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

特許第4294322号
(P4294322)

(45)発行日　平成21年7月8日(2009.7.8)　(24)登録日　平成21年4月17日(2009.4.17)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	560B
G06F 1/00	(2006.01)	G06F	12/14	520D
G11B 20/10	(2006.01)	G06F	12/14	520P
H04L 9/08	(2006.01)	G06F	12/14	530C
		G06F	12/14	530E

請求項の数 10　(全 19 頁)　最終頁に続く

(21)出願番号　特願2002-571970 (P2002-571970)
(86)(22)出願日　平成14年1月28日 (2002.1.28)
(65)公表番号　特表2004-534291 (P2004-534291A)
(43)公表日　平成16年11月11日 (2004.11.11)
(86)国際出願番号　PCT/IB2002/000245
(87)国際公開番号　WO2002/073378
(87)国際公開日　平成14年9月19日 (2002.9.19)
審査請求日　平成17年1月7日 (2005.1.7)
(31)優先権主張番号　01200898.3
(32)優先日　平成13年3月12日 (2001.3.12)
(33)優先権主張国　欧州特許庁 (EP)

(73)特許権者　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　１
(74)代理人　100087789
弁理士　津軽　進
(74)代理人　100092048
弁理士　沢田　雅男
(72)発明者　ベル　ヘンドリック　ジェイ
オランダ国　５６５６　アー　アー　アインドーフェン　プロフホルストラーン　６

最終頁に続く

(54)【発明の名称】コンテンツアイテムを保護しながら記憶するための受信デバイスおよび再生デバイス

(57)【特許請求の範囲】

【請求項１】

コンテンツアイテムを保護しながら記憶するための受信デバイスであって、

前記コンテンツアイテムをダウンロードするためのダウンロード手段と、

前記ダウンロードされたコンテンツアイテムを記憶媒体に書き込むための書き込み手段と、

ライセンスサーバからライセンスファイルを獲得するためのライセンシング手段であって、前記ライセンスファイルが、少なくとも、前記ダウンロードされたコンテンツアイテムを前記記憶媒体に書き込む許可を有するライセンシング手段と、を有する受信デバイスにおいて、

再生デバイスのグループに連係する暗号化キーで前記ライセンスファイルを暗号化するための、また、前記暗号化されたライセンスファイルを前記記憶媒体に書き込むために前記暗号化されたライセンスファイルを前記書き込み手段に供給するための、ライセンスロッキング手段を有し、

前記ライセンスロッキング手段が、さらに、前記グループの選択された識別子を受信するように、また、前記選択された識別子に連係する前記暗号化キーをキーサーバから獲得するように、構成されていることを特徴とする受信デバイス。

【請求項２】

前記ライセンスロッキング手段が、ライセンスロッカ暗号化キー(LLEK)で前記ライセンスファイルを暗号化するように、また、前記再生デバイスのグループに連係する前記暗号

化キーで前記LLEKを暗号化するように、さらに、前記暗号化されたLLEKを前記記憶媒体に書き込むために前記暗号化されたLLEKを前記書き込み手段に供給するように、構成されていることを特徴とする請求項1に記載の受信デバイス。

【請求項３】

前記暗号化キーが、公開／秘密キーペアの前記公開キーであることを特徴とする請求項1に記載の受信デバイス。

【請求項４】

前記コンテンツアイテムが、オーディオデータ、ビデオデータの少なくとも1つを有することを特徴とする請求項1に記載の受信デバイス。

【請求項５】

記憶媒体上に記憶されているコンテンツアイテムをかけるための再生デバイスであって、

前記記憶媒体上に記憶されている、前記コンテンツアイテムに対するライセンスファイル内の許可にしたがって、前記コンテンツアイテムを再生するための再生手段を有する再生デバイスにおいて、

前記ライセンスファイルが、前記記憶媒体上に暗号化されて記憶されていること、および、さらに、

1つ以上の解読キーを記憶するための保護記憶手段であって、各解読キーが再生デバイスのそれぞれのグループに連係している保護記憶手段と、

記憶されている解読キーが、前記暗号化されているライセンスファイルを解読するのに適しているか否かを確認するための復調手段であって、もしそうであれば、

前記記憶されている解読キーを用いて前記ライセンスファイルを解読し、そして、前記解読されたライセンスファイルを前記再生手段に供給するための復調手段と、

前記再生デバイスに連係する公開／秘密キーペアの公開キーをコンテンツ配信管理システム(CDMS)に登録するための登録手段であって、当該公開／秘密キーペアの前記秘密キーが前記保護記憶手段に記憶されている登録手段において、当該公開キーで暗号化されている、再生デバイスのグループに連係する解読キーを受信して、当該暗号化されている解読キーを解読し、そして、当該解読キーを前記保護記憶手段に記憶させる登録手段とを、有することを特徴とする再生デバイス。

【請求項６】

前記ライセンスファイルが、ライセンスロッカ暗号化キー(LLEK)で暗号化されて記憶されており、当該LLEKが、LLEK暗号化キーで暗号化されて前記記憶媒体に記憶されており、前記1つ以上の解読キーが、LLEK解読キーであり、前記復調手段が、記憶されているLLEK解読キーが前記暗号化されているLLEKを解読するのに適しているか否かを確認し、もしそうであれば、前記記憶されているLLEK解読キーを用いて前記暗号化されているLLEKから前記LLEKを獲得し、前記LLEKを用いて前記ライセンスファイルを解読するように構成されていることを特徴とする請求項5に記載の再生デバイス。

【請求項７】

前記コンテンツアイテムが、オーディオデータ、ビデオデータの少なくとも1つを有することを特徴とする請求項5に記載の再生デバイス。

【請求項８】

前記記憶されている解読キーが、公開／秘密キーペアの前記秘密キーであることを特徴とする請求項5に記載の再生デバイス。

【請求項９】

受信デバイスとして機能するように実行されるときに、プログラム可能なデバイスをイネーブルにするためのコンピュータプログラムであって、

コンテンツアイテムをダウンロードするためのダウンロード手段と、

前記ダウンロードされたコンテンツアイテムを記憶媒体に書き込むための書き込み手段と、

ライセンスサーバからライセンスファイルを獲得するためのライセンシング手段であっ

て、前記ライセンスファイルが、少なくとも、前記ダウンロードされたコンテンツアイテムを前記記憶媒体に書き込む許可を有するライセンシング手段と、を有するコンピュータプログラムにおいて、

再生デバイスのグループに連係する暗号化キーで前記ライセンスファイルを暗号化するための、また、前記暗号化されたライセンスファイルを前記記憶媒体に書き込むために前記暗号化されたライセンスファイルを、前記コンテンツアイテムを前記記憶媒体に書き込むための書き込み手段に供給するための、ライセンスロッキング手段を有し、

前記ライセンスロッキング手段が、さらに、前記グループの選択された識別子を受信するように、また、前記選択された識別子に連係する前記暗号化キーをキーサーバから獲得するように、構成されていることを特徴とするコンピュータプログラム。

【請求項１０】

再生デバイスとして機能するように実行されるときに、プログラム可能なデバイスをイネーブルにするためのコンピュータプログラムであって、

記憶媒体上に記憶されている、コンテンツアイテムに対するライセンスファイル内の許可にしたがって、前記コンテンツアイテムを再生するための再生手段を有するコンピュータプログラムにおいて、

前記ライセンスファイルが前記記憶媒体上に暗号化されて記憶されていること、および、さらに、

記憶されている解読キーが、前記暗号化されているライセンスファイルを解読するのに適しているか否かを確認するための復調手段であって、もしそうであれば、

前記記憶されている解読キーを用いて前記ライセンスファイルを解読し、そして、前記解読されたライセンスファイルを前記コンテンツアイテムを再生するための再生手段に供給するための復調手段と、

前記再生デバイスに連係する公開／秘密キーペアの公開キーをコンテンツ配信管理システム(CDMS)に登録するための登録手段であって、当該公開／秘密キーペアの前記秘密キーが保護記憶手段に記憶されている登録手段において、当該公開キーで暗号化されている、再生デバイスのグループに連係する解読キーを受信して、当該暗号化されている解読キーを解読し、そして、当該解読キーを前記保護記憶手段に記憶させる登録手段とを、有することを特徴とするコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、コンテンツアイテムを保護しながら記憶するための受信デバイスであって、前記コンテンツアイテムをダウンロードするためのダウンロード手段と、前記ダウンロードされたコンテンツアイテムを記憶媒体に書き込むための書き込み手段と、ライセンスサーバからライセンスファイルを獲得するためのライセンシング手段であって、前記ライセンスファイルが、少なくとも、前記ダウンロードされたコンテンツアイテムを前記記憶媒体に書き込む許可を有するライセンシング手段と、を有する受信デバイスに関するものである。

【０００２】

本発明は、さらに、記憶媒体に記憶されているコンテンツアイテムを再生するための再生デバイスであって、記憶媒体上に記憶されているコンテンツアイテムをかけるための再生デバイスであって、前記記憶媒体上に記憶されている、前記コンテンツアイテムに対するライセンスファイル内の許可にしたがって、前記コンテンツアイテムを再生するための再生手段を有する再生デバイスに関するものである。

【背景技術】

【０００３】

Napster (http://www.napster.com/)やGnutella (http://www.gnutella.co.uk/)のようなファイル共有サービスが、インターネット上で広く知られている。それらは、通常MP3フォーマットの、音楽などのコンテンツアイテムを交換するために、何百万人ものユーザ

に使用されている。各ユーザは、他の全ての人に、自分自身の音楽コレクションを提示することができ、それは、全ての人が、ダウンロードに利用可能な大きな音楽選集を持つことを可能にする。しかしながら、それらのファイル共有サービスに提示される音楽は、通常、ポピュラー音楽であり、著作権所有者の許可なしに提示される。著作権所有者が、自身の権利についてのロイヤリティを得ることを保証するために、ユーザに会費を請求し始めているファイル共有サービスもある。そうすると、会費収入の一部を、著作権所有者に支払うために用いることができる。

【０００４】

ユーザが、権限なしにダウンロードしたコンテンツアイテムを配信することを防止するために、それらのアイテムは、保護された状態で利用可能にされる。例えば、それらは、暗号化されたフォーマットで配信することができ、それによって、受信デバイス上のソフトウェアが、再生を許可するが、暗号化されていない形式で記憶することを許可しない。コンテンツアイテムを保護する1つの技術は、例えば、米国特許第5,892,900号によって公知である、Intertrust社 “Digifile“ 技術である。この特許によれば、音楽は、保護されたデジタルコンテナ、即ち、Digifileに記憶される。受信機は、ライセンスサーバからライセンスファイルを獲得しなければならない。このライセンスファイルは、一連の許可、例えば、音楽を再生する許可、あるいは、コンテンツアイテムを記憶媒体に記憶させる許可を備えている。ユーザは、もちろん、各許可に対して、一定の金額を支払わなければならない。ライセンスファイルは、また、Digifile内部の音楽にアクセスするために必要な暗号キー、あるいは、他の情報を含有している。再生デバイスが、1つのライセンスを獲得すると、それは、音楽を解読し、ユーザに対してそれをかけることができる。そのユーザは、そのDigifileを他人に配信することができるが、それらの他人は、彼ら自身のライセンスファイルを買わなければ、その音楽を解読することができない。コンテンツアイテムを保護する他の技術も、同様に動作する。

【０００５】

その許可は、そのDigifileと一緒に他のデバイスに転送でき、したがって、その他のデバイスは、そのコンテンツを再生できる。しかしながら、このことは、通常、その他のデバイスが、Digifileおよび許可を転送するために、その受信機に接続されているということを必要とする。そうでなければ、ライセンスファイルを、ユーザに結ぶこともできるが、これは、ユーザが、コンテンツを再生したいと思っている全てのデバイスに、自分自身を本人であると証明しなければならないという欠点を持っている。

【０００６】

公知の構成は、ユーザが、音楽を買って聴くということに関して、一般に慣れている考え方と合致しないという欠点を持っている。ユーザが、店でコンパクトディスク(CD)を購入するとき、彼は、一度支払えば、その後、彼の所有している全てのデバイスで、さらには、他人のものであるデバイスによっても、そのCDをかけることができる。彼は、その音楽を再生する度毎に支払わなければならないなどと予想もしないし、あるいは、他のデバイスに音楽を転送するのにやっかいな行動や、それに連係する許可を行わなければならないなどと考えもしない。さらに、使用ごとの支払い方式の場合、支払いを可能にし、かつ、ライセンスファイルを供給することができるように、再生デバイスは、ネットワークに接続されていなければならない。これは、これらの構成において、携帯デバイスを用いることを困難にする。

【０００７】

【特許文献１】米国特許第５,８９２,９００号

【発明の開示】

【課題を解決するための手段】

【０００８】

本発明の1つの目的は、冒頭に記載の受信デバイスであって、記憶媒体上のコンテンツアイテムの使用に永続的な制御を与え、さらに、ユーザの使用の考え方に合致した受信デバイスを提供することである。

【０００９】
この目的は、本発明によれば、再生デバイスのグループに連係する暗号化キーで前記ライセンスファイルを暗号化するための、また、前記暗号化されたライセンスファイルを前記記憶媒体に書き込むために前記暗号化されたライセンスファイルを前記書き込み手段に供給するための、ライセンスロッキング手段によって特徴付けられる受信デバイスにおいて実現される。コンテンツアイテムがそのような受信デバイスによって記憶される記憶媒体は、制限なくコピーできるが、それらのコンテンツアイテムは、暗号化キーに連係する、また、ライセンスファイルにしたがう、グループの再生デバイス上でしかかけることができない。
【００１０】
ユーザは、自分が、コンテンツアイテムをかけたいと思う再生デバイスのグループを1回決定すれば済む。彼は、例えば、全ての再生デバイスを、それを購入した後直ちに1つのグループに加えることによって、それをなすことができる。そして、彼は、受信デバイスによって書き込まれた記憶媒体を自由に用いることができる。ユーザが新しい再生デバイスを購入したときには、それらは、いつでもグループに加えることができるから、グループを拡張することが、常に可能であり、以下に明らかになるように、コンテンツアイテムは、グループ内のどのデバイスもそれにアクセスできるように記憶される。
【００１１】
特定のデバイスしか読み出すことのできないように、例えば、好ましくはセッションキーを用いて、その特定のデバイスの公開キーでデータを暗号化することによって、データを暗号化すること自体は、知られている。このことは、その代りに、ライセンスファイルを、グループ内の各再生デバイスについて1度ずつ、複数の公開キーを用いて複数回、暗号化することもできるということを意味している。これは、記憶媒体上のデータ量が、幾分増加するという欠点、および、より重要には、そのときには、グループに新しいデバイスを加えて、それをコンテンツアイテムにアクセスさせるということが不可能であるという欠点を持っている。ライセンスファイルは、この場合、暗号化時点で既にそのグループ内にある再生デバイスしか、ライセンスファイルを解読できないように暗号化されており、したがって、受信デバイスが、新しく加えられたデバイスの公開キーでライセンスファイルを暗号化するためにライセンスファイルを獲得するということは不可能である。グループキーを用いれば、何らの余分なステップも、受信デバイスに必要なく、何らの変更も、記憶媒体になされる必要がない。新しく加えられた再生デバイスは、単純に、そのグループに対する解読キーを獲得して、ライセンスファイルを解読することができる。
【００１２】
一実施例の場合、前記ライセンスロッキング手段が、ライセンスロッカ暗号化キー(LLEK)で前記ライセンスファイルを暗号化するように、また、前記再生デバイスのグループに連係する前記暗号化キーで前記LLEKを暗号化するように、さらに、前記暗号化されたLLEKを前記記憶媒体に書き込むために前記暗号化されたLLEKを前記書き込み手段に供給するように、構成されている。暗号化されたLLEKを解読できる再生デバイスは、したがって、ライセンスファイルを解読することもできる。そうすると、ライセンスファイルは、その中の許可にしたがって、コンテンツアイテムを再生するために用いることができる。これは、さらなる柔軟性を供給する。
【００１３】
さらなる一実施例の場合、前記暗号化キーが、公開／秘密キーペアの前記公開キーである。対応する秘密キーは、グループ内の再生デバイスにおいて利用可能であり、したがって、それらの再生デバイスは、暗号化されたライセンスファイルを簡単に解読することができる。これは、今や、暗号化キーが、保護される必要がなく、したがって、受信デバイスが、このキーを守るための何らの処置も取らなくてもよいという、さらなる利点を持つ。もしも、暗号化キーが、秘密（対称な）キーだったとしたら、悪意あるユーザが、受信デバイスからそのキーを盗み出し、そして、ライセンスファイルを解読して、任意のデバイスで、そのコンテンツアイテムを再生するであろう。

【００１４】
さらなる一実施例の場合、前記コンテンツアイテムが、オーディオデータ、ビデオデータのうちの少なくとも1つを有する。Napsterのような音楽共有サービスの流行は、音楽や他のオーディオコンテンツの配信に対する大きな要求があるということを明らかにしている。ネットワークのバンド幅が、ビデオデータの大規模配信を許容するほど十分に大きければ、同じことが、ビデオに対しても期待されるはずである。記憶媒体への保護配信を容易にする本発明による受信デバイスを提供することによって、人々のグループ間の配信が、可能になる。
【００１５】
さらなる一実施例の場合、前記ライセンスロッキング手段が、さらに、前記グループの選択された識別子を受信するように、また、前記選択された識別子に連係する前記暗号化キーをキーサーバから獲得するように、構成されている。ユーザが、複数のグループを決定した場合には、記憶媒体にコンテンツアイテムを書き込むときに、どの1つを用いるかを選択できるのが好ましい。キーサーバ上にグループに対する公開キーを置くことによって、1人のユーザが、他のユーザの再生できるコンテンツアイテムを保護しながら記憶するということが可能になる。したがって、例えば、そのユーザは、友人に対して登録されたグループの公開キーを用いて、記憶媒体に一連の歌をダウンロードし、記憶させることができる。次いで、彼は、その記憶媒体を、その友人に、例えば、プレゼントとして、与えることができ、友人は、それを、自分のグループの全てのデバイスで再生することができる。これは、そのユーザが、彼の友人が好んでいることを知っているコンテンツアイテムだけを含め、それによって、好みに合わせて変更できるプレゼントを創り出すことが可能になる。
【００１６】
本発明のさらなる1つの目的は、冒頭に記載の再生デバイスであって、記憶媒体上のコンテンツアイテムの使用に永続的に制御を与え、さらに、ユーザの使用の考え方に合致した受信デバイスを提供することである。
【００１７】
この目的は、本発明によれば、前記ライセンスファイルが、前記記憶媒体上に暗号化されて記憶されていること、および、さらに、1つ以上の解読キーを記憶するための保護記憶手段であって、各解読キーが再生デバイスのそれぞれのグループに連係している保護記憶手段と、記憶されている解読キーが、前記暗号化されているライセンスファイルを解読するのに適しているか否かを確認するための復調手段であって、もしそうであれば、前記記憶されている解読キーを用いて前記ライセンスファイルを解読し、そして、前記解読されたライセンスファイルを前記再生手段に供給するための復調手段と、を有することを特徴とする再生デバイスにおいて達成される。ライセンスファイルは、暗号化されて記憶されるから、それを解読できる再生デバイスしか、コンテンツアイテムにアクセスし、用いることができない。コンテンツアイテムが記憶媒体に書き込まれたとき、ユーザによって選ばれた再生デバイスが、正しいグループにあれば、正しい解読キーが、保護記憶手段に提供される。
【００１８】
一実施例の場合、前記ライセンスファイルが、ライセンスロッカ暗号化キー(LLEK)で暗号化されて記憶されており、当該LLEKが、LLEK暗号化キーで暗号化されて前記記憶媒体に記憶されており、前記1つ以上の解読キーが、LLEK解読キーであり、前記復調手段が、記憶されているLLEK解読キーが前記暗号化されているLLEKを解読するのに適しているか否かを確認し、もしそうであれば、前記記憶されているLLEK解読キーを用いて前記暗号化されているLLEKから前記LLEKを獲得し、前記LLEKを用いて前記ライセンスファイルを解読するように構成されている。セッションキーとしてLLEKを用いることは、さらなる柔軟性を与える。
【００１９】
さらなる一実施例の場合、前記解読キーが、公開／秘密キーペアの前記秘密キーである

。公開キー暗号化を用いることは、それを秘密にしておく必要が全くないので、暗号化キーの配信を、ずっと容易にする。暗号キーは、今や単に平文で、それを用いてライセンスファイルを暗号化する受信デバイスに伝送することができる。そのとき、対応する秘密解読キーを持っている再生デバイスしか、そのライセンスファイルを解読できないし、そのライセンスファイルにアクセスできない。

【００２０】

さらなる一実施例の場合、再生デバイスは、前記再生デバイスに連係する公開／秘密キーペアの公開キーをコンテンツ配信管理システム(CDMS)に登録するための登録手段であって、当該公開／秘密キーペアの前記秘密キーが前記保護記憶手段に記憶されている登録手段(306)において、当該公開キーで暗号化されている解読キーを受信して、当該暗号化されている解読キーを解読し、そして、前記解読キーを前記保護記憶手段に記憶させる登録手段を、さらに有する。このように再生デバイスへの、グループに対する秘密キーの配信を容易にすることによって、秘密キーは、悪意あるユーザに曝されることが決してなく、また、どんな再生デバイスも、登録することなく秘密キーにアクセスできないということが達成される。

【００２１】

本発明は、さらに、本発明による前記受信デバイスとして機能するように実行させるときに、プログラム可能なデバイスをイネーブルにするためのコンピュータプログラム製品に関するものである。

【００２２】

本発明は、さらに、本発明による前記再生デバイスとして機能するように実行させるときに、プログラム可能なデバイスをイネーブルにするためのコンピュータプログラム製品に関するものである。

【発明を実施するための最良の形態】

【００２３】

本発明のこれらの、そして、他の観点が、図面中に示される実施例を参照して明白になり、解明される。

【００２４】

図面を通じて、同じ参照番号は、同等の、または、対応する観点を表わしている。図面に表わされている観点のいくつかは、通常、ソフトウェアにインプリメントされており、そういうものとして、ソフトウェアモジュールまたはオブジェクトのようなソフトウェア実体を表現している。

【００２５】

図1は、インターネットのようなネットワークを介して接続された送信デバイス101および受信デバイス110を有する構成100を線図的に示している。そのネットワークには、また、キーサーバ130およびライセンスサーバ140も接続されており、それらの働きは、以下に明らかになる。構成100は、受信デバイス110が、送信デバイス101からのコンテンツアイテム102のようなコンテンツアイテムをダウンロードすることを可能にする。好適な一実施例の場合、送信デバイス101および受信デバイス110は、ピアツーピア型に接続され、それによって、それらは、互いにファイルを共有することが可能になる。この実施例において、受信デバイス110が、送信デバイス101に直接コンタクトする必要なく、送信デバイス101上のどのファイルを利用可能であるかを見出せるように、ディレクトリサーバ（図示せず）を、設けることができる。これは、特に、送信デバイス101が、互いに接続された、そして、ピアツーピア型に受信デバイス110に接続された複数の送信デバイスの1つであるときに有用である。そのような場合には、受信デバイス110は、さらに、ピアツーピア型に、その構成内の他のデバイスに対して送信デバイスとして作動するように構成してもよい。他の1つの実施例において、送信デバイス101は、受信デバイス110がコンテンツアイテムをダウンロードできるファイルサーバである。

【００２６】

用語「コンテンツアイテム」は、人々がダウンロードしたいと思う任意の種類の素材の

ことをいう。特に、それは、テレビジョン番組、映画、音楽、記事、あるいは、著作のようなアイテムのことをいう。コンテンツアイテム102は、送信デバイス101上で保護された状態で利用可能にされる。好適な一実施例の場合、コンテンツアイテム102は、例えば、米国特許第5,892,900号によって公知であるIntertrust社 “Digifile“ フォーマットで、利用可能にされる。CD-2フォーマットのような、コンテンツアイテムを保護する他の技術を用いることもできる。保護フォーマットのコンテンツアイテム102は、オプション的に、非保護フォーマットのコンテンツアイテムの典型である‘teaser’を伴ってもよい。これは、ユーザが、teaserを見て、コンテンツアイテム102が彼の好みであるか否かを、それを購入する必要なく見出すことを可能にする。

【００２７】

受信デバイス110は、以下に明らかにするように、コンテンツアイテム102を、それがそのような保護フォーマットで利用可能にされたときに、ダウンロードすることができる。受信デバイス110は、例えば、セットトップボックス、パーソナルコンピュータ、ホームネットワークのゲートウェイ、あるいは、コンシューマエレクトロニクス(CE)デバイスとすることが出来る。次に、適切な許可を得て、それは、場合によっては別個の再生デバイス（図示せず）の助けを受けて、コンテンツアイテム102を再生することができる。例えば、受信デバイス110は、コンテンツアイテム102をダウンロードし、そして、それをユーザにかけることのできるパーソナルエンターテインメントシステムに、それを伝送するセットトップボックスであってもよい。

【００２８】

ユーザは、ライセンスサーバ140から、コンテンツアイテム102とともに使用するためのライセンスファイルを購入することができる。このライセンスファイルは、一連の許可、例えば、音楽を再生する許可、あるいは、コンテンツアイテムを記憶媒体に記憶させる許可を備えている。ユーザは、もちろん、各許可に対して、一定の金額を支払わなければならない。この費用は、ユーザにクレジットカード情報を供給させることによって、あるいは、ユーザを識別して、ユーザの口座に金額を請求することによって、あるいは、ネットワーク上の支払いを操作する他の公知の仕方を用いて、提供させることができる。そのライセンスファイルは、また、コンテンツアイテム102にアクセスするために必要な解読キー、あるいは、他の情報を含有している。

【００２９】

ユーザが、コンテンツアイテム102を記憶するための許可を購入してしまうと、受信デバイス110は、そのコンテンツアイテム102を記憶媒体111、望ましくは記録可能なコンパクトディスクに、書き込むことができる。もちろん、記録可能なデジタル多用途ディスク(DVD)、ハードディスク、あるいは、固体メモリカードのような他の記憶媒体に書き込んでもよい。コンテンツアイテム102は、保護様式で、例えば、それがダウンロードされたのと同じ保護フォーマットで、記憶媒体111に書き込まれる。しかしながら、例えば、記憶媒体111からコンテンツアイテム102を読み出すデバイスが、コンテンツアイテム102がダウンロードされた保護フォーマットを処理できないときには、コンテンツの保護配信に異なる技術を用いることが好都合であろう。

【００３０】

次に、ユーザは、リムーバブルな記憶媒体であることが望ましい記憶媒体111を、ビデオ再生デバイス120あるいはオーディオ再生デバイス121のような適切な再生デバイスに供給することができる。そうすると、それらは、記憶媒体からコンテンツアイテム102を読み出し、ユーザにそれをかけることができる。そうするためには、それらは、コンテンツアイテム102に対するライセンスファイルに設けられている許可を再生する必要がある。どのようにしてそれらがこの許可を得るかは、図3を参照して、以下に説明される。

【００３１】

図2は、より詳細に、受信デバイス110を線図的に示している。コンテンツアイテム102は、上に説明したように、ダウンロードモジュール201によってダウンロードされる。ダウンロードモジュール201は、例えば、周知のNapsterファイル共有クライアントのダウン

ロード部品とすることが出来る。コード変換モジュール202は、ダウンロードされたコンテンツアイテム102を、記憶媒体111に記憶するのに適切なフォーマットに変換することによって、そのコンテンツアイテム102を処理する。これには、コンテンツアイテム102を解読することと、別の暗号化技術を用いて、それを暗号化することとが含まれるであろう。しかしながら、元の保護フォーマットが、受け入れられるものであれば、コード変換モジュール202は、必要ない。次に、書き込みモジュール203が、そのコンテンツアイテム102を記憶媒体111に書き込む。

【００３２】

ライセンシングモジュール204が、ライセンスサーバ140からライセンスファイル141を獲得する。このライセンスファイル141は、少なくとも、コンテンツアイテム102を記憶媒体111に書き込む許可を有していなければならない。記憶許可が、記憶されたコンテンツアイテム102を再生する許可を含蓄していなければ、ライセンスファイル141は、さらに、再生する許可も有していなければならない。ライセンシングモジュール204は、ライセンスサーバ140とユーザとの間をインターフェースし、公知のライセンシングモジュール、例えば、Intertrust構成に設けられているようなライセンシングモジュールとしてインプリメントできる。このライセンシングモジュールは、ユーザに対するインターフェースを備えており、それを用いて、ユーザは、少額では1回再生、アンケートへの記入と交換では無料の1回再生、あるいは、もっと高額では1ケ月間の再生などの、コンテンツアイテム102に対するライセンス条件を選ぶことができる。

【００３３】

ライセンシングモジュール204は、ライセンスファイル141を、それが適切な許可を持っていれば、ライセンスファイル141の暗号化バージョン（以後、「ライセンスロッカ」と呼ぶ）を生み出すライセンスロッキングモジュール205に供給する。ライセンスファイル141は、セッションキー（以後、「ライセンスロッカ暗号化キー(LLEK)」と呼ぶ）を用いて暗号化されるのが望ましい。LLEKは、例えば、128ビット暗号化アルゴリズムを、ライセンスファイル141を暗号化するのに用いるときに、望みの長さのシーケンス、例えば、MD5のような128ビットハッシュ関数を得るために、擬似乱数ジェネレータの出力をハッシュすることによってセッションキーを生成する公知の技術を用いて生成することができる。

【００３４】

ライセンスロッキングモジュール205は、ライセンスロッカを、それをコンテンツアイテム102とともに記憶媒体111に書き込む書き込みモジュール203に供給する。ある記憶媒体、例えば、記録可能なコンパクトディスクにおいては、全てのデータを、一度に、媒体に書き込む必要がある。そのような記憶媒体が用いられたときには、書き込みモジュール203は、全てのデータが得られるまで、書き込まれるデータをバッファしなければならないこともある。例えば、リムーバブルなハードディスクでは、それは、もちろん、必要とされない。

【００３５】

次に、LLEKも、記憶媒体111に書き込まれるが、暗号化された形でである。記憶媒体111からLLEKを読み出し、それを解読できる再生デバイスは、ライセンスロッカからライセンスファイル141を解読でき、その後、コンテンツアイテム102を再生することができる。コンテンツアイテム102およびライセンスファイル141をこのように設けることによって、本発明は、ユーザが、ネットワーク105に接続する必要のない再生デバイスに記憶されたコンテンツアイテム102を再生できるという目的を達成する。

【００３６】

セッションキーを用いることに替えて、ライセンスファイル141を、暗号化キーによって直接暗号化することもでき、それに対応する解読キーは、その後に記憶媒体111にアクセスする再生デバイスに使用可能である。暗号化は、対称であっても、非対称であってもよい。

【００３７】

コンテンツアイテム102の再生は、限られた数の再生デバイスに限定されるのが望まし

い。それは、著作権所有者が、コンテンツアイテム102の使用を制御することを可能にするからである。しかしながら、構成100をユーザの考え方に合致させるために、コンテンツをかけるデバイスの管理は、記憶媒体111自体へのコンテンツアイテム102の記憶と独立でなければならない。たいてい、コンテンツの購買者は、自分自身がそれをかけるだけではなく、彼の家族も、その家族の持ち物である種々のデバイスで、それをかけている。友人や隣人も、コンテンツアイテム102を聴きたいと思うかもしれない。一般的に言えば、コンテンツアイテム102の再生は、ある1つのグループの人々、あるいは、当該グループの人々の所有する1つのグループのデバイスに対して許可されるべきである。デバイスのグループを区別するために、各グループは、グループIDを割り当てられる。コンテンツアイテム102は、グループIDにリンクされ、したがって、グループ内のいずれのデバイスも、記憶媒体111からコンテンツアイテム102を再生することができる。この目的のために、ライセンスファイルは、グループ内のいずれのデバイスもそれを解読できるが、グループ外のデバイスは解読できないように暗号化される。

【００３８】

好適な一実施例の場合、LLEKは、そのグループに連係する公開／秘密キーペアのうちの公開キーで暗号化され、それによって、そのグループ内の全てのデバイスが、対応する秘密キーにアクセスできる。そうでなければ、秘密キー暗号化図式を用いることができる。ライセンスロッキングモジュール205は、ユーザが、例えば、受信デバイス110に結合されたディスプレイに表示されるリストから、グループIDを選択するように促し、そして、例えば、そのグループに対する公開キーをキーサーバ130から検索することによって、その公開キーを獲得する。その後、それは、そのグループに対する公開キーでLLEKを暗号化し、そして、その暗号化されたLLEKを記憶媒体111に書き込むための書き込みモジュール203に供給する。ここで、記憶媒体111を、ビデオ再生デバイス120あるいはオーディオ再生デバイス121のような再生デバイスに供給することができる。

【００３９】

受信デバイス110は、プロセッサに上述のステップを実行させるように構成されたコンピュータプログラム製品200として実現できる。コンピュータプログラム製品200は、当該コンピュータプログラム製品が、受信デバイス110として機能するように実行されるときに、プログラム可能なデバイスをイネーブルにする。公開キー暗号化図式が用いられているとき、受信デバイス110は、どんな秘密キーへの何らのアクセスも必要でないから、例えば、Napsterのようなファイル共有プログラムに対する追加としてPC上にロードされてランできるコンピュータプログラム製品200として、受信デバイスを完全に実現することが可能である。これは、依然として著作権所有者の望む制御を取り去ることなく、ユーザが、音楽ファイルをダウンロードし、再配信できる、Napsterクライアントに対する拡張サービスを提供する。

【００４０】

図3は、オーディオ再生デバイス121を、より詳細に線図的に示している。ビデオ再生デバイス120のような他の再生デバイスも、同様に実現できる。ユーザは、記憶媒体111を、例えば、それを格納ユニット301に挿入することによって、再生デバイス121に供給することができる。復号モジュール302は、記憶媒体111から暗号化されたライセンスファイル141を読み出し、保護記憶モジュール309に記憶されている秘密キーを用いて、それを解読する。好適な一実施例の場合、復号モジュール302は、記憶媒体111から暗号化されたLLEKを読み出し、記憶されている秘密キーを用いて、その暗号化されたLLEKを解読する。復号モジュール302は、その後、このようにして得られたLLEKを用いて、ライセンスロッカを解読し、ライセンスファイル141を獲得する。

【００４１】

解読ステップが、保護記憶モジュール309に記憶されていない秘密キーを必要とすることも起こり得る。その場合には、復号モジュール302は、ライセンスファイル141を解読することができない。また、再生デバイス121は、2つ以上のグループに含まれるかもしれない。その場合には、それは、それがはいっている各グループにつき1つずつの、それの保

護記憶モジュールに記憶された複数の解読キーを持っている。したがって、復号モジュール302は、最初に、正しい秘密キーが保護記憶モジュール309に記憶されているか否かを確認し、それから、この確認に基づいて、ライセンスファイル141を解読するか、または、解読キーが失われているためにライセンスファイル141を獲得することが不可能であることをユーザに通知しなければならない。

【００４２】

その確認は、色々の仕方で、例えば、記憶されている秘密キーに対するキー識別子と、暗号化されたライセンスファイル141と一緒に記憶されている識別子とを比較することによって、なすことができる。そうでなければ、ライセンスファイル141が、バージョン番号あるいは固定テキスト記号列のような既知情報ピースを有していてもよい。その場合には、復号モジュール302は、ライセンスファイル141の解読を試み、次いで、その出力と、期待される既知情報ピースとを比較することができる。期待される既知情報ピースが、その出力の中に失われているときには、解読されたキーが、正しくなかったことになる。そうでなければ、秘密キーが、それらが属するグループに対する識別子を有していてもよく、また、記憶媒体111が、ライセンスファイル141が暗号化されたグループに対する識別子を有していてもよい。そうすると、復号モジュール302は、保護記憶モジュール309において後者の識別子を検索し、マッチングする識別子を有する秘密キーを探し出す。復号モジュールは、また、有効なライセンスファイルを得るために用いることのできる解読キーが見つかるまで、単純に、各解読キーでライセンスファイル141の解読を試みてもよい。

【００４３】

解読ステップは、ある程度、どのようにして秘密キーが保護記憶モジュール309に記憶されるかに依存して、色々に実現できる。このモジュール309は、解読ソフトウェアを埋め込まれたハードウェアモジュールとして実現でき、したがって、復号モジュール302が、暗号化されたライセンスファイル141をモジュール309に供給し、モジュール309が、適切な解読キーを用いて、それを解読し、そして、復号モジュール302に、暗号で記したのではない形式のライセンスファイル141を戻すことができる。実際の秘密キーは、不正にいじれないようにできているハードウェア内に記憶されており、悪意のあるユーザによって読み出されることがないから、これは、大きな保護確保を供給する。そうでなければ、保護記憶モジュール309は、単純に、復号モジュール302が、秘密解読キーを読み出して、ライセンスファイル141自体を解読することができる読み出し専用メモリ(ROM)であることもできる。モジュール309は、スマートカード上に設けることができる。

【００４４】

復号モジュール302は、ライセンスファイル141を再生モジュール305に供給する。再生モジュール305は、記憶媒体111から、記憶されているコンテンツアイテム102を読み出し、ライセンスファイル141内に再生に対する許可が存在することを確かめる。その通りであれば、それは、例えば、スピーカ206にオーディオ信号を生成させることによって、コンテンツアイテム102をかける。

【００４５】

保護記憶モジュール309において、再生デバイス121にインストールされた秘密キーは、単純に、図2を参照して上に略述したような受信機111によって用いられる公開キーに対応する、グループの秘密キーであることもできる。これは、グループの秘密キーが、そのグループに加えられる全てのデバイスに配信されなければならないということを必要とし、あまり実際的でなく、スマートカードのように高度に不正にいじりにくいハードウェアが用いられない限り、全く保護されない。いずれにせよ、これは、ユーザが、そのグループ内の各デバイスについて1枚ずつの数のそのようなスマートカードを手に入れることを必要とし、それは、やっかいなことである。

【００４６】

したがって、全ての再生デバイスが、それ自身に連係する公開／秘密キーペアを持ち、そして、それによって、秘密キーが、再生デバイスの内部に保護されながらインストールされているのが、好ましい。これは、例えば、再生デバイスが製造される工場でなすこと

ができる。さらなるセキュリティのために、デバイスに対する公開／秘密キーペアは、Certifying Authority（CA：認証局）のような独立組織によって生成させ、製造者によるインストールのために工場に供給させることも可能である。

【００４７】

再生デバイス121は、再生デバイスに対する固有識別子とともに、登録のための公開キーをCDMS（コンテンツ配信管理システム）310に供給することのできる登録モジュール306を持っている。この固有識別子は、例えば、製造者番号、型番号、シリアル番号を有することができる。その登録は、ユーザの要求によって、あるいは、再生デバイス121に初めてスイッチが入れられたとき、あるいは、他の適当なときに、行うことができる。そうでなければ、公開キーが、製造者によるキーペアのインストール時に、CAによって登録させてもよい。

【００４８】

図4を参照して以下に明らかにするように、CDMS 310は、次に、グループ内の各デバイスに対して1度、そのデバイスの登録された公開キーを用いて、そのグループに対する秘密キーを暗号化する。暗号化された秘密キーは、次いで、それらを、自身の秘密キーを用いて解読できる、再生デバイスの登録モジュールに送り返される。その後、再生デバイスは、その保護記憶モジュールに秘密キーを記憶する。その瞬間から、再生デバイスは、グループの公開キーで暗号化された、どのライセンスファイル141も、そのグループに対する対応する秘密キーを用いて、解読することができる。このようなグループに対する秘密キーの配信を容易にすることによって、秘密キーは、悪意あるユーザに曝されることが決してなく、また、どんな再生デバイスも、登録することなく秘密キーにアクセスできないということが達成される。このことは、例えば、ユーザが、規模の大きなデバイスのグループにコンテンツアイテム102を配信するための許可を欲しいときには、そのユーザに、より高い料金を請求することを可能にする。さらに、グループ内のデバイスの数は、著作権所有者の意向にしたがって制限できる。

【００４９】

再生デバイス120は、プロセッサに上述のステップを実行させるように構成されたコンピュータプログラム製品300として実現できる。コンピュータプログラム製品300は、当該コンピュータプログラム製品が、受信デバイス110として機能するように実行されるときに、プログラム可能なデバイスをイネーブルにする。秘密キーが、他のデバイスにコピーされないことを確実にするように注意しなければならない。他のデバイスへのコピーは、他のデバイスが、再生デバイス120を装うことを可能にし、それは、記憶されたコンテンツアイテム111がかけられるはずの全てのデバイスに料金を請求する可能性を破るからである。

【００５０】

図4は、構成100の他の1実施例を線図的に示しており、それは、グループおよびデバイスを登録する処理を図示している。CDMS 310は、グループG1，G2，G3および各グループ内のデバイスD1，…，D9のリスト402を保持している。ユーザは、CDMS 310に新しいグループの創設を要求することができる。そうすると、CDMS 310は、そのグループに対する公開／秘密キーペアを生成する。次いで、そのグループに対する公開キーを、受信デバイス110によるダウンロードのために、キーサーバ130に設けることができる。グループに対する公開キーをキーサーバ130に設けることによって、1人のユーザが、他のユーザの再生できるコンテンツアイテムを保護しながら記憶するということが可能になる。したがって、例えば、そのユーザは、友人に対して登録されたグループの公開キーを用いて、記憶媒体111に一連の歌をダウンロードし、記憶させることができる。次いで、彼は、その記憶媒体111を、その友人に、例えば、プレゼントとして、与えることができ、友人は、それを、自分のグループの全てのデバイスでかけることができる。友人が好んでいることを知っているコンテンツアイテムだけを含め、そして、それらを友人のグループを用いて記憶させることによって、そのユーザは、好みに合わせて変更できるプレゼントを創り出す。

【００５１】

ユーザが、1つのグループを登録すると、彼は、それに再生デバイスを加えることができる。彼が加えたいと望んでいるデバイスが、まだ登録されていなければ、そのユーザは、例えば、そのデバイスの登録モジュール306をアクティブにすることによって、それがデバイスリスト403に加えられるように、最初に、それを登録しなければならない。デバイスをグループに加える際、CDMS 310が、そのデバイスの公開キーで秘密キーを暗号化する。例えば、ユーザが、デバイスD6をグループG1に加えるとき、CDMS 310が、公開キーPK6でG1の秘密キーを暗号化する。この暗号化された秘密キーは、デバイスD6の復調モジュール302によって必要とされる。彼が加えたいと望んでいるデバイスが、CDMS 310で登録されれば、彼は、単純に、それを、CDMS 310によって供給される、デバイス識別子UID1，…，UID9および連係する公開キーPK1，…，PK9を有するデバイスリスト403から選択し、そして、それをそのグループに加えることができる。

【００５２】

ユーザは、また、例えば、グループ内のデバイスの数がCDMS 310によって制限されているときに新しいデバイスのための空きをつくるために、そのグループに対するリストからデバイスを取り除いてもよい。これは、ユーザが、グループに対するリストからデバイスを取り去っても、依然として、そのデバイス上で、そのグループに提供するように意図されたコンテンツをかけることを可能にする。これは、そのデバイスが、LLEKを解読でき、したがって、ライセンスファイル141を解読でき、そして、コンテンツアイテム102をかけることのできる、そのグループに対する秘密キーを依然として持っているから可能なのである。これは、例えば、グループに対する公開／秘密キーペアを周期的に入れ替え、そして、そのときに、グループに対するリスト上のデバイスに新しい秘密キーを供給することだけによって防ぐことができる。さらに、グループに加えられる、あるいは、グループから取り除かれる全てのデバイスに対して登録料を要求することは、自分のグループに対するリストをひんぱんに操作しようというユーザの気持を減少させる。

【００５３】

キーサーバ130によって供給される公開キーが真正であるということを確実にするために、それらの公開キーを、キーサーバ130上で利用可能にする前に、Certifying Authority（CA：認証局）で認証することができる。受信デバイス110に、CAに対する認証を与えることができ、したがって、それは、認証が真正であることを証明し、それによって、そのグループの公開キーが真正であることを証明する。CAに対する認証あるいは公開キーは、受信デバイス110に製造者がロードすることもできるし、あるいは、必要なときにキーサーバ130からダウンロードすることもできる。しかしながら、製造者による受信デバイス130へのCAに対する認証のローディングの方が、悪意あるユーザがその認証を取り替える機会を、より少なくしか提供しないから、より保護される。

【００５４】

コンテンツアイテム102を記憶媒体111にこのようにして記憶させるさらなる利点は、適当なグループ内にない再生デバイスが、それでも、新しいライセンスファイルを獲得すれば、コンテンツアイテム102にアクセスできるということである。コンテンツアイテム102は、結局、任意の適切なライセンスファイルでアクセスできる保護フォーマットで記憶されている。したがって、自分のお気に入りの音楽トラックを持つ記憶媒体111を創り出したユーザは、その記憶媒体111を、そのユーザのグループの外部にデバイスがある友人に貸すことができる。そうすると、その友人は、1回再生ライセンスを購入して、記憶媒体111のトラックにアクセスし、そのユーザが何を好きなのかを見出すことができる。彼も、同様にそれらの音楽を好きであれば、彼は、そのユーザに、彼のグループに加わらないかを尋ねる、あるいは、彼自身でそれらのトラックをダウンロードする。そのユーザは、彼が所有するデバイスおよび友人が所有するデバイスを含む新しいグループを創り出し、そして、彼ら2人ともが好きなトラックを有する新しい記憶媒体を創り出すこともできる。

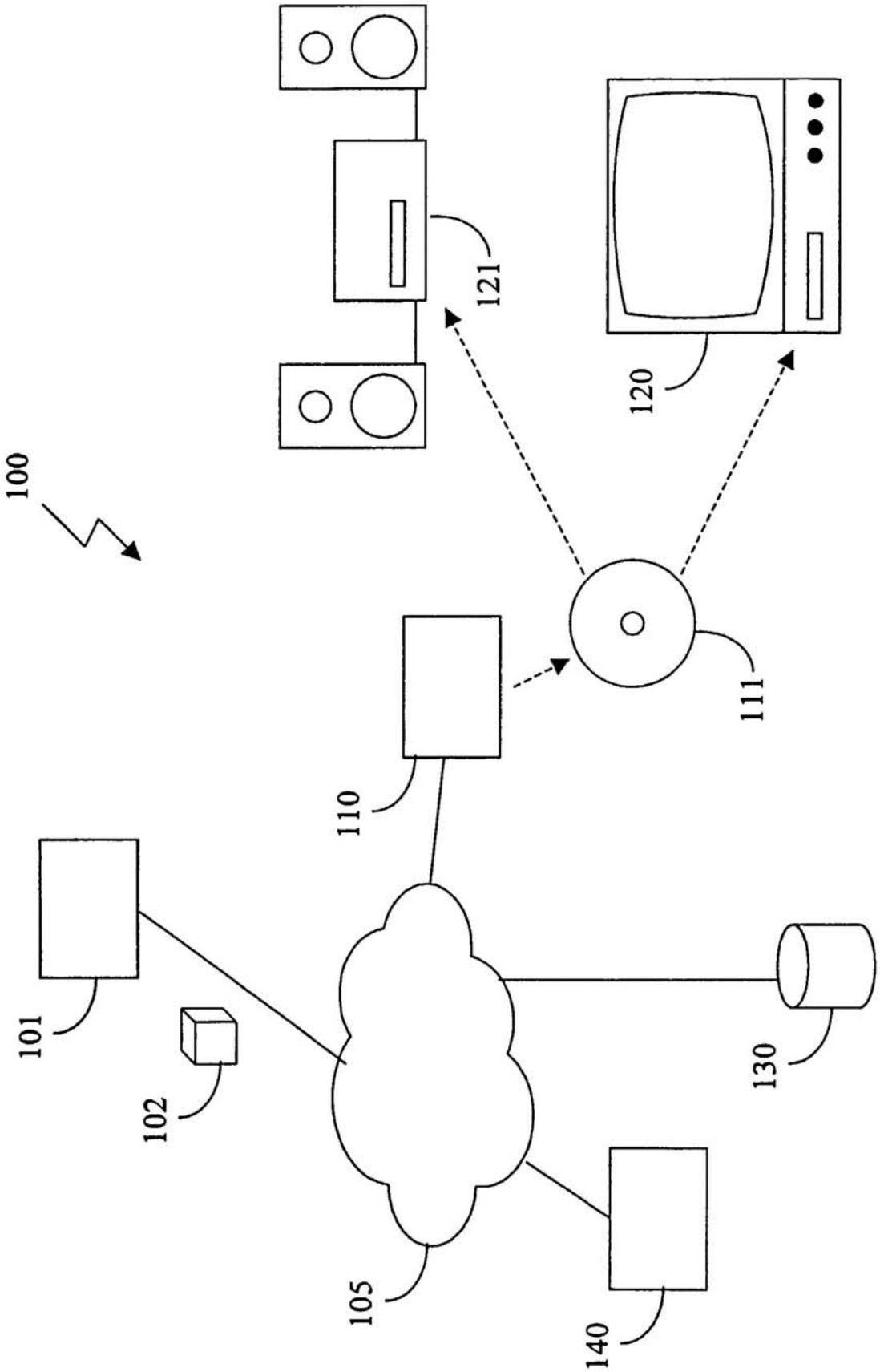
【図面の簡単な説明】

【００５５】

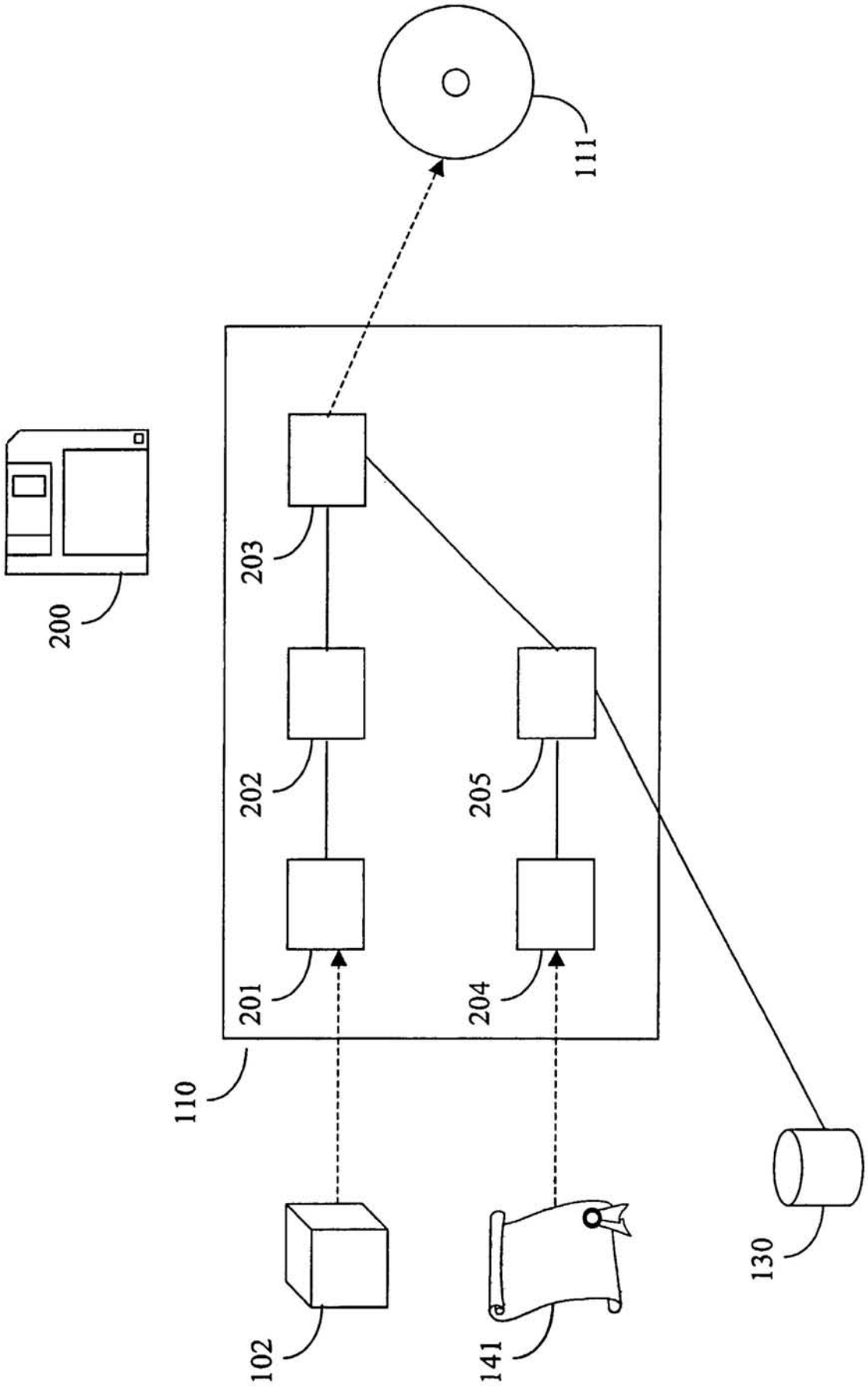
【図１】本発明による構成の第1の実施例を線図的に示す。

【図２】本発明による受信デバイスを、より詳細に線図的に示す。
【図３】本発明による再生デバイスを、より詳細に線図的に示す。
【図４】本発明による構成の第2の実施例を線図的に示す。
【符号の説明】
【００５６】
101　送信デバイス
102　コンテンツアイテム
110　受信デバイス
111　記憶媒体
120　ビデオ再生デバイス
121　オーディオ再生デバイス
130　キーサーバ
140　ライセンスサーバ
141　ライセンスファイル
201　ダウンロードモジュール
203　書き込みモジュール
204　ライセンシングモジュール
205　ライセンスロッキングモジュール
302　復号モジュール
305　再生モジュール
306　登録モジュール
309　保護記憶モジュール
310　コンテンツ配信管理システム(CDMS)

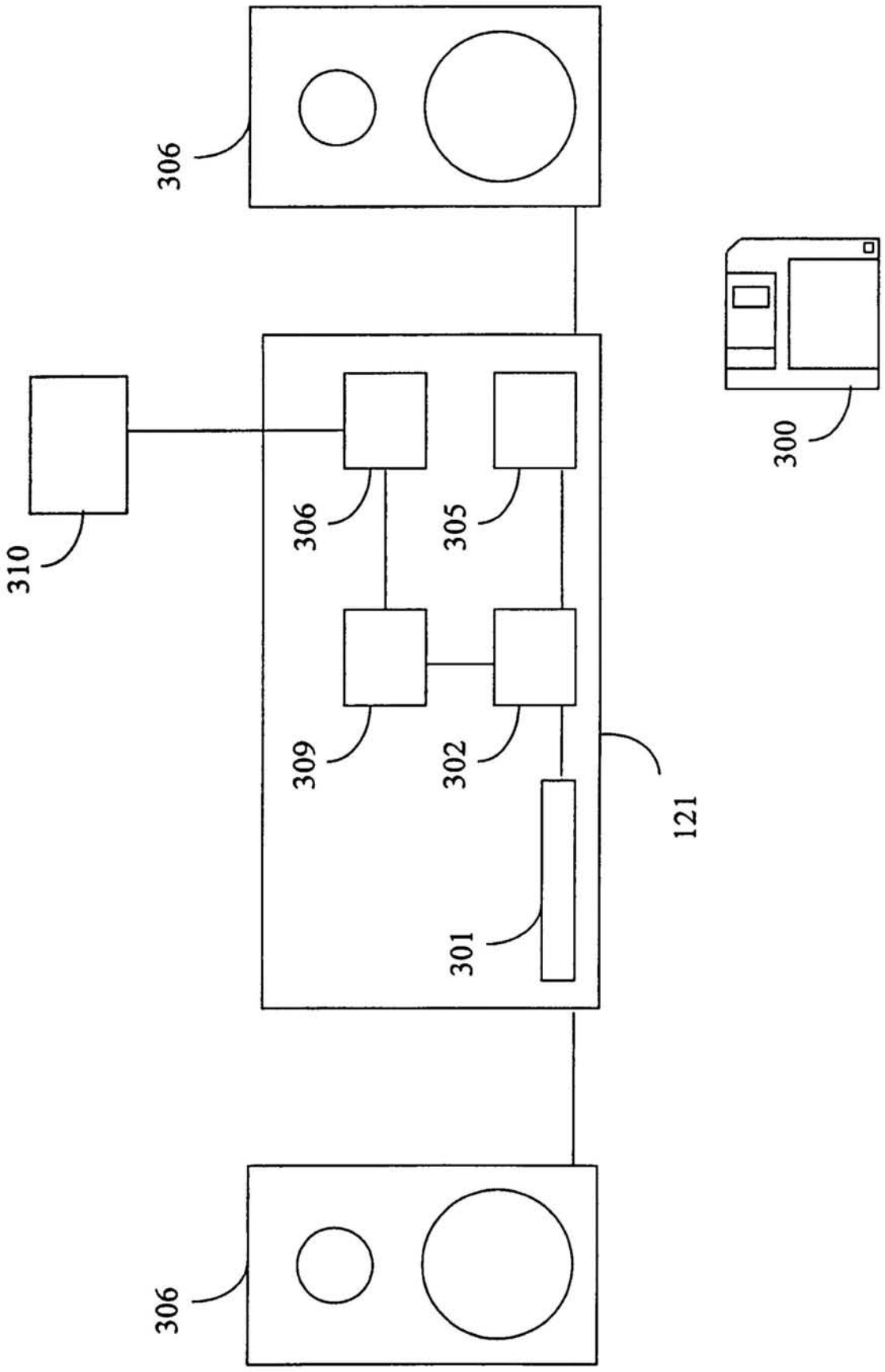
【図１】



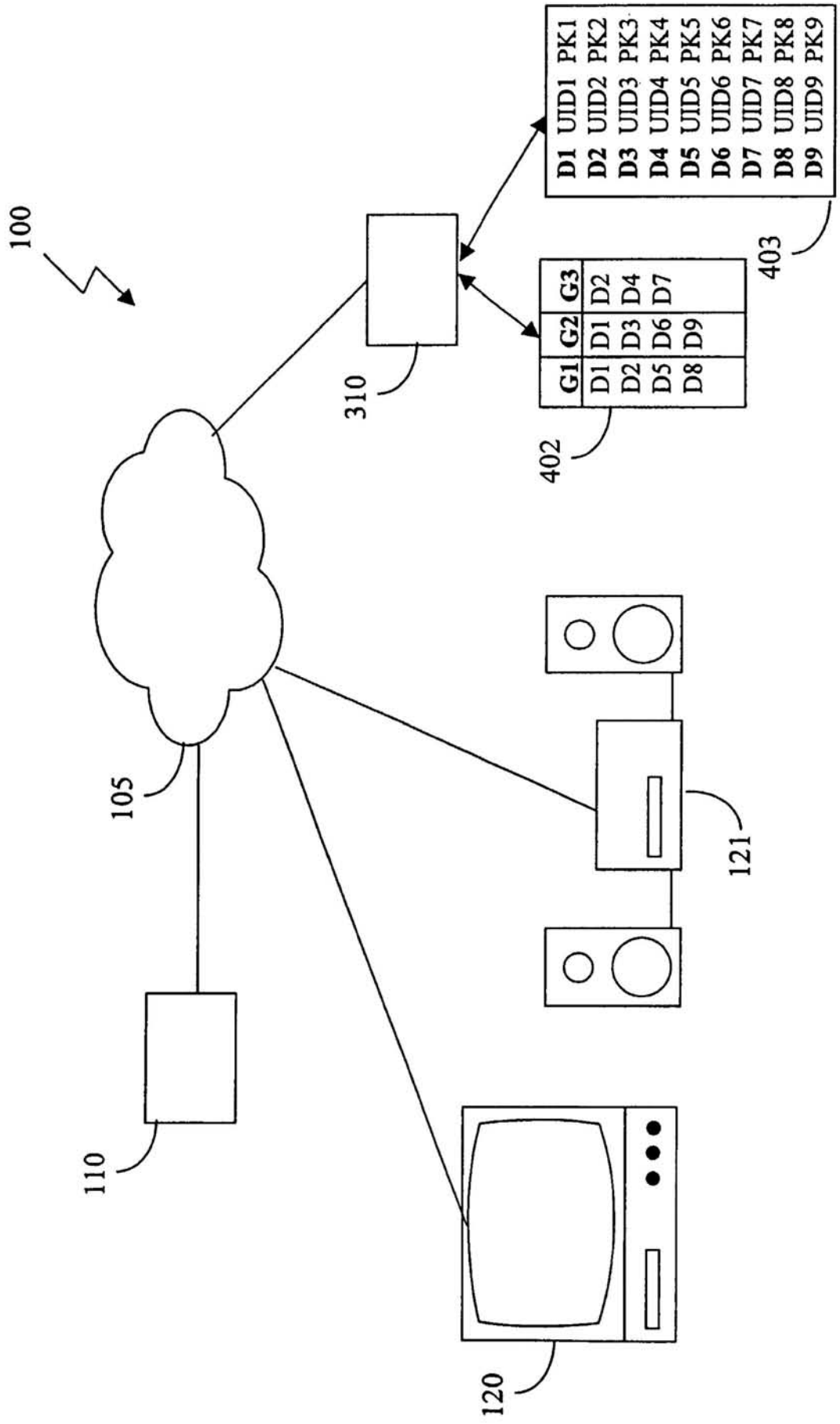
【図２】



【図３】



【図４】


100
105
110
120
121
310
402
403
D1 UID1 PK1
D2 UID2 PK2
D3 UID3 PK3
D4 UID4 PK4
D5 UID5 PK5
D6 UID6 PK6
D7 UID7 PK7
D8 UID8 PK8
D9 UID9 PK9
G1 G2 G3
D1 D1 D2
D2 D3 D4
D5 D6 D7
D8 D9

フロントページの続き

(51)Int.Cl.	FI	
	G06F 12/14	540B
	G06F 1/00	370E
	G11B 20/10	H
	H04L 9/00	601A

(72)発明者 ロクホフ ゲラルドゥス シー ピー
オランダ国 5656 アー アー アインドーフェン プロフホルストラーン 6
(72)発明者 ブロイゴム ミシェル アール
オランダ国 5656 アー アー アインドーフェン プロフホルストラーン 6
(72)発明者 エンゲレン ディルク ヴィ アール
オランダ国 5656 アー アー アインドーフェン プロフホルストラーン 6
(72)発明者 ファン デア ポエル ペーター
オランダ国 5656 アー アー アインドーフェン プロフホルストラーン 6

審査官 岸野 徹

(56)参考文献 特開平10－083297（JP, A）
特開2000－138664（JP, A）
特開平11－283327（JP, A）
国際公開第00／052558（WO, A1）
特開平10－210025（JP, A）

(58)調査した分野(Int.Cl., DB名)
G06F 21/24
H04L 9/08