８】

Ｓ４におけるログイン認証が失敗した場合、所定のエラーメッセージがユーザ端末３０に表示され、Ｓ３の処理に戻る。一方、Ｓ４におけるログイン認証が成功すると、仲介サーバ２０の制御部２１は、所定のログイン処理を実行し、ユーザ端末３０に対し、メニュー画面Ｇ２の表示データを送信する（Ｓ５）。

【００８９】

ユーザ端末３０においては、表示データを受信すると、制御部３１は、メニュー画面Ｇ２を表示部３５に表示させる（Ｓ６）。制御部３１は、操作部３４の検出信号に基づいて、仲介システム２に対し、ユーザの要求を送信する（Ｓ７）。Ｓ７においては、会計業務支援サービスに係る種々の要求が送信されてよいが、ここでは説明の簡略化のために、入出金明細の照会要求、又は、振込処理の実行要求の何れかが送信される場合を説明する。例えば、入出金明細の照会要求は、メニュー画面Ｇ２の入出金明細照会の項目が選択された場合に送信され、振込処理の実行要求は、メニュー画面Ｇ２の振込処理の項目が選択された後に、振込内容入力画面Ｇ５において振込内容が入力された場合に送信される。

【００９０】

仲介システム２においては、要求を受信すると、仲介サーバ２０の制御部２１は、参照系ＡＰＩ１００又は更新系ＡＰＩ１０１の何れの利用要求を受信したかを判定する（Ｓ８）。Ｓ８においては、入出金明細の照会要求であれば、参照系ＡＰＩ１００の利用要求であると判定され、振込処理の実行要求であれば、更新系ＡＰＩ１０１の利用要求であると判定される。

【００９１】

参照系ＡＰＩ１００の利用要求であると判定された場合（Ｓ８；参照系）、制御部２１は、ユーザの参照系トークンが記憶部２２に記録されているか否かを判定する（Ｓ９）。Ｓ９においては、制御部２１は、仲介システム２のユーザアカウントに関連付けて、参照系トークンが記憶部２２に記憶されているか否かを判定する。参照系トークンが記録されていないと判定された場合（Ｓ９；Ｎ）、仲介システム２とＡＰＩ提供システム１との間で、参照系トークンを発行するための参照系トークン発行処理が実行される（Ｓ１０）。

【００９２】

図８は、参照系トークン発行処理の詳細を示す図である。図８に示すように、仲介システム２において、仲介サーバ２０の制御部２１は、ＡＰＩ提供システム１へのリダイレクトを実行する（Ｓ１０１）。ＡＰＩ提供システム１のＵＲＬが予め記憶部２２に記憶されており、Ｓ１０１においては、制御部２１は、当該ＵＲＬに基づいてリダイレクトを実行する。なお、先述したように、ＡＰＩ提供システム１へのリダイレクトが実行される旨を予めユーザ端末３０に表示させ、ユーザの同意を得てもよいし、リダイレクト処理がユーザ端末３０において実行されてもよい。

【００９３】

Ｓ１０１におけるリダイレクトが実行されると、ユーザ端末３０がＡＰＩ提供システム１にアクセスし、ＡＰＩ提供システム１において、ＡＰＩ提供サーバ１０の制御部１１は、ユーザ端末３０に対し、ログイン画面Ｇ３の表示データを送信する（Ｓ１０２）。

【００９４】

ユーザ端末３０においては、表示データを受信すると、制御部３１は、ログイン画面Ｇ３を表示部３５に表示させる（Ｓ１０３）。ログイン画面Ｇ３から入力されたユーザアカウントとパスワードがＡＰＩ提供システム１に送信され、ＡＰＩ提供サーバ１０の制御部１１は、ログイン認証を実行する（Ｓ１０４）。Ｓ１０４においては、ユーザ端末３０は、ユーザがログイン画面Ｇ３で入力したユーザアカウントとパスワードの組み合わせを送信し、ＡＰＩ提供システム１は、ユーザデータベースに格納された当該組み合わせと一致するか否かを判定する。

【００９５】
Ｓ１０４におけるログイン認証が失敗した場合、所定のエラーメッセージがユーザ端末３０に表示され、Ｓ１０３の処理に戻る。一方、Ｓ１０４におけるログイン認証が成功すると、ＡＰＩ提供サーバ１０の制御部１１は、所定のログイン処理を実行してＣｏｏｋｉｅを発行し、ユーザ端末３０に対し、Ｃｏｏｋｉｅを送信する（Ｓ１０５）。Ｓ１０５においては、制御部１１は、リアルタイムクロック等から取得した現在日時の所定時間後の時間をＣｏｏｋｉｅの有効期限に設定する。先述したように、Ｃｏｏｋｉｅは、所定の関数に基づいて発行されるようにすればよい。なお、Ｓ１０４におけるログイン処理が成功した後は、ユーザ端末３０がＡＰＩ提供システム１と通信する場合には、ＡＰＩ提供システム１のユーザアカウントが適宜送信されるものとする。ユーザ端末３０においては、Ｃｏｏｋｉｅを受信すると、制御部３１は、Ｃｏｏｋｉｅを記憶部３２に記録する（Ｓ１０６）。

【００９６】
また、ＡＰＩ提供サーバ１０の制御部１１は、仲介システム２に対し、所定の認可コードを送信する（Ｓ１０７）。Ｓ１０７で送信される認可コードは、ログイン認証が成功し、参照系トークンの発行が許可されたことを示す情報である。仲介システム２においては、認可コードを受信すると、仲介サーバ２０の制御部２１は、参照系トークンの発行要求を送信する（Ｓ１０８）。参照系トークンの発行要求は、例えば、ＯＡｕｔｈ２．０のプロトコルで定められた所定形式の情報が送信されることで行われる。

【００９７】
ＡＰＩ提供システム１においては、発行要求を受信すると、ＡＰＩ提供サーバ１０の制御部１１は、参照系トークンを発行する（Ｓ１０９）。Ｓ１０９においては、制御部１１は、記憶部１２のユーザデータベースに、ＡＰＩ提供システム１のユーザアカウントと関連付けて、発行した参照系トークンを格納する。制御部１１は、仲介システム２に対し、Ｓ１０９で発行した参照系トークンを送信する（Ｓ１１０）。仲介システム２においては、参照系トークンを受信すると、仲介サーバ２０の制御部２１は、参照系トークンを記憶部２２に記録する（Ｓ１１１）。Ｓ１１１においては、例えば、制御部２１は、仲介システム２のユーザアカウントと関連付けて、参照系トークンを記録する。

【００９８】
以上の処理によって参照系トークンが発行されると、図７に戻り、仲介システム２においては、仲介サーバ２０の制御部２１は、Ｓ１０で発行された参照系トークンに基づいて、参照系ＡＰＩ１００の利用要求を送信する（Ｓ１１）。参照系ＡＰＩ１００の利用要求には、参照する口座を識別するための情報が含まれているものとする。例えば、仲介サーバ２０の記憶部２２に、ユーザごとに支店名と口座番号の組み合わせを記憶しておき、当該組み合わせを利用要求に含めてもよいし、ＡＰＩ提供システム１と仲介システム２とで互いのユーザアカウントを連携しておき、ＡＰＩ提供システム１又は仲介システム２のユーザアカウントを利用要求に含めることで、ユーザの口座が特定されてもよい。

【００９９】
ＡＰＩ提供システム１においては、参照系ＡＰＩ１００の利用要求を受信すると、ＡＰＩ提供サーバ１０の制御部１１は、ユーザデータベースに基づいて、参照系アクセストークンが有効か否かを判定する（Ｓ１２）。Ｓ１２においては、制御部１１は、参照系アクセストークンの有効期限内であるか否かを判定する。

【０１００】
参照系アクセストークンが有効であると判定された場合（Ｓ１２；Ｙ）、制御部１１は、口座データベースに基づいて、参照系ＡＰＩ１００の応答として、仲介システム２に対し、入出金明細の照会結果を送信する（Ｓ１３）。Ｓ１３においては、制御部１１は、参照系ＡＰＩ１００の利用要求に基づいて、参照対象となる口座を特定する。そして、制御部１１は、当該口座の入出金明細情報を取得して、照会結果として送信する。

【０１０１】
仲介システム２においては、入出金明細の照会結果を受信すると、仲介サーバ２０の制

御部２１は、受信した照会結果に基づいて、ユーザ端末３０に対し、入出金明細画面Ｇ４の表示データを送信する（Ｓ１４）。ユーザ端末３０においては、表示データを受信すると、入出金明細画面Ｇ４を表示部３５に表示させる（Ｓ１５）。なお、ユーザがメニュー画面Ｇ２に戻る操作をした場合には、Ｓ６の処理に戻る。

【０１０２】

一方、Ｓ１２において、参照系アクセストークンが無効であると判定された場合（Ｓ１２；Ｎ）、図９に移り、制御部１１は、仲介システム２に対し、参照系アクセストークンが無効である旨の無効エラー通知を送信する（Ｓ１６）。無効エラー通知は、例えば、ＯＡｕｔｈ２．０のプロトコルで定められた所定形式の情報が送信されることで行われる。

【０１０３】

仲介システム２においては、無効エラー通知を受信すると、仲介サーバ２０の制御部２１は、記憶部２２に記憶された参照系リフレッシュトークンを送信する（Ｓ１７）。ＡＰＩ提供システム１においては、参照系リフレッシュトークンを受信すると、ＡＰＩ提供サーバ１０の制御部１１は、記憶部１２に記憶されたユーザデータベースに基づいて、受信したリフレッシュトークンが有効か否かを判定する（Ｓ１８）。Ｓ１８においては、制御部１１は、リフレッシュトークンの有効期限内であるか否かを判定する。

【０１０４】

参照系トークンのリフレッシュトークンが無効であると判定された場合（Ｓ１８；Ｎ）、制御部１１は、仲介システム２に対し、リフレッシュトークンが無効である旨の無効エラー通知を送信し（Ｓ１９）、Ｓ１０の参照系トークン発行処理に移行する。この場合、図８に示す参照系トークン発行処理が再び実行され、ログイン認証が成功すると、ユーザ端末３０にＣｏｏｋｉｅが送信され、仲介システム２に新たな参照系トークンが送信される。

【０１０５】

一方、Ｓ１８において、参照系リフレッシュトークンが有効であると判定された場合（Ｓ１８；Ｙ）、制御部１１は、参照系アクセストークンを再発行し、仲介システム２に対し、当該再発行した参照系アクセストークンを送信する（Ｓ２０）。Ｓ２０の処理は、Ｓ１０９の処理と同様であるが、Ｓ２０では、参照系アクセストークンだけが発行される。なお、参照系リフレッシュトークンの有効期限は延長されるようにしてよい。

【０１０６】

仲介システム２においては、参照系アクセストークンを受信すると、仲介サーバ２０の制御部２１は、参照系アクセストークンを記憶部２２に記録する（Ｓ２１）。Ｓ２１においては、例えば、制御部２１は、仲介システム２のユーザアカウントと関連付けて、参照系アクセストークンを記録する。その後、Ｓ１１の処理に移行する。

【０１０７】

一方、図７のＳ８において、更新系ＡＰＩ１０１の利用要求であると判定された場合（Ｓ８；更新系）、図１０に移り、制御部２１は、ＡＰＩ提供システム１に対し、更新系アクセストークンの発行要求を送信する（Ｓ２２）。更新系アクセストークンの発行要求は、例えば、ＯＡｕｔｈ２．０のプロトコルで定められた所定形式の情報が送信されることで行われる。

【０１０８】

ＡＰＩ提供システム１においては、要求を受信すると、ＡＰＩ提供サーバ１０の制御部１１は、ユーザ端末３０との間でＣｏｏｋｉｅ認証を実行する（Ｓ２３）。Ｓ２３においては、ＡＰＩ提供サーバ１０は、ユーザ端末３０にＣｏｏｋｉｅの送信を要求し、ユーザ端末３０は、当該要求に応じて、記憶部３２に記憶されたＣｏｏｋｉｅ（Ｓ１０６で記録されたＣｏｏｋｉｅ）を送信する。

【０１０９】

なお、Ｃｏｏｋｉｅに有効期限を設定する場合には、Ｓ２３において、制御部１１は、Ｃｏｏｋｉｅが有効期限内であるか否かを判定してもよいし、ユーザ端末３０においてＣｏｏｋｉｅが有効期限内であるか否かが判定されてもよい。更に、ユーザ端末３０におい

てＣｏｏｋｉｅが有効ではないと判定された場合には、Ｓ２３のＣｏｏｋｉｅ認証が実行されることなく、Ｓ１０における参照系トークン発行処理が実行され、Ｃｏｏｋｉｅが再発行されてもよい。

【０１１０】

Ｓ２３において、Ｃｏｏｋｉｅ認証に失敗した場合（Ｓ２３；Ｎ）、仲介システム２とＡＰＩ提供システム１との間で参照系トークン発行処理が実行され（Ｓ２４）、Ｓ２２の処理に戻る。Ｓ２４の処理は、Ｓ１０の処理と同様であり、図８に示す参照系トークン発行処理が実行され、ログイン認証が成功すると、ユーザ端末３０にＣｏｏｋｉｅが送信され、仲介システム２に新たな参照系トークンが送信される。これにより、Ｓ２２の処理に戻ると、Ｓ２３において、Ｃｏｏｋｉｅ認証が成功する。

【０１１１】

一方、Ｓ２３において、Ｃｏｏｋｉｅ認証に成功した場合（Ｓ２３；Ｙ）、ＡＰＩ提供サーバ１０の制御部１１は、ユーザ端末３０に対し、暗証番号入力画面Ｇ６の表示データを送信する（Ｓ２５）。なお、Ｓ２２における更新系アクセストークンの発行要求とともに、振込内容入力画面Ｇ５において入力された振込内容が送信され、Ｓ２５においては、制御部１１は、当該振込内容を含む暗証番号入力画面Ｇ６の表示データを送信してもよい。

【０１１２】

ユーザ端末３０においては、表示データを受信すると、制御部３１は、暗証番号入力画面Ｇ６を表示部３５に表示させる（Ｓ２６）。Ｓ２６においては、振込内容とともに、暗証番号を入力することができる状態となる。暗証番号入力画面Ｇ６から入力された暗証番号がＡＰＩ提供システム１に送信され、ＡＰＩ提供サーバ１０の制御部１１は、暗証番号認証を実行する（Ｓ２７）。Ｓ２７においては、ユーザ端末３０は、ユーザが暗証番号入力画面Ｇ６で入力した暗証番号を送信し、ＡＰＩ提供システム１は、口座データベースに格納された暗証番号と一致するか否かを判定する。

【０１１３】

Ｓ２７における暗証番号認証が失敗した場合、所定のエラーメッセージがユーザ端末３０に表示され、Ｓ２６の処理に戻る。一方、Ｓ２７における暗証番号認証が成功すると、ＡＰＩ提供サーバ１０の制御部１１は、仲介システム２に対し、所定の認可コードを送信する（Ｓ２８）。Ｓ２８で送信される認可コードは、暗証番号認証が成功し、更新系アクセストークンの発行が許可されたことを示す情報である。仲介システム２においては、認可コードを受信すると、仲介サーバ２０の制御部２１は、更新系アクセストークンの発行要求を送信する（Ｓ２９）。

【０１１４】

ＡＰＩ提供システム１においては、発行要求を受信すると、ＡＰＩ提供サーバ１０の制御部１１は、更新系アクセストークンを発行する（Ｓ３０）。Ｓ３０においては、制御部１１は、記憶部１２のユーザデータベースに、ＡＰＩ提供システム１のユーザアカウントと関連付けて、発行した更新系アクセストークンを格納する。制御部１１は、仲介システム２に対し、Ｓ３０で発行した更新系アクセストークンを送信する（Ｓ３１）。

【０１１５】

仲介システム２においては、更新系アクセストークンを受信すると、仲介サーバ２０の制御部２１は、更新系アクセストークンを記憶部２２に格納する（Ｓ３２）。Ｓ３２においては、例えば、制御部２１は、仲介システム２のユーザアカウントと関連付けて、更新系アクセストークンを記録する。制御部２１は、発行された更新系アクセストークンに基づいて、更新系ＡＰＩ１０１の利用要求を送信する（Ｓ３３）。更新系ＡＰＩ１００の利用要求には、振込内容を示す情報が含まれていてもよいし、振込内容は、Ｓ２２の処理の時点で送信されていてもよい。

【０１１６】

ＡＰＩ提供システム１においては、更新系ＡＰＩ１０１の利用要求を受信すると、ＡＰＩ提供サーバ１０の制御部１１は、ユーザデータベースに基づいて、更新系アクセストー

クンが有効か否かを判定する（Ｓ３４）。Ｓ３４においては、制御部１１は、アクセストークンの有効期限内であるか否かを判定する。

【０１１７】

更新系アクセストークンが無効であると判定された場合（Ｓ３４；Ｎ）、更新系アクセストークンが無効である旨の無効エラー通知が仲介システム２に送信され、Ｓ２２の処理に戻る。この場合、更新系アクセストークンの発行がやり直される。一方、更新系アクセストークンが有効であると判定された場合（Ｓ３４；Ｙ）、制御部１１は、更新系ＡＰＩ１０１の応答として、振込処理を実行する（Ｓ３５）。Ｓ３５においては、制御部１１は、振込内容入力画面Ｇ５において入力された内容の振込を実行し、口座データベースを更新する。

【０１１８】

制御部１１は、仲介システム２に対し、Ｓ３５における振込処理の実行結果を送信する（Ｓ３６）。仲介システム２においては、振込処理の実行結果を受信すると、仲介サーバ２０の制御部２１は、受信した実行結果に基づいて、ユーザ端末３０に対し、振込完了画面Ｇ７の表示データを送信する（Ｓ３７）。ユーザ端末３０においては、表示データを受信すると、振込完了画面Ｇ７を表示部３５に表示させる（Ｓ３８）。なお、ユーザがメニュー画面Ｇ２に戻る操作をした場合には、Ｓ６の処理に戻る。

【０１１９】

ＡＰＩ提供システム１によれば、参照系ＡＰＩ１００の利用要求が送信された場合のログイン認証でＣｏｏｋｉｅが発行されてユーザ端末３０に記憶され、更新系ＡＰＩ１０１の利用要求が送信された場合にＣｏｏｋｉｅ認証が実行される。これにより、参照系ＡＰＩ１００を利用するユーザが更新系ＡＰＩ１０１を利用しようとしていること（即ち、参照系の権限を与えたユーザ端末３０と同じ端末であること）を確認することができるので、仲介システム２を介して複数のＡＰＩを提供する場合のセキュリティを高めることができる。また、更新系ＡＰＩ１０１を利用するためには、少なくとも、参照系ＡＰＩ１００の利用時のログイン認証と、Ｃｏｏｋｉｅ認証と、の２段階の認証をする必要があるため、セキュリティ性を高めることができる。また、更新系の認証ではログイン認証が行われないので、ユーザがユーザアカウントとパスワードを２回入力するといった手間を省くことができる。更に、異なる種類の認証情報を用いることで、よりセキュリティ性を高めることができる。

【０１２０】

また、更新系ＡＰＩ１０１を利用するための暗証番号認証は、Ｃｏｏｋｉｅ認証が成功しないと実行されないので、更新系ＡＰＩ１０１を利用するための認証を複数回実行することで、セキュリティを効果的に高めることができる。また、暗証番号認証を実行する場合には、更新系ＡＰＩ１０１を利用するためには、少なくとも、参照系ＡＰＩ１００の利用時のログイン認証、Ｃｏｏｋｉｅ認証、及び暗証番号認証の３段階の認証をする必要があるため、セキュリティ性を効果的に高めることができる。更に、これら３つの認証を異なる種類の認証情報で実行することで、よりセキュリティ性を高めることができる。

【０１２１】

また、更新系ＡＰＩ１０１を利用するための暗証番号認証の際に、振込内容が表示されるので、悪意のある第三者による不正な振込に未然に気付くことができる。例えば、仲介システム２がハッキング等の不正アクセスを受け、ユーザの身に覚えのない振込が第三者によって試みられたり（例えば、振込内容入力画面Ｇ５においてユーザが振込内容を入力することなく、第三者の手によって振込内容が不正に入力される等）、ユーザによる振込手続き中に第三者によって不正に割り込まれて振込先や金額の改ざんがなされようとしたりしている（例えば、振込内容入力画面Ｇ５においてユーザが振込内容を入力してから、暗証番号入力画面Ｇ６が表示されるまでの間に、第三者によって改ざんが行われる）ことを発見することができる。

【０１２２】

また、Ｃｏｏｋｉｅに有効期限を設けることで、セキュリティを効果的に高めることが

できる。
【０１２３】
また、更新系アクセストークンの有効期限を、参照系アクセストークンの有効期限よりも短く設定することで、セキュリティを効果的に高めることができる。
【０１２４】
また、更新系アクセストークンに基づく更新系ＡＰＩ１０１の提供回数や利用期間に制限を設けることで、セキュリティを効果的に高めることができる。例えば、更新系アクセストークンをワンタイム化することで、セキュリティを効果的に高めることができる。
【０１２５】
また、Ｃｏｏｋｉｅ認証に失敗した場合には、参照系トークン発行処理が実行され、ログイン認証からやり直されるので、セキュリティを効果的に高めることができる。
【０１２６】
［５．変形例］
なお、本発明は、以上に説明した実施の形態に限定されるものではない。本発明の趣旨を逸脱しない範囲で、適宜変更可能である。
【０１２７】
例えば、Ｃｏｏｋｉｅ認証の後に暗証番号認証が実行される場合を説明したが、Ｃｏｏｋｉｅ認証の前に暗証番号認証が実行されてもよい。また例えば、ＡＰＩ提供システム１は、第３認証部１０７を省略し、暗証番号認証は省略してもよい。
【０１２８】
また例えば、ＡＰＩ提供システム１では、参照系ＡＰＩ１００、更新系ＡＰＩ１０１、データ記憶部１０２、第１認証部１０３、第１発行部１０４、第１提供部１０５、第２認証部１０６、第３認証部１０７、第２発行部１０８、及び第２提供部１０９が、ＡＰＩ提供サーバ１０で実現される場合を説明したが、これら各機能は、ＡＰＩ提供システム１内の複数のコンピュータで分担されてもよい。
【０１２９】
例えば、ＡＰＩ提供システム１がＡＰＩ提供サーバ１０とは別にデータベースサーバを有する場合には、データ記憶部１０２は、データベースサーバにより実現されてもよい。また例えば、ＡＰＩ提供システム１がＡＰＩ提供サーバ１０とは別に認証サーバを有する場合には、参照系ＡＰＩ１００、更新系ＡＰＩ１０１、第１提供部１０５、及び第２提供部１０９がＡＰＩ提供サーバ１０によって実現され、第１認証部１０３、第１発行部１０４、第２認証部１０６、第３認証部１０７、及び第２発行部１０８が認証サーバによって実現されてもよい。
【０１３０】
また例えば、ＡＰＩ提供システム１が、複数のＡＰＩ提供サーバ１０を有する場合には、第１のＡＰＩ提供サーバ１０によって参照系ＡＰＩ１００が実現され、第２のＡＰＩ提供サーバ１０によって更新系ＡＰＩ１０１が実現されてもよい。また例えば、ＡＰＩ提供システム１が、複数の認証サーバを有する場合には、第１の認証サーバによって、第１認証部１０３と第１発行部１０４が実現され、第２の認証サーバによって、第２認証部１０６、第３認証部１０７、及び第２発行部１０８が実現されてもよい。
【０１３１】
また例えば、ＡＰＩ提供システム１のＡＰＩによって金融サービスが提供される場合を説明したが、ＡＰＩが提供するサービスは、任意のサービスであってよい。例えば、電子商取引において、商品ページを参照する参照系ＡＰＩと、商品ページの編集するための編集系ＡＰＩと、のセキュリティレベルを分けて、編集系ＡＰＩに実施形態で説明したＣｏｏｋｉｅ認証を導入してもよい。また例えば、保険サービスにおいて、保険商品の参照をするための閲覧系ＡＰＩと、保険商品の編集をするための編集系ＡＰＩと、のセキュリティレベルを分けて、編集系ＡＰＩに実施形態で説明したＣｏｏｋｉｅ認証を導入してもよい。また例えば、旅行予約サービスにおいて、旅行商品の閲覧をするための閲覧系ＡＰＩと、旅行商品の編集をするための編集系ＡＰＩと、のセキュリティレベルを分けて、編集

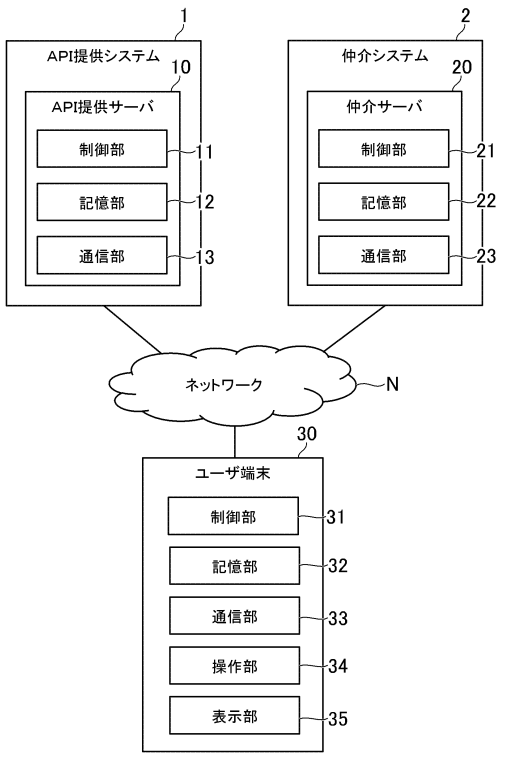
系ＡＰＩに実施形態で説明したＣｏｏｋｉｅ認証を導入してもよい。また例えば、ＳＮＳにおいて、自分や他人の投稿を閲覧するための閲覧系ＡＰＩと、新規投稿をするための投稿系ＡＰＩと、のセキュリティレベルを分けて、投稿系ＡＰＩに実施形態で説明したＣｏｏｋｉｅ認証を導入してもよい。

【符号の説明】

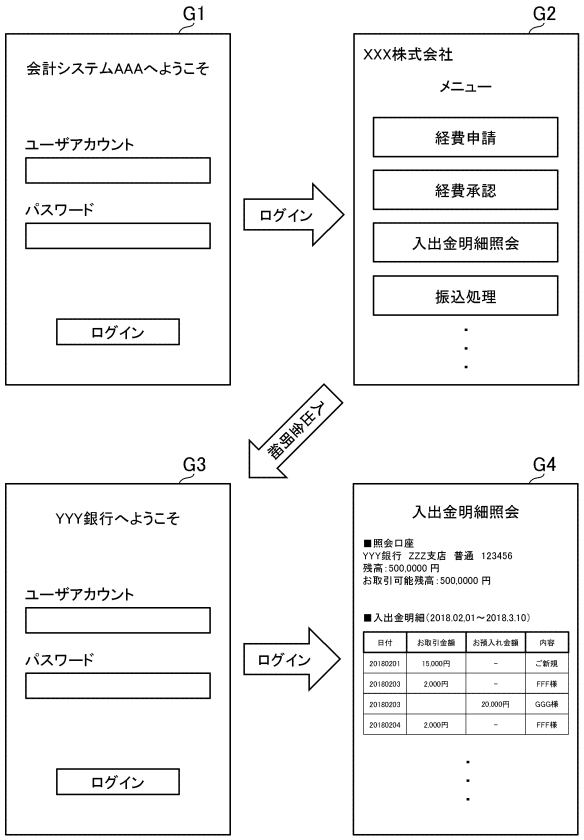
【０１３２】

１　ＡＰＩ提供システム、１０　ＡＰＩ提供サーバ、１１，２１，３１　制御部、１２，２２，３２　記憶部、１３，２３，３３　通信部、２　仲介システム、２０　仲介サーバ、３０　ユーザ端末、３４　操作部、３５　表示部、Ｇ１　ログイン画面、Ｇ２　メニュー画面、Ｇ３　ログイン画面、Ｇ４　入出金明細画面、Ｇ５　振込内容入力画面、Ｇ６　暗証番号入力画面、Ｇ７　振込完了画面、１００　参照系ＡＰＩ、１０１　更新系ＡＰＩ、１０２　データ記憶部、１０３　第１認証部、１０４　第１発行部、１０５　第１提供部、１０６　第２認証部、１０７　第３認証部、１０８　第２発行部、１０９　第２提供部。

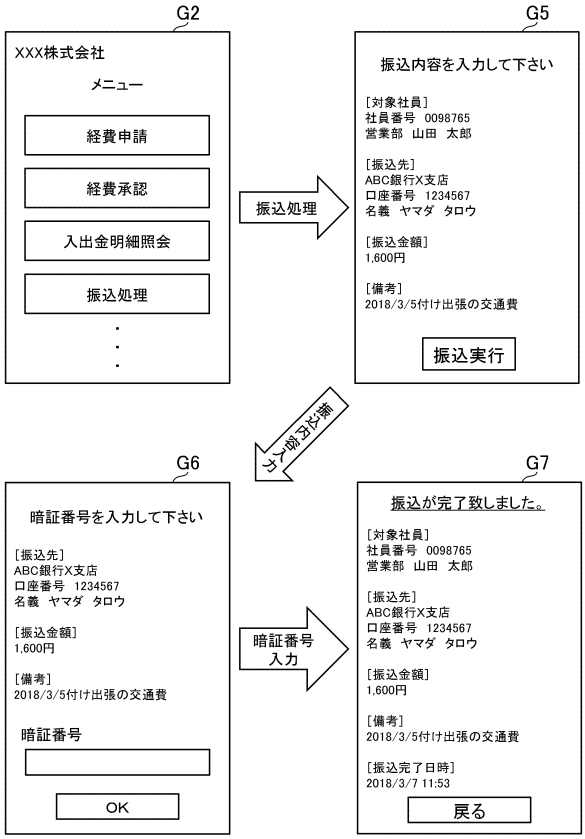
【図１】



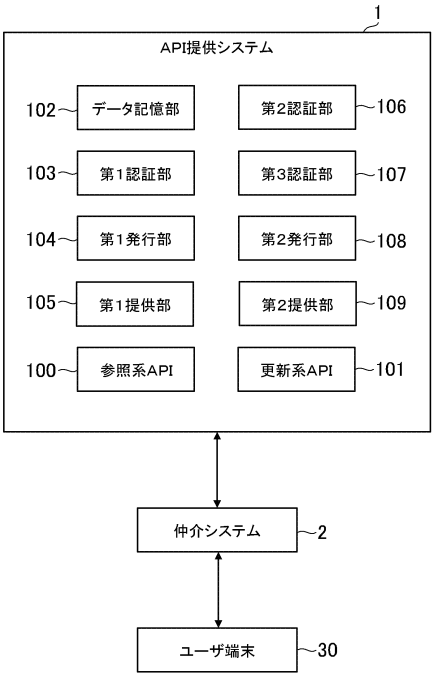
【図２】



【図３】



【図４】



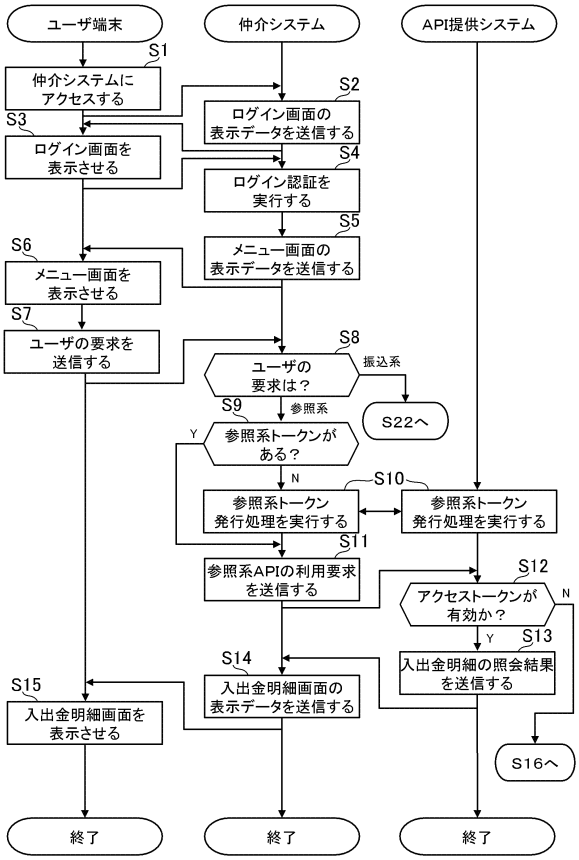
【図５】

ユーザアカウント	ユーザ名	パスワード	Cookie	参照系トークン	更新系トークン	口座属性情報
u00001	XXX株式会社	******	Cookie情報1 有効期限 2018/3/7 12:00	参照系アクセストークン1 有効期限 2018/3/7 12:00 参照系リフレッシュトークン1 有効期限 2018/3/7 12:00	更新系アクセストークン1 有効期限 2018/3/7 11:55	A支店 0123456 XXX株式会社
u00002	UUU	******	-	-	-	B支店 9876543 UUU
u00003	株式会社OOO	******	Cookie情報3 有効期限 2018/3/7 12:25	参照系アクセストークン3 有効期限 2018/3/7 12:25 参照系リフレッシュトークン3 有効期限 2018/3/7 12:25	-	A支店 5678901 株式会社OOO
u00004	有限会社PPP	******	Cookie情報4 有効期限 2018/3/7 12:18	参照系アクセストークン4 有効期限 2018/3/7 12:18 参照系リフレッシュトークン4 有効期限 2018/3/7 12:18	更新系アクセストークン4 有効期限 2018/3/7 11:57	D支店 3210987 有限会社PPP
・・・	・・・	・・・	・・・	・・・	・・・	・・・

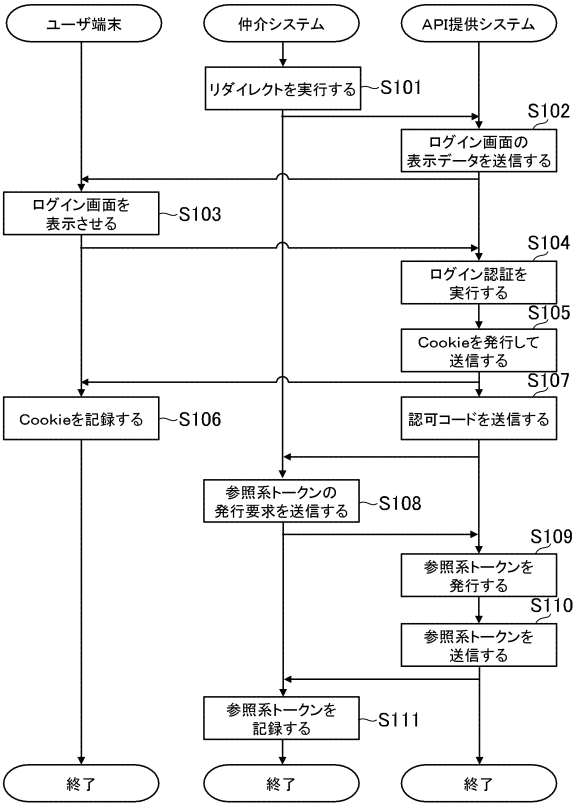
【図６】

支店名	口座番号	口座名義人	残高情報	暗証番号	入出金明細情報
A支店	123456	XXX株式会社	5000000	****	入出金明細情報1
B支店	9876543	UUU	1200000	****	入出金明細情報2
A支店	5678901	株式会社OOO	2500000	****	入出金明細情報3
D支店	3210987	有限会社PPP	2800000	****	入出金明細情報4
・・・	・・・	・・・	・・・	・・・	・・・

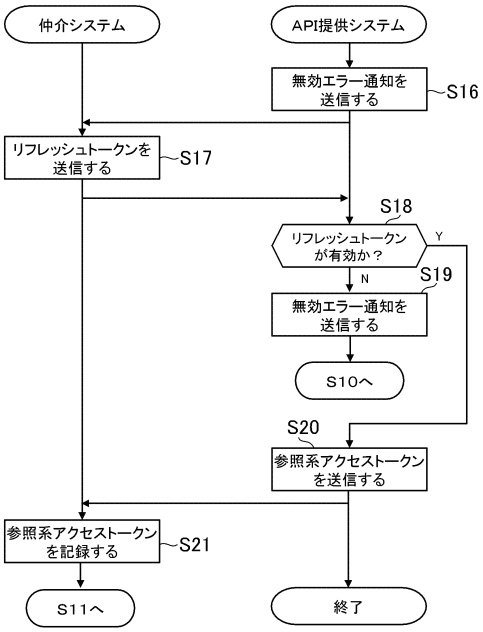
【図７】


ユーザ端末
仲介システム
API提供システム
S1
仲介システムにアクセスする
S2
ログイン画面の表示データを送信する
S3
ログイン画面を表示させる
S4
ログイン認証を実行する
S5
メニュー画面の表示データを送信する
S6
メニュー画面を表示させる
S7
ユーザの要求を送信する
S8
ユーザの要求は？
振込系
S22へ
S9
参照系
参照系トークンがある？
Y
N
S10
参照系トークン発行処理を実行する
参照系トークン発行処理を実行する
S11
参照系APIの利用要求を送信する
S12
アクセストークンが有効か？
N
Y
S13
入出金明細の照会結果を送信する
S14
入出金明細画面の表示データを送信する
S15
入出金明細画面を表示させる
S16へ
終了
終了
終了

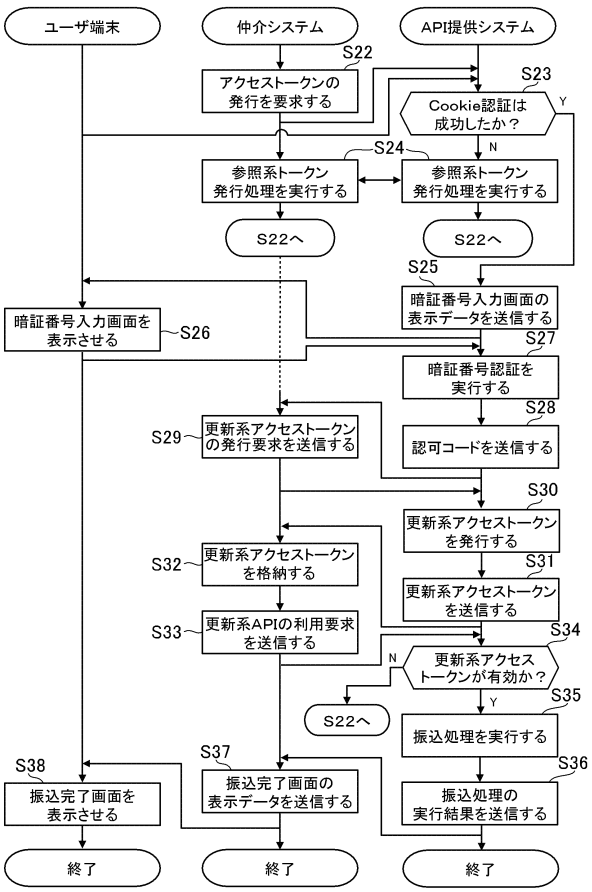
【図８】


ユーザ端末
仲介システム
API提供システム
リダイレクトを実行する
S101
S102
ログイン画面の表示データを送信する
ログイン画面を表示させる
S103
S104
ログイン認証を実行する
S105
Cookieを発行して送信する
S107
Cookieを記録する
S106
認可コードを送信する
参照系トークンの発行要求を送信する
S108
S109
参照系トークンを発行する
S110
参照系トークンを送信する
参照系トークンを記録する
S111
終了
終了
終了

【図９】


仲介システム
API提供システム
無効エラー通知を送信する
S16
リフレッシュトークンを送信する
S17
S18
リフレッシュトークンが有効か？
Y
N
S19
無効エラー通知を送信する
S10へ
S20
参照系アクセストークンを送信する
参照系アクセストークンを記録する
S21
S11へ
終了

【図１０】


ユーザ端末
仲介システム
API提供システム
S22
アクセストークンの発行を要求する
S23
Cookie認証は成功したか？
Y
N
S24
参照系トークン発行処理を実行する
参照系トークン発行処理を実行する
S22へ
S22へ
S25
暗証番号入力画面の表示データを送信する
暗証番号入力画面を表示させる
S26
S27
暗証番号認証を実行する
S28
認可コードを送信する
S29
更新系アクセストークンの発行要求を送信する
S30
更新系アクセストークンを発行する
S31
更新系アクセストークンを送信する
S32
更新系アクセストークンを格納する
S33
更新系APIの利用要求を送信する
S34
更新系アクセストークンが有効か？
N
Y
S22へ
S35
振込処理を実行する
S36
振込処理の実行結果を送信する
S37
振込完了画面の表示データを送信する
S38
振込完了画面を表示させる
終了
終了
終了

フロントページの続き

(56)参考文献 特開２００８－１９７９７３（ＪＰ，Ａ）
米国特許出願公開第２０１４／０２８２９８３（ＵＳ，Ａ１）
米国特許出願公開第２０１７／０００６０２１（ＵＳ，Ａ１）
特表２０１０－５２５４７１（ＪＰ，Ａ）
特表２００３－５２７６４６（ＪＰ，Ａ）
特開２０１５－１２５５１０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／００
２１／３０－２１／４６
Ｇ０６Ｑ２０／００－２０／４２
Ｇ０６Ｑ４０／００－４０／０８