(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4181772号
(P4181772)

(45)発行日　平成20年11月19日(2008.11.19)　(24)登録日　平成20年9月5日(2008.9.5)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330D
G06F 21/24	(2006.01)	G06F	15/00	330B
G06F 13/00	(2006.01)	G06F	15/00	330F
		G06F	15/00	330G
		G06F	12/14	520A

請求項の数 8　(全 19 頁)　最終頁に続く

(21)出願番号　特願2001-367137(P2001-367137)
(22)出願日　平成13年11月30日(2001.11.30)
(65)公開番号　特開2003-167854(P2003-167854A)
(43)公開日　平成15年6月13日(2003.6.13)
審査請求日　平成16年11月15日(2004.11.15)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100090273
弁理士　國分　孝悦
(72)発明者　田頭　信博
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
(72)発明者　若尾　聡
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
(72)発明者　須賀　祐治
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

最終頁に続く

(54)【発明の名称】サービス提供装置、サービス提供方法、コンピュータ読み取り可能な記録媒体及びコンピュータプログラム

(57)【特許請求の範囲】

【請求項１】

パスワード認証方式により利用者を認証するパスワード認証手段と、

ＩＣカード認証方式により利用者を認証するＩＣカード認証手段と、

バイオメトリクス認証方式により利用者を認証するバイオメトリクス認証手段と、

前記パスワード認証手段、前記ＩＣカード認証手段、及び前記バイオメトリクス認証手段の認証結果と、前記パスワード認証手段、前記ＩＣカード認証手段、及び前記バイオメトリクス認証手段のうち、認証された認証手段の種類及び数とに応じて、前記利用者の端末装置に対して、当該利用者の端末装置におけるコンテンツの表示及び編集のアクセス制御を行うアクセス制御手段とを有し、

前記アクセス制御手段は、

前記パスワード認証手段、前記ＩＣカード認証手段、及び前記バイオメトリクス認証手段のうち、何れか１つの認証手段で認証された場合は、前記利用者の端末装置に対して、当該利用者の端末装置における前記コンテンツの表示を許可し、

前記パスワード認証手段、前記ＩＣカード認証手段、及び前記バイオメトリクス認証手段のうち、前記バイオメトリクス認証手段を含む２つの認証手段で認証された場合は、前記利用者の端末装置に対して、当該利用者の端末装置における前記コンテンツの編集を許可することを特徴とするサービス提供装置。

【請求項２】

前記アクセス制御手段は、

前記パスワード認証手段、前記ＩＣカード認証手段、及び前記バイオメトリクス認証手段のうち、前記ＩＣカード認証手段と前記パスワード認証手段とで認証され、かつ、前記バイオメトリクス認証手段で認証されなかった場合は、前記利用者の端末装置に対して、当該利用者の端末装置における前記コンテンツの編集を許可しないことを特徴とする請求項１に記載のサービス提供装置。

【請求項３】

前記アクセス制御手段は、

前記パスワード認証手段、前記ＩＣカード認証手段、及び前記バイオメトリクス認証手段のうち、何れの認証手段でも認証されなかった場合は、前記利用者の端末装置に対して、当該利用者の端末装置における前記コンテンツの表示を許可しないことを特徴とする請求項１又は２に記載のサービス提供装置。

【請求項４】

パスワード認証方式によりサービス提供装置のパスワード認証手段が利用者を認証するパスワード認証工程と、

ＩＣカード認証方式によりサービス提供装置のＩＣカード認証手段が利用者を認証するＩＣカード認証工程と、

バイオメトリクス認証方式によりサービス提供装置のバイオメトリクス認証手段が利用者を認証するバイオメトリクス認証工程と、

前記パスワード認証工程、前記ＩＣカード認証工程、及び前記バイオメトリクス認証工程の認証結果と、前記パスワード認証工程、前記ＩＣカード認証工程、及び前記バイオメトリクス認証工程のうち、認証された認証工程の種類及び数とに応じて、サービス提供装置のアクセス制御手段が、前記利用者の端末装置に対して、当該利用者の端末装置におけるコンテンツの表示及び編集のアクセス制御を行うアクセス制御工程とを有し、

前記アクセス制御工程は、

前記パスワード認証工程、前記ＩＣカード認証工程、及び前記バイオメトリクス認証工程のうち、何れか１つの認証工程で認証された場合は、前記利用者の端末装置に対して、当該利用者の端末装置における前記コンテンツの表示を許可し、

前記パスワード認証工程、前記ＩＣカード認証工程、及び前記バイオメトリクス認証工程のうち、前記バイオメトリクス認証工程を含む２つの認証工程で認証された場合は、前記利用者の端末装置に対して、当該利用者の端末装置における前記コンテンツの編集を許可することを特徴とするサービス提供方法。

【請求項５】

前記アクセス制御工程は、

前記パスワード認証工程、前記ＩＣカード認証工程、及び前記バイオメトリクス認証工程のうち、前記ＩＣカード認証工程と前記パスワード認証工程とで認証され、かつ、前記バイオメトリクス認証工程で認証されなかった場合は、前記利用者の端末装置に対して、当該利用者の端末装置における前記コンテンツの編集を許可しないことを特徴とする請求項４に記載のサービス提供方法。

【請求項６】

前記アクセス制御工程は、

前記パスワード認証工程、前記ＩＣカード認証工程、及び前記バイオメトリクス認証工程のうち、何れの認証工程でも認証されなかった場合は、前記利用者の端末装置に対して、当該利用者の端末装置における前記コンテンツの表示を許可しないことを特徴とする請求項４又は５に記載のサービス提供方法。

【請求項７】

請求項１～３の何れか１項に記載のサービス提供装置の各手段としてコンピュータを機能させることを特徴とするコンピュータプログラム。

【請求項８】

請求項７に記載のコンピュータプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、サービス提供装置、サービス提供方法、コンピュータ読み取り可能な記録媒体及びコンピュータプログラムに関し、特に、ネットワークを介してユーザに種々のサービスを提供するために用いて好適なものである。
【０００２】
【従来の技術】
インターネットに代表されるネットワークインフラの普及に伴い、ネットワークを利用したサービスが多く提供されるようになった。anonymous ftpに代表されるようにユーザ認証を伴わないサービスもあるが、telnetやrloginのようにユーザ認証を伴うサービスも多く存在する。このような背景のもと、パスワード、 ICカードやバイオメトリクス等様々なユーザ認証が実現されている。
【０００３】
例えば、銀行のCDやATMの利用時におけるパスワードの利用、telnetやrlogin等におけるパスワード利用などがある。また、ICカードを利用して建物への入退出管理や計算機への認証等が利用されている。さらに、高度な機密保持が必要な建物への入退出管理には指紋認証や網膜認証といったバイオメトリクス技術も利用されている。
【０００４】
一方、情報機器の発展と普及により、様々なコンテンツがデジタル化して利用されるようになった。コンテンツがデジタル化されたことにより、コンテンツの配信形態も多様化してきた。
【０００５】
このように多様化したコンテンツの配信形態は、CD-ROM、DVD-ROM等に代表されるようなデジタル記憶媒体を利用したメディア型配信と、インターネットを利用したコンテンツ配信に代表されるようなネットワーク型配信に分類することができる。
【０００６】
また、情報機器の高機能化によって取り扱われるコンテンツの品質が高くなり、コンテンツの品質が高くなることによってコンテンツの経済的価値が向上し、その結果としてコンテンツ保護が重要視されるようになった。
【０００７】
このようなコンテンツの保護対策として、上記メディア型配信においては、保護機能を付加したメディアを利用したセキュアなコンテンツ配信が実現されている。
【０００８】
具体的には、DVDプレイヤーやメモリースティック（登録商標）やSDカードのように、ハードウエア的に読み出しや書き込み等の制限を行うことにより暗号化鍵を管理したり、ハードウエア的に暗号化処理を実現してコンテンツの保護と機器の認証を行ったりして、保護機能を実現している。
【０００９】
また、上記ネットワーク型配信においては、i-mode（登録商標）に代表されるようにネットワークインフラに依存した形でのセキュアなコンテンツ配信が実現されている。
【００１０】
【発明が解決しようとする課題】
しかしながら、現在、利用されているユーザ認証方法では、各サービスに対して固定の認証方法だけしか提供されていない。
【００１１】
例えば、telnetやrloginのユーザ認証は、簡便なパスワードによる認証が用いられている。また、高度に機密保持が必要な建物への入退出管理のためのユーザ認証は、高度な認証技術であるバイオメトリクスによる認証が用いられている。
【００１２】

また、それぞれの認証方法に関しても、簡便であるか、または厳密な認証であるかの差はあるが、認証結果としては「可」または「不可」の二通りしか提供していない。このため、認証結果に応じて「サービスを提供する」または「サービスを提供しない」の二通りの判断しか行えなかった。

【００１３】

しかし、今後はユーザ端末の多様化から段階的なサービスの提供が考えられる。例えば、画像を閲覧するサービスに関して、高解像度の画像を表示可能な自宅のパーソナルコンピュータ（PC）からサービスを享受する場合と、低解像度であって、場合によっては二値画像しか表示できない携帯端末からサービスを享受する場合とでは、同じサービスでもサービスの品質にレベルが生じると考えられる。

【００１４】

また、別の例として、機密文書を閲覧するサービスに関して、社内から社内の機密文書にアクセスする場合等、地理的に安全な場所に位置する端末からサービスを享受する場合と、社外から社内の機密文書にアクセスする場合等、地理的に安全でない場所に位置する端末からサービスを享受する場合とでは、同じサービスでもサービスの機密度合いにレベルがあると考えられる。

【００１５】

しかし、従来の各サービスに対する固定の認証方法だけでは、前述したような段階的なサービス提供等の様々なサービス提供形態に適応的に対応できないという問題があった。

【００１６】

さらに、利用者の利用端末は、パーソナルコンピュータ（PC）、携帯端末といった様々な端末がある。この場合、例えば、低解像度の画像しか表示できない携帯端末に対して高解像度の画像を提供するというように過剰にサービスを提供してしまう可能性があった。

【００１７】

このような過剰なサービスは、有限であるネットワークの帯域と有限である利用端末の計算機資源の双方において、非常に無駄であり、非効率的であるという問題があった。

【００１８】

本発明は、上述の実情に鑑みてなされたものであり、ユーザの認証結果にレベルを持たせるようにすることを目的とする。

【００１９】

【課題を解決するための手段】

本発明のサービス提供装置は、パスワード認証方式により利用者を認証するパスワード認証手段と、ＩＣカード認証方式により利用者を認証するＩＣカード認証手段と、バイオメトリクス認証方式により利用者を認証するバイオメトリクス認証手段と、前記パスワード認証手段、前記ＩＣカード認証手段、及び前記バイオメトリクス認証手段の認証結果と、前記パスワード認証手段、前記ＩＣカード認証手段、及び前記バイオメトリクス認証手段のうち、認証された認証手段の種類及び数とに応じて、前記利用者の端末装置に対して、当該利用者の端末装置におけるコンテンツの表示及び編集のアクセス制御を行うアクセス制御手段とを有し、前記アクセス制御手段は、前記パスワード認証手段、前記ＩＣカード認証手段、及び前記バイオメトリクス認証手段のうち、何れか１つの認証手段で認証された場合は、前記利用者の端末装置に対して、当該利用者の端末装置における前記コンテンツの表示を許可し、前記パスワード認証手段、前記ＩＣカード認証手段、及び前記バイオメトリクス認証手段のうち、前記バイオメトリクス認証手段を含む２つの認証手段で認証された場合は、前記利用者の端末装置に対して、当該利用者の端末装置における前記コンテンツの編集を許可することを特徴とする。

【００２０】

本発明のサービス提供方法は、パスワード認証方式によりサービス提供装置のパスワード認証手段が利用者を認証するパスワード認証工程と、ＩＣカード認証方式によりサービス提供装置のＩＣカード認証手段が利用者を認証するＩＣカード認証工程と、バイオメトリクス認証方式によりサービス提供装置のバイオメトリクス認証手段が利用者を認証する

バイオメトリクス認証工程と、前記パスワード認証工程、前記ＩＣカード認証工程、及び前記バイオメトリクス認証工程の認証結果と、前記パスワード認証工程、前記ＩＣカード認証工程、及び前記バイオメトリクス認証工程のうち、認証された認証工程の種類及び数とに応じて、サービス提供装置のアクセス制御手段が、前記利用者の端末装置に対して、当該利用者の端末装置におけるコンテンツの表示及び編集のアクセス制御を行うアクセス制御工程とを有し、前記アクセス制御工程は、前記パスワード認証工程、前記ＩＣカード認証工程、及び前記バイオメトリクス認証工程のうち、何れか１つの認証工程で認証された場合は、前記利用者の端末装置に対して、当該利用者の端末装置における前記コンテンツの表示を許可し、前記パスワード認証工程、前記ＩＣカード認証工程、及び前記バイオメトリクス認証工程のうち、前記バイオメトリクス認証工程を含む２つの認証工程で認証された場合は、前記利用者の端末装置に対して、当該利用者の端末装置における前記コンテンツの編集を許可することを特徴とする。

【００２１】

本発明のコンピュータプログラムは、前記記載のサービス提供装置の各手段としてコンピュータを機能させることを特徴とする。

【００２２】

本発明のコンピュータ読み取り可能な記録媒体は、前記記載のコンピュータプログラムを記録したことを特徴とする。

【００２３】

【発明の実施の形態】

次に、添付の図面を参照しながら本発明のサービス提供装置、サービス提供方法、コンピュータ読み取り可能な記録媒体及びコンピュータプログラムの実施の形態について説明する。

【００２４】

図１は、本実施の形態のネットワークシステムの構成の一例を示した図である。

【００２５】

本実施の形態のネットワークシステムは、図１に示すように、サービス提供装置として配設されているサービス提供サーバ１１と、ユーザ１２とが、ネットワーク１３を介して互いに通信可能なように接続された構成としている。

【００２６】

なお、図１では、ネットワーク１３に対して、それぞれ１つのサービス提供サーバ１１、及びユーザ１２を接続するように構成しているが、これらの接続数は１つに限られることはなく、複数のサービス提供サーバ、及び複数のユーザを接続することも可能である。

【００２７】

本実施の形態のネットワークシステムにおけるサービスとは、キャラクタデータ、音声データまたは音楽データ（以下、音声/音楽データと表す）、静止画像データ、動画像データ、及びプログラム等のコンテンツを利用したサービス全般を指す。

【００２８】

例えば、音楽データ配信等に代表されるコンテンツの配信、画像データや音楽データ等の放送に代表されるコンテンツを利用した視聴サービス、及びアプリケーションサービスプロバイダによって提供されているプログラムの利用等を含む様々なアプリケーションサービスを指す。

【００２９】

また、これらのサービスは、ユーザ１２へ提供する時にサービスにレベルを持たせることが可能である。このサービスのレベルとしての要素は様々なものが考えられる。

【００３０】

例えば、音声/音楽データのコンテンツ配信サービスの場合には、配信する音声/音楽データの音質を変化させることでサービスにレベルを持たせることが可能である。また、画像データの配信サービスの場合には、配信する画像データの画質を変化させることでサービスにレベルを持たせることが可能である。

【００３１】
そして、音声/音楽データや動画像データの配信サービスの場合には、視聴可能な時間を変化させることでサービスにレベルを持たせることも可能である。さらに、プログラム利用のサービスの場合、利用可能な機能を制限することや、プログラムで利用できるコンテンツを制限することでサービスにレベルと持たせることが可能である。
【００３２】
また、本実施の形態のネットワークシステムにおいて、ユーザ１２が利用する端末には、機種番号等の機種を示す情報や、端末の属性を示す情報等の端末の持つ情報に対して、これらの情報の正当性を示す情報が付加されていることを特徴とする。
【００３３】
今後、ネットワーク１３を介して様々なサービスが提供され、課金処理等が行われることを考えると、各々の端末を確実に特定する必要性が生じる。また、悪意のあるユーザの悪意の行為も次第に高度になり、端末の持つ情報の改変の恐れもある。
【００３４】
そこで、これらの対策のために、端末のもつ情報（ユーザ１２の利用環境に関する情報）の正当性を示す情報を付加することが考えられる。
【００３５】
上記正当性を示す情報としては、デジタル署名が考えられ、例えば、あらかじめ端末製造時に製造メーカが機種番号に対するデジタル署名を機種番号と共に端末に付加しておく。これにより、製造メーカによってユーザ１２の利用環境に関する利用状況情報の正当性が保証されることを可能にする。
【００３６】
なお、上記正当性を示す情報としてデジタル署名を用いる方法は一例であって、正当性を示す情報は、これだけに限定しているわけでなく、例えば端末によって異なるユニークなシリアル番号であってもよい。
【００３７】
本実施の形態のネットワークシステムの基本方針は、図２に示すように、「サービス提供サーバ１１に対して、サービス提供サーバ１１の入り口における第１のアクセス制御とサービス提供サーバ１１の出口における第２のアクセス制御を行う」ことである。
【００３８】
ここで、上記アクセス制御するとは、コンテンツやサービスの流通を許可したり不許可としたり、またコンテンツやサービスの利用を制御したりすることを意味する。
【００３９】
サービス提供サーバ１１の入り口における第１のアクセス制御手段（ユーザアクセス制御手段）は、サービスを受けるためのユーザ認証時において、認証結果にレベルを持たせ、かつ、このレベルを持った認証結果に基づいてサービス提供サーバ１１へのアクセス制御を行うことであって、下記の認証手段と判断手段とによって実現されている。
【００４０】
また、サービス提供サーバ１１の出口における第２のアクセス制御手段（サービス提供手段）は、サービス提供時において、ユーザの利用環境に基づいて、提供するサービスの内容を段階的に制御することであって、下記の検証手段と変換手段によって実現されている。
【００４１】
次に、本実施の形態のサービス提供サーバ１１について詳細に説明する。図３に、サービス提供サーバ１１の構成の一例を示すブロック図を示す。
【００４２】
図３において、サービス提供サーバ１１は、受付手段１４と、少なくとも１つ以上の認証手段１５と、判断手段１６と、検索手段１７と、検証手段１８と、変換手段１９と、提供手段２０とを有している。
【００４３】

受付手段１４は、ユーザ１２からのサービス提供依頼を受け付ける。上記サービス提供依頼は、提供してもらいたいサービス情報を含むサービス提供依頼情報を含む。

【００４４】

また、上記サービス情報は、サービスを受けるための情報であって、例えば画像コンテンツの配信サービスの場合では、受信したい画像コンテンツの識別情報であったり、音声/音楽コンテンツの配信サービスの場合では、受信したい音声/音楽コンテンツの識別情報であったりする。

【００４５】

また、ソフトウェア利用のサービスの場合では、上記サービス情報は、ソフトウェアの識別情報、ソフトウェアの機能の識別情報、及びソフトウェアが扱うコンテンツの識別情報のうち、少なくとも１つを含む情報である。

【００４６】

図４は、音楽配信サービスを依頼する場合のサービス提供依頼情報の一例を示した図であって、上記サービス情報は、曲名や曲のスタート位置や演奏の繰り返し回数等から構成される。

【００４７】

図３に戻り、受付手段１４は、上記サービス提供依頼情報とユーザ１２に関する情報を判断手段１６へ送る。

【００４８】

判断手段１６は、上記サービス提供依頼情報とユーザ１２に関する情報を受け取り、必要に応じて、認証手段１５に認証を依頼する。そして、認証手段１５による認証結果から最終的な認証判断結果を決定し、上記サービス提供依頼情報と共に検索手段１７へ送る。なお、認証判断結果の決定方法については、後述する。

【００４９】

認証手段１５は、判断手段１６からの認証依頼に基づいて、ユーザ認証処理を実行する手段であって、複数の手段から構成されることも可能である。

【００５０】

この認証手段１５による認証方式は、例えば、ユーザ１２からパスワードを受け付け、サービス提供サーバ１１内に秘密に保管しているパスワードと比較し、一致した場合だけ正しく認証されたと判断するパスワード認証方式や、ユーザが保有しているICカードを利用し、ICカードが正しく認証された場合に認証されたと判断するICカード認証方式や、指紋、声紋、網膜パターン等の生体情報を利用したバイオメトリクス認証方式などが適応可能である。

【００５１】

ただし、本実施の形態のサービス提供サーバ１１では、利用する認証方法は上述した方法に特に限定されない。

【００５２】

認証時に認証手段１５が利用する認証情報は、認証時に認証手段５が直接得ることが可能である情報である。この場合、例えば、パスワード認証方式では、パスワードを入力する手段が必要になるし、ICカード認証方式ではICカードにアクセスする手段が必要になるし、バイオメトリクス認証方式ではバイオメトリクスを読み取るセンサが必要になるといったように、各々の認証方式に対応した手段が必要になる。しかし、本実施の形態のサービス提供サーバ１１は、上記個々の認証方式に依存した手段を限定しない。

【００５３】

また別の方法としては、上記サービス提供依頼情報に認証情報を含める方法も可能である。

【００５４】

図５に、音楽配信サービスを依頼する場合であって、認証手段５がパスワード認証方式の場合におけるサービス提供依頼情報の一例を示す。

【００５５】

図５に示すように、サービス提供依頼情報５０は、図４に示したサービス情報４０に加えて、パスワード認証に必要なパスワードに関する情報から構成される。

【００５６】

なお、上記パスワードに関する情報は、パスワード認証方式に依存して、そのままのパスワード情報であったり、暗号化等変換されたパスワード情報であったりする。

【００５７】

そして、最終的な認証判断結果の決定は、上記した１つ以上の認証手段１５の認証結果から行う。例えば、パスワードと、ICカードと、指紋の３種類の認証方法を利用した場合の認証状態を図６に示す。図６の各頂点は認証後の状態を表し、各枝は認証された場合の動作を表す。

【００５８】

つまり、図６において、頂点０は全ての認証に失敗している状態を表し、頂点１はパスワードだけで認証されている状態を表し、頂点２はICカードだけで認証されている状態を表し、頂点３は指紋だけで認証されている状態を表し、頂点４はパスワードとICカードで認証されている状態を表し、頂点５はパスワードと指紋で認証されている状態を表し、頂点６は指紋とICカードで認証されている状態を表し、頂点７はパスワードとICカードと指紋の全てで認証されている状態を表す。

【００５９】

初期状態では、頂点０の状態に位置し、パスワードによる認証に成功した場合、頂点１の状態へ移行する。さらに、頂点１の状態からICカードによる認証に成功した場合、頂点４の状態へ移行する。

【００６０】

以上に例示したように、本実施の形態のサービス提供サーバ１１に備えられている判断手段１６は、複数の認証手段１５による認証結果に基づいて、ユーザの認証状態を決定する。そして、判断手段１６は、ユーザ１２の認証状態に応じて、ユーザ１２の認証レベルを決定する。

【００６１】

検索手段１７は、サービスに必要なコンテンツを保管しているサービスデータベースを検索可能であって、上記認証判断結果とサービス情報に基づいてサービスデータベースからサービスデータ、つまりサービスに必要な全てのコンテンツを検索する。

【００６２】

そして、検索したサービスデータを上記サービス提供依頼情報と共に変換手段９へ送る。図３では、検索手段１７とサービスデータベースは同一のサービス提供サーバ１１内に構成されているように表記している。しかし、検索手段１７は上記サービスデータベースを検索可能であれば十分なので、ネットワーク１３を介して別のサーバに構成されているサービスデータベースを検索する場合も考えられる。

【００６３】

上記サービスデータベースは、コンテンツとサービスを保管し、さらには認証判断結果とサービスに対応したアクセス制御リストを保管し、上記認証判断結果とサービス情報からアクセス制御リストに従ってサービス提供を制御する。つまり、上記アクセス制御リストは、認証判断結果とコンテンツと動作からなる、３次元的な構成をなすリストとなる。

【００６４】

図１２に、パスワードとICカードと指紋の３つの認証方法を利用した場合であって、コンテンツが画像コンテンツである場合のアクセス制御リストの一例を示す。

【００６５】

図１２において、縦軸は認証判断手段１６の判断結果である。つまり、例では、パスワードとICカードと指紋の３つの認証方法を用いた場合であるので、上述の図６に示した認証状態遷移が想定可能であり、それらの認証状態を縦軸とした。

【００６６】

また、横軸は、画像コンテンツに対する多様化したサービスの例であって、低解像度と高

解像度のコンテンツに対して、それぞれ表示と編集の動作を例示している。

【００６７】

ただし、これらのサービスが画像コンテンツに対する全てのサービスではなく、「中解像度のコンテンツを印刷する」といった他にも様々なサービスが存在する。

【００６８】

さらに図１２に記した記号「○」はサービスの提供を許可することを表し、記号「×」はサービスの提供を許可しないことを表す。

【００６９】

図１２に示すように、本実施の形態のサービス提供サーバ１１では、認証判断の結果、つまり図６に示した頂点の位置によって、アクセス制御を決定することを第１の特徴とする。

【００７０】

ただし、上記アクセス制御リストの生成方法に関しては特に制限しない。このことは、例えば、図１３に示すようなアクセス制御リストを生成することにより、全ての認証方式で認証されない限り、サービスが提供されないといった最も強固なユーザ認証を実現することも可能にする。

【００７１】

また、図１４に示すように、例えば、いずれか１つの認証手段１５で認証された場合は、表示に関する利用が全て可能になり、いずれか２つの認証手段１５で認証された場合は、編集に関する利用も全て可能になるといったアクセス制御リストを生成することも可能である。

【００７２】

この場合、全ての認証手段１５によって認証されなくても、１つの認証手段５または２つの認証手段１５によって補うことが可能となっており、認証手段５の紛失や盗難等の認証情報の保管に関する信頼性を向上させることを可能にする。

【００７３】

また、セキュリティを考慮したシステムにおいては、ICカードを利用したシステムが実用化されている。このことからICカードの利用を前提とするシステム設計が要求されることが考えられるが、本実施の形態のサービス提供サーバ１１においては、図１５に示したアクセス制御リストを生成することにより、上記要求を実現可能とする。

【００７４】

図１５は、ICカードで認証されたことを含む認証状態である、状態２（図６における頂点２）と、状態４（図６における頂点４）と、状態６（図６における頂点６）と、状態７（図６における頂点７）においては、サービス全てを利用することが可能であるが、他の認証状態ではサービスが利用できないという制御を可能にする。

【００７５】

さらに、図１４に示した手法を用いることにより、ICカードがない場合でも、単一または複数のICカード以外の認証手段１５を用いて、ICカード認証と同等のサービスを提供することも可能である。

【００７６】

変換手段１９は、サービス提供依頼情報とサービスデータを受け取り、必要に応じて、検証手段１８に検証を依頼する。そして、検証手段１８による検証結果に基づいて、サービスデータを変換し、変換後のサービスデータを提供手段２０へ送る。サービスデータの変換方法については後述する。

【００７７】

検証手段１８は、変換手段１９からの検証要求を受け付け、検証処理を実行する手段である。上記検証処理は、ユーザの利用状況に関する利用状況情報の検証であって、利用状況情報と検証情報を用いて検証を行う。

【００７８】

上記利用状況情報は、ユーザ端末の機種番号であったり、端末の所在地であったり、端末

の接続状態を表す情報であったり、それらの組み合わせであったりする。

【００７９】

また、上記検証情報は、上述した利用状況情報の正当性を示す情報であって、例えばデジタル署名で実現可能である。

【００８０】

上記利用状況情報と検証情報は、１つ以上であって、ユーザ及び第三者のうちの少なくとも何れか一方から得る。これらの情報を得る方法は、検証時に検証手段１８が直接得る方法や、サービス提供依頼情報に利用状況情報と検証情報を含める方法も可能である。

【００８１】

音楽配信サービスを依頼する場合のサービス提供依頼情報の一例を図７に示す。

図７に示すように、サービス提供依頼情報７０は、図４に示したサービス情報４０に加えて、端末の機種番号、端末の表示能力に関する情報、端末の再生音質能力に関する情報、端末の位置情報等の利用状況情報と、利用状況情報の検証情報であるデジタル署名から構成される。

【００８２】

ユーザ１２の利用状況情報の正当性の検証方法は、上記検証情報に依存する。また、１つ以上の利用状況情報とこれに対する検証情報を受け取った場合の正当性の判断方法は、全ての利用状況情報の正当性が正当であると検証した場合に正当であると判断したり、過半数の利用状況情報の正当性が正当であると検証した場合に正当であると判断したりと、様々な正当性の判断方法が考えられるが、本実施の形態のサービス提供サーバ１１は、利用状況情報の正当性の判断方法を特に限定しない。

【００８３】

例えば、利用状況情報としてユーザの端末の機種番号を利用し、検証情報としてそれらのデジタル署名を利用する場合は、機種番号に対するデジタル署名を検証することにより、製造メーカによって利用状況情報の正当性が保証されることを可能にする。

【００８４】

上記サービスデータの変換方法とは、利用状況情報と検証結果に応じて、全てまたは一部のサービスデータ、つまりサービスに必要な全てまたは一部のコンテンツを変換して、サービスのレベルを変換することである。

【００８５】

例えば、コンテンツが画像である場合は、解像度の変換や色数の変換であったり、またコンテンツが音声/音楽である場合は、ビットレートの変換であったりする。

【００８６】

利用状況情報と検証結果に応じてサービスを変換するとは、例えば、「静止画像コンテンツを表示する」というサービスに対して、正当な「二値画像、縦１６０ピクセル、横１６０ピクセルを表示可能な携帯端末」という利用状況情報である場合の変換は、「二値画像、縦１６０ピクセル、横１６０ピクセルの静止画像コンテンツを表示する」といったように、利用環境に最適なサービスデータを決定する。

【００８７】

上記利用環境に最適なサービスを決定するための要因であるユーザ１２の利用環境に関する情報としては、利用端末の処理能力、利用端末の画像表示能力、利用端末の音声再生能力や音楽再生能力、コンテンツの送信速度、利用端末の印刷に関する情報、利用端末に接続されている周辺機器に関する情報、利用端末のネットワーク１３に関する情報等、様々なものが考えられる。

【００８８】

この他、利用環境に関する情報は、サービス提供サーバ１１が、ユーザ１２から受け取った利用状況情報に基づいて、ユーザ１２と異なるユーザまたは他のサーバから得ることのできる利用状況情報であってもよい。

【００８９】

さらに、上記のような内容の情報を、２つ以上を組み合わせて利用環境に関する情報とし

てもよい。
【００９０】
また、サービスの変換方法は、サービスと利用状況情報に依存している。ただし、本実施の形態のサービス提供サーバ１１は、サービスの変換方法については特に限定しない。
【００９１】
また、不正な利用環境情報に対しては、サービスのレベルを下げることや、サービスを提供しないことによって、万が一のシステム破壊時のサービスの漏洩を防止することを可能にする。
【００９２】
提供手段２０は、変換手段１９から送信されたサービスデータをもとに、サービスをユーザ１２へ提供する。
【００９３】
次に、図８のフローチャートを参照しながら、本実施の形態のサービス提供サーバ１１によりユーザ１２にサービスを提供する場合の動作を説明する。
【００９４】
まず、最初のステップＳ１０８０１において、ユーザ１２はサービス提供サーバ１１の受付手段１４に対してサービスの提供を依頼する。
【００９５】
ステップＳ１０８０２において、受付手段１４は、ユーザ１２からサービス提供依頼を受け付け、ステップＳ１０８０４へ進む。
【００９６】
ステップＳ１０８０４において、判断手段１６は、ユーザ認証するか否かを決定し、ユーザ認証する場合はステップＳ１０８０３へ進み、ユーザ認証しない場合はステップＳ１０８０５へ進む。
【００９７】
ステップＳ１０８０３において、認証手段１５は、判断手段１６からの認証要求によりユーザ認証し、ステップＳ１０８０４へ進む。
【００９８】
ステップＳ１０８０５において、判断手段１６は、１つ以上の認証結果に基づいて、認証判断結果を決定する。
【００９９】
ステップＳ１０８０６において、検索手段１７は、サービス情報と認証判断結果に基づいて、サービスデータベースからサービスデータを検索し、ステップＳ１０８０８へ進む。
【０１００】
ステップＳ１０８０８において、変換手段１９は、利用状況情報を検証するか否かを決定し、検証する場合はステップＳ１０８０７へ進み、検証しない場合はステップＳ１０８０９へ進む。
【０１０１】
ステップ１０８０７において、検証手段１９は、ユーザの利用状況情報を検証し、ステップ１０８０８へ進む。
【０１０２】
ステップＳ１０８０９において、変換手段１９は、検証結果に基づいて、サービスデータを変換する。
【０１０３】
ステップＳ１０８１０において、提供手段２０は、変換後のサービスデータに基づいたサービスをユーザ１２へ提供する。
【０１０４】
（本実施の形態の変形例１）
上述した本実施の形態では、ユーザ１２は単一のサービス提供サーバ１１にある認証手段１５に対して認証する場合について述べたが、図９に示すサーバ提供システムのように、

認証を行うサーバとサービスを提供するサーバとが異なるサーバで構成される場合も考えられる。

【０１０５】

なお、図９では、上述した実施の形態と同一構成の部分については図３と同一符号を付している。

【０１０６】

図９において、ユーザ１２の認証を行う第１のサービス提供サーバ２１と、サービスの提供を行う第２のサービス提供サーバ２２がネットワーク１３を介して接続されている。

【０１０７】

ユーザ１２は、第１のサービス提供サーバ２１に対してサービスの提供を依頼し、第１のサービス提供サーバ２１は、認証判断結果を第２のサービス提供サーバ２２へ送信し、第２のサービス提供サーバ２２は、認証判断結果に従ってユーザ１２へサービスを提供する。

【０１０８】

（本実施の形態の変形例２）

検証手段に関しても、図１０に示すように、複数のサーバで実現可能である。ユーザの端末が携帯電話である場合のネットワークシステムの構成を図１０に示す。

【０１０９】

なお、図１０についても、上述した実施の形態と同一構成の部分については図３と同一符号を付している。また、本例におけるサービス提供サーバ２３の検証手段以外の機能は、上述した実施の形態のサービス提供サーバ１１と同様である。

【０１１０】

図１０において、ユーザ１２は、利用状況情報として携帯電話の固有情報をサーバに送ることは可能であるが、携帯電話における通信路の状況の全てを利用状況情報として送ることはできない。確かに、ユーザ１２は仕様上の通信帯域等を知ることは可能であるが、混み具合等のような実際の通信路の状況を知ることができない。

【０１１１】

しかし、通信事業者２４は全てを知ることが可能である。そのため、サービス提供サーバ２３の検証手段２５は、利用状況情報として携帯電話のIDを受けた場合、携帯電話のIDから通信事業者２４を特定し、ユーザ１２から送られた携帯電話のIDを提示し、現在の通信状況を通信事業者２４に問い合わせる。

【０１１２】

通信事業者２４は、携帯電話のIDから現在の通信状況を調べ、検証情報と共に検証手段２５へ返信する。上記の手順により、検証手段２５は現在の通信路の状況を知ることが可能になる。

【０１１３】

さらに、この場合は、利用状況情報と検証情報をユーザ１２以外から受け取ることになり、利用状況情報の正当性の信頼性を上げることを可能にする。つまり、ユーザ１２から送られる利用状況情報と、これに対する検証情報だけでは、これらの情報の複製と再利用による不正を防ぐことはできない。

【０１１４】

しかし、利用状況情報と検証情報をユーザ１２以外からも受け取り、さらにそれらを加味して最終的な検証結果とすることで、検証情報の矛盾を検出することを可能にし、悪意のあるユーザの不正を防ぐことを可能にする。

【０１１５】

なお、上記例は可能性を示した一例であって、通信事業者２４の運用ポリシー等によりそのまま実現可能であるわけではない。しかし、検証者は、ユーザ１２から送信された利用状況情報を基にして、第三者から利用状況情報と検証情報の詳細を得られることを示している。

【０１１６】

なお、上記変形例１で説明した図９や、上記変形例２で示した図１０は、図３に示した機能を、機能ごとに分離した一つの構成形態であったり、１つの機能を１つ以上のサーバによる構成形態であったりするが、サービスデータベースの検索手段１７や認証手段１５も同様に、様々なサーバで構成する形態とすることも可能である。

【０１１７】

（本実施の形態の変形例３）

上述した本実施の形態において、端末がパーソナルコンピュータ（PC）等の汎用的な端末である場合、サーバ側の意図しない方法でコンテンツが利用される虞が考えられる。

【０１１８】

この対策としてサーバは、利用状況情報として端末が汎用的な端末である受け取った場合、サービスのレベルを下げてサービスを提供することが可能である。

【０１１９】

ただし、端末は汎用的な端末であっても、端末内で動作するプログラムは汎用的でなく、かつユーザ１２がプログラムを改変することが困難であるので、このプログラムの情報を利用状況情報としてサーバに送信した場合は、サービスのレベルを下げる必要はないと考えられる。

【０１２０】

さらに、先に述べたように、昨今のサービスは経済的価値が高まり、保護が必要となる。しかし、上述した実施の形態のネットワークシステムにおいては、サービス提供サーバ１１と、ある特定のユーザ１２の間でのサービスの漏洩を防止したシステムであって、第３のユーザを想定したシステムではない。

【０１２１】

つまり、第３のユーザは、ネットワーク１３を監視することにより、サービスを盗聴することが可能である。これに対しては、図１１に示すように、サービスを暗号化する方法で防止可能である。なお、図１１ついても、上述したものと同一構成の部分については図３、図１０と同一符号を付している。

【０１２２】

図１１においては、サービス提供サーバ２６に第１の暗号化/復号手段２７を加えて、提供するサービスを暗号化しユーザ２８へ提供するとともに、ユーザ２８側にも第２の暗号化/復号手段２９を加えて、提供される暗号化サービスを復号してサービスを享受している。なお、サービス提供サーバ２６は、上述したサービス提供サーバ１１、２２、２３に暗号化／復号手段２７を付加した構成であり、上記暗号化／復号手段２７以外の構成は、サービス提供サーバ１１、２２、２３と同じである。

【０１２３】

これにより、暗号化したサービスを復号できる特定のユーザだけに意味のあるサービスを提供することを可能にし、第３のユーザによるサービスの盗聴を防止することを可能にする。

【０１２４】

以上のように、本実施の形態及びその変形例では、サーバへの入り口、つまりユーザ認証時における第１のアクセス制御と、サーバからの出口、つまりサービス提供時における第２のアクセス制御を行うことを特徴とする。

【０１２５】

すなわち、上記第１のアクセス制御により、ユーザ１２の認証方式に適応的なサービスを提供することが可能になる。そして、上記第２のアクセス制御により、ユーザ１２の利用環境に最適なサービスを提供することが可能になる。

【０１２６】

したがって、上記第１のアクセス制御と第２のアクセス制御とを行うことにより、段階的なサービス等のユーザ認証の結果に適応的なサービスであって、ユーザの利用環境に適応的に対応したサービスを提供することが可能になる。

【０１２７】

特に、ユーザ１２が異なる利用端末でサービスを利用するといった、大域的な変化に対しては、第１のアクセス制御によってサービス提供を制御し、モバイル環境での利用による利用環境の変化といった、局所的な変化に対しては、第２のアクセス制御によってサービス提供を制御している。つまり、アクセス制御を行うポイントを２つ設けることにより、大域的な変化と局所的な変化の双方に対して、適応的なサービス提供を可能にしている。

【０１２８】

（本発明の他の実施形態）

上述した実施形態の機能を実現するべく各種のデバイスを動作させるように、該各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、上記実施形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【０１２９】

また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えば、かかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【０１３０】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施形態に含まれることは言うまでもない。

【０１３１】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって上述した実施形態の機能が実現される場合にも本発明に含まれることは言うまでもない。

【０１３２】

【発明の効果】

以上説明してきたように、本発明によれば、ユーザの認証結果にレベルを持たせることができ、コンテンツの表示及び編集のアクセス制御を可及的に適切、かつ、段階的に提供することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態を示し、ネットワークシステムの構成の一例を示した概要図である。

【図２】本発明の実施の形態を示し、サービス提供サーバの構成の一例を示した概要図である。

【図３】本発明の実施の形態を示し、サービス提供サーバの構成の一例を示したブロック図である。

【図４】本発明の実施の形態を示し、音楽配信サービスを依頼する場合のサービス提供依頼情報の内容の一例を示した図である。

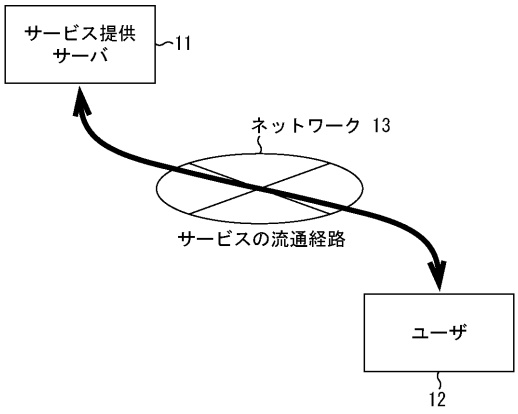
【図５】本発明の実施の形態を示し、第２のサービス提供依頼情報の内容の一例を示した図である。

【図６】本発明の実施の形態を示し、パスワードとICカードと指紋の３種類の認証方法を利用した場合の認証状態の一例を示した状態遷移図である。

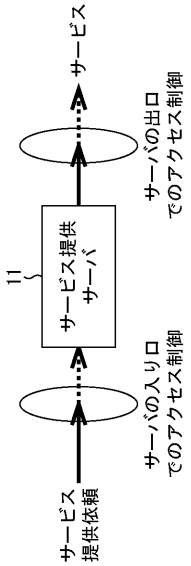
【図７】本発明の実施の形態を示し、音楽配信サービスを依頼する場合のサービス提供依

頼情報の内容の一例を示した図である。
【図８】本発明の実施の形態を示し、ネットワークシステムによりユーザにサービスを提供する場合の動作を説明するフローチャートである。
【図９】本発明の実施の形態の変形例１を示し、サービス提供サーバの構成の一例を示したブロック図である。
【図１０】本発明の実施の形態の変形例２を示し、サービス提供システムの構成の一例を示した概要図である。
【図１１】本発明の実施の形態の変形例３を示し、ネットワークシステムの構成の一例を示した概要図である。
【図１２】本発明の実施の形態を示し、アクセス制御リストの第１の例を示した図である。
【図１３】本発明の実施の形態を示し、アクセス制御リストの第２の例を示した図である。
【図１４】本発明の実施の形態を示し、アクセス制御リストの第３の例を示した図である。
【図１５】本発明の実施の形態を示し、アクセス制御リストの第４の例を示した図である。
【符号の説明】
１１、２３、２６　サービス提供サーバ
１２、２８　ユーザ
１３　ネットワーク
１５　認証手段
１６　判断手段
１７　検索手段
１８、２５　検証手段
１９　変換手段
２０　提供手段
２１　第１のサービス提供サーバ
２２　第２のサービス提供サーバ
４０、５０、７０　サービス提供依頼情報

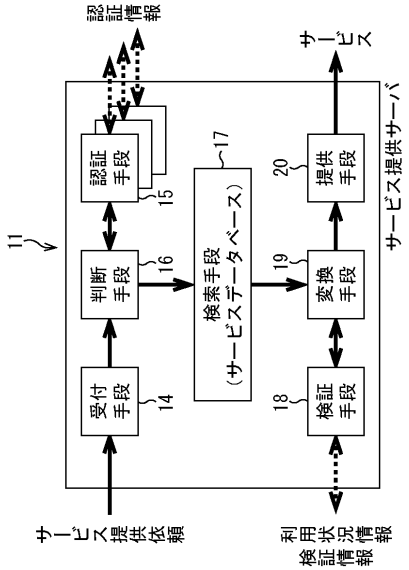
【図１】


サービス提供
サーバ
11
ネットワーク 13
サービスの流通経路
ユーザ
12

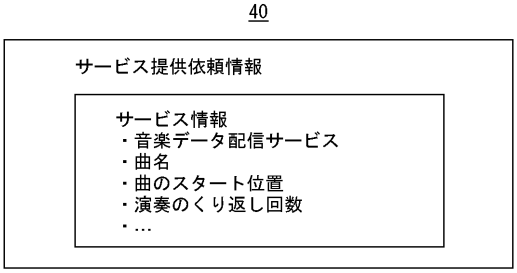
【図２】


サービス
サーバの出口
でのアクセス制御
11
サービス提供
サーバ
サーバの入り口
でのアクセス制御
サービス
提供依頼

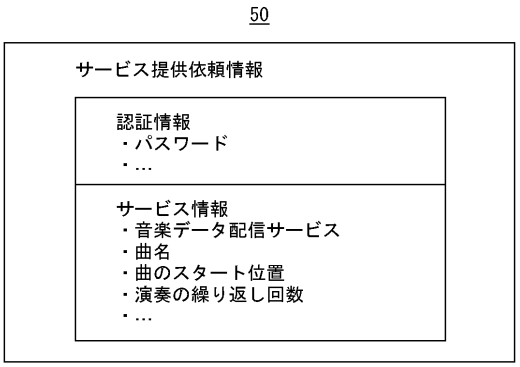
【図３】


認証情報
サービス
サービス提供サーバ
11
認証
手段
15
判断
手段
16
受付
手段
14
検索手段
（サービスデータベース）
17
提供
手段
20
変換
手段
19
検証
手段
18
サービス提供依頼
利用状況情報
検証情報

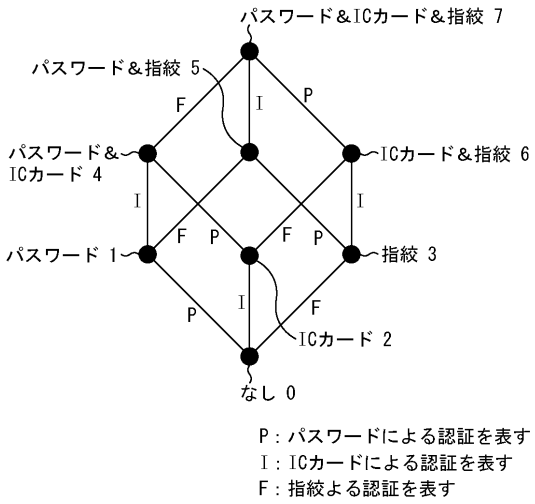
【図４】


40
サービス提供依頼情報
サービス情報
・音楽データ配信サービス
・曲名
・曲のスタート位置
・演奏のくり返し回数
・…

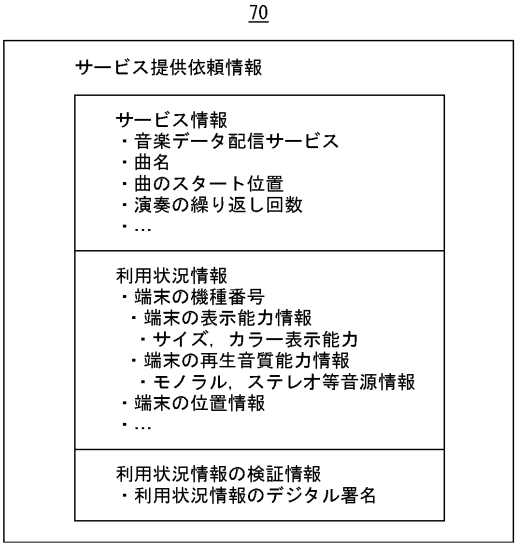
【図５】


50
サービス提供依頼情報
認証情報
・パスワード
・…
サービス情報
・音楽データ配信サービス
・曲名
・曲のスタート位置
・演奏の繰り返し回数
・…

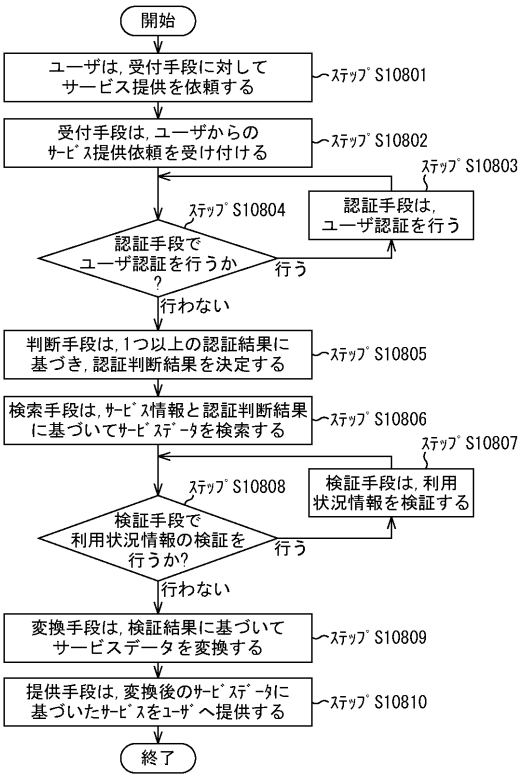
【図６】


パスワード&ICカード&指絞 7
パスワード&指絞 5
パスワード&
ICカード 4
ICカード&指絞 6
パスワード 1
指絞 3
ICカード 2
なし 0
F
I
P
P：パスワードによる認証を表す
I：ICカードによる認証を表す
F：指絞よる認証を表す

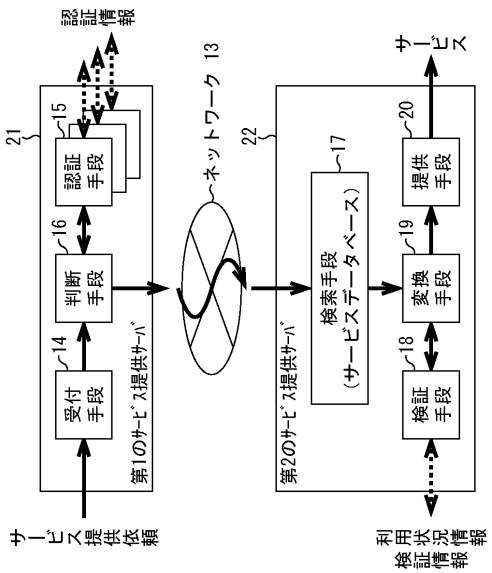
【図７】


70
サービス提供依頼情報
サービス情報
・音楽データ配信サービス
・曲名
・曲のスタート位置
・演奏の繰り返し回数
・…
利用状況情報
・端末の機種番号
・端末の表示能力情報
・サイズ，カラー表示能力
・端末の再生音質能力情報
・モノラル，ステレオ等音源情報
・端末の位置情報
・…
利用状況情報の検証情報
・利用状況情報のデジタル署名

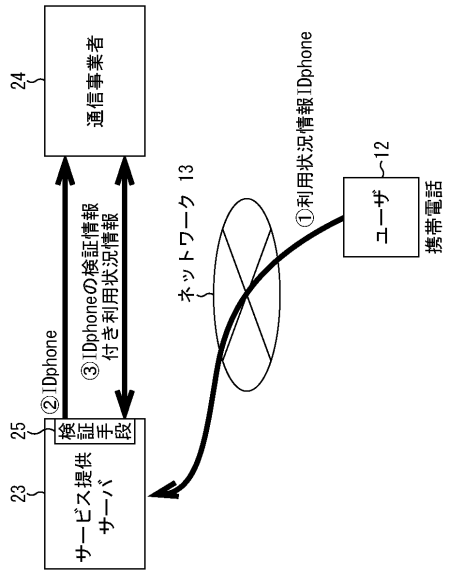
【図８】


開始
ユーザは，受付手段に対して
サービス提供を依頼する
ステップ S10801
受付手段は，ユーザからの
サービス提供依頼を受け付ける
ステップ S10802
ステップ S10803
認証手段は，
ユーザ認証を行う
ステップ S10804
認証手段で
ユーザ認証を行うか
？
行う
行わない
判断手段は，1つ以上の認証結果に
基づき，認証判断結果を決定する
ステップ S10805
検索手段は，サービス情報と認証判断結果
に基づいてサービスデータを検索する
ステップ S10806
ステップ S10807
検証手段は，利用
状況情報を検証する
ステップ S10808
検証手段で
利用状況情報の検証を
行うか?
行う
行わない
変換手段は，検証結果に基づいて
サービスデータを変換する
ステップ S10809
提供手段は，変換後のサービスデータに
基づいたサービスをユーザへ提供する
ステップ S10810
終了

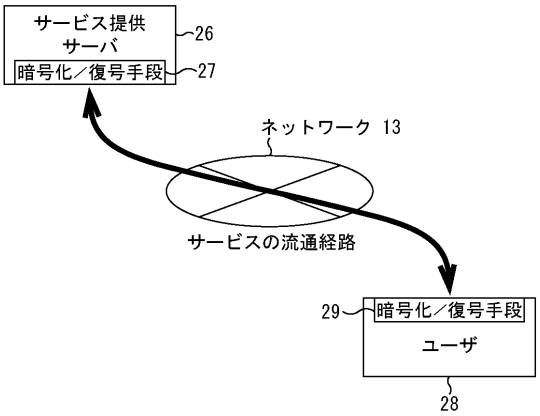
【図９】


認証情報
ネットワーク 13
サービス
21
22
15
16
14
17
18
19
20
認証
手段
判断
手段
受付
手段
検索手段
（サービスデータベース）
検証
手段
変換
手段
提供
手段
第1のサービス提供サーバ
第2のサービス提供サーバ
サービス提供依頼
利用状況情報
検証情報

【図１０】



【図１１】



【図１２】

○：サービスを許可
×：サービスを不許可

	低解像度表示	高解像度表示	低解像度編集	高解像度編集
頂点0	×	×	×	×
頂点1	○	×	×	×
頂点2	○	×	×	×
頂点3	○	×	×	×
頂点4	○	○	×	×
頂点5	○	○	○	×
頂点6	○	○	○	×
頂点7	○	○	○	○

【図１３】

○：サービスを許可
×：サービスを不許可

	低解像度表示	高解像度表示	低解像度編集	高解像度編集
頂点0	×	×	×	×
頂点1	×	×	×	×
頂点2	×	×	×	×
頂点3	×	×	×	×
頂点4	×	×	×	×
頂点5	×	×	×	×
頂点6	×	×	×	×
頂点7	○	○	○	○

【図１４】

○：サービスを許可
×：サービスを不許可

	低解像度表示	高解像度表示	低解像度編集	高解像度編集
頂点0	×	×	×	×
頂点1	○	○	×	×
頂点2	○	○	×	×
頂点3	○	○	×	×
頂点4	○	○	○	○
頂点5	○	○	○	○
頂点6	○	○	○	○
頂点7	○	○	○	○

【図１５】

○：サービスを許可
×：サービスを不許可

	低解像度表示	高解像度表示	低解像度編集	高解像度編集
頂点0	×	×	×	×
頂点1	×	×	×	×
頂点2	○	○	○	○
頂点3	×	×	×	×
頂点4	○	○	○	○
頂点5	×	×	×	×
頂点6	○	○	○	○
頂点7	○	○	○	○

フロントページの続き

(51)Int.Cl. FI
G06F 13/00 510A

審査官 平井 誠

(56)参考文献 特開２０００－０２９８２９（ＪＰ，Ａ）
特開２０００－２３２６３６（ＪＰ，Ａ）
特開平１１－２１９３４０（ＪＰ，Ａ）
特開平０７－０１３８４２（ＪＰ，Ａ）
特開平１１－０７３３９８（ＪＰ，Ａ）
特開平０７－０６４９１１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
G06F 21/20
G06F 13/00