(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4470071号
(P4470071)
(45)発行日　平成22年6月2日(2010.6.2)　(24)登録日　平成22年3月12日(2010.3.12)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675Z
G06K 17/00 (2006.01)　G06K 17/00 L
G06K 17/00 B

請求項の数 13　(全 31 頁)

(21)出願番号　特願2008-52729(P2008-52729)
(22)出願日　平成20年3月3日(2008.3.3)
(65)公開番号　特開2009-212731(P2009-212731A)
(43)公開日　平成21年9月17日(2009.9.17)
審査請求日　平成21年7月31日(2009.7.31)

(73)特許権者　504134520
フェリカネットワークス株式会社
東京都品川区大崎１丁目１１番１号
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(72)発明者　畑岡　純
東京都品川区大崎１－１１－１　フェリカネットワークス株式会社内
(72)発明者　疋田　智治
東京都品川区大崎１－１１－１　フェリカネットワークス株式会社内
最終頁に続く

(54)【発明の名称】カード発行システム、カード発行サーバ、カード発行方法およびプログラム

(57)【特許請求の範囲】
【請求項１】
ＩＣチップを搭載した情報処理端末と、ネットワークを介して前記情報処理端末と接続可能なサービス提供サーバおよびカード発行サーバとを含むカード発行システムであって、
前記サービス提供サーバは、
前記情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成する認証チケット作成部と、
前記認証チケット作成部により作成された前記認証チケットを前記カード発行サーバに送信する認証チケット送信部と、
を備え、
前記カード発行サーバは、
前記認証チケット送信部により送信された前記認証チケットを復号化して前記認証チケットを検証する認証チケット検証部と、
前記認証チケット検証部により検証された前記認証チケットの検証結果を前記サービス提供サーバに通知する検証結果通知部と、
前記認証チケットの検証結果とともに前記カード発行サーバと接続するための接続情報を前記サービス提供サーバに送信する接続情報送信部と、
前記認証チケットのアクセス認証情報と、前記情報処理端末の前記ＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、

を備え、
前記情報処理端末は、
前記接続情報に基づいて前記カード発行サーバに接続する接続部と、
前記ＩＣチップに設けられる前記アクセス認証情報を記憶する認証情報記憶部と、
を備えることを特徴とする、カード発行システム。
【請求項２】
ＩＣチップを搭載した情報処理端末およびサービス提供サーバとネットワークを介して接続可能な、カード発行サーバであって、
前記サービス提供サーバは、前記情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成し、
前記サービス提供サーバにより作成された認証チケットを受信する認証チケット受信部と、
前記認証チケット受信部により受信された前記認証チケットを復号化して前記認証チケットを検証する認証チケット検証部と、
前記認証チケット検証部により検証された前記認証チケットの検証結果を前記サービス提供サーバに通知する検証結果通知部と、
前記認証チケットの検証結果とともに前記カード発行サーバと接続するための接続情報を前記サービス提供サーバに送信する接続情報送信部と、
前記認証チケットのアクセス認証情報と、前記情報処理端末の前記ＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、
を備えることを特徴とする、カード発行サーバ。
【請求項３】
前記サービス提供サーバは、認証用秘密鍵を用いて前記アクセス認証情報に電子署名を付加して前記認証チケットを作成し、
前記認証チケット検証部は、前記認証用秘密鍵に対応する認証用公開鍵を用いて前記認証チケットに付加された電子署名を検証することを特徴とする、請求項２に記載のカード発行サーバ。
【請求項４】
前記カード発行サーバは、ネットワークを介して前記サービス提供サーバを代行するサービス代行サーバと接続され、
前記サービス提供サーバは、前記サービス代行サーバに許諾するサービスの情報を暗号化して認証ライセンスを作成し、前記サービス代行サーバは、前記認証ライセンスに、前記情報処理端末によるアクセスを認証するためのアクセス認証情報を付加し暗号化して前記認証チケットを作成し、
前記認証チケットを復号化して前記認証ライセンスを取得する認証ライセンス取得部と、
前記認証ライセンス取得部により取得された前記認証ライセンスを復号化して前記認証ライセンスを検証する認証ライセンス検証部と、
を備え、
前記認証チケット検証部は、前記認証ライセンス検証部により検証された認証ライセンスに基づいて、前記認証チケットを検証することを特徴とする、請求項２に記載のカード発行サーバ。
【請求項５】
前記サービス提供サーバは、第１認証用秘密鍵を用いて前記利用者認証情報に第１電子署名を付加して前記認証ライセンスを作成し、前記サービス代行サーバは、前記認証ライセンスに前記アクセス認証情報を付加し、さらに第２認証用秘密鍵を用いて第２電子署名を付加して前記認証チケットを作成し、
前記認証ライセンス検証部は、前記第１認証用秘密鍵に対応する第１認証用公開鍵を用いて前記認証ライセンスに付加された前記第１電子署名を検証し、
前記認証チケット検証部は、前記認証ライセンス検証部により検証された前記認証ライ

センスに含まれる前記第２認証用秘密鍵に対応する第２認証用公開鍵を用いて前記認証チケットに付加された前記第２電子署名を検証することを特徴とする、請求項４に記載のカード発行サーバ。

【請求項６】

前記アクセス認証情報には、少なくとも、前記情報処理端末が利用する処理の情報、前記ＩＣチップの識別情報、前記ＩＣチップの発行元情報が含まれることを特徴とする、請求項２に記載のカード発行サーバ。

【請求項７】

前記アクセス認証情報には、前記ＩＣチップへの書き込みが可能か否かを判断する書き込み判断情報が含まれ、

前記認証情報検証部は、前記書き込み判断情報に基づいて、前記ＩＣチップへの書き込みを判断することを特徴とする、請求項２に記載のカード発行サーバ。

【請求項８】

前記アクセス認証情報には、前記ＩＣチップへのデータ書き込みまたは前記ＩＣチップに書き込まれたデータの利用が可能な機器の制限情報が含まれることを特徴とする、請求項２に記載のカード発行サーバ。

【請求項９】

チャレンジレスポンス認証により前記サービス提供サーバを認証するチャレンジレスポンス認証部を備えることを特徴とする、請求項２に記載のカード発行サーバ。

【請求項１０】

前記チャレンジレスポンス認証部は、チャレンジレスポンス認証により前記サービス代行サーバを認証することを特徴とする、請求項９に記載のカード発行サーバ。

【請求項１１】

前記サービス提供サーバの要求に応じて、前記情報処理端末の前記ＩＣチップへのアクセス状況を通知するアクセス状況通知部を備えることを特徴とする、請求項２に記載のカード発行サーバ。

【請求項１２】

前記アクセス状況通知部は、前記サービス提供サーバの要求に応じて、前記ＩＣチップに記憶された前記アクセス認証情報を前記サービス提供サーバに送信するアクセス認証情報送信部を備えることを特徴とする、請求項１１に記載のカード発行サーバ。

【請求項１３】

コンピュータを、

ＩＣチップを搭載した情報処理端末およびサービス提供サーバとネットワークを介して接続可能な、カード発行サーバであって、

前記サービス提供サーバは、前記情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成し、

前記サービス提供サーバにより作成された認証チケットを受信する認証チケット受信部と、

前記認証チケット受信部により受信された前記認証チケットを復号化して前記認証チケットを検証する認証チケット検証部と、

前記認証チケット検証部により検証された前記認証チケットの検証結果を前記サービス提供サーバに通知する検証結果通知部と、

前記認証チケットの検証結果とともに前記カード発行サーバと接続するための接続情報を前記サービス提供サーバに送信する接続情報送信部と、

前記認証チケットのアクセス認証情報と、前記情報処理端末の前記ＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、

を備えるカード発行サーバとして機能させるための、プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】
本発明は、カード発行システム、カード発行サーバ、カード発行方法およびプログラムに関し、特に、効率的にＩＣチップへの不正アクセスを防止することが可能なカード発行システム、カード発行サーバ、カード発行方法およびプログラムに関する。
【背景技術】
【０００２】
近年、携帯電話などに搭載されるＩＣチップに、金融機関等のサービス提供者により発行されるカードのカード番号や、当該カードにより利用可能なサービスの種類等を書き込み、ＩＣチップが搭載された携帯電話をサービス提供者が発行したカードと同様に利用できる技術が実現されている。通常、ＩＣチップは耐タンパ性を有しており、ＩＣチップに書き込まれたデータはセキュアに保持されている。セキュア情報を保持したＩＣチップへのアクセスやデータの書き込みを行うためには、ＩＣチップにアクセスするためのシステムを構築したり、ＩＣチップにアクセスするための情報を開示したりする必要がある。そのため、サービス提供者の依頼に基づいて、カード発行代行者がＩＣチップへのアクセスやデータの書き込み等行っている。
【０００３】
また、携帯電話などに搭載されたＩＣチップにネットワーク経由でアクセスする場合には、ＩＣチップを制御しているクライアントアプリからのリクエストが必要となる。したがって、ＩＣチップにアクセスしてカードの発行を行うためには、カード発行代行者、サービス提供者、クライアントアプリの三者間において相互に認証する必要がある。当該三者間の認証には、ワンタイムパスワード等を用いて実現可能である。ワンタイムパスワードを用いた認証は、例えば以下の方法が挙げられる。
【０００４】
まず、携帯電話のクライアントアプリとサービス提供者のサーバとの間の認証が行われた後、サービス提供者のサーバ（以下サービス提供サーバと称する。）とカード発行代行者のサーバ（以下カード発行サーバと称する。）との間で相互認証を行う。そして、カード発行サーバは、クライアントアプリからのリクエストを認証するためのワンタイムパスワード（トークン）を、サービス提供サーバを経由して携帯電話のクライアントアプリに通知する。これにより、カード発行サーバは、カード情報を書き込む対象となるＩＣチップを搭載した携帯電話のクライアントアプリを特定することができる。携帯電話のクライアントアプリは、カード発行サーバへのリクエスト送信時に、通知されたトークンをカード発行サーバに通知し、カード発行サーバは通知されたトークンを検証することにより携帯電話のクライアントアプリの認証を行う。
【０００５】
上記方式の場合、クライアントアプリの認証は、クライアントアプリからのリクエスト送信時のみしか行うことができない。トークンの取得を事前にオフラインで実施しておくこともできるが、この場合、カード発行サーバにおけるトークンの保持機関が長くなるため、システムへの負荷が増加してしまうという問題があった。そこで、この問題を解決するために、クライアントアプリから送信された個別化情報に基づいて生成された認証用ライセンスを用いて三者間の相互認証を実現する技術が開示されている（例えば特許文献１）。特許文献１では、クライアントアプリから個別化情報を送信されたサービス提供サーバが認証用ライセンスを生成し、生成された認証用ライセンスがクライアントアプリからカード発行サーバに送信される。カード発行サーバは、送信された認証用ライセンスを検証することにより、クライアントアプリ、携帯端末、サービス提供サーバの認証を行うことが可能となる。
【０００６】
【特許文献１】特開２００６－２４６０１５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】

ここで、カード発行サーバが、インターネット等のネットワーク経由で携帯電話に搭載されたＩＣチップにアクセスする場合には、事前にＩＣチップの正当性を検証する必要がある。しかしながら、上記特許文献１では、クライアントアプリとサービス提供サーバとカード発行サーバとの三者間の相互認証を実現することができるが、カード発行サーバが、事前にＩＣチップの検証を行ったり、ＩＣチップに記憶されたカード情報等を検知したりすることができないという問題があった。また、サービス提供サーバは、カード発行サーバが実施した処理結果を効率的に確認することができないという問題があった。

【０００８】

そこで、本発明は、上記問題に鑑みてなされたものであり、本発明の目的とするところは、ＩＣチップに記憶されたカード情報へのアクセス前にＩＣチップの個別情報を取得して、事前にＩＣチップの検証をして、効率的にＩＣチップへの不正アクセスを防止することが可能な、新規かつ改良された、カード発行システム、カード発行サーバ、カード発行方法およびプログラムを提供することにある。

【課題を解決するための手段】

【０００９】

上記課題を解決するために、本発明のある観点によれば、ＩＣチップを搭載した情報処理端末と、ネットワークを介して情報処理端末と接続可能なサービス提供サーバおよびカード発行サーバとを含むカード発行システムが提供される。上記サービス提供サーバは、情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成する認証チケット作成部と、認証チケット作成部により作成された認証チケットをカード発行サーバに送信する認証チケット送信部と、を備える。

【００１０】

カード発行サーバは、認証チケット送信部により送信された認証チケットを復号化して認証チケットを検証する認証チケット検証部と、認証チケット検証部により検証された認証チケットの検証結果をサービス提供サーバに通知する検証結果通知部と、認証チケットの検証結果とともにカード発行サーバと接続するための接続情報をサービス提供サーバに送信する接続情報送信部と、認証チケットのアクセス認証情報と、情報処理端末のＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、を備える。上記情報処理端末は、接続情報に基づいてカード発行サーバに接続する接続部と、ＩＣチップに設けられるアクセス認証情報を記憶する認証情報記憶部と、を備える。

【００１１】

かかる構成によれば、サービス提供サーバが情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成して、当該認証チケットがカード発行サーバに送信される。カード発行サーバは、認証チケットを検証して、検証結果をサービス提供サーバに通知したり、カード発行サーバに接続するための接続情報を送信したりする。そして、サービス提供サーバ経由で接続情報を送信された情報処理端末がカード発行サーバに接続して、カード発行サーバが情報処理端末のＩＣチップにアクセスすることができる。

【００１２】

上記課題を解決するために、本発明の別の観点によれば、ＩＣチップを搭載した情報処理端末およびサービス提供サーバとネットワークを介して接続可能な、カード発行サーバであって、サービス提供サーバは、情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成し、サービス提供サーバにより作成された認証チケットを受信する認証チケット受信部と、認証チケット受信部により受信された認証チケットを復号化して認証チケットを検証する認証チケット検証部と、認証チケット検証部により検証された認証チケットの検証結果をサービス提供サーバに通知する検証結果通知部と、認証チケットの検証結果とともにカード発行サーバと接続するための接続情報をサービス提供サーバに送信する接続情報送信部と、認証チケットのアクセス認証情報と、情報処理端末のＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、を備えるカード発行サーバが提供される。

【００１３】
かかる構成により、サービス提供サーバが情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成して、当該認証チケットがカード発行サーバに送信される。カード発行サーバは、認証チケットを検証して、検証結果をサービス提供サーバに通知したり、カード発行サーバに接続するための接続情報を送信したりする。そして、サービス提供サーバ経由で接続情報を送信された情報処理端末がカード発行サーバに接続して、カード発行サーバが情報処理端末のＩＣチップにアクセスすることができる。
【００１４】
また、サービス提供サーバは、認証用秘密鍵を用いてアクセス認証情報に電子署名を付加して認証チケットを作成し、認証チケット検証部は、認証用秘密鍵に対応する認証用公開鍵を用いて認証チケットに付加された電子署名を検証するようにしてもよい。
【００１５】
また、カード発行サーバは、ネットワークを介してサービス提供サーバを代行するサービス代行サーバと接続され、サービス提供サーバは、サービス代行サーバに許諾するサービスの情報を暗号化して認証ライセンスを作成し、サービス代行サーバは、認証ライセンスに、情報処理端末によるアクセスを認証するためのアクセス認証情報を付加し暗号化して認証チケットを作成し、認証チケットを復号化して認証ライセンスを取得する認証ライセンス取得部と、認証ライセンス取得部により取得された認証ライセンスを復号化して認証ライセンスを検証する認証ライセンス検証部と、を備え、認証チケット検証部は、認証ライセンス検証部により検証された認証ライセンスに基づいて、認証チケットを検証するようにしてもよい。
【００１６】
かかる構成により、サービス提供サーバがサービス代行サーバに依頼する処理のみを実行可能な認証ライセンスを作成して、当該認証ライセンスに基づいて認証チケットを作成する。このように、認証チケットを多段構成とすることにより、サービス提供サーバがサービス代行サーバに代行処理を依頼するに際し、セキュリティを維持して実行可能な処理を限定できることとなる。また、認証ライセンスおよび認証チケットの各々に異なる認証鍵を利用する多段構成とすることにより、サービス提供サーバがサービス代行サーバ等に処理を代行する場合においても、相互に認証をすることが可能となる。
【００１７】
サービス提供サーバは、第１認証用秘密鍵を用いて利用者認証情報に第１電子署名を付加して認証ライセンスを作成し、サービス代行サーバは、認証ライセンスにアクセス認証情報を付加し、さらに第２認証用秘密鍵を用いて第２電子署名を付加して認証チケットを作成し、認証ライセンス検証部は、第１認証用秘密鍵に対応する第１認証用公開鍵を用いて認証ライセンスに付加された第１電子署名を検証し、認証チケット検証部は、認証ライセンス検証部により検証された認証ライセンスに含まれる第２認証用秘密鍵に対応する第２認証用公開鍵を用いて認証チケットに付加された第２電子署名を検証するようにしてもよい。
【００１８】
かかる構成により、このように、認証ライセンスおよび認証チケットの各々に異なる認証鍵を利用する多段構成とすることにより、サービス提供サーバがサービス代行サーバ等に処理を代行する場合においても、相互に認証を可能とし、代行させる処理を制限することが可能となる。
【００１９】
アクセス認証情報には、少なくとも、情報処理端末が利用する処理の情報、ＩＣチップの識別情報、ＩＣチップの発行元情報が含まれるようにしてもよい。情報端末が利用する処理の情報とは、サービス提供者が提供するサービスに関する処理の情報である。これにより、認証チケットに基づいてＩＣチップの認証をすることが可能となる。
【００２０】

アクセス認証情報には、ＩＣチップへの書き込みが可能か否かを判断する書き込み判断情報が含まれ、認証情報検証部は、書き込み判断情報に基づいて、ＩＣチップへの書き込みを判断するようにしてもよい。これにより、特定のＩＣカード対応端末やＩＣカードのみに対する処理を実行することが可能となる。アクセス認証情報には、ＩＣチップへのデータ書き込みまたはＩＣチップに書き込まれたデータの利用が可能な機器の制限情報が含まれるようにしてもよい。

【００２１】

チャレンジレスポンス認証によりサービス提供サーバを認証するようにしてもよい。また、チャレンジレスポンス認証部は、チャレンジレスポンス認証によりサービス代行サーバを認証するようにしてもよい。これにより、よりセキュリティを高めた認証を行うことが可能となる。

【００２２】

また、サービス提供サーバの要求に応じて、情報処理端末のＩＣチップへのアクセス状況を通知するアクセス状況通知部を備えるようにしてもよい。また、アクセス状況通知部は、サービス提供サーバの要求に応じて、ＩＣチップに記憶されたアクセス認証情報をサービス提供サーバに送信するアクセス認証情報送信部を備えてもよい。これにより、クライアントアプリが信頼できない場合や、クライアントアプリとサービス提供サーバとの間の通信経路が信頼できない場合などにおいて、クライアントアプリに対する正確な処理結果をサービス提供サーバが把握することが可能となる。

【００２３】

上記課題を解決するために、本発明の別の観点によれば、ＩＣチップを搭載した情報処理端末と、ネットワークを介して情報処理端末と接続可能なサービス提供サーバおよびカード発行サーバとを含むカード発行システムが提供される。上記サービス提供サーバは、情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成する認証チケット作成部と、認証チケット作成部により作成された認証チケットを情報処理端末に送信する認証チケット送信部と、を備える。上記情報処理端末は、サービス提供サーバに備わる認証チケット送信部により送信された認証チケットをカード発行サーバに送信する認証チケット送信部を備える。

【００２４】

上記カード発行サーバは、情報処理端末に備わる認証チケット送信部により送信された認証チケットを復号化して認証チケットを検証する認証チケット検証部と、認証チケット検証部により検証された認証チケットの検証結果を情報処理端末に通知する検証結果通知部と、認証チケットの検証結果とともにカード発行サーバと接続するための接続情報を情報処理端末に送信する接続情報送信部と、認証チケットのアクセス認証情報と、情報処理端末のＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、を備える。

【００２５】

かかる構成によれば、サービス提供サーバにより作成された認証チケットを情報処理端末のクライアントアプリに送信し、クライアントアプリがカード発行サーバと接続して認証チケットを送信することによりＩＣカードの認証処理を実行することが可能となる。これにより、サービス提供サーバとカード発行サーバとの通信を削減し、サービス提供サーバの構築工数も削減することが可能となる。

【００２６】

上記課題を解決するために、本発明の別の観点によれば、ＩＣチップを搭載した情報処理端末およびサービス提供サーバとネットワークを介して接続可能な、カード発行サーバであって、サービス提供サーバは、情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成し、情報処理端末を経由してサービス提供サーバにより作成された認証チケットを受信する認証チケット受信部と、認証チケット受信部により受信された認証チケットを復号化して認証チケットを検証する認証チケット検証部と、認証チケット検証部により検証された認証チケットの検証結果を前期情報処理端末

に通知する検証結果通知部と、認証チケットのアクセス認証情報と、情報処理端末のＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、を備えるカード発行サーバが提供される。

【００２７】

上記課題を解決するために、本発明の別の観点によれば、ＩＣチップを搭載した情報処理端末と、ネットワークを介して情報処理端末と接続可能なサービス提供サーバおよびサービス代行サーバおよびカード発行サーバとを含むカード発行システムが提供される。上記サービス提供サーバは、サービス提供サーバがサービス代行サーバに許諾するサービスの情報を暗号化して認証ライセンスを作成する認証ライセンス作成部と、認証ライセンス作成部により作成された認証ライセンスをサービス代行サーバに送信する認証ライセンス送信部と、を備える。上記サービス代行サーバは、認証ライセンス送信部により送信された認証ライセンスに、情報処理端末によるアクセスを認証するためのアクセス認証情報を付加して暗号化し、認証チケットを作成する認証チケット作成部と、認証チケット作成部により作成された認証チケットをカード発行サーバに送信する認証チケット送信部と、を備える。

【００２８】

上記カード発行サーバは、認証チケット送信部により送信された認証チケットを復号化して認証ライセンスを取得する認証ライセンス取得部と、認証ライセンス取得部により取得された認証ライセンスを復号化して認証ライセンスを検証する認証ライセンス検証部と、認証ライセンス検証部により検証された認証ライセンスに基づいて、認証チケットを検証する認証チケット検証部と、を備える。

【００２９】

上記課題を解決するために、本発明の別の観点によれば、ＩＣチップを搭載した情報処理端末と、ネットワークを介して情報処理端末と接続可能なサービス提供サーバおよびカード発行サーバとを用いて実現されたカード発行方法であって、サービス提供サーバが、情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成するステップと、認証チケットをカード発行サーバに送信するステップと、カード発行サーバが、サービス提供サーバにより送信された認証チケットを復号化して認証チケットを検証するステップと、検証された認証チケットの検証結果をサービス提供サーバに通知するステップと、認証チケットの検証結果とともにカード発行サーバと接続するための接続情報をサービス提供サーバに送信するステップと、認証チケットのアクセス認証情報と、情報処理端末のＩＣチップに記憶されたアクセス認証情報とを比較して検証するステップと、情報処理端末が、接続情報に基づいてカード発行サーバに接続するステップと、を含むカード発行方法が提供される。

【００３０】

上記課題を解決するために、本発明の別の観点によれば、ＩＣチップを搭載した情報処理端末と、ネットワークを介して情報処理端末と接続可能なサービス提供サーバおよびカード発行サーバとを用いて実現されるカード発行方法であって、サービス提供サーバが、情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成するステップと、認証チケットを情報処理端末に送信するステップと、情報処理端末が、サービス提供サーバにより送信された認証チケットをカード発行サーバに送信するステップと、カード発行サーバが、情報処理端末に備わる認証チケット送信部により送信された認証チケットを復号化して認証チケットを検証するステップと、検証された認証チケットの検証結果を情報処理端末に通知するステップと、認証チケットの検証結果とともにカード発行サーバと接続するための接続情報を情報処理端末に送信するステップと、

認証チケットのアクセス認証情報と、情報処理端末のＩＣチップに記憶されたアクセス認証情報とを比較して検証するステップと、を含むカード発行方法が提供される。

【００３１】

上記課題を解決するために本発明の別の観点によれば、ＩＣチップを搭載した情報処理端末と、ネットワークを介して情報処理端末と接続可能なサービス提供サーバおよびサー

ビス代行サーバおよびカード発行サーバとを用いて実現されるカード発行方法であって、サービス提供サーバが、サービス提供サーバがサービス代行サーバに許諾するサービスの情報を暗号化して認証ライセンスを作成するステップと、認証ライセンスをサービス代行サーバに送信するステップと、サービス代行サーバが、認証ライセンス送信部により送信された認証ライセンスに、情報処理端末によるアクセスを認証するためのアクセス認証情報を付加して暗号化し、認証チケットを作成するステップと、認証チケットをカード発行サーバに送信するステップと、カード発行サーバが、認証チケットを復号化して認証ライセンスを取得するステップと、取得された認証ライセンスを復号化して認証ライセンスを検証するステップと、検証された認証ライセンスに基づいて、認証チケットを検証するステップと、を含むカード発行方法が提供される。

【００３２】

上記課題を解決するために本発明の別の観点によれば、コンピュータを、ＩＣチップを搭載した情報処理端末およびサービス提供サーバとネットワークを介して接続可能な、カード発行サーバであって、サービス提供サーバは、情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成し、サービス提供サーバにより作成された認証チケットを受信する認証チケット受信部と、認証チケット受信部により受信された認証チケットを復号化して認証チケットを検証する認証チケット検証部と、認証チケット検証部により検証された認証チケットの検証結果をサービス提供サーバに通知する検証結果通知部と、認証チケットの検証結果とともにカード発行サーバと接続するための接続情報をサービス提供サーバに送信する接続情報送信部と、認証チケットのアクセス認証情報と、情報処理端末のＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、を備えるカード発行サーバとして機能させるための、プログラムが提供される。

【００３３】

また、上記コンピュータを、上記カード発行サーバは、ネットワークを介してサービス提供サーバを代行するサービス代行サーバと接続され、サービス提供サーバは、サービス代行サーバに許諾するサービスの情報を暗号化して認証ライセンスを作成し、サービス代行サーバは、認証ライセンスに、情報処理端末によるアクセスを認証するためのアクセス認証情報を付加し暗号化して認証チケットを作成し、認証チケットを復号化して認証ライセンスを取得する認証ライセンス取得部と、認証ライセンス取得部により取得された認証ライセンスを復号化して認証ライセンスを検証する認証ライセンス検証部と、を備え、認証チケット検証部は、認証ライセンス検証部により検証された認証ライセンスに基づいて、認証チケットを検証するカード発行サーバとして機能させるようにしてもよい。

【００３４】

上記課題を解決するために、本発明の別の観点によれば、コンピュータを、ＩＣチップを搭載した情報処理端末およびサービス提供サーバとネットワークを介して接続可能な、カード発行サーバであって、サービス提供サーバは、情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成し、情報処理端末を経由してサービス提供サーバにより作成された認証チケットを受信する認証チケット受信部と、認証チケット受信部により受信された認証チケットを復号化して認証チケットを検証する認証チケット検証部と、認証チケット検証部により検証された認証チケットの検証結果を前期情報処理端末に通知する検証結果通知部と、認証チケットのアクセス認証情報と、情報処理端末のＩＣチップに記憶されたアクセス認証情報とを比較して検証する認証情報検証部と、を備えるカード発行サーバとして機能させるためのプログラムが提供される。

【発明の効果】

【００３５】

以上説明したように本発明によれば、ＩＣチップに記憶されたカード情報へのアクセス前にＩＣチップの個別情報を取得して、事前にＩＣチップの検証をして、効率的にＩＣチップへの不正アクセスを防止することができる。

【発明を実施するための最良の形態】

【００３６】
以下に添付図面を参照しながら、本発明の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。
【００３７】
（第１の実施形態）
まず、本発明の第１の実施形態にかかるカード発行システムの概要について説明する。図１は、本実施形態にかかるカード発行システム１０の構成例を示した説明図である。図１に示したように、カード発行システム１０は、情報処理端末１００と、サービス提供サーバ２００と、カード発行サーバ３００と、ネットワーク５０などを含んで構成される。情報処理端末１００と、サービス提供サーバ２００と、カード発行サーバ３００とは、ネットワーク５０を介して接続されている。ネットワーク５０は、例えばインターネット、電話回線網、衛星通信網等の公衆回線網や、ＷＡＮ、ＬＡＮ、ＩＰ－ＶＰＮ等の専用回線網などで構成されており、有線、無線を問わない。
【００３８】
情報処理端末１００は、ＩＣチップ１５０を搭載した携帯端末である。以下では、情報処理端末１００の一例として、ＩＣチップ１５０を搭載した携帯電話を本発明の情報処理端末に適用して説明するが、かかる例に限定されるものではない。情報処理端末１００は、例えば、ＩＣチップを搭載したＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）、腕時計、携帯音楽プレーヤ等であってもよい。ＩＣチップ１５０は、情報処理装置１００にＩＣチップ１５０が組み込まれていてもよいし、ＩＣチップが接触または非接触通信等により接続されていてもよい。
【００３９】
ＩＣチップ１５０は、耐タンパ性を有するセキュアメモリである。また、ＩＣチップ１５０は、接触通信可能であっても、非接触通信可能であってもよい。情報処理端末１００は、複数のＩＣチップを搭載していてもよく、用途に応じて各ＩＣチップを使い分ける構成としてもよい。以下では、主に、サービス提供サーバ２００により提供されるサービスを提供可能な一つのＩＣチップを搭載された情報処理端末１００を例に挙げて説明する。なお、情報処理端末１００におけるネットワーク５０を介した接続とは、ＨＴＴＰやＨＴＴＰＳなどによるＴＣＰ／ＩＰ通信のみでなく、情報処理端末１００が具備する通信機能一般を指し、赤外線通信、２次元バーコードによる通信、メールなどを含む。
【００４０】
サービス提供サーバ２００は、情報処理端末１００に搭載されるＩＣチップ１５０に対して、データの書き込みや読み込みなどを実行することで、情報処理端末１００を使用する利用者にサービスを提供する。サービス提供サーバ２００は、金融機関等のサービス提供者が有するサーバであって、カード会社等の有するサーバを例示できる。サービス提供サーバ２００は、ＩＣチップ１５０へのデータの書き込みや読み込みなどのＩＣカード発行処理をカード発行サーバ３００に依頼する。サービス提供サーバ２００がカード発行サーバ３００にＩＣカードの発行を依頼する場合には、情報処理端末１００を認証する必要がある。
【００４１】
そこで、サービス提供サーバ２００は、情報処理端末１００とネットワーク５０を介して接続して、情報処理端末１００の要求に応じて、ＩＣカードを発行するために必要な認証チケットを作成する機能を有する。ここで、ＩＣカードとは、情報処理端末１００に搭載されるＩＣチップに書き込まれるカード情報を意味し、ＩＣカード発行処理とは、ＩＣチップ１５０へのデータの書き込みや読み込みを意味する。
【００４２】
サービス提供サーバ２００により作成される認証チケットについては後で詳細に説明するが、認証チケットには、主に、ＩＣカードの個別情報や、ＩＣカードへの書き込みデータなどが含まれる。なお、本実施形態においては、１のサービス提供サーバがネットワー

クに接続されているが、かかる例に限定されず、複数のサービス提供サーバがネットワークに接続されていてもよい。この場合、情報処理端末１００は、複数のサービス提供サーバから各々提供されるサービスを利用することができる。

【００４３】

カード発行サーバ３００は、情報処理端末１００とネットワーク５０を介して接続して、サービス提供サーバ２００からの依頼に基づき、情報処理端末１００のＩＣチップ１５０に対してアプリケーションの登録や削除、ＩＣカードのカード情報の書き込みや読み込みなどのカードアクセスを代行する機能を有する。カード発行サーバ３００は、カード発行を代行するカード発行代行者の有するサーバを例示できる。

【００４４】

カード発行サーバ３００は、ＩＣカードへのアクセスを行うために、ＩＣチップ１５０を認証するための鍵情報や、複数のサービス提供サーバ２００毎に異なるアプリケーションの登録や削除のための情報などを保持する。カード発行サーバ３００は、情報処理端末１００の認証をするために、サービス提供サーバ２００により作成された認証チケットを検証する。認証チケットが検証され、情報処理端末１００の正当性が確認された後に、カード発行サーバ３００によるＩＣカードの発行処理が実行される。

【００４５】

このように、カード発行サーバ３００がＩＣカードの発行処理を実行する前に認証チケットを検証することにより、事前にＩＣチップ１５０の個別情報を取得してＩＣチップ１５０の正当性を検証したり、ＩＣチップ１５０に書き込まれたＩＣカードのカード情報等を確認したりすることが可能となる。

【００４６】

また、カード発行サーバ３００は、上記認証チケットの検証と合せて、ワンタイムパスワード等を利用して、ＩＣカードへのアクセス結果や、ＩＣカードの情報等をサービス提供サーバ２００に通知することができる。これにより、カード発行サーバ３００がＩＣカードの発行処理を行っているときや、発行処理後などに、随時、アクセス処理の結果を確認することができ、効率的に不正なアクセスを防止することが可能となる。

【００４７】

以上、カード発行システム１０の概要を説明した。次に、カード発行システム１０の情報処理端末１００、サービス提供サーバ２００、カード発行サーバ３００の詳細な構成を説明する。図２は、情報処理端末１００、サービス提供サーバ２００、カード発行サーバ３００の機能構成を示すブロック図である。図２に示したように、情報処理端末１００は、入出力部１０２、クライアントアプリ１０４、ＩＣチップ制御部１０６、通信制御部１０８、ＩＣチップ１５０などを備える。

【００４８】

クライアントアプリ１０４は、情報処理端末１００内のプログラムであって、情報処理端末１００を使用する利用者にサービスを提供したり、ＩＣカードを発行するための認証要求をしたりする機能を有する。また、通信制御部１０８を介してＩＣチップ１５０の個別情報をサービス提供サーバ２００に送信する機能を有する。ＩＣチップ制御部１０６は、ＩＣチップ１５０とクライアントアプリ１０４や通信制御部１０８との間でのデータの授受を行う機能を有する。ＩＣチップ１５０は、情報処理端末１００に搭載され、外部装置と接触通信または非接触通信する機能を有し、耐タンパ性を有するセキュアメモリである。ＩＣチップ１５０は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｃｅｓｓｉｎｇ　Ｕｎｉｔ）、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）、記憶部などを含んでいてもよい。本実施形態においては、ＩＣチップ１５０は主に記憶部を有し、記憶部に認証情報記憶部１５２を有している場合について説明する。

【００４９】

通信制御部１０８は、インターネット等のネットワークに接続するための通信デバイス等で構成された通信インタフェースであって、ネットワークを介してサービス提供サーバ

２００、もしくはカード発行サーバ３００との間でデータの送受信を行う機能を有する。
【００５０】
入出力部１０２は、情報処理端末１００に備わる入力および出力インタフェースである。入力インタフェースは、例えば、テンキーやボタン、タッチパネル等であり、ユーザの入力を受け付ける機能を有する。出力インタフェースは、例えば、ディスプレイ表示やランプなどの表示装置や、スピーカなどの音声出力装置等である。以上、情報処理端末１００の機能構成について説明した。
【００５１】
次に、サービス提供サーバ２００の機能構成について説明する。サービス提供サーバ２００は、公開鍵登録部２０２、認証チケット作成部２０４、アクセス状況問い合わせ部２０６、通信制御部２０８などを備える。公開鍵登録部２０２は、後述するアクセス認証情報に電子署名を付加するための認証用秘密鍵と対になる認証用公開鍵を、公開鍵証明書を発行する認証局５００に事前に登録する機能を有する。認証用の認証鍵は、上記のように対となる秘密鍵と公開鍵を利用してもよいし、カード発行サーバ３００と共有の共有鍵を利用してもよい。
【００５２】
暗号化には、ＲＳＡ等の非対称鍵や、ＤＥＳまたはＡＳＥ等の対象鍵などのいかなる鍵の場合であっても実施可能である。なお、対称鍵の場合、秘密裏に鍵を相手方に配布する必要があるため、通信網から直接配布するのではなく、内容証明付き郵送等の手段で配布される。本実施形態では、公開かぎ暗号方式を利用して暗号化や電子署名の付加を行う場合について説明する。

【００５３】
認証チケット作成部２０４は、情報処理端末１００によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成する機能を有する。アクセス認証情報は、認証用秘密鍵で暗号化してもよいし、認証用秘密鍵を用いて電子署名を付加したものを認証チケットとしてもよい。
【００５４】
例えば、暗号アルゴリズムとして、鍵付きハッシュ（ＨＭＡＣ）を利用する場合は、アクセス認証情報を入力データとし、サービス提供サーバ２００とカード発行サーバ３００との間で事前に共有している鍵を鍵としてＨＭＡＣ演算を実施した結果をアクセス認証情報の電子署名として付加してもよい。また、ＲＳＡを利用する場合には、アクセス認証情報を入力データとし、それらのハッシュ値をサービス提供サーバの認証用秘密鍵で暗号化したものをアクセス認証情報の電子署名として付加してもよいし、認証用秘密鍵でアクセス認証情報を暗号化してもよい。
【００５５】
図３を参照して、アクセス認証情報と、認証チケットについて説明する。図３は、アクセス認証情報および認証チケットの内容を説明する説明図である。図３に示したように、アクセス認証情報２０４２は、チケット利用条件、ＩＣカード書き込みデータ、ＩＣカード読み取りデータとの比較データなどを含む。チケット利用条件には、利用する処理の情報、クライアントアプリの接続経路、チケットのＩＤ、チケットの有効期間開始日時、チケットの有効期間終了日時、チケットの利用可能回数、ＩＣカード個体情報、ＩＣカード種別情報、ＩＣカードイシュア種別情報、クライアントアプリＩＤ、ＩＣカード対応端末ハードウェアＩＤ、ＩＣカード対応端末所有者ＩＤなどが含まれる。
【００５６】
チケット利用条件は、カード発行サーバ３００が利用可能な処理である。クライアントアプリ接続経路は、クライアントアプリがカード発行サーバ３００に接続する接続経路である。ＩＣカード個体情報は、カード発行サーバ３００がカードアクセスを実行するＩＣカードのＩＣカードを識別する個体情報である。ＩＣカード書き込みデータは、カード発行サーバ３００がＩＣチップ１５０に書き込むデータである。また、比較データは、ＩＣ

チップ１５０から読み込んだＩＣカードのデータと比較するためのデータであって、当該比較データを検証した結果に応じて、実際にＩＣカードに書き込みデータを書き込むか否かを判断することができる。当該比較データの利用については、後で詳細に説明する。アクセス認証情報２０４２は、上記した認証用秘密鍵によって暗号化または、電子署名データが付加されて、認証チケット２０４４が作成される。

【００５７】

図２に戻り、アクセス状況問い合わせ部２０６は、カード発行サーバ３００に対して、ＩＣカードへのアクセス状況を問い合わせる機能を有する。当該アクセス状況は、カード発行サーバ３００がＩＣカードに対して実施した処理の結果である。これにより、クライアントアプリが信頼できない場合や、クライアントアプリとサービス提供サーバ２００との間の通信経路が信頼できない場合などにおいて、クライアントアプリに対する正確な処理結果をサービス提供サーバ２００が把握することが可能となる。

【００５８】

通信制御部２０８は、インターネット等のネットワークに接続するための通信デバイス等で構成された通信インタフェースであって、ネットワークを介して情報処理端末１００またはカード発行サーバ３００との間でデータの送受信を行う機能を有する。通信制御部２０８は、認証情報受信部２１０、認証チケット送信部２１２、アクセス状況受信部２１４などを含む。認証情報受信部２１０は、情報処理端末１００のクライアントアプリ１０４から送信されるアクセス認証情報を受信して、認証チケット作成部２０４に提供する機能を有する。

【００５９】

認証チケット送信部２１２は、認証チケット作成部２０４により作成された認証チケットを、ネットワークを介してカード発行サーバ３００に送信する機能を有する。また、アクセス状況受信部２１４は、カード発行サーバ３００から、ＩＣカードへのアクセス状況を受信してアクセス状況問い合わせ部２０６に提供する機能を有する。以上、サービス提供サーバ２００の機能構成について説明した。

【００６０】

次に、カード発行サーバ３００の機能構成について説明する。カード発行サーバ３００は、通信制御部３０２、公開鍵取得部３０４、認証チケット検証部３０６、検証結果通知部３０８、認証情報検証部３１０、アクセス状況通知部３１８などを備える。通信制御部３０２は、インターネット等のネットワークに接続するための通信デバイス等で構成された通信インタフェースであって、ネットワークを介して情報処理端末１００またはサービス提供サーバ２００との間でデータの送受信を行う機能を有する。

【００６１】

通信制御部３０２は、認証チケット受信部３１２、接続情報送信部３１４、ＩＣカードアクセス部３１６、アクセス認証情報送信部３２０などを含む。認証チケット受信部３１２は、サービス提供サーバ２００により作成された認証チケットを受信して、認証チケット検証部３０６に提供する機能を有する。接続情報送信部３１４は、検証結果通知部３０８による検証結果の通知とともに、接続情報を情報処理端末１００のクライアントアプリ１０４に送信する機能を有する。ＩＣカードアクセス部３１６は、情報処理端末１００のＩＣチップ１５０にアクセスして、ＩＣチップ１５０のＩＣカード情報等の読み込みまたは書き込みを行い、ＩＣカードの情報を認証情報検証部３１０に提供する機能を有する。アクセス認証情報送信部３２０は、サービス提供サーバ２００の要求に応じて、ＩＣチップ１５０へのアクセス状況を通知するとともに、ＩＣチップ１５０に書き込まれたアクセス認証情報をサービス提供サーバ２００に送信する機能を有する。

【００６２】

公開鍵取得部３０４は、サービス提供サーバ２００により認証局５００に登録された認証用の公開鍵を取得して、認証チケット検証部３０６に提供する機能を有する。認証チケット検証部３０６は、認証チケット受信部３１２により提供された認証チケットを、公開鍵取得部３０４より提供された認証用の公開鍵を用いて復号化したり、付加された電子署

名を検証したりして、送信された認証チケットの正当性を検証する。

【００６３】

また、認証チケット検証部３０６は、認証チケットのアクセス認証情報について検証を行う。例えば、認証チケットの有効期間が適切であるか否か、認証チケットの利用可能回数が、実際に認証チケットを利用した回数を超過していないかを検証する。また、チケットのＩＣカード種別情報から、チップ毎に実行可能な処理が適切に選択されているかを検証する。クライアントアプリとカード発行サーバ３００との間でＩＣチップ１５０に記憶されたＩＣカードへの書き込み等が開始されてからエラーが発生した場合、通信断などが発生するためにサービス提供サーバ２００ではエラーの原因を把握することは困難である。上記のとおりチップ毎に実行可能な処理が適切に選択されているか否かを検証することができれば、より早い段階でエラー検知が可能となる。

【００６４】

また、ＩＣチップイシュア毎にアプリケーションの登録や削除、データの書き込みや読み込みなどの処理の制限をしている場合には、認証チケットのＩＣカードイシュア種別情報から、ＩＣチップイシュア毎に実行可能な処理が適切に選択されているかを検証する。上記のＩＣカード種別情報による検証と同様に、ＩＣカードイシュア種別情報を用いて検証することにより、より早い段階でエラー検知が可能となる。認証チケット検証部３０６は、認証チケットの検証結果を、検証結果通知部３０８に提供する。

【００６５】

検証結果通知部３０８は、認証チケット検証部３０６により提供された認証チケットの検証結果をサービス提供サーバ２００に通知する機能を有する。検証結果通知部３０８は、認証チケットの検証結果とともに、情報処理端末１００がカード発行サーバ３００と接続するための接続情報を接続情報送信部３１４に提供する。

【００６６】

認証情報検証部３１０は、認証チケット検証部３０６により検証されたアクセス認証情報と、ＩＣカードアクセス部３１６がＩＣチップ１５０にアクセスすることにより取得したＩＣチップに記憶されたアクセス認証情報とを比較して検証する機能を有する。ここで、図４を参照して認証情報検証部３１０によるＩＣカードの検証について説明する。図４は、認証チケット２０４６およびＩＣチップ１５０に記憶されたアクセス認証情報１５２２の内容を示した説明図である。認証情報検証部３１０は、接続経路の確認、ＩＣカード個別情報の確認、ＩＣカードから読み取ったデータとの比較用データの確認等を行う。

【００６７】

接続経路の確認は、情報処理端末１００が、認証チケットのアクセス認証情報に含まれるカード発行サーバ３００への接続経路に従ってカード発行サーバ３００へ接続されているかを検証する。当該確認は、接続経路だけでなく、接続回線やプロトコル等により確認するようにしてもよい。

【００６８】

ＩＣカードの個別情報の確認は、認証チケットのアクセス認証情報に含まれるＩＣカードカードのＩＣカード個体情報、ＩＣカード種別情報、ＩＣカードイシュア種別情報、クライアントアプリＩＤ、ＩＣカード対応ハードウェアＩＤ、ＩＣカード対応端末所有者ＩＤと、ＩＣカードに記憶されているアクセス認証情報とが一致しているか否かを検証する。当該検証により、特定のＩＣカード対応端末やＩＣカードのみに対する処理を実行することが可能となる。

【００６９】

ＩＣカードから読み取ったデータとの比較用データの確認は、認証チケットのアクセス認証情報に含まれる比較データと、ＩＣカードから実際に取得したデータが一致しているか否かを検証する。ＩＣカード上の特定領域のデータを比較検証することにより、認証チケットが盗難された場合のリプレイ攻撃などを防止することが可能となる。また、ＩＣカードから読み取った値に応じてＩＣカードへの書き込みデータ値を動的に変更することも可能である。比較データの利用例について、図５および図６を参照して詳細に説明する。

図５および図６は、比較データの利用例について説明する説明図である。

【００７０】

図５に示したように、カード発行サーバ３００の認証情報検証部３１０は、認証チケットに記載された利用条件との一致を確認した後に、ＩＣカードへの処理を実行する。例えば、認証チケットの利用条件が、ＩＣカードのデータ領域１が「００００」の時のみ利用可能となっていた場合について説明する。図５に示したように、ＩＣカードのデータ領域が「００００」であった場合には、データの書き込みをすることができる。そして、認証チケットの利用条件に、データ領域１が「００００」場合に、データ領域１を「０００１」とし、データ領域２を「２２２２」に同時に更新するとされていた場合には、ＩＣカードのデータ領域１を「０００１」、データ領域２を「２２２２」に更新する。

【００７１】

また、認証チケットの記載条件に応じてデータを動的に更新する場合も考えられる。例えば、認証チケットの利用条件が、データ領域が「００００」の場合、データ領域１を「０００１」とし、データ領域２を「２２２２」に同時に更新するとされていた場合には、ＩＣカードのデータ領域１が「００００」であった場合には、データ領域１を「０００１」とし、データ領域２を「２２２２」に更新するようにしてもよい。

【００７２】

同様に、認証チケットの利用条件が、データ領域１が「０００１」の場合、データ領域１を「０００２」とし、データ領域２を「３３３３」に同時に更新するとされていた場合には、ＩＣカードのデータ領域１が「０００１」であった場合には、データ領域１を「０００２」とし、データ領域２を「３３３３」に更新するようにしてもよい。また、認証チケットの利用条件が、データ領域が「０００２」の場合、データ領域１を「０００２」とし、データ領域３を「ＢＢＢＢ」に同時に更新するとされていた場合には、ＩＣカードのデータ領域１が「０００２」であった場合には、データ領域１を「０００２」とし、データ領域３を「ＢＢＢＢ」に更新するようにしてもよい。図６は、複数の認証チケットの利用条件があった場合のデータ領域の更新について説明する説明図である。図６に示したように、ＩＣカードのデータ領域１が「０００１」であるため、「データ領域１が「０００１」の場合」のチケット利用条件に基づいて、データが更新される。具体的には、チケット利用条件のデータ領域１が「０００１」の場合には、データ領域１を「０００２」とし、データ領域２を「３３３３」に同時に更新するとあるため、図６に示したように、データ領域１を「０００２」とし、データ領域２を「３３３３」に同時に更新する。以上、比較データの利用例について説明した。

【００７３】

図２に戻り、アクセス状況通知部３１８は、サービス提供サーバ２００の要求に応じて、ＩＣチップ１５０へのアクセス状況を通知する機能を有する。例えば、ＩＣカードにアクセスする前にサービス提供サーバ２００よりアクセス状況の問い合わせがあった場合には、ＩＣカードとの間で通信が開始されたか否かを通知することができる。また、ＩＣカードにアクセス後、ＩＣカードへの処理実行中にサービス提供サーバ２００よりアクセス状況の問い合わせがあった場合には、ＩＣカードとの間での処理状況を通知することができる。さらに、ＩＣカードへの処理が終了した場合には、ＩＣカードとの間で実施された処理の処理結果を通知することができる。これにより、クライアントアプリが信頼できない場合や、クライアントアプリとサービス提供サーバ２００との間の通信経路が信頼できない場合などにおいて、クライアントアプリに対する正確な処理結果をサービス提供サーバ２００が把握することが可能となる。

【００７４】

アクセス認証情報送信部３２０は、サービス提供サーバの要求に応じて、ＩＣチップに記憶されたアクセス認証情報をサービス提供サーバ２００に送信する機能を有する。これによりサービス提供サーバ２００は、アクセス状況を問い合わせると同時に、ＩＣカードから読み込んだデータを取得して、効率的なシーケンスを実現することが可能となる。以上、カード発行サーバ３００の機能構成について説明した。

【００７５】
次に、カード発行システム１０において実行されるカード発行方法について説明する。図７は、カード発行システム１０において実行されるカード発行方法の流れを示したタイミングチャートである。図７に示したように、まず、クライアントアプリ１０４が、サービス提供サーバ２００にアクセス認証情報を送信する（Ｓ１０２）。ステップＳ１０２において送信されるアクセス認証情報は、ＩＣカードのＩＣカード個別情報のみであってもよく、サービス提供サーバ２００が認証チケットを作成するためのアクセス認証情報の一部であってもよい。
【００７６】
ステップＳ１０２においてクライアントアプリ１０４からアクセス認証情報を送信されたサービス提供サーバ２００は、アクセス認証情報を暗号化したり、電子署名を付加したりすることにより認証チケットを作成する（Ｓ１０４）。ステップＳ１０４において作成した認証チケットを、カード発行サーバ３００に送信する（Ｓ１０６）。
【００７７】
ステップＳ１０６においてサービス提供サーバ２００より認証チケット送信されたカード発行サーバ３００は、認証チケットを検証する（Ｓ１０８）。ステップＳ１０８における認証チケットの検証においては、上記したように、認証チケットが正しく復号できるか、正しい電子署名が付加されているか、アクセス認証情報に含まれる利用条件の確認等を行う。ステップＳ１０８における認証チケットの検証については、後で詳細に説明する。
【００７８】
ステップＳ１０８において検証された認証チケットの検証結果が、サービス提供サーバ２００に送信される（Ｓ１１０）。また、クライアントアプリ１０４がカード発行サーバ３００と接続するための接続情報がサービス提供サーバ２００に送信される（Ｓ１１２）。ステップＳ１１２において、カード発行サーバ３００から接続情報を送信されたサービス提供サーバ２００は、当該接続情報をクライアントアプリ１０４に送信する（Ｓ１１４）。
【００７９】
ステップＳ１１４においてサービス提供サーバ２００から、カード発行サーバ３００への接続情報を送信されたクライアントアプリ１０４は、当該接続情報に基づいて、カード発行サーバ３００に接続する（Ｓ１１６）。ステップＳ１１６においてクライアントアプリ１０４に接続されたカード発行サーバ３００は、クライアントアプリ１０４からの接続状況と、クライアントアプリ１０４の個別情報とから、クライアントアプリ１０４の正当性を確認したうえで、ＩＣチップ１５０にアクセスする（Ｓ１１８）。
【００８０】
そして、ステップＳ１１８においてＩＣチップ１５０にアクセスして取得したＩＣチップ１５０のＩＣカードの個別情報と、認証チケットのアクセス認証情報とを比較して検証する（Ｓ１２０）。ステップＳ１２０における認証情報の検証については、後で詳細に説明する。ステップＳ１２０における検証の結果、ＩＣカードの正当性が確認された場合に、ＩＣチップ１５０へＩＣカードのカード情報の書き込みをしたり、カード情報の更新を行ったりする（Ｓ１２２）。以上、カード発行システム１０において実行されるカード発行方法について説明した。
【００８１】
次に、図８に基づいて認証チケットの検証について詳細に説明する。図８は、認証チケットの検証処理を説明する説明図である。図８に示したように、まず、認証チケットのフォーマットが適正であるかチェックする（Ｓ２０２）。次に、カード発行サーバ３００において利用可能な処理が指定されているか否かをチェックする（Ｓ２０４）。そして、カード発行サーバ３００で利用可能な接続経路が指定されているか否かをチェックする（Ｓ２０６）。
【００８２】
過去に利用されたものと同一の認証チケットＩＤが指定されていないか、利用可能回数

が指定されている場合には、認証チケットの利用可能回数の範囲内かをチェックする（Ｓ２０８）。また、認証チケットの利用可能期間が指定されているかをチェックし、指定されている場合には、利用可能期間内か否かをチェックする（Ｓ２１０）。ＩＣカード種別情報で実行可能な処理が、利用する処理の情報として適切に選択されているかをチェックする（Ｓ２１２）。ＩＣカードイシュア種別情報で実行可能な処理が、利用する処理の情報として適切に選択されているかをチェックする（Ｓ２１４）。正しい電子署名が付加されているか、または認証チケットが暗号化されている場合には正しく復号できるかをチェックする（Ｓ２１６）。上記認証チケットの検証処理は、すべての処理を同時に行ってもよく、処理の順番は問わない。以上、認証チケットの検証処理について説明した。

【００８３】

次に、図９に基づいて、ＩＣカードの認証情報の検証について説明する。図９は、ＩＣカードの認証情報の検証処理を説明する説明図である。図９に示したように、まず、接続経路が指定されたものと同一であるかをチェックする（Ｓ２２０）。ステップＳ２２０においては、接続経路のチェックだけでなく、接続回線や、プロトコル、チップの接続Ｉ／Ｆ、チップのかぎの状態などをチェックしてもよい。次に、ＩＣカード個体情報が認証チケットのＩＣカード個体情報と同一かチェックする（Ｓ２２２）。

【００８４】

そして、ＩＣカード種別情報が認証チケットのＩＣカード種別情報と同一かチェックする（Ｓ２２４）。また、ＩＣカードイシュア情報が認証チケットのＩＣカードイシュア情報と同一かチェックする（Ｓ２２６）。さらに、クライアントアプリＩＤが認証チケットのクライアントアプリＩＤと同一かチェックする（Ｓ２２８）。ＩＣカード対応端末ハードウェアＩＤが認証チケットのＩＣカード対応端末ハードウェアＩＤと同一かチェックする（Ｓ２３０）。ＩＣカード対応端末所有者ＩＤが認証チケットのＩＣカード対応端末所有者ＩＤと同一かチェックする（Ｓ２３２）。そして、ＩＣカード読み取りデータが認証チケットで指定された読み取りデータと同一であるかチェックする（Ｓ２３４）。上記ＩＣカードの認証情報の検証処理は、すべての処理を同時に行ってもよく、処理の順番は問わない。以上ＩＣカードの認証情報の検証処理について説明した。

【００８５】

次に、図１０に基づいて、カード発行システム１０におけるアクセス情報問い合わせ処理について説明する。図１０は、アクセス情報問い合わせ処理を示したタイミングチャートである。図１０に示したように、サービス提供サーバ２００がカード発行サーバ３００にＩＣカードへのアクセス状況を問い合わせる（Ｓ１３０）。ステップＳ１３０においてサービス提供サーバ２００からアクセス状況を問い合わせられたカード発行サーバ３００は、サービス提供サーバ２００へのＩＣカードへのアクセス状況を通知する（Ｓ１３２）。ステップＳ１３２においては、カード発行サーバ３００は、クライアントアプリ１０４からの接続もされていないため、情報処理端末１００と未接続の旨の通知をする。

【００８６】

そして、クライアントアプリ１０４からカード発行サーバ３００への接続が行われる（Ｓ１３４）。ステップＳ１３４における接続の後に、サービス提供サーバ２００からアクセス状況の問い合わせがあり（Ｓ１３６）、カード発行サーバ３００がアクセス状況を通知する（Ｓ１３７）。ステップＳ１３７においては、カード発行サーバ３００は、クライアントアプリ１０４からの接続があった旨の通知をする。

【００８７】

そして、カード発行サーバ３００からＩＣチップへのアクセスが行われる（Ｓ１４０）。ステップＳ１４０のアクセスの後に、サービス提供サーバ２００からアクセス状況の問い合わせがあり（Ｓ１４２）、カード発行サーバ３００がアクセス状況を通知する（Ｓ１４４）。ステップＳ１４４においては、カード発行サーバ３００は、ＩＣチップへのアクセス結果や、どこまで処理が実施されたか、処理の実行結果などのアクセス状況を通知する。当該アクセス状況の問い合わせは、ＩＣチップへのアクセス中も実行可能である。

【００８８】

なお、サービス提供サーバ２００は、ワンタイムのＩＤなどを利用して、カード発行サーバに対してクライアントアプリ１０４の処理状況を確認するようにしてもよい。これにより、クライアントアプリ１０４がカード発行サーバ３００に接続されたか、クライアントアプリ１０４がカード発行サーバ３００に接続されたがエラーとなったか、クライアントアプリ１０４がカード発行サーバ３００に接続され正常に処理が完了したかなどの処理状況を把握することが可能となる。以上、カード発行システム１０におけるアクセス情報問い合わせ処理について説明した。

【００８９】

以上、第１実施形態にかかるカード発行システム１０について説明した。カード発行システム１０によれば、サービス提供サーバ２００が情報処理端末によるアクセスを認証するためのアクセス認証情報を暗号化して認証チケットを作成して、当該認証チケットがカード発行サーバ３００に送信される。カード発行サーバ３００は、認証チケットを検証して、検証結果をサービス提供サーバに通知したり、カード発行サーバ３００に接続するための接続情報を送信したりする。そして、サービス提供サーバ２００経由で接続情報を送信された情報処理端末１００がカード発行サーバ３００に接続して、カード発行サーバ３００が情報処理端末１００のＩＣチップ１５０にアクセスすることができる。

【００９０】

サービス提供サーバ２００から送信される認証チケットには、ＩＣカードの個別情報等がふくまれているため、ＩＣカードにアクセスする前に、事前にＩＣチップの検証をして、ＩＣカードが対応していない処理などを早期に検知することが可能となり、効率的に不正なアクセスを防止することができる。

【００９１】

（第２実施形態）

次に、本発明の第２の実施形態にかかるカード発行システムの概要について説明する。本実施形態にかかるカード発行システム１０′は、情報処理端末１００′、サービス提供サーバ２００′、カード発行サーバ３００′を備える。カード発行システム１０′の構成は第１実施形態にかかるカード発行システム１０の構成とほぼ同様であるため、詳細な説明は省略する。本実施形態においては、情報処理端末１００′が信頼できるクライアントである場合である点が第１実施形態と異なる点である。情報処理端末１００′が信頼できるクライアントである場合とは、簡易にパケット解析が可能なアプリケーションなどを搭載可能な端末ではなく、携帯端末のような組込み端末である場合や、情報処理端末１００′において認証チケットの内容を参照されても問題ない場合などが挙げられる。

【００９２】

この場合には、サービス提供サーバ２００′により作成された認証チケットを情報処理端末１００′のクライアントアプリに送信し、クライアントアプリがカード発行サーバ３００′と接続して認証チケットを送信することによりＩＣカードの認証処理を実行することが可能となる。これにより、サービス提供サーバ２００′とカード発行サーバ３００との通信を削減し、サービス提供サーバ２００の構築工数も削減することが可能となる。なお、本実施形態においては、サービス提供サーバ２００′において認証チケットを作成しているが、かかる例に限定されない。例えば、情報処理端末１００′がサービス提供サーバ２００′と同様の機能を有するようにしてもよい。具体的には、情報処理端末１００′が認証チケットを作成するための秘密鍵を保持し、認証チケットを作成するようにしてもよい。以上、本実施形態にかかるカード発行システム１０′の概要を説明した。

【００９３】

次に、図１１に基づいて、カード発行システム１０′の情報処理端末１００′、サービス提供サーバ２００′、カード発行サーバ３００′の機能構成について説明する。図１１は、情報処理端末１００′、サービス提供サーバ２００′、カード発行サーバ３００′の機能構成を示すブロック図である。情報処理端末１００′は、第１実施形態の情報処理端末１００とほぼ同様の機能を有するため、詳細な説明は省略する。上記の通り、情報処理端末１００′は、信頼できるクライアントである。また、第１実施形態の情報処理端末と

特に異なる点は、サービス提供サーバ２００′により作成された認証チケットを認証チケット受信部１１０が受信して、認証チケット送信部１１２が当該認証チケットをカード発行サーバ３００′に送信する点である。

【００９４】

サービス提供サーバ２００′についても、第１実施形態のサービス提供サーバ２００とほぼ同様の機能を有するため、詳細な説明は省略する。第１実施形態のサービス提供サーバ２００′と特に異なる点は、認証チケット作成部２０４により作成された認証チケットを提供された認証チケット送信部２１２′が、認証チケットをカード発行サーバ３００′ではなく、情報処理端末１００′のクライアントアプリ１０４に送信する点である。クライアントアプリ１０４に送信された認証チケットは、クライアントアプリ１０４からカード発行サーバ３００′に送信される。これにより、サービス提供サーバ２００′とカード発行サーバ３００′との間の通信を削減し、サービス提供サーバ２００′の構築工数を削減することが可能となる。

【００９５】

カード発行サーバ３００′についても、第１実施形態のカード発行サーバ３００とほぼ同様の機能を有するため、詳細な説明は省略する。第１実施形態のカード発行サーバ３００と特に異なる点は、情報処理端末１００′から送信された認証チケットを認証チケット受信部３１２′が受信して認証チケット検証部３０６に提供する点である。また、検証結果通知部３０８の検証結果および当該検証結果と同時に送信される接続情報は、接続情報送信部３１４′により情報処理端末１００′のクライアントアプリ１０４に送信される。第１実施形態では、検証結果および接続情報は、サービス提供サーバ２００を経由してクライアントアプリ１０４に送信されたが、本実施形態では、直接クライアントアプリ１０４に送信することができる。これにより、サービス提供サーバ２００′とカード発行サーバ３００′との間の通信を削減することが可能となる。以上、カード発行システム１０′にかかる各装置の機能構成について説明した。

【００９６】

次に、カード発行システム１０′において実行されるカード発行方法について説明する。本実施形態にかかるカード発行方法について、第１実施形態と同様の処理については、詳細な説明は省略する。図１２は、カード発行システム１０′において実行されるカード発行方法の流れを示したタイミングチャートである。図１２に示したように、まず、クライアントアプリ１０４が、サービス提供サーバ２００′にアクセス認証情報を送信する（Ｓ３０２）。ステップＳ３０２においてクライアントアプリ１０４からアクセス認証情報を送信されたサービス提供サーバ２００′は、アクセス認証情報を暗号化したり、電子署名を付加したりすることにより認証チケットを作成する（Ｓ３０４）。ステップＳ３０４において作成した認証チケットを、クライアントアプリ１０４に送信する（Ｓ３０６）。

【００９７】

ステップＳ３０６においてサービス提供サーバ２００′より認証チケット送信されたクライアントアプリ１０４は、認証チケットをカード発行サーバ３００′に送信する（Ｓ３０８）。ステップＳ３０８において、クライアントアプリ１０４から認証チケットを送信されたカード発行サーバ３００′は、認証チケットを検証する（Ｓ３１０）。ステップＳ３１０における認証チケットの検証においては、上記したように、認証チケットが正しく復号できるか、正しい電子署名が付加されているか、アクセス認証情報に含まれる利用条件の確認等を行う。

【００９８】

ステップＳ３１０において検証された認証チケットの検証結果が、クライアントアプリ１０４に送信される（Ｓ３１２）。また、クライアントアプリ１０４がカード発行サーバ３００と接続するための接続情報がクライアントアプリ１０４に送信される（Ｓ３１４）

。ステップＳ３１４においてカード発行サーバ３００′から、カード発行サーバ３００′への接続情報を送信されたクライアントアプリ１０４は、当該接続情報に基づいて、カード発行サーバ３００′に接続する（Ｓ３１６）。ステップＳ３１６においてクライアントアプリ１０４に接続されたカード発行サーバ３００′は、クライアントアプリ１０４からの接続状況と、クライアントアプリ１０４の個別情報とから、クライアントアプリ１０４の正当性を確認したうえで、ＩＣチップ１５０にアクセスする（Ｓ３１８）。

【００９９】

そして、ステップＳ３１８においてＩＣチップ１５０にアクセスして取得したＩＣチップ１５０のＩＣカードの個別情報と、認証チケットのアクセス認証情報とを比較して検証する（Ｓ３２０）。ステップＳ３２０における検証の結果、ＩＣカードの正当性が確認された場合に、ＩＣチップ１５０へＩＣカードのカード情報の書き込みをしたり、カード情報の更新を行ったりする（Ｓ３２２）。以上、カード発行システム１０′において実行されるカード発行方法について説明した。

【０１００】

以上、第２実施形態にかかるカード発行システム１０′について説明した。カード発行システム１０′よれば、サービス提供サーバ２００′により作成された認証チケットを情報処理端末１００′のクライアントアプリ１０４に送信し、クライアントアプリ１０４がカード発行サーバ３００′と接続して認証チケットを送信することによりＩＣカードの認証処理を実行することが可能となる。これにより、サービス提供サーバ２００′とカード発行サーバ３００′との通信を削減し、サービス提供サーバ２００′の構築工数も削減することが可能となる。

【０１０１】

（第３実施形態）

次に、本発明の第３の実施形態にかかるカード発行システムの概要について説明する。図１３は、本実施形態にかかるカード発行システム２０の構成例を示した説明図である。図１３に示したように、カード発行システム２０は、情報処理端末１０１、サービス提供サーバ２０１、カード発行サーバ３０１、サービス代行サーバ４００を備える。カード発行システム２０は、情報処理端末１０１、サービス提供サーバ２０１、カード発行サーバ３０１、サービス代行サーバ４００とは、ネットワーク５０を介して接続されている。本実施形態は、第１実施形態および第２実施形態とはサービス代行サーバ４００が備わっている点で大きく異なる。

【０１０２】

サービス代行サーバ４００は、サービス提供サーバ２０１からの依頼に基づいて、カード発行サーバ３０１と情報処理端末１０１との処理を代行する機能を有する。この場合、第１実施形態または第２実施形態のように、認証チケットが１層構成であると、サービス提供サーバ２０１が実行するすべての処理をサービス代行サーバ４００に許可しなければならないという問題があった。そこで、サービス提供サーバ２０１がサービス代行サーバ４００に依頼する処理のみを実行可能な認証ライセンスを作成して、当該ライセンスに基づいて認証チケットを作成することとする。このように、認証チケットを多段構成とすることにより、サービス提供サーバ２０１がサービス代行サーバ４００に代行処理を依頼するに際し、セキュリティを維持して実行可能な処理を限定できることとなる。

【０１０３】

本実施形態において、認証チケットを多段構成とするためには、認証ライセンスと認証チケットの各々を暗号化したり電子署名を付加したりする必要がある。例えば、ＲＳＡ等の非対象鍵による電子署名検証を利用する場合には、ライセンスを作成するサービス提供サーバ２０１が認証用鍵ペア１（Ｐｋ１／Ｓｋ１）を用意し、認証チケットを作成するサービス代行サーバ４００が認証用鍵ペア２（Ｐｋ２／Ｓｋ２）を用意する。カード発行サーバ３０１には、認証用公開鍵（Ｐｋ１）を事前に登録したり、認証局を設置している場合には、カード発行サーバ３０１が認証用公開鍵１（Ｐｋ１）を認証局から取得したりしておく必要がある。

【０１０４】
上記の認証用鍵を用いた多段構成による認証の概要は以下のとおりである。サービス提供サーバ２０１は、サービス代行サーバ４００の認証用秘密鍵２（Ｓｋ２）と対となる、認証用公開鍵２（Ｐｋ２）を含む認証情報を作成して、認証用秘密鍵１（Ｓｋ１）を用いて電子署名を付加した認証ライセンスを作成する。認証ライセンスの詳細については後で詳細に説明する。サービス代行サーバ４００は、サービス提供サーバ２０１から送信された認証ライセンスにＩＣカードの個別情報を付加して認証用秘密鍵２（Ｓｋ２）を用いて電子署名を付加した認証チケットを作成する。
【０１０５】
サービス代行サーバ４００により作成された認証チケットを受信したカード発行サーバ３０１は、事前に取得した認証用公開鍵１（Ｐｋ１）を利用してチケットに含まれる電子署名を検証し、ライセンスに含まれる認証用公開鍵２（Ｐｋ２）の正当性を確認する。認証用公開鍵２（Ｐｋ２）の正当性が確認された後、認証用公開鍵２（Ｐｋ２）を利用して、認証チケットの電子署名検証を行って、認証チケットの正当性を検証する。
【０１０６】
このように、認証ライセンスおよび認証チケットの各々に異なる認証鍵を利用する多段構成とすることにより、サービス提供サーバ２０１がサービス代行サーバ４００等に処理を代行する場合においても、相互に認証を可能とし、代行させる処理を制限することが可能となる。本実施形態においては、認証チケットが多段構成となっている点以外の認証チケットの検証およびＩＣカードの検証については、第１実施形態および第２実施形態と同様の構成となっているため、詳細な説明は省略する。以上、カード発行システム２０の概要を説明した。
【０１０７】
次に、カード発行システム２０の情報処理端末１０１、サービス提供サーバ２０１、カード発行サーバ３０１、サービス代行サーバ４００の詳細な構成を説明する。図１４は、情報処理端末１０１、サービス提供サーバ２０１、カード発行サーバ３０１、サービス代行サーバ４００の機能構成を示すブロック図である。情報処理端末１０１は、第１実施形態にかかる情報処理端末１００とほぼ同様の機能を有するため、詳細な説明は省略する。第１実施形態の情報処理端末１００と異なる点は、ＩＣチップ１５０の個別情報をサービス代行サーバ４００に送信する点である。
【０１０８】
サービス提供サーバ２０１は、公開鍵登録部２０２、公開鍵取得部２０３、通信制御部２０９、認証ライセンス作成部２２０などを備える。公開鍵登録部２０２は、上記した認証用鍵ペア１の認証用公開鍵１（Ｐｋ１）を認証局５００に事前に登録する機能を有する。公開鍵取得部２０３は、サービス代行サーバ４００により認証局５００に登録された認証用の公開鍵を取得して、認証ライセンス作成部２２０に提供する機能を有する。認証ライセンス作成部２２０は、例えば上記した認証用公開鍵（Ｐｋ２）を取得する。認証ライセンス作成部２２０は、サービス代行サーバ４００に許諾するサービスの情報を暗号化して認証ライセンスを作成する機能を有する。ここで、図１５に基づいて、サービス代行サーバ４００に許諾するサービスの情報（以下、ライセンス情報と称する。）および認証ライセンスについて説明する。図１５は、ライセンス情報２２０２および認証ライセンス２２０４の内容を説明する説明図である。図１５に示したように、ライセンス情報２２０２は、ライセンスの利用条件を含む、ライセンスの利用条件には、利用可能な処理のリスト、利用可能な接続経路のリスト、ライセンスのＩＤ、ライセンスの有効期間開始日時、ライセンスの有効期間終了日時、ライセンスの利用可能回数、ライセンス利用定義、認証用公開鍵２（Ｐｋ２）などが含まれる。
【０１０９】
ライセンス利用定義には、カード発行サーバ３０１においてアクセスするＩＣカードのＩＣカード個体情報、クライアントアプリＩＤ、ＩＣカード対応端末ハードウェアＩＤ、ＩＣカード対応端末所有者ＩＤやカード発行サーバ３０１から送信されるチャレンジ（ワ

ンタイムのＩＤやパスワード情報など）などをチケット情報に含める必要があるかなどの条件を定義することができる。認証用公開鍵２（Ｐｋ２）を含むライセンス情報２２０２は、認証用秘密鍵１（Ｓｋ１）を用いて電子署名が付加されて認証ライセンス２２０４が作成される。図１４に戻り、認証ライセンス作成部２２０は、作成した認証ライセンスを認証ライセンス送信部２２２に提供する。

【０１１０】

通信制御部２０９は、インターネット等のネットワークに接続するための通信デバイス等で構成された通信インタフェースであって、ネットワークを介してサービス代行サーバ４００との間でデータの送受信を行う機能を有する。通信制御部２０９は、認証ライセンス送信部２２２などを備える。認証ライセンス作成部２２０より認証ライセンスを提供された認証ライセンス送信部２２２は、当該認証ライセンスをサービス代行サーバ４００に送信する。なお、本実施形態においては、認証ライセンスをネットワークを介してサービス代行サーバ４００に送信しているが、かかる例に限定されず、認証ライセンスをオフラインでサービス代行サーバ４００に送信するようにしてもよい。

【０１１１】

サービス代行サーバ４００は、認証チケット作成部４０２および通信制御部４０４、公開鍵登録部４１０などを備える。認証チケット作成部４０２は、認証ライセンス受信部４０６により受信された認証ライセンスの利用条件に応じてアクセス認証情報を作成し、当該アクセス認証情報を暗号化したり、認証用秘密鍵２（Ｓｋ２）を用いて電子署名を付加したりして認証チケットを作成する機能を有する。ここで、図１６に基づいて、アクセス認証情報４０２２および認証チケット４０２４について説明する。図１６は、アクセス認証情報４０２２および認証チケット４０２４の内容を説明する説明図である。

【０１１２】

図１６に示したように、アクセス認証情報４０２２は、第１実施形態にかかるアクセス認証情報にライセンスが付加されている点以外はほぼ同様であるため、詳細な説明は省略する。なお、アクセス認証情報４０２２に、カード発行サーバから送信されるチャレンジ（ワンタイムのＩＤやパスワード情報）などを含めるようにしてもよい。アクセス認証情報４０２２は、上記した認証用秘密鍵２（Ｓｋ２）によって電子署名データが付加されて認証チケット４０２４が作成される。ここで、ライセンスを電子署名データの対象としなくてもよい。図１４に戻り、認証チケット作成部４０２により作成された認証チケットは、認証チケット送信部４０８に提供される。

【０１１３】

通信制御部４０４は、インターネット等のネットワークに接続するための通信デバイス等で構成された通信インタフェースであって、ネットワークを介して情報処理端末１０１、サービス提供サーバ２０１、カード発行サーバ３０１との間でデータの送受信を行う機能を有する。また、通信制御部４０４は、認証ライセンス受信部４０６、認証チケット送信部４０８などを備える。認証ライセンス受信部４０６は、サービス提供サーバ２０１により作成された認証ライセンスを受信する機能を有する。認証チケット送信部４０８は、認証チケット作成部４０２に提供された認証チケットをカード発行サーバ３０１に送信する機能を有する。公開鍵登録部４１０は、認証用秘密鍵（Ｓｋ２）と対となる認証用公開鍵２（Ｐｋ２）を認証局５００に事前に登録する機能を有する。

【０１１４】

カード発行サーバ３０１は、通信制御部３０３、公開鍵取得部３０４、認証ライセンス検証部３２４、認証チケット検証部３０７、検証結果通知部３０８、認証情報検証部３１０などを備える。通信制御部３０３は、インターネット等のネットワークに接続するための通信デバイス等で構成された通信インタフェースであって、ネットワークを介して情報処理端末１０１またはサービス代行提供サーバ４００との間でデータの送受信を行う機能を有する。

【０１１５】

通信制御部３０３は、認証チケット受信部３１３、接続情報送信部３１５、ＩＣカード

アクセス部３１６などを含む。認証チケット受信部３１３は、サービス代行サーバ４００により作成された認証チケットを受信して、認証ライセンス検証部３２４に提供する機能を有する。接続情報送信部３１５は、検証結果通知部３０８による検証結果の通知とともに、接続情報を情報処理端末１００のクライアントアプリ１０４に送信する機能を有する。ＩＣカードアクセス部３１６は、情報処理端末１０１のＩＣチップ１５０にアクセスして、ＩＣチップ１５０のＩＣカード情報等の読み込みまたは書き込みを行い、ＩＣカードの情報を認証情報検証部３１０に提供する機能を有する。

【０１１６】

公開鍵取得部３０４は、サービス提供サーバ２０１により認証局５００に登録された認証用の公開鍵を取得して、認証チケット検証部３０７に提供する機能を有する。本実施形態においては、公開鍵取得部３０４は、上記の認証用公開鍵１（Ｐｋ１）を認証局から取得する。

【０１１７】

認証ライセンス検証部３２４は、受信した認証ライセンスを復号化して認証ライセンスを検証する機能を有する。認証ライセンスに電子署名が付加されている場合には、当該電子署名を認証用公開鍵（Ｐｋ１）を用いて検証して、認証ライセンスに含まれる認証用公開鍵（Ｐｋ２）の正当性を確認する。認証チケット検証部３０７は、認証ライセンス検証部３２４により、正当性を確認された認証用公開鍵（Ｐｋ２）を利用して認証チケットの電子署名検証を行って、チケットの正当性を検証する機能を有する。また、第１実施形態の認証チケット検証部３０６と同様に、認証チケットのアクセス認証情報について検証を行う。認証ライセンス検証部３２４は、認証チケットの検証結果を、検証結果通知部３０８に提供する。

【０１１８】

検証結果通知部３０８は、認証チケット検証部３０７により提供された認証チケットの検証結果をサービス代行サーバ４００に通知する機能を有する。検証結果通知部３０８は、認証チケットの検証結果とともに、情報処理端末１０１がカード発行サーバ３０１と接続するための接続情報を接続情報送信部３１５に提供する。認証情報検証部３１０は、第１実施形態にかかるカード発行サーバ３００の認証情報検証部３１０とほぼ同様の機能を有するため詳細な説明は省略する。

【０１１９】

以上、カード発行システム２０の各装置の機能構成について説明した。次に、カード発行システム２０において実行されるカード発行方法について説明する。図１７は、カード発行システム２０において実行されるカード発行方法の流れを示したタイミングチャートである。図１７に示したように、まず、サービス提供サーバ２０１が、サービス代行サーバ４００に許諾するサービスの情報を含むライセンス情報を暗号化して、認証ライセンスを作成する（Ｓ４０２）。サービス提供サーバ２０１は、ステップＳ４０２において作成された認証ライセンスをサービス代行サーバ４００に送信する（Ｓ４０４）。

【０１２０】

そして、クライアントアプリ１０４は、アクセス認証情報をサービス代行サーバ４００に送信する（Ｓ４０６）。ステップＳ４０６におけるクライアントアプリ１０４によるアクセス認証情報の送信は、サービス提供サーバ２０１から認証ライセンスが送信された後に送信されてもよいし、予め送信されていてもよい。ステップＳ４０４においてサービス提供サーバ２０１から認証ライセンスを送信され、ステップＳ４０６においてクライアントアプリ１０４からアクセス認証情報を送信されたサービス代行サーバは、認証ライセンスおよびアクセス認証情報に基づいて、認証チケットを作成する（Ｓ４０８）。サービス代行サーバ４００は、ステップＳ４０８において作成した認証チケットをカード発行サーバ３０１に送信する（Ｓ４１０）。

【０１２１】

ステップＳ４１０においてサービス代行サーバ４００から認証チケットを送信されたカ

ード発行サーバ３０１は、認証チケットに含まれる認証ライセンスを復号化して認証ライセンスを検証する（Ｓ４１４）。上記したように、認証チケットおよび認証ライセンスに電子署名データが付加されている場合には、認証用公開鍵１（Ｐｋ１）を利用して認証チケットに含まれる電子署名を検証し認証ライセンスに含まれる認証用公開鍵２（Ｐｋ２）の正当性を確認するようにしてもよい。ステップＳ４１４において認証ライセンスの検証を行ったのち、認証チケットの検証を行う（Ｓ４１６）。上記したように、認証チケットに電子署名データが付与されている場合には、認証ライセンスに含まれる認証用公開鍵２（Ｐｋ２）を利用して認証チケットの電子署名検証を行って、認証チケットの検証を行う。

【０１２２】

ステップＳ４１６において検証された認証チケットの検証結果が、サービス代行サーバ４００に送信される（Ｓ４１８）。また、クライアントアプリ１０４がカード発行サーバ３０１と接続するための接続情報がサービス代行サーバ４００に送信される（Ｓ４２０）。ステップＳ４２０において、カード発行サーバ３０１から接続情報を送信されたサービス代行サーバ４００は、当該接続情報をクライアントアプリ１０４に送信する（Ｓ４２２）。

【０１２３】

ステップＳ４２２においてサービス代行サーバ４００から、カード発行サーバ３０１への接続情報を送信されたクライアントアプリ１０４は、当該接続情報に基づいて、カード発行サーバ３０１に接続する（Ｓ４２４）。ステップＳ４２４においてクライアントアプリ１０４に接続されたカード発行サーバ３０１は、クライアントアプリ１０４からの接続状況と、クライアントアプリ１０４の個別情報とから、クライアントアプリ１０４の正当性を確認したうえで、ＩＣチップ１５０にアクセスする（Ｓ４２６）。

【０１２４】

そして、ステップＳ４２６においてＩＣチップ１５０にアクセスして取得したＩＣチップ１５０のＩＣカードの個別情報と、認証チケットのアクセス認証情報とを比較して検証する（Ｓ４２８）。ステップＳ４２８における検証の結果、ＩＣカードの正当性が確認された場合に、ＩＣチップ１５０へＩＣカードのカード情報の書き込みをしたり、カード情報の更新を行ったりする（Ｓ４３０）。以上、カード発行システム２０において実行されるカード発行方法について説明した。

【０１２５】

以上、第３実施形態にかかるカード発行システム２０について説明した。カード発行システム２０によれば、サービス提供サーバ２０１がサービス代行サーバ４００に依頼する処理のみを実行可能な認証ライセンスを作成して、当該認証ライセンスに基づいて認証チケットを作成する。このように、認証チケットを多段構成とすることにより、サービス提供サーバ２０１がサービス代行サーバ４００に代行処理を依頼するに際し、セキュリティを維持して実行可能な処理を限定できることとなる。また、認証ライセンスおよび認証チケットの各々に異なる認証鍵を利用する多段構成とすることにより、サービス提供サーバ２０１がサービス代行サーバ４００等に処理を代行する場合においても、相互に認証をすることが可能となる。

【０１２６】

以上、添付図面を参照しながら本発明の好適な実施形態について詳細に説明したが、本発明はかかる例に限定されない。本発明の属する技術の分野における通常の知識を有する者であれば、特許請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本発明の技術的範囲に属するものと了解される。

【０１２７】

例えば、上記実施形態では、カード発行サーバは、認証チケットを利用して情報処理端末の認証をすることとしたが、本発明はかかる例に限定されない。例えば、サービス提供サーバとの認証においては、チャレンジレスポンスを利用した認証方式により認証をする

ようにしてもよい。このように、カード発行サーバは、認証チケットを利用した認証と、チャレンジレスポンスを利用した認証とを組み合わせて認証するようにしてもよい。どのような認証方式を利用するかは、サービス提供サーバの選択に基づき決定するようにしてもよい。

【図面の簡単な説明】

【０１２８】

【図１】本発明の第１の実施形態にかかるカード発行システムの構成例を示した説明図である。

【図２】同実施形態にかかる情報処理端末、サービス提供サーバ、カード発行サーバの機能構成を示すブロック図である。

【図３】同実施形態にかかるアクセス認証情報および認証チケットの内容を説明する説明図である。

【図４】同実施形態にかかる認証チケットおよびＩＣチップに記憶されたアクセス認証情報の内容を示した説明図である。

【図５】同実施形態にかかる比較データの利用例について説明する説明図である。

【図６】同実施形態にかかる比較データの利用例について説明する説明図である。

【図７】同実施形態にかかるカード発行方法の流れを示したタイミングチャートである。

【図８】同実施形態にかかる認証チケットの検証処理を説明する説明図である。

【図９】同実施形態にかかるＩＣカードの認証情報の検証処理を説明する説明図である。

【図１０】同実施形態にかかるアクセス情報問い合わせ処理を示したタイミングチャートである。

【図１１】本発明の第２の実施形態にかかる情報処理端末、サービス提供サーバ、カード発行サーバの機能構成を示すブロック図である。

【図１２】同実施形態にかかるカード発行方法の流れを示したタイミングチャートである。

【図１３】本発明の第３の実施形態にかかるカード発行システムの構成例を示した説明図である。

【図１４】同実施形態にかかる情報処理端末、サービス提供サーバ、カード発行サーバの機能構成を示すブロック図である。

【図１５】同実施形態にかかるライセンス情報および認証ライセンスの内容を説明する説明図である。

【図１６】同実施形態にかかるアクセス認証情報および認証チケットの内容を説明する説明図である。

【図１７】同実施形態にかかるカード発行方法の流れを示したタイミングチャートである。

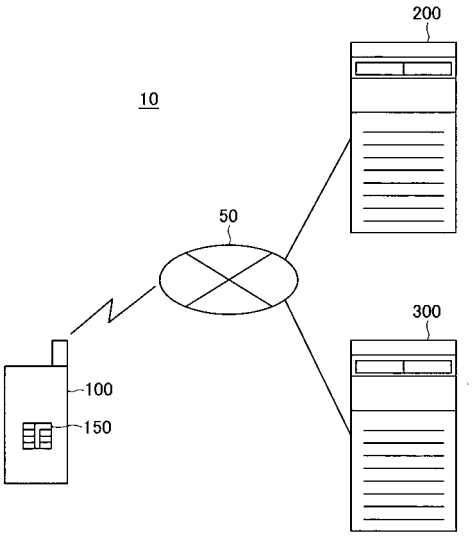
【符号の説明】

【０１２９】

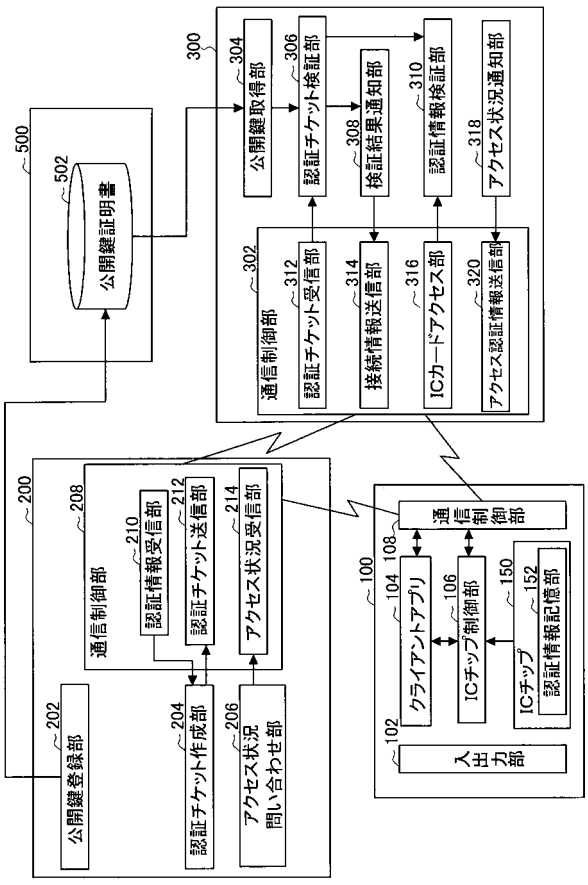
１００　１００′　１０１　情報処理端末
１０４　クライアントアプリ
１５０　ＩＣチップ
２００　２００′　２０１　サービス提供サーバ
２０４　認証チケット作成部
２０６　アクセス状況問い合わせ部
２１２　認証チケット送信部
２２０　認証ライセンス作成部
３００　３００′　３０１　カード発行サーバ
３０６　認証チケット検証部
３０８　検証結果通知部
３１０　認証情報検証部
３１４　接続情報送信部

４００　　サービス代行サーバ
４０２　　認証チケット作成部

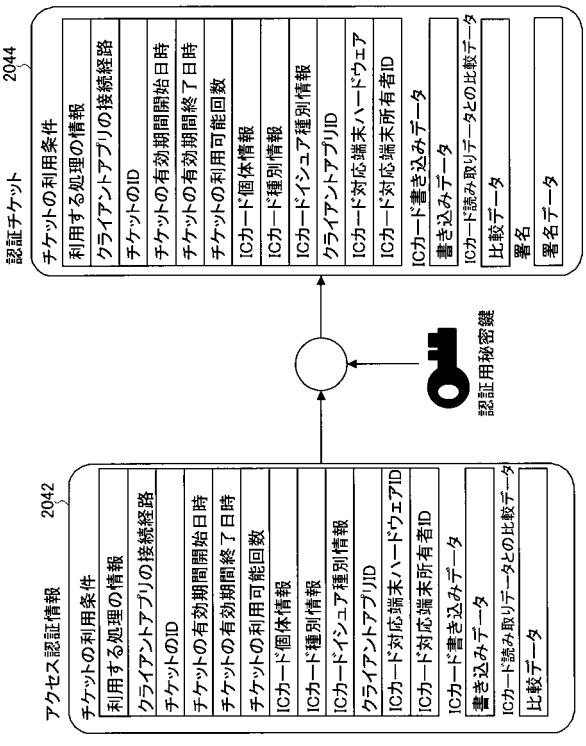
【図１】



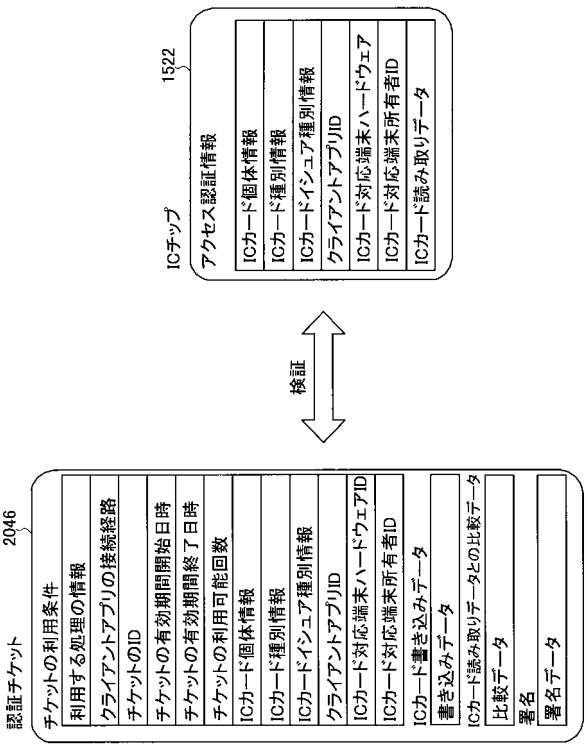
【図２】



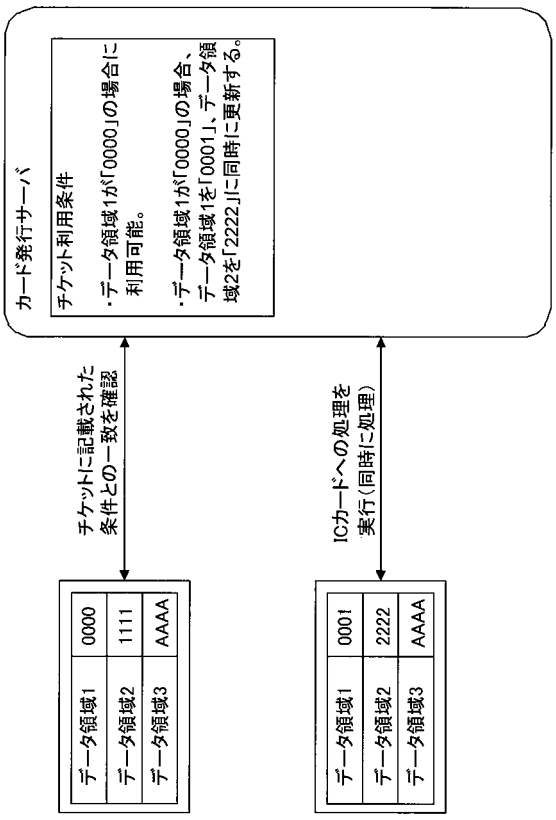
【図３】


認証チケット
2044
チケットの利用条件
利用する処理の情報
クライアントアプリの接続経路
チケットのID
チケットの有効期間開始日時
チケットの有効期間終了日時
チケットの利用可能回数
ICカード個体情報
ICカード種別情報
ICカードインシュア種別情報
クライアントアプリID
ICカード対応端末ハードウェア
ICカード対応端末所有者ID
ICカード書き込みデータ
書き込みデータ
ICカード読み取りデータとの比較データ
比較データ
署名
署名データ
認証用秘密鍵
アクセス認証情報
2042
チケットの利用条件
利用する処理の情報
クライアントアプリの接続経路
チケットのID
チケットの有効期間開始日時
チケットの有効期間終了日時
チケットの利用可能回数
ICカード個体情報
ICカード種別情報
ICカードインシュア種別情報
クライアントアプリID
ICカード対応端末ハードウェアID
ICカード対応端末所有者ID
ICカード書き込みデータ
書き込みデータ
ICカード読み取りデータとの比較データ
比較データ

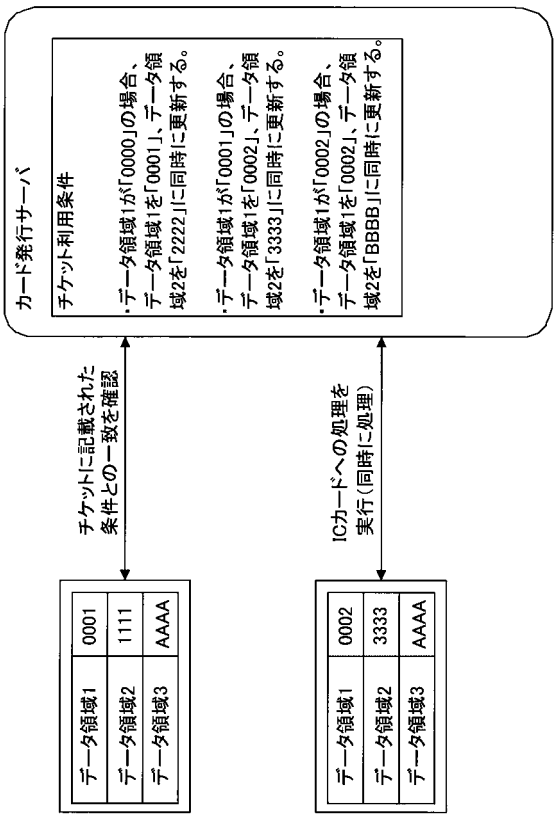
【図４】


ICチップ
1522
アクセス認証情報
ICカード個体情報
ICカード種別情報
ICカードインシュア種別情報
クライアントアプリID
ICカード対応端末ハードウェア
ICカード対応端末所有者ID
ICカード読み取りデータ
検証
認証チケット
2046
チケットの利用条件
利用する処理の情報
クライアントアプリの接続経路
チケットのID
チケットの有効期間開始日時
チケットの有効期間終了日時
チケットの利用可能回数
ICカード個体情報
ICカード種別情報
ICカードインシュア種別情報
クライアントアプリID
ICカード対応端末ハードウェアID
ICカード対応端末所有者ID
ICカード書き込みデータ
書き込みデータ
ICカード読み取りデータとの比較データ
比較データ
署名
署名データ

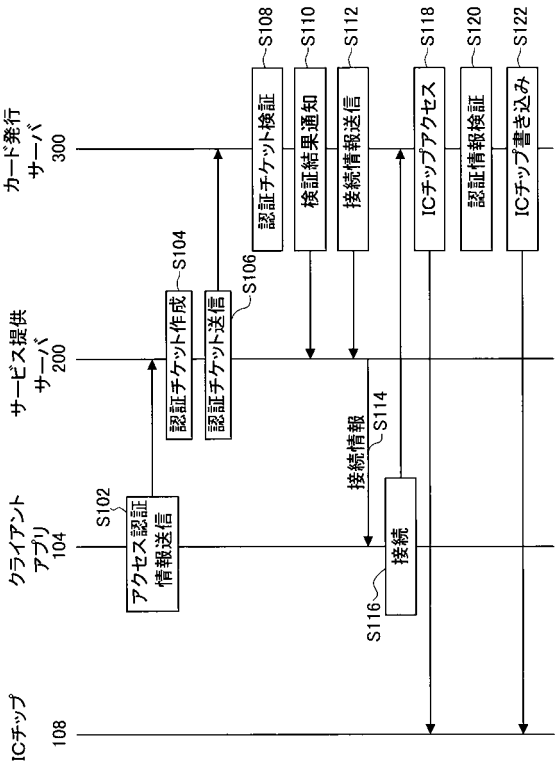
【図５】


カード発行サーバ
チケット利用条件
・データ領域1が「0000」の場合に利用可能。
・データ領域1が「0000」の場合、データ領域1を「0001」、データ領域2を「2222」に同時に更新する。
チケットに記載された条件との一致を確認
ICカードへの処理を実行（同時に処理）
データ領域1 0000
データ領域2 1111
データ領域3 AAAA
データ領域1 0001
データ領域2 2222
データ領域3 AAAA

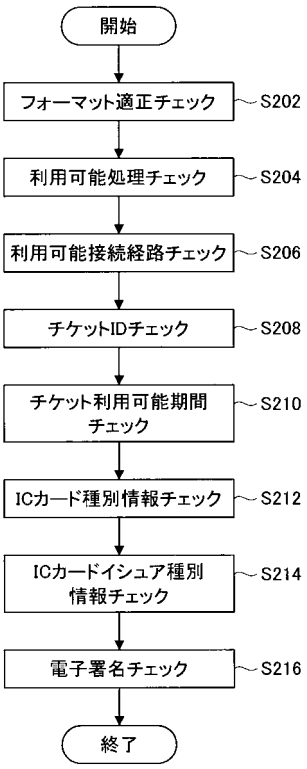
【図６】


カード発行サーバ
チケット利用条件
・データ領域1が「0000」の場合、データ領域1を「0001」、データ領域2を「2222」に同時に更新する。
・データ領域1が「0001」の場合、データ領域1を「0002」、データ領域2を「3333」に同時に更新する。
・データ領域1が「0002」の場合、データ領域1を「0002」、データ領域2を「BBBB」に同時に更新する。
チケットに記載された条件との一致を確認
ICカードへの処理を実行（同時に処理）
データ領域1 0001
データ領域2 1111
データ領域3 AAAA
データ領域1 0002
データ領域2 3333
データ領域3 AAAA

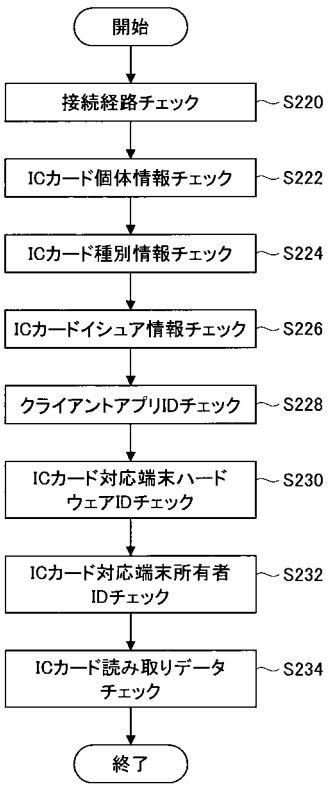
【図７】


カード発行サーバ 300
サービス提供サーバ 200
クライアントアプリ 104
ICチップ 108
S102
アクセス認証情報送信
S104
認証チケット作成
S106
認証チケット送信
S108
認証チケット検証
S110
検証結果通知
S112
接続情報送信
S114
接続情報
S116
接続
S118
ICチップアクセス
S120
認証情報検証
S122
ICチップ書き込み

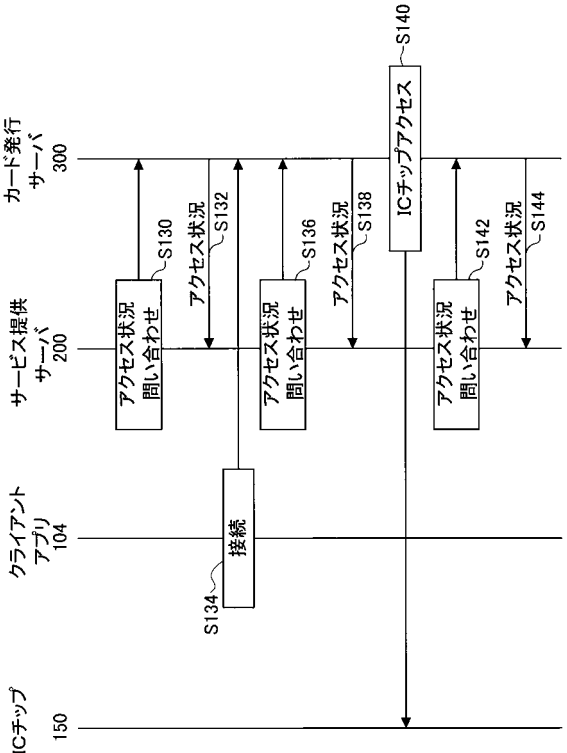
【図８】


開始
フォーマット適正チェック
S202
利用可能処理チェック
S204
利用可能接続経路チェック
S206
チケットIDチェック
S208
チケット利用可能期間チェック
S210
ICカード種別情報チェック
S212
ICカードイシュア種別情報チェック
S214
電子署名チェック
S216
終了

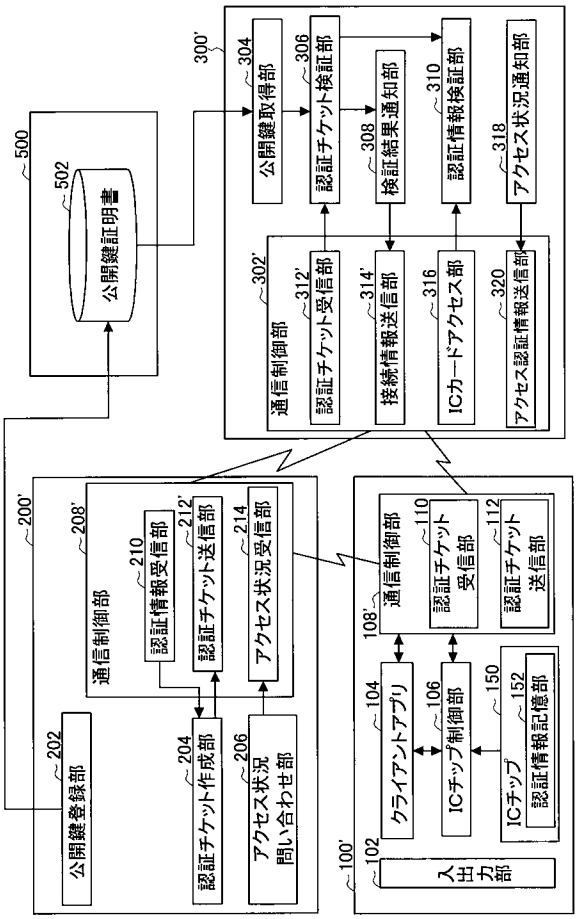
【図９】


開始
接続経路チェック
S220
ICカード個体情報チェック
S222
ICカード種別情報チェック
S224
ICカードイシュア情報チェック
S226
クライアントアプリIDチェック
S228
ICカード対応端末ハードウェアIDチェック
S230
ICカード対応端末所有者IDチェック
S232
ICカード読み取りデータチェック
S234
終了

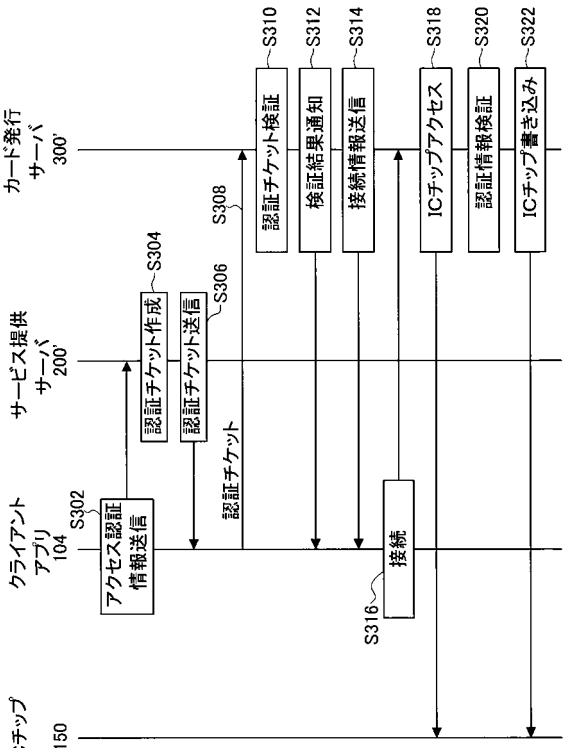
【図１０】


カード発行サーバ 300
サービス提供サーバ 200
クライアントアプリ 104
ICチップ 150
S130
アクセス状況問い合わせ
S132
アクセス状況
S134
接続
S136
アクセス状況問い合わせ
S138
アクセス状況
S140
ICチップアクセス
S142
アクセス状況問い合わせ
S144
アクセス状況

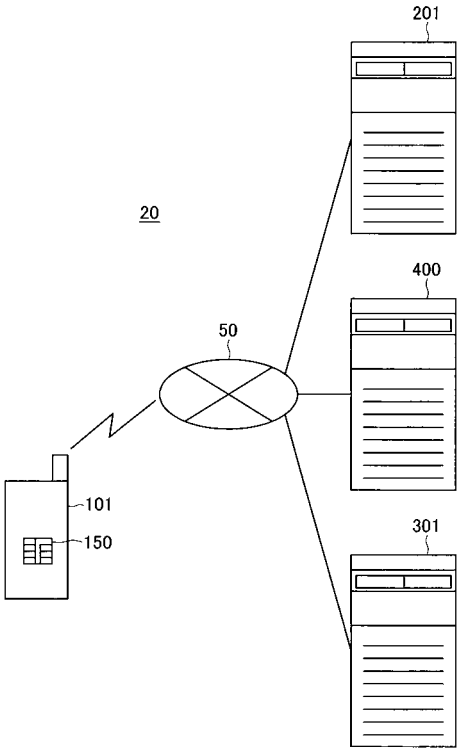
【図１１】



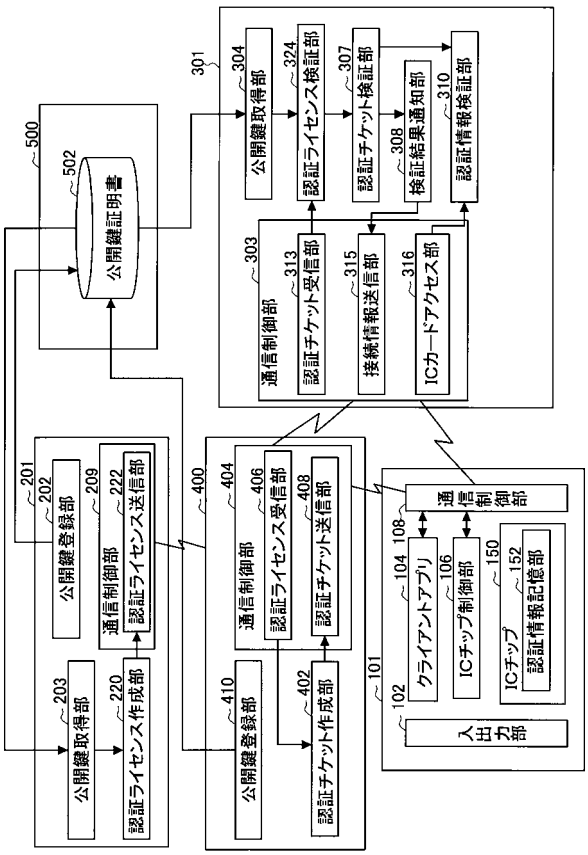
【図１２】



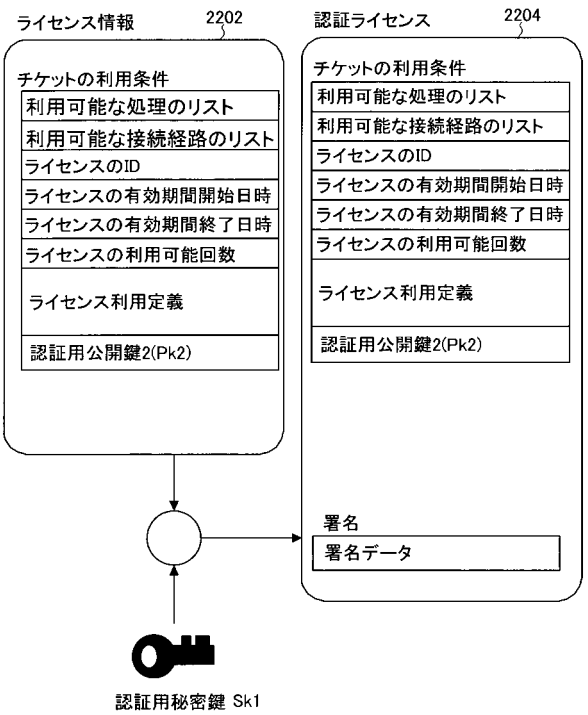
【図１３】



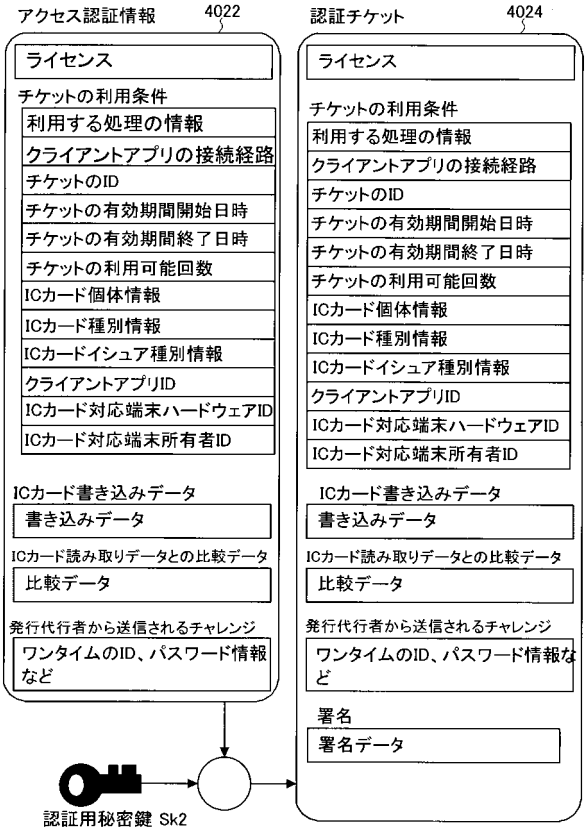
【図１４】



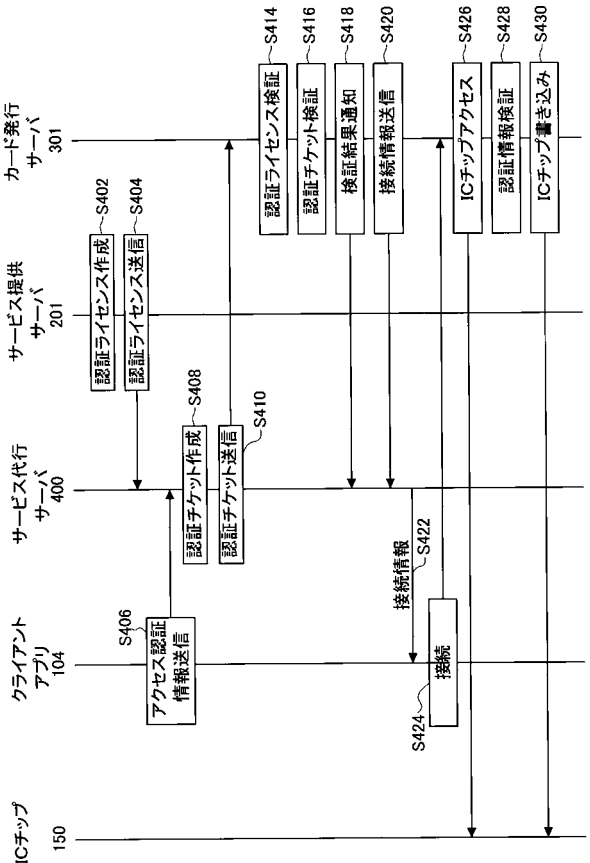
【図１５】


ライセンス情報
2202
チケットの利用条件
利用可能な処理のリスト
利用可能な接続経路のリスト
ライセンスのID
ライセンスの有効期間開始日時
ライセンスの有効期間終了日時
ライセンスの利用可能回数
ライセンス利用定義
認証用公開鍵2(Pk2)
認証ライセンス
2204
チケットの利用条件
利用可能な処理のリスト
利用可能な接続経路のリスト
ライセンスのID
ライセンスの有効期間開始日時
ライセンスの有効期間終了日時
ライセンスの利用可能回数
ライセンス利用定義
認証用公開鍵2(Pk2)
署名
署名データ
認証用秘密鍵 Sk1

【図１６】


アクセス認証情報
4022
ライセンス
チケットの利用条件
利用する処理の情報
クライアントアプリの接続経路
チケットのID
チケットの有効期間開始日時
チケットの有効期間終了日時
チケットの利用可能回数
ICカード個体情報
ICカード種別情報
ICカードイシュア種別情報
クライアントアプリID
ICカード対応端末ハードウェアID
ICカード対応端末所有者ID
ICカード書き込みデータ
書き込みデータ
ICカード読み取りデータとの比較データ
比較データ
発行代行者から送信されるチャレンジ
ワンタイムのID、パスワード情報など
認証チケット
4024
ライセンス
チケットの利用条件
利用する処理の情報
クライアントアプリの接続経路
チケットのID
チケットの有効期間開始日時
チケットの有効期間終了日時
チケットの利用可能回数
ICカード個体情報
ICカード種別情報
ICカードイシュア種別情報
クライアントアプリID
ICカード対応端末ハードウェアID
ICカード対応端末所有者ID
ICカード書き込みデータ
書き込みデータ
ICカード読み取りデータとの比較データ
比較データ
発行代行者から送信されるチャレンジ
ワンタイムのID、パスワード情報など
署名
署名データ
認証用秘密鍵 Sk2

【図１７】


カード発行サーバ 301
サービス提供サーバ 201
サービス代行サーバ 400
クライアントアプリ 104
ICチップ 150
S402
認証ライセンス作成
S404
認証ライセンス送信
S406
アクセス認証情報送信
S408
認証チケット作成
S410
認証チケット送信
S414
認証ライセンス検証
S416
認証チケット検証
S418
検証結果通知
S420
接続情報送信
S422
接続情報
S424
接続
S426
ICチップアクセス
S428
認証情報検証
S430
ICチップ書き込み

フロントページの続き

審査官　青木　重徳

(56)参考文献　特表２００５－５０５９９１（ＪＰ，Ａ）
国際公開第０１／０６９４７５（WO，Ａ１）
特開２００７－１７２５８８（ＪＰ，Ａ）
特表２００５－５１７３４７（ＪＰ，Ａ）
特開２００５－３１１９０４（ＪＰ，Ａ）
Larry J. Hughes, Jr 著／長原宏治　監訳，“インターネットセキュリティ”，日本，株式会社インプレス，１９９７年　2月２１日，初版，ｐ．８６－１０８，INTERNET Exciting Technology Series
吉永尚史，服部易憲，佐藤哲夫，吉田雅裕，鷲尾諭，“ｉ－ｍｏｄｅ　ＦｅｌｉＣａの開発”，ＮＴＴ　ＤｏＣｏＭｏテクニカル・ジャーナル，日本，社団法人電気通信協会，２００４年１０月　1日，Ｖｏｌ．１２，Ｎｏ．３，ｐ．２５－３２

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｋ　１７／００