(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003 年11 月20 日 (20.11.2003)

PCT

(10) 国際公開番号
WO 03/096204 A1

(51) 国際特許分類[7]: G06F 15/00, 12/14, 17/60, H04L 9/32

(21) 国際出願番号: PCT/JP03/05604

(22) 国際出願日: 2003 年5 月2 日 (02.05.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-136533 2002 年5 月13 日 (13.05.2002) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

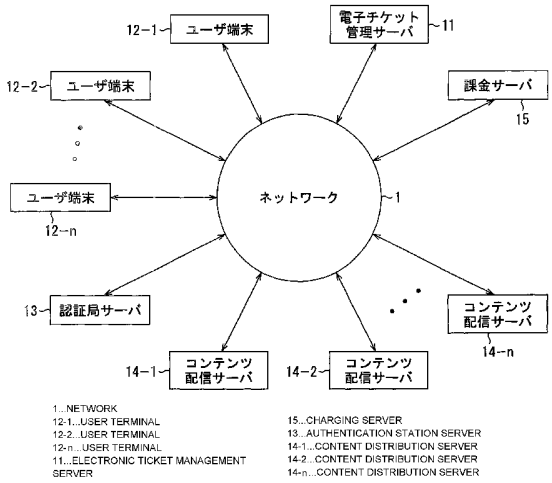
(75) 発明者/出願人 (米国についてのみ): 中野 雄彦 (NAKANO,Takehiko) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 小室 輝芳 (KOMURO,Teruyoshi) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 稲本 義雄 (INAMOTO,Yoshio); 〒160-0023 東京都 新宿区 西新宿７丁目１１番１８号 ７１１ビルディング４階 Tokyo (JP).

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE AND METHOD, INFORMATION PROCESSING SYSTEM, RECORDING MEDIUM, AND PROGRAM

(54) 発明の名称: 情報処理装置および方法、情報処理システム、記録媒体、並びにプログラム



(57) Abstract: An information processing device and method, an information processing system, a recording medium, and a program capable of acquiring information not limited by a device when they have a right to acquire information circulating via a network. A user terminal (12) transmits an electronic ticket having its digital signature to an electronic ticket management server (11) and requests for information used to access a content distribution server (14) distributing a content corresponding to the electronic ticket. The electronic ticket management server (11) checks the digital signature to judge whether the electronic ticket is authentic. If the signature is judged to be authentic, the electronic ticket management server (11) transmits to the user terminal (12) an encryption key for accessing the content distribution server, the key being stored in the server (11). The user terminal (12) accesses the content distribution server (14) by using the encryption key and receives a content distribution. The present invention can be applied to a content distribution system.

(57) 要約: 本発明は、ネットワークを介して流通する情報を取得する権利を所有するとき、機器に制限されることなく情報を取得することができるようにした情報処理装置および方法、情報処理システム、記録媒体、並びにプログラムに関する。ユーザ端末１２は、自らの電子署名つきの電子チケットを電子チケット管理サーバ１１に送付し、その電子チケットに対応するコンテンツを配信するコンテンツ配信サーバ１４にアクセスするための情報を要求する。電子チケット管理サーバ１１は、電子署名を確認して電子チケッ

[続葉有]

WO 03/096204 A1

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

トが正当なものであるか否かを判定し、正当なものである時、自らで記憶しているコンテンツ配信サーバにアクセスするための暗号鍵をユーザ端末１２に送付する。ユーザ端末１２は、受信した暗号鍵を用いてコンテンツ配信サーバ１４にアクセスして、コンテンツの配信を受ける。本発明は、コンテンツを配信するシステムに適用することができる。

明細書

情報処理装置および方法、情報処理システム、記録媒体、並びにプログラム

技術分野

本発明は、情報処理装置および方法、情報処理システム、記録媒体、並びにプログラムに関し、特に、コンテンツプロバイダがコンテンツを配信するシステムにおいて、コンテンツプロバイダに支払われるコンテンツの対価を、コンテンツの配信を受けるユーザの評価に応じて設定できるようにした情報処理装置および方法、情報処理システム、記録媒体、並びにプログラムに関する。

背景技術

インターネットなどのネットワークを通じて音楽や映画コンテンツを配信するサービスが普及しつつある。

このようなネットワークを利用した音楽や映画コンテンツの配信においては、まず、コンテンツの利用を希望するユーザが、暗号を解くためのデータ、いわゆる鍵データをコンテンツの配給元から購入することで、配信されるコンテンツへのアクセス権を購入する。さらに、コンテンツの配給元は、配信するコンテンツをその鍵データに対応する手法で暗号化し、これをユーザに配信する。ユーザは、この鍵データを用いて配信されたコンテンツを復号して、元のコンテンツを再生する。

しかしながら、上記の鍵データは、ユーザが購入する際に、コンテンツ配給元にアクセスする際に使用した機器に記憶されることで、その機器がその鍵データを用いて暗号化されたコンテンツを復号することで使用できる構成となっている。このため、鍵データを購入した際に使用した機器以外の他の機器に鍵データだけを移すと言ったことができない。結果として、ユーザは、この鍵データ（すなわち、コンテンツデータへのアクセス権）を購入したにもかかわらず、例えば、他の機器を利用してコンテンツにアクセスすると言ったことができず、他の機器で

使用するには、さらにもう１つの鍵データを購入せざるを得ないという課題があった。また、鍵データを機器間で移動させることができないため、この鍵データそのものをユーザ間でプレゼントすると言ったことができないという課題があった。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、アクセス権を鍵データによって管理するのではなく、アクセス権の所有者の情報だけを管理することにより、アクセス権を所有する本人であることが確認されれば、機器やアクセス権の購入者に限らず、コンテンツへのアクセスを自由にできるようにするものである。

本発明の第１の情報処理装置は、所定の情報を取得する権利を示す電子チケットを記憶する記憶手段と、電子チケットを識別するチケットIDと、チケットIDに対する電子署名をその他の情報処理装置に送信する送信手段と、チケットIDと電子署名に基づいて、その他の情報処理装置より送信されてくる所定の情報を取得するための暗号鍵を受信する受信手段と、受信手段により受信された暗号鍵を使用して、所定の情報を取得する取得手段とを備えることを特徴とする。

前記電子チケットには、チケットIDに加えて、取得可能な所定の情報を識別するアクセス情報ID、チケットID、またはアクセス情報IDに対する電子署名を含ませるようにすることができる。

前記アクセス情報IDには、所定の情報のインターネット上のURLを含ませるようにすることができる。

前記記憶手段には、電子チケットに加えて、電子チケットに含まれる情報に対する電子署名と、電子チケットに含まれる情報に対する電子署名の検証用の公開鍵、電子チケットの所有者を識別するユーザID、並びに公開鍵、およびユーザIDに対する電子署名を含むユーザ証明書を記憶させるようにすることができ、

送信手段には、電子チケットと共に、電子署名、およびユーザ証明書をその他の情報処理装置に送信させるようにすることができる。

前記電子チケットの所有者を識別するユーザIDを、所有者とは異なる他の所有者にユーザIDに変更するようにその他の情報処理装置に要求する要求手段をさらに設けるようにすることができる。

前記要求手段が、電子チケットの所有者を識別するユーザIDを、所有者とは異なる他の所有者のユーザIDに変更するように、その他の情報処理装置に要求するとき、変更に伴う対価を設定する対価設定手段をさらに設けるようにすることができる。

前記対価設定手段には、変更に伴う対価を所有者により設定された対価とするようにさせることができる。

前記対価設定手段には、変更に伴う対価を他の所有者により設定された対価とするようにさせることができる。

前記所定の情報には、映画、または、音楽を含ませるようにすることができる。

本発明の第1の情報処理方法は、所定の情報を取得する権利を示す電子チケットを記憶する記憶ステップと、電子チケットを識別するチケットIDと、チケットIDに対する電子署名をその他の情報処理装置に送信する送信ステップと、チケットIDと電子署名に基づいて、その他の情報処理装置より送信されてくる所定の情報を取得するための暗号鍵を受信する受信ステップと、受信ステップの処理で受信された暗号鍵を使用して、所定の情報を取得する取得ステップとを含むことを特徴とする。

本発明の第1の記録媒体のプログラムは、所定の情報を取得する権利を示す電子チケットの記憶を制御する記憶制御ステップと、電子チケットを識別するチケットIDと、チケットIDに対する電子署名のその他の情報処理装置への送信を制御する送信制御ステップと、チケットIDと電子署名に基づいて、その他の情報処理装置より送信されてくる所定の情報を取得するための暗号鍵の受信を制御

する受信制御ステップと、受信制御ステップの処理で受信された暗号鍵の使用と、所定の情報の取得を制御する取得制御ステップとを含むことを特徴とする。

本発明の第１のプログラムは、所定の情報を取得する権利を示す電子チケットの記憶を制御する電子チケット記憶制御ステップと、電子チケットを識別するチケットIDと、チケットIDに対する電子署名の第１の情報処理装置への送信を制御する送信制御ステップと、チケットIDと電子署名に基づいて、第１の情報処理装置より送信されてくる所定の情報を取得するための暗号鍵の受信を制御する受信制御ステップと、受信制御ステップの処理で受信された暗号鍵の使用と、所定の情報の取得を制御する取得制御ステップとをコンピュータに実行させることを特徴とする。

本発明の第２の情報処理装置は、電子チケットを識別するチケットIDと、チケットID毎に対応する所定の情報の取得を可能にする暗号鍵を記憶する記憶手段と、他の情報処理装置より送信されてくる、電子チケットを識別するチケットIDと、チケットIDに対する電子署名を受信する受信手段と、チケットIDに対する電子署名が正当なものであるか否かを判定する判定手段と、判定手段の判定結果に基づいて、チケットIDに対応する所定の情報の取得を可能にする暗号鍵を、その他の情報処理装置に送信する送信手段とを備えることを特徴とする。

前記電子チケットには、チケットIDに加えて、取得可能な所定の情報を識別するアクセス情報ID、チケットID、またはアクセス情報IDに対する電子署名を含ませるようにすることができる。

前記アクセス情報IDには、所定の情報のインターネット上のURLを含ませるようにすることができる。

前記電子チケットには、チケットID、または、電子署名に加えて、電子チケットの所有者を識別するユーザIDを含ませるようにすることができる。

前記記憶手段には、電子チケットを識別するチケットIDと、チケットID毎に対応する所定の情報の取得を可能にする暗号鍵に加えて、チケットID毎に所定の情報の取得にかかる状態を記憶させるようにすることができる。

前記送信手段が、チケットIDに対応する所定の情報の取得を可能にする暗号鍵を、その他の情報処理装置に送信するとき、チケットID毎に所定の情報の取得にかかる状態を変更させる状態変更手段をさらに設けるようにさせることができる。

前記状態変更手段には、送信手段が、チケットIDに対応する所定の情報の取得を可能にする暗号鍵を、その他の情報処理装置に送信するとき、チケットID毎に所定の情報の取得にかかる状態のうち、取得可能回数を変更させるようにすることができる。

前記状態変更手段には、送信手段が、チケットIDに対応する所定の情報の取得を可能にする暗号鍵を、その他の情報処理装置に送信するとき、チケットID毎に所定の情報の取得にかかる状態のうち、取得可能な期限を変更させるようにすることができる。

前記記憶手段には、電子チケットを識別するチケットIDと、チケットID毎に対応する所定の情報の取得を可能にする暗号鍵に加えて、チケットID毎にその所有者を識別するユーザIDを記憶させるようにすることができる。

前記電子署名には、ユーザIDを含ませるようにすることができ、電子署名に含まれた電子チケットの使用者のユーザIDと、記憶手段により記憶されている電子チケットの所有者のユーザIDとを比較し、比較結果に応じて、電子チケットの所有者と使用者が一致しているか否かを確認する確認手段をさらに設けるようにさせることができる。

前記他の情報処理装置より送信されてくる電子チケットのユーザIDの変更要求を受信する変更要求受信手段と、変更要求に対応して、記憶手段により記憶されている電子チケットのユーザIDを、所有者とは異なる他の所有者のIDに変更するユーザID変更手段とをさらに設けるようにさせることができる。

前記変更要求受信手段は、電子チケットのユーザIDの変更要求に加えて、変更にかかる対価の情報を受信し、ユーザID変更手段が、記憶手段により記憶されている電子チケットのユーザIDを、所有者とは異なる他の所有者のIDに変

更するとき、対価の情報に基づいた課金を行う課金手段をさらに設けるようにさせることができる。

本発明の第２の情報処理方法は、電子チケットを識別するチケットIDと、チケットID毎に対応する所定の情報の取得を可能にする暗号鍵を記憶する記憶ステップと、他の情報処理装置より送信されてくる、電子チケットを識別するチケットIDと、チケットIDに対する電子署名を受信する受信ステップと、チケットIDに対する電子署名が正当なものであるか否かを判定する判定ステップと、判定ステップの処理での判定結果に基づいて、チケットIDに対応する所定の情報の取得を可能にする暗号鍵を、その他の情報処理装置に送信する送信ステップとを含むことを特徴とする。

本発明の第２の記録媒体のプログラムは、電子チケットを識別するチケットIDと、チケットID毎に対応する所定の情報の取得を可能にする暗号鍵の記憶を制御する記憶制御ステップと、他の情報処理装置より送信されてくる、電子チケットを識別するチケットIDと、チケットIDに対する電子署名の受信を制御する受信制御ステップと、チケットIDに対する電子署名が正当なものであるか否かの判定を制御する判定制御ステップと、判定制御ステップの処理での判定結果に基づいて、チケットIDに対応する所定の情報の取得を可能にする暗号鍵の、その他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とする。

本発明の第２のプログラムは、電子チケットを識別するチケットIDと、チケットID毎に対応する所定の情報の取得を可能にする暗号鍵の記憶を制御する記憶制御ステップと、他の情報処理装置より送信されてくる、電子チケットを識別するチケットIDと、チケットIDに対する電子署名の受信を制御する受信制御ステップと、チケットIDに対する電子署名が正当なものであるか否かの判定を制御する判定制御ステップと、判定制御ステップの処理での判定結果に基づいて、チケットIDに対応する所定の情報の取得を可能にする暗号鍵の、その他の情報処理装置への送信を制御する送信制御ステップとをコンピュータに実行させる。

本発明の情報処理システムは、第１の情報処理装置が、所定の情報を取得する権利を示す電子チケットを記憶する第１の記憶手段と、電子チケットを識別するチケットIDと、チケットIDに対する電子署名を第２の情報処理装置に送信する第１の送信手段と、チケットIDと電子署名に基づいて、第２の情報処理装置より送信されてくる所定の情報を取得するための暗号鍵を受信する第１の受信手段と、第１の受信手段により受信された暗号鍵を使用して、所定の情報を取得する取得手段とを備え、第２の情報処理装置が、電子チケットを識別するチケットIDと、チケットID毎に対応する所定の情報の取得を可能にする暗号鍵を記憶する第２の記憶手段と、第１の情報処理装置より送信されてくる、電子チケットを識別するチケットIDと、チケットIDに対する電子署名を受信する第２の受信手段と、チケットIDに対する電子署名が正当なものであるか否かを判定する判定手段と、判定手段の判定結果に基づいて、チケットIDに対応する所定の情報の取得を可能にする暗号鍵を、第１の情報処理装置に送信する第２の送信手段とを備えることを特徴とする。

本発明の第１の情報処理装置および方法、並びに第１のプログラムにおいては、所定の情報を取得する権利を示す電子チケットが記憶され、電子チケットを識別するチケットIDと、チケットIDに対する電子署名がその他の情報処理装置に送信され、チケットIDと電子署名に基づいて、その他の情報処理装置より送信されてくる所定の情報を取得するための暗号鍵が受信され、受信された暗号鍵が使用されて、所定の情報が取得される。

本発明の第２の情報処理装置および方法、並びに第２のプログラムにおいては、電子チケットを識別するチケットIDと、チケットID毎に対応する所定の情報の取得を可能にする暗号鍵が記憶され、他の情報処理装置より送信されてくる、電子チケットを識別するチケットIDと、チケットIDに対する電子署名が受信され、チケットIDに対する電子署名が正当なものであるか否かが判定され、判定結果に基づいて、チケットIDに対応する所定の情報の取得を可能にする暗号鍵が、その他の情報処理装置に送信される。

本発明の情報処理システムにおいては、第１の情報処理装置により、所定の情報を取得する権利を示す電子チケットが記憶され、電子チケットを識別するチケットIDと、チケットIDに対する電子署名が第２の情報処理装置に送信され、チケットIDと電子署名に基づいて、第２の情報処理装置より送信されてくる所定の情報を取得するための暗号鍵が受信され、受信された暗号鍵が使用されて、所定の情報が取得され、第２の情報処理装置により、電子チケットを識別するチケットIDと、チケットID毎に対応する所定の情報の取得を可能にする暗号鍵が記憶され、第１の情報処理装置より送信されてくる、電子チケットを識別するチケットIDと、チケットIDに対する電子署名が受信され、チケットIDに対する電子署名が正当なものであるか否かが判定され、判定結果に基づいて、チケットIDに対応する所定の情報の取得を可能にする暗号鍵が、第１の情報処理装置に送信される。

図面の簡単な説明

図１は、本発明を適用したコンテンツ配信システムのブロック図である。

図２は、図１の電子チケット管理サーバのブロック図である。

図３は、図１のユーザ端末のブロック図である。

図４は、図１の認証局サーバのブロック図である。

図５は、図１のコンテンツ配信サーバのブロック図である。

図６は、図１の課金サーバのブロック図である。

図７は、図２の電子チケット管理サーバの機能ブロック図である。

図８は、電子チケットを説明する図である。

図９は、図７の電子チケットデータベースの構成を説明する図である。

図１０は、図３のユーザ端末の機能ブロック図である。

図１１は、図４の認証局サーバの機能ブロック図である。

図１２は、図５のコンテンツ配信サーバの機能ブロック図である。

図１３は、図６の金融サーバの機能ブロック図である。

図１４は、電子チケット購入処理を説明するフローチャートである。

図１５は、コンテンツ配信処理を説明するフローチャートである。

図１６は、電子チケット管理サーバのブロック図である。

図１７は、図１６の電子チケット管理サーバの機能ブロック図である。

図１８は、図１７の電子チケットデータベースの構成を説明する図である。

図１９は、電子チケット購入処理を説明するフローチャートである。

図２０は、コンテンツ配信処理を説明するフローチャートである。

図２１は、電子チケット管理サーバのブロック図である。

図２２は、ユーザ端末のブロック図である。

図２３は、電子チケット管理サーバの機能ブロック図である。

図２４は、図２３の電子チケットデータベースの構成を説明する図である。

図２５は、ユーザ端末の機能ブロック図である。

図２６は、電子チケットの構成を示す図である。

図２７は、電子チケット購入処理を説明するフローチャートである。

図２８は、コンテンツ配信処理を説明するフローチャートである。

図２９は、コンテンツ配信処理を説明するフローチャートである。

図３０は、電子チケット管理サーバのブロック図である。

図３１は、ユーザ端末のブロック図である。

図３２は、図３０の電子チケット管理サーバの機能ブロック図である。

図３３は、図３１のユーザ端末の機能ブロック図である。

図３４は、図３１のユーザ端末による電子チケット移動処理を説明するフローチャートである。

図３５は、移動される電子チケットの構成を説明する図である。

図３６は、図３１のユーザ端末による電子チケット移動処理を説明するフローチャートである。

図３７は、図３１のユーザ端末による電子チケット移動処理を説明するフローチャートである。

図３８は、移動される電子チケットの構成を説明する図である。

図３９は、図３０の電子チケット管理サーバによるコンテンツ配信処理を説明するフローチャートである。

図４０は、図３０の電子チケット管理サーバによるコンテンツ配信処理を説明するフローチャートである。

図４１は、課金サーバによる課金処理を説明するフローチャートである。

発明を実施するための最良の形態

図１は、本発明に係るコンテンツ配信システムの一実施の形態の構成を示す図である。

電子チケット管理サーバ１１は、ネットワーク１を介して各ユーザの所有するユーザ端末１２－１乃至１２－ｎからの要求に応じて、例えば、音楽や映画などのコンテンツ毎に電子チケットを発行し供給する。電子チケット管理サーバ１１は、各電子チケットを購入したユーザの情報を管理して、ユーザ端末１２－１乃至１２－ｎからのコンテンツ配信サーバ１４－１乃至１４－ｎに対するアクセス要求（コンテンツの配信要求）があったとき、電子チケットの種類に応じて、コンテンツの取得に必要な暗号鍵を供給する。尚、ここで、ユーザ端末１２－１乃至１２－ｎ、および、コンテンツ配信サーバ１４－１乃至１４－ｎを個々に区別する必要がない場合、単に、ユーザ端末１２、および、コンテンツ配信サーバ１４と称する。また、以下においては、他の機器についても同様に称する。

ユーザ端末１２－１乃至１２－ｎは、各ユーザの保有する端末装置であり、ユーザの操作に応じて、所定のコンテンツの電子チケットを電子チケット管理サーバ１１より購入し、また、購入した電子チケットに対応したコンテンツを配信するコンテンツ配信サーバ１４－１乃至１４－ｎにアクセスし、コンテンツを取得して（コンテンツの配信を受けて）再生する。

認証局サーバ１３は、各ユーザ端末１２－１乃至１２－ｎについて、ユーザが使用する秘密鍵に対応する公開鍵の電子証明書を生成し、ユーザ端末１２－１乃至１２－ｎに供給する。

コンテンツ配信サーバ１４－１乃至１４－ｎは、各々が音楽や映画などのコンテンツを配信する業者により管理運営されるサーバであり、各コンテンツに対応する電子チケットを所有するユーザ端末１２にコンテンツのデータを配信する。

課金サーバ１５は、銀行やクレジットカード会社などの金融機関により管理運営されるサーバであり、電子チケット管理サーバ１１、または、ユーザ端末１２からの要求に応じて、電子チケットの購入、または、電子チケットの移動に際して必要な課金処理を行うサーバである。

図２は、本発明に係る電子チケット管理サーバ１１の構成を示す図である。CPU（Central Processing Unit）３１は、ROM（Read Only Memory）３２、または記憶部３８に記憶されているデータやプログラム（電子チケットデータベース３８ａ、電子チケット管理プログラム３８ｂ、および、署名管理プログラム３８ｃ）に従って各種の処理を実行する。RAM（Random Access Memory）３３には、CPU３１が実行するプログラムやデータなどが適宜記憶される。これらのCPU３１、ROM３２、およびRAM３３は、バス３４により相互に接続されている。

CPU３１にはまた、バス３４を介して入出力インタフェース３５が接続されている。入出力インタフェース３５には、キーボード、マウス、マイクロホンなどよりなる入力部３６、ディスプレイ、スピーカなどよりなる出力部３７が接続されている。CPU３１は、入力部３６から入力される指令に対応して各種の処理を実行する。そして、CPU３１は、処理の結果得られた画像や音声等を出力部３７に出力する。

入出力インタフェース３５に接続されている記憶部３８は、例えばハードディスクなどで構成され、CPU４１が実行するプログラムや各種のデータを記憶する。通信部３９は、図１のネットワーク１で示す、例えば、インターネット、その他のネットワークを介して外部の装置と通信する。

また、記憶部３８は、電子チケットデータベース３８ａ、電子チケット管理プログラム３８ｂ、および、署名管理プログラム３８ｃ等のプログラムを記憶しており、CPU３１は、これらのプログラムを読み出して対応する処理を実行する。さらに、記憶部３８は、この他にも、基本プログラムであるOS（Operating System）３０１（図７）や、ドライバ３０２（図７）も記憶している。尚、各種のプログラムについては、図７を参照して後述する。

また、記憶部３８に記憶されるプログラムは、上述のほかにも、通信部３９を介してプログラムを取得し、記憶部３８に記憶してもよい。

入出力インタフェース３５に接続されているドライブ４０は、磁気ディスク５１、光ディスク５２、光磁気ディスク５３、或いは半導体メモリ５４などが装着されたとき、それらを駆動し、そこに記録されているプログラムやデータなどを取得する。取得されたプログラムやデータは、必要に応じて記憶部３８に転送され、記憶される。

次に、図３を参照して、ユーザ端末１２の構成について説明する。ユーザ端末１２は、基本的に図２で説明した電子チケット管理サーバ１１の構成と同様である。すなわち、ユーザ端末１２のCPU７１，ROM７２，RAM７３，バス７４，入出力インタフェース７５，入力部７６，出力部７７，記憶部７８，通信部７９，ドライブ８０，磁気ディスク９１，光ディスク９２，光磁気ディスク９３、および半導体メモリ９４は、図２の電子チケット管理サーバ１１の CPU３１，ROM３２，RAM３３，バス３４，入出力インタフェース３５，入力部３６，出力部３７，記憶部３８，通信部３９，ドライブ４０，磁気ディスク５１，光ディスク５２，光磁気ディスク５３、および半導体メモリ５４に対応するものであり、同様の機能を有するものである。

但し、記憶部７８に記憶されているプログラムは、図２の電子チケット管理サーバ１１の記憶部３８に記憶されているプログラムとは異なる。記憶部７８は、電子チケット管理プログラム７８ａ、署名管理プログラム７８ｂ、およびコンテンツ再生プログラム７８ｃを記憶しており、CPU７１は、これらのプログラムを

適宜読み出して実行する。さらに、記憶部７８は、基本プログラムであるOS３１１（図１０）や、ドライバ３１２（図１０）も記憶している。尚、各種のプログラムについては、図１０を参照して後述する。

次に、図４を参照して、認証局サーバ１３の構成について説明する。認証局サーバ１３は、基本的に図２，図３で説明した電子チケット管理サーバ１１、および、ユーザ端末１２の構成と同様である。すなわち、認証局サーバ１３のCPU１１１，ROM１１２，RAM１１３，バス１１４，入出力インタフェース１１５，入力部１１６，出力部１１７，記憶部１１８，通信部１１９，ドライブ１２０，磁気ディスク１３１，光ディスク１３２，光磁気ディスク１３３、および半導体メモリ１３４は、図２の電子チケット管理サーバ１１のCPU３１，ROM３２，RAM３３，バス３４，入出力インタフェース３５，入力部３６，出力部３７，記憶部３８，通信部３９，ドライブ４０，磁気ディスク５１，光ディスク５２，光磁気ディスク５３、および半導体メモリ５４、または、図３のユーザ端末１２のCPU７１，ROM７２，RAM７３，バス７４，入出力インタフェース７５，入力部７６，出力部７７，記憶部７８，通信部７９，ドライブ８０，磁気ディスク９１，光ディスク９２，光磁気ディスク９３、および半導体メモリ９４に対応するものであり、同様の機能を有するものである。

但し、記憶部１１８に記憶されているプログラムは、図２の電子チケット管理サーバ１１の記憶部３８、または、図３のユーザ端末１２の記憶部７８に記憶されているプログラムとは異なる。記憶部１１８は、電子証明書発行プログラム１１８ａを記憶しており、CPU１１１は、これらのプログラムを適宜読み出して実行する。さらに、記憶部１１８は、この他にも、基本プログラムであるOS３２１（図１１）や、ドライバ３２２（図１１）も記憶している。尚、各種のプログラムについては、図１１を参照して後述する。

次に、図５を参照して、コンテンツ配信サーバ１４の構成について説明する。コンテンツ配信サーバ１４は、基本的に図２乃至図４で説明した電子チケット管理サーバ１１、ユーザ端末１２、および認証局サーバ１３の構成と同様である。

すなわち、コンテンツ配信サーバ１４のCPU１５１，ROM１５２，RAM１５３，バス１５４，入出力インタフェース１５５，入力部１５６，出力部１５７，記憶部１５８，通信部１５９，ドライブ１６０，磁気ディスク１７１，光ディスク１７２，光磁気ディスク１７３、および半導体メモリ１７４は、図２の電子チケット管理サーバ１１のCPU３１，ROM３２，RAM３３，バス３４，入出力インタフェース３５，入力部３６，出力部３７，記憶部３８，通信部３９，ドライブ４０，磁気ディスク５１，光ディスク５２，光磁気ディスク５３、および半導体メモリ５４、図３のユーザ端末１２のCPU７１，ROM７２，RAM７３，バス７４，入出力インタフェース７５，入力部７６，出力部７７，記憶部７８，通信部７９，ドライブ８０，磁気ディスク９１，光ディスク９２，光磁気ディスク９３、および半導体メモリ９４、または、図４の認証局サーバ１３のCPU１１１，ROM１１２，RAM１１３，バス１１４，入出力インタフェース１１５，入力部１１６，出力部１１７，記憶部１１８，通信部１１９，ドライブ１２０，磁気ディスク１３１，光ディスク１３２，光磁気ディスク１３３、および半導体メモリ１３４に対応するものであり、同様の機能を有するものである。

但し、記憶部１５８に記憶されているプログラムは、図２の電子チケット管理サーバ１１の記憶部３８、図３のユーザ端末１２の記憶部７８、または図４の認証局サーバ１３の記憶部１１８に記憶されているプログラムとは異なる。記憶部１５８は、コンテンツ管理プログラム１５８ａ、および署名管理プログラム１５８ｂを記憶しており、CPU１５１は、これらのプログラムを適宜読み出して実行する。さらに、記憶部１５８は、図５には図示しないが、この他にも、基本プログラムであるOS３３１（図１２）や、ドライバ３３２（図１２）も記憶している。尚、各種のプログラムについては、図１２を参照して後述する。

次に、図６を参照して、課金サーバ１５の構成について説明する。課金サーバ１５は、基本的に図２乃至図５で説明した電子チケット管理サーバ１１、ユーザ端末１２、認証局サーバ１３、およびコンテンツ配信サーバ１４の構成と同様である。すなわち、課金サーバ１５のCPU１９１，ROM１９２，RAM１９３，バス１

９４，入出力インタフェース１９５，入力部１９６，出力部１９７，記憶部１９８，通信部１９９，ドライブ２００，磁気ディスク２１１，光ディスク２１２，光磁気ディスク２１３、および半導体メモリ２１４は、図２の電子チケット管理サーバ１１のCPU３１，ROM３２，RAM３３，バス３４，入出力インタフェース３５，入力部３６，出力部３７，記憶部３８，通信部３９，ドライブ４０，磁気ディスク５１，光ディスク５２，光磁気ディスク５３、および半導体メモリ５４、図３のユーザ端末１２のCPU７１，ROM７２，RAM７３，バス７４，入出力インタフェース７５，入力部７６，出力部７７，記憶部７８，通信部７９，ドライブ８０，磁気ディスク９１，光ディスク９２，光磁気ディスク９３、および半導体メモリ９４、または、図４の認証局サーバ１３のCPU１１１，ROM１１２，RAM１１３，バス１１４，入出力インタフェース１１５，入力部１１６，出力部１１７，記憶部１１８，通信部１１９，ドライブ１２０，磁気ディスク１３１，光ディスク１３２，光磁気ディスク１３３、および半導体メモリ１３４、図５のコンテンツ配信サーバ１４のCPU１５１，ROM１５２，RAM１５３，バス１５４，入出力インタフェース１５５，入力部１５６，出力部１５７，記憶部１５８，通信部１５９，ドライブ１６０，磁気ディスク１７１，光ディスク１７２，光磁気ディスク１７３、および半導体メモリ１７４に対応するものであり、同様の機能を有するものである。

但し、記憶部１９８に記憶されているプログラムは、図２の電子チケット管理サーバ１１の記憶部３８、図３のユーザ端末１２の記憶部７８、図４の認証局サーバ１３の記憶部１１８、または図５の記憶部１５８に記憶されているプログラムとは異なる。記憶部１９８は、課金処理管理プログラム１９８ａを記憶しており、CPU１９１は、これらのプログラムを適宜読み出して実行する。さらに、記憶部１９８は、図５には図示しないが、この他にも、基本プログラムであるOS３４１（図１３）や、ドライバ３４２（図１３）も記憶している。尚、各種のプログラムについては、図１３を参照して後述する。

次に、図７の機能ブロック図を参照して、電子チケット管理サーバ１１の機能について説明する。尚、以下の機能ブロック図においては、基本的にソフトウェアにより実現される機能を示しているが、各ソフトウェアと同等の機能を果たす、例えば、チップセットなどからなるハードウェアとして構成するようにしてもよい。

電子チケット管理サーバ１１のCPU３１は、その基本ソフトウェアであるOS３０１を実行させる。OS３０１は、例えば、MicroSoft社のWindows（登録商標）xp、ME、または2000などである。電子チケット管理サーバ１１のCPU３１は、そのOS３０１上で、ドライバ３０２を介して上述の電子チケットデータベース３８ａ、電子チケット管理プログラム３８ｂ、および署名管理プログラム３８ｃを実行させている。

電子チケットデータベース３８ａは、電子チケット管理プログラム３８ｂがコンテンツに対応して電子チケットを発行するとき、電子チケットを識別するチケットID、電子チケットにより配信されるコンテンツを取得するためのアクセス先の情報を示すアクセス情報ID、および、アクセス情報IDに基づいてアクセスした際にアクセス用の認証に用いられるアクセス用暗号鍵の情報をチケット毎に記憶するデータベースである。

電子チケット管理プログラム３８ｂは、図８で示すような電子チケットを発行する。すなわち、図８で示すように、電子チケットは、チケットID、アクセス情報ID、および、電子署名から構成されている。チケットIDは、電子チケットを識別する固有のIDである。アクセス情報IDは、電子チケットにより配信されるコンテンツを取得するためのアクセス先の情報を示すIDであり、例えば、アクセス先となるコンテンツ配信サーバ１４のURL（Universal Resource Locator）などである。また、アクセス情報IDには、各電子チケットのユーザの銀行口座番号やクレジットカード番号を含めるようにすることもできる。

電子署名は、電子チケットを生成するサーバの秘密鍵により、署名対象の情報（ここでは、チケットIDとアクセス情報ID）、あるいは情報をハッシュ関数で

処理した結果であるメッセージダイジェストを暗号化したものである。今の場合、電子チケットは、電子チケット管理サーバ１１により生成されるので、電子チケット管理サーバ１１の秘密鍵Ｋ０により暗号化される。また、電子署名は、生成時に使用した秘密鍵に対応する公開鍵で復号し、署名対象の情報、あるいは同情報のメッセージダイジェストと一致することを確認することで、署名対象の情報が確かに秘密鍵の所有者によって署名されたものであると検証することができる。以後、電子署名の検証とはこのような署名対象情報の確認処理を指すものとする。

さらに、電子チケットは、これ以外の情報を含むようにしても良く、例えば、タイトル名、アーティスト名、アイコン、有効期限などの情報を含むようにしても良い。

電子チケットデータベース３８ａは、例えば、図９で示すように生成された電子チケットの情報がデータベース化されたものであり、電子チケット管理プログラム３８ｂにより生成される。図９の例においては、電子チケットＳ乃至Ｚが記録されている。図中上段からチケット名、チケットID、アクセス情報IDとしてアクセス先URL、および、アクセス用暗号鍵が記録されている。今の場合、チケットＳについては、チケットIDが「T11」、アクセス先URLが「http://aaa.com/」アクセス用暗号鍵が「AA1」とそれぞれ記憶されている。チケットＴについては、チケットIDが「T22」、アクセス先URLが「http://bbb.com/」アクセス用暗号鍵が「BB1」とそれぞれ記憶されている。チケットＵについては、チケットIDが「T33」、アクセス先URLが「http://ccc.com/」アクセス用暗号鍵が「CC1」とそれぞれ記憶されている。チケットＶについては、チケットIDが「T44」、アクセス先URLが「http://ddd.com/」アクセス用暗号鍵が「DD1」とそれぞれ記憶されている。チケットＷについては、チケットIDが「T55」、アクセス先URLが「http://eee.com/」アクセス用暗号鍵が「EE1」とそれぞれ記憶されている。チケットＺについては、チケットIDが「T66」、アクセス先URLが「http://fff.com/」アクセス用暗号鍵が「FF1」とそれぞれ記憶されている。

署名管理プログラム３８ｃは、各種の処理の際に送信されるデータに対して、自らの秘密鍵Ｋ０を用いて電子署名を生成する。また、署名管理プログラム３８ｃは、他のユーザにより添付される電子署名に対応する公開鍵を取得し、その公開鍵で電子署名を復号して、送信されてきたデータが正当なものであるか否かを判定する。

次に、図１０の機能ブロック図を参照して、ユーザ端末１２の機能について説明する。

ユーザ端末１２のCPU７１は、その基本ソフトウェアであるOS３１１を実行させ、そのOS３１１上で、ドライバ３１２を介して上述の電子チケット管理プログラム７８ａ、署名管理プログラム７８ｂ、およびコンテンツ再生プログラム７８ｃを実行させている。

電子チケット管理プログラム７８ａは、ネットワーク１を介して電子チケット管理サーバ１１にアクセスして、電子チケットを購入する処理を実行し、購入したチケットを記憶する。今の場合、電子チケット管理プログラム７８ａが、図９に対応するチケットＳ，Ｔを購入した状態が示されている。電子チケット管理プログラム７８ａは、ユーザによる操作内容に従って、電子チケット管理サーバ１１にアクセスし、電子チケットに対応するコンテンツの配信を受けるのに必要な情報の提供を要求する。このとき、電子チケット管理プログラム７８ａは、要求する電子チケットと共に、署名管理プログラム７８ｂの秘密鍵Ｋ１により生成された電子チケットに対する電子署名を添付して電子チケット管理サーバ１１にアクセスし、電子チケットに対応するコンテンツの配信に必要な情報の提供を要求する。

さらに、電子チケット管理プログラム７８ａは、コンテンツの配信に必要な情報、例えば、アクセス先URLやアクセス用暗号鍵の情報を取得し、これらの情報に基づいて、コンテンツ配信サーバ１４にアクセスし、コンテンツの供給を受け、コンテンツ再生プログラム７８ｃに出力する。コンテンツ再生プログラム７

８ｃは、電子チケット管理プログラム７８ａにより取得されたコンテンツを再生し、出力部７７に出力する。

次に、図１１の機能ブロック図を参照して、認証局サーバ１３の機能について説明する。認証局サーバ１３のCPU１１１は、その基本ソフトウェアであるOS３２１を実行させ、そのOS３２１上で、ドライバ３２２を介して上述の電子証明書発行プログラム１１８ａを実行させている。

電子証明書発行プログラム１１８ａは、所定のユーザ端末１２の公開鍵および／あるいはユーザIDに対して、対応する電子署名を生成および添付し、ユーザ端末１２の電子証明書を生成する。例えば、図１０で示すユーザ端末１２の場合、秘密鍵Ｋ１に対して、公開鍵Ｋ１’（秘密鍵Ｋ１により暗号化された情報を復号する鍵であり、以下においては、秘密鍵の番号に「’」を付して称するものとする）が公開されているので、ユーザ端末１２から電子証明書の作成が要求されると、電子証明書発行プログラム１１８ａは、公開鍵Ｋ１’および／あるいはユーザIDに対して、自らの秘密鍵Ｋ２を用いて電子署名Ｓ１を生成したのち、それを公開鍵Ｋ１’および／あるいはユーザIDに添付して電子証明書を作成してユーザ端末１２に返信し、さらに、秘密鍵Ｋ２に対応する公開鍵（電子証明書検証用公開鍵）Ｋ２’を公開する。ここでユーザIDは、ユーザ端末１２を識別できる情報であり、初めて電子証明書を生成するときに電子証明書発行プログラム１１８ａが割り付ける。一方、ユーザ端末１２は、自らの秘密鍵Ｋ１に対する公開鍵Ｋ１’および／あるいはユーザIDと、電子署名Ｓ１からなる電子証明書を公開する。尚、以下において、公開された情報、例えば、公開鍵などは、ネットワーク１上に接続された物であれば、いずれにおいても取得可能であるものとする。

このような処理により、第３者は、ユーザ端末１２の公開鍵Ｋ１’および／あるいはユーザIDが正当なものであるか否かを判断する時、ユーザ端末１２より公開されている電子証明書を取得して電子署名Ｓ１を抽出し、認証局サーバ１３より公開されている公開鍵Ｋ２を用いて、電子署名Ｓ１が公開鍵Ｋ１’および／あるいはユーザIDと対応するかを検証することにより、ユーザ端末１２から公

開されている公開鍵Ｋ１’および／あるいはユーザIDが正当なものであると判断することができる。

次に、図１２の機能ブロック図を参照して、コンテンツ配信サーバ１４の機能について説明する。コンテンツ配信サーバ１４のCPU１５１は、その基本ソフトウェアであるOS３３１を実行させ、そのOS３３１上で、ドライバ３３２を介して上述のコンテンツ管理プログラム１５８ａおよび署名管理プログラム１５８ｂを実行させている。

コンテンツ管理プログラム１５８ａは、ユーザ端末１２からのアクセス要求に基づいてコンテンツを配信する。より詳細には、コンテンツ管理プログラム１５８ａは、ユーザ端末１２からのアクセスに応じて、所定のコンテンツを配信（供給）する。

署名管理プログラム１５８ｂは、他のユーザにより添付される電子署名に対応する公開鍵を取得し、その公開鍵で電子署名を復号して、送信されてきたデータが正当なものであるか否かを判定する。

次に、図１３の機能ブロック図を参照して、課金サーバ１５の機能について説明する。課金サーバ１５のCPU１９１は、その基本ソフトウェアであるOS３４１を実行させ、そのOS３４１上で、ドライバ３４２を介して上述の課金処理プログラム１９８ａを実行させている。

課金処理プログラム１９８ａは、電子チケット管理サーバ１１からの要求に基づいて、ユーザ端末１２間、または、ユーザ端末１２とコンテンツ配信サーバ１４間で流通する電子チケットの利用にかかる対価の課金処理を実行する。

次に、図１４のフローチャートを参照して、ユーザ端末１２が電子チケット管理サーバ１１から電子チケットを購入する際の処理について説明する。

ステップＳ１において、電子チケット管理プログラム７８ａは、電子チケットの購入が指示されたか否かを判定し、電子チケットの購入が指示されるまでその処理を繰り返す。ステップＳ１において、例えば、ユーザが入力部７６を操作し

て所望の電子チケットの購入を指示したと判定された場合、その処理は、ステップＳ２に進む。

ステップＳ２において、電子チケット管理プログラム７８ａは、通信部７９を制御し、ネットワーク１を介して、電子チケット管理サーバ１１に購入が指示された電子チケットの購入の要求を送信する。

ステップＳ２１において、電子チケット管理サーバ１１の電子チケット管理プログラム３８ｂは、通信部３９を制御して、電子チケットの購入が要求されているか否かを判定し、電子チケットの購入が要求されていると判定されるまで、その処理を繰り返す。例えば、上述のように、ステップＳ２の処理により、ユーザ端末１２の電子チケット管理プログラム７８ａから電子チケットの購入の要求が送信されてきた場合、その処理は、ステップＳ２２に進む。

ステップＳ２２において、電子チケット管理サーバ１１の電子チケット管理プログラム３８ｂは、通信部３９を制御してネットワーク１を介して課金サーバ１５にアクセスし、購入要求のあったユーザ端末１２の口座より電子チケットの対価にかかる課金処理を要求し、実行させる。

ステップＳ４１において、課金処理プログラム１９８ａは、通信部１９９を制御して電子チケットの課金処理が要求されたか否かを判定し、課金の要求があるまでその処理を繰り返す。例えば、ステップＳ２２の処理により、課金処理の要求があると判定された場合、ステップＳ４２において、課金処理プログラム１９８ａは、対応する電子チケットに対する課金処理を実行し、処理結果を電子チケット管理サーバ１１に送付する。

ステップＳ２３において、電子チケット管理サーバ１１の電子チケット管理プログラム３８ｂは、電子チケットの購入希望のあった電子チケットを発行し、通信部３９を制御し、ネットワーク１を介してユーザ端末１２に送信する。より詳細には、電子チケット管理プログラム３８ｂは、図８で示したように、電子チケットのチケットIDと、要求のあったコンテンツを配信するコンテンツ配信サーバ１４のアクセス先を示すアクセス情報IDに対して、署名管理プログラム３８

cに自身の秘密鍵Ｋ０を用いて電子署名を生成させ、これらからなる電子チケットを発行して、ユーザ端末１２に送信する。

ステップＳ３において、電子チケット管理プログラム７８ａは、電子チケット管理サーバ１１より送信されてくる電子チケットを受信し、記憶部７８に記憶させる。

一方、ステップＳ２４において、電子チケット管理サーバ１２の電子チケット管理プログラム３８ｂは、発行した電子チケットのチケットIDとアクセス情報IDを電子チケットデータベース３８ａに登録する。

今の場合、例えば、図１０で示すようにユーザ端末で電子チケットＳ，Ｔが購入されているので、対応する電子チケットの情報が図９で示す電子チケットＳ，Ｔとして登録されることになる。また、この例においては、このように電子チケットが、電子チケットデータベース３８ａに登録されると、その電子チケットは、有効な（使用可能な）電子チケットであるものとして判断される。

次に、図１５のフローチャートを参照して、電子チケットを用いたコンテンツの配信処理を説明する。

ステップＳ８１において、電子チケット管理プログラム７８ａは、コンテンツの配信が要求されたか否かを判定し、コンテンツの配信が要求されるまでその処理を繰り返す。ステップＳ８１において、例えば、ユーザが入力部７６を操作して、図１０中の電子チケットＳに対応するコンテンツの配信を要求した場合、その処理は、ステップＳ８２に進む。

ステップＳ８２において、電子チケット管理プログラム７８ａは、電子チケットＳを電子チケット管理サーバ１１に出力して、電子チケットＳに対応するコンテンツの配信を要求する。

ステップＳ１０１において、電子チケット管理プログラム３８ｂは、コンテンツの配信が要求されたか否かを判定し、コンテンツの配信が要求されるまでその処理を繰り返す。例えば、ステップＳ８２の処理によりコンテンツの配信が要求

された場合、コンテンツの配信の要求があったと判定され、その処理は、ステップＳ１０２に進む。

ステップＳ１０２において、電子チケット管理プログラム３８ｂは、ユーザ端末１２より送信されてきた電子チケットを受信し、さらに、署名管理プログラム３８ｃに電子チケットに対する電子署名を確認させる。

ステップＳ１０３において、署名管理プログラム３８ｂは、電子チケットに対する電子署名が正しいものであるか否かを判定する。より詳細には、署名管理プログラム３８ｃは、電子署名を、公開されている秘密鍵Ｋ０に対応する公開鍵Ｋ０’（今の場合、この電子チケットＳは、電子チケット管理サーバ１１自身で発行しているので、自らが公開している公開鍵Ｋ０’）を取得し、その公開鍵Ｋ０’で電子チケットに対する電子署名を復号し、得られたデータが電子チケットＳと同じ物であるか否かを比較し、例えば、両者が同じ物である時、電子署名が正しいと判断し、その処理は、ステップＳ１０４に進む。

ステップＳ１０４において、電子チケット管理プログラム３８ｂは、ユーザ端末１２から送信されてきた電子チケットが有効なものであるか、すなわち、電子チケットデータベース３８ａに登録された電子チケットであるか否かを判定する。今の場合、電子チケットＳであるので、図９で示すように登録された電子チケットであるので、有効であると判断され、その処理は、ステップＳ１０５に進む。

ステップＳ１０５において、電子チケット管理プログラム３８ｂは、電子チケットデータベース３８ａを読出し、今現在配信の要求のあったコンテンツに対応するコンテンツ配信サーバ１４のアクセスに必要なアクセス用暗号鍵を読み出して、通信部３９を制御してネットワーク１を介してユーザ端末１２に送信する。今の場合、電子チケットＳがユーザ端末１２より送信されてきているので、図９で示すように電子チケットＳに対応するアクセス用暗号鍵「AA1」がユーザ端末１２に送信されることになる。

ステップＳ８３において、電子チケット管理プログラム７８ａは、電子チケット管理サーバ１１よりアクセス用暗号鍵が送信されてきたか否かを判定する。今

の場合、電子チケットＳに対応するアクセス用暗号鍵「AA1」が送信されてきているので、アクセス用暗号鍵が送信されてきたと判定され、その処理は、ステップＳ８４に進む。

ステップＳ８４において、電子チケット管理プログラム７８ａは、電子チケットに含まれているアクセス情報 ID に基づいたコンテンツ配信サーバ１４にアクセスし、コンテンツの配信を要求する。

ステップＳ１２１において、コンテンツ配信サーバ１４のコンテンツ管理プログラム１５８ａは、コンテンツの配信要求があるか否かを判定し、配信の要求があるまでその処理を繰り返す。今の場合、ステップＳ８４の処理によりコンテンツの配信要求があったので、コンテンツの配信要求があったと判定され、その処理は、ステップＳ１２２に進む。

ステップＳ１２２において、コンテンツ管理プログラム１５８ａは、配信要求のあったコンテンツをユーザ端末１２に配信する。なお、正当なユーザ端末１２以外からの不正アクセスを防止するため、ユーザ端末１２はコンテンツへのアクセス用暗号鍵をコンテンツ配信サーバ１４に送り、コンテンツ配信サーバ１４のコンテンツ管理プログラム１５８ａは、ユーザ端末１２より送信されてきたアクセス用暗号鍵が正しいか否かを判定し、正しいと判定された時、ユーザ端末１２を自らにアクセスさせ、配信要求のあったコンテンツをユーザ端末１２に配信するようにすることも考えられる。

ステップＳ８５において、コンテンツ再生プログラム７８ｃは、コンテンツ配信サーバ１４より配信されてきたコンテンツを再生し、出力部７７に出力し、例えば、コンテンツが映画の場合、画像を表示するとともに音声を出力し、また、コンテンツが音楽であった場合、音声を出力する。

ステップＳ１０３において、電子署名が正しく無いと判定された場合、その処理は、ステップＳ１０６に進み、電子チケット管理プログラム３８ｂは、電子署名が無効であることをユーザ端末１２に通知する。

ステップＳ８３において、ステップＳ１０３の処理によりアクセス用暗号鍵が送付されてこないので、その処理は、ステップＳ８６に進み、電子チケット管理プログラム７８ａは、通知内容、すなわち、今の場合、電子署名が正しくなかったことを出力部７７より出力（表示）させる。

ステップＳ１０４において、チケットが有効ではない、すなわち、ユーザ端末１２より送信されてきた電子チケットが、電子チケットデータベース３８ａに登録されたものではなかった場合、その処理は、ステップＳ１０７に進む。

ステップＳ１０７において、電子チケット管理プログラム３８ｂは、電子チケットが無効であることをユーザ端末１２に通知する。

この場合、ステップＳ８３において、電子チケットが無効であることが通知されてくるので、ステップＳ８６において、電子チケットが無効であることが出力される（表示される）。

以上のような処理により、電子署名が付された改ざんが困難な電子チケットを用いて、電子チケットを有するユーザ端末１２だけが、コンテンツ配信サーバ１４にアクセスできるようにすることができ、安全な電子コンテンツの配信を可能とすることができる。尚、ステップＳ１０５の処理において、アクセスに必要なアクセス用暗号鍵の送信方法としては、例えば、ユーザ端末１２から、後述する電子証明書を取得し、その中の公開鍵でアクセス用暗号鍵を暗号化してユーザ端末１２に送付するようにすることで、アクセス用暗号鍵を安全に送付することができる。この方法は、ステップＳ１２２の処理で述べた、ユーザ端末１２からコンテンツ配信サーバ１４への暗号鍵の送信を行う場合にも使える。

次に、電子チケットに利用可能回数を設定した場合のコンテンツ配信システムについて説明する。

図１６は、電子チケットに利用可能回数を設定し、この回数を管理するときの電子チケット管理サーバ１１の構成を示している。尚、図１６において、図２の電子チケット管理サーバ１１における場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。

図１６の電子チケット管理サーバ１１は、図２の電子チケット管理サーバ１１と基本的な構成は同様であるが、記憶部３８に記憶されている電子チケットデータベース３８ａ、および、電子チケット管理プログラム３８ｂに替えて、電子チケットデータベース３８ａ’、および、電子チケット管理プログラム３８ｂ’が記憶されている点が異なる。

電子チケットデータベース３８ａ’は、電子チケットデータベース３８ａと基本的な構造は同様であるが、さらに、利用可能な回数を示す残回数のデータを電子チケット毎に記憶している。

電子チケット管理プログラム３８ｂ’は、電子チケット管理プログラム３８ｂと基本的に同様のものであるが、さらに、上述の電子チケットデータベース３８ａ’に新たに加えられた情報である利用可能回数を示す残回数を、電子チケットが登録される際に記録すると共に、コンテンツの配信要求の度に残回数を１回ずつ減らしていく。

次に、図１７の機能ブロック図を参照して、図１６で示した電子チケット管理サーバ１１の機能について説明する。

基本的な機能は、図７で示した電子チケット管理サーバ１１の機能と同様であるが、電子チケットデータベース３８ａ、および、電子チケット管理プログラム３８ｂに替えて、電子チケットデータベース３８ａ’、および、電子チケット管理プログラム３８ｂ’の機能が設けられている。

電子チケットデータベース３８ａ’は、電子チケットデータベース３８ａと基本的な構造は同様であるが、例えば、図１８で示すように、利用可能な回数を示す残回数のデータを電子チケット毎に記憶している。今の場合、図９で示した電子チケットデータベース３８ａの情報に加えて、残回数が記憶されており、電子チケットＳについては、残回数が１、電子チケットＴについては、残回数が２、電子チケットＵについては、残回数が１０、電子チケットＶについては、残回数が３、電子チケットＷについては、残回数が５、電子チケットＺについては、残回数が１として、それぞれ記憶されている。この残回数は、電子チケット管理プ

ログラム３８ｂ’が、電子チケットを新たに登録する際に記録するものであるが、この回数は、例えば、電子チケットの代金に応じたものとして記録するようにしても良いし、デフォルトの値を決めて常にその回数を入れるようにしても良い。また、電子チケット管理プログラム３８ｂ’は、ユーザ端末１２からコンテンツの配信の要求がある度に、この残回数を更新し（１回ずつ減らし）、最終的に残回数が０となったところで、その電子チケットの情報を削除する。このように電子チケットの情報が削除されることにより、実質的に、その電子チケットは無効とされることになる。

次に、図１９のフローチャートを参照して、電子チケットに利用可能回数を設定した場合の電子チケットの購入処理について説明する。

尚、ステップＳ１４１乃至Ｓ１４３、ステップＳ１５１乃至Ｓ１５３、および、ステップＳ１７１，Ｓ１７２の処理は、図１４のフローチャートを参照して説明したステップＳ１乃至Ｓ３、ステップＳ２１乃至Ｓ２３、およびステップＳ４１，Ｓ４２の処理と同様であるので、その説明は省略する。

ステップＳ１５４において、電子チケット管理サーバ１２の電子チケット管理プログラム３８ｂ’は、発行した電子チケットのチケットIDとアクセス情報IDに加えて、残回数の情報を電子チケットデータベース３８ａ’に登録する。このような処理により、図１８で示すような電子チケットデータベース３８ａ’が生成され、今の場合、電子チケットＳの残回数が「１」として記録されたことになる。

次に、図２０のフローチャートを参照して、電子チケットに利用可能回数を設定した場合のコンテンツ配信処理について説明する。

尚、ステップＳ１９１乃至Ｓ１９６、ステップＳ２１１乃至Ｓ２１４，Ｓ２１８，Ｓ２１９、および、ステップＳ２４１，Ｓ２４２の処理は、図１５のフローチャートを参照して説明したステップＳ８１乃至Ｓ８６、ステップＳ１０１乃至Ｓ１０４，Ｓ１０６，Ｓ１０７、および、ステップＳ１２１，Ｓ１２２の処理と同様であるので、その説明は省略する。

ステップＳ２１５において、電子チケット管理プログラム３８ｂ’は、電子チケットデータベース３８ａ’を読出し、今現在配信の要求のあったコンテンツに対応するコンテンツ配信サーバ１４のアクセスに必要なアクセス用暗号鍵を読み出して、通信部３９を制御してネットワーク１を介してユーザ端末１２に送信すると共に、残回数を１回減らす。

今の場合、電子チケットＳがユーザ端末１２より送信されてきているので、図９で示すように電子チケットＳに対応するアクセス用暗号鍵 AA1 がユーザ端末１２に送信されることになる。また、この処理により、図１８で示すように電子チケットＳの残回数は、１回であったので１回減らされて０回となる。

ステップＳ２１６において、電子チケット管理プログラム３８ｂ’は、そのチケットに残回数があるか、すなわち、まだ、アクセス権が残されているか否かを判定し、残回数が無い場合、その処理は、ステップＳ２１７に進む。

今の場合、電子チケットＳの残回数は、上述のように０回となっているので、残回数はないと判定され、ステップＳ２１７において、電子チケット管理プログラム３８ｂ’は、電子チケットデータベース３８ａ’上の電子チケットＳの情報を削除する。また、ステップＳ２１６において、残回数があると判定された場合、ステップＳ２１７の処理は、スキップされることになる。

以上のような処理により、電子署名が付された改ざんが困難な電子チケットを用いて、電子チケットを有するユーザ端末１２だけが、コンテンツ配信サーバ１４にアクセスできるようにすることができ、安全な電子コンテンツの配信を可能とすることができ、さらに、電子チケットの利用可能回数を考慮した処理を行うことにより、電子チケットの対価に合わせたコンテンツの配信処理を行うことが可能となる。

また、以上の例においては、利用可能回数を残回数として記憶する場合について説明してきたが、それ以外の利用制限について管理するようにしても良く、例えば、利用可能回数だけでなく、コンテンツを最初に利用した時点からの期間などを管理するようにしても良い。

次に、電子チケットが電子チケット管理サーバ１１に登録される際（ユーザ端末１２により電子チケットが購入される際）に、個々のユーザを識別するユーザIDをも登録し、電子チケットの個々の利用者を特定できるようにした場合のコンテンツ配信システムについて説明する。

図２１は、上述のように電子チケットが登録される際に、個々のユーザを識別するユーザIDを登録させるときの電子チケット管理サーバ１１の構成を示している。尚、図２１において、図２、または、図１６の電子チケット管理サーバ１１における場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。

図２１の電子チケット管理サーバ１１は、図１６の電子チケット管理サーバ１１と基本的な構成は同様であるが、記憶部３８に記憶されている電子チケットデータベース３８ａ’、電子チケット管理プログラム３８ｂ’、および、署名管理プログラム３８ｃに替えて、電子チケットデータベース３８ａ’’、電子チケット管理プログラム３８ｂ’’、および、署名管理プログラム３８ｃ’が記憶されている点が異なる。

電子チケットデータベース３８ａ’’は、電子チケットデータベース３８ａ’と基本的な構造は同様であるが、さらに、電子チケットを所有するユーザを識別するユーザIDの情報を電子チケット毎に記憶している。

電子チケット管理プログラム３８ｂ’’は、電子チケット管理プログラム３８ｂ’と基本的に同様のものであるが、さらに、上述の電子チケットデータベース３８ａ’’に新たに加えられた情報であるユーザIDの情報を、電子チケットが登録される際に記録する。

署名管理プログラム３８ｃ’は、署名管理プログラム３８ｃと基本的に同様のものであるが、さらに、認証局サーバ１３により発行される電子証明書に対応する電子証明書確認用の公開鍵をネットワーク１上から取得し、電子証明書に含まれる公開鍵とユーザIDの正当性を、それらに対する電子署名を検証することで確認する。

図２２は、上述のように電子チケットが登録される際に、個々のユーザを識別するユーザIDを登録させるときのユーザ端末１２の構成を示している。尚、図２２において、図３のユーザ端末１２における場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。

図２２のユーザ端末１２は、図３のユーザ端末１２と基本的な構成は同様であるが、記憶部７８に記憶されている電子チケット管理プログラム７８ａ、および、署名管理プログラム７８ｂに替えて、電子チケット管理プログラム７８ａ’、および、署名管理プログラム７８ｂ’が記憶されている点が異なる。

電子チケット管理プログラム７８ａ’は、図３の電子チケット管理プログラム７８と基本的には同様のものであるが、さらに、電子チケットを購入する際、ユーザIDの情報も電子チケット管理サーバ１１に送付する。

署名管理プログラム７８ｂ’は、図３の署名管理プログラム７８ｂと基本的には、同様のものであるが、さらに、電子チケットを購入する際、または、電子チケットを使用してコンテンツの配信を要求する際に、予め電子証明書を認証局サーバ１３から取得し、これを添付する。

次に、図２３の機能ブロック図を参照して、図２１の電子チケット管理サーバ１１の機能について説明する。

電子チケットデータベース３８’’は、図１８の電子チケットデータベース３８ａ’と基本的な構造は同様であるが、図２４で示すように、さらに、電子チケットを所有するユーザを識別するユーザIDの情報を電子チケット毎に記憶している。すなわち、図２４の場合、電子チケットＳには、ユーザIDとして「１１１」が、電子チケットＴには、ユーザIDとして「２２２」が、電子チケットＵには、ユーザIDとして「３３３」が、電子チケットＶには、ユーザIDとして「４４４」が、電子チケットＷには、ユーザIDとして「５５５」が、電子チケットＺには、ユーザIDとして「６６６」が、記憶されている。

電子チケット管理プログラム３８ｂ’’は、電子チケット管理プログラム３８ｂ’と基本的に同様のものであるが、さらに、上述の電子チケットデータベース

３８ａ’’に新たに加えられた情報であるユーザIDの情報を、電子チケットが登録される際に記録する。また、署名管理プログラム３８ｃ’に対して電子証明書の確認処理を行う際に、電子チケットデータベース３８ａ’’にアクセスして、電子チケットのチケットIDに対応するユーザIDを読み出す。

署名管理プログラム３８ｃ’は、署名管理プログラム３８ｃと基本的に同様のものであるが、さらに、認証局サーバ１３により発行される電子証明書に対応する電子証明書確認用の公開鍵をネットワーク１上から取得し、ユーザ端末１２より電子チケットと共に送付されてくる電子証明書に含まれる公開鍵とユーザIDの正当性を、それらに対する電子署名を検証することで確認する。

次に、図２５の機能ブロック図を参照して、図２２のユーザ端末１２により実現されるユーザ端末１２の機能について説明する。

図２５のユーザ端末１２の基本的な機能は、図１０で示したユーザ端末１２の機能と同様であるが、電子チケット管理プログラム７８ａ、および、署名管理プログラム７８ｂに替えて、電子チケット管理プログラム７８ａ’、および、署名管理プログラム７８ｂ’の機能が設けられている。

電子チケット管理プログラム７８ａ’は、電子チケット管理プログラム７８ａと基本的な構造は同様であるが、さらに、上述のように電子チケットを購入する際に、これまでの情報に加えてユーザIDを付加して、電子チケット管理サーバ１１に送信する。

署名管理プログラム７８ｂ’は、図２５で示すように、これまでの秘密鍵Ｋ１に加えて、電子証明書３１３を予め認証局サーバ１３より取得し、記憶部７８に記憶させておいて、電子チケットを利用して、コンテンツの配信を受ける際に添付して電子チケット管理サーバ１１に送信する。

より詳細には、電子チケット管理プログラム７８ａ’が電子チケットを電子チケット管理サーバ１１に送付して、コンテンツの配信を要求する場合、署名管理プログラム７８ｂ’は、送付する電子チケットに対する、自らの秘密鍵Ｋ１による電子署名を生成して、図２６で示すように電子チケットに添付する。さらに、

署名管理プログラム７８ｂ’は、図２６のような形式にされた電子チケットに電子証明書を添付し、これを電子チケット管理プログラム７８ａ’が、電子チケット管理サーバ１１に送信する。

次に、図２７のフローチャートを参照して、ユーザIDをも登録させて、電子チケットを購入する際の処理について説明する。

尚、ステップＳ２６１，Ｓ２６３、ステップＳ２８１乃至Ｓ２８３、および、ステップＳ３０１，Ｓ３０２の処理は、図１９のステップＳ１４１，Ｓ１４３、ステップＳ１５１乃至Ｓ１５３、および、ステップＳ１７１，Ｓ１７２の処理と同様であるので、その処理の説明は省略する。

ステップＳ２６２において、電子チケット管理プログラム７８ａ’は、電子チケット管理サーバ１１に電子チケットの購入を要求すると共に、ユーザを識別するユーザIDを送付する。

ステップＳ２８４において、電子チケット管理サーバ１２の電子チケット管理プログラム３８ｂ’’は、発行した電子チケットのチケットIDとアクセス情報IDに加えて、残回数の情報と、さらに、ユーザ端末１２より送信されてきたユーザIDを電子チケットデータベース３８ａ’’に登録する。このような処理により、図２４で示すような電子チケットデータベース３８ａ’が生成され、今の場合、電子チケットＳの残回数が「１」として記録され、さらに、ユーザIDとして「１１１」が記録されたことになる。

次に、図２８，図２９のフローチャートを参照して、電子チケットが電子チケット管理サーバ１１に登録される際（ユーザ端末１２により電子チケットが購入される際）に、個々のユーザを識別するユーザIDをも登録し、電子チケットの個々の利用者を特定できるようにした場合のコンテンツ配信システムにおけるコンテンツ配信処理について説明する。

尚、図２８，図２９のフローチャートにおいて、ステップＳ３２１，Ｓ３２３乃至Ｓ３２６の処理、ステップＳ３４１，Ｓ３５０乃至Ｓ３５３，Ｓ３５５の処理、およびステップＳ３７１，Ｓ３７２の処理は、図２０のフローチャートを参

照して説明したステップＳ１９１，Ｓ１９３乃至Ｓ１９６の処理、ステップＳ２１１，Ｓ２１４乃至Ｓ２１７，Ｓ２１９の処理、および、ステップＳ２４１乃至Ｓ２４２の処理と同様であるので、その処理の説明は省略する。

ステップＳ３２２において、ユーザ端末１２の電子チケット管理プログラム７８ａ’は、電子チケットに、その電子署名と、電子証明書３１３を添付して電子チケット管理サーバ１１に送付して、コンテンツの配信を要求する。より詳細には、電子チケット管理プログラム７８ａ’は、今の場合、電子チケットＳを署名管理プログラム７８ｂ’に出力して、秘密鍵Ｋ１を用いて電子署名を生成し、電子チケットＳに添付する。さらに、電子チケット管理プログラム７８ａ’は、署名管理プログラム７８ｂ’に対して、電子署名が添付された電子チケットＳに電子証明書を添付させ、電子チケットＳ、電子署名、および、電子証明書からなる情報を電子チケット管理サーバ１１に送信すると共に、コンテンツの配信を要求する。

ステップＳ３４２において、電子チケット管理サーバ１１の電子チケット管理プログラム３８ｂ’’は、署名つき電子チケットと、電子証明書３１３を受信して、まず、署名管理プログラム３８ｃ’に電子証明書３１３の電子署名の確認をさせる。すなわち、電子証明書３１３は、認証局サーバ１３により予め生成されたものであり、認証局サーバ１３から、この電子証明書に対応する電子証明書確認用の公開鍵が公開されている。そこで、電子チケット管理サーバ１１は、署名管理プログラム３８ｃ’に、公開されている電子証明書確認用の公開鍵を認証局サーバ１３から取得し、この電子証明書確認用の公開鍵で電子証明書を検証させる。すると、電子証明書の検証結果として、ユーザ ID３１３ａと公開鍵Ｋ１’が、それらに対する電子署名と対応する正当なものかどうかが確認できる。

ステップＳ３４３において、署名管理プログラム３８ｃ’は、電子証明書に含まれていたユーザ ID３１３ａ公開鍵Ｋ１’がそれらに対する電子署名と対応するかを判定し、対応する時、それらユーザ ID と公開鍵が正当なものであるとみなし、その処理は、ステップＳ３４４に進む。

ステップＳ３４４において、署名管理プログラム３８ｃ’は、電子証明書に含まれていた公開鍵を用いて、電子チケットに添付されている電子署名（図２６）を確認する。すなわち、今の場合、電子チケットＳが送付されてきており、その電子チケットＳに添付された電子署名は、ユーザ端末１２の署名管理プログラム７８ｂ’の秘密鍵Ｋ１により電子チケットＳに対して付与されたものである。そこで、署名管理プログラム３８ｃ’は、電子証明書に含まれていた公開鍵Ｋ１’を用いて、電子チケットＳとそれに添付された電子書名が対応するものであるかを確認する。

ステップＳ３４５において、署名管理プログラム３８ｃ’は、ユーザの電子署名は、正当なものであるか否かを判定する。すなわち、署名管理プログラム３８ｃ’は、送信されてきた電子チケットＳと、それに添付された電子書名が対応することを確認した時、確かに電子証明書に含まれるユーザ ID のユーザによる電子署名であると判断し、その処理は、ステップＳ３４６に進む。

ステップＳ３４６において、署名管理プログラム３８ｂ’’は、電子チケットの電子署名（図８）を確認する。すなわち、署名管理プログラム３８ｂ’’は、電子チケットが発行された時に発行元で生成された電子署名を確認する。すなわち、今の場合、電子チケットＳは、電子チケット管理サーバ１１が自らで発行したものであるので、電子チケットを発行したときに使用した秘密鍵Ｋ０に対応する公開鍵Ｋ０’を読出し（他のサーバで発行されたものであれば、その他のサーバで公開している公開鍵を読出し）、その公開鍵Ｋ０’で電子チケットの電子署名が、チケット ID、および、アクセス情報 ID に対するものであるかを検証する。

ステップＳ３４７において、署名管理プログラム３８ｂ’’は、この電子署名が、電子チケットＳのチケット ID、および、アクセス情報 ID に対するものだと確認した場合、その電子チケットは正当なものであるとみなし、その処理は、ステップＳ３４８に進む。

ステップＳ３４８において、電子チケット管理プログラム３８ｂ’’は、電子チケットに含まれているチケットIDを読み出し、電子チケットデータベース３８ａ’’と照合して、対応するユーザIDを読み出す。

ステップＳ３４９において、電子チケット管理プログラム３８ｂ’’は、電子チケットに含まれていたユーザIDと、チケットIDに基づいて、電子チケットデータベース３８ａ’’に登録されたユーザIDとが一致するか否かを判定し、例えば、一致するとき、コンテンツの配信を要求してきたユーザ端末１２の所有者が、電子チケットデータベース３８ａ’’に登録された正規のユーザであるとみなし、その処理は、ステップＳ３５０の処理（図２９）に進み、それ以降の処理が繰り返される。

ステップＳ３４３において、電子証明書に含まれるユーザIDが不正である場合、ステップＳ３４５において、ユーザの電子署名が不正である場合、ステップＳ３４７において、電子チケットの電子署名が不正なものである場合、および、ステップＳ３４９において、電子チケットに含まれていたユーザIDが、電子チケットデータベース３８ａ’’に登録されたユーザIDでは無い場合、いずれにおいても、その処理は、ステップＳ３５４の処理に進み、電子チケットが使用不能であることが通知される。

以上のような処理により、電子署名が付された改ざんが困難な電子チケットを用いて、電子チケットを有するユーザ端末１２だけが、コンテンツ配信サーバ１４にアクセスできるようにすることができ、安全な電子コンテンツの配信をと可能とすることができ、さらに、電子チケットの利用可能回数を考慮した処理を行うことにより、電子チケットの対価に合わせたコンテンツの配信処理を行うことが可能となる。さらに、電子証明書、電子署名、および、ユーザIDから、コンテンツの配信を要求したユーザが、正規のユーザであることを確認したうえでコンテンツを配信することができるので、いわゆる、なりすましによる不正なコンテンツの配信を防止することが可能となる。

以上のような、構成によりユーザを特定して、正規のユーザだけがコンテンツの配信を受けることができるので、ユーザの登録を変更することで、電子チケットの権利を譲渡するようなことができる。

そこで、次に、電子チケットの権利を他のユーザに譲渡することが可能となるコンテンツ配信システムについて説明する。

図３０は、上述のように電子チケットの権利を他のユーザに譲渡することが可能となるコンテンツ配信システムにおける電子チケット管理サーバ１１の構成を示している。尚、図３０において、図２、図１６、または、図２１の電子チケット管理サーバ１１における場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。

図３０の電子チケット管理サーバ１１は、図２１の電子チケット管理サーバ１１と基本的な構成は同様であるが、記憶部３８に記憶されている電子チケット管理プログラム３８ｂ’’、および、署名管理プログラム３８ｃ’に替えて、電子チケット管理プログラム３８ｂ’’’、および、署名管理プログラム３８ｃ’’が記憶されている点が異なる。

図３１は、上述のように電子チケットの権利を他のユーザに譲渡することが可能となるコンテンツ配信システムにおけるユーザ端末１２の構成を示している。尚、図３１において、図３、または、図２２のユーザ端末１２における場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。

図３１のユーザ端末１２は、図２２のユーザ端末１２と基本的な構成は同様であるが、記憶部７８に記憶されている電子チケット管理プログラム７８ａ’、および、署名管理プログラム７８ｂ’に替えて、電子チケット管理プログラム７８ａ’’、および、署名管理プログラム７８ｂ’’が記憶されている点が異なる。

次に、図３２の機能ブロック図を参照して、図３０の電子チケット管理サーバ１１の機能について説明する。

電子チケット管理プログラム３８ｂ’’’は、電子チケット管理プログラム３８ｂ’’と基本的に同様のものであるが、さらに、電子チケットの移動元のユーザより入力される電子チケットの移動先と、移動元の情報に基づいて、電子チケットデータベース３８ａ’’の内容を更新する。

署名管理プログラム３８ｃ’’は、移動先となるユーザ端末１２からの電子チケットおよびそれに付随する電子署名と電子証明書を、それぞれの公開鍵を用いて復号し、正規の電子署名、または、電子証明書であることを確認する。

次に、図３３の機能ブロック図を参照して、図３１のユーザ端末１２の機能について説明する。

電子チケット管理プログラム７８ａ’’は、図２２の電子チケット管理プログラム７８と基本的には同様のものであるが、さらに、電子チケットを他のユーザに譲渡する（電子チケットの権利を移動させる）処理を実行する。

すなわち、電子チケット管理プログラム７８ａ’’は、電子チケットの移動元となるユーザが使用する場合、ユーザによる入力部７６の操作内容に対応して入力された情報に従って、電子チケットの移動先のユーザIDと移動させる電子チケットの代金を署名管理プログラム７８ｂ’’に出力して、電子署名付きの情報にさせた後、さらに、電子証明書を添付して、電子チケットの移動先となるユーザ端末１２に送付する。

また、電子チケット管理プログラム７８ａ’’は、電子チケットの移動先となるユーザによって操作される場合、移動元となるユーザ端末１２からの電子証明書が添付された電子署名付きの電子チケットを受信すると共に、移動先のユーザによる入力部７６の操作内容に対応して入力された情報に従って、電子チケットの代金を署名管理プログラム７８ｂ’’に出力して、受信した電子チケットの情報に移動先のユーザ端末１２の電子署名を付けた後、さらに、電子証明書を添付して、電子チケット管理サーバ１１に送付する。

署名管理プログラム７８ｂ’’は、図２２の署名管理プログラム７８ｂ’と基本的には、同様のものであるが、さらに、電子チケットの移動元となるユーザ端

末１２においては、移動先のユーザIDと移動元ユーザによる電子チケットの指定代金の情報に電子署名を付加すると共に、電子証明書を添付する。また、署名管理プログラム７８ｂ’’は、電子チケットの移動先となるユーザ端末１２においては、移動元のユーザ端末１２より送付されてきた電子署名付きの情報に移動先のユーザによる指定代金の情報を付加して、電子署名を付加すると共に、電子証明書を添付する。

次に、図３４のフローチャートを参照して、電子チケットの移動元となるユーザ端末１２－１による電子チケットの移動処理について説明する。尚、以下の説明においては、移動元のユーザ端末１２－１、移動先のユーザのユーザ端末１２－２と称する。また、秘密鍵Ｋ１、公開鍵Ｋ１’、電子証明書３１３、ユーザID３１３ａ、電子チケット管理プログラム７８ａ’’、および、署名管理プログラム７８ｂ’’においても、移動元のユーザ端末１２－１のものには、「－１」を、移動先のユーザ端末１２－２のものには「－２」を付する。

ステップＳ４０１において、電子チケット管理プログラム７８ａ’’－１は、他のユーザへの電子チケットの移動が要求されたか否かを判定し、他のユーザへの電子チケットの移動が要求されるまでその処理を繰り返す。ステップＳ４０１において、例えば、電子チケットＳの移動が要求されると、その処理は、ステップＳ４０２に進む。

ステップＳ４０２において、電子チケット管理プログラム７８ａ’’－１は、移動先となるユーザID３１３－２が入力されたか否かを判定し、入力されるまでその処理を繰り返す。ステップＳ４０２において、移動先となるユーザIDが入力されるとその処理は、ステップＳ４０３に進む。

ステップＳ４０３において、電子チケット管理プログラム７８ａ’’－１は、移動元ユーザによる電子チケットの指定代金が入力されたか否かを判定し、移動元ユーザによる指定代金が入力されるまでその処理を繰り返す。例えば、ステップＳ４０３において、移動元ユーザにより電子チケットの指定代金が入力されるとその処理はステップＳ４０４に進む。

ステップＳ４０４において、電子チケット管理プログラム７８ａ’’－１は、署名管理プログラム７８ｂ’’－１を制御して、図３５で示すように、電子チケット、移動先のユーザ、移動元の指定代金の情報に、それらに対する電子署名を秘密鍵Ｋ１－１により生成および添付し、さらに、移動元の電子証明書３１３を添付して、移動先のユーザの所有するユーザ端末１２－２に移動通知として送付する。

ここで、図３６のフローチャートを参照して、電子チケットの移動先のユーザの所有するユーザ端末１２－２による電子チケットの移動処理について説明する。

ステップＳ４２１において、電子チケット管理プログラム７８ａ’’－２は、電子チケットの移動通知が送付されてきたか否かを判定し、移動通知が送付されてくるまでその処理を繰り返す。例えば、図３４のフローチャート中のステップＳ４０４の処理により、移動通知が送付されてきた場合、その処理は、ステップＳ４２２に進む。

ステップＳ４２２において、電子チケット管理プログラム７８ａ’－２’は、電子チケットの移動が承認されたか、すなわち、他のユーザからの電子チケットの譲渡を受けるか否かをユーザが判定し、例えば、ユーザ端末１２－２のユーザが、ユーザ端末１２－１のユーザからの電子チケットの譲渡を受ける、すなわち、移動が承認された場合、その処理は、ステップＳ４２３に進む。

ステップＳ４２３において、電子チケット管理プログラム７８ａ’’－２は、移動通知を受信し、署名管理プログラム７８ｂ’’－２を制御して、移動元ユーザの電子証明書を検証させる。すなわち、署名管理プログラム７８ｂ’’－２は、電子チケット管理プログラム７８ａ’’－２に制御され、移動通知に含まれていた移動元ユーザの電子証明書３１３－１を、認証局サーバ１３により発行されて公開されている電子証明書３１３－１を確認するための公開鍵を取得および使用し、電子証明書３１３－１に含まれている移動元ユーザの公開鍵Ｋ１’－１と、移動元ユーザのユーザＩＤ３１３ａ－１が、それらに対する電子署名と対応するか確認する。

ステップＳ４２４において、署名管理プログラム７８ｂ’’－２は、電子証明書３１３－１に含まれている移動元ユーザの公開鍵Ｋ１’－１と、移動元ユーザのユーザ ID３１３ａ－１が、正当なものか否かを判定する。ステップＳ４２４において、電子証明書３１３－１に含まれている移動元ユーザの公開鍵Ｋ１’－１と、移動元ユーザのユーザ ID３１３ａ－１が正当と判定された場合、移動元の電子証明書が正規のものであると判定し、その処理は、ステップＳ４２５に進む。

ステップＳ４２５において、署名管理プログラム７８ｂ’’－２は、電子証明書に含まれている移動元のユーザ端末１２－１の公開鍵Ｋ１’－１を使って移動元による電子署名が、電子署名の対象である電子チケット、移動先のユーザ ID、および、移動元の指定代金の情報と対応するかを確認する。

ステップＳ４２６において、署名管理プログラム７８ｂ’’－２は、移動通知に含まれていた移動元ユーザの電子署名が正規のものか、すなわち、移動通知に含まれていた電子チケット、移動先のユーザ ID、および、移動元の指定代金の情報が、移動元ユーザの電子署名と対応するか否かを判定し、対応したと判定された場合、その移動通知が確かにユーザ ID３１３ａ－１のユーザから送られたものだと判定し、その処理は、ステップＳ４２７に進む。

ステップＳ４２７において、署名管理プログラム７８ｂ’’－２は、移動先のユーザ ID３１３ａ－２を、自らのユーザ ID３１３ａ－２とを比較して確認する。ステップＳ４２８において、署名管理プログラム７８ｂ’’－２は、移動先のユーザ ID３１３ａ－２が、自らのユーザ ID３１３ａ－２と一致するか否かを判定し、例えば、一致すると判定された場合、移動先のユーザが、自らであるとみなし、その処理は、ステップＳ４２９に進む。

ステップＳ４２９（図３７）において、署名管理プログラム７８ｂ’’－２は、電子チケットに含まれる電子チケットを発行したサーバの電子署名を確認する。すなわち、署名管理プログラム７８ｂ’’－２は、電子チケットＳを発行した電

子チケット管理サーバ１１により公開されている公開鍵を取得し、電子署名が、署名対象の電子チケット情報と対応するかを検証する。

ステップＳ４３０において、署名管理プログラム７８ｂ’’－２は、電子チケットが正規のものであるか否かを判定する。すなわち、署名管理プログラム７８ｂ’’－２は、電子署名が電子チケット情報に対応したか否かを判定し、例えば、対応したと判定された場合、その処理は、ステップＳ４３１に進む。

ステップＳ４３１において、電子チケット管理プログラム７８ａ’’－２は、移動先のユーザからの電子チケットの代金が別途指定されたか否かを判定し、例えば、移動先のユーザから別途代金の指定がされなかった場合、その処理は、ステップＳ４３２に進む。

ステップＳ４３２において、電子チケット管理プログラム７８ａ’’－２は、移動元ユーザの指定代金を移動先ユーザの指定代金に設定する。

ステップＳ４３３において、電子チケット管理プログラム７８ａ’’－２は、署名管理プログラム７８ｂ’’－２を制御して、図３８で示すように、移動元ユーザからの電子チケット、移動先ユーザのユーザ ID、移動元ユーザの指定代金、移動元ユーザの電子署名、移動先ユーザの指定代金の情報に対して、秘密鍵Ｋ１－２により移動先ユーザの電子署名を生成させる。

ステップＳ４３４において、電子チケット管理プログラム７８ａ’’－２は、移動元ユーザからの電子チケット、移動先ユーザのユーザ ID、移動元ユーザの指定代金、移動元ユーザの電子署名、移動先ユーザの指定代金の情報と、それらに対する移動先ユーザの電子署名を、電子チケットの移動通知として電子チケット管理サーバ１１に送信する。

ステップＳ４３１において、移動先ユーザにより別途電子チケットの指定代金が入力された場合、ステップＳ４３５において、電子チケット管理プログラム７８ａ’’－２は、別途入力された指定代金を移動先ユーザの指定代金として設定する。

ステップＳ４２４において、移動元ユーザの電子証明書が正規のものではないと判定された場合、ステップＳ４２６において、移動元ユーザの電子署名が正規のものではない場合、ステップＳ４２８において、指定された移動先ユーザのユーザIDが自らのユーザIDではなかった場合、または、ステップＳ４３０において、電子チケットの電子署名が正規のものではなかった場合、ステップＳ４３６において、電子チケット管理プログラム７８ａ’’－２は、電子チケットが使用不能、すなわち、移動通知の情報が正規のものではないことを移動先ユーザに通知する。

ステップＳ４２２において、移動が承認されなかった場合、ステップＳ４３７において、電子チケット管理プログラム７８ａ’’－２は、電子チケットが不要である、すなわち、電子チケットの移動が認められなかったことを移動元ユーザの所有するユーザ端末１２－１に通知する。

ここで、図３４のフローチャートの説明に戻る。

ステップＳ４０５において、移動元ユーザのユーザ端末１２－１の電子チケット管理プログラム７８ａ’’－１は、通知を受信したか否かを判定し、通知を受信するまでその処理を繰り返す。例えば、図３７のステップＳ４３７の処理により、電子チケットが不要であることを示す通知が送信され、これが受信された場合、その処理は、ステップＳ４０６に進む。

ステップＳ４０６において、電子チケット管理プログラム７８ａ’’－１は、受信した通知内容を表示する。すなわち、今の場合、移動先ユーザが電子チケットを不要であった旨の表示がなされ、電子チケットの移動が行われなかったことが移動元のユーザに通知される。

次に、図３９，図４０のフローチャートを参照して、図３７のフローチャートにおいて、ステップＳ４３４の処理で、電子チケット管理プログラム７８ａ’’－２により、移動元ユーザからの電子チケット、移動先ユーザのユーザID、移動元ユーザの指定代金、移動元ユーザの電子署名、移動先ユーザの指定代金の情報と、それらの電子署名からなる移動通知が電子チケット管理サーバ１１に送信

された場合の電子チケット管理サーバ１１の電子チケットの移動処理について説明する。

ステップＳ４５１において、電子チケット管理プログラム３８ｂ’’’は、電子チケットの移動通知が送付されてきたか否かを判定し、電子チケットの移動通知が送付されてくるまでその処理を繰り返す。例えば、図３７のフローチャートのステップＳ４３４の処理により、電子チケットの移動先ユーザのユーザ端末１２－２より電子チケットの移動通知が送付されてくると、その処理は、ステップＳ４５２に進む。

ステップＳ４５２において、電子チケット管理プログラム３８ｂ’’’は、移動通知を受信し、そこに含まれている移動元ユーザの電子証明書を検証する。すなわち、電子チケット管理プログラム３８ｂ’’’は、署名管理プログラム３８ｃ’’を制御して、移動通知に含まれている移動元ユーザの電子証明書に対応する認証局サーバ１３により公開されている電子証明書確認用の公開鍵を取得し、それを用いて、電子証明書に含まれる移動元ユーザのユーザIDと公開鍵Ｋ１’－１の情報が、それらに対する電子署名と対応するかを確認させる。

ステップＳ４５３において、署名管理プログラム３８ｃ’’は、移動元ユーザの電子証明書が正規のものであるか否かを判定し、その電子証明書に含まれる移動元ユーザのユーザIDと公開鍵Ｋ１’－１の情報が、それらに対する電子署名と対応した場合、その電子証明書が正規のものであるとみなし、その処理は、ステップＳ４５４に進む。

ステップＳ４５４において、署名管理プログラム３８ｃ’’は、移動元ユーザの電子証明書を確認した方法と同様の方法で、移動先ユーザの電子証明書を確認する。ステップＳ４５５において、署名管理プログラム３８ｃ’’は、ステップＳ４５３における移動元のユーザの電子証明書と同様の方法で、移動先ユーザの電子証明書が正規のものであるか否かを判定し、正規のものであると判定された場合、その処理は、ステップＳ４５６に進む。

ステップＳ４５６において、署名管理プログラム３８ｃ’’は、移動元ユーザによる電子署名を、移動元ユーザの電子証明書に含まれている公開鍵Ｋ１’－１で検証する。すなわち、署名管理プログラム３８ｃ’’は、移動元ユーザの電子証明書に含まれていた公開鍵Ｋ１’－１を用いて、移動元ユーザの電子署名が、署名対象の情報である電子チケット、移動先のユーザ ID、移動元の指定代金と対応するかを確認する。

ステップＳ４５７において、署名管理プログラム３８ｃ’’は、移動元ユーザによる電子署名が正規なものであるか否か、すなわち、移動元ユーザによる電子署名が、署名対象の情報である電子チケット、移動先のユーザ ID、移動元の指定代金と対応するか否かを判定する。ステップＳ４５７において、例えば、移動元ユーザによる電子署名と署名対象の情報が対応する場合、署名管理プログラム３８ｃ’’は、移動元ユーザによる電子署名が正規のものであるとみなし、その処理は、ステップＳ４５８に進む。

ステップＳ４５８において、署名管理プログラム３８ｃ’’は、ステップＳ４５６における処理と同様に方法で、移動先ユーザによる電子署名を、移動先ユーザの電子証明書に含まれている公開鍵Ｋ１’－２で検証する。

ステップＳ４５９において、署名管理プログラム３８ｃ’’は、ステップＳ４５７における処理と同様に方法で、移動先ユーザによる電子署名が、正規のものであるか否かを判定し、例えば、正規のものであると判定された場合、その処理は、ステップＳ４６０に進む。

ステップＳ４６０において、署名管理プログラム３８ｃ’’は、電子チケットの電子署名を確認する。すなわち、署名管理プログラム３８ｃ’’は、電子チケットの電子署名を、電子チケットを発行したサーバが公開する公開鍵を用いて、署名対象の情報であるチケット ID およびアクセス情報 ID と対応するか確認する。今の場合、電子チケットＳは、電子チケット管理サーバ１１自身により発行されているので、自らの公開鍵Ｋ０’により電子チケットの電子署名が検証される。

ステップＳ４６１において、署名管理プログラム３８ｃ’’は、電子チケットの電子署名が正規のものであるかを確認する。すなわち、署名管理プログラム３８ｃ’’は、電子署名が、署名対象の情報であるチケットIDとアクセス情報IDと対応するか否かを判定する。例えば、電子署名が、署名対象の情報であるチケットIDおよびアクセス情報IDと対応すると判定された場合、すなわち、電子チケットの署名が正規のものであると判定された場合、その処理は、ステップＳ４６２に進む。

ステップＳ４６２において、電子チケット管理プログラム３８ｂ’’’は、電子チケットのチケットIDに基づいて、電子チケットデータベース３８ａ’’を照合し、登録されている電子チケットＳのユーザIDを取得する。

ステップＳ４６３において、電子チケット管理プログラム３８ｂ’’’は、電子チケットの移動元のユーザのユーザIDと、電子チケットデータベース３８ａ’’に登録されたユーザIDとが一致するか否かを判定し、例えば、同じであると判定された場合、その処理は、ステップＳ４６４に進む。

ステップＳ４６４において、電子チケット管理プログラム３８ｂ’’’は、チケットIDから、電子チケットが今現在有効であるか否かを判定する。すなわち、電子チケット管理プログラム３８ｂ’’’は、電子チケットデータベース３８ａ’’に登録された情報から、例えば、残回数を確認し電子チケットが有効であるか否かを判定し、例えば、電子チケットが有効であると判定された場合、その処理は、ステップＳ４６５に進む。

ステップＳ４６５において、電子チケット管理プログラム３８ｂ’’’は、移動先ユーザの指定代金が移動元ユーザの指定代金以上であるか否かを判定し、例えば、移動先ユーザの指定代金が移動元ユーザの指定代金以上であると判定した場合、すなわち、移動元ユーザと移動先ユーザ間で代金の折り合いがついていると判定し、その処理は、ステップＳ４６６に進む。

ステップＳ４６６において、電子チケット管理プログラム３８ｂ’’’は、移動先ユーザの指定代金を移動先ユーザの口座から徴収し、移動元ユーザの口座に移すように課金サーバ１５に処理を要求する。

ここで、図４１のフローチャートを参照して、課金サーバ１５の処理について説明する。尚、図４１のステップＳ４８１，Ｓ４８２の処理は、図１４のステップＳ４１，Ｓ４２の処理と同様であるので、その処理の説明は省略する。

ここで、図４０のフローチャートの説明に戻る。

ステップＳ４６７において、電子チケット管理プログラム３８ｂ’’’は、電子チケットデータベースにアクセスし、電子チケットのチケットIDと共に組み合わせて登録されているユーザIDを移動元のユーザIDから移動先のユーザIDに変更し、更に移動元ユーザ端末１２－１に結果を通知する。

ステップＳ４５３において、移動元ユーザの電子証明書が正規ではないと判定された場合、ステップＳ４５５において、移動先ユーザの電子証明書が正規ではないと判定された場合、ステップＳ４５７において、移動元ユーザの電子署名が正規ではないと判定された場合、ステップＳ４５９において、移動先ユーザの電子署名が正規ではないと判定された場合、ステップＳ４６１において、電子チケットの電子署名が正規のものではないと判定された場合、ステップＳ４６３において、電子チケットに含まれているチケットIDと、電子チケットデータベース３８ａ’’に登録された電子チケットのチケットIDとが一致しない場合、ステップＳ４６４において、チケットが有効ではない場合、ステップＳ４６５において、移動先ユーザの指定代金が移動元ユーザの指定代金以上ではない場合、ステップＳ４６８において、電子チケット管理プログラム３８ｂ’’’は、電子チケットの移動が不能であることを移動元ユーザのユーザ端末１２－１に通知する。

尚、以上の例において、電子チケットの所有者（電子チケットデータベースのユーザIDが登録されたユーザ）は、特定のユーザであることを前提に説明してきたが、電子チケットの所有者は、特定のユーザのみならず、例えば、グループなどとしてもよく、複数のユーザであってもよいし、さらには、無制限といった

設定にするようにしても良い。従って、電子チケットの所有者の移動においても、特定のユーザから複数のグループや、無制限といったように移動させることも可能である。

また、ユーザの電子署名付きの電子チケットと、電子証明書のセットは、第３者により盗聴されると、いわゆるなりすましにより不正な使用が可能となることが考えられる。この場合、ユーザ端末１２でも利用可能回数（残回数）のカウンタを持ち、電子チケットを利用する度にカウンタを変化させ、このカウンタの値を電子署名付きの電子チケットと、電子証明書のセットに含ませるようにすることで、電子チケット管理サーバ１１は、変化するカウンタの値と残回数を照合するようにすることで、不正な使用を防止させるようにすることができる。

さらに、以上の例においては、電子証明書を常に添付してデータを送受信していたが、例えば、電子チケット管理サーバ１１などでユーザ ID と対応付けて記憶しておくようにすれば、データの授受の度に電子証明書を添付する必要は無くなる。

また、電子チケットの所有者を移動させる例の応用例として、所定期間を設定し、その期間内で最も高い指定代金を設定したユーザに電子チケットの所有権を移動させるようにしてもよく。このような構成とすることにより、電子チケットのネットオークションシステムを構築させることもできる。

以上の処理により、電子チケットの所有者を変更させることが可能となるので、ユーザ端末によって、例えば、上述のようなコンテンツの配信を受ける権利を購入したような際にも、コンテンツの配信を受けるための機器の制限をなくすことができ、さらに、権利として他のユーザへの譲渡なども簡単に行うことができる。

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストール

することで、各種の機能を実行させることが可能な、例えば汎用のパーソナルコンピュータなどに記録媒体からインストールされる。

この記録媒体は、図２乃至図６に示すように電子チケット管理サーバ１１、ユーザ端末１２、認証局サーバ１３、コンテンツ配信サーバ１４、および課金サーバ１５に予め組み込まれた状態でユーザに提供される、プログラムが記録されている記憶部３８，７８，１１８，１５８，１９８だけではなく、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク５１，９１，１３１，１７１，２１１（フレキシブルディスクを含む）、光ディスク５２，９２，１３２，１７２，２１２（CD-ROM(Compact Disk-Read Only Memory)，DVD（Digital Versatile Disk）を含む）、光磁気ディスク５３，９３，１３３，１７３，２１３（MD（Mini-Disc）（登録商標）を含む）、もしくは半導体メモリ５４，９４，１３４，１７４，２１４（Memory Stick を含む）などよりなるパッケージメディアにより構成される。

尚、本明細書では、コンテンツはコンテンツ配信サーバ１４から配信する例について記述したが、ユーザ端末１２に対して、コンテンツを磁気ディスク５１，９１，１３１，１７１，２１１（フレキシブルディスクを含む）、光ディスク５２，９２，１３２，１７２，２１２（CD-ROM(Compact Disk-Read Only Memory)，DVD（Digital Versatile Disk）を含む）、光磁気ディスク５３，９３，１３３，１７３，２１３（MD（Mini-Disc）（登録商標）を含む）、もしくは半導体メモリ５４，９４，１３４，１７４，２１４（Memory Stick を含む）などによって供給する場合も考えられる。この場合は、電子チケットのアクセス情報 ID には上記記録媒体に格納されるコンテンツのファイルが特定できる情報が含まれることになる。

尚、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理は、もちろん、必ずしも時

系列的に処理されなくとも、並列的あるいは個別に実行される処理を含むものである。

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

産業上の利用可能性

本発明によれば、ネットワークを介して流通する情報を取得する権利を所有するとき、機器に制限されることなく情報を取得することが可能となり、さらに、ネットワークを介して流通する情報を取得する権利を自由に譲渡することが可能となる。

請求の範囲

1． 所定の情報を取得する情報処理装置において、

前記所定の情報を取得する権利を示す電子チケットを記憶する記憶手段と、

前記電子チケットを識別するチケットID、および、前記チケットIDに対する電子署名をその他の情報処理装置に送信する送信手段と、

前記チケットIDと前記電子署名に基づいて、前記その他の情報処理装置より送信されてくる前記所定の情報を取得するための暗号鍵を受信する受信手段と、

前記受信手段により受信された暗号鍵を使用して、前記所定の情報を取得する取得手段と

を備えることを特徴とする情報処理装置。

2． 前記電子チケットは、前記チケットIDに加えて、取得可能な前記所定の情報を識別するアクセス情報ID、前記チケットID、または前記アクセス情報IDに対する電子署名を含む

ことを特徴とする請求の範囲第1項に記載の情報処理装置。

3． 前記アクセス情報IDは、前記所定の情報のインターネット上のURLを含む

ことを特徴とする請求の範囲第2項に記載の情報処理装置。

4． 前記記憶手段は、前記電子チケットに加えて、前記電子チケットに含まれる情報に対する電子署名と、前記電子チケットに含まれる情報に対する電子署名の検証用の公開鍵、前記電子チケットの所有者を識別するユーザID、並びに前記公開鍵、および前記ユーザ ID に対する電子署名を含むユーザ証明書を記憶し、

前記送信手段は、前記電子チケットと共に、前記電子署名、および前記ユーザ証明書をその他の情報処理装置に送信する

ことを特徴とする請求の範囲第1項に記載の情報処理装置。

5． 前記電子チケットの所有者を識別するユーザIDを、前記所有者とは異なる他の所有者にユーザIDに変更するように前記その他の情報処理装置に要求する要求手段をさらに備える

ことを特徴とする請求の範囲第１項に記載の情報処理装置。

６．　前記要求手段が、前記電子チケットの所有者を識別するユーザ ID を、前記所有者とは異なる他の所有者のユーザ ID に変更するように、前記その他の情報処理装置に要求するとき、変更に伴う対価を設定する対価設定手段をさらに備える

ことを特徴とする請求の範囲第５項に記載の情報処理装置。

７．　前記対価設定手段は、変更に伴う対価を前記所有者により設定された対価とする

ことを特徴とする請求の範囲第６項に記載の情報処理装置。

８．　前記対価設定手段は、変更に伴う対価を前記他の所有者により設定された対価とする

ことを特徴とする請求の範囲第６項に記載の情報処理装置。

９．　前記所定の情報は、映画、または、音楽を含む

ことを特徴とする請求の範囲第１項に記載の情報処理装置。

１０．　所定の情報を取得する情報処理装置の情報処理方法において、

前記所定の情報を取得する権利を示す電子チケットを記憶する記憶ステップと、

前記電子チケットを識別するチケット ID と、前記チケット ID に対する電子署名をその他の情報処理装置に送信する送信ステップと、

前記チケット ID と前記電子署名に基づいて、前記その他の情報処理装置より送信されてくる前記所定の情報を取得するための暗号鍵を受信する受信ステップと、

前記受信ステップの処理で受信された暗号鍵を使用して、前記所定の情報を取得する取得ステップと

を含むことを特徴とする情報処理方法。

１１．　所定の情報を取得する情報処理装置を制御するプログラムであって、

前記所定の情報を取得する権利を示す電子チケットの記憶を制御する記憶制御ステップと、

前記電子チケットを識別するチケットIDと、前記チケットIDに対する電子署名のその他の情報処理装置への送信を制御する送信制御ステップと、

前記チケットIDと前記電子署名に基づいて、前記その他の情報処理装置より送信されてくる前記所定の情報を取得するための暗号鍵の受信を制御する受信制御ステップと、

前記受信制御ステップの処理で受信された暗号鍵の使用と、前記所定の情報の取得を制御する取得制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

１２．　所定の情報を取得する情報処理装置を制御するコンピュータに、

前記所定の情報を取得する権利を示す電子チケットの記憶を制御する電子チケット記憶制御ステップと、

前記電子チケットを識別するチケットIDと、前記チケットIDに対する電子署名の第１の情報処理装置への送信を制御する送信制御ステップと、

前記チケットIDと前記電子署名に基づいて、前記第１の情報処理装置より送信されてくる前記所定の情報を取得するための暗号鍵の受信を制御する受信制御ステップと、

前記受信制御ステップの処理で受信された暗号鍵の使用と、前記所定の情報の取得を制御する取得制御ステップと

を実行させるプログラム。

１３．　電子チケットを管理する情報処理装置において、

前記電子チケットを識別するチケットIDと、前記チケットID毎に対応する所定の情報の取得を可能にする暗号鍵を記憶する記憶手段と、

他の情報処理装置より送信されてくる、前記電子チケットを識別するチケットIDと、前記チケットIDに対する電子署名を受信する受信手段と、

前記チケットIDに対する電子署名が正当なものであるか否かを判定する判定手段と、

前記判定手段の判定結果に基づいて、前記チケットIDに対応する前記所定の情報の取得を可能にする暗号鍵を、前記その他の情報処理装置に送信する送信手段と

を備えることを特徴とする情報処理装置。

１４．　前記電子チケットは、前記チケットIDに加えて、取得可能な前記所定の情報を識別するアクセス情報ID、前記チケットID、またはアクセス情報IDに対する電子署名を含む

ことを特徴とする請求の範囲第１３項に記載の情報処理装置。

１５．　前記アクセス情報IDは、前記所定の情報のインターネット上のURLを含む

ことを特徴とする請求の範囲第１４項に記載の情報処理装置。

１６．　前記電子チケットは、前記チケットID、または、前記電子署名に加えて、前記電子チケットの所有者を識別するユーザIDを含む

ことを特徴とする請求の範囲第１３項に記載の情報処理装置。

１７．　前記記憶手段は、前記電子チケットを識別するチケットIDと、前記チケットID毎に対応する所定の情報の取得を可能にする暗号鍵に加えて、前記チケットID毎に前記所定の情報の取得にかかる状態を記憶する

ことを特徴とする請求の範囲第１３項に記載の情報処理装置。

１８．　前記送信手段が、前記チケットIDに対応する前記所定の情報の取得を可能にする暗号鍵を、前記その他の情報処理装置に送信するとき、前記チケットID毎に前記所定の情報の取得にかかる状態を変更させる状態変更手段をさらに備える

ことを特徴とする請求の範囲第１７項に記載の情報処理装置。

１９．　前記状態変更手段は、前記送信手段が、前記チケットIDに対応する前記所定の情報の取得を可能にする暗号鍵を、前記その他の情報処理装置に送信するとき、前記チケットID毎に前記所定の情報の取得にかかる状態のうち、取得可能回数を変更させる

ことを特徴とする請求の範囲第１８項に記載の情報処理装置。

２０．　前記状態変更手段は、前記送信手段が、前記チケットIDに対応する前記所定の情報の取得を可能にする暗号鍵を、前記その他の情報処理装置に送信するとき、前記チケットID毎に前記所定の情報の取得にかかる状態のうち、取得可能な期限を変更させる

ことを特徴とする請求の範囲第１８項に記載の情報処理装置。

２１．　前記記憶手段は、前記電子チケットを識別するチケットIDと、前記チケットID毎に対応する所定の情報の取得を可能にする暗号鍵に加えて、前記チケットID毎にその所有者を識別するユーザIDを記憶する

ことを特徴とする請求の範囲第１３項に記載の情報処理装置。

２２．　前記電子署名は、前記ユーザIDを含み、

前記電子署名に含まれた前記電子チケットの使用者の前記ユーザIDと、前記記憶手段により記憶されている前記電子チケットの所有者の前記ユーザIDとを比較し、比較結果に応じて、前記電子チケットの所有者と使用者が一致しているか否かを確認する確認手段をさらに備える

ことを特徴とする請求の範囲第２１項に記載の情報処理装置。

２３．　前記他の情報処理装置より送信されてくる電子チケットのユーザIDの変更要求を受信する変更要求受信手段と、

前記変更要求に対応して、前記記憶手段により記憶されている電子チケットのユーザIDを、前記所有者とは異なる他の所有者のIDに変更するユーザID変更手段とをさらに備える

ことを特徴とする請求の範囲第２２項に記載の情報処理装置。

２４．　前記変更要求受信手段は、電子チケットのユーザIDの変更要求に加えて、変更にかかる対価の情報を受信し、

前記ユーザID変更手段が、前記記憶手段により記憶されている電子チケットのユーザIDを、前記所有者とは異なる他の所有者のIDに変更するとき、前記対価の情報に基づいた課金を行う課金手段をさらに備える

ことを特徴とする請求の範囲第２３項に記載の情報処理装置。

２５．　電子チケットを管理する情報処理装置の情報処理方法において、

前記電子チケットを識別するチケットIDと、前記チケットID毎に対応する所定の情報の取得を可能にする暗号鍵を記憶する記憶ステップと、

他の情報処理装置より送信されてくる、前記電子チケットを識別するチケットIDと、前記チケットIDに対する電子署名を受信する受信ステップと、

前記チケットIDに対する電子署名が正当なものであるか否かを判定する判定ステップと、

前記判定ステップの処理での判定結果に基づいて、前記チケットIDに対応する前記所定の情報の取得を可能にする暗号鍵を、前記その他の情報処理装置に送信する送信ステップと

を含むことを特徴とする情報処理方法。

２６．　電子チケットを管理する情報処理装置を制御するプログラムであって、

前記電子チケットを識別するチケットIDと、前記チケットID毎に対応する所定の情報の取得を可能にする暗号鍵の記憶を制御する記憶制御ステップと、

他の情報処理装置より送信されてくる、前記電子チケットを識別するチケットIDと、前記チケットIDに対する電子署名の受信を制御する受信制御ステップと、

前記チケットIDに対する電子署名が正当なものであるか否かの判定を制御する判定制御ステップと、

前記判定制御ステップの処理での判定結果に基づいて、前記チケットIDに対応する前記所定の情報の取得を可能にする暗号鍵の、前記その他の情報処理装置への送信を制御する送信制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

２７．　電子チケットを管理する情報処理装置を制御するコンピュータに、

前記電子チケットを識別するチケットIDと、前記チケットID毎に対応する所定の情報の取得を可能にする暗号鍵の記憶を制御する記憶制御ステップと、

他の情報処理装置より送信されてくる、前記電子チケットを識別するチケットIDと、前記チケットIDに対する電子署名の受信を制御する受信制御ステップと、

前記チケットIDに対する電子署名が正当なものであるか否かの判定を制御する判定制御ステップと、

前記判定制御ステップの処理での判定結果に基づいて、前記チケットIDに対応する前記所定の情報の取得を可能にする暗号鍵の、前記その他の情報処理装置への送信を制御する送信制御ステップと

を実行させるプログラム。

２８．　所定の情報を取得する第１の情報処理装置と、電子チケットを管理する第２の情報処理装置からなる情報処理システムにおいて、

前記第１の情報処理装置は、

前記所定の情報を取得する権利を示す電子チケットを記憶する第１の記憶手段と、

前記電子チケットを識別するチケットIDと、前記チケットIDに対する電子署名を第２の情報処理装置に送信する第１の送信手段と、

前記チケットIDと前記電子署名に基づいて、前記第２の情報処理装置より送信されてくる前記所定の情報を取得するための暗号鍵を受信する第１の受信手段と、

前記第１の受信手段により受信された暗号鍵を使用して、前記所定の情報を取得する取得手段と

を備え、

前記第２の情報処理装置は、

前記電子チケットを識別するチケットIDと、前記チケットID毎に対応する所定の情報の取得を可能にする暗号鍵を記憶する第２の記憶手段と、

第１の情報処理装置より送信されてくる、前記電子チケットを識別するチケットIDと、前記チケットIDに対する電子署名を受信する第２の受信手段と、

前記チケットIDに対する電子署名が正当なものであるか否かを判定する判定手段と、

前記判定手段の判定結果に基づいて、前記チケットIDに対応する前記所定の情報の取得を可能にする暗号鍵を、前記その他の情報処理装置に送信する第2の送信手段と

を備える

ことを特徴とする情報処理システム。

図１

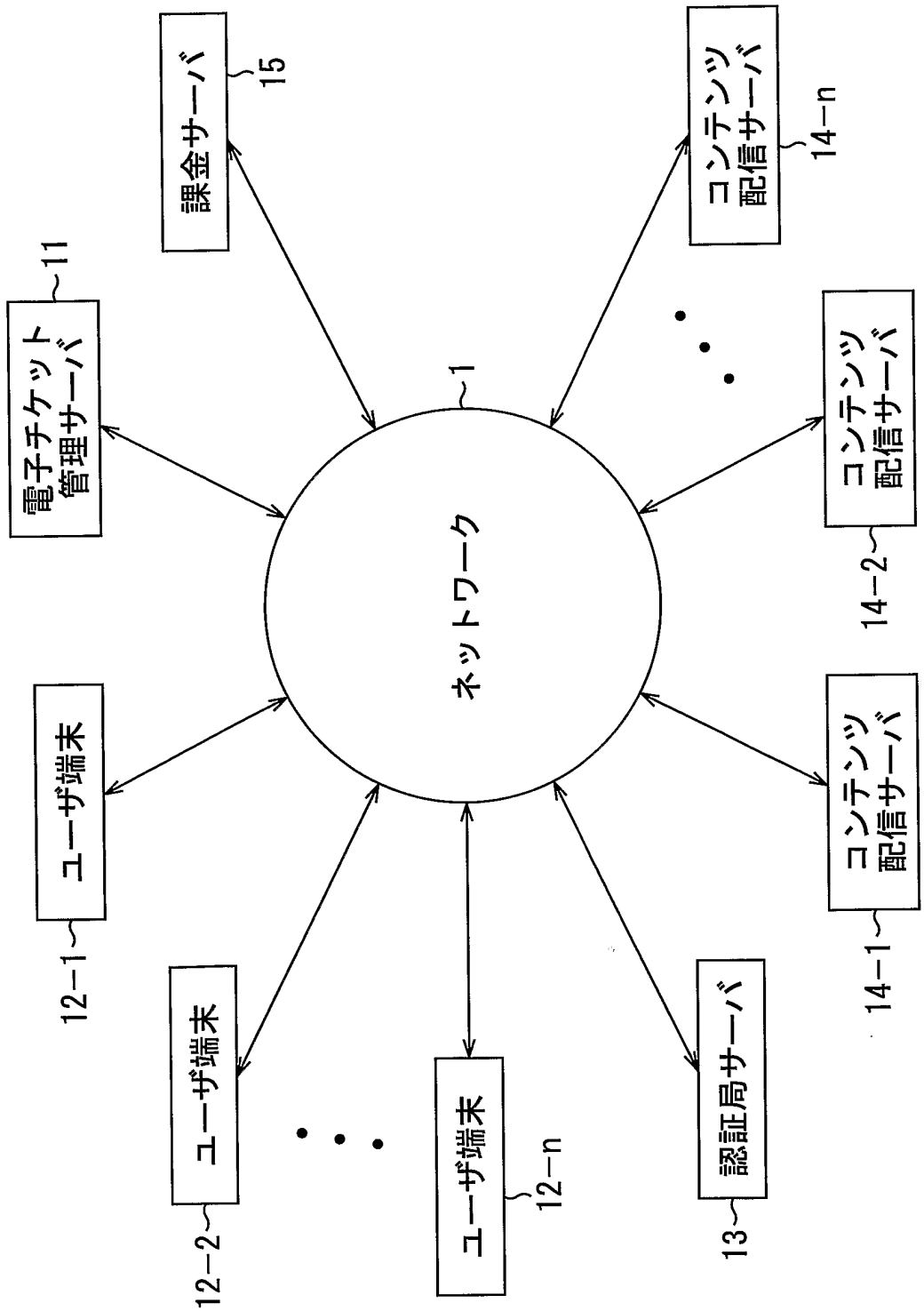

ネットワーク
1
課金サーバ
15
電子チケット
管理サーバ
11
ユーザ端末
12−1
ユーザ端末
12−2
ユーザ端末
12−n
認証局サーバ
13
コンテンツ
配信サーバ
14−1
コンテンツ
配信サーバ
14−2
コンテンツ
配信サーバ
14−n

図２

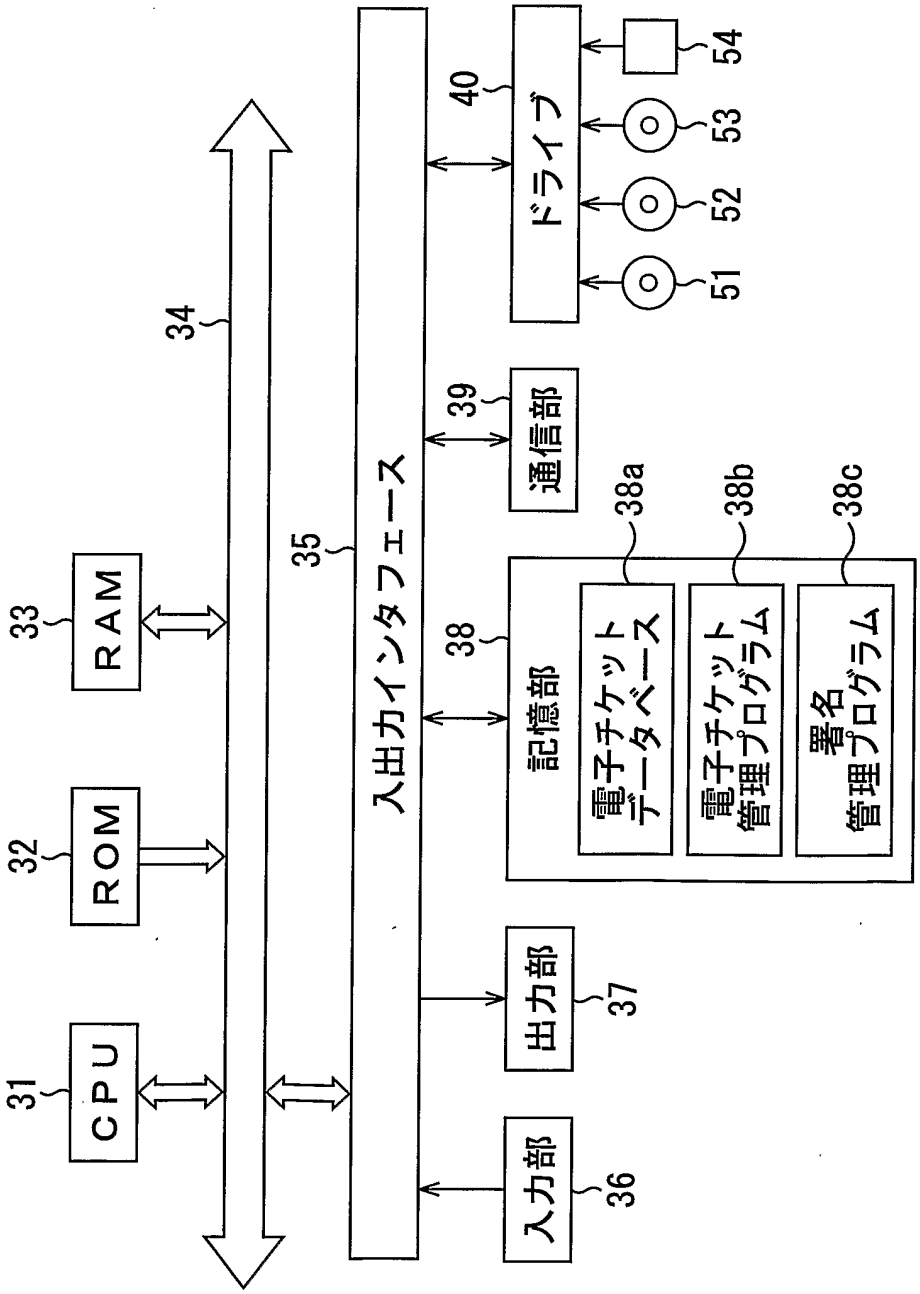

CPU
31
ROM
32
RAM
33
34
35
入出力インタフェース
入力部
36
出力部
37
38
記憶部
電子チケット
データベース
38a
電子チケット
管理プログラム
38b
署名
管理プログラム
38c
39
通信部
40
ドライブ
51
52
53
54

図３

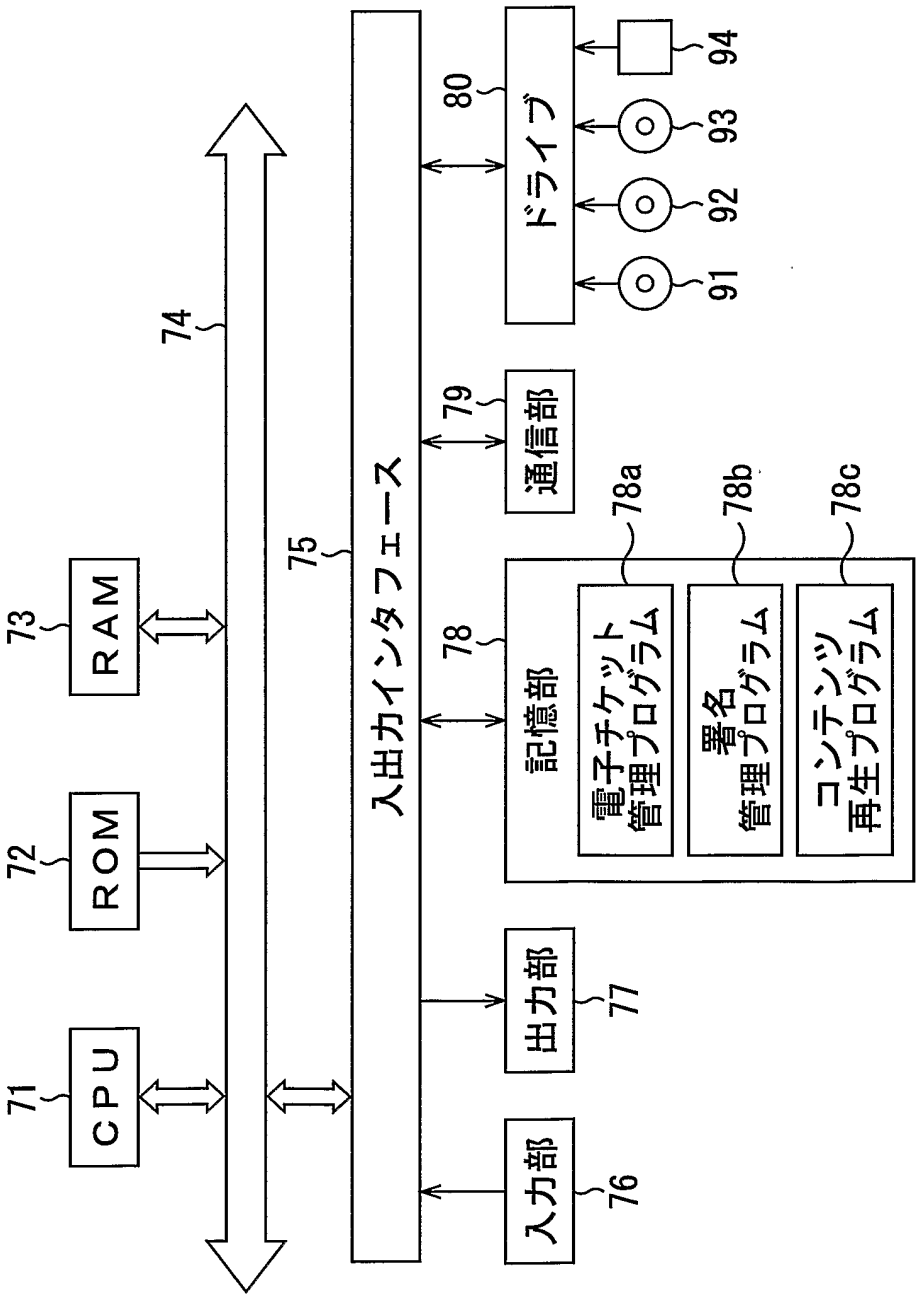

CPU
71
ROM
72
RAM
73
74
入出力インタフェース
75
入力部
76
出力部
77
記憶部
78
78a
電子チケット管理プログラム
78b
署名管理プログラム
78c
コンテンツ再生プログラム
通信部
79
ドライブ
80
91
92
93
94

図４

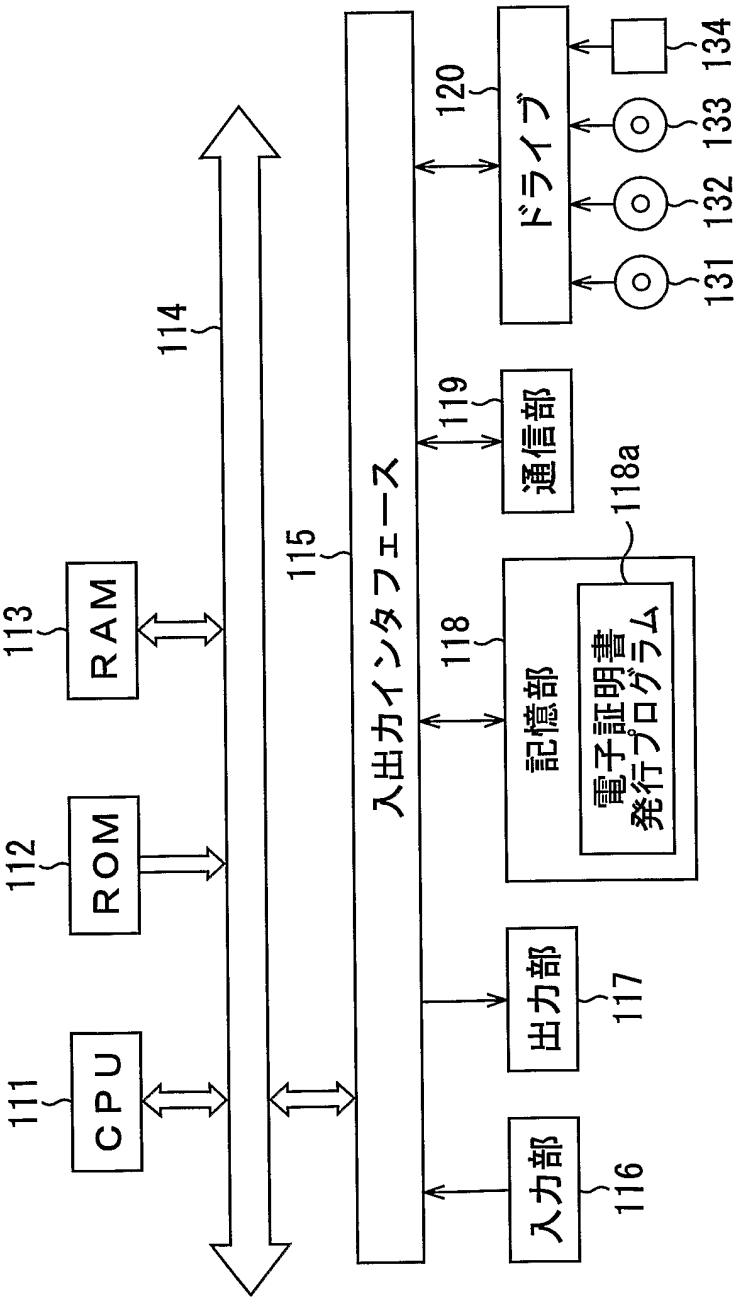

CPU
111
ROM
112
RAM
113
114
115
入出力インタフェース
入力部
116
出力部
117
記憶部
118
電子証明書
発行プログラム
118a
通信部
119
ドライブ
120
131
132
133
134

図5

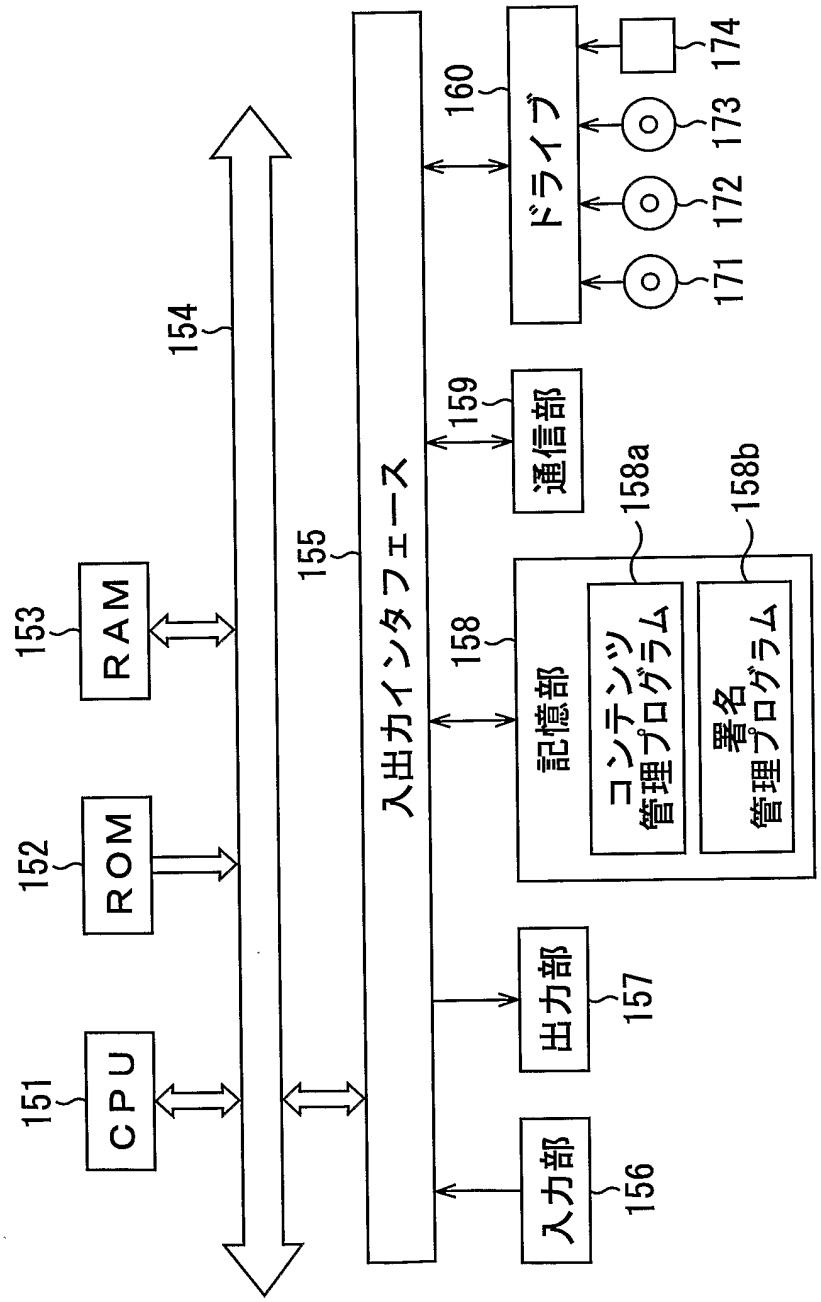

CPU
151
ROM
152
RAM
153
154
155
入出力インタフェース
158
記憶部
158a
コンテンツ管理プログラム
158b
署名管理プログラム
159
通信部
160
ドライブ
171
172
173
174
出力部
157
入力部
156

図６

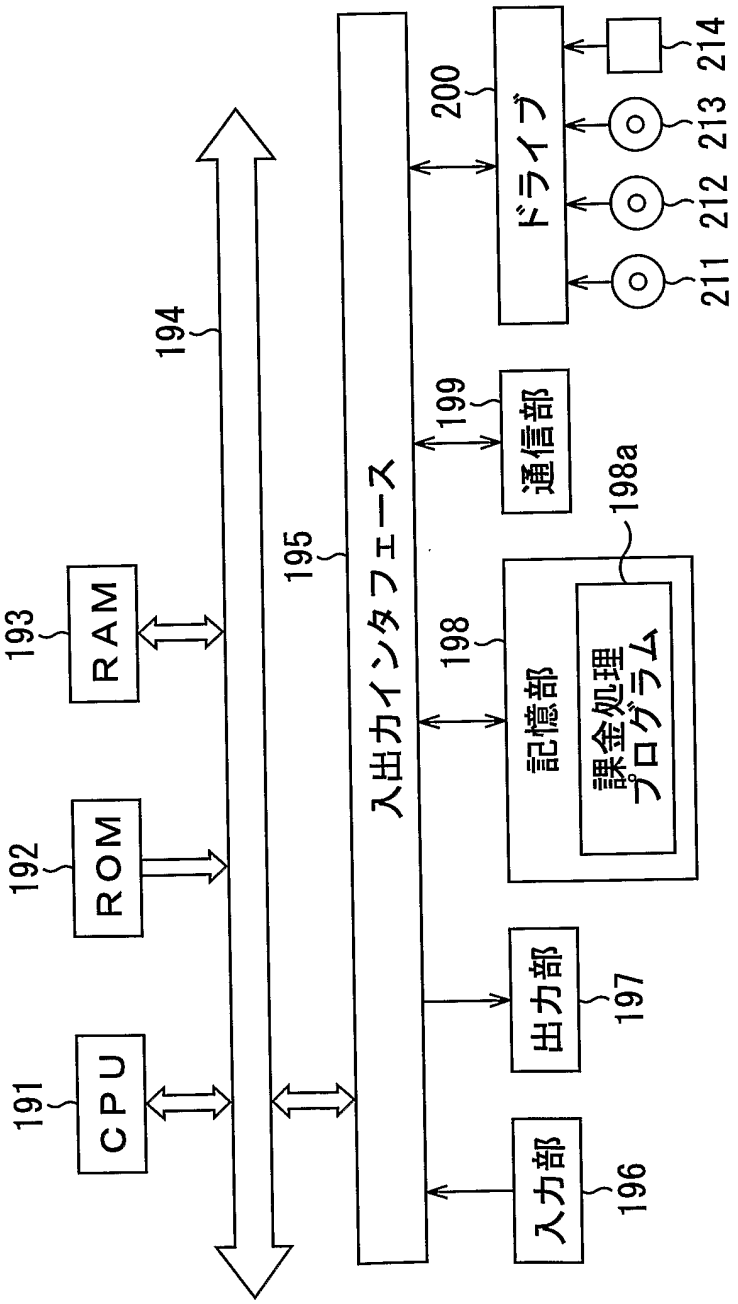

CPU
191
ROM
192
RAM
193
194
195
入出力インタフェース
入力部
196
出力部
197
記憶部
198
198a
課金処理プログラム
通信部
199
ドライブ
200
211
212
213
214

図７

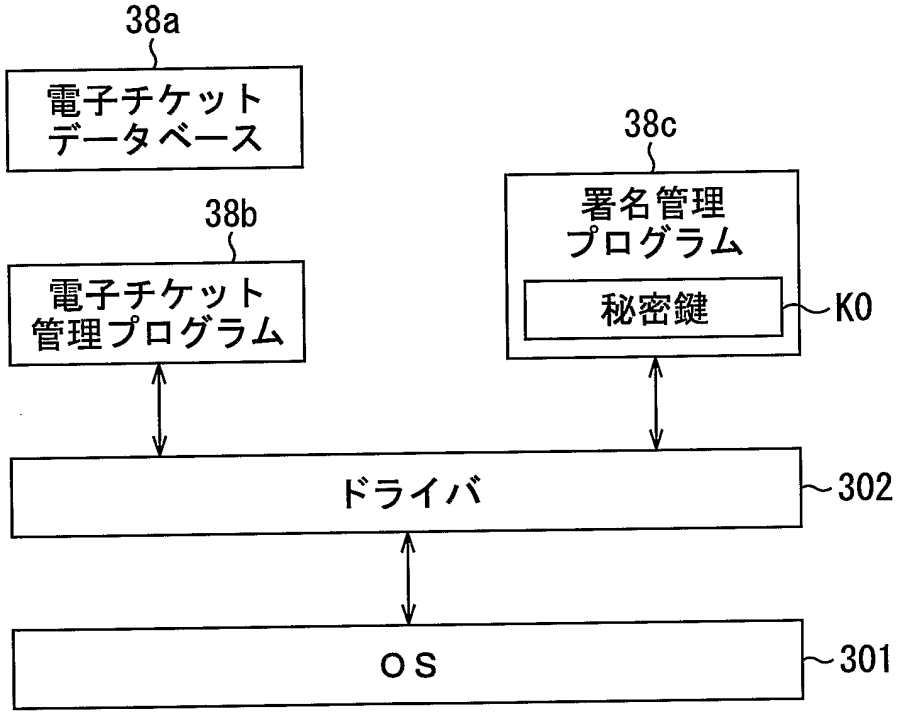

38a
電子チケット
データベース
38b
電子チケット
管理プログラム
38c
署名管理
プログラム
秘密鍵
K0
ドライバ
302
ＯＳ
301

図８

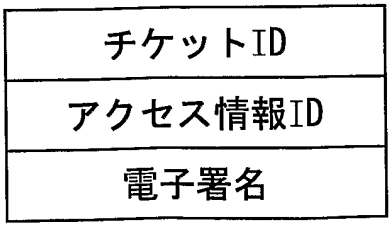

チケットID
アクセス情報ID
電子署名

図９

		電子チケットS	電子チケットT	電子チケットU	電子チケットV	電子チケットW	電子チケットZ
	チケットID	T11	T22	T33	T44	T55	T66
	アクセス情報ID	http://aaa.com/	http://bbb.com/	http://ccc.com/	http://ddd.com/	http://eee.com/	http://fff.com/
	アクセス用暗号鍵	AA1	BB1	CC1	DD1	EE1	FF1

図10

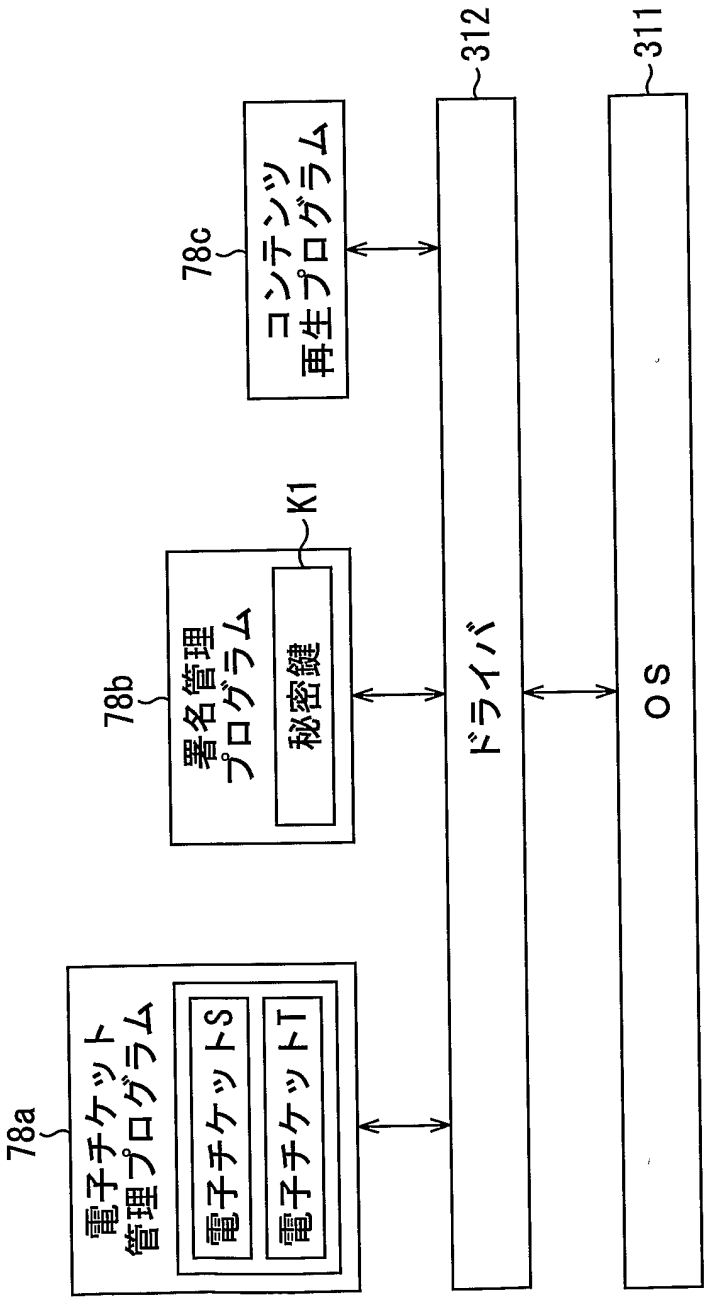

78a
電子チケット
管理プログラム
電子チケットS
電子チケットT
78b
署名管理
プログラム
K1
秘密鍵
78c
コンテンツ
再生プログラム
ドライバ
312
OS
311

図11

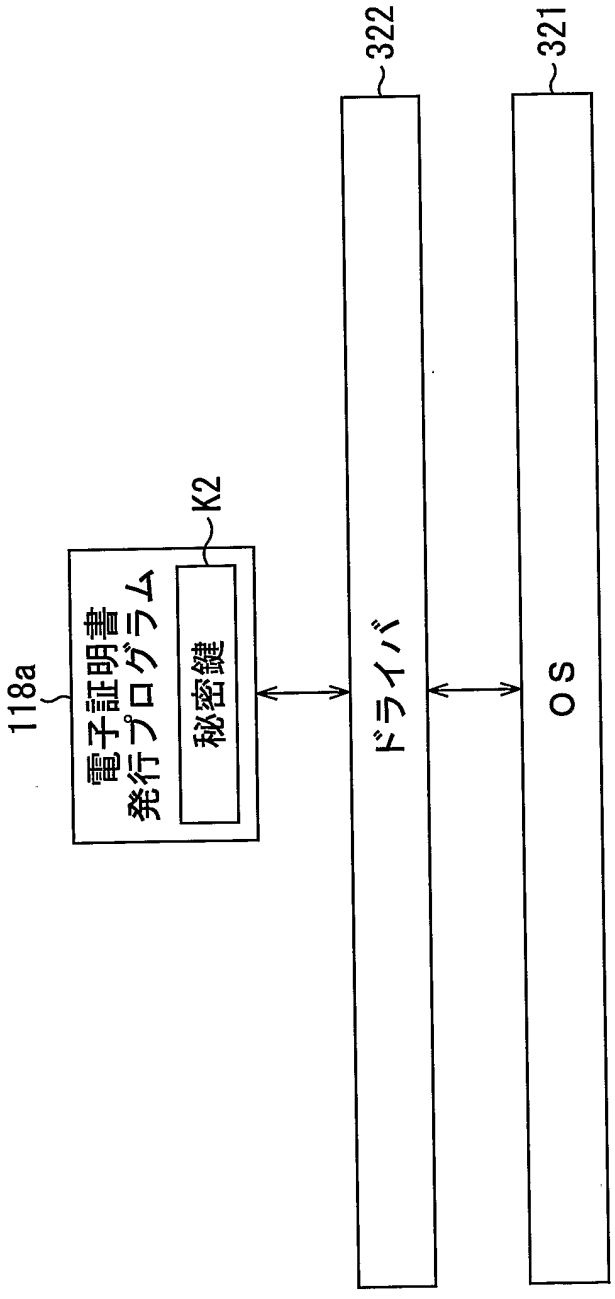


図12

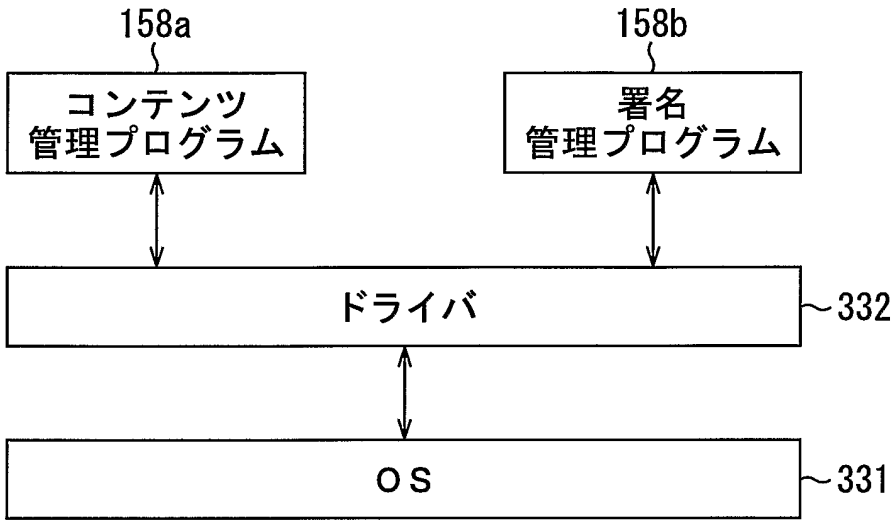

158a
158b
コンテンツ
管理プログラム
署名
管理プログラム
ドライバ
332
OS
331

図13

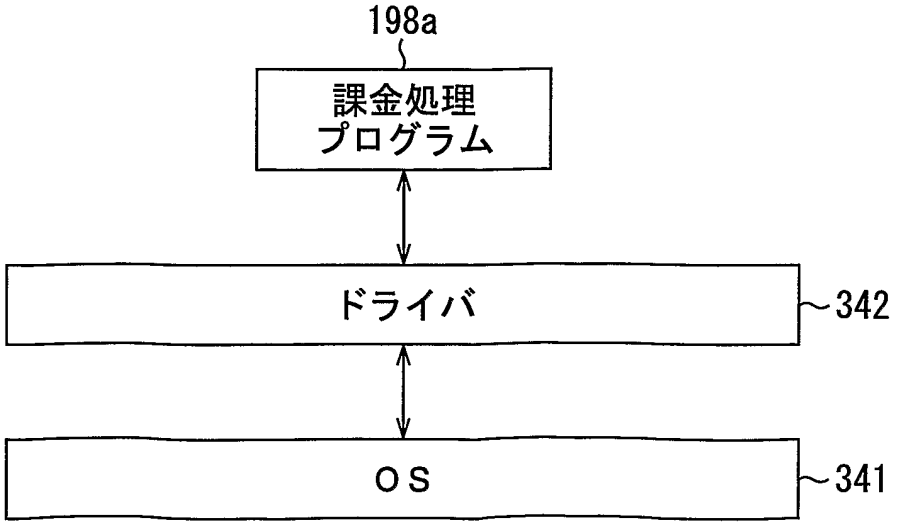

198a
課金処理
プログラム
ドライバ
342
OS
341

図14

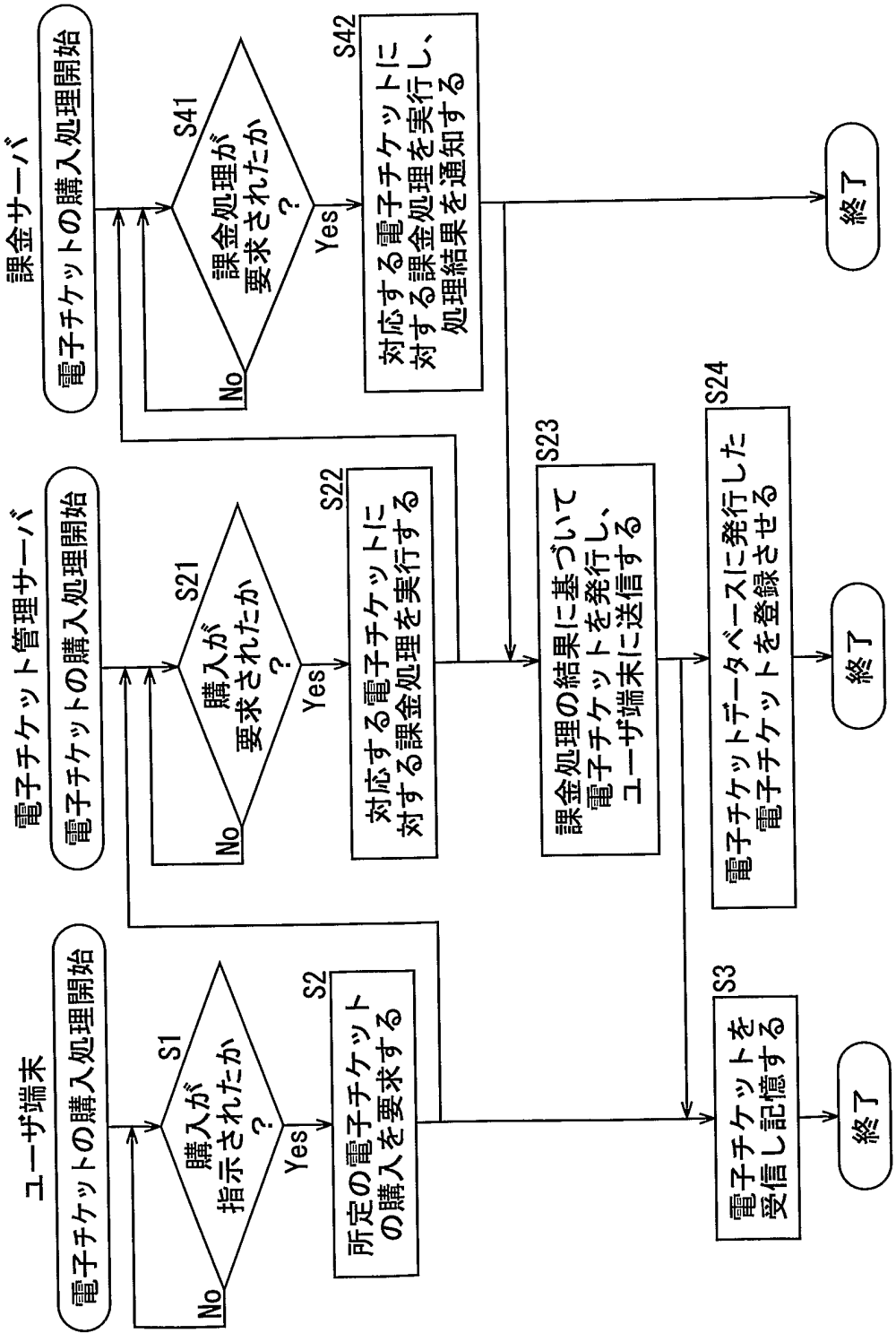

ユーザ端末
電子チケットの購入処理開始
S1
購入が指示されたか？
No
Yes
S2
所定の電子チケットの購入を要求する
電子チケット管理サーバ
電子チケットの購入処理開始
S21
購入が要求されたか？
No
Yes
S22
対応する電子チケットに対する課金処理を実行する
課金サーバ
電子チケットの購入処理開始
S41
課金処理が要求されたか？
No
Yes
S42
対応する電子チケットに対する課金処理を実行し、処理結果を通知する
S23
課金処理の結果に基づいて電子チケットを発行し、ユーザ端末に送信する
S24
電子チケットデータベースに発行した電子チケットを登録させる
S3
電子チケットを受信し記憶する
終了
終了
終了

図15

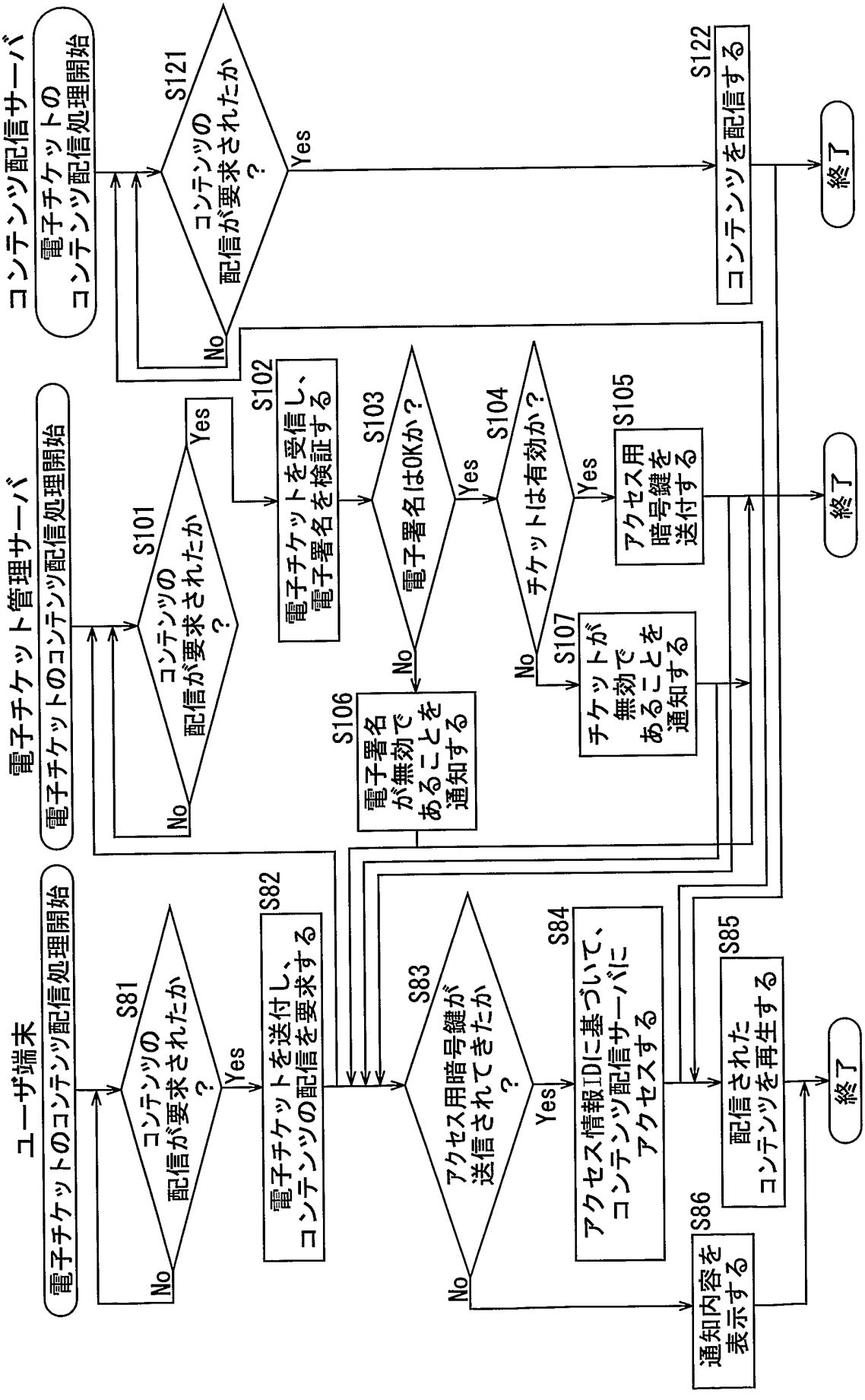

ユーザ端末
電子チケットのコンテンツ配信処理開始
S81
コンテンツの配信が要求されたか？
No
Yes
S82
電子チケットを送付し、コンテンツの配信を要求する
S83
アクセス用暗号鍵が送信されてきたか？
No
Yes
S84
アクセス情報IDに基づいて、コンテンツ配信サーバにアクセスする
S85
配信されたコンテンツを再生する
終了
S86
通知内容を表示する
電子チケット管理サーバ
電子チケットのコンテンツ配信処理開始
S101
コンテンツの配信が要求されたか？
No
Yes
S102
電子チケットを受信し、電子署名を検証する
S103
電子署名はOKか？
No
Yes
S106
電子署名が無効であることを通知する
S104
チケットは有効か？
No
Yes
S107
チケットが無効であることを通知する
S105
アクセス用暗号鍵を送付する
終了
コンテンツ配信サーバ
電子チケットのコンテンツ配信処理開始
S121
コンテンツの配信が要求されたか？
No
Yes
S122
コンテンツを配信する
終了

図16

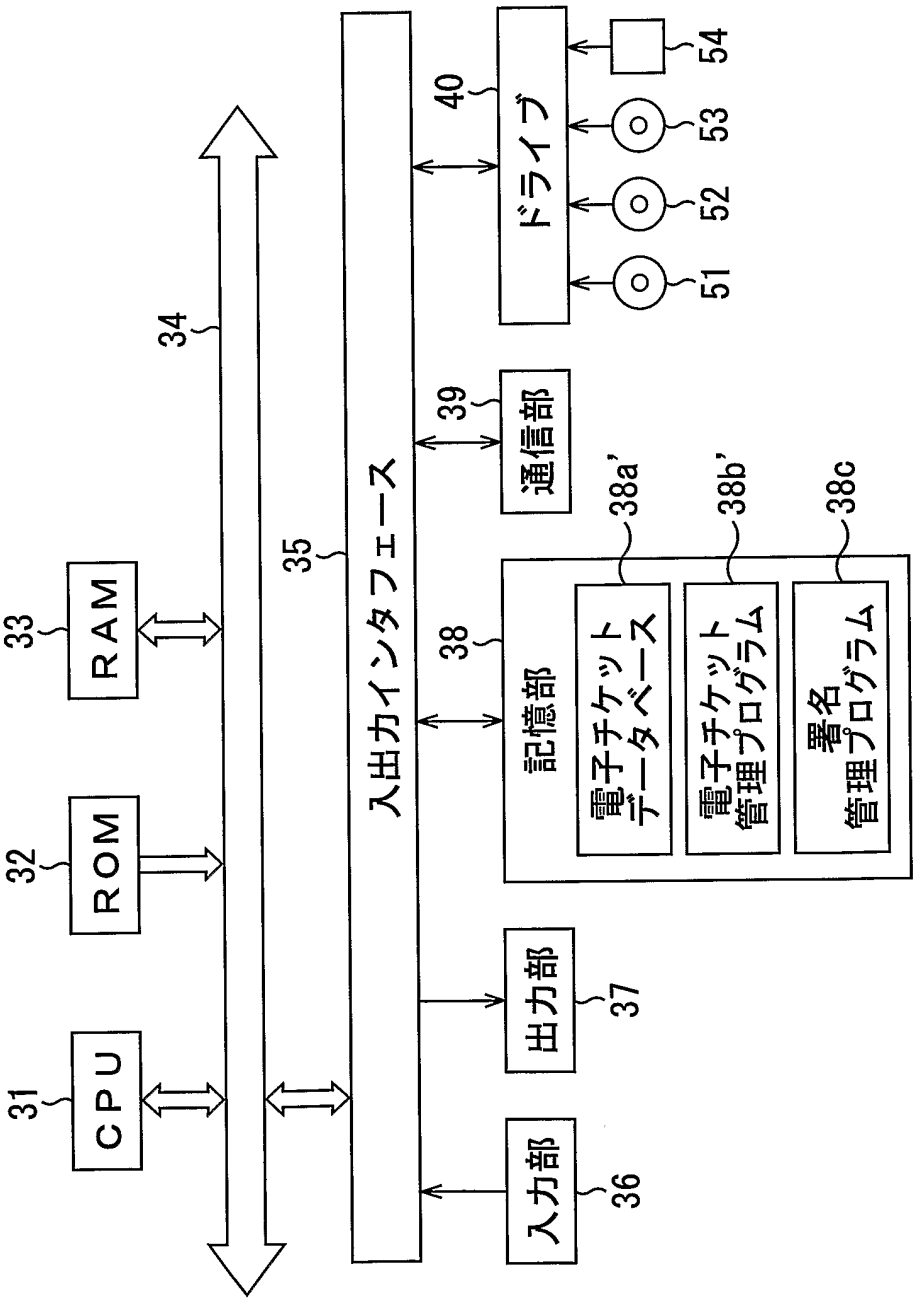

CPU
31
ROM
32
RAM
33
34
35
入出力インタフェース
入力部
36
出力部
37
記憶部
38
電子チケット
データベース
38a'
電子チケット
管理プログラム
38b'
署名
管理プログラム
38c
通信部
39
ドライブ
40
51
52
53
54

図17

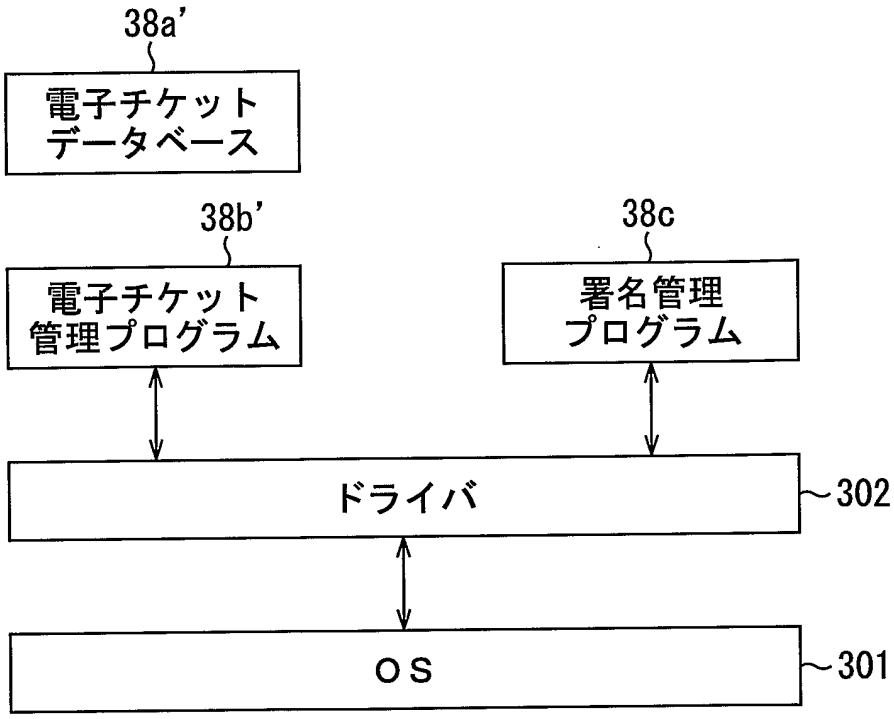

38a'
電子チケット
データベース
38b'
電子チケット
管理プログラム
38c
署名管理
プログラム
ドライバ
302
OS
301

図18

		電子チケットS	電子チケットT	電子チケットU	電子チケットV	電子チケットW	電子チケットZ
	チケットID	T11	T22	T33	T44	T55	T66
	アクセス情報ID	http://aaa.com/	http://bbb.com/	http://ccc.com/	http://ddd.com/	http://eee.com/	http://fff.com/
	アクセス用暗号鍵	AA1	BB1	CC1	DD1	EE1	FF1
	残回数	1	2	10	3	5	1

図19

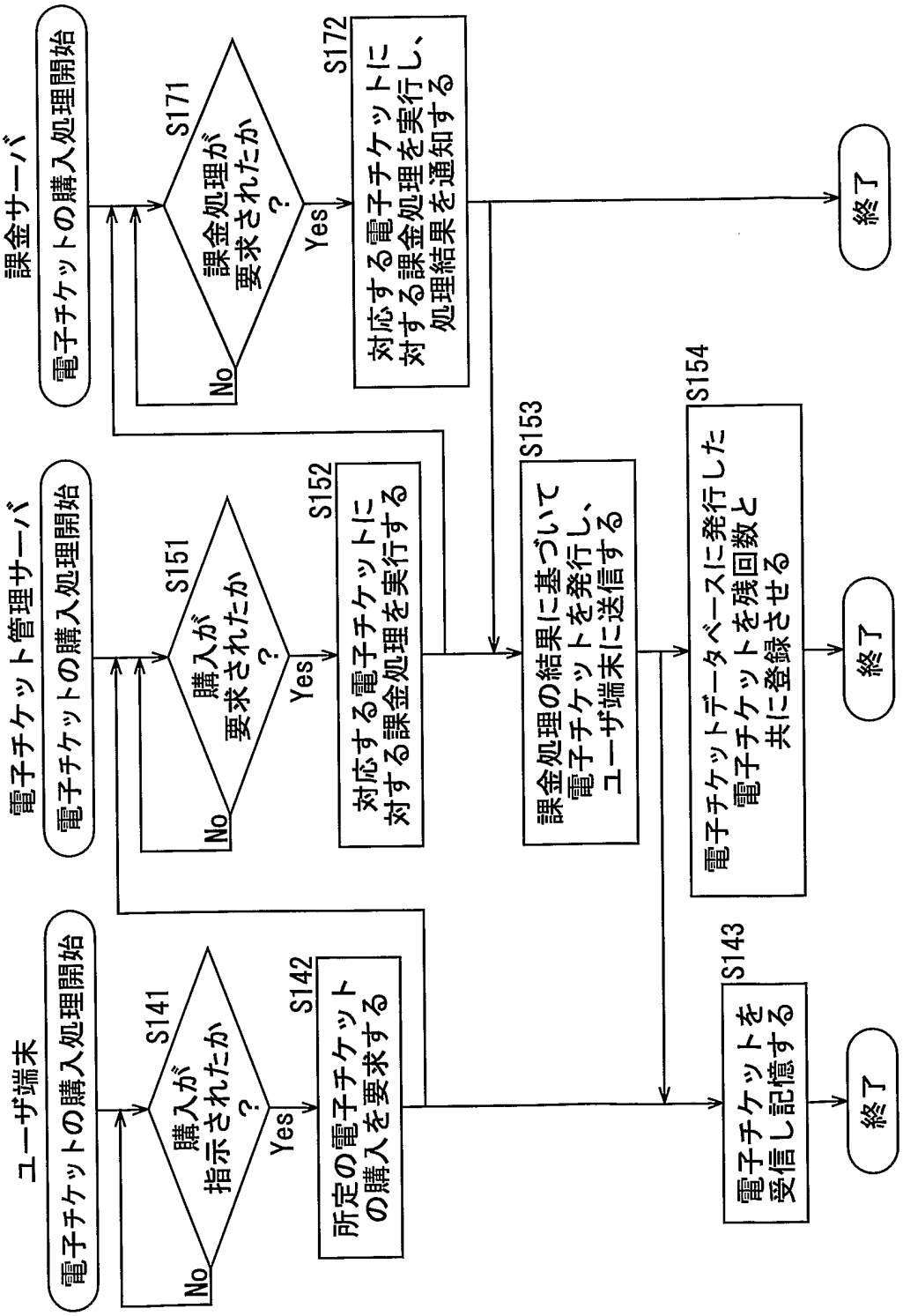

ユーザ端末
電子チケットの購入処理開始
S141
購入が指示されたか？
No
Yes
S142
所定の電子チケットの購入を要求する
電子チケット管理サーバ
電子チケットの購入処理開始
S151
購入が要求されたか？
No
Yes
S152
対応する電子チケットに対する課金処理を実行する
課金サーバ
電子チケットの購入処理開始
S171
課金処理が要求されたか？
No
Yes
S172
対応する電子チケットに対する課金処理を実行し、処理結果を通知する
S153
課金処理の結果に基づいて電子チケットを発行し、ユーザ端末に送信する
S154
電子チケットデータベースに発行した電子チケットを残回数と共に登録させる
S143
電子チケットを受信し記憶する
終了
終了
終了

図20

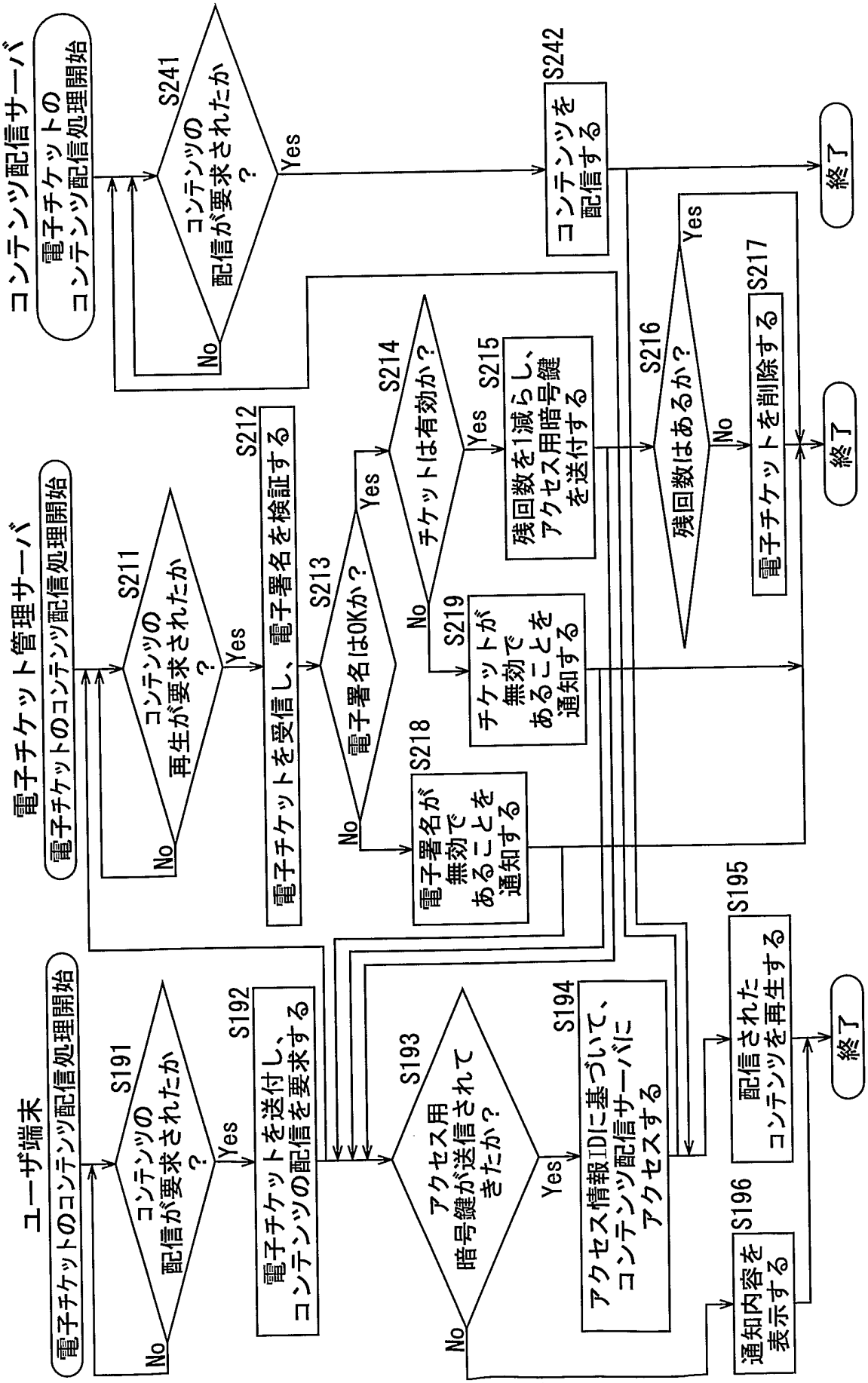

ユーザ端末
電子チケットのコンテンツ配信処理開始
S191
コンテンツの配信が要求されたか？
No
Yes
S192
電子チケットを送付し、コンテンツの配信を要求する
S193
アクセス用暗号鍵が送信されてきたか？
No
Yes
S194
アクセス情報IDに基づいて、コンテンツ配信サーバにアクセスする
S195
配信されたコンテンツを再生する
S196
通知内容を表示する
終了
電子チケット管理サーバ
電子チケットのコンテンツ配信処理開始
S211
コンテンツの再生が要求されたか？
No
Yes
S212
電子チケットを受信し、電子署名を検証する
S213
電子署名はOKか？
No
Yes
S214
チケットは有効か？
No
Yes
S215
残回数を1減らし、アクセス用暗号鍵を送付する
S216
残回数はあるか？
No
Yes
S217
電子チケットを削除する
S218
電子署名が無効であることを通知する
S219
チケットが無効であることを通知する
終了
コンテンツ配信サーバ
電子チケットのコンテンツ配信処理開始
S241
コンテンツの配信が要求されたか？
No
Yes
S242
コンテンツを配信する
終了

図21

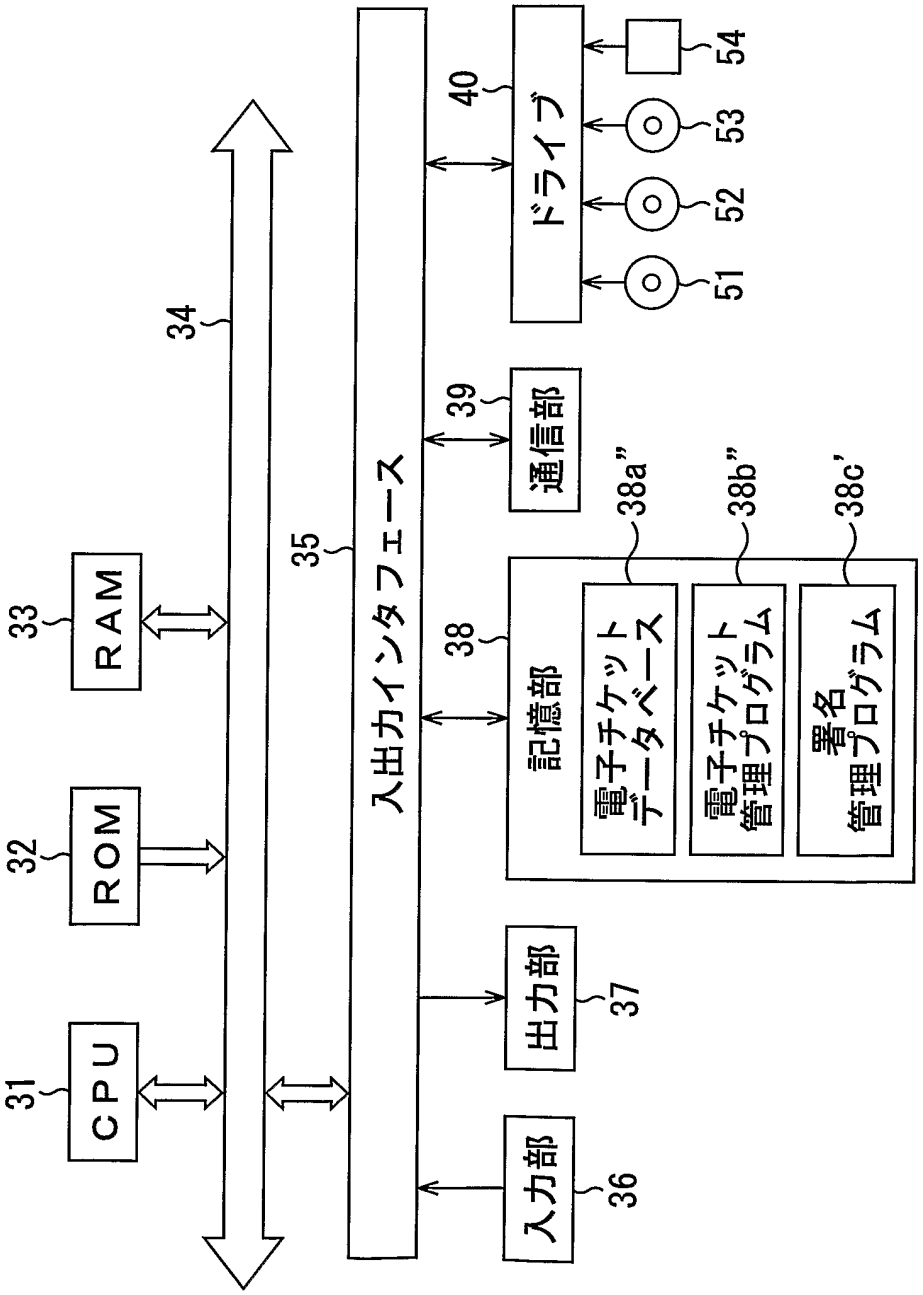

CPU
31
ROM
32
RAM
33
34
35
入出力インタフェース
入力部
36
出力部
37
38
記憶部
電子チケット
データベース
38a”
電子チケット
管理プログラム
38b”
署名
管理プログラム
38c’
39
通信部
40
ドライブ
51
52
53
54

図22

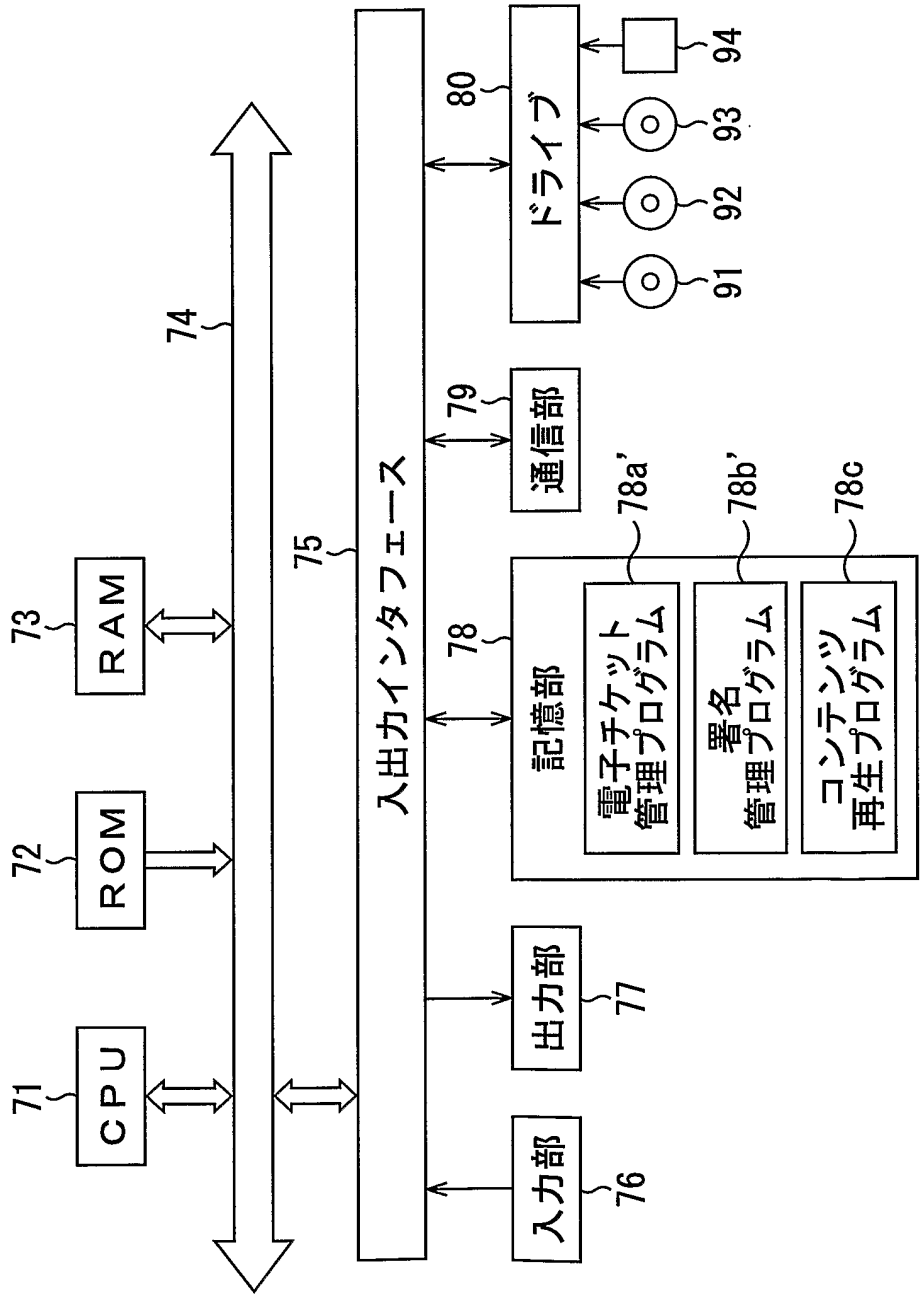

71
CPU
72
ROM
73
RAM
74
75
入出力インタフェース
76
入力部
77
出力部
78
記憶部
78a'
電子チケット管理プログラム
78b'
署名管理プログラム
78c
コンテンツ再生プログラム
79
通信部
80
ドライブ
91
92
93
94

図23

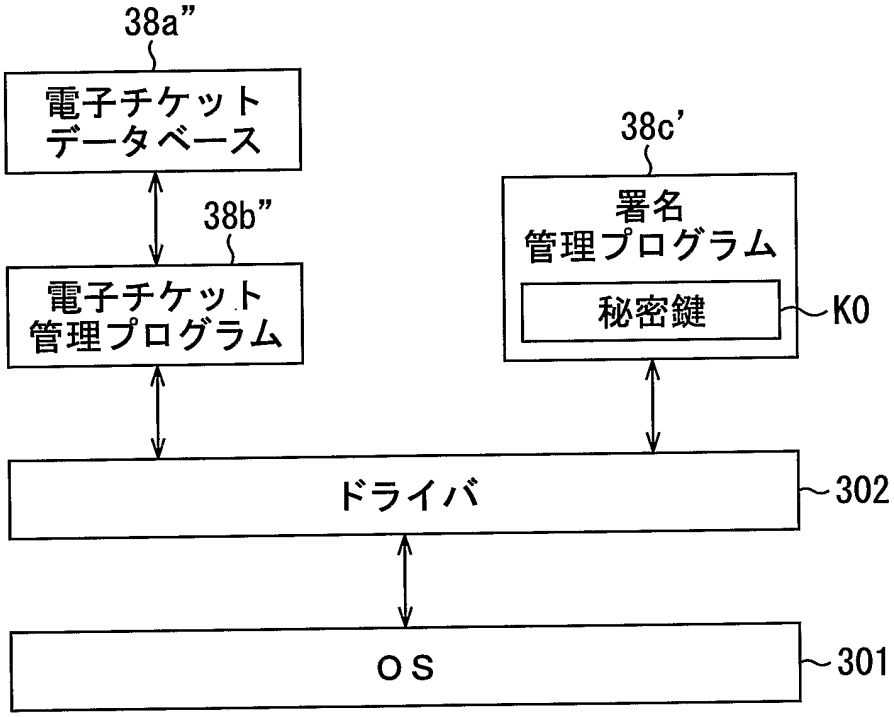

38a”
電子チケット
データベース
38b”
電子チケット
管理プログラム
38c’
署名
管理プログラム
秘密鍵
K0
ドライバ
302
OS
301

図24

		電子チケットS	電子チケットT	電子チケットU	電子チケットV	電子チケットW	電子チケットZ
	チケットID	T11	T22	T33	T44	T55	T66
	アクセス情報ID	http://aaa.com/	http://bbb.com/	http://ccc.com/	http://ddd.com/	http://eee.com/	http://fff.com/
	アクセス用暗号鍵	AA1	BB1	CC1	DD1	EE1	FF1
	残回数	1	2	10	3	5	1
	ユーザID	111	222	333	444	555	666

図25

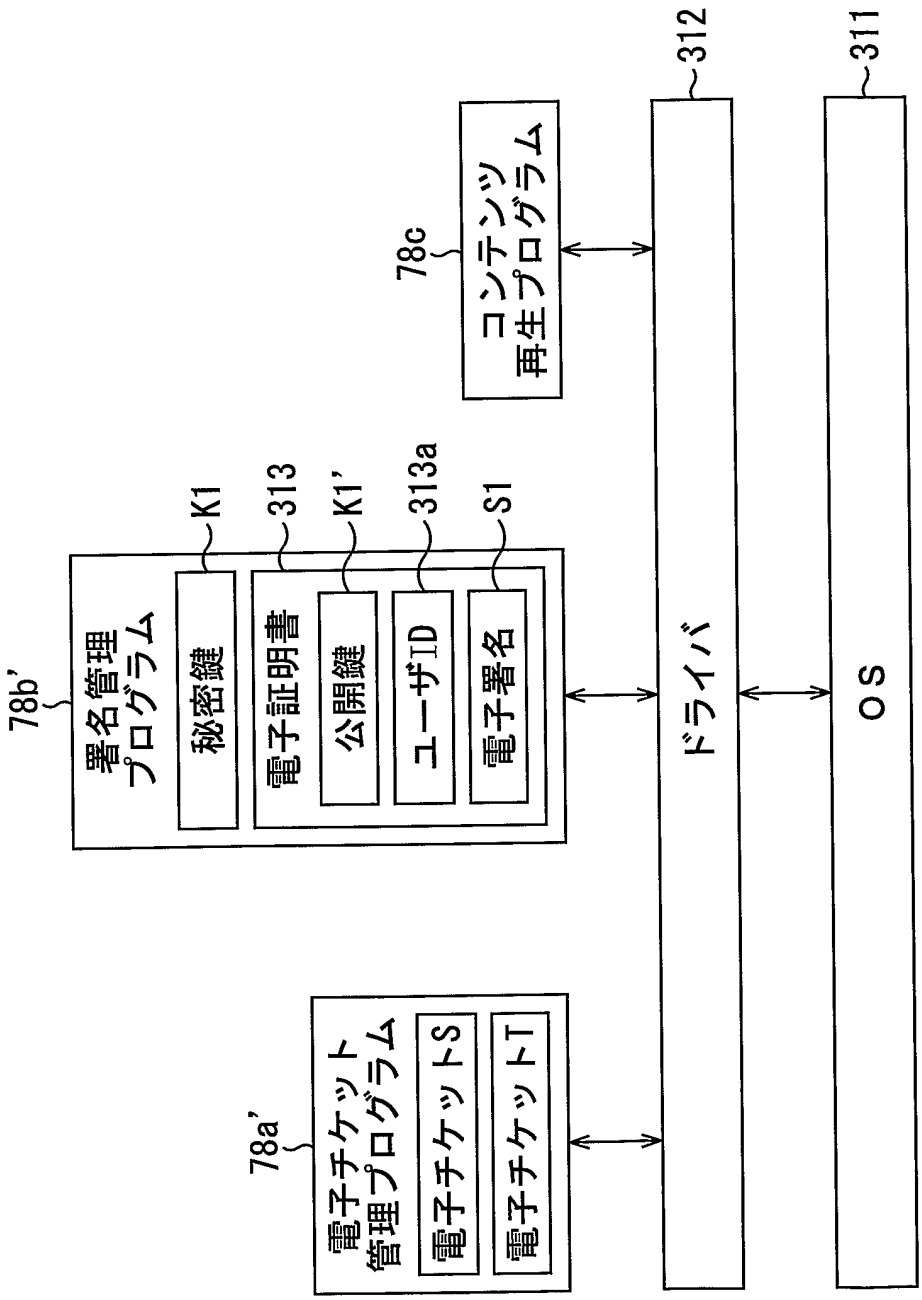

78b'
署名管理
プログラム
K1
秘密鍵
313
電子証明書
K1'
公開鍵
313a
ユーザID
S1
電子署名
78c
コンテンツ
再生プログラム
312
ドライバ
311
OS
78a'
電子チケット
管理プログラム
電子チケットS
電子チケットT

図26

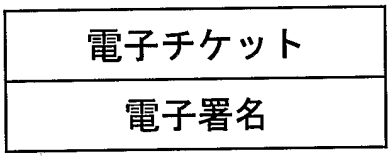


図27

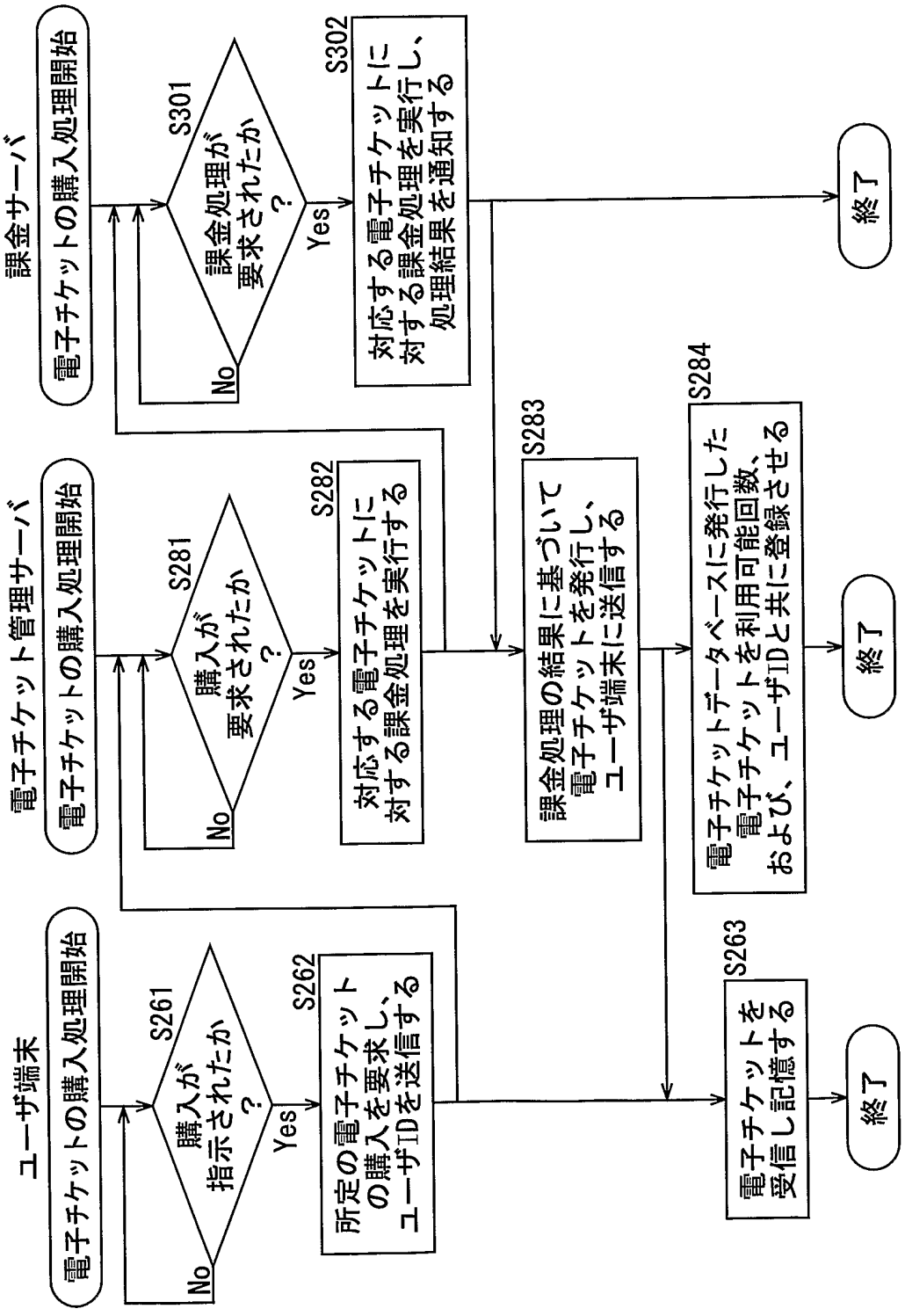

ユーザ端末
電子チケットの購入処理開始
S261
購入が指示されたか？
No
Yes
S262
所定の電子チケットの購入を要求し、ユーザIDを送信する
電子チケット管理サーバ
電子チケットの購入処理開始
S281
購入が要求されたか？
No
Yes
S282
対応する電子チケットに対する課金処理を実行する
課金サーバ
電子チケットの購入処理開始
S301
課金処理が要求されたか？
No
Yes
S302
対応する電子チケットに対する課金処理を実行し、処理結果を通知する
S283
課金処理の結果に基づいて電子チケットを発行し、ユーザ端末に送信する
S284
電子チケットデータベースに発行した電子チケットを利用可能回数、および、ユーザIDと共に登録させる
S263
電子チケットを受信し記憶する
終了
終了
終了

図28

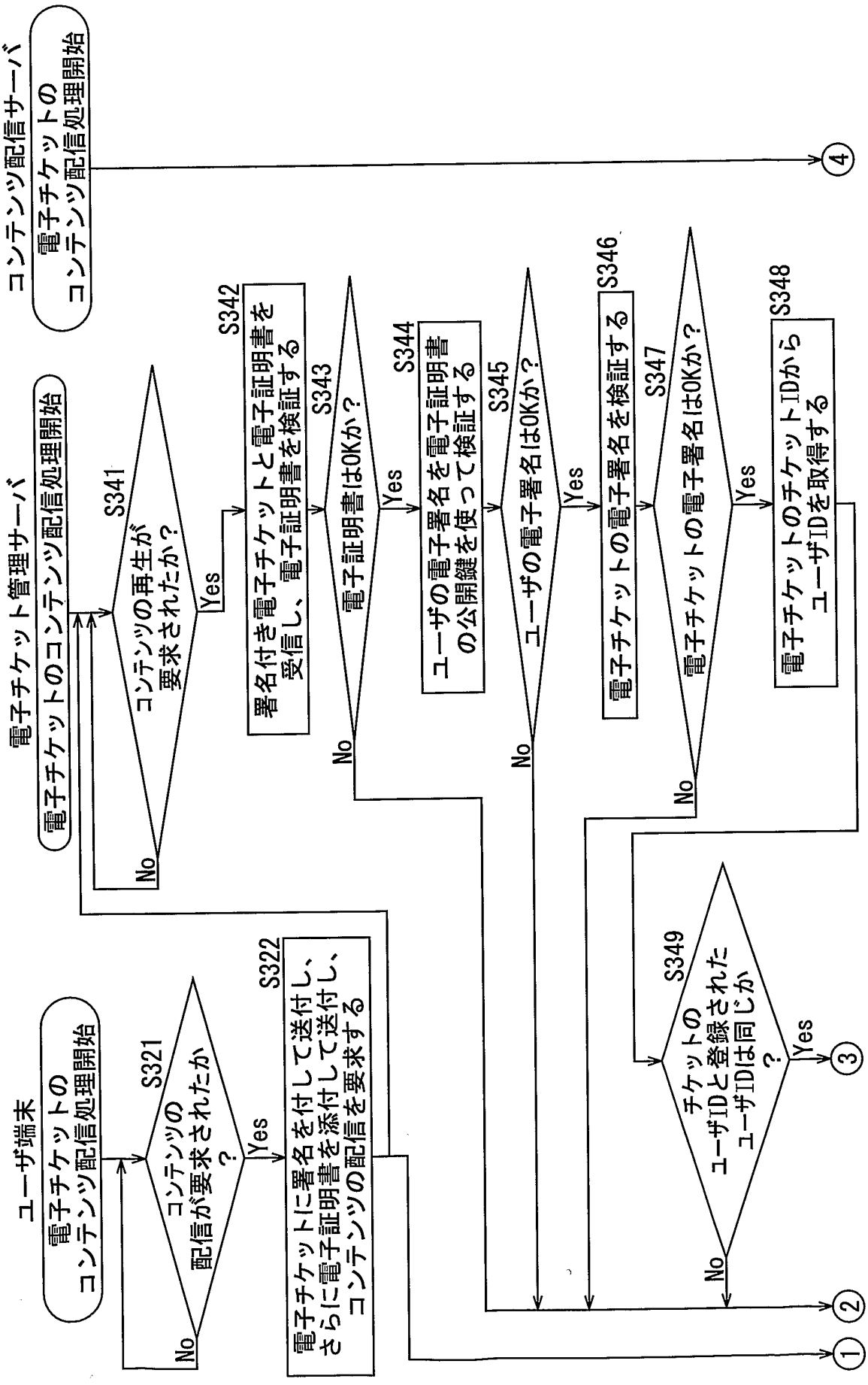

ユーザ端末
電子チケットの
コンテンツ配信処理開始
S321
コンテンツの
配信が要求されたか
？
No
Yes
S322
電子チケットに署名を付して送付し、
さらに電子証明書を添付して送付し、
コンテンツの配信を要求する
電子チケット管理サーバ
電子チケットのコンテンツ配信処理開始
S341
コンテンツの再生が
要求されたか？
No
Yes
S342
署名付き電子チケットと電子証明書を
受信し、電子証明書を検証する
S343
電子証明書はOKか？
No
Yes
S344
ユーザの電子署名を電子証明書
の公開鍵を使って検証する
S345
ユーザの電子署名はOKか？
No
Yes
S346
電子チケットの電子署名を検証する
S347
電子チケットの電子署名はOKか？
No
Yes
S348
電子チケットのチケットIDから
ユーザIDを取得する
S349
チケットの
ユーザIDと登録された
ユーザIDは同じか
？
No
Yes
コンテンツ配信サーバ
電子チケットの
コンテンツ配信処理開始
①
②
③
④

図29

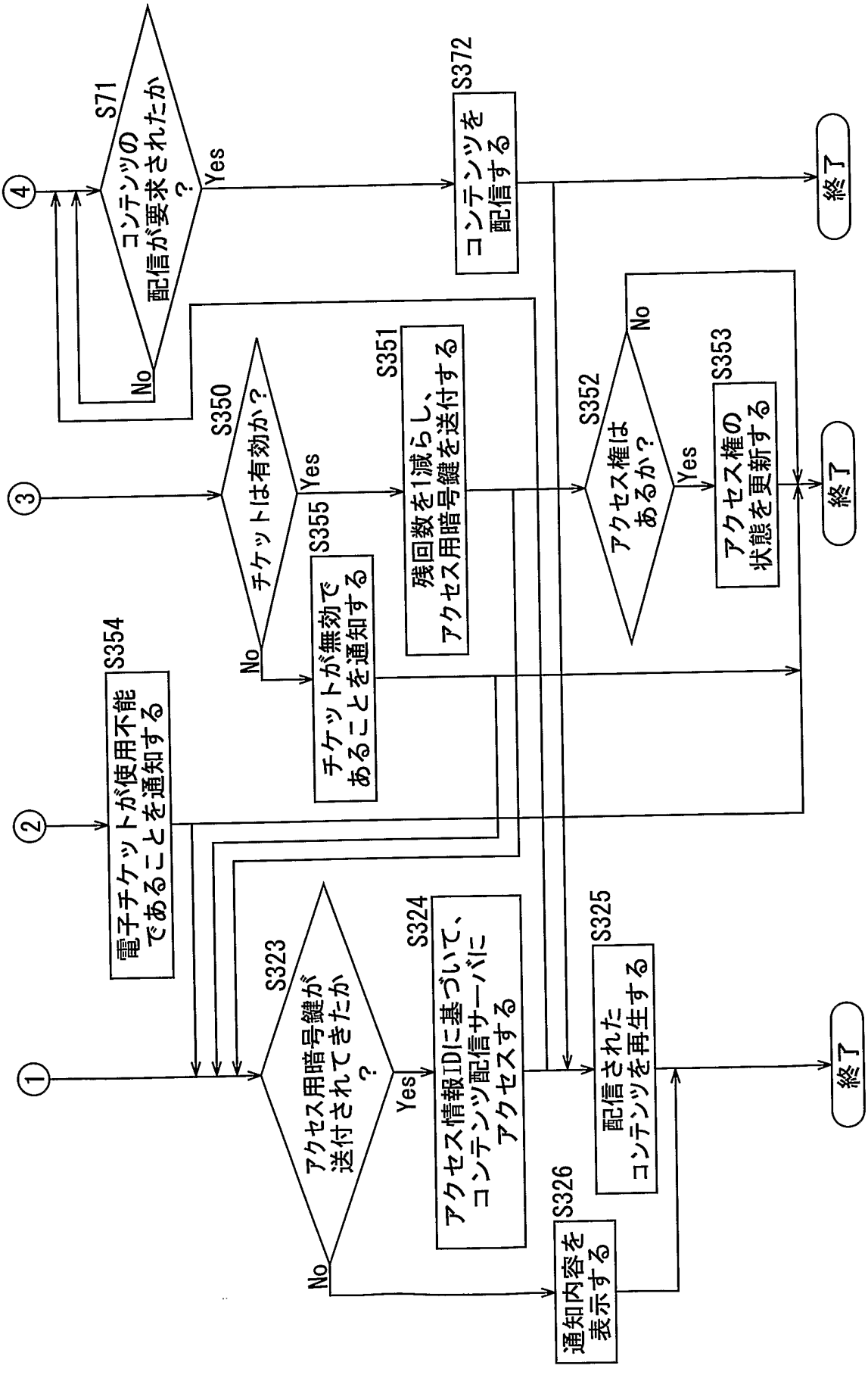

①
②
③
④
S71
コンテンツの配信が要求されたか？
Yes
No
S372
コンテンツを配信する
終了
S350
チケットは有効か？
Yes
No
S351
残回数を1減らし、アクセス用暗号鍵を送付する
S355
チケットが無効であることを通知する
S352
アクセス権はあるか？
Yes
No
S353
アクセス権の状態を更新する
終了
S354
電子チケットが使用不能であることを通知する
S323
アクセス用暗号鍵が送付されてきたか？
Yes
No
S324
アクセス情報IDに基づいて、コンテンツ配信サーバにアクセスする
S325
配信されたコンテンツを再生する
終了
S326
通知内容を表示する

図30

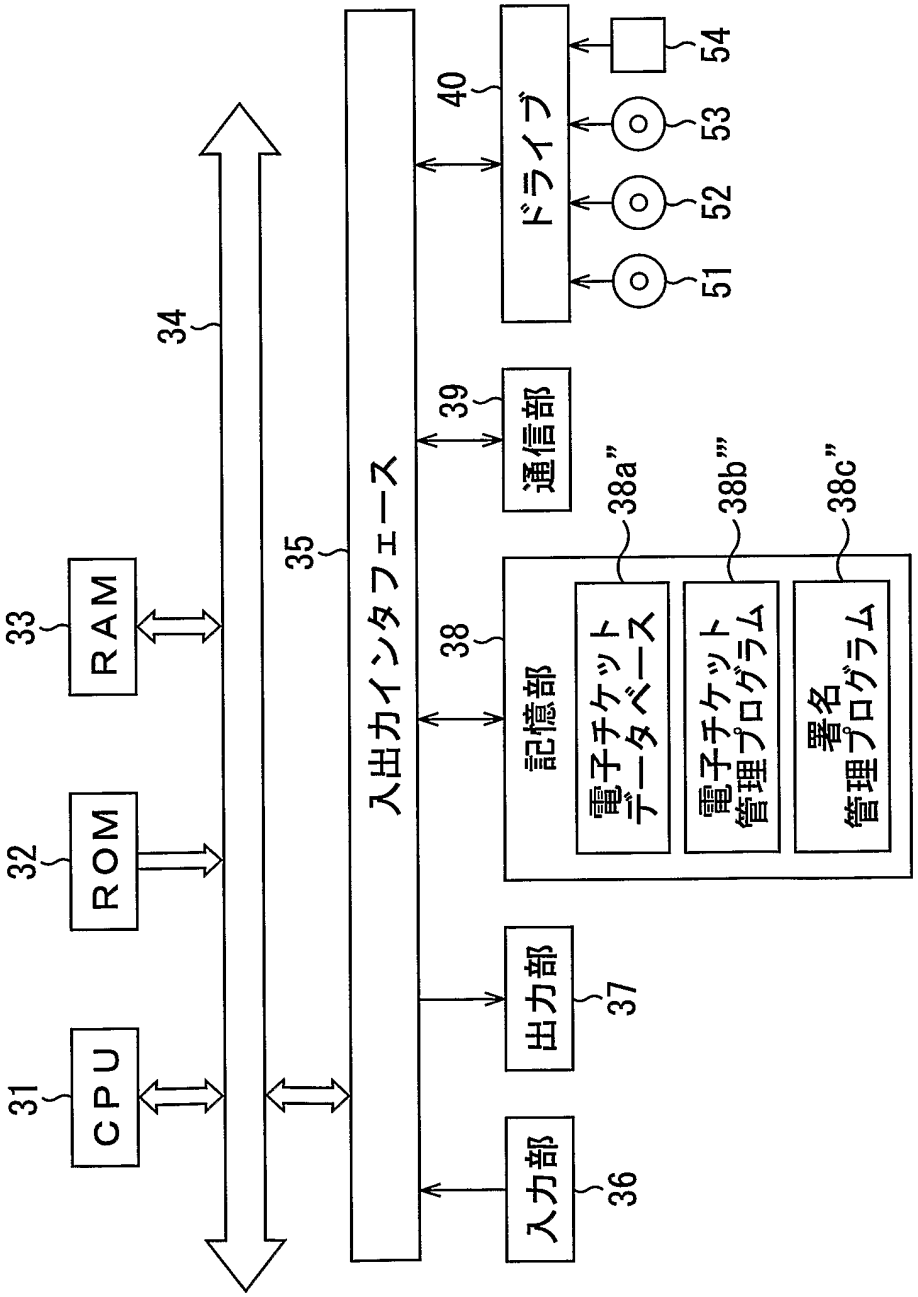

CPU
31
ROM
32
RAM
33
34
35
入出力インタフェース
入力部
36
出力部
37
38
記憶部
電子チケット
データベース
38a”
電子チケット
管理プログラム
38b”
署名
管理プログラム
38c”
39
通信部
40
ドライブ
51
52
53
54

図31

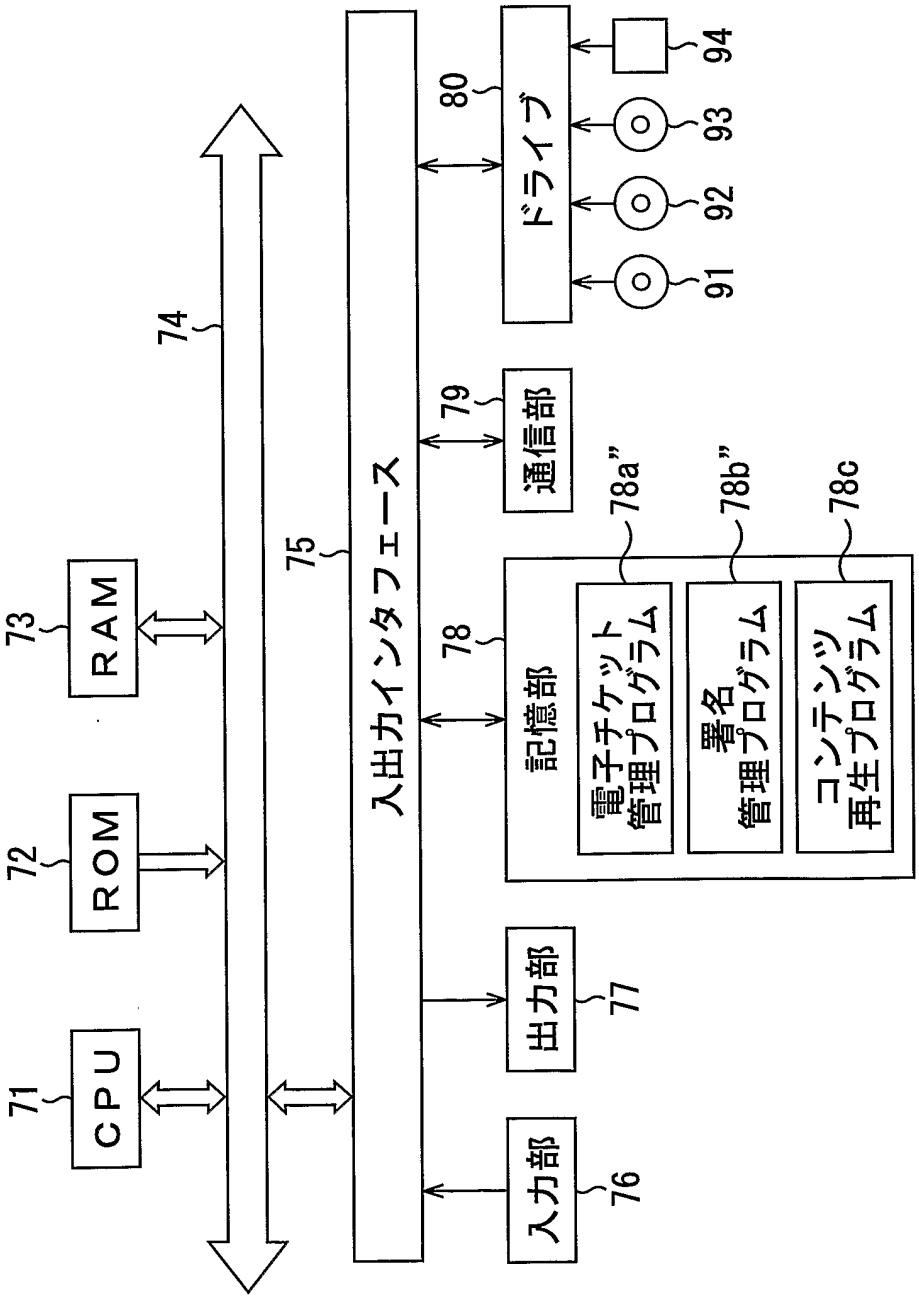

71
CPU
72
ROM
73
RAM
74
75
入出力インタフェース
76
入力部
77
出力部
78
記憶部
78a"
電子チケット管理プログラム
78b"
署名管理プログラム
78c
コンテンツ再生プログラム
79
通信部
80
ドライブ
91
92
93
94

図32

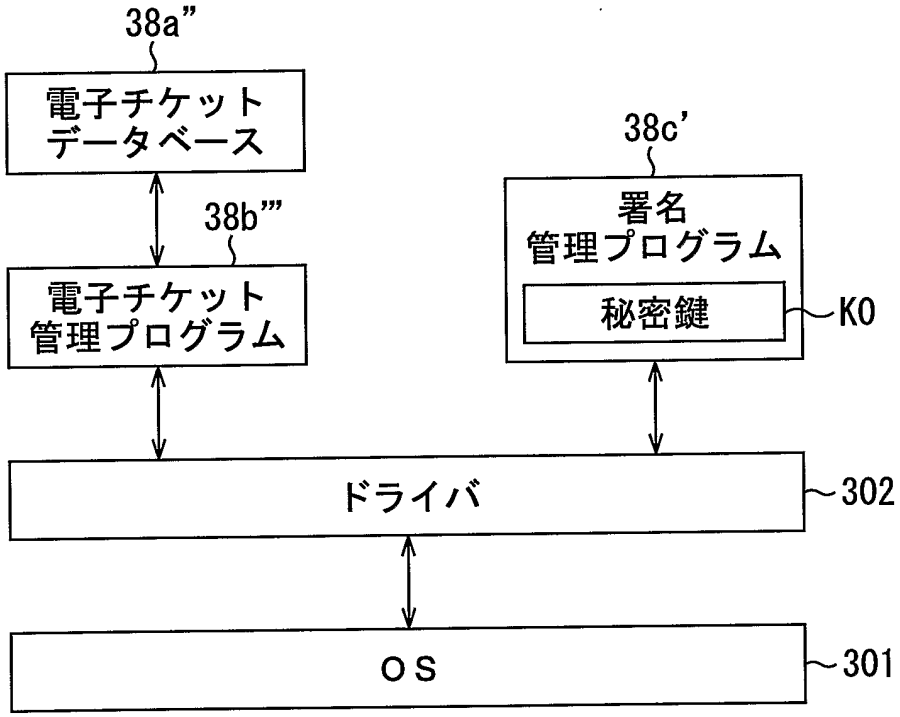

38a"
電子チケット
データベース
38b'''
電子チケット
管理プログラム
38c'
署名
管理プログラム
秘密鍵
K0
ドライバ
302
OS
301

図33

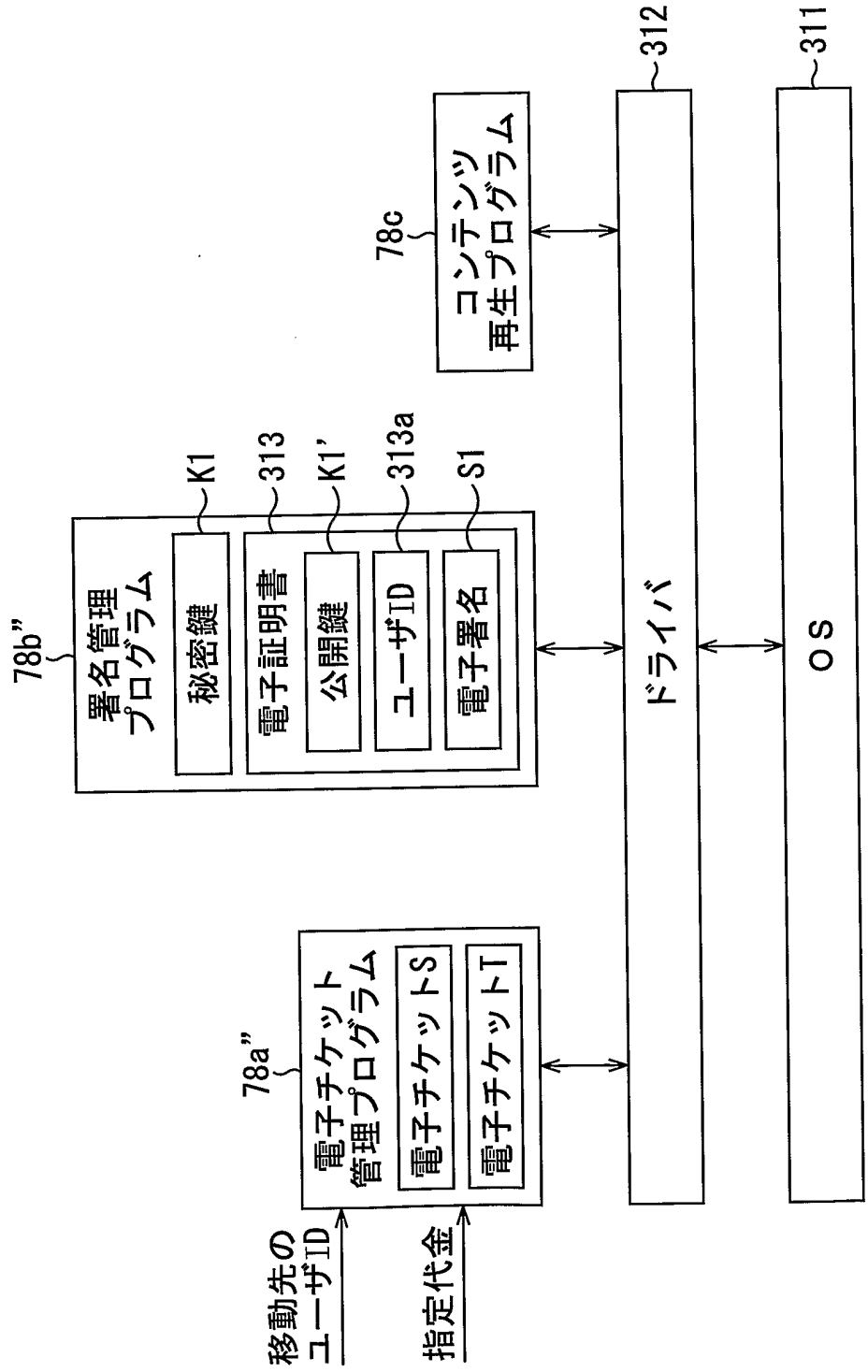

78a”
電子チケット
管理プログラム
電子チケットS
電子チケットT
78b”
署名管理
プログラム
秘密鍵
K1
電子証明書
313
公開鍵
K1’
ユーザID
313a
電子署名
S1
78c
コンテンツ
再生プログラム
ドライバ
312
OS
311
移動先の
ユーザID
指定代金

図34

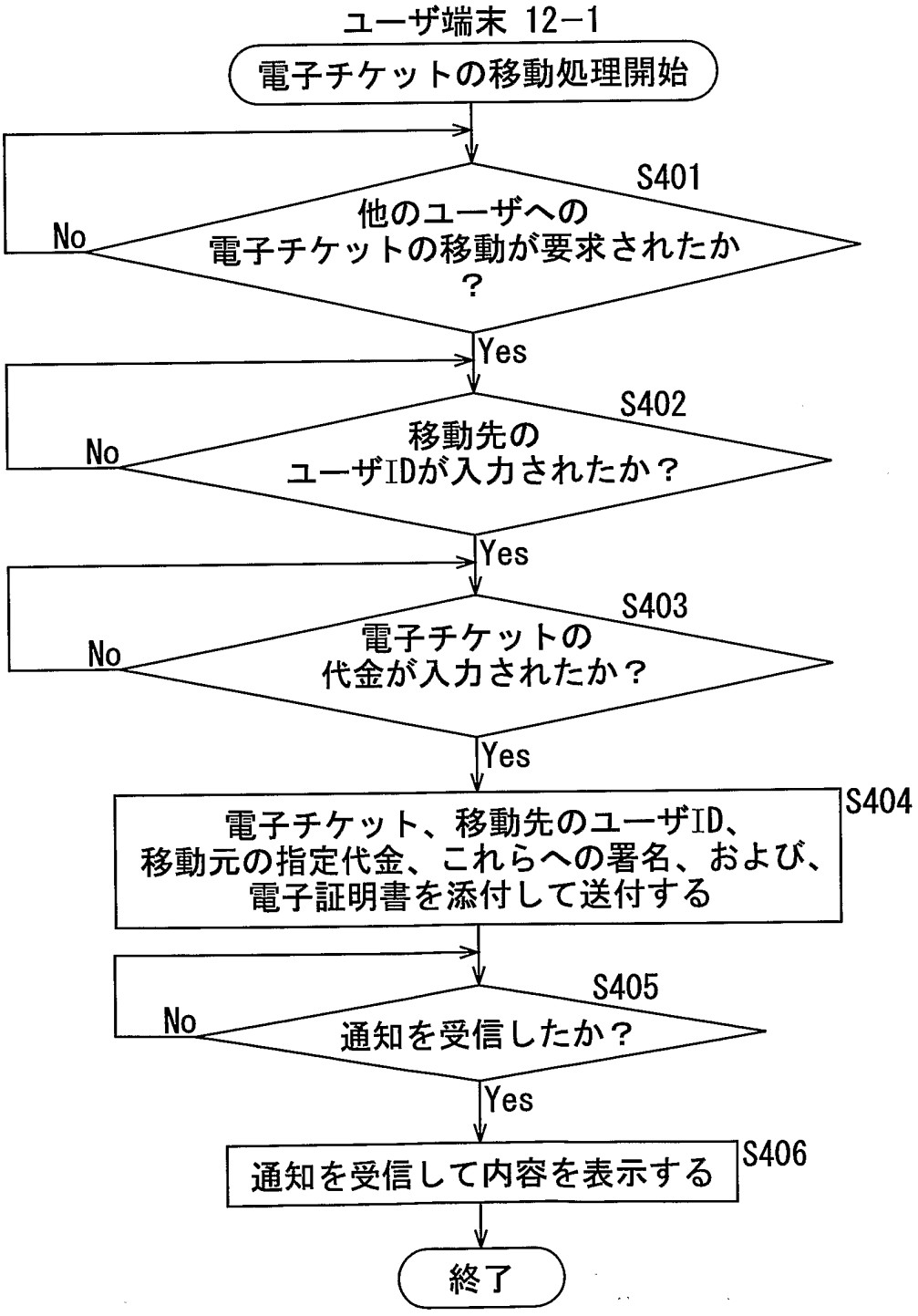

ユーザ端末 12−1
電子チケットの移動処理開始
S401
他のユーザへの
電子チケットの移動が要求されたか
？
No
Yes
S402
移動先の
ユーザIDが入力されたか？
No
Yes
S403
電子チケットの
代金が入力されたか？
No
Yes
S404
電子チケット、移動先のユーザID、
移動元の指定代金、これらへの署名、および、
電子証明書を添付して送付する
S405
通知を受信したか？
No
Yes
S406
通知を受信して内容を表示する
終了

図35

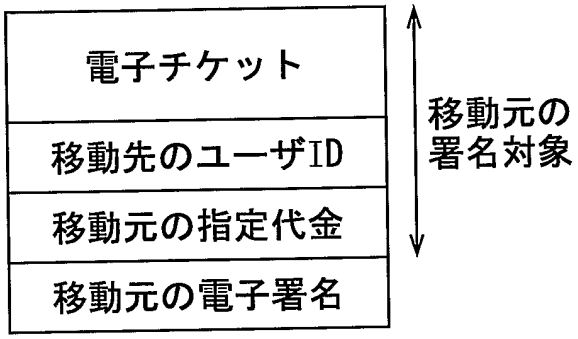


図36

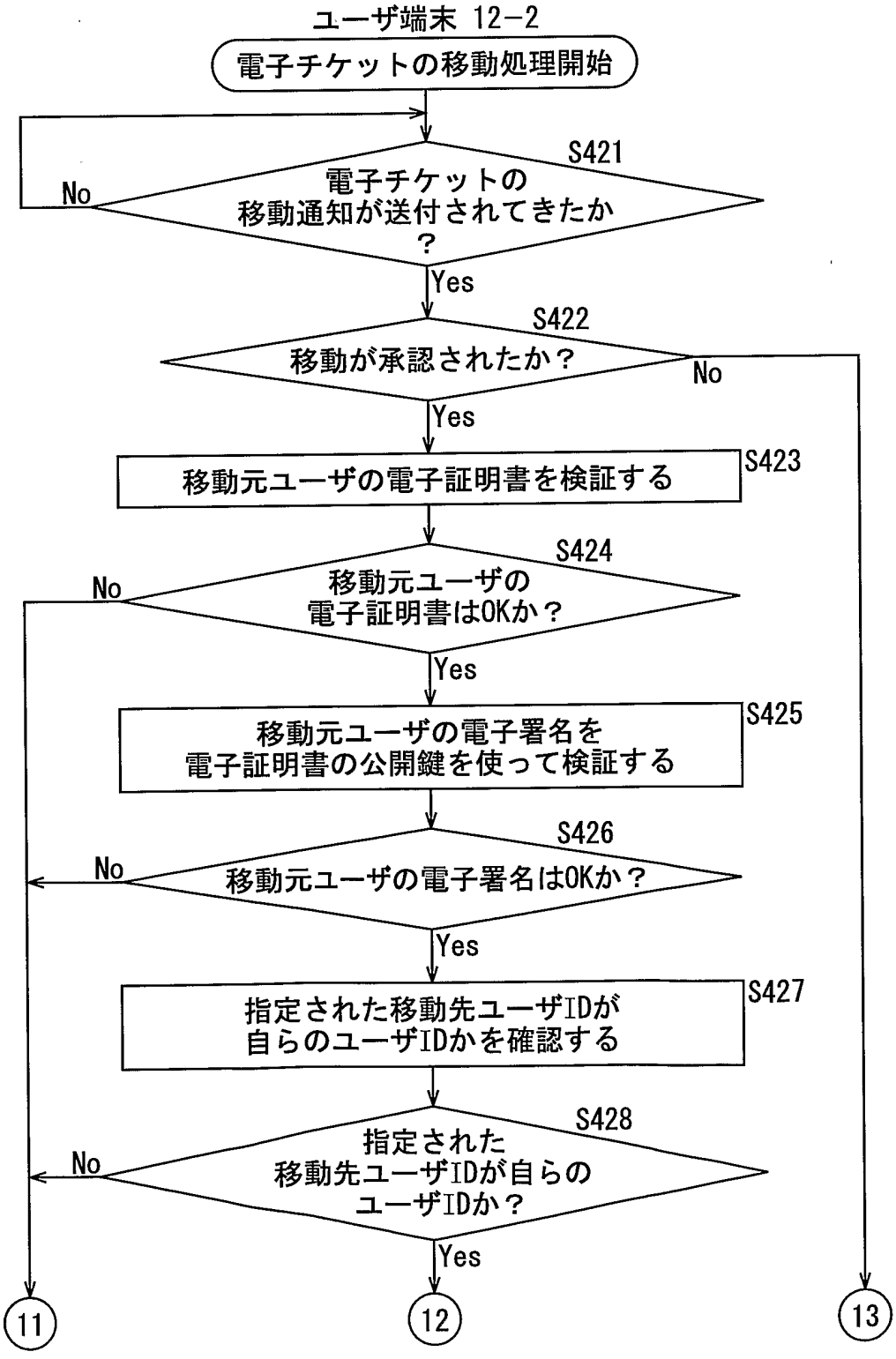

ユーザ端末 12-2
電子チケットの移動処理開始
S421
電子チケットの
移動通知が送付されてきたか
？
No
Yes
S422
移動が承認されたか？
No
Yes
移動元ユーザの電子証明書を検証する
S423
S424
移動元ユーザの
電子証明書はOKか？
No
Yes
移動元ユーザの電子署名を
電子証明書の公開鍵を使って検証する
S425
S426
移動元ユーザの電子署名はOKか？
No
Yes
指定された移動先ユーザIDが
自らのユーザIDかを確認する
S427
S428
指定された
移動先ユーザIDが自らの
ユーザIDか？
No
Yes
11
12
13

図37

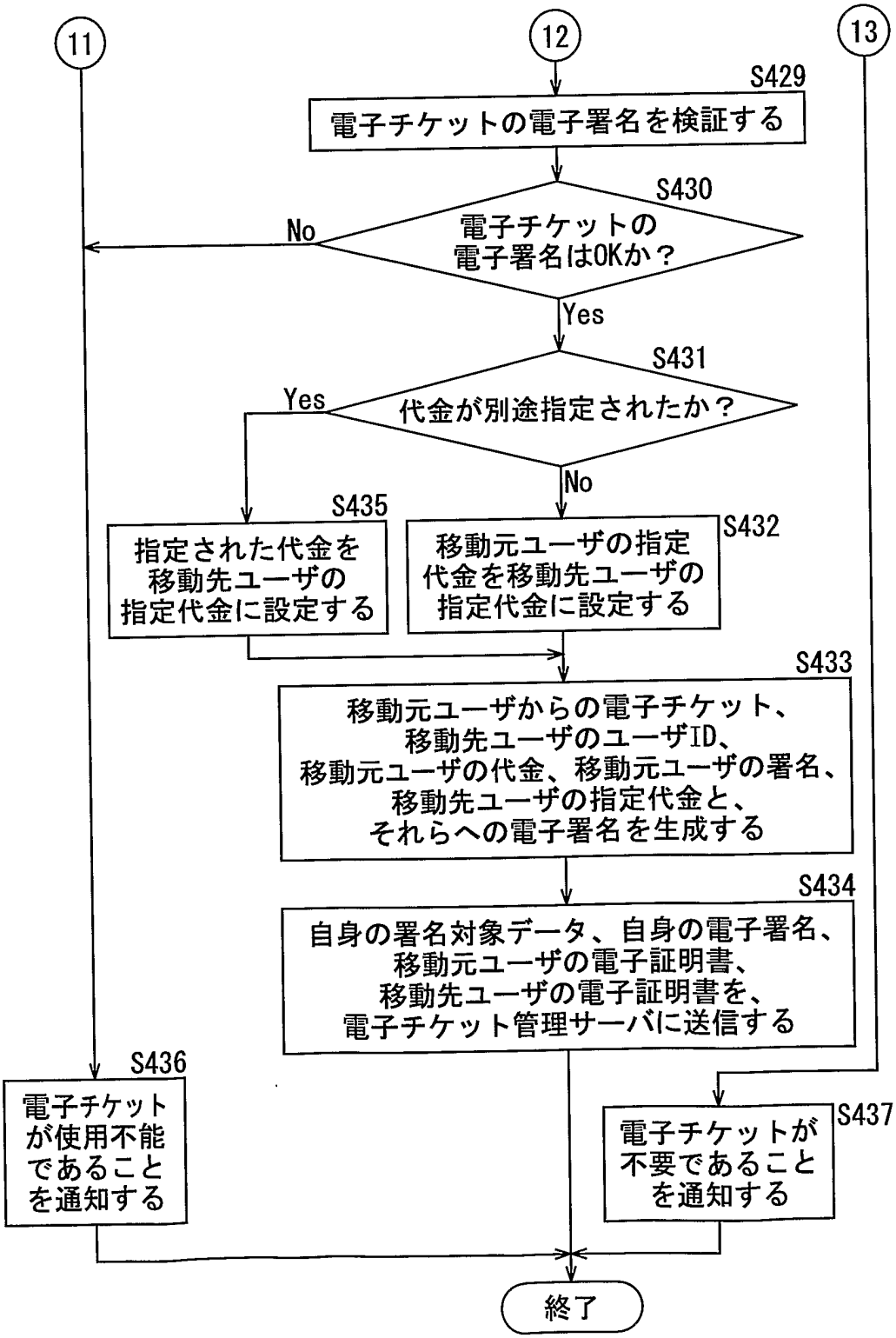

11
12
13
S429
電子チケットの電子署名を検証する
S430
電子チケットの
電子署名はOKか？
No
Yes
S431
代金が別途指定されたか？
Yes
No
S435
指定された代金を
移動先ユーザの
指定代金に設定する
S432
移動元ユーザの指定
代金を移動先ユーザの
指定代金に設定する
S433
移動元ユーザからの電子チケット、
移動先ユーザのユーザID、
移動元ユーザの代金、移動元ユーザの署名、
移動先ユーザの指定代金と、
それらへの電子署名を生成する
S434
自身の署名対象データ、自身の電子署名、
移動元ユーザの電子証明書、
移動先ユーザの電子証明書を、
電子チケット管理サーバに送信する
S436
電子チケット
が使用不能
であること
を通知する
S437
電子チケットが
不要であること
を通知する
終了

図38

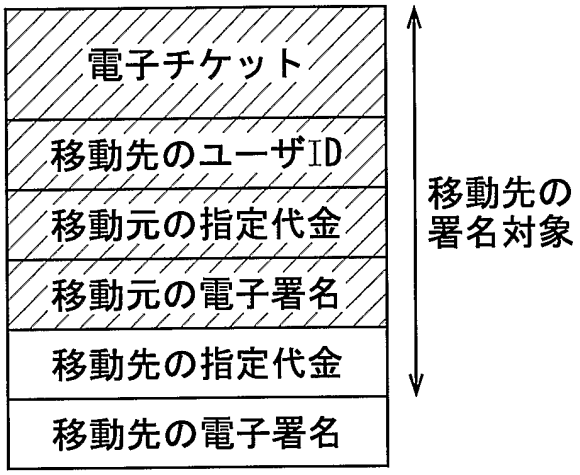

電子チケット
移動先のユーザID
移動元の指定代金
移動元の電子署名
移動先の指定代金
移動先の電子署名
移動先の
署名対象

図39

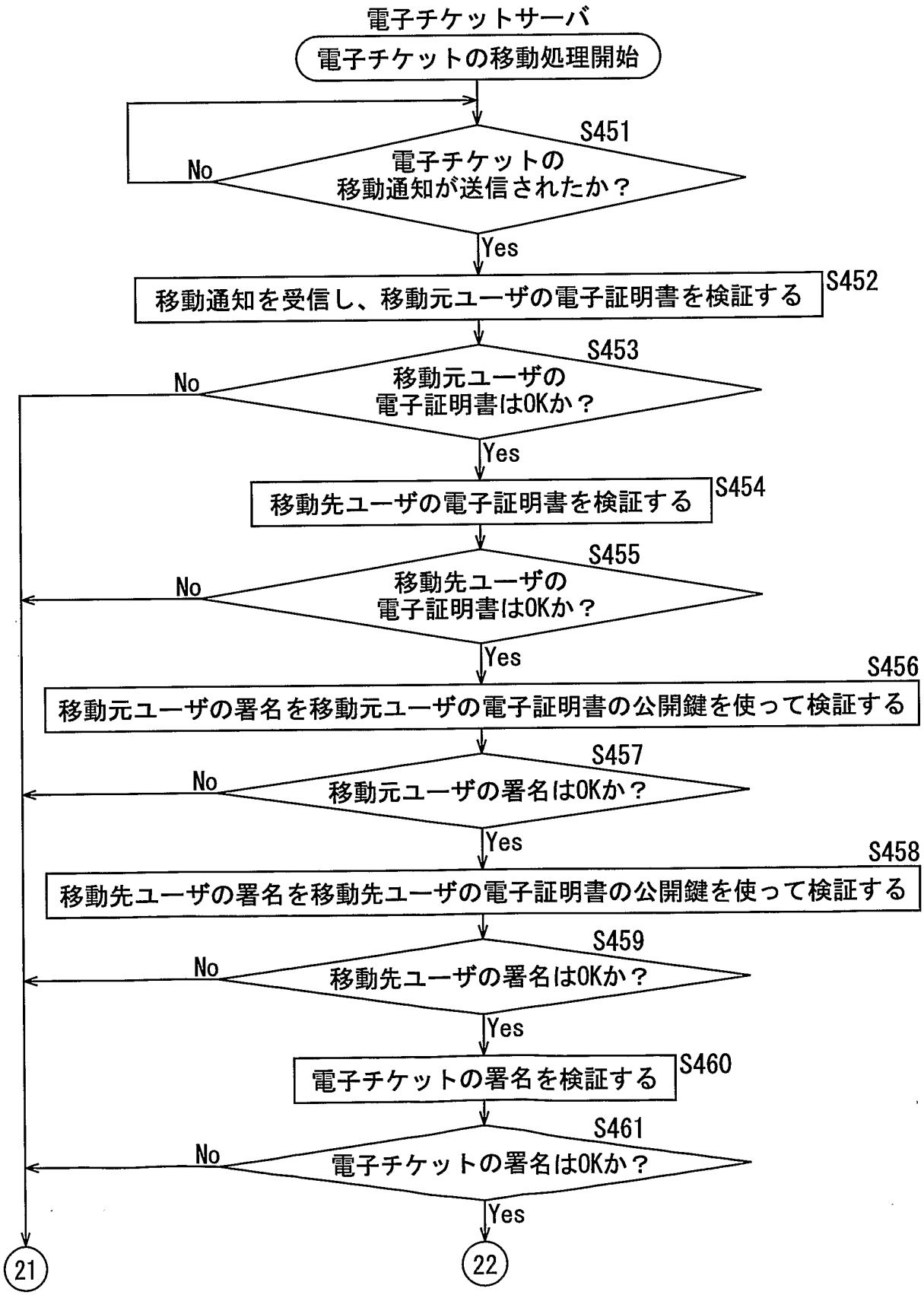

電子チケットサーバ
電子チケットの移動処理開始
S451
電子チケットの
移動通知が送信されたか？
No
Yes
移動通知を受信し、移動元ユーザの電子証明書を検証する
S452
S453
移動元ユーザの
電子証明書はOKか？
No
Yes
移動先ユーザの電子証明書を検証する
S454
S455
移動先ユーザの
電子証明書はOKか？
No
Yes
S456
移動元ユーザの署名を移動元ユーザの電子証明書の公開鍵を使って検証する
S457
移動元ユーザの署名はOKか？
No
Yes
S458
移動先ユーザの署名を移動先ユーザの電子証明書の公開鍵を使って検証する
S459
移動先ユーザの署名はOKか？
No
Yes
電子チケットの署名を検証する
S460
S461
電子チケットの署名はOKか？
No
Yes
21
22

図40

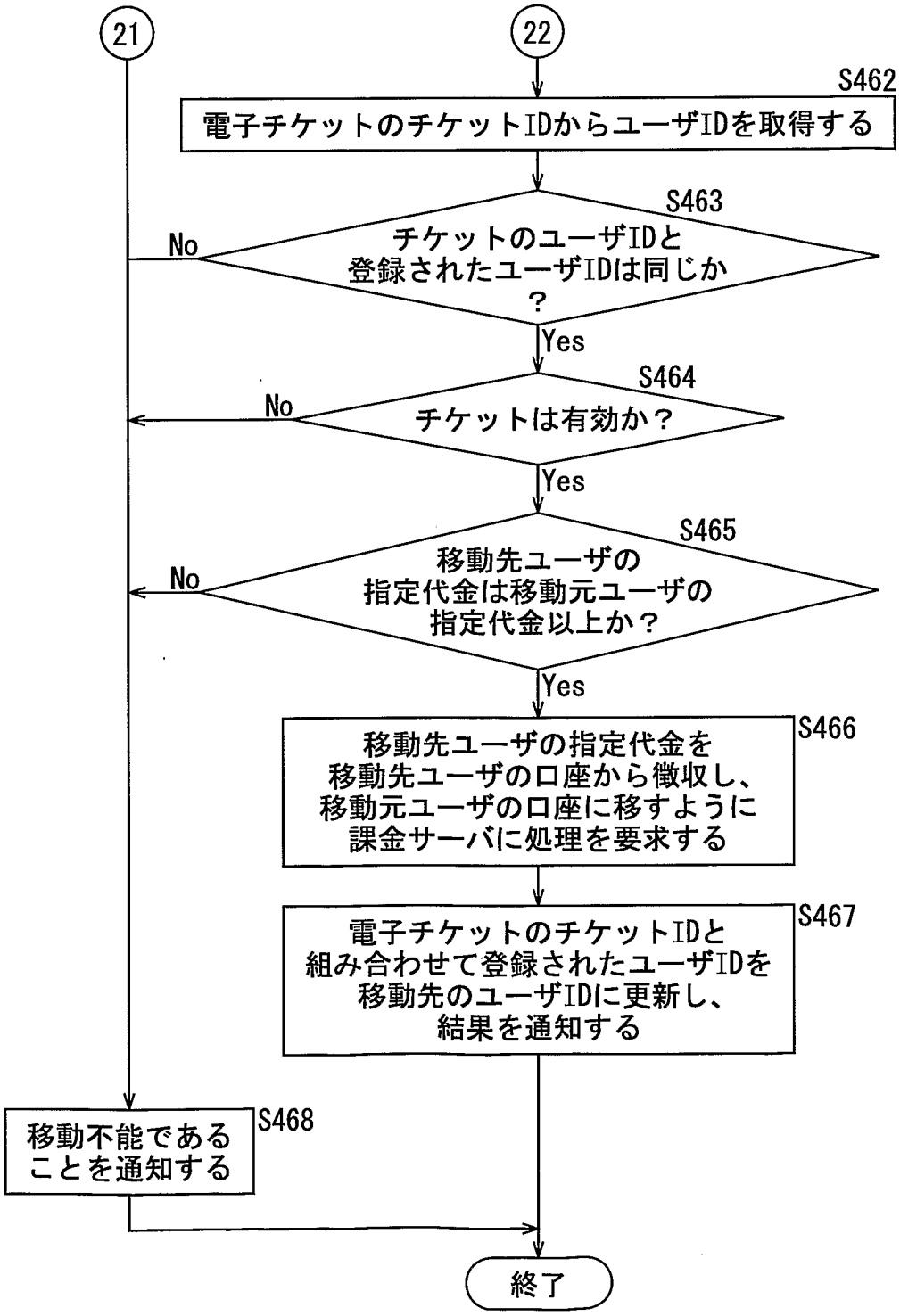
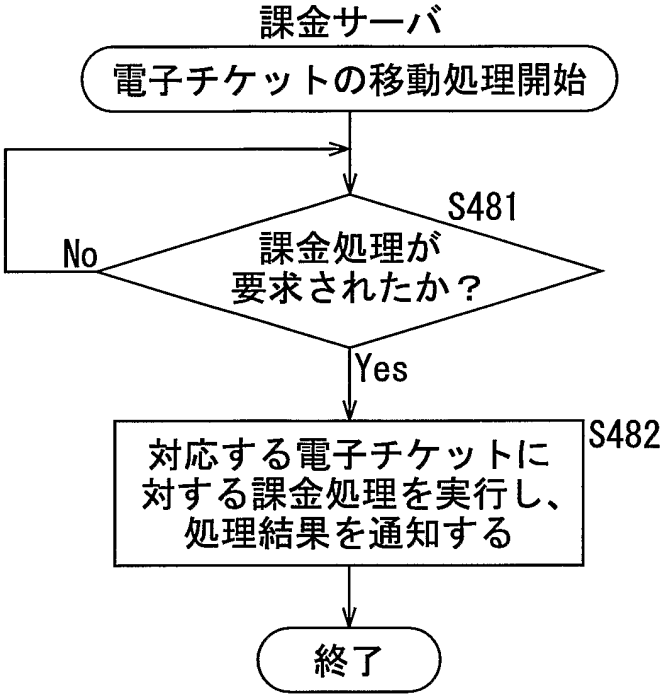

21
22
S462
電子チケットのチケットIDからユーザIDを取得する
S463
チケットのユーザIDと
登録されたユーザIDは同じか
？
No
Yes
S464
チケットは有効か？
No
Yes
S465
移動先ユーザの
指定代金は移動元ユーザの
指定代金以上か？
No
Yes
S466
移動先ユーザの指定代金を
移動先ユーザの口座から徴収し、
移動元ユーザの口座に移すように
課金サーバに処理を要求する
S467
電子チケットのチケットIDと
組み合わせて登録されたユーザIDを
移動先のユーザIDに更新し、
結果を通知する
S468
移動不能である
ことを通知する
終了

図41


課金サーバ
電子チケットの移動処理開始
S481
No
課金処理が
要求されたか？
Yes
S482
対応する電子チケットに
対する課金処理を実行し、
処理結果を通知する
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/05604

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00, 12/14, 17/60, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, 12/14, 17/60, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2003
Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/18566 A1 (Hitachi, Ltd., Tokyo), 14 February, 2002 (14.02.02), Full text; all drawings & EP 1176490 A2 & JP 2002-32344 A Full text; all drawings	1-28
A	JP 2000-209562 A (Canon Inc.), 28 July, 2000 (28.07.00), Full text; all drawings (Family: none)	1-28
A	US 2002/26581 A1 (Sony Corp.), 28 February, 2002 (28.02.02), Full text; all drawings & JP 2002-73573 A Full text; all drawings	1-28

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 May, 2003 (27.05.03)	10 June, 2003 (10.06.03)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/05604

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 9-114787 A (Nippon Telegraph And Telephone Corp.), 02 May, 1997 (02.05.97), Full text; all drawings (Family: none)	1-28
A	JP 2002-15146 A (NEC Corp.), 18 January, 2002 (18.01.02), Full text; all drawings (Family: none)	1-28
A	Hironobu YAMAMOTO et al., "Chosakuken o Hogo shita Ongaku Haishin Platform, NTT R & D", The Telecommunications Association, 10 October, 1999 (10.10.99), Vol.48, No.10, pages 762 to 769	1-28
A	Masayuki NAKAE et al., "User Yokyu ni Tekigo shita Service o Teikyo suru Capsule-ka Contents", Information Processing Society of Japan Kenkyu Hokoku (99-EIP-3), Information Processing Society of Japan, 30 January, 1999 (30.01.99), Vol.99, No.11, pages 79 to 86	1-28

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／０５６０４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Ｉｎｔ.Ｃｌ.[7]　Ｇ０６Ｆ１５／００，１２／１４，１７／６０，
Ｈ０４Ｌ９／３２

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Ｉｎｔ.Ｃｌ.[7]　Ｇ０６Ｆ１５／００，１２／１４，１７／６０，
Ｈ０４Ｌ９／３２

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　１９２２－１９９６年
日本国公開実用新案公報　　１９７１－２００３年
日本国登録実用新案公報　　１９９４－２００３年
日本国実用新案登録公報　　１９９６－２００３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	US 2002/18566 A1(Hitachi,Ltd.,Tokyo) 2002.02.14,全文,全図 & EP 1176490 A2 & JP 2002-32344 A 全文,全図	1-28
A	JP 2000-209562 A(キャノン株式会社) 2000.07.28,全文,全図(ファミリーなし)	1-28
A	US 2002/26581 A1(Sony Corporation) 2002.02.28,全文,全図 & JP 2002-73573 A 全文,全図	1-28

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２７．０５．０３	10.06.03

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	中野　裕二	５Ｂ	９４６２
	電話番号　０３－３５８１－１１０１　内線　３５４５		

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 9-114787 A(日本電信電話株式会社) 1997.05.02,全文,全図(ファミリーなし)	1-28
A	JP 2002-15146 A(日本電気株式会社) 2002.01.18,全文,全図(ファミリーなし)	1-28
A	山本 博伸ほか4名，著作権を保護した音楽配信プラットフォーム， NTT R&D，社団法人電気通信協会，1999.10.10， 第48巻 第10号，p.762-769	1-28
A	中江 政行ほか2名，ユーザ要求に適合したサービスを提供するカプセル化コンテンツ，情報処理学会研究報告(99-EIP-3)， 社団法人情報処理学会，1999.01.30，Vol.99 No.11，p.79-86	1-28