

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4310879号
(P4310879)

(45) 発行日 平成21年8月12日(2009.8.12)

(24) 登録日 平成21年5月22日(2009.5.22)

(51) Int.Cl.	F I	
G 1 1 B 20/10 (2006.01)	G 1 1 B	20/10 H
G 0 6 F 21/00 (2006.01)	G 0 6 F	15/00 3 3 O Z
G 0 9 C 1/00 (2006.01)	G 0 9 C	1/00 6 4 O B
H 0 4 L 9/10 (2006.01)	H 0 4 L	9/00 6 2 1 A
H 0 4 N 7/08 (2006.01)	H 0 4 N	7/08 Z
請求項の数 17 (全 20 頁) 最終頁に続く		

(21) 出願番号	特願2000-45902 (P2000-45902)	(73) 特許権者	000002185
(22) 出願日	平成12年2月23日(2000.2.23)		ソニー株式会社
(65) 公開番号	特開2001-236728 (P2001-236728A)		東京都港区港南1丁目7番1号
(43) 公開日	平成13年8月31日(2001.8.31)	(74) 代理人	100101801
審査請求日	平成18年11月10日(2006.11.10)		弁理士 山田 英治
		(74) 代理人	100093241
			弁理士 宮田 正昭
		(74) 代理人	100086531
			弁理士 澤田 俊夫
		(72) 発明者	寺尾 創
			東京都品川区北品川6丁目7番35号 ソニー株式会社内
		(72) 発明者	栗原 謙
			東京都品川区北品川6丁目7番35号 ソニー株式会社内
最終頁に続く			

(54) 【発明の名称】 コンテンツ再生システム及びコンテンツ再生方法、並びに、コンテンツの再生要求装置及び一時再生装置

(57) 【特許請求の範囲】

【請求項1】

トークンで復号化可能な暗号化コンテンツを再生するコンテンツ再生システムであって、

トークンを保有するとともに暗号化コンテンツの再生を要求する再生要求手段と、
該コンテンツの再生要求に回答して、前記再生要求手段に対してトークンの送付を要求して、トークンを利用して暗号化コンテンツの再生を行う一時再生手段と、
を具備することを特徴とするコンテンツ再生システム。

【請求項2】

前記再生要求手段と前記一時再生手段は、近距離無線データ通信により接続可能であることを特徴とする請求項1に記載のコンテンツ再生システム。 10

【請求項3】

前記再生要求手段は、1以上の暗号化コンテンツ及び各暗号化コンテンツに対するトークンを保有するとともに、保有する暗号化コンテンツを前記一時再生手段に転送することを特徴とする請求項1に記載のコンテンツ再生システム。

【請求項4】

前記一時再生手段は、1以上の再生要求手段から暗号化コンテンツを受信して蓄積する手段を備えることを特徴とする請求項1に記載のコンテンツ再生システム。

【請求項5】

前記一時再生手段は、再生要求されたコンテンツの識別子及びデジタル署名を添付した 20

形式のトークンの送付要求を前記再生要求手段に送信し、

前記再生要求手段は、デジタル署名の認証手続きが成功した場合のみトークンを前記一時再生手段に返信することを特徴とする請求項 1 に記載のコンテンツ再生要求システム。

【請求項 6】

前記一時再生手段は公開鍵暗号系の公開鍵及び秘密鍵を有し、

前記デジタル署名には前記一時再生手段の公開鍵が含まれ、

前記再生要求手段は、トークンを前記一時再生手段の公開鍵で暗号化して返信する、ことを特徴とする請求項 5 に記載のコンテンツ再生システム。

【請求項 7】

前記再生要求手段及び / 又は前記一時再生手段は、耐タンパ性のある回路パッケージ上に実装されていることを特徴とする請求項 1 に記載のコンテンツ再生システム。

10

【請求項 8】

前記再生要求手段と前記一時再生手段は近距離無線データ通信により接続可能であるとともに、該近距離無線データ通信により交信可能な領域内に前記再生要求手段が複数存在し、

前記一時再生手段は、トークンの送付要求を一斉送信する、ことを特徴とする請求項 1 に記載のコンテンツ再生システム。

【請求項 9】

トークンを保有するとともに暗号化コンテンツの再生を要求する再生要求装置と、該コンテンツの再生要求に応答して暗号化コンテンツの再生を行う一時再生装置とで構成されるシステム上で、トークンで復号化可能な暗号化コンテンツを再生するコンテンツ再生方法であって、

20

(a) 前記再生要求装置が、コンテンツ識別子を付してコンテンツの再生要求を送信するステップと、

(b) 前記一時再生装置が、再生要求されたコンテンツの識別子及びデジタル署名を添付した形式のトークンの送付要求を送信するステップと、

(c) 前記再生要求装置が、デジタル署名の認証手続きが成功した場合のみ、トークンを前記一時再生装置に返信するステップと、

(d) 前記一時再生装置が、受け取ったトークンを利用して再生要求されたコンテンツを再生するステップと、

30

を具備することを特徴とするコンテンツ再生方法。

【請求項 10】

前記再生要求装置と前記一時再生装置は、近距離無線データ通信により接続可能であることを特徴とする請求項 9 に記載のコンテンツ再生方法。

【請求項 11】

前記再生要求装置は、1 以上の暗号化コンテンツ及び各暗号化コンテンツに対するトークンを保有し、さらに、

(a) 前記再生要求装置があらかじめ暗号化コンテンツを前記一時再生装置に転送するステップと、

(a) 前記一時再生装置が、暗号化コンテンツを蓄積するステップと、

40

を具備することを特徴とする請求項 9 に記載のコンテンツ再生方法。

【請求項 12】

前記一時再生装置は公開鍵暗号系の公開鍵及び秘密鍵を有し、

前記ステップ (b) において送信される前記デジタル署名には前記一時再生装置の公開鍵が含まれ、

前記ステップ (c) では、前記再生要求装置は、トークンを前記一時再生装置の公開鍵で暗号化して返信する、

ことを特徴とする請求項 9 に記載のコンテンツ再生方法。

【請求項 13】

前記再生要求装置及び / 又は前記一時再生装置は、耐タンパ性のある回路パッケージ上

50

に実装されていることを特徴とする請求項 9 に記載のコンテンツ再生方法。

【請求項 14】

前記再生要求装置と前記一時再生装置は近距離無線データ通信により接続可能であるとともに、該近距離無線データ通信により交信可能な領域内に前記再生要求装置が複数存在し、

前記ステップ (b) では、前記一時再生装置は、トークンの送付要求を一斉送信する、ことを特徴とする請求項 9 に記載のコンテンツ再生方法。

【請求項 15】

トークンで復号化可能な暗号化コンテンツの再生を要求する再生要求装置であって、
 トークンを保持するトークン保持手段と、
 暗号化コンテンツを蓄積するコンテンツ蓄積手段と、
 外部機器とデータ交換するためのインターフェース手段と、
 該装置の動作を統括する制御する制御手段と、
 を具備することを特徴とする再生要求装置。

10

【請求項 16】

前記制御手段は、前記インターフェース手段経由でデジタル署名付きのトークン送付要求を受信したことに応答して、該デジタル署名に関する認証手続きに成功した場合にのみトークンを返信することを特徴とする請求項 15 に記載の再生要求装置。

【請求項 17】

前記デジタル署名にはトークン送付要求元の公開鍵が含まれており、
 前記制御手段は、該公開鍵を用いて暗号化したトークンを該要求元に返信することを特徴とする請求項 16 に記載の再生要求装置。

20

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル・コンテンツを利用するコンテンツ再生技術に係り、特に、音楽や映像などのようにコンテンツ作成者等が著作権を始めとする所定の使用権を有するコンテンツを安全に（すなわち著作権を保護しつつ）利用することができるコンテンツ再生技術に関する。

【0002】

更に詳しくは、本発明は、トークンを利用して暗号化コンテンツの使用を許可することで著作権保護を行うコンテンツ再生技術に係り、特に、暗号化コンテンツのトークンを所有する複数のユーザ間でコンテンツを共有することができるコンテンツ再生技術に関する。

30

【0003】

【従来の技術】

著作権とは、著作物を利用し得る相対的な排他的独占権であり、いわゆる無体財産権の 1 つに含まれる。ここで言う「著作物」とは、思想又は感情を創作的に表現したものであって、文芸、学術、美術又は音楽の範囲に属するものを指す。著作権は、例えば、各国の著作権法や、ベルヌ条約や万国著作権条約などの国際的な条約で保護されている。

【0004】

著作権の利用は、著作権者自身において行われるのはごく稀であり、他人が著作権を利用することに対して一定の対価を得て許諾するのが一般的である。例えば、楽曲などの音楽コンテンツに関する著作権を所有するレコード会社などは、音楽コンテンツを使用すなわち放送する放送局やコンテンツ配信業者に対して、コンテンツ使用回数に応じた著作権使用料を要求することができる。

40

【0005】

昨今、情報処理及び情報通信技術が飛躍的に進歩するとともに、文化的及び経済的な分野においては国際化が目覚しく進展してきた。かかる社会環境下では、著作権をめぐる情勢も刻々と変貌してきている。著作権保護の歴史は 15 世紀中ごろの印刷技術の発明に由来すると言われているが、現在では、あらゆるデータやコンテンツがデジタル化して計算機

50

システム上で取り扱うことが可能となり、これと相俟って、著作物の流通や販売の形態が変貌するとともに、著作物の複製もますます容易になってきた。したがって、情報技術の観点からも著作物の正当な利用を支援し若しくは不正利用を排除して、著作権の保護を拡充する必要があると思料される。

【 0 0 0 6 】

例えば、音楽コンテンツの流通・販売は、旧来では、もっぱらレコード盤やCD (Compact Disc) などの物理的なメディアを物理的な流通経路や販路を経由して店頭で陳列することで行われていた。ところが、最近では、デジタル・データとしての音楽コンテンツを、WWW (World Wide Web) サーバなどのWebサイト上で提供する、すなわちインターネットなどのパブリックなネットワーク環境下で配信するという、流通・販売の形態が普及しつつある。後者のコンテンツ配信・配布行為には、物理的なメディアの存在や物理的な流通・販売経路が全く省略される。すなわち、物理的な制約条件はほとんど課されず、各一般ユーザがコンテンツ取得を自在に行うことができる。

10

【 0 0 0 7 】

例えば、コンビニエンス・ストアなどの公共の場にデジタル・コンテンツ販売用の街頭端末を設置して、ユーザは其処で音楽コンテンツをダウンロードすなわち購入することができる。あるいは、ユーザ自らが電話回線経由で自宅から音楽データをダウンロードすることができる。また、モバイル環境の拡充により、携帯電話の回線を利用して、任意の時間帯に好きな場所でも音楽コンテンツをダウンロードすることが可能となってきた。

【 0 0 0 8 】

最近では、多機能携帯端末と呼ばれる携帯情報機器が出現してきている。この種の携帯型機器は、携帯電話機能やインターネット・アクセス機能を装備して音楽コンテンツをダウンロードするだけでなく、音楽コンテンツの再生機能や、さらに近隣の他の機器へデータやコンテンツを転送するための機器間無線通信機能などを備えている。機器間無線通信機能には、例えば"Bluetooth"などのような近距離無線データ通信技術を利用することができる。

20

【 0 0 0 9 】

ところで、旧来の物理的なメディアを介した音楽コンテンツの流通・販売は、記憶媒体の購入行為が著作物の使用許諾とほとんど等価であった。これに対し、デジタル・コンテンツの形態で流通・販売を行う場合、複製がより一層容易となることから、技術的な観点から著作物の複製や不正使用を抑制したり取り締まる必要がある。

30

【 0 0 1 0 】

音楽コンテンツの著作権保護は、例えば「トークン」と呼ばれる一種のライセンス・キーを用いることによって実現される。トークンを用いた音楽コンテンツの保護は、概ね以下のような手順によって実現される。すなわち、

【 0 0 1 1 】

- (1) 暗号化された形態で音楽コンテンツを配信・配布する。
- (2) 暗号化音楽コンテンツに対する秘密鍵をトークンとする。
- (3) 正規ユーザのコンテンツ再生装置にだけ、セキュリティ保証された経路でトークンを供給する。
- (4) 正規ユーザのコンテンツ再生装置内では、耐タンパ性を備えた回路モジュール内にトークンが格納され、暗号化音楽コンテンツの復号化に利用される。なお、トークン以外にもトークンを用いてコンテンツ再生を行うプログラム・コードなども耐タンパ性のある回路モジュール内で実行されることが好ましい。

40

【 0 0 1 2 】

この結果、正規ユーザの再生装置における正当使用時のみに限定して音楽コンテンツの復号化使用が許可されることになる。なお、耐タンパ性とは、回路パッケージが強固に封止され、内部データ解読などのために回路パッケージを分解しようと試みると回路自体の破損を招来し、必然的に内部アクセスが禁止されたような回路パッケージの性質を意味する。

50

【 0 0 1 3 】

旧来の音楽コンテンツ販売形態では、コンテンツ・メディアを所有することが正当なユーザであることの証しとなっていた。これに対し、デジタル・コンテンツで流通・販売を行う場合には、コンテンツではなくトークンの取得が正当なユーザであることの証しとなる。後者の場合、例えば多機能携帯端末上にトークンさえ保有していれば、随時ネットワーク経由で音楽コンテンツを入手してこれを再生することができる。すなわち、暗号化音楽コンテンツとトークンとを分離して利用することができ、物理的なメディアを常に持ち運ぶ必要がなくなる。当然、メディアの破損や紛失という物品を取り扱うときに固有の問題からも解放されることになる。

【 0 0 1 4 】

しかしながら、音楽コンテンツの再生には必ずトークンを必要とするので、トークンの管理上幾つかの問題がある。

【 0 0 1 5 】

例えば、2以上の機器上で音楽コンテンツを再生したい場合、旧来は物理的なメディアを機器間で移動・交換するだけで済んだが、暗号化コンテンツによる場合にはトークンを機器間で移動させなければならない。

【 0 0 1 6 】

機器間でのトークンの自由な複製を認めた場合、複製元及び複製先の双方の機器においてコンテンツ再生が可能となり便利であるが、トークンの無断複製を取り締まることが困難となり、コンテンツに対する著作権保護が充分でなくなる。また、複製を認めない形態で機器間のトークンの移動を許可した場合には、著作権保護は確実であるが、再び機器同士が離れるときにはトークンの置き忘れが問題となる。トークンの回収に失敗した元の機器上では、暗号化音楽コンテンツそのものを持っていてもその再生を行うことができない。トークンの置き忘れは、論理的には、メディアの置き忘れとほとんど等価である。

【 0 0 1 7 】

また、複数ユーザがトークン及び正規の再生機器を持ち寄り、単一の機器にトークンを集中させてコンテンツ再生を楽しむような場合、各ユーザが再び離散するときにトークンの取り違えを起こす危険がある。このようなトークンの取り違えは、論理的には、メディアの取り違えとほとんど等価である。

【 0 0 1 8 】

ここで、具体的な例について考察してみる。

【 0 0 1 9 】

例えば、日経エレクトロニクス1999.12.13(n.759)pp.139-150には、近距離無線データ通信技術としての"bluetooth"(前述)を自動車内のLAN(Local Area Network)に適用する旨の提案が記載されている。このような場合、各乗員が携行する携帯型機器と車載用オーディオ機器とを無線LANを用いて統合化して、手軽にハンズフリー環境を構築することができる。すなわち、各々の携帯型機器が保有する音楽コンテンツの出力ターゲットを車載用オーディオ機器に指定することにより、各乗員はヘッドセットなしに、通常は一人しか聴くことができない音楽コンテンツを車内に持ち寄って、その再生を共有することができる。ここで言う携帯型機器は、上述の多機能携帯端末でもよい。

【 0 0 2 0 】

このような利用形態においても、音楽コンテンツを再生する車載用オーディオ機器は、該当するトークンを保有しなければならない。

【 0 0 2 1 】

例えば、すべての携帯型機器が、音楽コンテンツとともにトークンを車載用オーディオ機器に移動させることにより、すべての乗員が持つ音楽コンテンツを1箇所で集中管理することができるので、便利である。個々の乗員は、車載用オーディオ機器が収集した曲名リストを無線LAN経由で受け取り、他の乗員から提供された楽曲を自由に選択することができる。また、携帯型機器よりも車載用オーディオ機器の方が記憶容量を大きくすること

10

20

30

40

50

ができるので、多数の音楽コンテンツを集中的に蓄積するには都合がよい。さらに、各乗員は、車載用オーディオ機器の多種多様なオーディオ機能を共有することができる。一般には、多機能携帯端末よりも車載用オーディオ機器の方が高価であり、高音質を提供することができる。

【0022】

しかしながら、各コンテンツに対する著作権保護を確実にしめるためには、トークンの無断複製や不正使用・転用を禁じた形式でトークンを移動し、さらに元の各携帯型機器に再び回収しなければならない。このようなトークンの移動・回収を直感的な操作で実現することは難しい。

【0023】

また、複数のユーザがトークンの回収を行うとき、トークンの置き忘れ/戻し忘れ、取り違え、紛失などのトラブルを起こす危険がある。「迷子」のトークンが出てきても、元の所有者のコンテンツ使用権を留保するためには、車載用オーディオ機器側が勝手にトークンを消去又は廃棄することができない。

【0024】

他方、トークンの移動なしに車内で音楽コンテンツを共有する方法として、元の携帯型機器上で再生したデータを、無線LANを利用して車載用オーディオ機器にリアルタイム伝送して、該オーディオ機器上で音声出力することが考えられる。この方法によれば、トークンは元の携帯型機器上に居続けるので、操作すなわちトークン管理が非常に簡素化される。

【0025】

しかしながら、車載用オーディオ機器上にすべての音楽コンテンツを集中させないので、ある乗員が持つ音楽コンテンツを他の乗員が自由に選択することはできない。また、コンテンツ再生を行う間、その携帯型機器はフル稼働状態なので消費電力が増す（一般に、携帯型機器はバッテリー駆動であり、消費電力の増大は深刻である）。また、論理的には、携帯型機器からライン・アウト出力して、車載用オーディオ機器を単にオーディオ・アンプとして利用するに過ぎないので、車載用オーディオ機器の多種多様なオーディオ機能を享受することができない。

【0026】

【発明が解決しようとする課題】

本発明の目的は、音楽や映像などのようにコンテンツ作成者等が著作権を始めとする所定の使用権を有するコンテンツを安全に（すなわち著作権を保護しつつ）利用することができる、優れたコンテンツ再生技術を提供することにある。

【0027】

本発明の更なる目的は、トークンを利用して暗号化コンテンツの使用を許可することで著作権保護を行うことができる、優れたコンテンツ再生技術を提供することにある。

【0028】

本発明の更なる目的は、暗号化コンテンツのトークンを所有する複数のユーザ間で、各自が持つコンテンツを共有することができる、優れたコンテンツ再生技術を提供することにある。

【0029】

【課題を解決するための手段】

本発明は、上記課題を参酌してなされたものであり、その第1の側面は、トークンで復号化可能な暗号化コンテンツを再生するコンテンツ再生システムであって、トークンを保有するとともに暗号化コンテンツの再生を要求する再生要求手段と、該コンテンツの再生要求に应答して、前記再生要求手段に対してトークンの送付を要求して、トークンを利用して暗号化コンテンツの再生を行う一時再生手段と、を具備することを特徴とするコンテンツ再生システムである。

【0030】

ここで、前記再生要求手段と前記一時再生手段は、近距離無線データ通信により接続可能

10

20

30

40

50

であってもよい。かかる近距離無線データ通信の一例は、"bluetooth"である。

【 0 0 3 1 】

また、前記再生要求手段は、1以上の暗号化コンテンツ及び各暗号化コンテンツに対するトークンを保有するとともに、保有する暗号化コンテンツを前記一時再生手段に転送するようにしてもよい。また、前記一時再生手段は、1以上の再生要求手段から受信した暗号化コンテンツを蓄積する手段を備えていてもよい。

【 0 0 3 2 】

また、前記一時再生手段は、再生要求されたコンテンツの識別子及びデジタル署名を添付した形式のトークンの送付要求を前記再生要求手段に送信するようにしてもよい。このような場合、前記再生要求手段は、デジタル署名の認証手続きが成功した場合のみトークンを前記一時再生手段に返信し、それ以外の場合は、なりすまし防止のためトークンの返信を行わないようにすることができる。

10

【 0 0 3 3 】

また、前記一時再生手段は公開鍵暗号系の公開鍵及び秘密鍵を有していてもよい。また、前記デジタル署名に前記一時再生手段の公開鍵を含めてもよい。このような場合、前記再生要求手段は、トークンを前記一時再生手段の公開鍵で暗号化することで、トークンを安全に返信することができる。

【 0 0 3 4 】

前記再生要求手段及び/又は前記一時再生手段を、耐タンパ性のある回路パッケージ上に実装することで、不正・悪質なユーザによるトークンやコンテンツの解析・漏洩・改竄などの不正行為を完全に排除して、セキュリティ・レベルを一段と向上させることができる。

20

【 0 0 3 5 】

前記再生要求手段と前記一時再生手段とが近距離無線データ通信により接続可能な利用環境下では、該近距離無線データ通信により交信可能な領域内に前記再生要求手段が複数存在していてもよい。このような場合、前記一時再生手段は、トークンの送付要求を一斉送信すれば効率的である。

【 0 0 3 6 】

また、本発明の第2の側面は、トークンを保有するとともに暗号化コンテンツの再生を要求する再生要求装置と、該コンテンツの再生要求に応答して暗号化コンテンツの再生を行う一時再生装置とで構成されるシステム上で、トークンで復号化可能な暗号化コンテンツを再生するコンテンツ再生方法であって、

30

(a) 前記再生要求装置が、コンテンツ識別子を付してコンテンツの再生要求を送信するステップと、

(b) 前記一時再生装置が、再生要求されたコンテンツの識別子及びデジタル署名を添付した形式のトークンの送付要求を送信するステップと、

(c) 前記再生要求装置が、デジタル署名の認証手続きが成功した場合のみ、トークンを前記一時再生装置に返信するステップと、

(d) 前記一時再生装置が、受け取ったトークンを利用して再生要求されたコンテンツを再生するステップと、

40

を具備することを特徴とするコンテンツ再生方法である。

【 0 0 3 7 】

ここで、前記再生要求装置と前記一時再生装置は、近距離無線データ通信により接続可能であってもよい。かかる近距離無線データ通信の一例は、"bluetooth"である。

【 0 0 3 8 】

また、前記再生要求装置は、1以上の暗号化コンテンツ及び各暗号化コンテンツに対するトークンを保有し、さらに、

(a) 前記再生要求装置があらかじめ暗号化コンテンツを前記一時再生装置に転送するステップと、

(a) 前記一時再生装置が、暗号化コンテンツを蓄積するステップと、

50

を具備してもよい。

【0039】

また、前記一時再生装置は公開鍵暗号系の公開鍵及び秘密鍵を有していてもよい。また、前記ステップ(b)において送信される前記デジタル署名に前記一時再生装置の公開鍵を含めることができる。このような場合、前記ステップ(c)では、前記再生要求装置は、トークンを前記一時再生装置の公開鍵で暗号化することで、トークンを安全に返信することが可能となる。

【0040】

前記再生要求装置及び/又は前記一時再生装置を、耐タンパ性のある回路パッケージ上に実装することで、不正・悪質なユーザによるトークンやコンテンツの解析・漏洩・改竄などの不正行為を完全に排除して、セキュリティ・レベルを一段と向上させることができる。

10

【0041】

前記再生要求装置と前記一時再生装置とが近距離無線データ通信により接続可能な利用環境下では、該近距離無線データ通信により交信可能な領域内に前記再生要求装置が複数存在していてもよい。このような場合、前記ステップ(b)において、前記一時再生装置はトークンの送付要求を一斉送信すれば効率的である。

【0042】

また、本発明の第3の側面は、トークンで復号化可能な暗号化コンテンツの再生を要求する再生要求装置であって、

20

トークンを保持するトークン保持手段と、
暗号化コンテンツを蓄積するコンテンツ蓄積手段と、
外部機器とデータ交換するためのインターフェース手段と、
該装置の動作を統括する制御する制御手段と、
を具備することを特徴とする再生要求装置である。

【0043】

本発明の第3の側面に係る再生要求装置において、前記制御手段は、前記インターフェース手段経由でデジタル署名付きのトークン送付要求を受信したことに応答して、該デジタル署名に関する認証手続きに成功した場合にのみトークンを返信することにより、外部機器によるなりすましを好適に排除することができる。

30

【0044】

また、前記デジタル署名にトークン送付要求元の公開鍵が含まれている場合には、前記制御手段は、該公開鍵を用いてトークンを暗号化することで、該要求元に対してトークンを安全に返信することができる。

【0045】

また、本発明の第4の側面は、トークンで復号化可能な暗号化コンテンツを一時的に再生する一時再生装置であって、

デジタル署名を保持する署名保持手段と、
自身の秘密鍵を保持する秘密鍵保持手段と、
暗号化コンテンツを蓄積するコンテンツ蓄積手段と、
外部機器とデータ交換するためのインターフェース手段と、
平文化されたコンテンツを再生するコンテンツ再生手段と、
該装置の動作を統括する制御する制御手段と、
を具備することを特徴とする一時再生装置である。

40

【0046】

本発明の第4の側面に係る一時再生装置において、前記制御手段は、前記インターフェース手段経由でコンテンツの再生要求を受信したことに応答して、該要求されたコンテンツに対応するトークンの送付を要求するために、デジタル署名付きのトークン送付要求を送信することができる。トークンの送付要求先では、このデジタル署名を用いて一時再生装置を認証することができ、なりすましを好適に排除することができる。

50

【0047】

また、前記制御手段は、トークン送付要求に対するトークンの返信を受けたことに応答して、トークンを用いてコンテンツの再生を実行せしめることができる。

【0048】

また、一時再生装置は、さらに、トークンを一時的にのみ保持するトークン保持手段を備えていてもよい。

【0049】

ここで言う一時的なトークンの保持とは、トークンを長期間保存せず、上記の再生要求装置が近距離無線データ通信可能な範囲外に持ち出される時期にトークンを廃棄することの他、トークンを複製したり外部の機器に無断で転送したりしないことを含み、略言すれば 10
正規ユーザの証しであるトークンを著作権の使用許諾の範囲（若しくは取引の通念上許容し得る範囲）でのみ保存することを意味する。

【0050】

【作用】

本発明に係るコンテンツ再生システムは、再生要求手段と一時再生手段とで構成される。例えば、再生要求手段は各ユーザ毎に持ち運ぶ携帯型機器として、一時再生手段は各ユーザ間で再生機能を共有することができるオーディオ機器として実装される。したがって、再生要求手段と一時再生手段との間には、一対一、多対一、又は、多対多の関係が形成される。より好ましくは、一時再生手段は、再生要求手段よりも高機能なコンテンツ再生機能を備えている。 20

【0051】

再生要求手段と一時再生手段の間は、例えば"bluetooth"のような近距離無線データ通信を用いて相互接続が実現され、パケットの交換が可能である。

【0052】

各々の再生要求手段は、通常、暗号化コンテンツとこれに対応するトークンを保有しており、あらかじめ暗号化コンテンツだけを一時再生手段に転送しておく。

【0053】

再生要求手段が一時再生手段に対してコンテンツの再生要求を発行すると、一時再生手段は、コンテンツの復号化に必要なトークンの送付を再生要求手段に要求する。該トークン要求は、好ましくは、再生要求されたコンテンツの識別子と、一時再生手段のデジタル署名を含んでいる。また、再生要求手段が複数存在する場合には、一時再生手段はトークン送付要求を一斉送信してもよい。 30

【0054】

再生要求手段は、トークン送付要求を受信すると、デジタル署名を基に一時再生手段を認証する。そして、認証が成功裏に終了した場合にのみトークンを返信し、認証に失敗した場合にはトークンの不正利用を防止するためにトークンの返信を行わない。また、トークンは秘密性の高い情報なので、一時再生手段の公開鍵などで暗号化して送付することが好ましい。

【0055】

トークンを受け取った一時再生手段は、暗号化コンテンツを復号化してこれを再生することができる。すなわち、本来的に暗号化コンテンツを所有する再生要求手段は、自らコンテンツ再生を行わない代わりに、高機能な再生能力を持つ一時再生手段において、安全にコンテンツ再生を実行させることができる。 40

【0056】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0057】

【発明の実施の形態】

本明細書中では、本発明の具体的な実施の形態として、車載用オーディオ機器を搭載した自動車内に、暗号化コンテンツとのそのトークンを正規に所有する複数のユーザが各自の 50

携帯型機器を持ち込み、それぞれの機器間は無線LANのような伝送路で相互接続されているような局所的な機器間環境を具体例として取り上げることにする。以下、図面を参照しながら本発明の実施例について詳解する。

【0058】

図1には、本発明の実施に供される携帯型機器10のハードウェア構成を模式的に示している。携帯型機器の一例は、いわゆる「多機能携帯端末」と呼ばれる製品であり、携帯電話機能やインターネット・アクセス機能を装備して音楽コンテンツをダウンロードするだけでなく、音楽コンテンツの再生機能や、さらに近隣の他の機器へデータやコンテンツを転送するための機器間無線通信機能などを備えている。

【0059】

同図に示すように、携帯型機器10は、機器内部の動作を統括的に制御する中央制御部11の他に、無線電波を送受信するためのRF送受信部12と、音楽コンテンツを蓄積するコンテンツ蓄積部13と、中央制御部11のためのローカル・メモリ14と、音楽コンテンツを再生して音声データとして外部出力するための再生部15と、車載用オーディオ機器50（後述）との間で近距離無線データ通信などの手段により相互接続するためのインターフェース部16とで構成される。

【0060】

この携帯型機器10が暗号化音楽コンテンツや、その正当な使用許諾としてのトークンを入手するためには、例えば、所定のコンテンツ・プロバイダのアクセス・ポイントに携帯電話回線などで接続して、RF送受信部12によって受信する。暗号化音楽コンテンツはコンテンツ格納部13に蓄積され、また、トークンはローカル・メモリ14に保存される。

【0061】

ローカル・メモリ14は、機器10の動作制御用のプログラム・コードを不揮発的に格納する機能部分と、トークンその他の中央制御部11の作業データを一時的又は揮発的に書き込むための機能部分とで構成される。本実施例において利用するプログラム・コードや作業データの一部は秘密性が高いので、中央制御部11及びローカル・メモリ14を耐タンパ性のあるLSI (Large Scale Integration) チップで構成することが好ましい。

【0062】

この携帯型機器10上で音楽コンテンツを再生するためには、中央制御部11は、コンテンツ格納部13から所望の暗号化音楽コンテンツを読み出すとともに、該当するトークンをローカル・メモリ14から取り出して、トークンを利用して音楽コンテンツを復号化して、再生部15にて音声出力する。なお、コンテンツ再生は、コンテンツをコンテンツ格納部13に蓄積することなく、コンテンツ受信とリアルタイムで再生動作を行ってもよい。

【0063】

携帯型機器10は、スタンドアロン状態で音楽コンテンツの再生を行う場合のためには、オーディオ・アンプ及びスピーカなどからなる再生部15が必要である。但し、車載用オーディオ機器50側のコンテンツ再生機能をもっぱら利用する場合には、再生部15は不要となる。

【0064】

また、携帯型機器10上で一旦蓄積された音楽コンテンツを、インターフェース部16経由で、車載用オーディオ機器50などの外部機器に転送して、外部で再生することもできる。但し、その手順の詳細については後述に譲る。

【0065】

また、図2には、本発明の実施に供される携帯型機器の他の形態10-2について模式的に図解している。

【0066】

同図に示すように、携帯型機器10-2は、機器内部の動作を統括的に制御する中央制御部11の他に、音楽コンテンツを担持したメディアからデータを読み取るためのメディア

10

20

30

40

50

読取部 17 と、中央制御部 11 のためのローカル・メモリ 14 と、音楽コンテンツを再生して音声データとして外部出力するための再生部 15 と、車載用オーディオ機器 50（後述）との間で近距離無線データ通信などの手段により相互接続するためのインターフェース部 16 とで構成される。

【0067】

この携帯型機器 10 - 2 が暗号化音楽コンテンツを入手するためには、所望のメディアをメディア読取部 17 に装填すればよい。また、コンテンツの正当な使用許諾としてのトークンは、メディアと同一又は別個の流通経路を経て入手することができ、図 2 には示していないコンソールを介して機器 10 - 2 内に入力することができる。トークンは、ローカル・メモリ 14 に保存される。

10

【0068】

ローカル・メモリ 14 は、機器 10 - 2 の動作制御用のプログラム・コードを不揮発的に格納する機能部分と、トークンその他の中央制御部 11 の作業データを一時的又は揮発的に書き込むための機能部分とで構成される。本実施例において利用するプログラム・コードや作業データの一部は秘密性が高いので、中央制御部 11 及びローカル・メモリ 14 を耐タンパ性のある LSI チップで構成することが好ましい。

【0069】

この携帯型機器 10 - 2 上で音楽コンテンツを再生するためには、中央制御部 11 は、メディア読取部 17 によって装填したメディア上から所望の暗号化音楽コンテンツを読み出すとともに、該当するトークンをローカル・メモリ 14 から取り出して、トークンを利用して音楽コンテンツを復号化して、再生部 15 にて音声出力する。

20

【0070】

携帯型機器 10 - 2 は、スタンドアロン状態で音楽コンテンツの再生を行う場合のためには、オーディオ・アンプ及びスピーカなどからなる再生部 15 が必要である。但し、車載用オーディオ機器 50 側のコンテンツ再生機能をもっぱら利用する場合には、再生部 15 は不要となる。

【0071】

また、携帯型機器 10 - 2 上で一旦蓄積された音楽コンテンツを、インターフェース部 16 経由で、車載用オーディオ機器 50 などの外部機器に転送して、外部で再生することもできる。但し、その手順の詳細については後述に譲る。

30

【0072】

図 3 には、本発明の実施に供される車載用オーディオ機器 50 のハードウェア構成を模式的に示している。この車載用オーディオ機器 50 は、図 1 及び図 2 を参照しながら説明した携帯型機器 10 とは、例えば近距離無線データ通信技術を用いて接続することができる。すなわち、各乗員が車内に携帯型機器 10 を持ち込むことで、車載用オーディオ機器 50 は複数の携帯型機器 10 と交信して、これらとの協働的動作により、高機能な音楽コンテンツ再生サービスを実現することができる（後述）。

【0073】

図 3 に示すように、車載用オーディオ機器 50 は、機器内部の動作を統括的に制御する中央制御部 51 の他に、中央制御部 51 のためのローカル・メモリ 54 と、音楽コンテンツを再生して音声データとして外部出力するためのオーディオ・アンプやスピーカからなる再生部 55 と、携帯型機器 10（前述）との間で近距離無線データ通信などの手段により相互接続するためのインターフェース部 56 と、各乗員の携帯型機器 10 から送られてくる暗号化音楽コンテンツを蓄積するコンテンツ蓄積部 53 とを備えている。

40

【0074】

さらに、携帯型機器 10 が車内にインストールされない状態でも、音楽コンテンツの再生を楽しむために、車載用オーディオ機器 50 自身も、音楽コンテンツを担持したメディアからデータを読み取るためのメディア読取部 57 を備えていてもよい。

【0075】

各乗員が車内に携帯型機器 10 を持ち込むと、例えば近距離無線データ通信機能を用いて

50

、各機器 10 は、車載用オーディオ機器 50 が提供する実行環境に動的にインストールされる。そして、各々の携帯型機器 10 が暗号化音楽コンテンツを車載用オーディオ機器 50 に転送することで、車載用オーディオ機器 50 においてすべての音楽コンテンツの再生動作を一元的に集中管理することができる。

【0076】

車載用オーディオ機器 50 上で暗号化音楽コンテンツを再生するためには、元のコンテンツ所有者すなわち携帯型機器 10 側から該当するトークンを譲り受ける必要がある。但し、携帯型機器 10 が無制限にトークンを譲渡したのでは、音楽コンテンツに関する著作権保護が危ぶまれる。そこで、本実施例では、各携帯型機器 10 は、後述する所定の認証手続きを成功した車載用オーディオ機器 50 にのみトークンの譲渡を許可するようになって

10

【0077】

認証手続きに成功する車載用オーディオ機器 50 の必須の条件は、受け取ったトークンを一時的にのみ保持し、音楽コンテンツの再生など必要な時期を経過すると自動的にトークンを廃棄すること、トークンを転用したり他の機器に勝手に転送しないことなど、トークンの使用制限を遵守すること（すなわち、コンテンツに関する著作権保護を確約する機器であること）である。

【0078】

認証手続きに必要なデジタル署名や秘密鍵は、ローカル・メモリ 54 内に保管される。ローカル・メモリ 54 は、機器 50 の動作制御用のプログラム・コードを不揮発的に格納する機能部分と、トークンその他の中央制御部 51 の作業データを一時的又は揮発的に書き込むための機能部分とで構成される。本実施例において利用するプログラム・コードや作業データの一部は秘密性が高いので、中央制御部 51 及びローカル・メモリ 54 を耐タンパ性のある LSI チップで構成することが好ましい。

20

【0079】

なお、ここで言う「秘密鍵」とは公開鍵暗号系の秘密鍵のことである。公開鍵暗号方式は、一方の鍵で暗号化すると他方の鍵でしか復号化することができないような 2 種類の鍵（非対称鍵）を用いた暗号方式のことである。一方の鍵をユーザ本人しか知らない秘密鍵とし、他方の鍵を第三者に公開する公開鍵として用いることで、公開鍵で暗号化した秘密文書や、秘密鍵で暗号化したデジタル署名を利用することが可能となる（周知）。

30

【0080】

次いで、携帯型機器 10 と車載用オーディオ機器 50 との協働的動作によって実現される音楽コンテンツ再生サービスの処理手順について説明する。ここで言う音楽コンテンツの再生は、車載用オーディオ機器 50 による一時的若しくは 1 回限りのコンテンツ再生を意味することを理解されたい。

【0081】

図 4 には、携帯型機器 10 と車載用オーディオ機器 50 との間で実現される音楽コンテンツ再生サービスの処理手順を図解している。但し、同図に示す例では、説明の簡素化のため、携帯型機器 10 と車載用オーディオ機器 50 を一対一の関係とする。また、図示の例では、携帯型機器 10 は、音楽コンテンツの再生を要求する「再生要求機」として機能するとともに、車載用オーディオ機器 50 側は該要求に応答して一時的にコンテンツ再生を行う「一時再生機」として機能するものとする。

40

【0082】

本実施例に係る車載用オーディオ機器 50 が搭載されている車内に携帯型機器 10 を持ち込むことにより、携帯型機器 10 は近距離無線データ通信により車載用オーディオ機器 50 に接続される。近距離無線データ通信の一例は、"bluetooth" である。

【0083】

再生要求を発行する前に、携帯型機器 10 は、自ら蓄積している暗号化音楽コンテンツをあらかじめ一時再生機 50 側に転送しておく（T1）。

【0084】

50

図5には、暗号化音楽コンテンツのデータ構造の例を示している。同図に示すように、暗号化音楽コンテンツは、データ本体61とヘッダ部62で構成されている。データ本体は、音楽コンテンツを格納するためのフィールドであり、暗号化された状態で書き込まれる。他方のヘッダ部62には、曲名やアーティスト名、コンテンツID（例えばISRC（International Standard Recording Code））などの制御情報が含まれている。曲名などの制御情報を、一時再生機50の認証手続きの前に利用可能にするために、ヘッダ部62は暗号化されない平文の状態であることが好ましい。

【0085】

一時再生機50側では、このような暗号化音楽コンテンツを受け取ると、これをそのままコンテンツ蓄積部53に格納しておく（S1）。

10

【0086】

次いで、再生要求機10側では、携帯型機器10に備わるコンソール（図示しない）によって、一時再生機50側に対して再生要求を発行する（T2）。

【0087】

この再生要求は、特定の楽曲の再生を指示する「再生指示パケット」として、近距離無線データ通信により送信される。図6には、再生指示パケットのデータ構造を例示している。同図に示すように、再生指示パケットは、再生コマンドと、曲名に相当するコンテンツIDとを含んでおり、特定の楽曲の再生を指定することができる。

【0088】

暗号化音楽コンテンツを再生するためには、該当するトークンが必要である。そこで、一時再生機50側では、再生要求機10から受け取ったパケットが再生指示パケットであることを判断すると、自身のデジタル署名を含んだトークン要求パケットを生成して（S2）、該要求パケットを近距離無線データ通信を用いて再生要求機10側に送信する（T3）。

20

【0089】

図7には、トークン要求パケットのデータ構造を例示している。同図に示すように、トークン要求パケットは、トークン要求コマンドと、曲名に相当するコンテンツIDと、デジタル署名とで構成されている。また、デジタル署名は、一時再生機50自身の公開鍵と、認証処理に用いる特定の文字列とで構成される。

【0090】

トークン要求コマンド及びコンテンツIDは平文形式である。これに対し、デジタル署名は、認証用秘密鍵で暗号化された秘密データで構成されているので、不正使用者によるなりすましを防止することができる。また、デジタル署名は、一時再生機すなわち車載用オーディオ機器50の製造時に耐タンパ性のある回路チップ内にあらかじめ書き込まれていることが好ましい。

30

【0091】

認証用の秘密鍵及び公開鍵は、例えば、携帯型機器10及び/又は車載用オーディオ機器50の製造業者などにより管理される。このうち認証用の公開鍵の方は、携帯型機器10を含む一般第三者が広く利用することができる。なお、本発明を好適に実現する上では、製造業者及びその製品は、コンテンツの著作権保護を確約することを前提とする。

40

【0092】

再生要求機10側では、このトークン要求パケットを受け取ると、該パケットからデジタル署名を切り出して、一時再生機50の認証を行う（S11）。この認証手続きは、より具体的には、デジタル署名を認証用公開鍵（前述）で復号化して、認証用の特定文字列が意味のある形態で復元することができたか否かを判断することで行われる。

【0093】

認証手続きが成功裏に終了した場合、再生要求機10は、トークン要求パケット内に含まれるコンテンツIDに相当するトークンを取り出し、そのコピーをデジタル署名から復元された一時再生機10の公開鍵で暗号化する（S12）。そして、この暗号化されたトークンのコピーを、近距離無線データ通信を用いて一時再生機50側に返信する（T4）。

50

【 0 0 9 4 】

トークンのコピーを受け取った一時再生機 5 0 側では、自分自身の秘密鍵を用いてこれを復号化して、トークンを取り出す (S 3)。そして、トークンを揮発的な状態で保持する (S 4)。

【 0 0 9 5 】

ここで言う揮発的な状態とは、トークンを長期間保存せず携帯型機器 1 0 が車外に搬出される時期にトークンを廃棄することの他、トークンを複製したり外部の機器に無断で転送したりしないことを含み、略言すれば正規ユーザの証しであるトークンを著作権の使用許諾の範囲 (若しくは取引の通念上許容し得る範囲) でのみ保存することを意味する。

【 0 0 9 6 】

一時再生機 5 0 は、再生要求された音楽コンテンツをコンテンツ蓄積部 5 3 から取り出すとともに、取得したトークンを用いてこれを復号化する (S 5)。そして、D A (Digital-Analog) 変換して音声データに再現して (S 6)、オーディオ・アンプ及びスピーカなどからなる再生部 5 5 によって外部出力する (S 7)。

【 0 0 9 7 】

なお、再生要求機 1 0 及び一時再生機 5 0 の各々の側において、斜線で示されている部分は、外部からの侵入・解読・漏洩・改竄などの危険を排した安全な処理を行う必要がある。したがって、これら斜線領域に該当するプログラム・コードは非分割処理として構成されるとともに、耐タンパ性のある回路装置上に実装されていることがより好ましい。

【 0 0 9 8 】

上記の説明では、例えば特定の自動車内において携帯型機器 1 0 と車載用オーディオ機器 5 0 とが一对一の関係にある場合について限定した。このような場合、図 8 に示すように、ユーザは、携帯型機器 1 0 のコンソール画面を介して、音楽コンテンツの転送、再生指示、一時再生認証などを行うことができる。

【 0 0 9 9 】

しかしながら、多くの場合、単一の車内に数人が乗り合う結果として、複数の携帯型機器 1 0 が共存するとともに 1 台の車載用オーディオ機器 5 0 を共有することになる。このような場合、携帯型機器 1 0 と車載用オーディオ機器 5 0 とは、一对一ではなく多対一の関係形成し、図 9 に示すように、1 台の車載用オーディオ機器 5 0 が、複数の携帯型機器 1 0 から音楽コンテンツを取得したり、複数の携帯型機器 1 0 からの再生要求を捌くことになる。

【 0 1 0 0 】

本発明は、携帯型機器 1 0 と車載用オーディオ機器 5 0 とが多対一関係を形成する場合であっても、上述と同様に好適に動作するが、このことを図 1 0 に示すチャートを参照しながら以下に詳解する。但し、図 1 0 中で示す各機器間のトランザクションは、原則として、近距離無線データ通信を用いて行われるものとする。

【 0 1 0 1 】

まず、各乗員が自分の携帯型機器 # 1 , # 2 , # 3 ... を車内に持ち込むと、近距離無線データ通信を用いることで、車載用オーディオ機器すなわち一時再生機 5 0 との間で接続が確立する。

【 0 1 0 2 】

このような状態で、各携帯型機器 # 1 , # 2 , # 3 ... は自分が蓄積している暗号化コンテンツを、順次、一時再生機 5 0 側に転送する。

【 0 1 0 3 】

暗号化音楽コンテンツは、図 5 を参照して説明したように、暗号化コンテンツからなるデータ本体 6 1 と平文のままのヘッダ部 6 2 で構成される。したがって、一時再生機 5 0 側では、各音楽コンテンツに関する認証手続きやトークン送付 (後述) を行う前に、収集した音楽コンテンツに関する曲名リストを生成することができる。

【 0 1 0 4 】

車内に居る各携帯型機器 # 1 , # 2 , # 3 ... は、一時再生機 5 0 に対して曲名リストの送

10

20

30

40

50

付を要求することができる。これに回答して、一時再生機 5 0 は、曲名リストをパケット形式で返信する。

【 0 1 0 5 】

図 1 1 には、曲名リスト送付パケットのデータ構造を例示している。同図に示すように、曲名リストは、各音楽コンテンツのヘッダ部を切り出したものを所定フォーマットに従い連結したものでよい。

【 0 1 0 6 】

曲名リスト送付パケットを受信した各携帯型機器 # 1 , # 2 , # 3 ... 側では、一時再生機 5 0 において再生サービスが提供される曲名リストをコンソール・パネル上に表示することができる。また、各携帯型機器のユーザは、コンソール・パネル上で所望の楽曲を選曲することができる。選曲した結果、携帯型機器は一時再生機 5 0 に対して再生要求を発行する。この再生要求は、図 6 に示すように、選曲された楽曲に相当するコンテンツ ID を付した再生指示パケットの形式で送付される。

10

【 0 1 0 7 】

他方、一時再生機 5 0 側では、暗号化音楽コンテンツを再生するためには、該当するトークンが必要である。そこで、一時再生機 5 0 は、自身のデジタル署名を含んだトークン要求パケットを生成して、各携帯型機器 # 1 , # 2 , # 3 ... に対してブロードキャスト（一斉送信）する。

【 0 1 0 8 】

トークン要求パケットのデータ構造は、図 7 を参照しながら既に説明した通りである。すなわち、トークン要求パケットは、トークン要求コマンドと、曲名に相当するコンテンツ ID と、デジタル署名で構成されている。デジタル署名は、一時再生機 5 0 自身の公開鍵と、認証処理に用いる特定の文字列とで構成される。トークン要求コマンド及びコンテンツ ID は平文形式である。これに対し、デジタル署名は、認証用秘密鍵で暗号化されているので、不正使用者によるなりすましを防止することができる。

20

【 0 1 0 9 】

図 1 2 には、トークン要求パケットを受信したときに各携帯型機器 # 1 , # 2 , # 3 ... が実行する処理手順をフローチャートの形式で示している。以下、このフローチャートに従って説明する。

【 0 1 1 0 】

携帯型機器 1 0 は、まず、トークン要求パケットの中からデジタル署名を取り出し、これを認証用公開鍵（前述）で復号化して（ステップ S 5 1 ）、認証作業を行う（ステップ S 5 2 ）。該認証作業では、デジタル署名の中から認証用の特定文字列を意味のある形式で復元することができたか否かを判断する。

30

【 0 1 1 1 】

認証に失敗した場合には、トークンを要求した一時再生機 5 0 がなりすましすなわち不正な再生装置である可能性があるので、トークン送付処理を行わず、本処理ルーチン全体を打ち切る。

【 0 1 1 2 】

他方、認証が成功裏に終了した場合には、携帯型機器 1 0 は、トークン要求パケット中で指定されたコンテンツ ID に相当するトークンを自身が保有するか否か（言い換えれば、自身が当該コンテンツの正当なユーザであるか否か）、探索してみる（ステップ S 5 3 ）。

40

【 0 1 1 3 】

該当するトークンを発見できなかった場合には、自身が当該コンテンツの正当なユーザではないので、トークン送付処理を行わず、本処理ルーチン全体を打ち切る。

【 0 1 1 4 】

他方、該当するトークンを発見できた場合には、トークンのコピーを、デジタル署名中に含まれている一時再生機 5 0 の公開鍵で暗号化して、一時再生機 5 0 に返信する（ステップ S 5 5 ）。

50

【0115】

一時再生機50側では、トークンのコピーを受け取ると、自らの秘密鍵でこれを復号化してトークンを得ることができる。この結果、再生要求された音楽コンテンツを再生することが可能になる。

【0116】

なお、"bluetooth"などのような近距離無線データ通信は、無線データの到達範囲がカー・ステレオなどの音声が届く範囲とほとんど同等である。したがって、車載用オーディオ機器50が近距離無線データ通信によりトークンを保持する携帯型機器10の存在を認識できるような場合には、トークンの所有者自身が音楽コンテンツを聴くことになるので、元の携帯型機器以外の再生装置上でコンテンツ再生を行っても、著作権の観点から問題はないものと思料される。また、このような状況下において、トークン所有者ではない他の携帯型機器から再生要求が発行されても、同様に権利解釈上の問題がないものと解される。

10

【0117】

本実施例に係る音楽コンテンツの再生方式によれば、再生指示を受け取った一時再生機にトークン又はそのコピーが安全に自動転送されるので、携帯型機器10及び車載オーディオ機器50の間でトークンを移動させる手間を省くことができる。

【0118】

また、携帯型機器のユーザがコンテンツ再生を要求する再生機を逐次的に切り替えるような場合であっても、各一時再生機は、トークンを揮発的にのみ保持し、無断で他の用途に転用しないことが保証されているので、トークンの管理が簡素化される。

20

【0119】

また、再生要求機と一時再生機とが多対多の関係を形成している場合にも、本発明を適用することができる。この場合、同一の音楽コンテンツが複数の一時再生機上にある場合も想定される。このような場合、どの再生機にトークンを送るべきかはユーザすなわちトークンの正当な所有者が決めるべきことであり、音楽コンテンツ転送とは別にトークン転送の手続きが必要となる。

【0120】

すなわち、本発明によれば、再生機を変える毎に逐次必要な手続を繰り返すという手間を省くことができる。

30

【0121】

メディア同様、トークンの場合も、置き忘れ、紛失、取り違いなどの問題が発生し得ることは既に述べた通りである。例えば、何台もの自動車に乗り分けてドライブに行き、途中で乗員が自動車を乗り換えるような場合、どの自動車に音楽コンテンツを転送したか、あるいはどの自動車にトークンを置き去りにしたかなど、交錯してしまう。

【0122】

これに対し、本発明によれば、認証を得た信頼の置ける一時再生機にトークンのコピーを送付するので、元の再生要求機はトークンを回収する必要がなく、トークンを置き去りにしてしまうという心配が全くない。

【0123】

[追補]

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

40

【0124】

【発明の効果】

以上詳記したように、本発明によれば、音楽や映像などのようにコンテンツ作成者等が著作権を始めとする所定の使用权を有するコンテンツを安全に(すなわち著作権を保護しつ

50

つ)利用することができる、優れたコンテンツ再生技術を提供することができる。

【0125】

また、本発明によれば、トークンを利用して暗号化コンテンツの使用を許可することで著作権保護を行うことができる、優れたコンテンツ再生技術を提供することができる。

【0126】

また、本発明によれば、暗号化コンテンツのトークンを所有する複数のユーザ間でコンテンツを共有することができる、優れたコンテンツ再生技術を提供することができる。

【図面の簡単な説明】

【図1】本発明の実施に供される携帯型機器10のハードウェア構成を模式的に示した機能ブロック図である。

10

【図2】本発明の実施に供される携帯型機器の他の形態10-2を模式的に示した機能ブロック図である。

【図3】本発明の実施に供される車載用オーディオ機器50のハードウェア構成を模式的に示した機能ブロック図である。

【図4】携帯型機器10と車載用オーディオ機器50との間で実現される音楽コンテンツ再生サービスの処理手順を示したチャートである(但し、携帯型機器10と車載用オーディオ機器50を一对一の関係とする)。

【図5】暗号化音楽コンテンツ送付パケットのデータ構造の例を示した図である。

【図6】再生指示パケットのデータ構造の例を示した図である。

【図7】トークン要求パケットのデータ構造の例を示した図である。

20

【図8】車内での携帯型機器10を用いた操作手順を描写した図である。

【図9】車内での携帯型機器10を用いた操作手順を描写した図である。

【図10】携帯型機器10と車載用オーディオ機器50とが多対一の関係を形成した場合における各機器の動作手順を示したチャートである。

【図11】曲名リスト送付パケットのデータ構造の例を示した図である。

【図12】トークン要求パケットを受信したときの携帯型機器10が実行する処理手順を示したフローチャートである。

【符号の説明】

10...携帯型機器

11...中央制御部

12...RF送受信部

13...コンテンツ格納部

14...メモリ

15...再生部

16...インターフェース部

17...メディア読取部

50...車載用オーディオ機器

51...中央制御部

53...コンテンツ格納部

54...メモリ

55...再生部

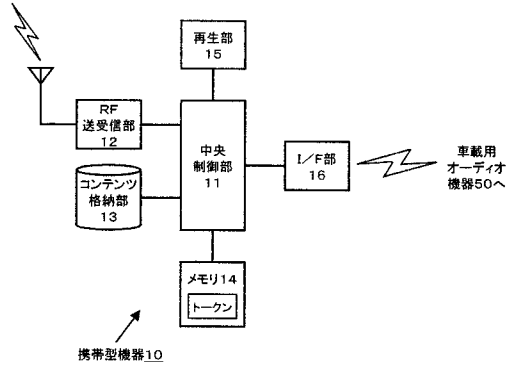
56...インターフェース部

57...メディア読取部

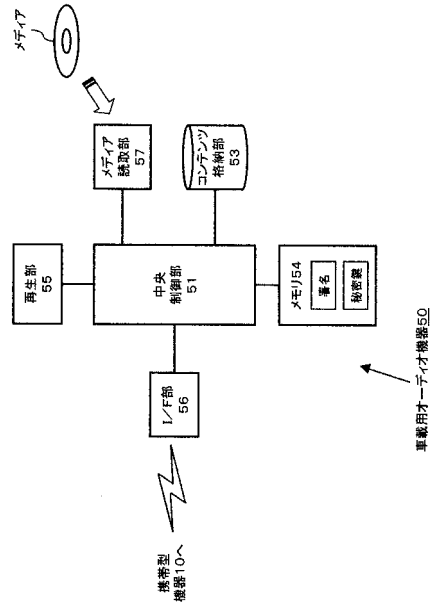
30

40

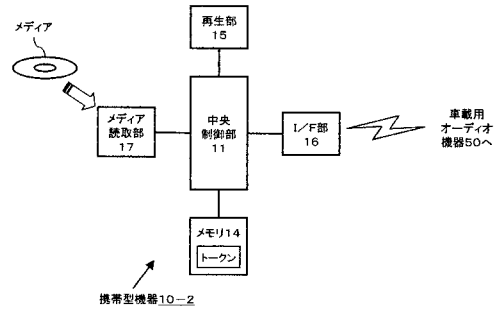
【図 1】



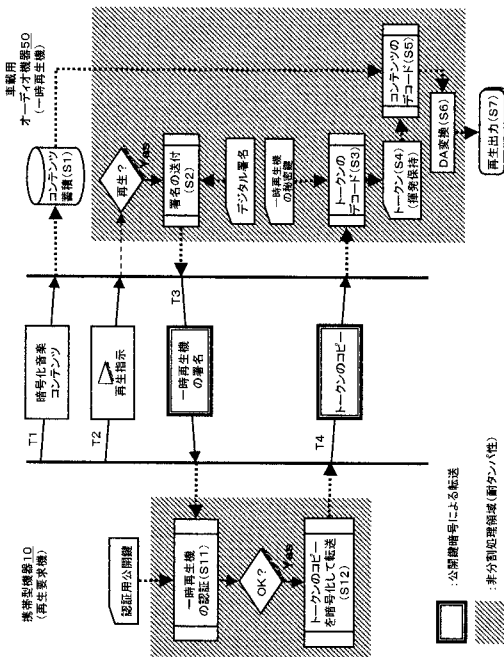
【図 3】



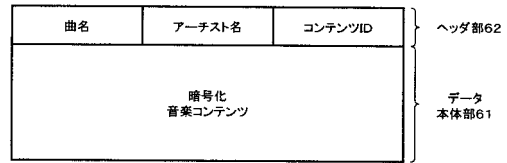
【図 2】



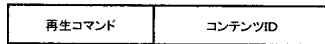
【図 4】



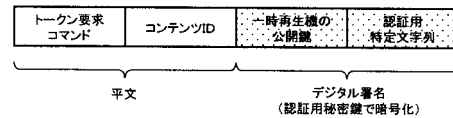
【図 5】



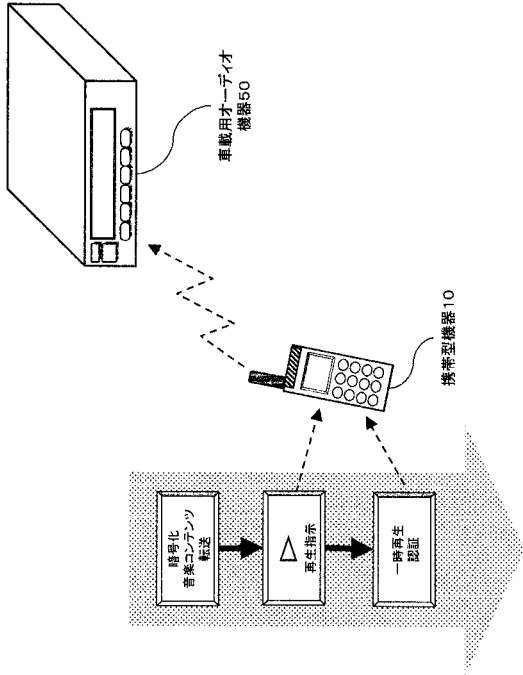
【図 6】



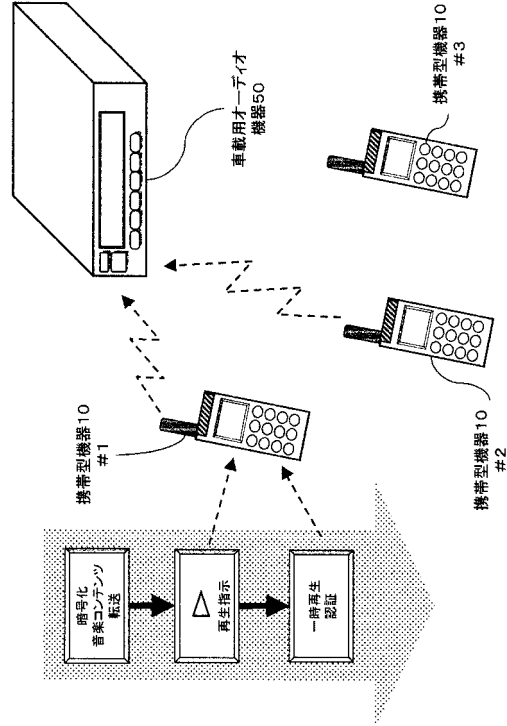
【図 7】



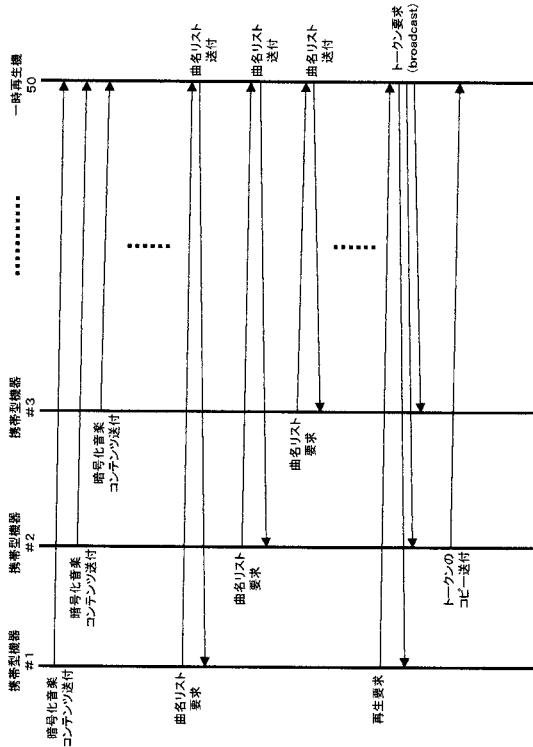
【図8】



【図9】



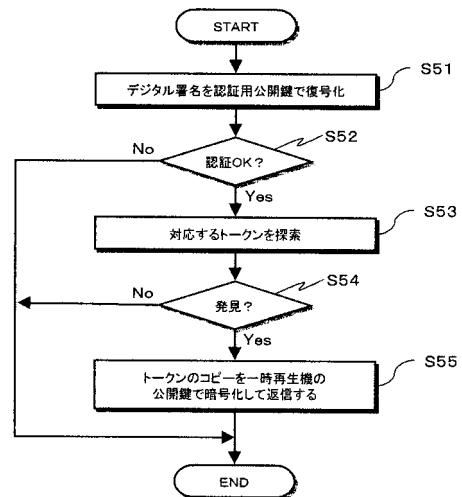
【図10】



【図11】

曲名	アーティスト名	コンテンツID
曲名	アーティスト名	コンテンツID
曲名	アーティスト名	コンテンツID
曲名	アーティスト名	コンテンツID

【図12】



フロントページの続き

(51) Int. Cl. F I
H 0 4 N 7/081 (2006.01) H 0 4 N 7/167 Z
H 0 4 N 7/167 (2006.01)

審査官 高野 美帆子

(56) 参考文献 特開平 1 1 - 3 2 8 8 5 0 (J P , A)
特開 2 0 0 1 - 0 1 6 3 2 5 (J P , A)

(58) 調査した分野 (Int. Cl. , D B 名)

G11B 20/10
G06F 12/14
G06F 15/00
G06F 21/00
G09C 1/00
H04L 9/10
H04N 7/08
H04N 7/081
H04N 7/167