(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7469756号
(P7469756)

(45)発行日　令和6年4月17日(2024.4.17)

(24)登録日　令和6年4月9日(2024.4.9)

(51)国際特許分類

		FI		
H04L 9/32 (2006.01)		H04L	9/32	200B
G09C 1/00 (2006.01)		G09C	1/00	640E
		H04L	9/32	200D

請求項の数　22　（全47頁）

(21)出願番号　特願2020-527589(P2020-527589)
(86)(22)出願日　令和1年6月26日(2019.6.26)
(86)国際出願番号　PCT/JP2019/025434
(87)国際公開番号　WO2020/004486
(87)国際公開日　令和2年1月2日(2020.1.2)
審査請求日　令和4年6月24日(2022.6.24)
(31)優先権主張番号　特願2018-121031(P2018-121031)
(32)優先日　平成30年6月26日(2018.6.26)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　500088667
日本通信株式会社
東京都港区虎ノ門４丁目１番２８号
(74)代理人　110002860
弁理士法人秀和特許事務所
(72)発明者　福田 尚久
日本国東京都港区虎ノ門４丁目１番２８号 日本通信株式会社内
(72)発明者　ダイクマン，グレッグ
日本国東京都港区虎ノ門４丁目１番２８号 日本通信株式会社内
(72)発明者　横山 裕昭
日本国東京都港区虎ノ門４丁目１番２８号 日本通信株式会社内
(72)発明者　渋谷 靖

最終頁に続く

(54)【発明の名称】　オンラインサービス提供システム

(57)【特許請求の範囲】

【請求項１】

サービス提供者が提供するオンラインサービスを、前記サービス提供者とは異なる者が提供する中間サービスを介して、携帯機器から安全に利用可能な仕組みを提供するオンラインサービス提供システムであって、

登録されたユーザに対し、インターネットを通じて前記オンラインサービスを提供するサービス提供サーバと、

前記ユーザに対し、インターネットを通じて前記中間サービスを提供する中間サーバと、

前記ユーザが所持している携帯機器であるユーザ機器に設けられるＩＣチップと、

前記ユーザ機器が有する本体プロセッサにより実行され、前記ユーザ機器を前記中間サービスを利用するための端末として機能させるアプリケーションプログラムと、を有し、

前記ＩＣチップは、

少なくとも、前記ユーザ機器を使用する者の正当性を確認するためのユーザ認証に用いられる本人情報、前記ユーザの秘密鍵、前記秘密鍵とペアになる前記ユーザの公開鍵、及び、前記公開鍵を含む前記ユーザの電子証明書を非一時的に記憶するメモリと、

少なくとも、前記本体プロセッサにより実行されるプログラムから与えられる情報を前記本人情報と照合することにより前記ユーザ認証を行う認証機能、及び、前記本体プロセッサにより実行されるプログラムから与えられるデータに対し前記秘密鍵を用いた電子署名を行う電子署名機能を有するプロセッサと、

を有し、通信用のＳＩＭカード上に重ねて貼り付けられた状態でＳＩＭカードスロットに

装着されるものであり、
前記ＩＣチップの前記メモリは、前記本体プロセッサにより実行されるプログラムが直接に読み書きできないエリアを有しており、
少なくとも前記本人情報及び前記秘密鍵は、前記エリア内に格納され、
前記ＩＣチップの前記プロセッサは、前記本体プロセッサにより実行されるプログラムに対して、複数のＡＰＩを提供するものであり、
前記複数のＡＰＩは、前記認証機能を利用するための認証ＡＰＩ及び前記電子署名機能を利用するための電子署名ＡＰＩを少なくとも含み、前記ＩＣチップの前記メモリから前記秘密鍵を読みだすためのＡＰＩを含んでおらず、
前記アプリケーションプログラムは、前記ユーザ機器を、
前記ユーザ機器を使用する者から取得した情報に基づき、前記認証ＡＰＩを介して前記ＩＣチップの前記認証機能を利用して、前記ユーザ認証を行うユーザ認証手段、及び、
前記ユーザ認証により前記ユーザ機器を使用する者が正当であると確認された場合に、前記電子署名ＡＰＩを介して前記ＩＣチップの前記電子署名機能を利用して電子署名を生成し、生成された前記電子署名を含むログイン要求をインターネットを通じて前記中間サーバに送信する送信手段、として機能させ、
前記中間サーバは、
前記ユーザ機器から前記ログイン要求を受信した場合に、前記ユーザの電子証明書を用いて前記ログイン要求に含まれる前記電子署名を検証することによって前記ログイン要求の正当性を確認し、前記ログイン要求が正当であると確認された場合に前記ユーザ機器からの前記中間サービスの利用を許可すると共に、アクセス要求を前記サービス提供サーバに送信する制御手段と、
を有し、
前記サービス提供サーバは、
前記中間サーバから前記アクセス要求を受信した場合に、前記アクセス要求の正当性を確認し、前記アクセス要求が正当であると確認された場合に前記中間サーバによる前記オンラインサービスの利用を許可するアクセス制御手段と、
を有することを特徴とするオンラインサービス提供システム。
【請求項２】
前記ユーザ認証により前記ユーザ機器を使用する者が正当であると確認されると、前記電子署名機能の機能制限が解除され、前記アプリケーションプログラムから前記電子署名ＡＰＩを介した前記電子署名機能の利用が可能となる
ことを特徴とする請求項１に記載のオンラインサービス提供システム。
【請求項３】
前記中間サーバの前記制御手段は、前記ログイン要求に含まれる前記電子署名とともに前記アクセス要求を前記サービス提供サーバに送信し、
前記サービス提供サーバは、前記ユーザの電子証明書を用いて前記電子署名を検証することによって前記アクセス要求の正当性を確認する
ことを特徴とする請求項１又は２に記載のオンラインサービス提供システム。
【請求項４】
前記中間サーバの前記制御手段は、前記ユーザのユーザＩＤ及びパスワードとともに前記アクセス要求を前記サービス提供サーバに送信し、
前記サービス提供サーバは、前記ユーザの前記ユーザＩＤ及び前記パスワードを検証することによって前記アクセス要求の正当性を確認する
ことを特徴とする請求項１又は２に記載のオンラインサービス提供システム。
【請求項５】
前記中間サーバの前記制御手段は、前記ユーザのユーザＩＤと前記サービス提供サーバが予め発行したアクセストークンとともに前記アクセス要求を前記サービス提供サーバに送信し、
前記サービス提供サーバは、前記ユーザの前記ユーザＩＤ及び前記アクセストークンを

検証することによって前記アクセス要求の正当性を確認する
ことを特徴とする請求項１又は２に記載のオンラインサービス提供システム。
【請求項６】
前記送信手段は、前記ユーザ認証により前記ユーザ機器を使用する者が正当であると確認された場合に、前記電子署名ＡＰＩを介して前記ＩＣチップの前記電子署名機能を利用して、前記オンラインサービスの手続に必要な情報を記述したメッセージに対し電子署名を行い、電子署名付きメッセージを含む手続要求をインターネットを通じて前記中間サーバに送信し、
前記中間サーバは、前記ユーザ機器から前記手続要求を受信した場合に、前記ユーザの電子証明書を用いて前記手続要求に含まれる前記電子署名付きメッセージを検証することによって前記手続要求の正当性を確認し、前記手続要求が正当であると確認された場合に前記手続要求に含まれる前記メッセージを含む手続実行要求を前記サービス提供サーバに送信し、
前記サービス提供サーバは、前記中間サーバから前記手続実行要求を受信した場合に、前記手続実行要求の正当性を確認し、前記手続実行要求が正当であると確認された場合に前記手続実行要求に含まれる前記メッセージに記述された情報に基づく手続を実行する
ことを特徴とする請求項１～５のいずれかに記載のオンラインサービス提供システム。
【請求項７】
前記中間サーバは、前記電子署名付きメッセージを含む前記手続実行要求を前記サービス提供サーバに送信し、
前記サービス提供サーバは、前記ユーザの電子証明書を用いて前記手続実行要求に含まれる前記電子署名付きメッセージを検証することによって前記手続実行要求の正当性を確認する
ことを特徴とする請求項６に記載のオンラインサービス提供システム。
【請求項８】
前記送信手段は、前記サービス提供サーバの公開鍵を用いて前記メッセージを暗号化した後、前記電子署名ＡＰＩを介して前記ＩＣチップの前記電子署名機能を利用して前記暗号化されたメッセージに対し電子署名を行う
ことを特徴とする請求項７に記載のオンラインサービス提供システム。
【請求項９】
前記中間サーバは、前記ユーザのユーザＩＤ及びパスワードとともに前記手続実行要求を前記サービス提供サーバに送信し、
前記サービス提供サーバは、前記ユーザの前記ユーザＩＤ及び前記パスワードを検証することによって前記手続実行要求の正当性を確認する
ことを特徴とする請求項６に記載のオンラインサービス提供システム。
【請求項１０】
前記中間サーバは、前記ユーザのユーザＩＤと前記サービス提供サーバが予め発行したアクセストークンとともに前記手続実行要求を前記サービス提供サーバに送信し、
前記サービス提供サーバは、前記ユーザの前記ユーザＩＤ及び前記アクセストークンを検証することによって前記手続実行要求の正当性を確認する
ことを特徴とする請求項６に記載のオンラインサービス提供システム。
【請求項１１】
前記中間サーバと前記サービス提供サーバとの間の通信が暗号化されている
ことを特徴とする請求項１～１０のいずれかに記載のオンラインサービス提供システム。
【請求項１２】
前記中間サーバと前記サービス提供サーバとの間が専用線で接続される
ことを特徴とする請求項１～１１のいずれかに記載のオンラインサービス提供システム。
【請求項１３】
前記中間サーバは、多段接続された複数の中間サーバから構成される
ことを特徴とする請求項１～１２のいずれかに記載のオンラインサービス提供システム。

【請求項１４】
　前記複数のＡＰＩは、前記メモリの内部に前記秘密鍵と前記公開鍵を生成する鍵生成機能を利用するための鍵生成ＡＰＩを含む
ことを特徴とする請求項１～１３のいずれかに記載のオンラインサービス提供システム。
【請求項１５】
　前記ＩＣチップは、前記ＩＣチップを一意に特定しうる識別情報を有しており、
　前記ユーザ機器と前記中間サーバ及び／又は前記サービス提供サーバとの間で、前記識別情報により前記ＩＣチップが特定された通信が行われる
ことを特徴とする請求項１～１４のいずれかに記載のオンラインサービス提供システム。
【請求項１６】
　前記アプリケーションプログラムは、前記中間サーバ及び／又は前記サービス提供サーバと前記ＩＣチップとの対応付けを行う対応付け情報を有しており、前記対応付け情報に基づいて、前記中間サーバ及び／又は前記サービス提供サーバとの通信において利用する前記ＩＣチップを特定する
ことを特徴とする請求項１～１４のいずれかに記載のオンラインサービス提供システム。
【請求項１７】
　前記ユーザ機器と前記中間サーバ及び／又は前記サービス提供サーバとの間で、前記ユーザ機器が備える通信用のＳＩＭカードのＩＭＳＩ又はそのＩＭＳＩに対応付けられたＩＰアドレスにより前記ＳＩＭカードが特定された通信が行われる
ことを特徴とする請求項１～１６のいずれかに記載のオンラインサービス提供システム。
【請求項１８】
　前記ユーザ機器が有する本体プロセッサにより実行され、前記ＩＣチップをセットアップするための機能を提供するセットアッププログラムを有している
ことを特徴とする請求項１～１７のいずれかに記載のオンラインサービス提供システム。
【請求項１９】
　前記セットアッププログラムは、前記ユーザ機器を、
　認証局に対して電子証明書の発行要求を送信する手段、および、
　前記認証局より前記電子証明書を受信し、前記ＩＣチップの前記メモリに前記電子証明書を格納する手段、
として機能させる
ことを特徴とする請求項１８に記載のオンラインサービス提供システム。
【請求項２０】
　前記セットアッププログラムは、前記ユーザ機器を、
　前記ユーザ機器が備える通信用のＳＩＭカードから電話番号及び／又はＩＭＳＩを読み出す手段、
　前記電話番号及び／又はＩＭＳＩを前記認証局に通知するための手段、
　前記認証局から前記電話番号又は前記ＩＭＳＩにより特定される宛先に送信された情報を受信する手段、
として機能させる
ことを特徴とする請求項１９に記載のオンラインサービス提供システム。
【請求項２１】
　前記情報は、ＳＭＳにより前記ユーザ機器に送信される
ことを特徴とする請求項２０に記載のオンラインサービス提供システム。
【請求項２２】
　前記情報は、インターネットを介したデータ通信により前記ユーザ機器に送信される
ことを特徴とする請求項２０に記載のオンラインサービス提供システム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明は、携帯機器からオンラインサービスを利用する際のセキュリティを向上する技

術に関する。
【背景技術】
【０００２】
インターネットの普及により多種多様なオンラインサービスが登場し、多くの人々に利用されている。一方で、サイバーセキュリティ問題は日増しに増大しているため、安心・安全にオンラインサービスを利用するためのセキュリティ対策が求められている。
【０００３】
例えば、オンラインバンキングサービスにおいては、昨今、中間者攻撃（ＭＩＴＭ：Man In The Middle）と呼ばれるサイバー攻撃による被害が急増している。ＭＩＴＭ攻撃は、マルウェアや偽サイトを使って、オンラインバンキングの利用者と金融機関との間の通信を乗っ取り（通信内容を改ざんし）、利用者と金融機関の双方に気づかれることなく不正な送金処理などを行う攻撃手法である。ＭＩＴＢ（Man In The Browser）もＭＩＴＭの一種である。なお、ＡＴＭ網を利用した送金処理は古くから行なわれていたが、従来は専用線を利用していたためサイバー攻撃のリスクは極めて低かった。これに対し、インターネットのようなオープンなネットワークを利用するオンラインサービスは、ＭＩＴＭ攻撃のような様々な脅威に晒されるのである。
【０００４】
現在のオンラインバンキングサービスでは、セキュリティ対策として、ワンタイムパスワード発行器を利用する方法が広く用いられている。これは、サービス利用者にあらかじめワンタイムパスワード発行器を配布しておき、サービスへのログイン時や送金処理を行う際などに、ワンタイムパスワード発行器で生成・表示されるワンタイムパスワードを使って認証を行うという方法である（特許文献１参照）。しかしこの方法は、ＭＩＴＭ攻撃に対しては効果がない。ＭＩＴＭ攻撃の一種であるＭＩＴＢ攻撃では、マルウェアや偽サイトによりログインＩＤやワンタイムパスワードなどの認証情報を利用者自身に入力させ、それらの認証情報をそのまま使って利用者へのなりすましを行うからである。
【０００５】
そこで最近では、ＭＩＴＭ攻撃への対策として「トランザクション認証」と呼ばれる対策をとる金融機関が増えてきている。トランザクション認証は、一般的に、利用者とサーバの間のトランザクションの暗号化（電子署名）と、ブラウザとは別経路のセッションを利用したトランザクション内容の確認との組み合わせにより実現される。トランザクション内容の確認には、トークンと呼ばれる専用のデバイスが利用されることが多い（特許文献２参照）。
【先行技術文献】
【特許文献】
【０００６】
【文献】特開２０１６－０７１５３８号公報
【文献】特開２０１２－０４８７２８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
トランザクション認証は、利用者とサーバの間のトランザクションに電子署名を行うため、ＭＩＴＭ攻撃には有効な対策である。しかしながら、現在主流であるハードウェアトークンを用いる方法はいくつかの課題が指摘されている。一つは、ユーザにとっての利便性の低さである。スマートフォンやタブレット端末などの携帯機器（モバイルデバイス）でオンラインサービスを利用することを想定した場合、ユーザは外出先に常にトークンを携帯しなければならず面倒である。しかも、サービスごとにトークンが異なるため、利用するサービスが増えるほど携帯するトークンの数も増えてしまい、実用性に欠ける。さらに、盗難や紛失のリスクを考慮すると、トークンを持ち歩くことに抵抗を感じる人も多い。二つ目は、サービス提供者の負担コストである。サービス提供者は、オンラインサービスの利用者全員にトークンを配布し管理する必要があり、そのコストは無視できない。

【０００８】
　また、銀行法改正（２０１８年６月施行）を受けて、各金融機関が、口座管理や電子送金などを代行する電子決済等代行業者に対して、ＡＰＩ（Application Programming Interface）を開放する動きが進んでいる。したがって、今後は、金融機関とユーザの２者間のセキュリティだけでなく、金融機関（オンラインサービスの提供者）と電子決済等代行業者（中間サービスの提供者）とユーザの３者間のセキュリティを確保する必要が出てくる。
【０００９】
　本発明は上記実情に鑑みなされたものであって、モバイルの利便性を損なうことなく、セキュアなサービス利用を実現可能な、新たなセキュリティ技術を提供することを目的とする。また、本発明のさらなる目的は、オンラインサービスの提供者と中間サービスの提供者とユーザの３者間の高度なセキュリティを確保することのできる、新たなセキュリティ技術を提供することにある。
【課題を解決するための手段】
【００１０】
　本発明の第一側面は、
　サービス提供者が提供するオンラインサービスを、前記サービス提供者とは異なる者が提供する中間サービスを介して、携帯機器から安全に利用可能な仕組みを提供するオンラインサービス提供システムであって、
　登録されたユーザに対し、インターネットを通じて前記オンラインサービスを提供するサービス提供サーバと、
　前記ユーザに対し、インターネットを通じて前記中間サービスを提供する中間サーバと、
　前記ユーザが所持している携帯機器であるユーザ機器に設けられるＩＣチップと、
　前記ユーザ機器が有する本体プロセッサにより実行され、前記ユーザ機器を前記中間サービスを利用するための端末として機能させるアプリケーションプログラムと、を有し、
　前記ＩＣチップは、
　　少なくとも、前記ユーザ機器を使用する者の正当性を確認するためのユーザ認証に用いられる本人情報、前記ユーザの秘密鍵、前記秘密鍵とペアになる前記ユーザの公開鍵、及び、前記公開鍵を含む前記ユーザの電子証明書を非一時的に記憶するメモリと、
　　少なくとも、前記アプリケーションプログラムから与えられる情報を前記本人情報と照合することにより前記ユーザ認証を行う認証機能、及び、前記アプリケーションプログラムから与えられるデータに対し前記秘密鍵を用いた電子署名を行う電子署名機能を有するプロセッサと、
を有しており、
　前記アプリケーションプログラムは、前記ユーザ機器を、
　　前記ユーザ機器を使用する者から取得した情報に基づき、前記ＩＣチップの前記認証機能を利用して、前記ユーザ認証を行うユーザ認証手段、及び、
　　前記ユーザ認証により前記ユーザ機器を使用する者が正当であると確認された場合に、前記ＩＣチップの前記電子署名機能を利用して電子署名を生成し、生成された前記電子署名を含むログイン要求をインターネットを通じて前記中間サーバに送信する送信手段、として機能させ、
　前記中間サーバは、
　　前記ユーザに関する情報として、前記ユーザの電子証明書を記憶するユーザ情報記憶手段と、
　　前記ユーザ機器から前記ログイン要求を受信した場合に、前記ユーザの電子証明書を用いて前記ログイン要求に含まれる前記電子署名を検証することによって前記ログイン要求の正当性を確認し、前記ログイン要求が正当であると確認された場合に前記ユーザ機器からの前記中間サービスの利用を許可すると共に、前記ログイン要求に含まれる前記電子署名を含むアクセス要求をインターネットを通じて前記サービス提供サーバに送信する制御手段と、

を有し、
前記サービス提供サーバは、
前記ユーザに関する情報として、前記ユーザの電子証明書を記憶するユーザ情報記憶手段と、
前記中間サーバから前記アクセス要求を受信した場合に、前記ユーザの電子証明書を用いて前記アクセス要求に含まれる前記電子署名を検証することによって前記アクセス要求の正当性を確認し、前記アクセス要求が正当であると確認された場合に前記中間サーバが前記ユーザの代わりに前記オンラインサービスを利用することを許可するアクセス制御手段と、
を有することを特徴とするオンラインサービス提供システムを提供する。

【００１１】
本発明の第二側面は、
ユーザが所持している携帯機器であるユーザ機器が有する本体プロセッサにより実行され、前記ユーザ機器を、サービス提供サーバがインターネットを通じて提供するオンラインサービスを前記サービス提供サーバとは異なる中間サーバが提供する中間サービスを介して利用するための端末として機能させるアプリケーションプログラムであって、
前記ユーザ機器には、
少なくとも、前記ユーザ機器を使用する者の正当性を確認するためのユーザ認証に用いられる本人情報、前記ユーザの秘密鍵、前記秘密鍵とペアになる前記ユーザの公開鍵、及び、前記公開鍵を含む前記ユーザの電子証明書を非一時的に記憶するメモリと、
少なくとも、前記アプリケーションプログラムから与えられる情報を前記本人情報と照合することにより前記ユーザ認証を行う認証機能、及び、前記アプリケーションプログラムから与えられるデータに対し前記秘密鍵を用いた電子署名を行う電子署名機能を有するプロセッサと、
を有するＩＣチップが設けられており、
前記アプリケーションプログラムは、前記ユーザ機器を、
前記ユーザ機器を使用する者から取得した情報に基づき、前記ＩＣチップの前記認証機能を利用して、前記ユーザ認証を行うユーザ認証手段、及び、
前記ユーザ認証により前記ユーザ機器を使用する者が正当であると確認された場合に、前記ＩＣチップの前記電子署名機能を利用して電子署名を生成し、生成された前記電子署名を含むログイン要求をインターネットを通じて前記中間サーバに送信する送信手段、
として機能させることを特徴とするアプリケーションプログラムを提供する。

【００１２】
本発明は、上記のサービス提供サーバ、又は、中間サーバ、又は、上記のＩＣチップとアプリケーションプログラムを備える携帯機器、又は、上記の処理の少なくとも一部を含むオンラインサービス提供方法、又は、上記のＩＣチップとアプリケーションプログラムによる処理の少なくとも一部を含む携帯機器の制御方法、又は、上記のアプリケーションプログラムを非一時的に記憶したコンピュータ読取可能な記憶媒体、として捉えることもできる。

【発明の効果】

【００１３】
本発明によれば、モバイルの利便性を損なうことなく、セキュアなサービス利用を実現可能な、新たなセキュリティ技術を提供することができる。また、本発明によれば、オンラインサービスの提供者と中間サービスの提供者とユーザの３者間の高度なセキュリティを確保することのできる、新たなセキュリティ技術を提供することができる。

【図面の簡単な説明】

【００１４】
【図１】図１は、本発明に係るオンラインサービス提供システムの特徴の一つを示す図である。
【図２】図２は、オンラインサービスを提供するサービス提供サーバの構成を示すブロッ

ク図である。
【図３】図３は、オンラインサービスを利用するために使用するユーザ機器の構成を示すブロック図である。
【図４】図４は、ＳＩＭカードとＩＣカードの外観及び装着形態を模式的に示す図である。
【図５】図５は、ＳＩＭカードとＩＣカードのハードウェア構成を模式的に示すブロック図である。
【図６】図６は、ユーザ機器とＩＣカードの論理的な構成を模式的に示すブロック図である。
【図７】図７は、ＩＣカードの発行手続を説明する図である。
【図８】図８は、ＩＣカードの発行手続を説明する図である。
【図９】図９は、ＩＣカード管理データベースのデータ構造を示す図である。
【図１０】図１０は、中間サービスへの登録手続の流れを示す図である。
【図１１】図１１は、中間サービスへの登録手続の流れ（図１０の続き）を示す図である。
【図１２】図１２は、中間サービスへの登録手続においてユーザ機器に表示される画面例である。
【図１３】図１３は、中間サービスのログイン認証の流れを示す図である。
【図１４】図１４は、中間サービスのログイン認証においてユーザ機器に表示される画面例である。
【図１５】図１５は、中間サービスの利用時の流れを示す図である。
【図１６】図１６は、中間サービスの利用時にユーザ機器に表示される画面例である。
【図１７】図１７は、セキュアエレメントを内蔵するユーザ機器のハードウェア構成を模式的に示すブロック図である。
【図１８】図１８は、ＳＩＭカードを備えるユーザ機器のハードウェア構成を模式的に示すブロック図である。
【図１９】図１９は、電子証明書のポストインストールを説明する図である。
【図２０】図２０は、ユーザ機器と中間サーバ又はサービス提供サーバとの間で通信を行う際に、ユーザ機器において利用されるＩＣチップを特定するための仕組みの一例を示す図である。
【図２１】図２１は、ユーザ機器と中間サーバ又はサービス提供サーバとの間で通信を行う際に、ユーザ機器において利用されるＩＣチップを特定するための仕組みの一例を示す図である。
【図２２】図２２は、中間サービスへの登録手続の流れを示す図である。
【図２３】図２３は、中間サービスのログイン認証の流れを示す図である。
【図２４】図２４は、中間サービスの利用時の流れを示す図である。
【図２５】図２５は、中間サービスへの登録手続の流れを示す図である。
【図２６】図２６は、中間サービスへの登録手続の流れを示す図である。
【図２７】図２７は、中間サービスのログイン認証の流れを示す図である。
【図２８】図２８は、中間サービスの利用時の流れを示す図である。
【図２９】図２９Ａ～図２９Ｃは、サーバの多段接続の例を示す図である。
【図３０】図３０は、中間サービスへの登録手続の流れを示す図である。
【図３１】図３１は、中間サービスのログイン認証の流れを示す図である。
【図３２】図３２は、中間サービスのログイン認証の流れを示す図である。
【図３３】図３３は、中間サービスの利用時の流れを示す図である。
【図３４】図３４は、中間サービスの利用時の流れを示す図である。
【発明を実施するための形態】
【００１５】
＜オンラインサービス提供システムの概要＞
図１は、本発明に係るオンラインサービス提供システムの特徴の一つである、サブＳＩＭと呼ばれるＩＣカードを利用した公開鍵暗号による手続内容署名（トランザクション署名）の流れを示している。図１において、サービス提供者は、インターネットを通じてオ

ンラインサービスを提供する者であり、例えば、オンラインバンキングサービスを提供する銀行などが該当する。中間サービス提供者は、サービス提供者が提供するオンラインサービスを代行（仲介）するサービス（本明細書では、これを「中間サービス」又は「代行サービス」と称す）を提供する者であり、例えば、口座管理や電子送金や収支管理などのＷＥＢサービスを提供する電子決済等代行業者などが該当する。

【００１６】

ユーザが所持するユーザ機器（スマートフォンなど）には、中間サービスを利用するためのアプリケーションプログラム（以下「アプリ（ＡＰＰ）」とも称す）がインストールされていると共に、サブＳＩＭと呼ばれるＩＣカードが装着されている。サブＳＩＭには、当該ユーザ固有の秘密鍵が格納されている。なお、日本国内で本サービスを実施する場合、秘密鍵のペアとなる公開鍵については、電子署名及び認証業務に関する法律（平成１２年法律第１０２号。以下、「電子署名法」という。）に基づく認定を受けている認証局に事前に登録され、認証局より電子証明書が発行されているものとする。

【００１７】

上記システムにおいて、ユーザがアプリから振込などの手続を行おうとすると、まず、ＰＩＮコード、パスワード、又は生体認証などによるユーザ認証（本人認証）が要求される。ユーザ認証に成功すると（つまり、アプリを操作している者がユーザ本人であることが確認されると）、サブＳＩＭの機能制限が解除され、サブＳＩＭが提供する機能を利用可能なモードとなる。アプリは、サブＳＩＭの機能を利用して、手続内容が記述された手続メッセージ（トランザクション）を秘密鍵で暗号化し電子署名を生成する。この電子署名と手続メッセージを中間サービスの中間サーバに送ると、該中間サーバが、対応する電子証明書を用いて電子署名の検証を行う。検証の結果、正当なユーザから送られてきた手続メッセージであり、かつ、内容が改ざんされていないことが確認されると、中間サーバは、電子署名と手続メッセージをオンラインサービスのサーバに転送する。すると、該サーバが、対応する電子証明書を用いて電子署名の検証を行い、正当なユーザから送られてきた手続メッセージであり、かつ、内容が改ざんされていないことが確認されると、手続メッセージの内容に従い振込などの手続を実行する。

【００１８】

このような方法によれば、「サービス提供者」と「中間サービス提供者」と「ユーザ」の３者の間で、公開鍵暗号を用いた高度なセキュリティを実現することができる。この方法は、ユーザ機器以外のデバイス（従来のトークンのようなもの）を持ち歩く必要がなく、ユーザ機器単体で中間サービスを介したオンラインサービスの利用を可能とするため、利便性が高い。また、本人認証だけで電子署名を用いたセキュアな手続が可能なため、スマートかつ簡便な操作性を実現できる。

【００１９】

さらに、サブＳＩＭと呼ばれるＩＣカードに格納された秘密鍵と、ＩＣカードが提供する暗号化機能を利用するため、セキュアなデータ通信を実現できる。この秘密鍵は漏えいのリスクが小さく、また、ＰＩＮコードやパスワードや生体認証による本人認証をクリアしなければ秘密鍵や暗号化機能を利用することもできないので、第三者による不正利用のリスクを可及的に小さくできる。

【００２０】

また、サービス提供者にとっては、トークンのようなデバイスを配布したり管理したりする必要がなくなり、運用コストの低減を期待できる。また電子署名法に基づく認定を受けている認証局が発行した電子証明書を利用して電子署名が付されたデータは、電子署名法第３条により、ユーザ本人が真正に作成したものと推定されるため、訴訟リスクを低減できるという利点もある。

【００２１】

＜中間サーバ＞

図２Ａは、中間サーバの構成を示すブロック図である。中間サーバ２１は、中間サービス提供者による中間サービスをインターネットを通じて提供するサーバである。以下、銀

行などの金融機関によるオンラインでの金融取引サービス（いわゆるオンラインバンキング）の各種手続を代行する中間サービスを例にとり、中間サーバ２１の説明を行うが、これはあくまで一つの適用例にすぎず、本発明はあらゆる種類の中間サービスに好ましく適用可能である。

【００２２】

中間サーバ２１は、主な機能として、ユーザ登録部２１０、ユーザ情報記憶部２１１、ログイン制御部２１２、代行制御部２１３を有する。ユーザ登録部２１０は、ユーザの新規登録処理を行う機能である。ユーザ情報記憶部２１１は、登録されたユーザの情報を記憶・管理するデータベースである。ログイン制御部２１２は、ユーザからのログイン要求に応答して中間サービスの利用の可否及びオンラインサービスのアクセスの可否を制御する機能である。代行制御部２１３は、ユーザからの手続要求に応答してオンラインサービスの該当手続の代行を制御する機能である。これらの機能及びその処理の詳細は後述する。

【００２３】

中間サーバ２１は、例えば、ＣＰＵ（プロセッサ）、メモリ（ＲＡＭ）、ストレージ（ＨＤＤ、ＳＳＤなど）、通信Ｉ／Ｆ、入出力装置などを備えた汎用のコンピュータにより構成することができる。その場合、上述した機能及びその処理は、ストレージに格納されたプログラムをメモリに展開し、ＣＰＵがプログラムを実行することによって実現される。なお、中間サーバ２１は、１台のコンピュータで構成してもよいし、分散コンピューティングやクラウドコンピューティングにより構成してもよい。また、汎用のコンピュータではなく、専用のコンピュータにより構成してもよいし、上述した機能又はその処理の一部をソフトウェアではなくＡＳＩＣやＦＰＧＡなどで構成してもよい。

【００２４】

＜サービス提供サーバ＞

図２Ｂは、サービス提供サーバの構成を示すブロック図である。サービス提供サーバ２０は、サービス提供者によるオンラインサービス（ＷＥＢサービス）をインターネットを通じて提供するサーバである。以下、銀行などの金融機関によるオンラインでの金融取引サービス（いわゆるオンラインバンキング）を例にとり、サービス提供サーバ２０の説明を行うが、これはあくまで一つの適用例にすぎず、本発明はあらゆる種類のオンラインサービスに好ましく適用可能である。

【００２５】

サービス提供サーバ２０は、主な機能として、ユーザ登録部２００、ユーザ情報記憶部２０１、アクセス制御部２０２、手続制御部２０３を有する。ユーザ登録部２００は、ユーザの新規登録処理を行う機能である。ユーザ情報記憶部２０１は、登録されたユーザの情報を記憶・管理するデータベースである。アクセス制御部２０２は、中間サーバ２１からのアクセス要求に応答してオンラインサービスのアクセスの可否を制御する機能である。手続制御部２０３は、中間サーバ２１からの手続要求に応答してオンラインサービスの該当手続の実行を制御する機能である。これらの機能及びその処理の詳細は後述する。

【００２６】

サービス提供サーバ２０は、例えば、ＣＰＵ（プロセッサ）、メモリ（ＲＡＭ）、ストレージ（ＨＤＤ、ＳＳＤなど）、通信Ｉ／Ｆ、入出力装置などを備えた汎用のコンピュータにより構成することができる。その場合、上述した機能及びその処理は、ストレージに格納されたプログラムをメモリに展開し、ＣＰＵがプログラムを実行することによって実現される。なお、サービス提供サーバ２０は、１台のコンピュータで構成してもよいし、分散コンピューティングやクラウドコンピューティングにより構成してもよい。また、汎用のコンピュータではなく、専用のコンピュータにより構成してもよいし、上述した機能又はその処理の一部をソフトウェアではなくＡＳＩＣやＦＰＧＡなどで構成してもよい。

【００２７】

＜ユーザ機器＞

図３は、ユーザが中間サービスを利用するために使用する携帯機器（「ユーザ機器」と称す）の構成を示すブロック図である。本実施形態では、ユーザ機器３０の一例としてス

マートフォンを例示するが、これはあくまで一つの適用例にすぎない。ユーザ機器３０としては、中間サービスを利用するためのアプリケーションプログラムを実行するためのプロセッサとメモリを有し、ＳＩＭカード（Subscriber Identity Module Card）が装着され、かつ、インターネットとの接続が可能な携帯型の電子機器であればいかなるデバイスを用いてもよい。スマートフォンの他、例えば、タブレット端末、モバイルＰＣ、ウェアラブルＰＣ、スマートウォッチ、スマートグラス、スマートウォレット、携帯ゲーム機などを例示できる。

【００２８】

ユーザ機器３０は、主なハードウェア資源として、ＣＰＵ（プロセッサ）３００、メモリ３０１、ストレージ３０２、タッチパネルディスプレイ３０３、通信モジュール３０４、電源３０５、ＳＩＭカード３０６、ＩＣカード３０７、ＮＦＣチップ３２０を有する。メモリ３０１はＲＡＭであり、ＣＰＵ３００がワーキングメモリとして使用する記憶領域を提供する。ストレージ３０２はアプリケーションプログラムや各種のデータを格納するための不揮発性の記憶媒体であり、例えば、内蔵のＥＥＰＲＯＭ、カードスロットに装着されるフラッシュメモリなどが該当する。タッチパネルディスプレイ３０３は、表示装置と入力装置を兼ねたデバイスである。通信モジュール３０４は、ユーザ機器３０によるデータ通信や音声通信を担うデバイスである。本実施形態の通信モジュール３０４は、３Ｇや４Ｇ／ＬＴＥなどの携帯電話網を利用した通信、Ｗｉ－Ｆｉによる通信、近距離無線通信などに対応しているものとする。電源３０５は、ユーザ機器３０に対し電力を供給するものであり、リチウムイオンバッテリと電源回路から構成される。ＳＩＭカード３０６は、携帯電話網を利用した通信の加入者情報が記録された接触型のＩＣカードである。ＩＣカード３０７も、ＳＩＭカード３０６と同じく接触型のＩＣカードである。ＩＣカード３０７は、中間サービス及びオンラインサービスのセキュアな利用を実現するためにユーザ機器３０に付加的に装着されたデバイスである。ＮＦＣチップ３２０は、ＮＦＣ（Near Field Communication）規格の近距離無線通信機能とそれを利用したアプリケーションを提供するＩＣチップである。なお、本実施形態では、ＳＩＭカード３０６、ＩＣカード３０７、ＮＦＣチップ３２０を別のハードウェアで構成したが、ＳＩＭカード３０６及び／又はＩＣカード３０７にＮＦＣの機能を搭載してもよい。

【００２９】

＜ＩＣカード＞

図４は、ＳＩＭカード３０６とＩＣカード３０７の外観及び装着形態を模式的に示し、図５は、ＳＩＭカード３０６とＩＣカード３０７のハードウェア構成を模式的に示すブロック図である。

【００３０】

ＳＩＭカード３０６は、幅１５ｍｍ×高さ１２ｍｍ×厚み０．７６ｍｍの樹脂プレート上にＩＣチップ４０が実装された構造を有する。図５に示すように、ＩＣチップ４０は、プロセッサ４０１、ＲＡＭ４０２、不揮発性メモリ４０３、及び、８つのピン（電極）４０４を有する。不揮発性メモリ４０３には、ＳＩＭカード３０６のユニークなシリアルナンバー（ＩＣＣＩＤ）、加入者識別情報（ＩＭＳＩ）などのデータと、プロセッサ４０１で実行されるプログラムとが格納されている。８つのピン４０４は、電源入力端子、リセット端子、クロック端子、アース端子、プログラム用電圧入力端子、Ｉ／Ｏ端子、予備端子を含む。

【００３１】

ＳＩＭカード３０６は、ユーザが移動体通信事業者（ＭＮＯ）又は仮想移動体通信事業者（ＭＶＮＯ）の提供する移動通信サービスに加入したときに、その事業者から提供されるものである。ＳＩＭカード３０６に格納されるデータやプログラムは事業者ごとに相違しているが、ＳＩＭカード３０６自体の基本的な構造は国際規格に準拠している限りにおいて同一である。なお、本実施形態では、ｍｉｃｒｏ－ＳＩＭを例に挙げたが、ＳＩＭカードとしてはｍｉｎｉ－ＳＩＭやｎａｎｏ－ＳＩＭを用いることもできる。

【００３２】

ＩＣカード３０７は、幅と高さがＳＩＭカード３０６と同じ又は略同じサイズであり、厚みが約０．１～０．２mm程度の可撓性フィルムにＩＣチップ４１が埋め込まれた構造を有する。ＩＣチップ４１も、プロセッサ４１１、ＲＡＭ４１２、不揮発性メモリ４１３、及び、８つのピン（電極）４１４を有している。ＩＣカード３０７の不揮発性メモリ４１３には、オンラインサービスのセキュアな利用を実現するためのデータ及びプログラムが格納される（詳細は後述する）。

【００３３】

ＩＣカード３０７の８つのピン４１４は、ＩＣカード３０７の表面と裏面の両方に露出しており、かつ、ＳＩＭカード３０６の８つのピン４０４と同じ配列になっている。図４に示すように、このＩＣカード３０７をＳＩＭカード３０６に重ねて貼り付けることにより、ＩＣカード３０７とＳＩＭカード３０６の対応するピン（電極）同士が物理的・電気的に接続されることとなる。ＩＣカード３０７は極めて薄いため、ＩＣカード３０７を貼り付けた状態のＳＩＭカード３０６をユーザ機器３０のＳＩＭカードスロット３０８に装着することが可能である。図５は、ＩＣカード３０７とＳＩＭカード３０６がＳＩＭカードスロット３０８に装着された状態を模式的に示している。ＩＣカード３０７の表面のピン４１４がユーザ機器３０の制御基板３０９の端子３１０に接続され、ＳＩＭカード３０６のピン４０４はＩＣカード３０７のピン４１４を介して制御基板３０９の端子３１０に接続されることとなる。

【００３４】

ユーザ機器３０のＣＰＵ３００は、ＩＣカード３０７とＳＩＭカード３０６のいずれに対しても選択的にアクセスすることができる。言い換えると、ユーザ機器３０のＣＰＵ３００で動作するアプリケーションプログラムは、ＩＣカード３０７と通信を行うモードとＳＩＭカード３０６と通信を行うモードを選択的に切り替えることができる。前者のモードの場合、ＩＣカード３０７のプロセッサ４１１は、ユーザ機器３０から受信した信号（命令）を自身で処理し、ＳＩＭカード３０６には伝送しない。他方、後者のモードの場合は、ＩＣカード３０７のプロセッサ４１１は、ユーザ機器３０とＳＩＭカード３０６の間の信号を仲介する（スルーする）動作を行う。本実施形態のように、通信用のＳＩＭカード３０６に重ね貼りするタイプのＩＣカード３０７は「サブＳＩＭ」とも呼ばれる。

【００３５】

サブＳＩＭタイプのＩＣカード３０７を用いることにより、次のようなメリットがある。ＳＩＭカードスロットを有する携帯機器であれば、ＩＣカード３０７の装着が可能である（すなわち、携帯機器側に特別な構造や細工が一切不要であり、ほとんど全ての携帯機器にＩＣカード３０７の装着が可能である）。ＳＩＭカードスロットが１つしかない携帯機器に対しても（言い換えると、ＳＩＭカードスロットの空きが無い場合でも）、ＩＣカード３０７を装着可能である。また、通信用のＳＩＭカード３０６とＩＣカード３０７とは機能的には完全に独立しており、互いに影響を与えることが無いため、ＩＣカード３０７を装着した後も音声通信やデータ通信をこれまで同様利用することができる。しかも、どの事業者のＳＩＭカードに対しても追加可能であるため、導入・普及が容易である。

【００３６】

＜ＩＣカードの機能＞

図６は、ユーザ機器３０とＩＣカード３０７の論理的な構成を模式的に示すブロック図である。

【００３７】

ユーザ機器３０には、中間サーバ２１が提供する中間サービスを利用するためのアプリケーションプログラム６０（以下単に「本体アプリ６０」と称す）がインストールされている。この本体アプリ６０は、中間サービス提供者（本実施形態の場合は電子決済等代行業者など）により配布されるプログラムであり、ユーザは中間サービスの利用に先立ちインターネット上のアプリケーションディストリビュータを通じて本体アプリ６０をダウンロードしインストールする。

【００３８】

本体アプリ６０は、主な機能として、メイン処理部６００、ユーザ認証部６０１、セキュリティ処理部６０２を有している。メイン処理部６００は、中間サービスの利用画面の表示や入力の制御、中間サーバ２１とのデータ送受信などを担う機能である。ユーザ認証部６０１は、ユーザ機器３０を使用する者の正当性を確認する処理を担う機能である。ここでのユーザ認証は、ユーザ機器３０を現に操作している者が正当な者（ユーザ本人、あるいは、正当なユーザから許可を受けている者）かどうかを確認することが目的である。セキュリティ処理部６０２は、ＩＣカード３０７の機能を利用してデータの暗号化や電子署名などのセキュリティ処理を実行する機能である。

【００３９】

ＩＣカード３０７の不揮発性メモリ４１３（以下単に「メモリ４１３」と称す）には、上述したユーザ認証に用いられる本人情報６１０、ユーザの秘密鍵６１１と公開鍵６１２のペア、ユーザの電子証明書６１３、ハッシュ関数６１４、プログラム６１５などが格納されている。メモリ４１３のアドレス空間は、外部からのアクセス（読み書き）が可能なエリア４１３０と、外部からのアクセスが不可能なエリア（つまりＩＣカード３０７のプロセッサ４１１しかアクセスできないエリア）４１３１とを有している。セキュリティ処理で用いるデータ（本人情報６１０、秘密鍵６１１、公開鍵６１２、電子証明書６１３、ハッシュ関数６１４、プログラム６１５など）はいずれもエリア４１３１内に格納され、外部（例えば本体アプリ６０など）からは直接に読み書きできないようになっている。ＩＣカード３０７のシリアル番号６１６、製造番号６１７などのデータはエリア４１３０内に格納され、外部から読み出し可能となっている。

【００４０】

ＩＣカード３０７のプロセッサ４１１は、外部のアプリに対して、セキュリティ機能に関するいくつかのＡＰＩ（Application Programming Interface）を提供する。図６では、一例として、認証機能６２０、暗号化機能６２１、電子署名機能６２２、本人情報変更機能６２３、鍵生成機能６２４、公開鍵読出機能６２５、電子証明書書込機能６２６、電子証明書読出機能６２７を示している。これらの機能は、プロセッサ４１１がプログラム６１５を実行することによって実現されるものである。

【００４１】

認証機能６２０は、外部から与えられる情報を、メモリ４１３に格納されている本人情報６１０と照合することにより、ユーザ認証を行う機能である。認証機能６２０以外の機能６２１～６２７は、ユーザ認証に成功しなければ利用できないようになっている。ユーザ認証の方法は何でもよい。例えばＰＩＮコード認証であれば、認証機能６２０は、本体アプリ６０のユーザ認証部６０１からユーザの入力したコード（例えば４ケタの数字）を受け取り、その入力コードが本人情報６１０として登録されているＰＩＮコードと一致するか確認し、一致していれば「ＯＫ」、一致していなければ「ＮＧ」という結果を返す。パスワード認証であれば、認証機能６２０は、本体アプリ６０のユーザ認証部６０１からユーザの入力したパスワード（例えば６～１６文字のパスワード）を受け取り、その入力パスワードが本人情報６１０として登録されているパスワードと一致するか確認し、一致していれば「ＯＫ」、一致していなければ「ＮＧ」という結果を返す。生体認証の場合であれば、認証機能６２０は、本体アプリ６０のユーザ認証部６０１からユーザの生体情報（顔画像、声紋、虹彩、指紋、静脈など）を受け取り、その生体情報から抽出される特徴と本人情報６１０として登録されている本人特徴とを比較することにより本人か否かを判定し、本人と判定されたら「ＯＫ」、そうでなければ「ＮＧ」という結果を返す。ＰＩＮコード認証とパスワード認証と生体認証のうちの２つ以上を組み合わせたり、さらに他の認証方法を組み合わせることで、さらに高度なセキュリティを実現してもよい。

【００４２】

暗号化機能６２１は、外部から与えられるデータに対し秘密鍵６１１を用いた暗号化を行う機能である。例えば、暗号化機能６２１は、本体アプリ６０のセキュリティ処理部６０２からデータを受け取り、そのデータを秘密鍵６１１を用いて暗号化し、暗号化されたデータ（暗号文）を返す。なお、暗号アルゴリズムはＲＳＡ、ＤＳＡ、ＥＣＤＳＡなどが

好ましいが、それら以外のアルゴリズムを利用してもよい。
【００４３】
電子署名機能６２２は、外部から与えられるデータに対し秘密鍵６１１を用いた電子署名を行う機能である。暗号化機能６２１との違いは、与えられたデータそのものを暗号化するのではなく、与えられたデータのハッシュ値を暗号化する点である。例えば、電子署名機能６２２は、本体アプリ６０のセキュリティ処理部６０２からデータを受け取り、ハッシュ関数６１４によりハッシュ値を計算し、ハッシュ値を秘密鍵６１１を用いて暗号化し、暗号化されたハッシュ値を返す。ハッシュ関数は何を用いてもよい（本実施形態では、ＳＨＡ－１とＳＨＡ－２５６を用いる）。なお、電子署名の対象となるデータのサイズが小さい場合には、ハッシュ値ではなく、データそのものを暗号化したものを電子署名として用いてもよい。
【００４４】
本人情報変更機能６２３は、本人情報６１０をメモリ４１３に書き込んだり、メモリ４１３に格納されている本人情報６１０を更新又は削除する機能である。本体アプリ６０がＩＣカード３０７に対しユーザの情報を新規登録したり変更したりする場合には、この機能を利用する。
【００４５】
鍵生成機能６２４は、秘密鍵６１１と公開鍵６１２の鍵ペアを生成する機能である。ＩＣカード３０７の初期状態においては、本人情報６１０、秘密鍵６１１、公開鍵６１２、電子証明書６１３などのユーザに紐付く情報はメモリ４１３内に格納されておらず、後述するＩＣカード発行手続のときにメモリ４１３に登録される（この操作をＩＣカードの活性化と呼ぶ）。このとき、秘密鍵６１１の生成とメモリ４１３への格納を、ＩＣカード３０７内の閉じられた空間の中で行う構成としたことで、秘密鍵６１１の漏えいリスクを低減することができる。なお、本実施形態では、メモリ４１３から秘密鍵６１１を読み出すＡＰＩを用意していないので、秘密鍵６１１が外部に漏えいするリスクはゼロに近い。
【００４６】
公開鍵読出機能６２５はメモリ４１３から公開鍵６１２を読み出す機能である。また、電子証明書書込機能６２６はメモリ４１３に電子証明書６１３を書き込む機能であり、電子証明書読出機能６２７はメモリ４１３から電子証明書６１３を読み出す機能である。公開鍵６１２や電子証明書６１３は通信の相手先に配布するためのものなので、外部に読み出すことができるようになっている。なお、電子証明書６１３の書き込みは、ＩＣカード発行手続のときに必要となる。
【００４７】
以上述べた構成によれば、ユーザ機器３０の本体アプリ６０は、ＩＣカード３０７を利用することにより公開鍵暗号によるデータの暗号化や電子署名を簡便に実現できる。また、ＩＣカード３０７の暗号化や電子署名の機能を利用するにはユーザ認証が必要であり、しかも秘密鍵の漏えいリスクはゼロに近いため、極めて堅牢なセキュリティが担保される。
【００４８】
＜ＩＣカードの発行手続＞
図７及び図８を参照して、ＩＣカード３０７の発行手続（ＩＣカードの活性化）を説明する。図７はＩＣカード発行端末を示す図であり、図８はＩＣカードの発行手続の流れを示す図である。
【００４９】
ＩＣカード発行端末７０は、ＩＣカード３０７の新規発行を行う端末であり、例えば、携帯電話ショップ、サービス提供者の店頭（銀行など）、コンビニエンスストア、代理店窓口などに設置される。ＩＣカード発行端末７０は、ＩＣカードのリーダ／ライタを備えたコンピュータにより構成される。店員が操作するのであれば、汎用のパーソナルコンピュータやタブレット端末で構成してもよいし、ユーザ（ＩＣカードの申込者）本人に操作させるのであれば、キオスク端末にしてもよい。
【００５０】

図８に沿って、発行手続の流れを説明する。ここで、「ユーザ」は、オンラインサービスを利用するためにＩＣカード３０７を新規に申し込む者である（図８の説明では、「ユーザ」又は「申込者」と称す）。「窓口」は、ＩＣカード発行端末７０を利用してＩＣカード３０７の発行業務を行う者である。「通信サービス管理者」は、ＩＣカード３０７の発行や運用の管理を担う者である。通信サービス管理者は、例えば、ＩＣカード３０７の提供、認証局への電子証明書の申請、発行済みＩＣカードの管理、ＩＣカード３０７とＳＩＭカード３０６の紐付け管理、ＩＣカード３０７の無効化（例えばユーザ機器３０の紛失・盗難・廃棄のとき）などの役割を担う。ＩＣカード３０７のセキュリティ機能は様々なオンラインサービスに利用できるため、通信サービス管理者はオンラインサービスのサービス提供者や中間サービス提供者とは異なる事業体で構成するとよい。「認証局」は公開鍵の電子証明書の発行及び失効を行う者である。

【００５１】

ＩＣカードの申込者は、まず、窓口においてＩＣカードの利用申請を行う（ステップＳ８００）。利用申請にあたっては、申込者の本人確認情報を伝えると共に、本人確認書類（運転免許証など）を提出する。本人確認情報は、例えば、氏名、性別、生年月日、住所を含むとよい。また申込者は、ＩＣカードに登録するＰＩＮコードを指定する。窓口スタッフは、申込者から伝えられた情報を本人確認書類により照合することにより本人確認を行った後、それらの情報をＩＣカード発行端末７０に入力する（ステップＳ８０１）。なお、ＰＩＮコードが窓口スタッフに知得されないよう、ＰＩＮコードの入力だけは申込者本人に行わせてもよい。

【００５２】

次に、窓口スタッフがＩＣカード発行端末７０に新規のＩＣカード３０７をセットし、活性化（アクティベート）処理の開始を指示する。この段階のＩＣカード３０７のメモリ４１３には、図６に示す情報のうち、「ハッシュ関数６１４、プログラム６１５」のみが格納されており、ユーザに紐付く情報である「秘密鍵６１１、公開鍵６１２、電子証明書６１３」は未だ格納されておらず、本人情報６１０のＰＩＮコードは初期値（例えば「００００」）である。まずＩＣカード発行端末７０は、認証機能６２０を利用して初期値のＰＩＮコードにより認証を行った後に、本人情報変更機能６２３を利用して申込者が指定したＰＩＮコードの登録を行うと共に、鍵生成機能６２４に鍵ペアの生成を指示して秘密鍵６１１と公開鍵６１２を生成させる（ステップＳ８０２）。ＰＩＮコードと鍵ペアはメモリ４１３の所定のエリア４１３１に書き込まれる。続いて、ＩＣカード発行端末７０は、公開鍵読出機能６２５を利用してメモリ４１３から公開鍵６１２を読み出し、この公開鍵６１２とステップＳ８０１で入力された本人確認情報とからＣＳＲ（Certificate Signing Request）を作成し、通信サービス管理者の管理サーバに送信する（ステップＳ８０３）。

【００５３】

管理サーバは、ＩＣカード発行端末７０からＣＳＲを受信すると、そのＣＳＲを所定の認証局に対し送信する（ステップＳ８０４）。このとき、管理サーバは、本人確認情報に基づいて申込者の与信調査を実施してもよい。

【００５４】

認証局は、受信したＣＳＲに従って申込者の公開鍵の電子証明書を発行し、管理サーバへ送付する（ステップＳ８０５）。電子証明書は公開鍵とその所有者を証明するものである。ＩＴＵ－Ｔにより策定されたＸ．５０９の場合、電子証明書は、公開鍵、所有者情報（本人確認情報が該当）、認証局の電子署名、電子証明書の有効期限、発行者の情報を含んだデータである。なお、認証局の電子署名は、電子証明書に含まれる公開鍵と所有者情報から生成したハッシュ値を認証局の秘密鍵で暗号化したものである。

【００５５】

管理サーバは、発行された電子証明書をＩＣカード発行端末７０に送信する（ステップＳ８０６）。ＩＣカード発行端末７０は、ＩＣカード３０７の電子証明書書込機能６２６を利用して電子証明書をメモリ４１３に書き込む（ステップＳ８０７）。この段階で、Ｉ

Ｃカード３０７のメモリ４１３には、セキュリティ処理に必要なデータである、本人情報６１０（本実施形態ではＰＩＮコード）、秘密鍵６１１、公開鍵６１２、電子証明書６１３が揃ったことになる。

【００５６】

次に、ＩＣカード３０７を申込者のユーザ機器３０に装着する（ステップＳ８０８）。具体的には、ユーザ機器３０から通信用のＳＩＭカード３０６を取り出し、ＳＩＭカード３０６上にＩＣカード３０７を貼り付けた後、再びユーザ機器３０にＳＩＭカード３０６を挿入する。さらに、セットアッププログラムをユーザ機器３０にインストールし、セットアッププログラムによるＩＣカード３０７のセットアップ処理を実行する。ＩＣカード３０７の装着及びセットアップは、窓口スタッフが行ってもよいし、申込者自身が行ってもよい。

【００５７】

セットアップ処理では、ユーザ機器３０（で動作するセットアッププログラム）が、ＩＣカード３０７から「シリアル番号」と「製造番号」を読み出すと共に、ＳＩＭカード３０６から「電話番号」と「製造番号」を読み出す。また、セットアッププログラムは、ユーザ機器３０自体の情報として「ＩＭＥＩ（International Mobile Equipment Identity）」を取得する。そしてセットアッププログラムは、それらの情報と共にＩＣカード登録要求を通信サービス管理者の管理サーバへ送信する（ステップＳ８０９）。管理サーバは、ユーザ機器３０からＩＣカード登録要求を受信すると、そこに含まれるＩＣカード３０７とＳＩＭカード３０６とユーザ機器３０の情報をＩＣカード管理データベースに登録する（ステップＳ８１０）。

【００５８】

図９はＩＣカード管理データベースに格納されているＩＣカード管理情報のデータ構造の一例である。ＩＣカード３０７の「シリアル番号」及び「製造番号」に紐付けて、ＳＩＭカード３０６の「電話番号」及び「製造番号」とユーザ機器３０の「ＩＭＥＩ」が管理されている。図示しないが、ＩＣカード管理情報として、ユーザの本人確認情報（氏名、性別、住所、生年月日）、公開鍵、電子証明書の情報などを管理してもよい。

【００５９】

ＩＣカード管理情報の登録が完了すると、管理サーバが、ユーザ機器３０に対して登録完了を通知する（ステップＳ８１１）。これによりユーザ機器３０のセットアップが完了し、ＩＣカード３０７が利用可能な状態（活性化状態）となる。

【００６０】

なお、図８に示した発行手順はあくまで一例であり、異なる手順で発行手続を行っても構わない。例えば、秘密鍵、公開鍵、電子証明書、ＰＩＮコードが予め登録されたＩＣカード３０７を窓口に用意しておいてもよい。この場合は、ＩＣカード３０７への書き込み処理が不要なため、ＩＣカード発行端末７０を用いる必要がなくなり、ユーザ機器３０でのセットアップ処理だけで済み、ＩＣカードの発行手続が簡便となる。また、ＰＩＮコード認証ではなく、生体認証を用いる場合には、ＩＣカード３０７に本人情報として登録する生体情報（顔画像、声紋、虹彩、指紋など）をＩＣカード発行端末７０などを利用して入力すればよい。

【００６１】

＜中間サービスへの初回登録＞

図１０、図１１、及び図１２を参照して、中間サービスへの初回登録手続を説明する。図１０及び図１１は、中間サービスへの登録手続の流れを示す図であり、図１２は、ユーザ機器３０に表示される画面例である。なお、この段階では、オンラインサービスへのユーザ登録は既に済んでおり、オンラインサービス自体にログインするためのＩＤ・パスワードはユーザに付与されているものとする。

【００６２】

まず、ユーザは、ユーザ機器３０を操作し、本体アプリ６０のダウンロード及びインストールを行う（ステップＳ１００１）。そして、ユーザは、本体アプリ６０を起動し、中

間サービスのログイン画面を開く（ステップＳ１００２）。図１２に示すように、初回のログイン時には、ログイン画面１２０において中間サービスのユーザＩＤとパスワードを入力し、中間サービスにログインする（ステップＳ１００３）。このとき、本体アプリ６０は、中間サービスのユーザＩＤを不揮発性メモリに記憶する（ステップＳ１００４）。パスワードについては、セキュリティの観点からユーザ機器３０には記憶させないほうがよい。なお、ユーザＩＤとパスワードは、別途の手続である中間サービスの新規利用申込を行ったときに、中間サービス提供者から付与される情報である。

【００６３】

ログインが完了すると、中間サーバ２１は、所定の電文（内容はどのようなものでもよい）をユーザ機器３０に送信し、電子署名と電子証明書を要求する（ステップＳ１００５）。

【００６４】

本体アプリ６０のユーザ認証部６０１は、図１２に示すように、ＰＩＮコード入力画面１２１を表示する。ユーザによりＰＩＮコードが入力されると、ユーザ認証部６０１は、ＩＣカード３０７の認証機能６２０を利用して、入力されたＰＩＮコードが正しいか否かを確認する（ステップＳ１００６）。ＰＩＮコードが正しい場合（つまり、ユーザ認証に成功した場合）は、本体アプリ６０からＩＣカード３０７の他の機能６２１～６２７を利用可能となる。本体アプリ６０のセキュリティ処理部６０２は、ＩＣカード３０７の電子署名機能６２２を利用して、中間サーバ２１から受信した電文に電子署名を行うと共に、電子証明書読出機能６２７を利用して、メモリ４１３から電子証明書６１３を読み出す。そして、本体アプリ６０のメイン処理部６００は、電子署名付き電文と電子証明書６１３を中間サーバ２１に送信する（ステップＳ１００７）。

【００６５】

中間サーバ２１は、ユーザ機器３０から受信した電子証明書６１３を用いて電子署名付き電文を検証する（ステップＳ１００８）。「検証」とは、電子証明書６１３に含まれる公開鍵によって電子署名付き電文を復号し、復号結果と元の電文との一致を調べることにより、電子署名がユーザ本人によって行われたこと（つまり、ユーザの秘密鍵によって電子署名が作成されたこと）を確認する操作である。なお、電子署名が電文そのものを暗号化したデータである場合は復号結果と元の電文とを比較すればよく、電子署名が電文のハッシュ値を暗号化したデータである場合は復号結果と元の電文のハッシュ値とを比較すればよい。

【００６６】

検証に成功した場合、中間サーバ２１は、当該ユーザのユーザＩＤ・パスワードと電子証明書を紐付けて、ユーザ情報記憶部２１１に登録する（ステップＳ１００９）。そして、中間サーバ２１は、電子証明書の登録が完了した旨を本体アプリ６０へ通知する（ステップＳ１０１０）。中間サービスへの登録が完了すると、図１２に示すように、ユーザ機器３０にはメニュー画面１２２が表示される（ステップＳ１０１１）。

【００６７】

続いて、ユーザと中間サービスとオンラインサービスの間の紐付けの手順を説明する。この紐付け処理は、ユーザが中間サービスを介してオンラインサービスの何らかの手続をはじめて利用したときや、ユーザが中間サービスのメニュー画面から銀行口座情報の登録を行ったときなどに実行される。図１０及び図１１では、ユーザが残高照会を行う例を示している。

【００６８】

ユーザがメニュー画面１２２から「残高照会」を選択し、対象となる銀行口座の情報（銀行名、口座番号、口座名義など）を入力すると、本体アプリ６０が中間サーバ２１に対し残高照会要求を送信する（ステップＳ１０１２）。中間サーバ２１の代行制御部２１３は、照会先の銀行のサービス提供サーバ２０に対し残高照会要求を行う（ステップＳ１０１３）。この残高照会要求には、ユーザの銀行口座情報が含まれている。

【００６９】

サービス提供サーバ２０のアクセス制御部２０２は、当該ユーザによる中間サーバ２１経由のアクセスが初回である場合には、ユーザに対しオンラインサービスのＩＤ・パスワードの入力を要請する（ステップＳ１０１４）。具体的には、図１２に示すように、ユーザ機器３０にオンラインサービスのログイン画面１２３が表示されるので（ステップＳ１０１５）、ユーザはオンラインサービスのユーザＩＤとパスワードを入力し、オンラインサービスにログインする（ステップＳ１０１６）。

【００７０】

ログインが完了すると、サービス提供サーバ２０は、認証用電文（内容はどのようなものでもよい）をユーザ機器３０に送信し、電子署名と電子証明書を要求する（ステップＳ１０１７）。

【００７１】

本体アプリ６０のユーザ認証部６０１は、図１２に示すように、ＰＩＮコード入力画面１２４を表示する。ユーザによりＰＩＮコードが入力されると、ユーザ認証部６０１は、ＩＣカード３０７の認証機能６２０を利用して、入力されたＰＩＮコードが正しいか否かを確認する（ステップＳ１０１８）。ＰＩＮコードが正しい場合（つまり、ユーザ認証に成功した場合）は、本体アプリ６０からＩＣカード３０７の他の機能６２１～６２７を利用可能となる。本体アプリ６０のセキュリティ処理部６０２は、ＩＣカード３０７の電子署名機能６２２を利用して、サービス提供サーバ２０から受信した認証用電文に電子署名を行うと共に、電子証明書読出機能６２７を利用して、メモリ４１３から電子証明書６１３を読み出す。そして、本体アプリ６０のメイン処理部６００は、電子署名付き認証用電文と電子証明書６１３をサービス提供サーバ２０に送信する（ステップＳ１０１９）。このとき、本体アプリ６０は、認証用電文を不揮発性メモリに記憶する（ステップＳ１０２０）。

【００７２】

サービス提供サーバ２０は、ユーザ機器３０から受信した電子証明書６１３を用いて電子署名付き認証用電文を検証する（ステップＳ１０２１）。検証に成功した場合、サービス提供サーバ２０は、当該ユーザと中間サービスの組に対し、アクセストークンを発行する。本実施形態では、ＯＡｕｔｈ２．０の仕組みを利用して、中間サーバ２１によるオンラインサービスの代行を実現する。アクセストークンとは、中間サーバ２１がユーザに代わりオンラインサービスを利用する際の許可証のようなものである。ユーザ登録部２００は、認証用電文とアクセストークンと当該ユーザの電子証明書を紐付けて、ユーザ情報記憶部２０１に登録する（ステップＳ１０２３）。

【００７３】

そして、サービス提供サーバ２０は、発行したアクセストークンと当該ユーザの口座残高の情報を中間サーバ２１へ通知する（ステップＳ１０２４）。中間サーバ２１は、受け取ったアクセストークンと当該ユーザの中間サービスのＩＤとを紐付けて、ユーザ情報記憶部２１１に登録する（ステップＳ１０２５）。なお、図示しないが、中間サーバ２１は、サービス提供サーバ２０から、アクセストークンと共にリフレッシュトークンも受け取る。リフレッシュトークンは、アクセストークンの再発行に利用されるトークンである。これはＯＡｕｔｈ２．０の仕様であるため、ここでは詳しい説明は割愛する。

【００７４】

その後、中間サーバ２１は、口座残高の情報を本体アプリ６０へ通知する（ステップＳ１０２６）。図１２に示すように、ユーザ機器３０には口座残高の確認画面１２５が表示される（ステップＳ１０２７）。

【００７５】

＜中間サービスへのログイン＞

図１３及び図１４を参照して、中間サービスのログイン認証を説明する。図１３は、中間サービスのログイン認証の流れを示す図であり、図１４は、ユーザ機器３０に表示される画面例である。

【００７６】

ユーザが、ユーザ機器３０において本体アプリ６０を起動すると、ユーザ認証部６０１が、図１４に示すように、ＰＩＮコード入力画面１４０を表示する（ステップＳ１３００）。ユーザによりＰＩＮコードが入力されると、ユーザ認証部６０１は、ＩＣカード３０７の認証機能６２０を利用して、入力されたＰＩＮコードが正しいか否かを確認する（ステップＳ１３０１）。ＰＩＮコードが正しい場合（つまり、ユーザ認証に成功した場合）、本体アプリ６０のセキュリティ処理部６０２は、ＩＣカード３０７の電子署名機能６２２を利用して、中間サービスのユーザＩＤと認証用電文に対し電子署名を行う（ステップＳ１３０２）。そして、本体アプリ６０のメイン処理部６００は、ログイン要求を中間サーバ２１に送信する（ステップＳ１３０３）。ログイン要求には、中間サービスのユーザＩＤ、認証用電文、電子署名が付加されている。

【００７７】

中間サーバ２１のログイン制御部２１２は、ログイン要求を受信すると、ログイン要求に含まれるユーザＩＤに基づいて、ユーザ情報記憶部２１１から対応する電子証明書を読み出し、この電子証明書を用いて、ログイン要求に含まれている電子署名の検証を行う（ステップＳ１３０４）。また、必要に応じて、ログイン制御部２１２は、電子証明書の有効性を認証局に問い合わせてもよい（ステップＳ１３０５、Ｓ１３０６）。電子署名の検証に成功し、且つ、電子証明書の有効性が確認された場合、ログイン制御部２１２は、ログイン要求が正当なユーザからのものであると判断する。

【００７８】

続いて、中間サーバ２１のログイン制御部２１２は、ログイン要求に含まれるユーザＩＤに基づいて、ユーザ情報記憶部２１１からオンラインサービスのアクセストークンを読み出し、サービス提供サーバ２０にアクセス要求を送信する（ステップＳ１３０７）。このアクセス要求には、アクセストークンと、ログイン要求に含まれていた認証用電文及び電子署名とが付加されている。

【００７９】

サービス提供サーバ２０のアクセス制御部２０２は、アクセス要求を受信すると、アクセス要求に含まれるアクセストークンに基づいて、ユーザ情報記憶部２０１から対応する電子証明書を読み出し、この電子証明書を用いて、アクセス要求に含まれている電子署名の検証を行う（ステップＳ１３０８）。また、必要に応じて、アクセス制御部２０２は、電子証明書の有効性を認証局に問い合わせてもよい（ステップＳ１３０９、Ｓ１３１０）。電子署名の検証に成功し、且つ、電子証明書の有効性が確認された場合、アクセス制御部２０２は、アクセス要求が、ユーザから代行権限が与えられた中間サーバ２１からのものであると判断し、中間サーバ２１に対しアクセス許可を与える（ステップＳ１３１１）。

【００８０】

オンラインサービスのアクセス許可が得られたら、中間サーバ２１は、ログイン認証ＯＫを本体アプリ６０に通知する（ステップＳ１３１２）。以後、図１４に示すように、ユーザ機器３０に中間サービスのメニュー画面１４１が表示され、ユーザは希望する手続を行うことができようになる。

【００８１】

以上述べたログイン認証によれば、ユーザはＰＩＮコードを入力するだけでよいので、従来のＩＤ・パスワードを都度入力する方法や、トークンを用いる方法に比べて、非常に簡便な操作でログインが可能となる。しかも、ＩＣカード３０７により提供されるセキュリティ機能を利用しているため、高度のセキュリティも担保されている。

【００８２】

また、本実施形態の方法は、オンラインサービスのＩＤ・パスワードの情報を中間サービス側に一切提供することなく、中間サービスとオンラインサービスとの紐付けが可能となる。したがって、オンラインバンキングのＩＤ・パスワードを別の事業者に開示することに抵抗を感じる利用者でも、安心してこのサービスを利用することができる。

【００８３】

＜オンラインサービスの利用＞

図１５及び図１６を参照して、中間サービス利用時の手順を説明する。図１５は、中間サービス利用時の流れを示す図であり、図１６は、ユーザ機器３０に表示される画面例である。中間サービスへのログインは既に完了しており、ユーザ機器３０にはメニュー画面１６０が表示されているものとする。

【００８４】

ユーザがメニュー画面１６０から利用したい手続を選択すると、詳細画面１６１に遷移する（ステップＳ１５００）。図１６では、ユーザが「振込」を選択した場合の画面例が示されている。この詳細画面１６１においてユーザが必要な情報（例えば振込先、振込額など）を入力し、実行ボタンを押すと（ステップＳ１５０１）、本体アプリ６０のメイン処理部６００が、振込手続に必要な情報を記述した手続メッセージを作成する（ステップＳ１５０２）。

【００８５】

続いて、本体アプリ６０のユーザ認証部６０１が、ＰＩＮコード入力画面１６２を表示し、ＰＩＮコード認証を行う（ステップＳ１５０３）。ＰＩＮコード認証の手順は前述したものと同様のため、説明を省略する。ＰＩＮコード認証に成功した場合、本体アプリ６０のセキュリティ処理部６０２は、ＩＣカード３０７の電子署名機能６２２を利用して、手続メッセージに対し電子署名を行う（ステップＳ１５０４）。このとき、電子署名機能６２２は、手続メッセージのハッシュ値を計算し、このハッシュ値を秘密鍵６１１で暗号化することにより電子署名を生成してもよいし、手続メッセージ自体を秘密鍵６１１で暗号化することにより電子署名を生成してもよい。そして、本体アプリ６０のメイン処理部６００は、手続要求を中間サーバ２１に送信する（ステップＳ１５０５）。手続要求には、中間サービスのＩＤ、手続メッセージ、電子署名が付加されている。

【００８６】

中間サーバ２１の代行制御部２１３は、手続要求を受信すると、手続要求に含まれるユーザＩＤに基づいて、ユーザ情報記憶部２１１から対応する電子証明書を読み出し、この電子証明書を用いて、手続要求に含まれている電子署名の検証を行う（ステップＳ１５０６）。また、必要に応じて、代行制御部２１３は、電子証明書の有効性を認証局に問い合わせてもよい（ステップＳ１５０７、Ｓ１５０８）。電子署名の検証に成功し、且つ、電子証明書の有効性が確認された場合、代行制御部２１３は、手続要求が正当なユーザからのものであると判断する。すなわち、第三者によるなりすましがなく、かつ、手続メッセージの内容も改ざんされていないと判断するのである。

【００８７】

手続要求が正当なユーザからのものであると確認できた場合、代行制御部２１３は、手続要求に含まれるユーザＩＤ及び手続メッセージに基づいて、ユーザ情報記憶部２１１から対応するオンラインサービスのアクセストークンを読み出し、サービス提供サーバ２０に手続要求を送信する（ステップＳ１５０９）。この手続要求には、アクセストークンと、ユーザ機器３０から受信した手続メッセージ及び電子署名とが付加されている。

【００８８】

サービス提供サーバ２０の手続制御部２０３は、手続要求を受信すると、手続要求に含まれるアクセストークンに基づいて、ユーザ情報記憶部２０１から対応する電子証明書を読み出し、この電子証明書を用いて、手続要求に含まれている電子署名の検証を行う（ステップＳ１５１０）。また、必要に応じて、手続制御部２０３は、電子証明書の有効性を認証局に問い合わせてもよい（ステップＳ１５１１、Ｓ１５１２）。電子署名の検証に成功し、且つ、電子証明書の有効性が確認された場合、手続制御部２０３は、この手続要求が正当なユーザからのものであると判断する。すなわち、第三者によるなりすましがなく、かつ、手続メッセージの内容も改ざんされていないと判断するのである。

【００８９】

手続要求が正当なユーザからのものであると確認できた場合にのみ、手続制御部２０３は、手続メッセージに記述された情報に基づく手続（振込など）を実行する（ステップＳ１５１３）。手続が完了すると、手続制御部２０３は手続完了通知を中間サーバ２１に送

信し（ステップＳ１５１４）、中間サーバ２１が手続完了通知を本体アプリ６０に送信する（ステップＳ１５１５）。そうすると、図１６に示すように、手続完了画面１６３が表示される。

【００９０】

以上述べた処理によれば、ユーザはＰＩＮコードを入力するだけでよいので、従来のＩＤ・パスワードを都度入力する方法や、トークンを用いる方法に比べて、非常に簡便な操作で中間サービス及びオンラインサービスの利用が可能となる。しかも、ＩＣカード３０７により提供されるセキュリティ機能を利用しているため、高度のセキュリティも担保され、いわゆる中間者攻撃によるなりすましや手続メッセージの改ざんを防止することが可能となる。

【００９１】

なお、図１５の例では、ユーザ機器３０から送られる手続要求に平文の手続メッセージが含まれている。これは、中間サーバ２１（中間サービス提供者）でも手続メッセージの改ざんが行われていないかを検証できるようにするためである。しかしながら、場合によっては、手続メッセージの中に、サービス提供者以外の者に知られたくない情報もしくは伝える必要の無い情報が含まれていることも想定される。例えば、オンラインで住所変更手続を行う際には、その手続メッセージの中に変更後の住所情報が含まれることとなるが、住所のような個人情報はプライバシーに関わるため、中間サービス提供者に知られたくないと希望するユーザは少なくない。また、銀行は住所情報を管理する法的義務があるが、中間サービス提供者にはその義務はないため、中間サービス提供者の側も、必要のない個人情報は受け取りを避けたいと考えるかもしれない。

【００９２】

そこで、ユーザ機器３０がサービス提供サーバ２０（サービス提供者）の公開鍵を用いて手続メッセージを暗号化してもよい。すなわち、ユーザ機器３０の本体アプリ６０が、住所変更手続などの手続メッセージをサービス提供サーバ２０の公開鍵により暗号化した後、暗号化された手続メッセージに対しユーザの秘密鍵６１１による電子署名を行い、ＩＤ・暗号化された手続メッセージ・電子署名を含む手続要求を中間サーバ２１に送信するのである。

【００９３】

この方法によれば、中間サーバ２１は、電子署名を検証することによって、手続要求が正当なユーザから送られてきたものであることは確認できるが、手続メッセージの内容を確認することはできない。一方、サービス提供サーバ２０は、自身が保管する秘密鍵を用いて手続メッセージを復号することにより、手続メッセージの内容（ユーザの住所情報など）を確認でき、手続を遂行することができる。したがって、中間サービス提供者による中間サービスを経由しつつも、中間サービス提供者には秘匿した状態で、サービス提供者にのみ情報を伝達する、という仕組みが実現できる。

【００９４】

＜ＩＣカードの無効化＞

本実施形態のユーザ機器３０によれば、ＰＩＮコードや生体情報によるユーザ認証に成功しなければ、中間サービス及びオンラインサービスを利用することができない。したがって、仮にユーザ機器３０の紛失や盗難が起きた場合でも、第三者によるユーザ機器３０の不正使用のリスクは小さい。とはいえ、ＰＩＮコード認証や生体認証が破られる可能性はゼロではないことから、好ましくは、以下に述べるようなＩＣカードの無効化機能を実装するとよい。

【００９５】

（１）ＩＣカードの自滅機能

自滅とは、ＩＣカード３０７のプロセッサ４１１自身がＩＣカード３０７の機能を無効化する操作である。具体的な操作としては、外部（本体アプリ６０）からＩＣカード３０７の機能を利用できないようにロックをかけたり、メモリ４１３に格納されているデータ（鍵ペア、電子証明書など）を消去したりする方法などがある。例えば、誤ったＰＩＮコ

ードが連続して所定回数入力された場合、ＡＰＩ以外の方法でメモリ４１３へのアクセスが行われた場合などに、プロセッサ４１１は自滅を実行するとよい。

【００９６】

（２）ＩＣカードの無効化

通信サービス管理者が、ユーザから、ユーザ機器３０又はＩＣカード３０７の紛失・盗難の報告を受けた場合に、管理サーバからユーザ機器３０又はＩＣカード３０７に対して無効化信号を送信し、ＩＣカード３０７を無効化してもよい。あるいは、管理サーバが、ＩＣカード３０７の使用状況を監視し、異常を検知した場合（例えば、不使用状態が長期間続いた場合、使用頻度が突然増加した場合、大金を送金しようとした場合など）にＩＣカード３０７を無効化してもよい。あるいは、管理サーバが、ＩＣカード３０７とＳＩＭカード３０６とユーザ機器３０の組み合わせを監視し、ＩＣカード管理情報で管理されている情報との齟齬を検知した場合（例えば、ＩＣカードが単独又はＳＩＭカードと一緒に抜き取られ、他の携帯機器に装着された場合などに、そのような齟齬が発生し得る）にＩＣカード３０７を無効化してもよい。無効化の方法も、外部（本体アプリ６０）からＩＣカード３０７の機能を利用できないようにロックをかけたり、メモリ４１３に格納されているデータ（鍵ペア、電子証明書など）を消去したりする方法などがある。

【００９７】

（３）電子証明書の無効化

通信サービス管理者が、ユーザから、ユーザ機器３０又はＩＣカード３０７の紛失・盗難の報告を受けた場合に、管理サーバから認証局に対して当該ユーザの電子証明書の無効化を依頼してもよい。あるいは、管理サーバが、ＩＣカード３０７の使用状況やＩＣカード・ＳＩＭカード・ユーザ機器の組み合わせを監視し、異常を検知した場合に認証局に電子証明書の無効化を依頼してもよい。

【００９８】

＜その他＞

上述した実施形態は本発明の具体例の一つを説明したにすぎず、本発明の技術的範囲は上述した実施形態の内容に限定されるものではなく、また本発明はその技術思想の範囲内で様々な具体的形態を採り得るものである。例えば、本発明はオンラインバンキングサービス以外にも様々な種類のオンラインサービスに適用することができる。また、上述した実施形態ではサブＳＩＭタイプのＩＣカードを例示したが、ＳＩＭカードスロットを複数備える携帯機器であれば、一般的なｍｉｃｒｏ－ＳＩＭやｎａｎｏ－ＳＩＭと同じ仕様のＩＣカードを（通信用ＳＩＭカードとは別のスロットに）装着してもよい。あるいは、ＳＩＭカードスロット以外のスロットに装着するタイプのＩＣカードを用いてもよいし、携帯機器に内蔵されたＩＣチップ（例えばSecure Elementなど）を用いてもよい。また、上述した実施形態では、ログイン要求の中に電子署名付きユーザＩＤのみ含めたが、さらに電子証明書を一緒に送ってもよい。また、上述した実施形態では、ユーザ機器から中間サーバに送るデータにのみ電子署名を行ったが、中間サーバやサービス提供サーバがユーザ機器に送るデータに対し電子署名や暗号化を行うことも好ましい。その場合、中間サーバやサービス提供サーバは、自身の暗号鍵で電子署名や暗号化を行ってもよいし、ユーザの公開鍵で暗号化を行ってもよい。

【００９９】

＜セキュアエレメント＞

上述した実施形態では、サブＳＩＭタイプのＩＣカードによって暗号化機能（セキュリティ機能）を提供したが、暗号化機能の全部又は一部を、ユーザ機器３０に内蔵もしくは接続されたセキュアエレメント１６００によって提供してもよい。図１７は、セキュアエレメント１６００を内蔵するユーザ機器３０のハードウェア構成を模式的に示すブロック図である。

【０１００】

セキュアエレメント１６００とは格納したデータを外部から解析されることへの耐性（耐タンパー性）を持ち、主に機密情報を管理するために用いられるＩＣチップである。セ

キュアエレメント１６００は、ユーザ機器３０本体の制御基板３０９（プロセッサ１６１１、ＲＡＭ１６１２、不揮発性メモリ１６１３を有する）とは独立したＩＣチップであり、プロセッサ１６０１、ＲＡＭ１６０２、不揮発性メモリ１６０３を有している。セキュアエレメント１６００はユーザ機器３０本体のプロセッサ１６１１などと通信を行う。

【０１０１】

暗号化機能をセキュアエレメント１６００により提供する場合、暗号化機能で用いるデータ（図６に示す、本人情報６１０、秘密鍵６１１、公開鍵６１２、電子証明書６１３、ハッシュ関数６１４、プログラム６１５など）はセキュアエレメント１６００内の不揮発性メモリ１６０３に格納されるとよい。また、暗号化機能（図６に示す、認証機能６２０、暗号化機能６２１、電子署名機能６２２、本人情報変更機能６２３、鍵生成機能６２４、公開鍵読出機能６２５、電子証明書書込機能６２６、電子証明書読出機能６２７など）はセキュアエレメント１６００のプロセッサ１６０１がプログラム６１５を実行することにより提供されるとよい。

【０１０２】

以上述べた構成によれば、ユーザ機器以外のデバイス（従来のトークンのようなもの）を持ち歩く必要がなく、ユーザ機器単体でオンラインサービスの利用が可能となるため、利便性が高い。また、アプリの起動と本人認証だけで自動ログインが可能なため、スマートかつ簡便な操作性を実現できる。さらに、セキュアエレメント１６００に格納された秘密鍵と、セキュアエレメント１６００が提供する暗号化機能を利用するため、セキュアなデータ通信を実現できる。この秘密鍵は漏えいのリスクが小さく、また、ＰＩＮコードやパスワードや生体認証による本人認証をクリアしなければ秘密鍵や暗号化機能を利用することもできないので、第三者による不正利用のリスクを可及的に小さくできる。

【０１０３】

＜ＳＩＭカード＞

暗号化機能の全部又は一部が、ユーザ機器３０に内蔵もしくは接続されたＳＩＭカードによって提供されてもよい。図１８は、ＳＩＭカード１７００を備えるユーザ機器３０のハードウェア構成を模式的に示すブロック図である。

【０１０４】

ＳＩＭカード１７００は、プロセッサ１７０１、ＲＡＭ１７０２、不揮発性メモリ１７０３、及び、８つのピン１７０５（電極）を有する。不揮発性メモリ１７０３には、ＳＩＭカード１７００のユニークなシリアルナンバー（ＩＣＣＩＤ）、加入者識別情報（ＩＭＳＩ）などのデータと、暗号化機能で利用するデータと、プロセッサ１７０１で実行されるプログラムとが格納されている。８つのピン１７０５は、電源入力端子、リセット端子、クロック端子、アース端子、プログラム用電圧入力端子、Ｉ／Ｏ端子、予備端子を含む。

【０１０５】

図１８は、ＳＩＭカード１７００がＳＩＭカードスロット１７０４に装着された状態を模式的に示している。ＳＩＭカード１７００のピン１７０５がユーザ機器３０の制御基板３０９の端子１７０６に接続される。

【０１０６】

ＳＩＭカード１７００は、ユーザが移動体通信事業者（ＭＮＯ）又は仮想移動体通信事業者（ＭＶＮＯ）の提供する移動通信サービスに加入したときに、その事業者から提供されるものである。ＳＩＭカード１７００に格納されるデータやプログラムは事業者ごとに相違しているが、ＳＩＭカード１７００自体の基本的な構造は国際規格に準拠している限りにおいて同一である。ＳＩＭカード１７００としては、標準－ＳＩＭ、ｍｉｃｒｏ－ＳＩＭ、ｎａｎｏ－ＳＩＭのいずれのタイプを用いてもよい。

【０１０７】

暗号化機能をＳＩＭカード１７００により提供する場合、暗号化機能で用いるデータ（図６に示す、本人情報６１０、秘密鍵６１１、公開鍵６１２、電子証明書６１３、ハッシュ関数６１４、プログラム６１５など）はＳＩＭカード１７００内の不揮発性メモリ１７０３に格納されるとよい。また、暗号化機能（図６に示す、認証機能６２０、暗号化機能

６２１、電子署名機能６２２、本人情報変更機能６２３、鍵生成機能６２４、公開鍵読出機能６２５、電子証明書書込機能６２６、電子証明書読出機能６２７など）はＳＩＭカード１７００のプロセッサ１６０１がプログラム６１５を実行することにより提供されるとよい。

【０１０８】

以上述べた構成によれば、ユーザ機器以外のデバイス（従来のトークンのようなもの）を持ち歩く必要がなく、ユーザ機器単体でオンラインサービスの利用が可能となるため、利便性が高い。また、アプリの起動と本人認証だけで自動ログインが可能なため、スマートかつ簡便な操作性を実現できる。さらに、ＳＩＭカード１７００に格納された秘密鍵と、ＳＩＭカード１７００が提供する暗号化機能を利用するため、セキュアなデータ通信を実現できる。この秘密鍵は漏えいのリスクが小さく、また、ＰＩＮコードやパスワードや生体認証による本人認証をクリアしなければ秘密鍵や暗号化機能を利用することもできないので、第三者による不正利用のリスクを可及的に小さくできる。

【０１０９】

＜電子証明書のポストインストール＞

図１９を用いて、電子証明書のポストインストールについて説明する。図８に示した手順では、窓口において電子証明書がインストールされたＩＣカードをユーザに引き渡したのに対し、図１９に示す手順（ポストインストール）では、ユーザ機器に内蔵又は接続されたＩＣカードやＩＣチップに後から電子証明書を書き込むことができる点が異なる。

【０１１０】

ＩＣカードの申込者（ユーザ）は、まず、窓口においてＩＣカードの利用申請を行う（ステップＳ１８００）。利用申請にあたっては、ユーザの本人確認情報及び電話番号を手続端末に入力すると共に、本人確認書類（運転免許証、住民票など）を提出する。本人確認情報は、例えば、氏名、性別、生年月日、住所を含むとよい。電話番号は、ユーザ機器３０に装着された通信用のＳＩＭカードに割り当てられた電話番号である。ユーザは、これらの本人確認情報及び電話番号を手続端末に入力する（ステップＳ１８０１）。本人確認書類については、手続端末に備えられたカメラ又はスキャナによって電子データ化（例えば画像データ）されるとよい。手続端末は本人確認情報と本人確認書類と電話番号を通信サービス管理者に送信する（ステップＳ１８０２）。なお、ここではユーザが自ら手続端末を操作し、必要な情報を入力する手順を想定するが、図８の場合と同じように窓口スタッフが入力を代行してもよい。

【０１１１】

一方、ユーザは、暗号化機能をインストール及びアクティベートするための所定のプログラム（「セットアッププログラム」と呼ぶ）をユーザ機器３０にインストールする（図６に示す本体アプリ６０がセットアッププログラムを兼ねていてもよい）。そして、ユーザ機器３０のプロセッサは、セットアッププログラムによって、通信用のＳＩＭカードから電話番号とＩＭＳＩを読み込み（ステップＳ１８０３）、ＳＩＭカードの電話番号とＩＭＳＩを通信サービス管理者に送信する（ステップＳ１８０４）。

【０１１２】

この後、ユーザは、ＩＣカードを受け取り、ユーザ機器３０に装着する。この段階のＩＣカードのメモリには、図６に示す情報のうち、「ハッシュ関数、プログラム」のみが格納されており、ユーザに紐付く情報である「秘密鍵、公開鍵、電子証明書」は未だ格納されていない。

【０１１３】

通信サービス管理者は、電話番号をキーとして、ユーザ機器３０から受信した情報と手続端末から受信した情報の対応をとり、本人確認情報と本人確認書類とＳＩＭカードの電話番号及びＩＭＳＩとを紐づけて記憶する。そして、通信サービス管理者は、本人確認情報を本人確認書類と照合し、情報に齟齬がないかをチェックすることにより本人確認を行う（ステップＳ１８０６）。本人確認完了後、通信サービス管理者は、証明書発行依頼とユーザ機器３０から受信した通信用ＳＩＭカードの電話番号及び／又はＩＭＳＩを認証局

に送信する（ステップＳ１８０７）。なお、本例では電話番号及び／又はＩＭＳＩをユーザ機器３０が通信サービス管理者を介して間接的に認証局に通知したが、電話番号及び／又はＩＭＳＩをユーザ機器３０が直接的に認証局に通知してもよい。また、本例では本人確認書類の電子データを通信サービス管理者にネットワークを介して送信したが、本人確認書類の原本確認が必要な場合は、窓口又はユーザから通信サービス管理者に本人確認書類の原本を提出ないし郵送するようにしてもよい。この場合は、通信サービス管理者が本人確認書類の原本を受領したのち、ステップＳ１８０６の本人確認処理が開始される。

【０１１４】

証明書発行依頼を受信した認証局は、利用者識別符号を生成し、ＩＭＳＩ又は電話番号により特定される送信先に利用者識別符号を送信する（ステップＳ１８０８）。利用者識別符号の送信手段としては、例えば、ＳＭＳ（ショートメッセージサービス）を利用することができる。ユーザ機器３０のセットアッププログラムは、ＩＣカードの鍵生成機能６２４に鍵ペアの生成を指示して秘密鍵と公開鍵を生成させる（ステップＳ１８０９）。なお、利用者識別符号の送付（ステップＳ１８０８）と鍵ペア生成（ステップＳ１８０９）の順序は問わない。

【０１１５】

その後、ユーザ機器３０のセットアッププログラムは、ＩＣカードの公開鍵読出機能６２５を利用して、ＩＣカードのメモリから公開鍵を読み出し、この公開鍵と利用者識別符号とから電子証明書の発行要求であるＣＳＲ（Certificate Signing Request）を作成し、所定の認証局に送信する（ステップＳ１８１０）。

【０１１６】

認証局は、受信したＣＳＲに従ってユーザの公開鍵の電子証明書を発行し、ユーザ機器３０へ、有線インターネット経由あるいは無線インターネット経由で送信する（ステップＳ１８１１）。このとき、プロトコルとしてＨＴＴＰ（Hypertext Transfer Protocol）又はＨＴＴＰＳ（Hypertext Transfer Protocol Secure）を用いて送信してもよい。電子証明書を認証局から受信する処理も、ユーザ機器３０のセットアッププログラムによって行われる。

【０１１７】

電子証明書は電子的に利用者が本人であることを証明するものである。本実施形態では、電子証明書として、公開鍵とその所有者の同定情報を結びつける公開鍵証明書が用いられる。ＩＴＵ－Ｔにより策定されたＸ．５０９の場合、電子証明書は、公開鍵、所有者情報（本人確認情報が該当）、認証局の電子署名、電子証明書の有効期限、発行者の情報を含んだデータである。なお、認証局の電子署名は、電子証明書に含まれる公開鍵と所有者情報から生成したハッシュ値を認証局の秘密鍵で暗号化したものである。

【０１１８】

認証局が電子証明書をユーザ機器３０へ送信するタイミング、あるいは、ユーザ機器３０が電子証明書を認証局から受信するタイミングは、任意に制御できる。例えば、ユーザ機器３０のセットアッププログラムがバックグラウンドで定期的に認証局と通信を行い、電子証明書の発行が完了したか否かを確認し、準備が整った段階で電子証明書をダウンロードしてもよい。あるいは、認証局がＣＳＲを受信したときに、ユーザ機器３０に対し、電子証明書の発行予定日時（ダウンロードが可能となる日時）を通知してもよい。その場合、ユーザ機器３０のセットアッププログラムは、通知された発行予定日時の経過後に、認証局にアクセスし電子証明書を取得すればよい。あるいは、ＳＭＳやプッシュ通知などの仕組みを用いて、認証局が、電子証明書の発行が完了した旨をユーザ機器３０のセットアッププログラムに通知し、応答したセットアッププログラムに対し電子証明書を送信してもよい。このように、電子証明書の発行依頼と電子証明書のユーザ機器への送信とを異なるタイミングで行えるようにしたことにより、例えば、本人確認までの業務を店頭窓口で行い、電子証明書発行以降のフローはユーザが希望する時間帯に行うというように、時間や場所の制限のないオペレーションが可能となる。したがって、暗号化機能のインストール及びアクティベーションの利便性向上を図ることができる。なお、いずれの方法の場

合でも、ユーザ機器３０のセットアッププログラムは、利用者識別符号とともに通信用ＳＩＭカードの電話番号及び／又はＩＭＳＩを認証局に通知することによって、申込者本人の端末（正当な端末）であることを認証局に証明するとよい。これにより、電子証明書の発行依頼とユーザ機器への送信とが異なるタイミングで行われる場合においても、別人の端末に誤って電子証明書を送信するといったミスの発生を防ぐことができる。また、悪意をもった者が不正に電子証明書を取得することも抑制できるため、電子証明書の発行及び送信を安全に行うことができる。

【０１１９】

ユーザ機器３０のセットアッププログラムは、ＩＣカードの電子証明書書込機能６２６を利用して電子証明書をＩＣカードのメモリに書き込む（ステップＳ１８１２）。この段階で、ＩＣカードのメモリには、セキュリティ処理に必要なデータである、本人情報、秘密鍵、公開鍵、電子証明書が揃ったことになる。このとき、電子証明書をユーザ機器３０に搭載されるＳＩＭカードやセキュアエレメントに格納してもよい。

【０１２０】

ユーザ機器３０のセットアッププログラムは、ＩＣカードから「シリアル番号」と「製造番号」を読み出すと共に、通信用のＳＩＭカードから「電話番号」と「ＩＭＳＩ」を読み出す。また、セットアッププログラムは、ユーザ機器自体の情報として「ＩＭＥＩ（International Mobile Equipment Identity）」を取得する。そしてセットアッププログラムは、それらの情報と共にＩＣカード登録要求を通信サービス管理者の管理サーバへ送信する。管理サーバは、ユーザ機器３０からＩＣカード登録要求を受信すると、そこに含まれるＩＣカードとＳＩＭカードとユーザ機器の情報をＩＣカード管理データベースに登録する（ステップＳ１８１４）。

【０１２１】

ＩＣカード管理情報の登録が完了すると、管理サーバが、ユーザ機器３０に対して登録完了を通知する。これによりユーザ機器３０のセットアップが完了し、ＩＣカードが利用可能な状態（活性化状態）となる。

【０１２２】

なお、図１９に示した発行手順はあくまで一例であり、異なる手順で発行手続を行っても構わない。例えば、ＳＭＳの代わりにインターネットを介したデータ通信により利用者識別符号をユーザ機器に送信してもよい。このとき、通信用のＳＩＭカードのＩＭＳIを用いてユーザ機器のＩＰアドレスを特定してもよい。また、ＰＩＮコード認証ではなく、生体認証を用いる場合には、ＩＣカードに本人情報として登録する生体情報（顔画像、声紋、虹彩、指紋など）を手続端末などを利用して入力してもよい。

【０１２３】

＜ＩＣチップの特定＞

図２０は、ユーザ機器と中間サーバとの間で通信を行う際に、ユーザ機器において利用されるＩＣチップを特定するための仕組みの一例を示す図である。図２０の例では、ユーザ機器３０が２つのＩＣチップ１９０、１９１を有しており、ＩＣチップ１９０がサーバＡ１９２との通信に利用され、ＩＣチップ１９１がサーバＢ１９３との通信に利用されるものとする。ＩＣチップ１９０、１９１としては、前述したサブＳＩＭタイプのＩＣカード、通信用のＳＩＭカード、セキュアエレメントなどのほか、いかなるタイプのＩＣチップを利用してもよい。

【０１２４】

各ＩＣチップ１９０、１９１には、ユニークなＩＤが割り振られている。このＩＤは、ＩＣチップを一意に特定しうる識別情報であって、ＩＣチップの内蔵メモリ内に格納されている。図２０の例では、ＩＣチップ１９０のＩＤは「ａａａ１」であり、ＩＣチップ１９１のＩＤは「ｂｂｂ２」である。ＩＤとしては、他のＩＣチップと重ならなければいかなる情報でもよい。例えば、ＩＭＳＩ（International Mobile Subscriber Identity）、ＩＣＣＩＤ（Integrated Circuit Card ID）、電話番号、シリアル番号、製造番号などをＩＤとして用いることができる。また、ＩＭＳＩなどに対応づけられたＩＰアドレスを

ＩＤとして用いてもよい。
【０１２５】
ユーザ機器３０の本体アプリ６０は、サーバＡ１９２に送信するデータ（通信パケット）１９４のヘッダなどに、送信元の情報として、ＩＣチップ１９０のＩＤ「ａａａ１」を付加する。これにより、サーバＡ１９２は、ユーザ機器３０において使用されているＩＣチップ１９０を特定することができる。またサーバＡ１９２も、ユーザ機器３０に送信するデータ（通信パケット）１９４のヘッダなどに、送信先の情報として、ＩＣチップ１９０のＩＤ「ａａａ１」を付加する。このＩＤにより、本体アプリ６０は、サーバＡ１９２から受信したデータの処理を担当するＩＣチップ１９０を特定することができる。
【０１２６】
一方、ユーザ機器３０の本体アプリ６０は、サーバＢ１９３に送信するデータ（通信パケット）１９５のヘッダなどに、送信元の情報として、ＩＣチップ１９１のＩＤ「ｂｂｂ２」を付加する。これにより、サーバＢ１９３は、ユーザ機器３０において使用されているＩＣチップ１９１を特定することができる。またサーバＢ１９３も、ユーザ機器３０に送信するデータ（通信パケット）１９５のヘッダなどに、送信先の情報として、ＩＣチップ１９１のＩＤ「ｂｂｂ２」を付加する。このＩＤにより、本体アプリ６０は、サーバＡ１９２から受信したデータの処理を担当するＩＣチップ１９０を特定することができる。
【０１２７】
以上述べた構成によれば、ユーザ機器３０と各サーバとの間において、送信元又は送信先となるＩＣチップを特定したデータ送受信が行われるため、通信の安全性をより高めることができる。また、図２０に示すように、ＩＣチップとサーバの組み合わせが複数組ある場合には、本体アプリ６０がデータ１９４、１９５のヘッダに含まれるＩＤ情報に基づいて、データ１９４、１９５の処理に利用すべきＩＣチップ１９０、１９１を選択（切り替え）することができる。このような利点は、ユーザ機器３０が複数のＩＣチップを備えている場合や、ユーザ機器３０が複数のサーバとセキュアな通信を行う場合などに、特にメリットが大きい。
【０１２８】
図２０の例では、ユーザ機器３０と各サーバとの間で送受信されるデータにＩＣチップの識別情報を付加することによって、ＩＣチップとサーバとの対応付けを行ったが、別の方法で同様のことを実現しても構わない。例えば、図２１に示すように、本体アプリ６０が、ＩＣチップとサーバとの対応付けを行う対応付け情報１９６（以下、「対応テーブル１９６」と呼ぶ）を有していてもよい。対応テーブル１９６では、例えば、ＩＣチップの識別情報と、そのＩＣチップの暗号化機能を利用して通信を行うサーバの識別情報との対応付けが行われるとよい。ＩＣチップの識別情報としては、例えば、ＩＭＳＩ（International Mobile Subscriber Identity）、ＩＣＣＩＤ（Integrated Circuit Card ID）、電話番号、シリアル番号、製造番号、ＩＭＳＩに対応付けられたＩＰアドレスなどを用いてもよい。また、サーバの識別情報としては、例えば、サーバのＩＰアドレス、ＵＲＬなどを用いてもよい。図２１に示す方法の場合、本体アプリ６０が、サーバと通信を行う際に、対応テーブル１９６に基づいて、サーバとの通信において利用するＩＣチップを特定することができる。したがって、図２０の方法と同様の効果を奏することが可能である。
【０１２９】
＜サーバ間の通信のセキュリティ＞
上述した実施形態では、ユーザ機器３０と中間サーバ２１とサービス提供サーバ２０の３者間の通信を、ＩＣチップを利用した公開鍵暗号方式によって保護している。この方式は高度なセキュリティを確保できる点で好ましい形態であるが、３者間の通信のすべてをこの方式で行うことは必須ではない。例えば、ユーザ機器３０と中間サーバ２１の間は、通信の傍受やなりすましなどのサイバー攻撃のリスクが相対的に高いため、高度なセキュリティが望まれるのに対し、中間サーバ２１とサービス提供サーバ２０の間の通信は、サイバー攻撃のリスクが相対的に低い。したがって、例えば、ユーザ機器３０と中間サーバ２１の間の通信にはＩＣチップを利用した保護を適用し、中間サーバ２１とサービス提供

サーバ２０の間の通信は他の方式によりセキュリティを確保してもよい。他の方式としては、例えば、ＩＤとパスワードによる方式、アクセストークンによる方式、ＩＣチップとは異なる暗号化通信による方式、サーバ間を専用線で接続する方式などがある。以下に、それぞれの方式の一例を説明する。

【０１３０】

（１）ＩＤとパスワードによる方式

（初回登録）

図２２を参照して、中間サービスへの初回登録手続を説明する。図２２は、中間サービスへの登録手続の流れを示す。なお、この段階では、中間サーバ２１が提供する中間サービスへのユーザ登録とサービス提供サーバ２０が提供するオンラインサービスへのユーザ登録は既に済んでおり、中間サーバ２１が提供するサービスにログインするためのＩＤとパスワード（以後、便宜的に「ユーザＩＤ１」、「パスワード１」と記す）、及び、サービス提供サーバ２０が提供するサービスにログインするためのＩＤとパスワード（以後、便宜的に「ユーザＩＤ２」、「パスワード２」と記す）はユーザに付与されているものとする。

【０１３１】

まず、ユーザは、ユーザ機器３０を操作し、本体アプリ６０のダウンロード及びインストールを行う（ステップＳ２１００）。そして、ユーザは、本体アプリ６０を起動し、中間サーバ２１のログイン画面を開く（ステップＳ２１０１）。初回のログイン時には、ユーザがログイン画面において中間サーバ２１へのユーザＩＤ１とパスワード１を入力し、ユーザ機器３０がユーザＩＤ１とパスワード１とともにログイン要求を中間サーバ２１に送信する（ステップＳ２１０２）。このとき、本体アプリ６０は、中間サーバ２１へのユーザＩＤ１を不揮発性メモリに記憶する（ステップＳ２１０３）。パスワード１については、セキュリティの観点からユーザ機器３０には記憶させないほうがよい。なお、中間サーバ２１へのユーザＩＤ１とパスワード１は、別途の手続である中間サービスの新規利用申込を行ったときに、中間サービス提供者から付与される情報である。

【０１３２】

ユーザＩＤ１とパスワード１を中間サーバ２１が検証し、ログインが完了すると（ステップＳ２１０４）、中間サーバ２１は、所定の電文（内容はどのようなものでもよい）をユーザ機器３０に送信し、電子署名と電子証明書を要求する（ステップＳ２１０５）。

【０１３３】

本体アプリ６０のユーザ認証部６０１は、ＰＩＮコード入力画面を表示する。ユーザによりＰＩＮコードが入力されると、ユーザ認証部６０１は、ＩＣチップの認証機能６２０を利用して、入力されたＰＩＮコードが正しいか否かを確認する（ステップＳ２１０６）。ＰＩＮコードが正しい場合（つまり、ユーザ認証に成功した場合）は、本体アプリ６０からＩＣチップの他の機能を利用可能となる。本体アプリ６０のセキュリティ処理部６０２は、ＩＣチップの電子署名機能６２２を利用して、中間サーバ２１から受信した電文に電子署名を行うと共に、電子証明書読出機能６２７を利用して、メモリから電子証明書を読み出す。そして、本体アプリ６０のメイン処理部６００は、電子署名付き電文と電子証明書を中間サーバ２１に送信する（ステップＳ２１０７）。

【０１３４】

中間サーバ２１は、ユーザ機器３０から受信した電子証明書を用いて電子署名付き電文を検証する（ステップＳ２１０８）。検証に成功した場合、中間サーバ２１は、当該ユーザの中間サーバ２１へのユーザＩＤ１と電子証明書を紐付けて、ユーザ情報記憶部２１１に登録する（ステップＳ２１０９）。そして、中間サーバ２１は、電子証明書の登録が完了した旨を本体アプリ６０へ通知する（ステップＳ２１１０）。中間サーバ２１への登録が完了すると、ユーザ機器３０にはメニュー画面が表示される（ステップＳ２１１１）。

【０１３５】

（中間サービスへのログイン）

図２３を参照して、中間サービスのログイン認証を説明する。図２３は、中間サービス

のログイン認証の流れを示す。

【０１３６】

ユーザが、ユーザ機器３０において本体アプリ６０を起動すると、ユーザ認証部６０１が、ＰＩＮコード入力画面を表示する（ステップＳ２２００）。ユーザによりＰＩＮコードが入力されると、ユーザ認証部６０１は、ＩＣチップの認証機能６２０を利用して、入力されたＰＩＮコードが正しいか否かを確認する（ステップＳ２２０１）。ＰＩＮコードが正しい場合（つまり、ユーザ認証に成功した場合）、本体アプリ６０のセキュリティ処理部６０２は、ＩＣチップの電子署名機能６２２を利用して、中間サーバ２１へのユーザＩＤ１と認証用電文に対し電子署名を行う（ステップＳ２２０２）。そして、本体アプリ６０のメイン処理部６００は、ログイン要求を中間サーバ２１に送信する（ステップＳ２２０３）。ログイン要求には、中間サーバ２１へのユーザＩＤ１、サービス提供サーバ２０へのユーザＩＤ２とパスワード２、認証用電文、電子署名が付加されている。

【０１３７】

中間サーバ２１のログイン制御部２１２は、ログイン要求を受信すると、ログイン要求に含まれる中間サーバ２１へのユーザＩＤ１に基づいて、ユーザ情報記憶部２１１から対応する電子証明書を読み出し、この電子証明書を用いて、ログイン要求に含まれている電子署名の検証を行う（ステップＳ２２０４）。また、必要に応じて、ログイン制御部２１２は、電子証明書の有効性を認証局に問い合わせてもよい（ステップＳ２２０５、Ｓ２２０６）。電子署名の検証に成功し、且つ、電子証明書の有効性が確認された場合、ログイン制御部２１２は、ログイン要求が正当なユーザからのものであると判断し、サービス提供サーバ２０へのユーザＩＤ２とパスワード２を当該ユーザの中間サーバ２１へのユーザＩＤ１と紐付けて、ユーザ情報記憶部２１１に登録する（ステップＳ２２０７）。

【０１３８】

続いて、中間サーバ２１のログイン制御部２１２は、サービス提供サーバ２０にアクセス要求を送信する（ステップＳ２２０８）。このアクセス要求には、サービス提供サーバ２０へのユーザＩＤ２とパスワード２が付加されている。

【０１３９】

サービス提供サーバ２０のアクセス制御部２０２は、アクセス要求を受信すると、サービス提供サーバ２０へのユーザＩＤ２とパスワード２の検証を行う（ステップＳ２２０９）。ユーザＩＤ２とパスワード２の検証に成功した場合、アクセス制御部２０２は、このアクセス要求が、ユーザから代行権限が与えられた中間サーバ２１からのものであると判断し、中間サーバ２１に対しアクセス許可を与える（ステップＳ２２１０）。

【０１４０】

オンラインサービスのアクセス許可が得られたら、中間サーバ２１は、ログイン認証ＯＫを本体アプリ６０に通知する（ステップＳ２２１１）。以後、ユーザ機器３０に中間サービスのメニュー画面が表示され、ユーザは希望する手続を行うことができるようになる（ステップＳ２２１２）。

【０１４１】

以上述べた処理によれば、物理的なトークンを用いる方法に比べて、非常に簡便な操作で中間サービス及びオンラインサービスの利用が可能となる。

【０１４２】

（オンラインサービスの利用）

図２４を参照して、中間サービス利用時の手順を説明する。図２４は、中間サービス利用時の流れを示す図である。中間サービスへのログインは既に完了しており、ユーザ機器３０にはメニュー画面が表示されているものとする。

【０１４３】

ユーザがメニュー画面から利用したい手続を選択すると、詳細画面に遷移する（ステップＳ２３００）。この詳細画面においてユーザが必要な情報（例えば振込先、振込額など）を入力し、実行ボタンを押すと（ステップＳ２３０１）、本体アプリ６０のメイン処理部６００が、振込手続に必要な情報を記述した手続メッセージを作成する（ステップＳ２

３０２）。
【０１４４】
続いて、本体アプリ６０のユーザ認証部６０１が、ＰＩＮコード入力画面を表示し、ＰＩＮコード認証を行う（ステップＳ２３０３）。ＰＩＮコード認証の手順は前述したものと同様のため、説明を省略する。ＰＩＮコード認証に成功した場合、本体アプリ６０のセキュリティ処理部６０２は、ＩＣチップの電子署名機能６２２を利用して、手続メッセージに対し電子署名を行う（ステップＳ２３０４）。このとき、電子署名機能６２２は、手続メッセージのハッシュ値を計算し、このハッシュ値を秘密鍵で暗号化することにより電子署名を生成してもよいし、手続メッセージ自体を秘密鍵で暗号化することにより電子署名を生成してもよい。そして、本体アプリ６０のメイン処理部６００は、手続要求を中間サーバ２１に送信する（ステップＳ２３０５）。手続要求には、中間サーバ２１へのユーザＩＤ１、手続メッセージ、電子署名が付加されている。
【０１４５】
中間サーバ２１の代行制御部２１３は、手続要求を受信すると、手続要求に含まれるユーザの中間サーバへのユーザＩＤ１に基づいて、ユーザ情報記憶部２１１から対応する電子証明書を読み出し、この電子証明書を用いて、手続要求に含まれている電子署名の検証を行う（ステップＳ２３０６）。また、必要に応じて、代行制御部２１３は、電子証明書の有効性を認証局に問い合わせてもよい（ステップＳ２３０７、Ｓ２３０８）。電子署名の検証に成功し、且つ、電子証明書の有効性が確認された場合、代行制御部２１３は、手続要求が正当なユーザからのものであると判断する。すなわち、第三者によるなりすましがなく、かつ、手続メッセージの内容も改ざんされていないと判断するのである。
【０１４６】
手続要求が正当なユーザからのものであると確認できた場合、代行制御部２１３は、当該ユーザのサービス提供サーバ２０へのユーザＩＤ２とパスワード２を読み出し、サービス提供サーバ２０に手続要求を送信する（ステップＳ２３０９）。この手続要求には、ユーザ機器３０から受信した手続メッセージ及び電子署名が付加されている。
【０１４７】
サービス提供サーバ２０の手続制御部２０３は、手続要求を受信すると、ユーザＩＤ２とパスワード２の検証を行う（ステップＳ２３１０）。ユーザＩＤ２とパスワード２の検証に成功した場合、手続制御部２０３は、この手続要求が正当なユーザからのものであると判断する。すなわち、第三者によるなりすましがなく、かつ、手続メッセージの内容も改ざんされていないと判断するのである
【０１４８】
手続要求が正当なユーザからのものであると確認できた場合にのみ、手続制御部２０３は、手続メッセージに記述された情報に基づく手続（振込など）を実行する（ステップＳ２３１１）。手続が完了すると、手続制御部２０３は手続完了通知を中間サーバ２１に送信し、中間サーバ２１が手続完了通知を本体アプリ６０に送信する（ステップＳ２３１２、Ｓ２３１３）。そうすると、手続完了画面が表示される。
【０１４９】
以上述べた処理によれば、物理的なトークンを用いる方法などに比べて、非常に簡便な操作で中間サービス及びオンラインサービスの利用が可能となる。
【０１５０】
（２）アクセストークンによる方式
次に、アクセストークンを用いて中間サーバ２１からサービス提供サーバ２０へのアクセス権限の認可をする方式について、一例を示す。
【０１５１】
（初回登録）
図２５及び図２６を参照して、中間サービスへの初回登録手続を説明する。中間サーバ２１にユーザの電子証明書を登録する手順（ステップＳ２４００～Ｓ２４１０）は、図２２で説明した手順（ステップＳ２１００～Ｓ２１１０）と同様のため、説明を割愛する。

電子証明書の登録完了後、アクセストークン発行のための認可コードの発行とアクセストークンの発行が行われる。アクセストークンとは、中間サーバ２１がユーザに代わりオンラインサービスを利用する際の認可証のようなものである。本実施形態では、ＯＡｕｔｈ２．０の仕組みを利用して、中間サーバ２１によるオンラインサービスの代行を実現する。

【０１５２】

まず、認可コードの発行を行うため、登録完了通知を受け取ったのちユーザ機器３０は、中間サーバ２１へのユーザＩＤ１、サービス提供サーバ２０へのユーザＩＤ２とパスワード２、電子署名付き電文、電子証明書を中間サーバ２１に送信する（ステップＳ２４１１）。中間サーバ２１はユーザ機器３０から受信した電子証明書を用いて電子署名付き電文を検証する（ステップＳ２４１２）。検証に成功した場合、中間サーバ２１のユーザ登録部２００はサービス提供サーバ２０へのユーザＩＤ２と中間サーバ２１へのユーザＩＤ１を紐付けて、ユーザ情報記憶部２１１に登録する（ステップＳ２４１３）。その後、中間サーバ２１は、ユーザ機器３０から受信したサービス提供サーバ２０へのユーザＩＤ２・パスワード２とあわせて認可コードの発行要求をサービス提供サーバ２０に送信する（ステップＳ２４１４）。サービス提供サーバ２０は中間サーバ２１から受信したユーザＩＤ２・パスワード２を検証し、検証に成功した場合、サービス提供サーバ２０は受信したユーザＩＤ２に紐づく、アクセストークンを発行するための認可コードを発行する（ステップＳ２４１５）。サービス提供サーバ２０は、中間サーバ２１に、ユーザＩＤ２及び認可コードとともに認証結果を送信する（ステップＳ２４１６）。中間サーバ２１は受信したサービス提供サーバ２０へのユーザＩＤ２を中間サーバ２１へのユーザＩＤ１に変換し、認可コードと認証結果をユーザ機器３０に送信する（ステップＳ２４１７）。ユーザ機器３０は中間サーバ２１へのユーザＩＤ１及び認可コードとあわせてアクセストークン発行要求を中間サーバ２１に送信する（ステップＳ２４１８）。中間サーバ２１は受信した中間サーバ２１へのユーザＩＤ１をサービス提供サーバ２０へのユーザＩＤ２に変換し、ユーザＩＤ２と認可コードとアクセストークン発行要求をサービス提供サーバ２０に送信する（ステップＳ２４１９）。サービス提供サーバ２０は当該ユーザと中間サービスの組に対し、アクセストークンを発行する（ステップＳ２４２０）。ユーザ登録部２００は、発行したアクセストークンとサービス提供サーバ２０へのユーザＩＤ２を紐付けて、ユーザ情報記憶部２０１に登録する。

【０１５３】

そして、サービス提供サーバ２０は、サービス提供サーバ２０へのユーザＩＤ２と発行したアクセストークンを中間サーバ２１に送信する（ステップＳ２４２１）。中間サーバ２１は受け取ったアクセストークンと当該ユーザの中間サーバ２１へのユーザＩＤ１とを紐付けて、ユーザ情報記憶部２１１に登録する（ステップＳ２４２２）。なお、図示しないが、中間サーバ２１はサービス提供サーバ２０からアクセストークンと共にリフレッシュトークンも受け取る。リフレッシュトークンは、アクセストークンの再発行に利用されるトークンである。これはＯＡｕｔｈ２．０の仕様であるため、ここでは詳しい説明は割愛する。

【０１５４】

その後、中間サーバ２１は、アクセストークンの発行が完了した通知を本体アプリ６０へ通知し、ユーザ機器３０にはメニュー画面が表示される（ステップＳ２４２３、Ｓ２４２４）。

【０１５５】

（中間サービスへのログイン）

中間サービスへのログインではアクセストークンの検証を行う。図２７に、中間サービスへのログイン処理の流れを示す。図２７のステップＳ２６００～Ｓ２６０６の処理は、図２３のステップＳ２２００～Ｓ２２０６の処理とほぼ同様である。ただし、本例では、ログイン要求に付加される情報が、中間サーバ２１へのユーザＩＤ１と認証用電文と電子署名である点が、図２３の処理とは相違する。

【０１５６】

中間サーバ２１は、電子署名の正当性と電子証明書の有効性を確認したのち、サービス提供サーバ２０にアクセス要求を送信する（ステップＳ２６０７）。このとき、中間サーバ２１は、ログイン要求に含まれる中間サーバ２１へのユーザＩＤ１に基づいて、ユーザ情報記憶部２１１からサービス提供サーバ２０へのユーザＩＤ２とオンラインサービスのアクセストークンを読み出し、アクセス要求とともに送信する。

【０１５７】

サービス提供サーバ２０のアクセス制御部２０２は、アクセス要求を受信すると、アクセス要求に含まれるサービス提供サーバ２０へのユーザＩＤ２とアクセストークンの検証を行う（ステップＳ２６０８）。検証に成功した場合、アクセス制御部２０２は、アクセス要求がユーザから代行権限が与えられた中間サーバ２１からのものであると判断し、中間サーバ２１に対しアクセス許可を与える（ステップＳ２６０９）。

【０１５８】

オンラインサービスのアクセス許可が得られたら、中間サーバ２１は、ログイン認証ＯＫを本体アプリ６０に通知する（ステップＳ２６１０）。以後、ユーザ機器３０に中間サービスのメニュー画面が表示され、ユーザは希望する手続を行うことができようになる（ステップＳ２６１１）。

【０１５９】

以上述べた処理によれば、物理的なトークンを用いる方法に比べて、非常に簡便な操作で中間サービス及びオンラインサービスの利用が可能となる。

【０１６０】

（オンラインサービスの利用）

オンラインサービスでも、アクセストークンの検証を行う。図２８に、オンラインサービスの処理の流れを示す。図２８のステップＳ２７００～Ｓ２７０８の処理は、図２４のステップＳ２３００～Ｓ２３０８の処理と同様である。

【０１６１】

電子証明書によって手続要求が正当なユーザからのものであると確認できた場合、中間サーバ２１の代行制御部２１３は、サービス提供サーバ２０に手続要求を送信する（ステップＳ２７０９）。このとき、代行制御部２１３は、ユーザ機器３０から受信したユーザＩＤ１に基づいて、ユーザ情報記憶部２１１から対応するサービス提供サーバ２０へのユーザＩＤ２とオンラインサービスのアクセストークンを読み出し、サービス提供サーバ２０に手続要求を送信する（ステップＳ２７０９）。この手続要求には、アクセストークンと、ユーザ機器３０から受信した手続メッセージ及び電子署名とが付加されている。

【０１６２】

サービス提供サーバ２０の手続制御部２０３は、手続要求を受信すると、手続要求に含まれるサービス提供サーバ２０へのユーザＩＤ２とアクセストークンの検証を行う（ステップＳ２７１０）。検証に成功した場合、手続制御部２０３はこの手続要求が正当なユーザからのものであると判断する。

【０１６３】

手続要求が正当なユーザからのものであると確認できた場合にのみ、手続制御部２０３は、手続メッセージに記述された情報に基づく手続（振込など）を実行する（ステップＳ２７１１）。手続が完了すると、手続制御部２０３は手続完了通知を中間サーバ２１に送信し（ステップＳ２７１２）、中間サーバ２１が手続完了通知を本体アプリ６０に送信する（ステップＳ２７１３）。手続完了通知を受信したユーザ機器３０には、手続完了画面が表示される。

【０１６４】

以上述べた処理によれば、物理的なトークンを用いる方法に比べて、非常に簡便な操作で中間サービス及びオンラインサービスの利用が可能となる。

【０１６５】

（３）ＩＣチップとは異なる暗号化通信による方式

中間サーバ２１とサービス提供サーバ２０の間の通信を、ＩＣチップによる暗号化通信

とは異なる方式で、暗号化してもよい。例えば、中間サーバ２１とサービス提供サーバ２０の間で共通鍵を共有し、中間サーバ２１とサービス提供サーバ２０の間の通信を共通鍵で暗号化してもよい。あるいは、中間サーバ２１とサービス提供サーバ２０の間の通信を公開鍵暗号方式によって暗号化してもよい。また、ＳＳＬ／ＴＬＳ、ＩＰｓｅｃなどの暗号化通信を利用してもよい。

【０１６６】

このような暗号化通信による方式の場合も、ユーザはＰＩＮコードを入力するだけでよいので、従来の方法に比べて、非常に簡便な操作で中間サービス及びオンラインサービスの利用が可能となる。なお、（３）の暗号化通信は、（１）のユーザＩＤとパスワードを利用する方式や、（２）のアクセストークンを利用する方式と組み合わせてもよい。

【０１６７】

（４）サーバ間を専用線で接続する方式

専用線の仕組みを利用して、中間サーバ２１とサービス提供サーバ２０の間のセキュアな通信を実現することもできる。専用線とは、独占的に使用できる通信回線のことである。中間サーバ２１とサービス提供サーバ２０の間に物理的な専用線を設けてもよいし、仮想的な専用線（ＶＰＮ）を利用してもよい。

【０１６８】

このような専用線を利用する方式の場合も、ユーザはＰＩＮコードを入力するだけでよいので、従来の方法に比べて、非常に簡便な操作で中間サービス及びオンラインサービスの利用が可能となる。なお、（４）の専用線は、（１）のユーザＩＤとパスワードを利用する方式や、（２）のアクセストークンを利用する方式や、（３）の暗号化通信による方式と組み合わせてもよい。

【０１６９】

＜サーバの多段接続＞

上述した各実施形態では、ユーザ機器３０と中間サーバ２１とサービス提供サーバ２０の３者間の通信について説明したが、本発明は、中間サーバ２１及び／又はサービス提供サーバ２０を多段接続した構成に対して適用することもできる。

【０１７０】

図２９Ａは、ユーザ機器３０とサービス提供サーバ２０の間に２つ以上の中間サーバ２１Ａ、２１Ｂが従属的（直列的）に接続される構成を示している。例えば、第一の中間サーバ２１Ａは銀行サービスと連携して家計簿や資産管理のような付加価値サービスを提供する企業（Ｆｉｎｔｅｃｈ企業と呼ばれる）のサーバであり、第二の中間サーバ２１Ｂは Ｆｉｎｔｅｃｈ企業と銀行の間に介在して、電子証明書による検証やユーザの管理などの代行を行うサーバであり、サービス提供サーバ２０はオンラインバンキングサービスを提供する銀行システムである。電子証明書による検証やユーザの管理などの処理の一部又は全部をサービス提供サーバ２０から切り離し、別の中間サーバ２１Ｂで代行する構成とすることで、サービス提供サーバ２０の導入や運用が容易になると期待される。このような形態は、例えば、複数の銀行のサービス提供サーバ２０の電子証明書やユーザの管理を、一つの中間サーバ２１Ｂで集中的に代行する、というような場合に有利である。また、図２９Ａの構成は、Ｆｉｎｔｅｃｈ企業の中間サーバ２１Ａが、他のＦｉｎｔｅｃｈ企業の中間サーバ２１Ｂのサービスを利用する場合にも適用できる。例えば、個々のＦｉｎｔｅｃｈ企業が提供するサービスを束ねて統合的なＦｉｎｔｅｃｈサービスを提供することが想定される。

【０１７１】

図２９Ｂは、２つ以上のサービス提供サーバ２０Ａ、２０Ｂが直列的に接続される構成である。この構成は、例えば、ある銀行から他の銀行に送金する場合、銀行のサーバと証券のサーバとが連携する場合などに適用できる。

【０１７２】

図２９Ｃは、２つ以上の中間サーバ２１Ａ、２１Ｂと２つ以上のサービス提供サーバ２０Ａ、２０Ｂが直列的に接続される構成の例である。なお、中間サーバ２１及びサービス

提供サーバ２０の接続数は任意である。以下に中間サーバが２つ、サービス提供サーバが１つの場合の動作について説明する。

【０１７３】

（初回登録）

図３０を参照して、中間サービスへの初回登録手続を説明する。図３０は、中間サービスへの登録手続の流れを示す。なお、この段階では、中間サーバＡ（２１Ａ）が提供する中間サービスへのユーザ登録とサービス提供サーバ２０が提供するオンラインサービスへのユーザ登録は既に済んでおり、中間サーバＡが提供するサービスにログインするためのＩＤとパスワード（以後、便宜的に「ユーザＩＤ１」、「パスワード１」と記す）、及び、サービス提供サーバ２０が提供するサービスにログインするためのＩＤとパスワード（以後、便宜的に「ユーザＩＤ２」、「パスワード２」と記す）はユーザに付与されているものとする。なお、この例では、中間サーバＡ（２１Ａ）と中間サーバＢ（２１Ｂ）が協働してユーザに中間サービスを提供しており、ユーザは、中間サーバが多段接続されていることを意識することはない。

【０１７４】

まず、ユーザは、ユーザ機器３０を操作し、本体アプリ６０のダウンロード及びインストールを行う（ステップＳ２９００）。そして、ユーザは、本体アプリ６０を起動し、中間サーバＡのログイン画面を開く（ステップＳ２９０１）。初回のログイン時には、ログイン画面において中間サーバＡへのユーザＩＤ１とパスワード１を入力し、ユーザ機器３０がユーザＩＤ１とパスワード１とともにログイン要求を中間サーバＡに送信する。このとき、本体アプリは、中間サーバＡへのユーザＩＤ１を不揮発性メモリに記憶する（ステップＳ２９０３）。パスワード１については、セキュリティの観点からユーザ機器３０には記憶させないほうがよい。なお、中間サーバＡへのユーザＩＤ１とパスワード１は、別途の手続である中間サービスの新規利用申込を行ったときに、中間サービス提供者から付与される情報である。

【０１７５】

中間サーバＡがユーザＩＤ１とパスワード１を検証し、中間サーバＡへのログインが完了すると（ステップＳ２９０４）、中間サーバＡは、ユーザ機器３０から受信したユーザＩＤ１とパスワード１を中間サーバＢに送信する（ステップＳ２９０５）。同様に、中間サーバＢがユーザＩＤ１とパスワード１を検証し、中間サーバＢへのログインが完了すると（ステップＳ２９０６）、中間サーバＢは所定の電文（内容はどのようなものでもよい）を中間サーバＡに送信し、電子署名と電子証明書を要求する（ステップＳ２９０７）。中間サーバＡは中間サーバＢから受信した所定の電文をユーザ機器３０に送信する（ステップＳ２９０８）。

【０１７６】

本体アプリ６０のユーザ認証部６０１は、ＰＩＮコード入力画面を表示する。ユーザによりＰＩＮコードが入力されると、ユーザ認証部６０１は、ＩＣチップの認証機能６２０を利用して、入力されたＰＩＮコードが正しいか否かを確認する（ステップＳ２９０９）。ＰＩＮコードが正しい場合（つまり、ユーザ認証に成功した場合）は、本体アプリ６０からＩＣチップの他の機能を利用可能となる。本体アプリ６０のセキュリティ処理部６０２は、ＩＣチップの電子署名機能６２２を利用して、中間サーバＡから受信した電文に電子署名を行うと共に、電子証明書読出機能６２７を利用して、メモリから電子証明書を読み出す。そして、本体アプリ６０のメイン処理部６００は、電子署名付き電文と電子証明書を中間サーバＡに送信する（ステップＳ２９１０）。

【０１７７】

中間サーバＡは、ユーザ機器３０から受信した電子署名付き電文と電子証明書を中間サーバＢに送信する（ステップＳ２９１１）とともに、その電子証明書を用いて電子署名付き電文を検証する（ステップＳ２９１２）。検証に成功した場合、中間サーバＡは、当該ユーザのユーザＩＤ１と電子証明書を紐付けて、ユーザ情報記憶部に登録する（ステップＳ２９１３）。

【０１７８】
同様に、中間サーバＢも、電子証明書を用いて電子署名付き電文を検証する（ステップＳ２９１４）。検証に成功した場合、中間サーバＢは、当該ユーザのユーザＩＤ１と電子証明書を紐付けて、ユーザ情報記憶部に登録する（ステップＳ２９１６）。そして、中間サーバＢは、電子証明書の登録が完了した旨を中間サーバＡへ通知する（ステップＳ２９１６）。これを受けて、中間サーバＡは、電子証明書の登録が完了した旨を本体アプリ６０へ通知する（ステップＳ２９１７）。中間サービスへの登録が完了すると、ユーザ機器３０にはメニュー画面が表示される。
【０１７９】
（中間サービスへのログイン）
図３１及び図３２を参照して、中間サービスのログイン認証を説明する。図３１及びず３１は、中間サービスのログイン認証の流れを示す。
【０１８０】
ユーザが、ユーザ機器３０において本体アプリ６０を起動すると、ユーザ認証部６０１が、ＰＩＮコード入力画面を表示する（ステップＳ３０００）。ユーザによりＰＩＮコードが入力されると、ユーザ認証部６０１は、ＩＣチップの認証機能６２０を利用して、入力されたＰＩＮコードが正しいか否かを確認する（ステップＳ３００１）。ＰＩＮコードが正しい場合（つまり、ユーザ認証に成功した場合）、本体アプリ６０のセキュリティ処理部６０２は、ＩＣチップの電子署名機能６２２を利用して、中間サーバＡへのユーザＩＤ１と認証用電文に対し電子署名を行う（ステップＳ３００２）。そして、本体アプリ６０のメイン処理部６００は、ログイン要求を中間サーバＡに送信する（ステップＳ３００３）。ログイン要求には、中間サーバＡへのユーザＩＤ１、サービス提供サーバ２０へのユーザＩＤ２とパスワード２、認証用電文、電子署名が付加されている。
【０１８１】
中間サーバＡのログイン制御部２１２は、ログイン要求を受信すると、ログイン要求に含まれる中間サーバＡへのユーザＩＤ１に基づいて、ユーザ情報記憶部２１１から対応する電子証明書を読み出し、この電子証明書を用いて、ログイン要求に含まれている電子署名の検証を行う（ステップＳ３００４）。また、必要に応じて、ログイン制御部２１２は、電子証明書の有効性を認証局に問い合わせてもよい（ステップＳ３００５、Ｓ３００６）。電子署名の検証に成功し、且つ、電子証明書の有効性が確認された場合、ログイン制御部２１２は、ログイン要求が正当なユーザからのものであると判断する。
【０１８２】
続いて、中間サーバＡのログイン制御部２１２は、ログイン要求を中間サーバＢに送信する（ステップＳ３００７）。ログイン要求には、ユーザＩＤ１、ユーザＩＤ２とパスワード２、認証用電文、電子署名が付加されている。
【０１８３】
中間サーバＢのログイン制御部２１２は、ログイン要求を受信すると、ログイン要求に含まれるユーザＩＤ１に基づいて、ユーザ情報記憶部２１１から対応する電子証明書を読み出し、この電子証明書を用いて、ログイン要求に含まれている電子署名の検証を行う（ステップＳ３００８）。また、必要に応じて、ログイン制御部２１２は、電子証明書の有効性を認証局に問い合わせてもよい（ステップＳ３００９、Ｓ３０１０）。電子署名の検証に成功し、且つ、電子証明書の有効性が確認された場合、ログイン制御部２１２は、ログイン要求が正当なユーザからのものであると判断し、サービス提供サーバ２０へのユーザＩＤ２とパスワード２を当該ユーザの中間サーバＡへのユーザＩＤ１と紐付けて、ユーザ情報記憶部２１１に登録する（ステップＳ３０１１）。
【０１８４】
続いて、中間サーバＢのログイン制御部２１２は、サービス提供サーバ２０にアクセス要求を送信する（ステップＳ３０１２）。このアクセス要求には、サービス提供サーバ２０へのユーザＩＤ２とパスワード２が付加されている。
【０１８５】

サービス提供サーバ２０のアクセス制御部２０２は、アクセス要求を受信すると、サービス提供サーバ２０へのユーザＩＤ２とパスワード２の検証を行う（ステップＳ３０１３）。サービス提供サーバ２０へのユーザＩＤ２とパスワード２の検証に成功した場合、アクセス制御部２０２は、このアクセス要求が、ユーザから代行権限が与えられた中間サーバからのものであると判断し、中間サーバＢに対しアクセス許可を与える（ステップＳ３０１４）。

【０１８６】

オンラインサービスのアクセス許可が得られたら、中間サーバＢは、ログイン認証ＯＫを中間サーバＡに通知し（ステップＳ３０１５）、さらに中間サーバＡは、ログイン認証ＯＫを本体アプリ６０に通知する（ステップＳ３０１６）。以後、ユーザ機器３０に中間サービスのメニュー画面が表示され、ユーザは希望する手続を行うことができるようになる（ステップＳ３０１７）。

【０１８７】

以上述べた処理によれば、物理的なトークンを用いる方法に比べて、非常に簡便な操作で中間サービス及びオンラインサービスの利用が可能となる。

【０１８８】

（オンラインサービスの利用）

図３３及び図３４を参照して、中間サービス利用時の手順を説明する。図３３及び図３４は、中間サービス利用時の流れを示す図である。中間サービスへのログインは既に完了しており、ユーザ機器にはメニュー画面が表示されているものとする。

【０１８９】

ユーザがメニュー画面から利用したい手続を選択すると、詳細画面に遷移する（ステップＳ３２００）。この詳細画面においてユーザが必要な情報（例えば振込先、振込額など）を入力し、実行ボタンを押すと（ステップＳ３２０１）、本体アプリ６０のメイン処理部６００が、振込手続に必要な情報を記述した手続メッセージを作成する（ステップＳ３２０２）。

【０１９０】

続いて、本体アプリ６０のユーザ認証部６０１が、ＰＩＮコード入力画面を表示し、ＰＩＮコード認証を行う（ステップＳ３２０３）。ＰＩＮコード認証の手順は前述したものと同様のため、説明を省略する。ＰＩＮコード認証に成功した場合、本体アプリ６０のセキュリティ処理部６０２は、ＩＣチップの電子署名機能６２２を利用して、手続メッセージに対し電子署名を行う（ステップＳ３２０４）。このとき、電子署名機能６２２は、手続メッセージのハッシュ値を計算し、このハッシュ値を秘密鍵で暗号化することにより電子署名を生成してもよいし、手続メッセージ自体を秘密鍵で暗号化することにより電子署名を生成してもよい。そして、本体アプリ６０のメイン処理部６００は、手続要求を中間サーバＡに送信する（ステップＳ３２０５）。手続要求には、中間サーバＡへのユーザＩＤ１、手続メッセージ、電子署名が付加されている。

【０１９１】

中間サーバＡの代行制御部２１３は、手続要求を受信すると、手続要求に含まれるユーザの中間サーバへのユーザＩＤ１に基づいて、ユーザ情報記憶部２１１から対応する電子証明書を読み出し、この電子証明書を用いて、手続要求に含まれている電子署名の検証を行う（ステップＳ３２０６）。また、必要に応じて、中間サーバＡの代行制御部２１３は、電子証明書の有効性を認証局に問い合わせてもよい（ステップＳ３２０７、Ｓ３２０８）。電子署名の検証に成功し、且つ、電子証明書の有効性が確認された場合、中間サーバＡの代行制御部２１３は、手続要求が正当なユーザからのものであると判断する。すなわち、第三者によるなりすましがなく、かつ、手続メッセージの内容も改ざんされていないと判断するのである。

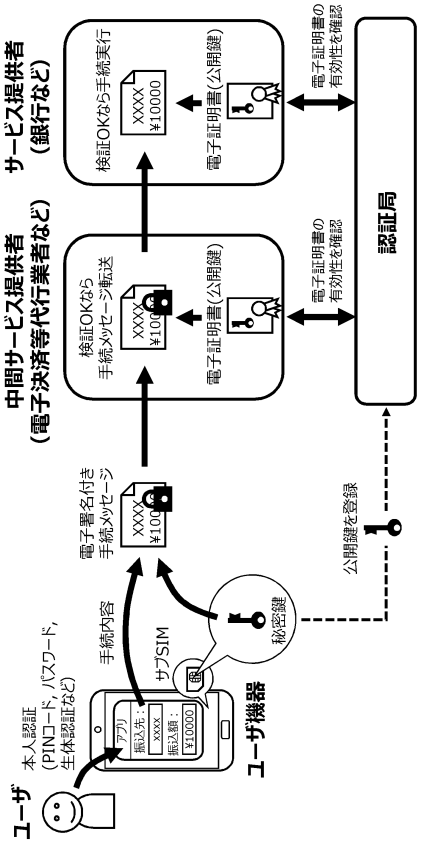
【０１９２】

手続要求が正当なユーザからのものであると確認できた場合、中間サーバＡの代行制御部２１３は、中間サーバＢに手続要求を送信する（ステップＳ３２０９）。この手続要求

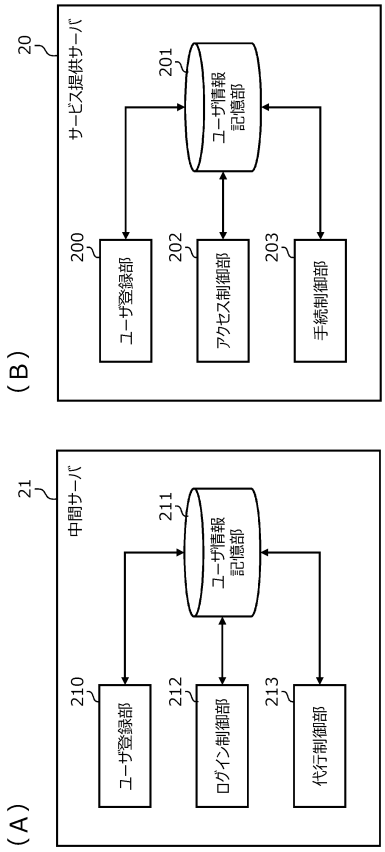
には、ユーザＩＤ１、手続メッセージ、電子署名が付加されている。
【０１９３】
中間サーバＢの代行制御部２１３は、手続要求を受信すると、手続要求に含まれるユーザＩＤ１に基づいて、ユーザ情報記憶部２１１から対応する電子証明書を読み出し、この電子証明書を用いて、手続要求に含まれている電子署名の検証を行う（ステップＳ３２１０）。また、必要に応じて、中間サーバＢの代行制御部２１３は、電子証明書の有効性を認証局に問い合わせてもよい（ステップＳ３２１１、Ｓ３２１２）。電子署名の検証に成功し、且つ、電子証明書の有効性が確認された場合、中間サーバＢの代行制御部２１３は、手続要求が正当なユーザからのものであると判断する。すなわち、第三者によるなりすましがなく、かつ、手続メッセージの内容も改ざんされていないと判断するのである。
【０１９４】
手続要求が正当なユーザからのものであると確認できた場合、中間サーバＢの代行制御部２１３は、サービス提供サーバ２０へのユーザＩＤ２とパスワード２を読み出し、サービス提供サーバ２０に手続要求を送信する（ステップＳ３２１３）。この手続要求には、ユーザ機器３０から受信した手続メッセージ及び電子署名が付加されている。
【０１９５】
サービス提供サーバ２０の手続制御部２０３は、手続要求を受信すると、ユーザＩＤ２とパスワード２の検証を行う（ステップＳ３２１４）。ユーザＩＤ２とパスワード２の検証に成功した場合、手続制御部２０３は、この手続要求が正当なユーザからのものであると判断する。すなわち、第三者によるなりすましがなく、かつ、手続メッセージの内容も改ざんされていないと判断するのである
【０１９６】
手続要求が正当なユーザからのものであると確認できた場合にのみ、手続制御部２０３は、手続メッセージに記述された情報に基づく手続（振込など）を実行する（ステップＳ３２１５）。手続が完了すると、手続制御部２０３は手続完了通知を中間サーバＢに送信し（ステップＳ３２１６）、中間サーバＢが中間サーバＡに手続完了通知を送信し（ステップＳ３２１７）、中間サーバＡが手続完了通知を本体アプリ６０に送信する（ステップＳ３２１８）。そうすると、手続完了画面が表示される。
【０１９７】
上述した各実施形態において、ユーザ機器３０が各サーバや認証局との間でインターネットを介したデータ通信を行う場合には、ユーザ機器３０が備える通信用のＳＩＭカードのＩＭＳＩ又はそのＩＭＳＩに対応付けられたＩＰアドレスによって、データの送信元あるいは送信先としてのＳＩＭカード（すなわちユーザ機器３０）が特定される。ＩＰアドレスは、動的に割り当てられるＩＰアドレスであってもよいし、固定のＩＰアドレスであってもよい。
【符号の説明】
【０１９８】
２０：サービス提供サーバ
２１：中間サーバ
３０：ユーザ機器
６０：アプリケーションプログラム
７０：ＩＣカード発行端末
３０６：ＳＩＭカード
３０７：ＩＣカード（サブＳＩＭ）
３０８：ＳＩＭカードスロット

【図面】

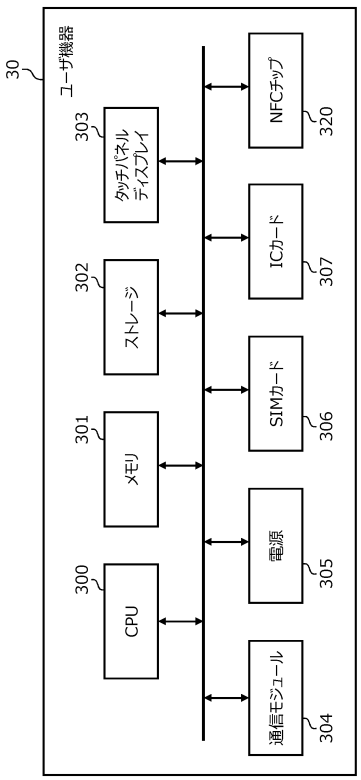
【図１】


ユーザ
本人認証
(PINコード、パスワード、
生体認証など)
ユーザ機器
アプリ
振込先：
xxxx
振込額：
¥10000
手続内容
サブSIM
秘密鍵
電子署名付き
手続メッセージ
XXXX
¥10000
公開鍵を登録
中間サービス提供者
(電子決済等代行業者など)
検証OKなら
手続メッセージ転送
電子証明書(公開鍵)
電子証明書の
有効性を確認
サービス提供者
(銀行など)
検証OKなら手続実行
電子証明書(公開鍵)
電子証明書の
有効性を確認
認証局

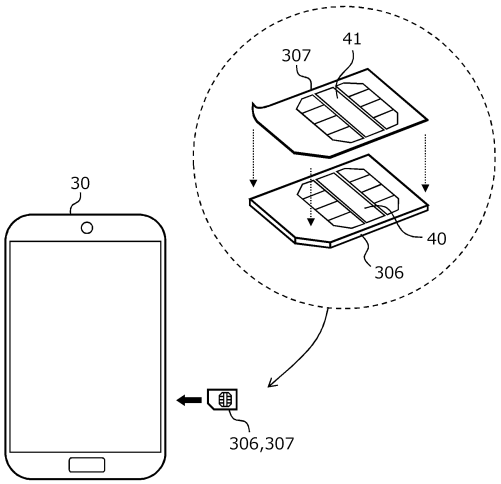
【図２】


(A)
21
中間サーバ
210
ユーザ登録部
211
ユーザ情報
記憶部
212
ログイン制御部
213
代行制御部
(B)
20
サービス提供サーバ
200
ユーザ登録部
201
ユーザ情報
記憶部
202
アクセス制御部
203
手続制御部

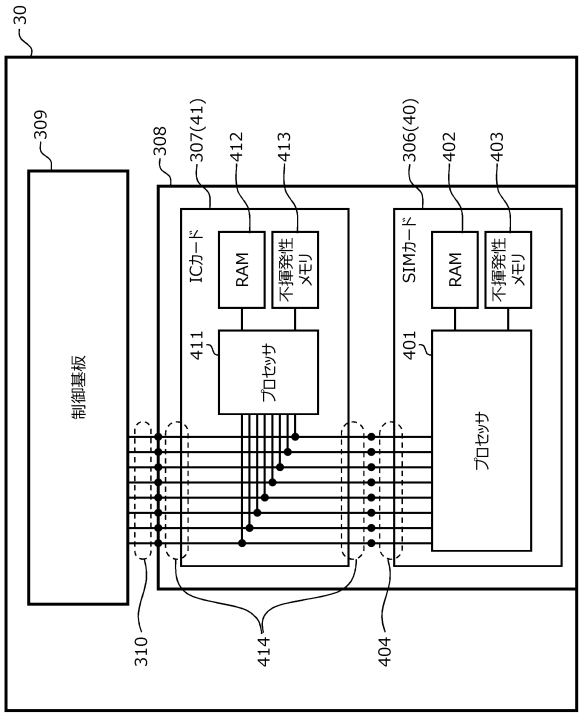
【図３】


30
ユーザ機器
300
CPU
301
メモリ
302
ストレージ
303
タッチパネル
ディスプレイ
304
通信モジュール
305
電源
306
SIMカード
307
ICカード
320
NFCチップ

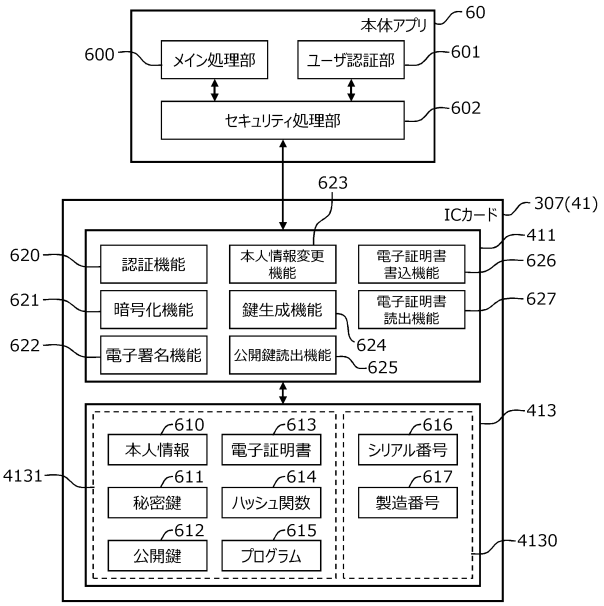
【図４】


30
306,307
307
41
40
306

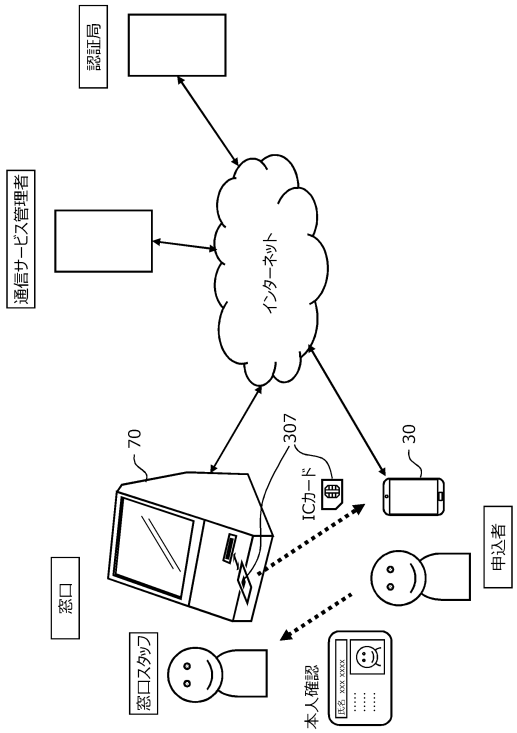
【図５】


30
309
308
307(41)
412
413
306(40)
402
403
制御基板
ICカード
RAM
不揮発性メモリ
411
プロセッサ
SIMカード
RAM
不揮発性メモリ
401
プロセッサ
310
414
404

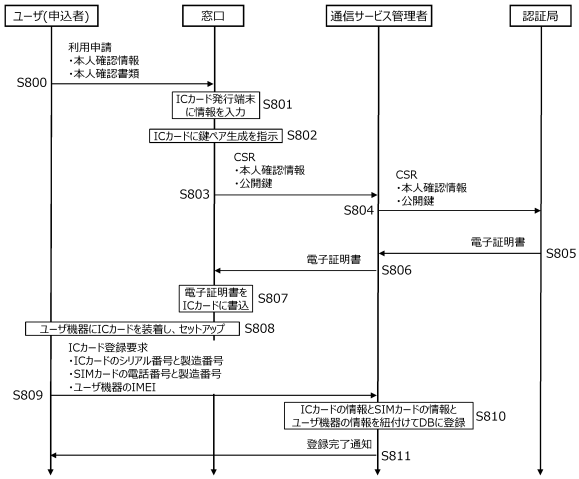
【図６】


本体アプリ
60
600
メイン処理部
ユーザ認証部
601
セキュリティ処理部
602
623
ICカード
307(41)
411
620
認証機能
本人情報変更機能
電子証明書書込機能
626
621
暗号化機能
鍵生成機能
電子証明書読出機能
627
622
電子署名機能
公開鍵読出機能
624
625
413
610
本人情報
613
電子証明書
616
シリアル番号
4131
611
秘密鍵
614
ハッシュ関数
617
製造番号
612
公開鍵
615
プログラム
4130

【図７】


認証局
通信サービス管理者
インターネット
70
307
ICカード
30
窓口
申込者
窓口スタッフ
本人確認

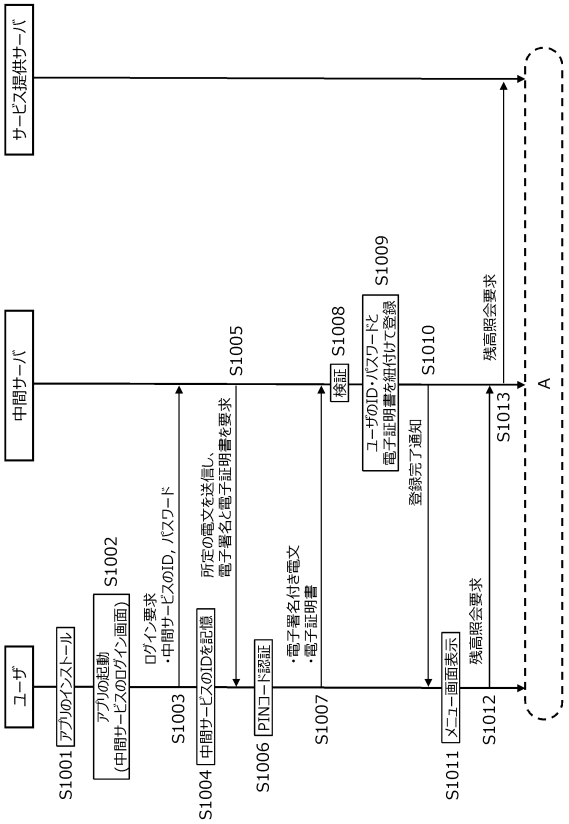
【図８】


ユーザ(申込者)
窓口
通信サービス管理者
認証局
利用申請
・本人確認情報
・本人確認書類
S800
ICカード発行端末に情報を入力
S801
ICカードに鍵ペア生成を指示
S802
CSR
・本人確認情報
・公開鍵
S803
CSR
・本人確認情報
・公開鍵
S804
電子証明書
S805
電子証明書
S806
電子証明書をICカードに書込
S807
ユーザ機器にICカードを装着し、セットアップ
S808
ICカード登録要求
・ICカードのシリアル番号と製造番号
・SIMカードの電話番号と製造番号
・ユーザ機器のIMEI
S809
ICカードの情報とSIMカードの情報とユーザ機器の情報を紐付けてDBに登録
S810
登録完了通知
S811

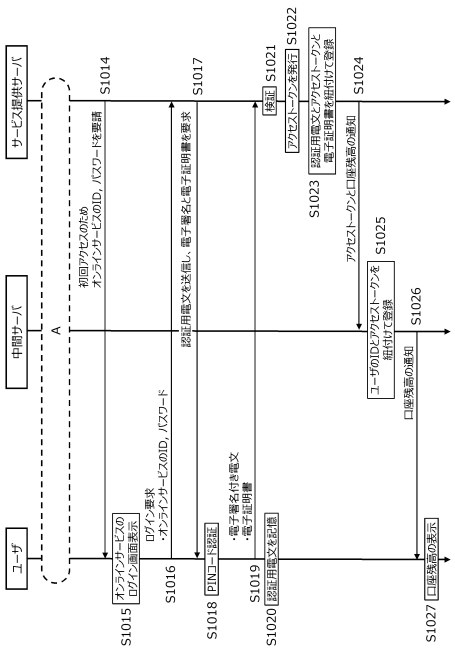
【図９】

ICカード		SIMカード		ユーザ機器
シリアル番号	製造番号	電話番号	製造番号	IMEI
10530	AZ003	090-xxxx-xxxx	ZDE21993	xx-xxxxxx-xxxxxx-x
00283	AE112	080-yyyy-yyyy	YAB02871	yy-yyyyyy-yyyyyy-y
25611	YY520	090-zzzz-zzzz	OPZ33910	zz-zzzzzz-zzzzzz-z

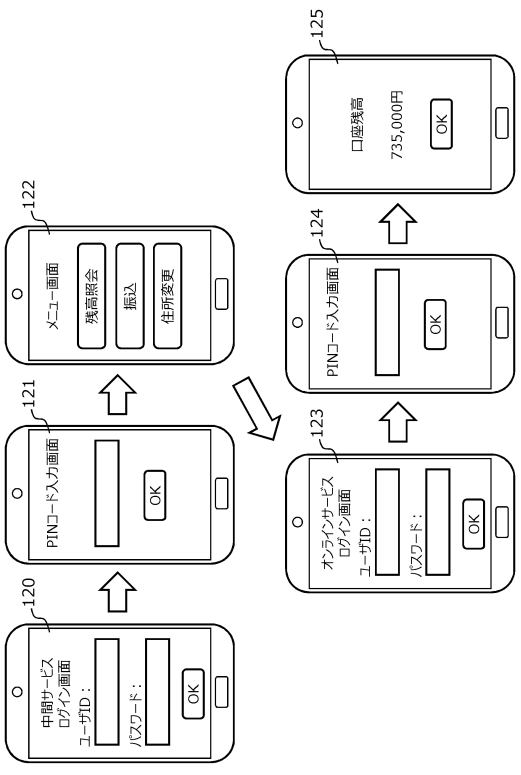
【図１０】



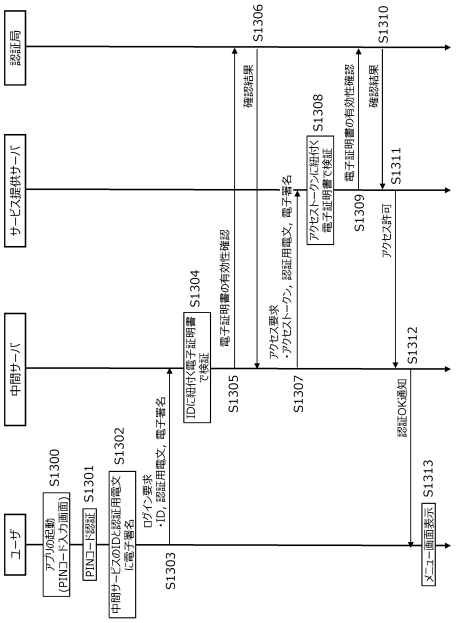
【図１１】



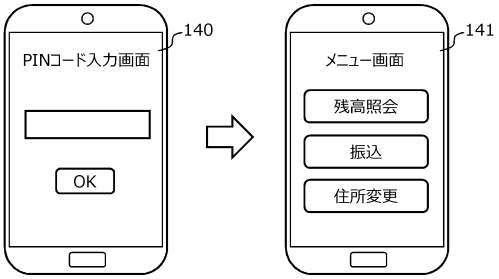
【図１２】



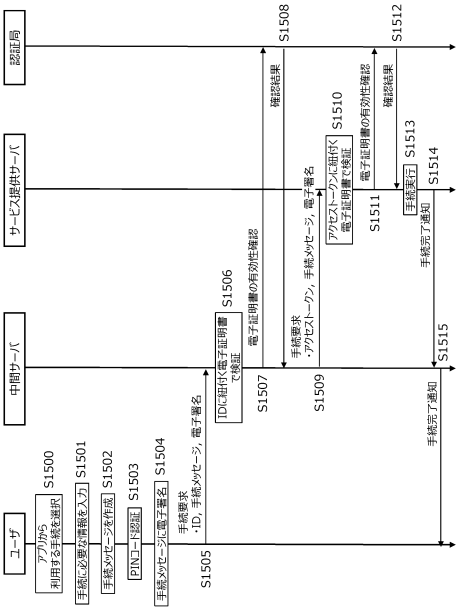
【図１３】



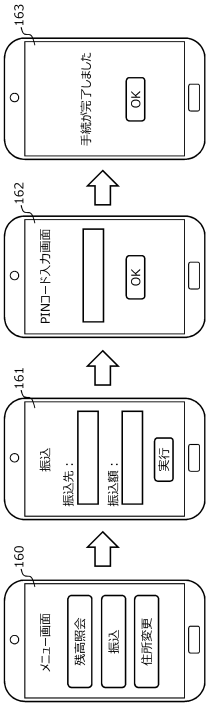
【図１４】



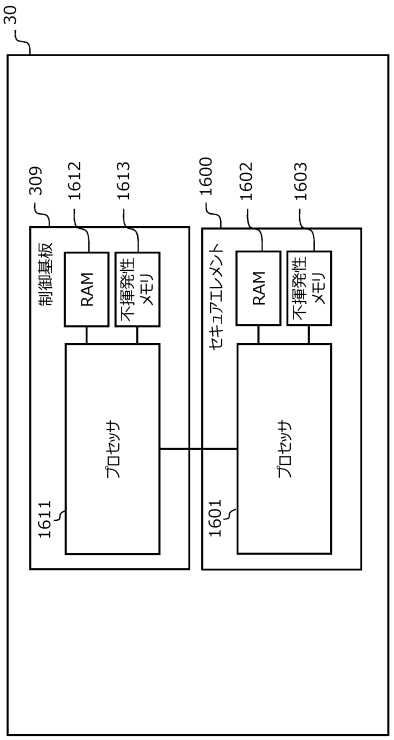
【図１５】



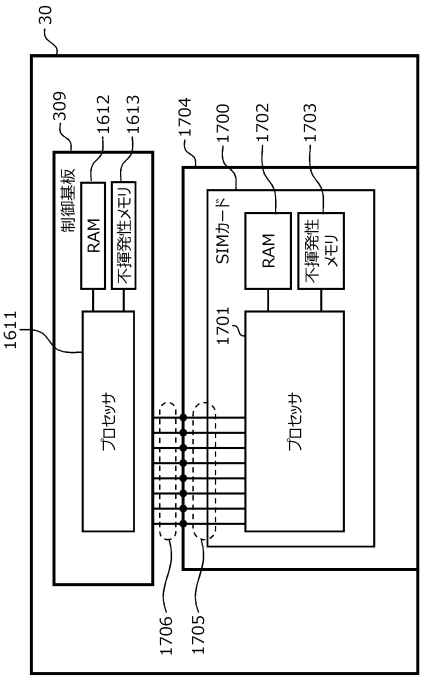
【図１６】



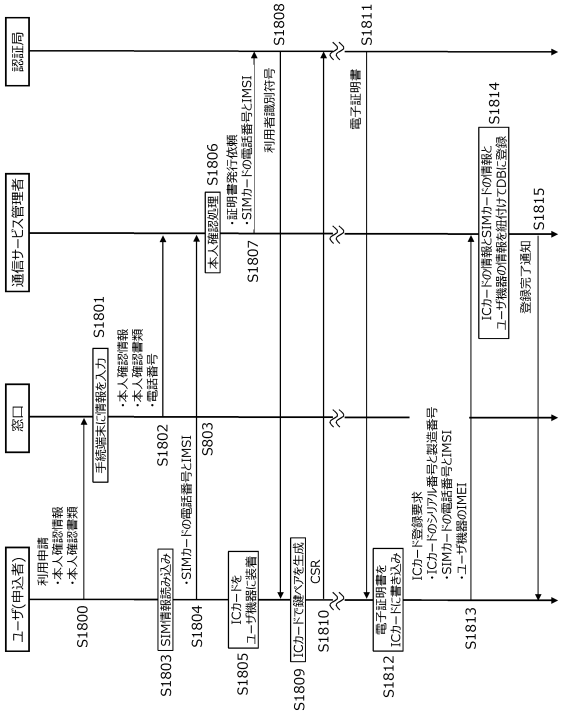
【図１７】



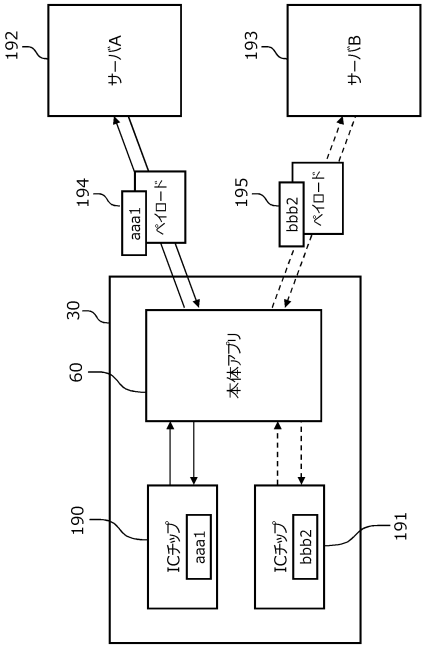
【図１８】



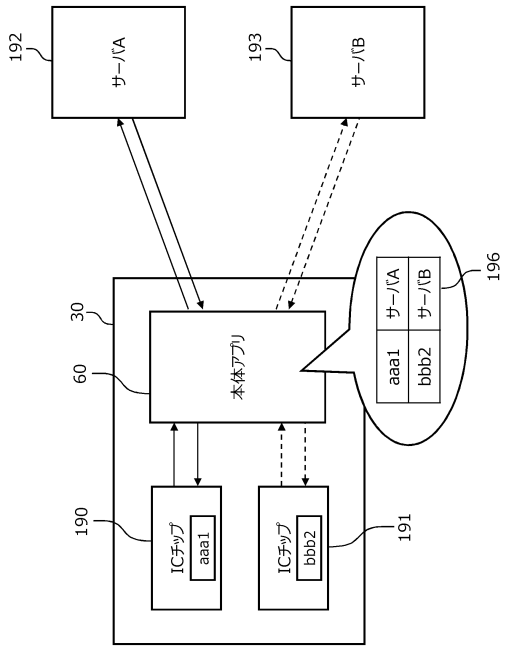
【図１９】



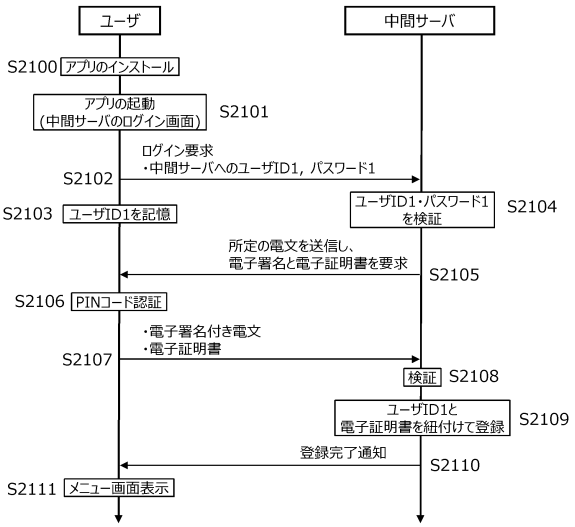
【図２０】



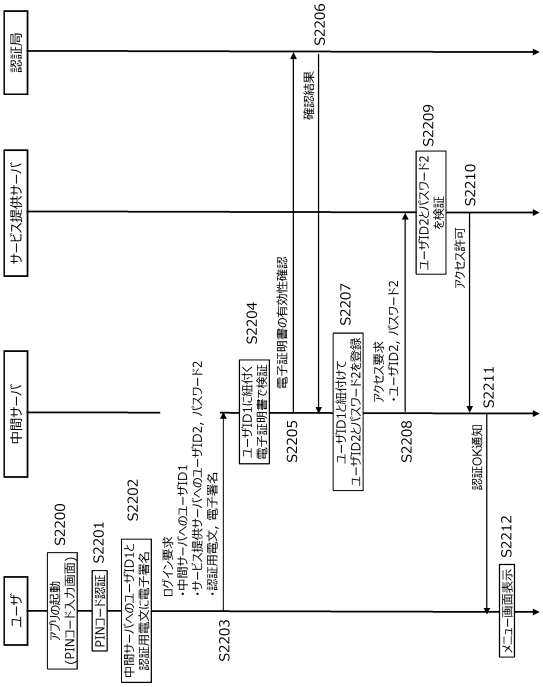
【図２１】



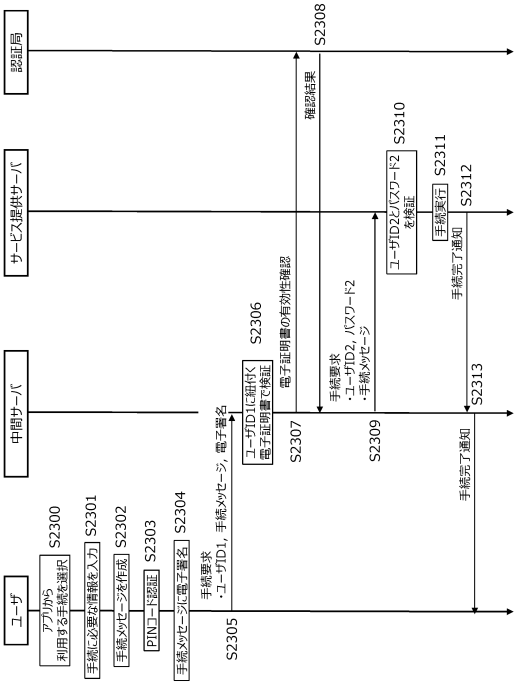
【図２２】



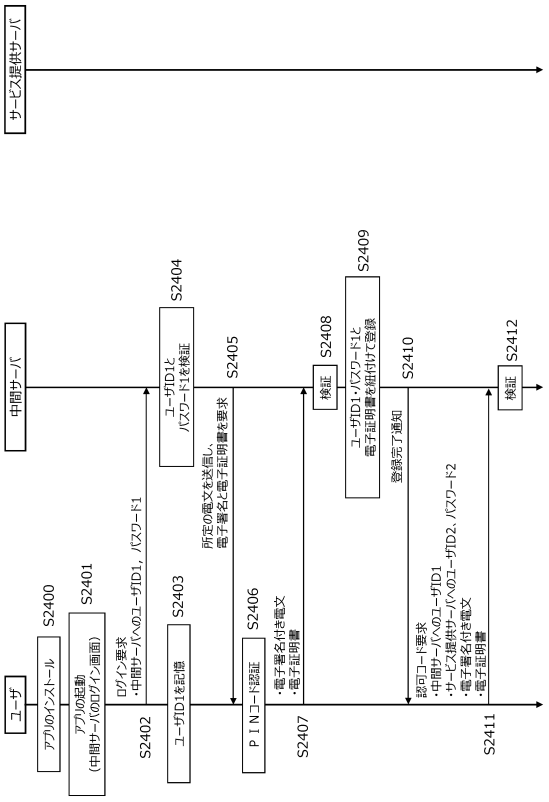
【図２３】



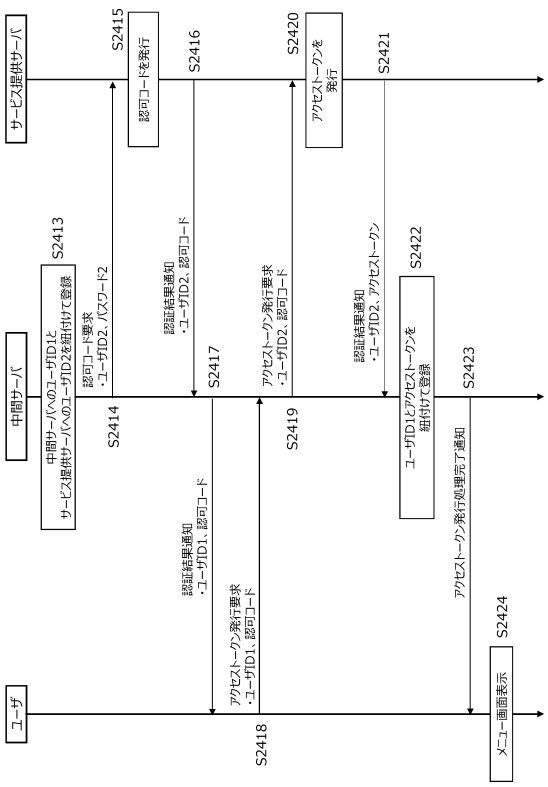
【図２４】



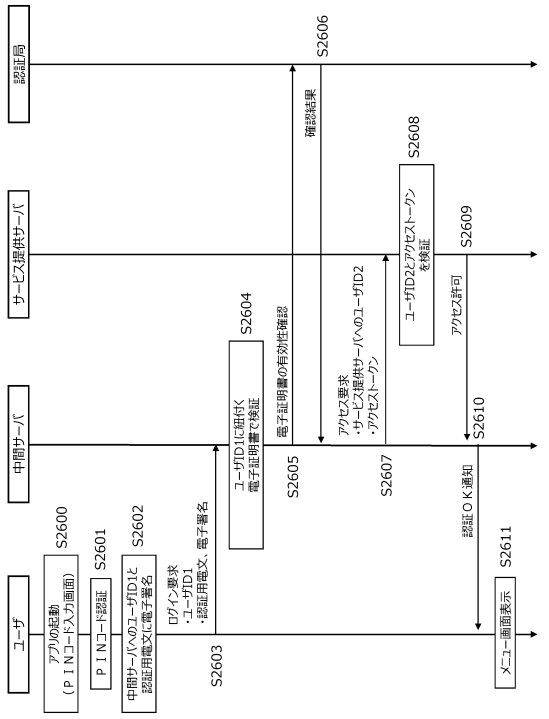
【図２５】



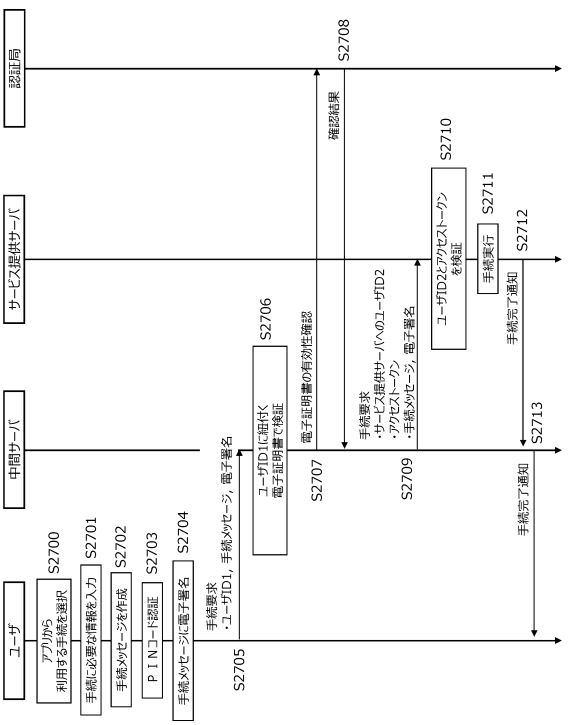
【図２６】



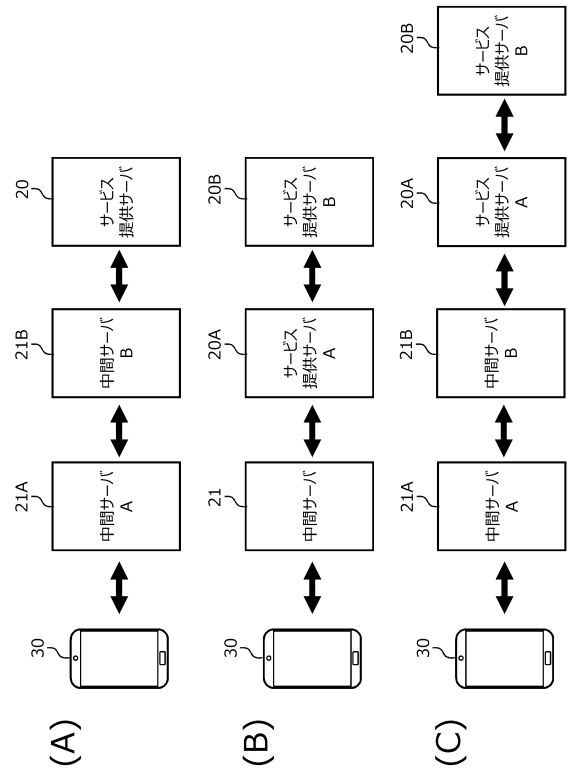
【図２７】



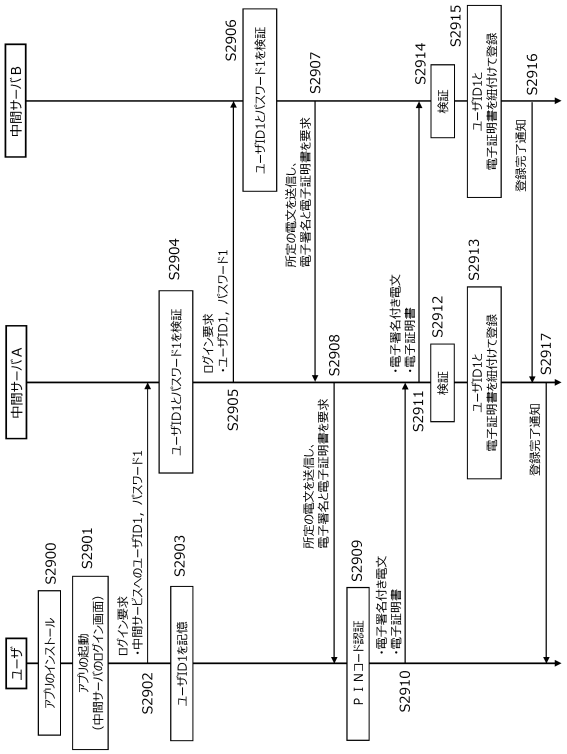
【図２８】



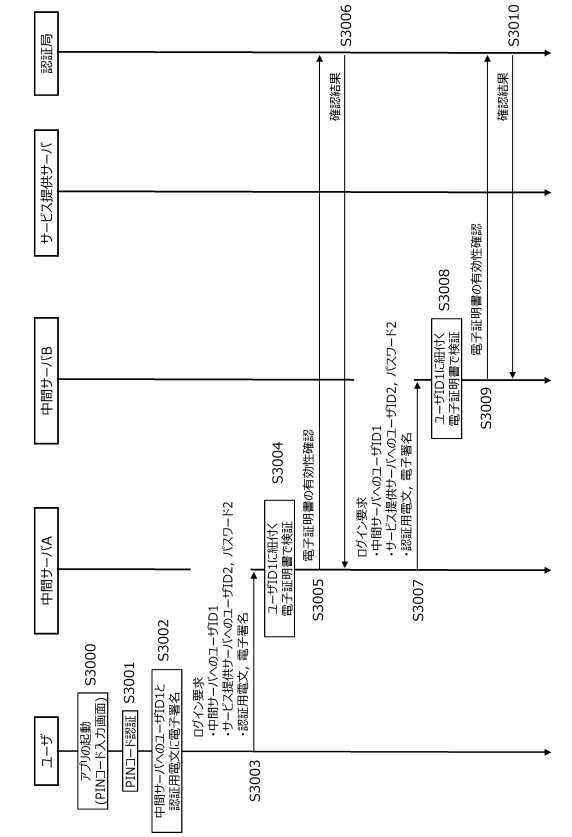
【図２９】



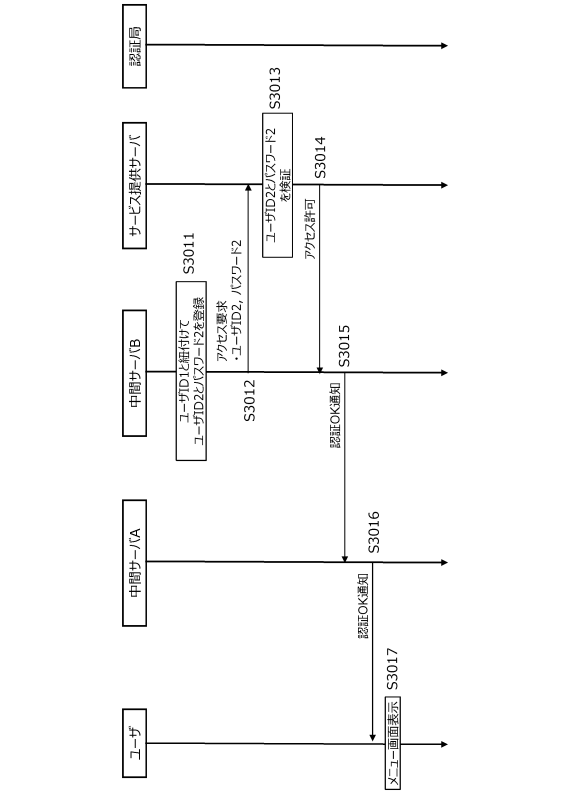
【図３０】



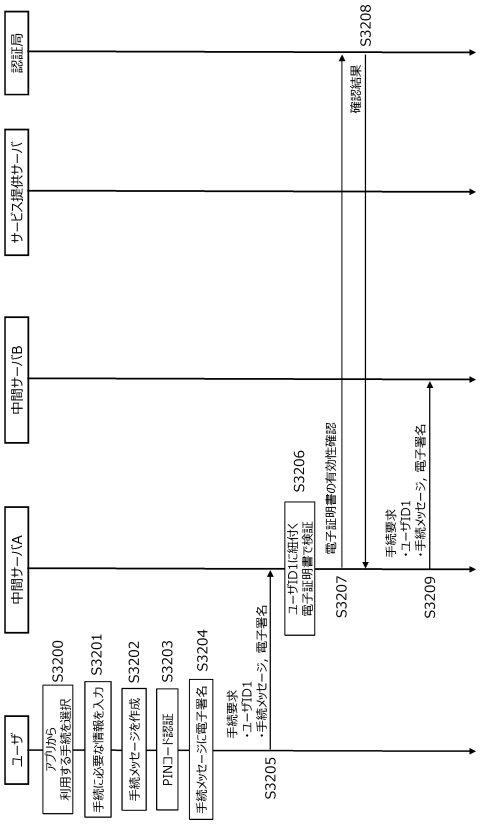
【図３１】



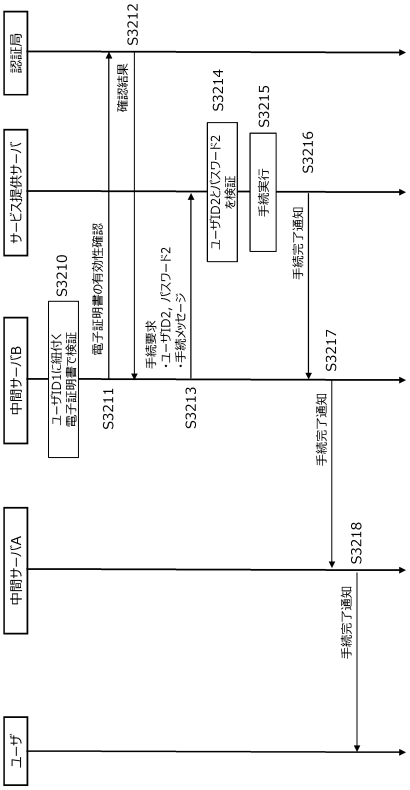
【図３２】



【図３３】


ユーザ
中間サーバA
中間サーバB
サービス提供サーバ
認証局
アプリから
利用する手続を選択
S3200
手続に必要な情報を入力
S3201
手続メッセージを作成
S3202
PINコード認証
S3203
手続メッセージに電子署名
S3204
手続要求
・ユーザID1
・手続メッセージ，電子署名
S3205
ユーザID1に紐付く
電子証明書で検証
S3206
電子証明書の有効性確認
S3207
確認結果
S3208
手続要求
・ユーザID1
・手続メッセージ，電子署名
S3209

【図３４】


ユーザ
中間サーバA
中間サーバB
サービス提供サーバ
認証局
ユーザID1に紐付く
電子証明書で検証
S3210
電子証明書の有効性確認
S3211
確認結果
S3212
手続要求
・ユーザID2，パスワード2
・手続メッセージ
S3213
ユーザID2とパスワード2
を検証
S3214
手続実行
S3215
手続完了通知
S3216
手続完了通知
S3217
手続完了通知
S3218

フロントページの続き

日本国東京都港区虎ノ門４丁目１番２８号 日本通信株式会社内
(72)発明者 林 昌孝
日本国東京都港区虎ノ門４丁目１番２８号 日本通信株式会社内

審査官 行田 悦資

(56)参考文献
特開２００９－２１７７２２（ＪＰ，Ａ）
特開２００７－０５８４５５（ＪＰ，Ａ）
国際公開第２０１７／０２２１２１（WO，Ａ１）
特開平１０－１７７５５２（ＪＰ，Ａ）
特開２０１４－０１０４８６（ＪＰ，Ａ）
特表２０１０－５０９８３８（ＪＰ，Ａ）
特開２００３－２９８５７４（ＪＰ，Ａ）
特開２００９－２３７７７４（ＪＰ，Ａ）
特開２０１７－１５７９８４（ＪＰ，Ａ）
国際公開第２００７／０９４０３５（WO，Ａ１）
特開平８－３２８４７０（ＪＰ，Ａ）
特表２０１３－５１１１８９（ＪＰ，Ａ）
国際公開第２００５／１１４５６１（WO，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０９Ｃ １／００