(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-524972
(P2006-524972A)
(43)公表日　平成18年11月2日(2006.11.2)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| H04L 9/14 | (2006.01) | H04L | 9/00 | 641 | 5J104 |
| G06Q 30/00 | (2006.01) | G06F | 17/60 | 302E | |

審査請求 有　予備審査請求 未請求　（全 31 頁）

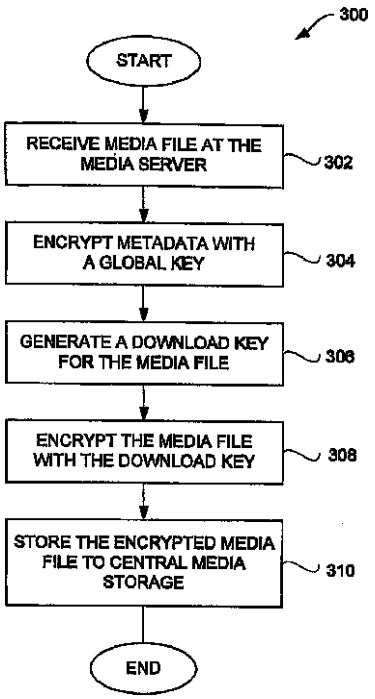
(21)出願番号　特願2006-513343 (P2006-513343)
(86)(22)出願日　平成16年4月26日 (2004.4.26)
(85)翻訳文提出日　平成17年11月9日 (2005.11.9)
(86)国際出願番号　PCT/US2004/012848
(87)国際公開番号　WO2004/097609
(87)国際公開日　平成16年11月11日 (2004.11.11)
(31)優先権主張番号　10/423,700
(32)優先日　平成15年4月25日 (2003.4.25)
(33)優先権主張国　米国 (US)

(71)出願人　503342960
アップル・コンピューター・インコーポレーテッド
APPLE COMPUTER INCORPORATED
アメリカ合衆国　カリフォルニア州９５０１４－２０８４　クパチーノ，インフィニット・ループ，１
(74)代理人　110000028
特許業務法人明成国際特許事務所
(72)発明者　ダウディ・トーマス
アメリカ合衆国　カリフォルニア州９４０８７　サニーベイル，カムサック・ドライブ，１６１０

最終頁に続く

(54)【発明の名称】セキュアなネットワークベースのコンテンツ配信のための方法およびシステム

(57)【要約】
【課題】ネットワークベースのコンテンツ配信のための方法およびシステムを提供する。
【解決手段】コンテンツの配信はセキュアなだけではなく、コントロールされている。このセキュリティは、ダウンロード中のメディアファイル内のコンテンツへのアクセスを制限し、それと同時にサーバまたはクライアントにおいて記憶されているあいだもアクセスを制限する。ある実施形態において、それぞれのメディアファイルは異なる、ランダムに生成されたキーで暗号化される。メディアファイルの配信に対するコントロールは、クライアントから他のクライアントへのメディアファイルの後に続く配信を制限するよう働きえる。他の実施形態において、このコントロールは、メディアファイルが同じユーザに関連する制限された数の異なるクライアント上で共有されることを許容しえる。このクライアントはアプリケーションで変わりえるが、一般に、メモリ記憶を有するコンピューティングデバイスである。しばしばクライアントは、コンテンツを記憶し、そのユーザに提示することができるパーソナルコンピュータまたは他のコ



【特許請求の範囲】
【請求項１】
メディアファイルを、それらがダウンロードの準備ができているように中央化されたメディア記憶に記憶する方法であって、
（ａ）メディアアイテムに関するメディアファイルを受け取ることであって、前記メディアファイルのそれぞれが少なくともメディアコンテンツデータを有する、受け取ること、
（ｂ）前記メディアファイルのそれぞれについてダウンロードキーを生成することであって、前記ダウンロードキーは前記メディアファイルのそれぞれについて異なる、生成すること、
（ｃ）前記メディアファイルのそれぞれを、前記ダウンロードキーの対応するもので暗号化することによって暗号化されたメディアファイルを作ること、および
（ｄ）前記暗号化されたメディアファイルを前記中央化されたメディア記憶に記憶すること
を含む方法。
【請求項２】
請求項１に記載の方法であって、
前記メディアファイルのそれぞれは少なくとも前記メディアコンテンツデータおよびメタデータを有し、前記メタデータは前記関連付けられたメディアアイテムの特性を記述し、かつ
前記方法は、
（ｅ）前記暗号化（ｃ）の前に、前記メディアファイルのそれぞれについての前記メタデータを共通キーで暗号化すること
をさらに含む方法。
【請求項３】
請求項１に記載の方法であって、前記中央化されたメディア記憶は、メディアサーバ内にあるか、またはメディアサーバに結合される方法。
【請求項４】
請求項３に記載の方法であって、前記暗号化されたメディアファイルは、データネットワークを介してユーザのローカルマシンにダウンロードされえる方法。
【請求項５】
請求項１に記載の方法であって、前記ユーザローカルマシンの少なくとも１つは、携帯コンピューティングデバイスおよびメディアプレーヤーのうちの１つである方法。
【請求項６】
ローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得する方法であって、
複数の入手可能なメディアファイルからメディアファイルを特定することであって、前記メディアファイルのそれぞれは少なくともメディアコンテンツデータを有する、特定すること、
前記特定されたメディアファイルへのアクセスを購入すること、
前記特定されたメディアファイルに対応するダウンロードキーを獲得すること、
前記特定されたメディアファイルをその暗号化されたかたちで前記ローカルマシンにダウンロードすること、
前記特定されたメディアファイルをその暗号化されないかたちに前記ダウンロードキーを用いて復号すること、
少なくとも１つのユーザキーを得ることであって、前記ユーザキーは前記ローカルマシンのユーザに関連付けられている、得ること、
少なくとも実質的にランダムであるコンテンツキーを生成すること、
前記特定されたメディアファイルの前記メディアコンテンツデータを前記コンテンツキーで暗号化すること、

前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作ること、
前記特定されたメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにすること、および
前記変更されたメディアファイルを前記ローカルマシンに記憶すること
を含む方法。
【請求項７】
請求項６に記載の方法であって、複数のメディアファイルが前記中央サーバマシン上に記憶され、前記メディアファイルのそれぞれは少なくともメタデータおよびメディアコンテンツデータを有し、前記メタデータは前記関連付けられたメディアアイテムの特性を記述する方法。
【請求項８】
請求項７に記載の方法であって、前記特定すること（ａ）は、
（ａ１）前記メディアファイルを前記サーバマシン上で前記メディアファイルについての前記メタデータの使用を通してブラウズすること、および
（ａ２）前記メディアファイルのうちの１つを前記特定されたメディアファイルとして特定すること
を含む方法。
【請求項９】
請求項８に記載の方法であって、前記メディアファイルのうちの前記１つを前記特定することは、ユーザによって実行される方法。
【請求項１０】
請求項６に記載の方法であって、前記記憶することは、前記変更されたメディアファイルを前記ローカルマシンに関連付けられたローカル記憶に記憶するよう動作する方法。
【請求項１１】
請求項１０に記載の方法であって、前記ローカル記憶は、前記ローカルマシン内のデータ記憶デバイスである方法。
【請求項１２】
請求項６に記載の方法であって、前記ローカルマシンは、前記中央サーバマシンにネットワーク上で結合し、前記ネットワークはインターネットを含む方法。
【請求項１３】
請求項６に記載の方法であって、
前記中央サーバマシンは、前記ユーザのそれぞれについてのアカウントを記憶し、それぞれのアカウントはそれに割り当てられた少なくとも１つのユーザキーを有し、
前記獲得することによって得られた前記ユーザキーは、前記ユーザに対応する前記アカウントに割り当てられた前記少なくとも１つのユーザキーである方法。
【請求項１４】
請求項１３に記載の方法であって、前記ユーザに関連付けられた前記ローカルマシンは、前記ユーザに対応する前記アカウントに割り当てられた少なくとも１つのユーザキーを記憶し、前記ユーザキーを前記獲得することは前記ローカルマシンから前記ユーザキーを得るように動作する方法。
【請求項１５】
ローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得する方法であって、
複数の入手可能なメディアファイルからメディアファイルを特定することであって、前記メディアファイルのそれぞれは少なくともメディアコンテンツデータを有する、特定すること、
前記特定されたメディアファイルへのアクセスを購入すること、
前記特定されたメディアファイルに対応するダウンロードキーを獲得すること、
前記特定されたメディアファイルをその暗号化されたかたちで前記ローカルマシンにダ

ウンロードすること、
少なくとも１つのユーザキーを得ることであって、前記ユーザキーは前記ローカルマシンのユーザに関連付けられている、得ること、
少なくとも実質的にランダムであるコンテンツキーを生成すること、
前記特定されたメディアファイルの前記メディアコンテンツデータを前記ダウンロードキーおよび前記コンテンツキーで転写すること、
前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作ること、
前記特定されたメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにすること、および
前記変更されたメディアファイルを前記ローカルマシンに記憶すること
を含む方法。
【請求項１６】
請求項１５に記載の方法であって、複数のメディアファイルが前記中央サーバマシン上に記憶され、前記メディアファイルのそれぞれは少なくともメタデータおよびメディアコンテンツデータを有し、前記メタデータは前記関連付けられたメディアアイテムの特性を記述する方法。
【請求項１７】
請求項１６に記載の方法であって、前記特定すること（ａ）は、
（ａ１）前記メディアファイルを前記サーバマシン上で前記メディアファイルについての前記メタデータの使用を通してブラウズすること、および
（ａ２）前記メディアファイルのうちの１つを前記特定されたメディアファイルとして特定すること
を含む方法。
【請求項１８】
請求項１７に記載の方法であって、前記メディアファイルのうちの前記１つを前記特定することは、ユーザによって実行される方法。
【請求項１９】
請求項１５に記載の方法であって、前記記憶することは、前記変更されたメディアファイルを前記ローカルマシンに関連付けられたローカル記憶に記憶するよう動作する方法。
【請求項２０】
請求項１５に記載の方法であって、前記ローカルマシンは、前記中央サーバマシンにネットワーク上で結合し、前記ネットワークはインターネットを含む方法。
【請求項２１】
請求項１５に記載の方法であって、
前記中央サーバマシンは、前記ユーザのそれぞれについてのアカウントを記憶し、それぞれのアカウントはそれに割り当てられた少なくとも１つのユーザキーを有し、
前記獲得することによって得られた前記ユーザキーは、前記ユーザに対応する前記アカウントに割り当てられた前記少なくとも１つのユーザキーである方法。
【請求項２２】
請求項２１に記載の方法であって、前記ユーザに関連付けられた前記ローカルマシンは、前記ユーザに対応する前記アカウントに割り当てられた少なくとも１つのユーザキーを記憶し、前記ユーザキーを前記獲得することは前記ローカルマシンから前記ユーザキーを得るように動作する方法。
【請求項２３】
ローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得する方法であって、
複数の入手可能なメディアファイルからメディアファイルを特定することであって、前記メディアファイルのそれぞれは少なくともメディアコンテンツデータを有する、特定すること、

前記特定されたメディアファイルへのアクセスを購入すること、
少なくとも１つのユーザキーを得ることであって、前記ユーザキーは前記ローカルマシンのユーザに関連付けられている、得ること、
少なくとも実質的にランダムであるコンテンツキーを生成すること、
前記特定されたメディアファイルの前記メディアコンテンツデータを前記コンテンツキーで暗号化すること、
前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作ること、および
前記特定されたメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにすること
を含む方法。
【請求項２４】
請求項２３に記載の方法であって、前記方法は、
前記特定されたメディアファイルをその暗号化されたかたちで前記ローカルマシンに後でダウンロードすること、および
前記変更されたメディアファイルを前記ローカルマシンに記憶すること
をさらに含む方法。
【請求項２５】
請求項２４に記載の方法であって、複数のメディアファイルが前記中央サーバマシン上に記憶され、前記メディアファイルのそれぞれは少なくともメタデータおよびメディアコンテンツデータを有し、前記メタデータは前記関連付けられたメディアアイテムの特性を記述する方法。
【請求項２６】
請求項２５に記載の方法であって、前記特定すること（ａ）は、
（ａ１）前記メディアファイルを前記サーバマシン上で前記メディアファイルについての前記メタデータの使用を通してブラウズすること、および
（ａ２）前記メディアファイルのうちの１つを前記特定されたメディアファイルとして特定すること
を含む方法。
【請求項２７】
請求項２６に記載の方法であって、前記メディアファイルのうちの前記１つを前記特定することは、ユーザによって実行される方法。
【請求項２８】
請求項２４に記載の方法であって、前記記憶することは、前記変更されたメディアファイルを前記ローカルマシンに関連付けられたローカル記憶に記憶するよう動作する方法。
【請求項２９】
請求項２８に記載の方法であって、前記ローカル記憶は、前記ローカルマシン内のデータ記憶デバイスである方法。
【請求項３０】
請求項２４に記載の方法であって、前記ローカルマシンは、前記中央サーバマシンにネットワーク上で結合し、前記ネットワークはインターネットを含む方法。
【請求項３１】
請求項２４に記載の方法であって、
前記中央サーバマシンは、前記ユーザのそれぞれについてのアカウントを記憶し、それぞれのアカウントはそれに割り当てられた少なくとも１つのユーザキーを有し、
前記獲得することによって得られた前記ユーザキーは、前記ユーザに対応する前記アカウントに割り当てられた前記少なくとも１つのユーザキーである方法。
【請求項３２】
請求項３１に記載の方法であって、前記ユーザに関連付けられた前記ローカルマシンは、前記ユーザに対応する前記アカウントに割り当てられた少なくとも１つのユーザキーを

記憶し、前記ユーザキーを前記獲得することは前記ローカルマシンから前記ユーザキーを得るように動作する方法。

【請求項３３】

コンテンツデータをメディアファイルからユーザに示す方法であって、

（ａ）示すべきメディアファイルを特定することであって、前記特定されたメディアファイルは少なくとも暗号化されたメディアコンテンツデータ、ユーザキー参照、および暗号化されたコンテンツキーを有する、特定すること、

（ｂ）ユーザキーを前記ユーザキー参照に基づいて前記特定されたメディアファイル内で得ること、

（ｃ）前記暗号化されたコンテンツキーを前記特定されたメディアファイルから得ること、

（ｄ）前記暗号化されたコンテンツキーを前記ユーザキーを用いて復号することによって、前記コンテンツキーを得ること、

（ｅ）前記特定されたメディアファイルの前記暗号化されたメディアコンテンツデータを前記コンテンツキーで復号すること、および

（ｆ）前記特定されたメディアファイルの前記メディアコンテンツデータを示すこと

を含む方法。

【請求項３４】

請求項３３に記載の方法であって、前記特定されたメディアファイルはローカルマシン上に記憶され、

前記示すこと（ｆ）は、前記特定されたメディアファイルの前記メディアコンテンツデータを前記ローカルマシンにおいて示す

方法。

【請求項３５】

請求項３４に記載の方法であって、前記得ること（ｂ）は、前記ユーザキーを前記ローカルマシンから前記ユーザキー参照に基づいて得る方法。

【請求項３６】

請求項３３に記載の方法であって、前記ローカルマシンはコンピューティングデバイスである方法。

【請求項３７】

請求項３３に記載の方法であって、前記ローカルマシンはメディアプレーヤーである方法。

【請求項３８】

請求項３３に記載の方法であって、前記メディアコンテンツデータを示すこと（ｆ）は、前記メディアコンテンツデータを再生および表示することのうちの１つ以上を含む方法。

【請求項３９】

請求項３３に記載の方法であって、前記特定されたメディアファイルは、オーディオコンテンツデータを持つオーディオファイル、視覚コンテンツデータを持つ画像ファイル、またはビデオコンテンツデータを持つビデオファイルである方法。

【請求項４０】

請求項３３に記載の方法であって、複数のメディアファイルが前記中央サーバマシン上に記憶され、前記メディアファイルのそれぞれは、異なるメディアファイルについてそれぞれ異なる、少なくともメタデータ、暗号化されたメディアコンテンツデータ、および暗号化されたコンテンツキーを有する方法。

【請求項４１】

請求項４０に記載の方法であって、前記特定すること（ａ）は、

（ａ１）前記メディアファイルを前記サーバマシン上で前記メディアファイルについての前記メタデータの使用を通してブラウズすること、および

（ａ２）前記メディアファイルのうちの１つを示されるべきと特定すること

を含む方法。
【請求項４２】
請求項４１に記載の方法であって、前記特定すること（ａ２）はユーザによって実行される方法。
【請求項４３】
請求項４０に記載の方法であって、前記ユーザキーを得ること（ｂ）は、
（ｂ１）前記ローカルマシンが少なくとも１つのユーザキーを記憶するかどうかを決定すること、
（ｂ２）前記決定すること（ｂ１）が前記ローカルマシンが少なくとも１つのユーザキーを記憶すると決定するとき、前記ユーザキーを前記ユーザキー参照に基づいて前記特定されたメディアファイル内から取り出すこと、および
（ｂ３）前記決定すること（ｂ１）が前記ローカルマシンが少なくとも１つのユーザキーを記憶しないと決定するとき、前記ローカルマシンの前記ユーザについてのユーザアカウントを確立すること
を含む方法。
【請求項４４】
請求項４３に記載の方法であって、前記確立すること（ｂ３）は、前記少なくとも１つのユーザキーが前記ローカルマシンに記憶されるようにする方法。
【請求項４５】
メディアファイルを、それらがダウンロードの準備ができているように中央化されたメディア記憶に記憶し、同時にローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得するコンピュータプログラムコードを少なくとも含むコンピュータで読み取り可能な媒体であって、
メディアアイテムに関するメディアファイルを受け取るコンピュータプログラムコードであって、前記メディアファイルのそれぞれが少なくともメディアコンテンツデータを有する、受け取るコンピュータプログラムコード、
前記メディアファイルのそれぞれについてダウンロードキーを生成するコンピュータプログラムコードであって、前記ダウンロードキーは前記メディアファイルのそれぞれについて異なる、生成するコンピュータプログラムコード、
前記メディアファイルのそれぞれを、前記ダウンロードキーの対応するもので暗号化することによって暗号化されたメディアファイルを作るコンピュータプログラムコード、
前記暗号化されたメディアファイルを前記中央化されたメディア記憶に記憶するコンピュータプログラムコード、
複数の入手可能なメディアファイルから購入されるべきメディアファイルを特定するコンピュータプログラムコードであって、前記メディアファイルのそれぞれは少なくともメディアコンテンツデータを有する、特定するコンピュータプログラムコード、
前記特定されたメディアファイルへのアクセスを購入するコンピュータプログラムコード、
前記特定されたメディアファイルに対応するダウンロードキーを獲得するコンピュータプログラムコード、および
前記特定されたメディアファイルをその暗号化されたかたちで前記ローカルマシンにダウンロードするコンピュータプログラムコード
を含むコンピュータで読み取り可能な媒体。
【請求項４６】
ローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得するコンピュータプログラムコードを少なくとも含むコンピュータで読み取り可能な媒体であって、
特定のメディアファイルを前記ローカルマシンにおいて前記サーバマシンから受け取るコンピュータプログラムコードであって、前記特定のメディアファイルは少なくともメディアコンテンツデータを有する、受け取るコンピュータプログラムコード、

前記特定のメディアファイルをその暗号化されないかたちに前記ダウンロードキーを用いて復号するコンピュータプログラムコード、
少なくとも１つのユーザキーを得るコンピュータプログラムコードであって、前記ユーザキーは前記ローカルマシンのユーザに関連付けられている、得るコンピュータプログラムコード、
少なくとも実質的にランダムであるコンテンツキーを生成するコンピュータプログラムコード、
前記特定のメディアファイルの前記メディアコンテンツデータを前記コンテンツキーで暗号化するコンピュータプログラムコード、
前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作るコンピュータプログラムコード、
前記特定のメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにするコンピュータプログラムコード、および
前記変更されたメディアファイルを前記ローカルマシンに記憶するコンピュータプログラムコード
を含むコンピュータで読み取り可能な媒体。
【請求項４７】
請求項４６に記載のコンピュータで読み取り可能な媒体であって、
示すべきメディアファイルを特定するコンピュータプログラムコードであって、前記特定されたメディアファイルは少なくとも暗号化されたメディアコンテンツデータ、ユーザキー参照、および暗号化されたコンテンツキーを有する、特定するコンピュータプログラムコード、
ユーザキーを前記ユーザキー参照に基づいて前記特定されたメディアファイル内で得るコンピュータプログラムコード、
前記暗号化されたコンテンツキーを前記特定されたメディアファイルから得るコンピュータプログラムコード、
前記暗号化されたコンテンツキーを前記ユーザキーを用いて復号することによって、前記コンテンツキーを得るコンピュータプログラムコード、
前記特定されたメディアファイルの前記暗号化されたメディアコンテンツデータを前記コンテンツキーで復号するコンピュータプログラムコード、および
前記特定されたメディアファイルの前記メディアコンテンツデータを示すコンピュータプログラムコード
をさらに含むコンピュータで読み取り可能な媒体。
【請求項４８】
請求項４７に記載のコンピュータで読み取り可能な媒体であって、
前記メディアファイルのそれぞれは、少なくとも前記メディアコンテンツデータおよびメタデータを少なくとも有し、前記メタデータは前記関連付けられたメディアアイテムの特性を記述し、
前記特定されたメディアファイルはローカルマシン上に記憶され、かつ
前記示すコンピュータプログラムコードは、前記特定されたメディアファイルの前記メディアコンテンツデータを前記ローカルマシンにおいて示す
コンピュータで読み取り可能な媒体。
【請求項４９】
ローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得するコンピュータプログラムコードを少なくとも含むコンピュータで読み取り可能な媒体であって、
特定のメディアファイルを前記ローカルマシンにおいて前記サーバマシンから受け取るコンピュータプログラムコードであって、前記特定のメディアファイルは少なくともメディアコンテンツデータを有する、受け取るコンピュータプログラムコード、
前記特定のメディアファイルをその暗号化されないかたちに前記ダウンロードキーを用

いて復号するコンピュータプログラムコード、
少なくとも１つのユーザキーを得るコンピュータプログラムコードであって、前記ユーザキーは前記ローカルマシンのユーザに関連付けられている、得るコンピュータプログラムコード、
少なくとも実質的にランダムであるコンテンツキーを生成するコンピュータプログラムコード、
前記特定のメディアファイルの前記メディアコンテンツデータを前記ダウンロードキーおよび前記コンテンツキーを用いて転写するコンピュータプログラムコード、
前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作るコンピュータプログラムコード、
前記特定のメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにするコンピュータプログラムコード、および
前記変更されたメディアファイルを前記ローカルマシンに記憶するコンピュータプログラムコード
を含むコンピュータで読み取り可能な媒体。
【請求項５０】
ローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得するコンピュータプログラムコードを少なくとも含むコンピュータで読み取り可能な媒体であって、
特定のメディアファイルを前記ローカルマシンにおいて前記サーバマシンから受け取るコンピュータプログラムコードであって、前記特定のメディアファイルは少なくともメディアコンテンツデータを有する、受け取るコンピュータプログラムコード、
前記特定のメディアファイルをその暗号化されないかたちに前記ダウンロードキーを用いて復号するコンピュータプログラムコード、
少なくとも１つのユーザキーを得るコンピュータプログラムコードであって、前記ユーザキーは前記ローカルマシンのユーザに関連付けられている、得るコンピュータプログラムコード、
少なくとも実質的にランダムであるコンテンツキーを生成するコンピュータプログラムコード、
前記特定のメディアファイルの前記メディアコンテンツデータを前記コンテンツキーで暗号化するコンピュータプログラムコード、
前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作るコンピュータプログラムコード、および
前記特定のメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにするコンピュータプログラムコード
を含むコンピュータで読み取り可能な媒体。
【請求項５１】
メディア配信システムであって、
複数のメディアファイルを記憶するメディア記憶であって、前記メディアファイルは少なくともメディアコンテンツデータを有するメディア記憶、および
前記メディア記憶に動作可能に接続されたメディアサーバであって、前記メディアサーバはダウンロードキーを、記憶されるべき前記メディアファイルのそれぞれについて生成し、前記ダウンロードキーは前記メディアファイルのそれぞれについて異なり、前記メディアファイルのそれぞれを前記ダウンロードキーのうちの前記対応する１つで暗号化することによって暗号化されたメディアファイルを作り、前記暗号化されたメディアファイルを前記メディア記憶に記憶するよう動作する
メディア配信システム。
【請求項５２】
請求項５１に記載のメディア配信システムであって、前記メディアサーバは、前記メディア記憶に記憶された前記暗号化されたメディアファイルから購入されるべき特定のメデ

ィアファイルを購入するリクエストを受け取り、前記特定されたメディアファイルへのアクセスを購入し、その暗号化されたかたちの前記特定のメディアファイルおよび前記特定のメディアファイルに対応するダウンロードキーをダウンロードするようさらに動作するメディア配信システム。

【請求項５３】

請求項５１に記載のメディア配信システムであって、前記メディア配信システムは、

前記メディアサーバにネットワークを介して結合する複数のユーザマシン

をさらに備え、

前記特定のメディアファイルおよび前記ダウンロードキーの前記ダウンロードは前記ユーザマシンのうちの特定の１つへなされる

メディア配信システム。

【請求項５４】

請求項５３に記載のメディア配信システムであって、前記メディアサーバは、複数の許可されたユーザのそれぞれについて複数のユーザキーを記憶するようさらに動作し、

前記メディアサーバは、ユーザキーを前記特定のユーザマシンにダウンロードするようさらに動作し、前記ユーザキーは、前記特定のユーザマシンと共に前記許可されたユーザのうちの特定の一人に特に関連付けられている

メディア配信システム。

【請求項５５】

請求項５４に記載のメディア配信システムであって、前記特定のユーザマシンは、前記特定のメディアファイルをその暗号化されないかたちに前記ダウンロードキーを用いて復号し、少なくとも実質的にランダムであるコンテンツキーを生成し、前記特定されたメディアファイルの前記メディアコンテンツデータを前記コンテンツキーで暗号化し、前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作り、前記特定されたメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにし、かつ前記変更されたメディアファイルを前記ローカルマシンに記憶するようさらに動作するメディア配信システム。

【請求項５６】

請求項５５に記載のメディア配信システムであって、前記特定のユーザマシンは、前記特定のメディアファイルを前記特定のユーザマシンにおいて後で示すよう動作するメディア配信システム。

【請求項５７】

請求項５６に記載のメディア配信システムであって、前記特定のメディアファイルを示すとき、前記特定のユーザマシンは、前記特定されたメディアファイル内で前記ユーザキー参照に基づいてユーザキーを得て、前記暗号化されたコンテンツキーを前記特定されたメディアファイルから得て、前記暗号化されたコンテンツキーを前記ユーザキーを用いて復号することによって、前記コンテンツキーを得て、前記特定されたメディアファイルの前記暗号化されたメディアコンテンツデータを前記コンテンツキーで復号し、かつ前記特定されたメディアファイルの前記メディアコンテンツデータを示すように動作するメディア配信システム。

【請求項５８】

請求項５１に記載のメディア配信システムであって、前記メディアファイル内の前記コンテンツは、音楽、写真またはビデオのうちの少なくとも１つに関するメディア配信システム。

【請求項５９】

請求項５１に記載のメディア配信システムであって、前記メディアファイルのそれぞれは、少なくとも前記メディアコンテンツデータおよびメタデータを有し、前記メタデータは前記関連付けられたメディアアイテムの特性を記述するメディア配信システム。

【請求項６０】

メディア配信システムであって、

複数のメディアファイルを記憶するメディア記憶であって、前記メディアファイルは少なくとも暗号化されたメディアコンテンツデータを有するメディア記憶、および
前記メディア記憶に動作可能に接続されたメディアサーバであって、前記メディアサーバは、前記メディアファイルが前記メディアサーバによって維持されるユーザアカウントによって許可されているユーザマシン上だけで示されえるように前記メディアファイルをセキュアなやり方でマシン群に配信するよう動作する
メディア配信システム。

【請求項６１】
請求項６０に記載のメディア配信システムであって、前記ユーザアカウントのそれぞれは、所定の、制限された個数のユーザマシンに関連付けられえるメディア配信システム。

【請求項６２】
請求項６１に記載のメディア配信システムであって、前記ユーザアカウントのそれぞれは、前記対応するユーザアカウントに関連付けられる少なくとも１つのユーザキーを含むメディア配信システム。

【請求項６３】
請求項６０に記載のメディア配信システムであって、前記メディアファイルのそれぞれは、暗号化されたメディアコンテンツデータ、ユーザキー参照、および暗号化されたコンテンツキーを少なくともさらに含むメディア配信システム。

【請求項６４】
請求項６３に記載のメディア配信システムであって、前記ユーザキー参照は、ユーザキーを特定し、前記メディアファイルにアクセスするために、前記ユーザキーは前記ユーザの前記関連付けられたユーザアカウントによって前記ユーザに利用可能でなければならないメディア配信システム。

【請求項６５】
請求項６３に記載のメディア配信システムであって、ユーザマシンにおいて特定のメディアファイルにアクセスするために、前記ユーザマシンは、前記ユーザキー参照によって参照されるユーザキーを有しなければならないメディア配信システム。

【請求項６６】
請求項６５に記載のメディア配信システムであって、前記特定のメディアファイルは、前記暗号化されたコンテンツキーを前記ユーザキーを用いて復号することによって前記コンテンツキーを得ること、および前記特定のメディアファイルの前記暗号化されたメディアコンテンツデータを前記コンテンツキーで復号することの動作を実行することによって前記ユーザマシンにおいて示されるメディア配信システム。

【請求項６７】
請求項６６に記載のメディア配信システムであって、前記特定のメディアファイルを前記示すことは、前記特定のメディアファイルを前記ユーザマシンにおいて再生することを伴うメディア配信システム。

【請求項６８】
請求項６６に記載のメディア配信システムにおいて、特定のユーザによって購入された前記メディアファイルのセットが前記特定のユーザと関連付けられた限定された個数のマシン上での使用について許可されえるメディア配信システム。

【請求項６９】
ローカルマシンにおいてメディアファイルを示すコンピュータプログラムコードを少なくとも含むコンピュータで読み取り可能な媒体であって、
示すべきメディアファイルを特定するコンピュータプログラムコードであって、前記特定されたメディアファイルは少なくとも暗号化されたメディアコンテンツデータ、ユーザキー参照、および暗号化されたコンテンツキーを有する、特定するコンピュータプログラムコード、
ユーザキーを前記ユーザキー参照に基づいて前記特定されたメディアファイル内で得るコンピュータプログラムコード、

前記暗号化されたコンテンツキーを前記特定されたメディアファイルから得るコンピュータプログラムコード、
前記暗号化されたコンテンツキーを前記ユーザキーを用いて復号することによって、前記コンテンツキーを得るコンピュータプログラムコード、
前記特定されたメディアファイルの前記暗号化されたメディアコンテンツデータを前記コンテンツキーで復号するコンピュータプログラムコード、および
前記特定されたメディアファイルの前記メディアコンテンツデータを示すコンピュータプログラムコード
を含むコンピュータで読み取り可能な媒体。
【請求項７０】
請求項６９に記載のコンピュータで読み取り可能な媒体であって、
ユーザは、前記特定されたメディアファイルの前記メディアコンテンツデータが示されるようリクエストし、
中央サーバマシンは、前記ユーザのそれぞれについてのアカウントを記憶し、それぞれのアカウントはそれに割り当てられた少なくとも１つのユーザキーを有し、かつ
前記獲得することによって得られた前記ユーザキーは、前記特定されたメディアファイルの前記メディアコンテンツデータが示されるようリクエストする前記ユーザに対応する前記アカウントに割り当てられた前記少なくとも１つのユーザキーである
コンピュータで読み取り可能な媒体。
【請求項７１】
請求項７０に記載のコンピュータで読み取り可能な媒体であって、前記ユーザに関連付けられた前記ローカルマシンは、前記ユーザに対応する前記アカウントに割り当てられた少なくとも１つのユーザキーを記憶し、前記ユーザキーを前記獲得することは前記ローカルマシンから前記ユーザキーを得るように動作するコンピュータで読み取り可能な媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンテンツ配信に関し、より具体的にはクライアント・サーバ環境におけるコンテンツ配信に関する。
【背景技術】
【０００２】
近年、インターネット上での音楽の送付つまり配信が人気を得てきている。ＭＰ３およびＭＰＥＧ４のような効率的ファイルフォーマットの発展のために、メディアファイルのサイズはインターネットを介したダウンロードを実用的にするだけ充分に小さくなってきている。また技術的発展は、高速インターネット接続およびメモリの低コストにつながっている。これら発展の組み合わせは、音楽およびビデオのためのようなメディアファイルのダウンロードを扱い得るものにし、それほど時間を必要とするものではなくしている。
【０００３】
音楽配信の一つの有名なアプローチは、ダウンロードに利用可能な多くのソングの記憶のための中央化されたサーバを用いるｍｐ３．ｃｏｍである。音楽配信の他の有名なアプローチは、ピアツーピア共有が利用されたＮａｐｓｔｅｒだった。ピアツーピア共有については、中央化されたサーバ上ではなく、多くのユーザのユーザマシン上に無数のソングが常駐する。
【０００４】
音楽配信のためのこれらオンラインアプローチには、大規模な著作権違反が伴った。音楽業界は、特にこれらオンライン音楽配信ウェブサイトの人気および関連する無許可複製およびメディアファイルの共有に懸念を示した。その著作権およびアーチストのためのロイヤルティ収入を保護するべく、音楽業界はこれら流行のオンライン音楽配信ウェブサイトを阻止するために法的措置を執った。
【発明の開示】

【発明が解決しようとする課題】
【０００５】
よって、ユーザにメディアファイルをダウンロードする容易さと便利さを提供しつつ、同時にメディアファイル中に含まれるコンテンツに対する著作権者の権利を保護する確実でコントロールされた環境を提供するオンラインコンテンツ配信への改良されたアプローチの要求が存在する。
【課題を解決するための手段】
【０００６】
大きく言って、本発明は、ネットワークベースのコンテンツ配信に関する。コンテンツの配信はセキュアなだけではなく、コントロールされている。このセキュリティは、ダウンロード中のメディアファイル内のコンテンツへのアクセスを制限し、それと同時にサーバまたはクライアントにおいて記憶されているあいだもアクセスを制限する。ある実施形態において、それぞれのメディアファイルは異なる、ランダムに生成されたキーで暗号化される。メディアファイルの配信に対するコントロールは、クライアントから他のクライアントへのメディアファイルの後に続く配信を制限するよう働きえる。他の実施形態において、このコントロールは、メディアファイルが同じユーザに関連する制限された数の異なるクライアント上で共有されることを許容しえる。このクライアントはアプリケーションで変わりえるが、一般に、メモリ記憶を有するコンピューティングデバイスである。しばしばクライアントは、コンテンツを記憶し、そのユーザに提示することができるパーソナルコンピュータまたは他のコンピューティングデバイスである。
【０００７】
本発明は、方法、システム、デバイス、装置、またはコンピュータで読み取り可能な媒体を含む多くのやり方で実現されえる。本発明のいくつかの実施形態が以下に説明される。
【０００８】
メディアファイルを、それらがダウンロードの準備ができているように中央化されたメディア記憶に記憶する方法として本発明のある実施形態は、メディアアイテムに関するメディアファイルを受け取ることであって、前記メディアファイルのそれぞれが少なくともメディアコンテンツデータを有する、受け取ること、前記メディアファイルのそれぞれについてダウンロードキーを生成することであって、前記ダウンロードキーは前記メディアファイルのそれぞれについて異なる、生成すること、前記メディアファイルのそれぞれを、前記ダウンロードキーの対応するもので暗号化することによって暗号化されたメディアファイルを作ること、および前記暗号化されたメディアファイルを前記中央化されたメディア記憶に記憶することを含む。
【０００９】
ローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得する方法として本発明のある実施形態は、複数の入手可能なメディアファイルからメディアファイルを特定することであって、前記メディアファイルのそれぞれは少なくともメディアコンテンツデータを有する、特定すること、前記特定されたメディアファイルへのアクセスを購入すること、前記特定されたメディアファイルに対応するダウンロードキーを獲得すること、前記特定されたメディアファイルをその暗号化されたかたちで前記ローカルマシンにダウンロードすること、前記特定されたメディアファイルをその暗号化されないかたちに前記ダウンロードキーを用いて復号すること、少なくとも１つのユーザキーを得ることであって、前記ユーザキーは前記ローカルマシンのユーザに関連付けられている、得ること、少なくとも実質的にランダムであるコンテンツキーを生成すること、前記特定されたメディアファイルの前記メディアコンテンツデータを前記コンテンツキーで暗号化すること、前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作ること、前記特定されたメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにすること、および前記変更されたメディアファイルを前記ローカルマシンに記憶することを含む。

【００１０】
ローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得する方法として本発明の他の実施形態は、複数の入手可能なメディアファイルからメディアファイルを特定することであって、前記メディアファイルのそれぞれは少なくともメディアコンテンツデータを有する、特定すること、前記特定されたメディアファイルへのアクセスを購入すること、前記特定されたメディアファイルに対応するダウンロードキーを獲得すること、前記特定されたメディアファイルをその暗号化されたかたちで前記ローカルマシンにダウンロードすること、少なくとも１つのユーザキーを得ることであって、前記ユーザキーは前記ローカルマシンのユーザに関連付けられている、得ること、少なくとも実質的にランダムであるコンテンツキーを生成すること、前記特定されたメディアファイルの前記メディアコンテンツデータを前記ダウンロードキーおよび前記コンテンツキーで転写すること、前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作ること、前記特定されたメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにすること、および前記変更されたメディアファイルを前記ローカルマシンに記憶することを含む。

【００１１】
ローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得する方法として本発明のさらに他の実施形態は、複数の入手可能なメディアファイルからメディアファイルを特定することであって、前記メディアファイルのそれぞれは少なくともメディアコンテンツデータを有する、特定すること、前記特定されたメディアファイルへのアクセスを購入すること、少なくとも１つのユーザキーを得ることであって、前記ユーザキーは前記ローカルマシンのユーザに関連付けられている、得ること、少なくとも実質的にランダムであるコンテンツキーを生成すること、前記特定されたメディアファイルの前記メディアコンテンツデータを前記コンテンツキーで暗号化すること、前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作ること、および前記特定されたメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにすることを含む。

【００１２】
コンテンツデータをメディアファイルからユーザに示す方法として本発明のある実施形態は、示すべきメディアファイルを特定することであって、前記特定されたメディアファイルは少なくとも暗号化されたメディアコンテンツデータ、ユーザキー参照、および暗号化されたコンテンツキーを有する、特定すること、ユーザキーを前記ユーザキー参照に基づいて前記特定されたメディアファイル内で得ること、前記暗号化されたコンテンツキーを前記特定されたメディアファイルから得ること、前記暗号化されたコンテンツキーを前記ユーザキーを用いて復号することによって、前記コンテンツキーを得ること、前記特定されたメディアファイルの前記暗号化されたメディアコンテンツデータを前記コンテンツキーで復号すること、および前記特定されたメディアファイルの前記メディアコンテンツデータを示すことを含む。

【００１３】
メディアファイルを、それらがダウンロードの準備ができているように中央化されたメディア記憶に記憶し、同時にローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得するコンピュータプログラムコードを少なくとも含むコンピュータで読み取り可能な媒体として本発明のある実施形態は、メディアアイテムに関するメディアファイルを受け取るコンピュータプログラムコードであって、前記メディアファイルのそれぞれが少なくともメディアコンテンツデータを有する、受け取るコンピュータプログラムコード、前記メディアファイルのそれぞれについてダウンロードキーを生成するコンピュータプログラムコードであって、前記ダウンロードキーは前記メディアファイルのそれぞれについて異なる、生成するコンピュータプログラムコード、前記メディアファイルのそれぞれを、前記ダウンロードキーの対応するもので暗号化することによって暗号

化されたメディアファイルを作るコンピュータプログラムコード、前記暗号化されたメディアファイルを前記中央化されたメディア記憶に記憶するコンピュータプログラムコード、複数の入手可能なメディアファイルから購入されるべきメディアファイルを特定するコンピュータプログラムコードであって、前記メディアファイルのそれぞれは少なくともメディアコンテンツデータを有する、特定するコンピュータプログラムコード、前記特定されたメディアファイルへのアクセスを購入するコンピュータプログラムコード、前記特定されたメディアファイルに対応するダウンロードキーを獲得するコンピュータプログラムコード、および前記特定されたメディアファイルをその暗号化されたかたちで前記ローカルマシンにダウンロードするコンピュータプログラムコードを含む。

【００１４】

ローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得するコンピュータプログラムコードを少なくとも含むコンピュータで読み取り可能な媒体として本発明のある実施形態は、特定のメディアファイルを前記ローカルマシンにおいて前記サーバマシンから受け取るコンピュータプログラムコードであって、前記特定のメディアファイルは少なくともメディアコンテンツデータを有する、受け取るコンピュータプログラムコード、前記特定のメディアファイルをその暗号化されないかたちに前記ダウンロードキーを用いて復号するコンピュータプログラムコード、少なくとも１つのユーザキーを得るコンピュータプログラムコードであって、前記ユーザキーは前記ローカルマシンのユーザに関連付けられている、得るコンピュータプログラムコード、少なくとも実質的にランダムであるコンテンツキーを生成するコンピュータプログラムコード、前記特定のメディアファイルの前記メディアコンテンツデータを前記コンテンツキーで暗号化するコンピュータプログラムコード、前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作るコンピュータプログラムコード、前記特定のメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにするコンピュータプログラムコード、および前記変更されたメディアファイルを前記ローカルマシンに記憶するコンピュータプログラムコードを含む。

【００１５】

ローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得するコンピュータプログラムコードを少なくとも含むコンピュータで読み取り可能な媒体として本発明のある実施形態は、特定のメディアファイルを前記ローカルマシンにおいて前記サーバマシンから受け取るコンピュータプログラムコードであって、前記特定のメディアファイルは少なくともメディアコンテンツデータを有する、受け取るコンピュータプログラムコード、前記特定のメディアファイルをその暗号化されないかたちに前記ダウンロードキーを用いて復号するコンピュータプログラムコード、少なくとも１つのユーザキーを得るコンピュータプログラムコードであって、前記ユーザキーは前記ローカルマシンのユーザに関連付けられている、得るコンピュータプログラムコード、少なくとも実質的にランダムであるコンテンツキーを生成するコンピュータプログラムコード、前記特定のメディアファイルの前記メディアコンテンツデータを前記ダウンロードキーおよび前記コンテンツキーを用いて転写するコンピュータプログラムコード、前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作るコンピュータプログラムコード、前記特定のメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにするコンピュータプログラムコード、および前記変更されたメディアファイルを前記ローカルマシンに記憶するコンピュータプログラムコードを含む。

【００１６】

ローカルマシンにおいて使用するためのメディアファイルを中央サーバマシンから獲得するコンピュータプログラムコードを少なくとも含むコンピュータで読み取り可能な媒体として本発明のある実施形態は、特定のメディアファイルを前記ローカルマシンにおいて前記サーバマシンから受け取るコンピュータプログラムコードであって、前記特定のメデ

ィアファイルは少なくともメディアコンテンツデータを有する、受け取るコンピュータプログラムコード、前記特定のメディアファイルをその暗号化されないかたちに前記ダウンロードキーを用いて復号するコンピュータプログラムコード、少なくとも１つのユーザキーを得るコンピュータプログラムコードであって、前記ユーザキーは前記ローカルマシンのユーザに関連付けられている、得るコンピュータプログラムコード、少なくとも実質的にランダムであるコンテンツキーを生成するコンピュータプログラムコード、前記特定のメディアファイルの前記メディアコンテンツデータを前記コンテンツキーで暗号化するコンピュータプログラムコード、前記コンテンツキーを前記ユーザキーで暗号化することによって暗号化されたコンテンツキーを作るコンピュータプログラムコード、および前記特定のメディアファイルを変更することによって、ユーザキー参照および前記暗号化されたコンテンツキーをさらに含むようにするコンピュータプログラムコードを含む。

【００１７】

メディア配信システムとして本発明のある実施形態は、少なくともメディア記憶およびメディアサーバを含む。メディア記憶は、複数のメディアファイルを記憶し、前記メディアファイルは少なくともメディアコンテンツデータを有する。メタデータはもし提供されるなら関連付けられるメディアアイテムの特性を記述する。前記メディアサーバはダウンロードキーを、記憶されるべき前記メディアファイルのそれぞれについて生成し、前記ダウンロードキーは前記メディアファイルのそれぞれについて異なり、前記メディアファイルのそれぞれを前記ダウンロードキーのうちの前記対応する１つで暗号化することによって暗号化されたメディアファイルを作り、前記暗号化されたメディアファイルを前記メディア記憶に記憶するよう動作する。

【００１８】

メディア配信システムとして本発明の他の実施形態は、少なくともメディア記憶およびメディアサーバを含む。メディア記憶は、複数のメディアファイルを記憶し、前記メディアファイルは少なくとも暗号化されたメディアコンテンツデータを有する。前記メディアサーバは、前記メディアファイルが前記メディアサーバによって維持されるユーザアカウントによって許可されているユーザマシン上だけで示されえるように前記メディアファイルをセキュアなやり方でマシン群に配信するよう動作する。

【００１９】

本発明の他の実施形態は、特定のユーザによって購入された前記メディアファイルのセットが前記特定のユーザと関連付けられた限定された個数のマシン上での使用について許可されえるメディア配信システムに関する。

【００２０】

ローカルマシンにおいてメディアファイルを示すコンピュータプログラムコードを少なくとも含むコンピュータで読み取り可能な媒体として本発明のある実施形態は、示すべきメディアファイルを特定するコンピュータプログラムコードであって、前記特定されたメディアファイルは少なくとも暗号化されたメディアコンテンツデータ、ユーザキー参照、および暗号化されたコンテンツキーを有する、特定するコンピュータプログラムコード、ユーザキーを前記ユーザキー参照に基づいて前記特定されたメディアファイル内で得るコンピュータプログラムコード、前記暗号化されたコンテンツキーを前記特定されたメディアファイルから得るコンピュータプログラムコード、前記暗号化されたコンテンツキーを前記ユーザキーを用いて復号することによって、前記コンテンツキーを得るコンピュータプログラムコード、前記特定されたメディアファイルの前記暗号化されたメディアコンテンツデータを前記コンテンツキーで復号するコンピュータプログラムコード、および前記特定されたメディアファイルの前記メディアコンテンツデータを示すコンピュータプログラムコードを含む。

【００２１】

本発明の他の局面および優位性は、以下の詳細な説明を添付の図面と併せるなら明らかになり、ここで図面は本発明の原理を例によって示す。

【発明を実施するための最良の形態】

【００２２】
本発明は、添付の図面と併せて以下の詳細な説明によって容易に理解されよう。図面において同様の参照番号は同様の構成要素を表す。
【００２３】
本発明は、ネットワークベースのコンテンツの配信に関する。コンテンツの配信はセキュアであるだけでなくコントロールされている。このセキュリティは、ダウンロードのあいだ、かつサーバまたはクライアントに記憶されているあいだにメディアファイル内のコンテンツへのアクセスを制限する。ある実施形態において、それぞれのメディアファイルは、異なる、ランダムに配信されたキーで暗号化される。メディアファイルの配信へのコントロールは、クライアントから他のクライアントへのメディアファイルの後に続く配信を制限するよう働きえる。他の実施形態において、このコントロールは、メディアファイルが、同じユーザに関係した限られた数の異なるクライアント上で共有されることを許可しえる。このクライアント群は、アプリケーションによって異なりえるが一般にはメモリ記憶を有するコンピューティングデバイスである。しばしば、このクライアントは、コンテンツを記憶およびそのユーザに提示することができるパーソナルコンピュータまたは他のコンピューティングデバイスである。
【００２４】
本発明は、クライアント・サーバ環境におけるコンテンツのコントロールされた配信のための方法およびシステムに関する。コントロールされた配信は、コンテンツへの無許可アクセスを制限するだけでなく、許可されたユーザによってコンテンツへの使用権を制限もするために暗号化およびユーザアカウントを利用する。
【００２５】
このコンテンツは例えば、オーディオ、ビデオ、または画像データでありえる。このコンテンツはまた、メディアコンテンツまたはメディア（オーディオ、ビデオ、または画像データを指すとき）とも呼ばれえる。このコンテンツは典型的には、メディアファイルとして知られるファイルに含まれる。このようなメディアファイルは、ディジタル形式を有し、データ記憶媒体上に記憶される。例えば、データ記憶媒体は、コンパクトディスク、磁気記憶装置、半導体メモリデバイス、光学記憶装置などに関係しえる。
【００２６】
本発明のこの局面の実施形態は、以下に図１～７を参照して説明される。しかし当業者は、これら図を参照してここで与えられた詳細な記載は例示的目的であって、本発明はこれら限定された実施形態を超えた範囲に達することがわかろう。
【００２７】
図１は、本発明のある実施形態によるメディア配信システム１００のブロック図である。メディア配信システム１００は、メディアサーバ１０２を含む。このメディアサーバ１０２は、メディアファイルを記憶、管理およびダウンロードする。メディアファイルは、ローカルメディアソース１０４またはリモートメディアソース１０６によってメディアサーバ１０２に与えられる。ローカルメディアソース１０４は、コンパクトディスク（ＣＤ）、磁気記憶デバイス、ディジタル多用途ディスク（ＤＶＤ）、またはディスクドライブの形でありえる。典型的には、ローカルメディアソース１０４は、メディア会社に提供され、ホスティング位置においてメディアサーバ１０２に届けられえる取り外し可能な媒体である。リモートメディアソース１０６は、インターネットのようなデータネットワーク１０８を通してメディアサーバ１０２に結合するコンピューティングデバイスに関連しえる。リモートメディアソース１０６は、メディアファイルをデータネットワーク１０８を通してメディアサーバ１０２へ送信またはストリーミングできる。メディアソース１０４、１０６からメディアサーバ１０２において受け取られたメディアファイルは、処理されてからメディア記憶１１０に記憶されえる。メディアファイルのメディアサーバ１０２における処理は、暗号化を用いてファイルを安全にしえ、また予想されるユーザ（すなわち購入者）にダウンロードするようメディアファイルを準備しえる。
【００２８】

メディア配信システム１００は、クライアントマシン１１２および１１４のユーザがメディアサーバ１０２にデータネットワーク（インターネット）１０８を介してアクセスすることを可能にする。したがって、クライアントマシン１１２および１１４のユーザは、メディアサーバ１０２と相互作用することができる。そのような相互作用を通して、クライアントマシン１１２および１１４のユーザは、メディア記憶１１０に記憶されたメディアファイルをブラウズし、購入のためにメディアファイルを選択し、購入したメディアファイルをダウンロードし、その後、それぞれのクライアントマシン１１２および１１４において購入したメディアファイルを再生することができる。メディア配信システム１００は、暗号化プロセスを通じてメディアファイルへのアクセスに対して制限を課するよう動作する。メディア配信システム１００はまた、ダウンロードされた購入したメディアファイルに対して使用制限が課せられるようにする。

【００２９】

クライアントマシン１１２および１１４は、汎用または特定目的のためのコンピューティングデバイスである。最近では、コンピューティングデバイスは、より小さく、よりコンパクトになっている。このコンピューティングデバイスはまた主に静止した、または携帯での使用のために設計されえる。本発明が適する携帯コンピューティングデバイスの一つのタイプは、ハンドヘルドコンピューティングデバイスとして知られる。ハンドヘルドコンピューティングデバイスは時には、汎用のパーソナルコンピュータであるよりは、特別なコンピューティングデバイスである。例えば、ハンドヘルドコンピューティングデバイスの一つのタイプは、携帯（またはパーソナル）メディアプレーヤーである。メディアプレーヤーはまた、家庭用電子製品とも呼ばれる。メディアプレーヤーは、ＭＰ３ファイル、ＭＰＥＧファイル、アドバンストオーディオコーディング（ＡＡＣ）ファイル、コンパクトディスクまたはＤＶＤのようなメディアをユーザのために再生する。ある実施形態において、メディアプレーヤーは、メディアプレーヤーによって再生されるメディアコンテンツの大量記憶を提供するためにディスクドライブを利用しえる。

【００３０】

図２は、本発明のある実施形態によるメディアサーバ２００のブロック図である。メディアサーバ２００は例えば、図１に示されるメディアサーバ１０２として用いるのに適する。この点で、メディアサーバ２００はネットワーク（例えばデータネットワーク１０８）およびメディア記憶（例えばメディア記憶１１０）に結合する。

【００３１】

メディアサーバ２００は、メディア記憶マネージャ２０２、メディア購入マネージャ２０４、メディアダウンロードマネージャ２０６、およびユーザアカウント２０８を含む。メディア記憶マネージャ２０２は、入力メディアファイルを受け取り、結果として生じるダウンロードのためにメディアファイルを処理し、ファイルをメディア記憶に記憶するよう動作する。メディア購入マネージャ２０４は、メディアサーバ２００とのオンライン・インタラクションを通じてクライアントマシン（例えば図１に示されるクライアントマシン１１２および１１４）のユーザが１つ以上のメディアファイルを購入することを手伝う。典型的には、メディア購入マネージャ２０４は、ユーザが電子商取引トランザクションを完了するのを手伝うことによって、ユーザが１つ以上のメディアファイルを受け取り、利用する権利を購入することを可能にする。メディアダウンロードマネージャ２０６は、メディアファイルを購入したユーザの適切なクライアントマシンに、購入されたメディアファイルをダウンロードすることを促進する。ユーザアカウント２０８は、システムのユーザに関するユーザ情報を記憶する。ある実施形態において、ユーザ情報は、それぞれのユーザに関連付けられたユーザキー群のセットを含む。このユーザキー群は、それについてのアクセス権を購入した特定のユーザについてメディアファイルを暗号化するとき、メディアサーバ２００によって用いられる。ユーザについてのユーザキー群の管理を通して、メディアサーバ２００は、メディアファイルを受け取ったり、利用したりすることができるクライアントマシンの個数またはタイプを制限しえる。

【００３２】

図３は、本発明のある実施形態によるメディア記憶処理３００のフロー図である。メディア記憶処理３００は、例えば、図１に示されるメディアサーバ１０２または図２に示されるメディア記憶マネージャ２０２によって実行される。

【００３３】

メディア記憶処理３００は、初めにメディアファイルをメディアサーバにおいて受け取る（３０２）。メディアファイルは、それがメディアデータを含むように構築され、さらにメタデータを含みえる。メタデータは、データの特性を記述する。例えば、メタデータは、名前、アーチスト、著作権情報、タイトルなどのような特性を示しえる。メディアファイルのメタデータは、オプションとして、例えばグローバルキーと共に暗号化される（３０４）。ある実施形態において、グローバルキーは、メディアサーバにおける全てのメディアファイルについてのメタデータを暗号化するのに用いられる。他の実施形態においてはもし所望であれば、異なるメディアサーバについては異なるグローバルキーが用いられえる。典型的にはメタデータは、それほど機密性が高くないので暗号化するための共通グローバルキーの使用が適切である。しかし、もしより強力な暗号化が望まれるなら、セキュリティのレベルを上げるために、より特別なキーが用いられえる。他の実施形態においては、メタデータは暗号化されない。

【００３４】

ダウンロードキーもメディアファイルについて生成される（３０６）。このダウンロードキーは、記憶されるべきそれぞれのメディアファイルについて生成される実質的にランダムな秘密鍵である。次に、メディアファイルがこのダウンロードキーで暗号化される（３０８）。ここで、メディアファイルは、その特定のメディアファイルに対応するダウンロードキーで暗号化される（３０８）。この時点で、メディアファイル（暗号化されたメディアファイル）は、暗号化を通じて機密が確保され、潜在的ユーザにダウンロードする準備ができている。メディアファイルが暗号化された（３０８）後、暗号化されたメディアファイルは中央メディア記憶に記憶される（３１０）。ある実施形態において、中央メディア記憶は図１のメディア記憶１１０である。操作３１０に続いて、メディア記憶処理３００は完了し終了する。

【００３５】

いったん中央メディア記憶に記憶されると、暗号化されたメディアファイルは、購入され、メディアファイルへの無許可のアクセスを防ぐために、購入者にその暗号化されたフォーマットで送信されえる。したがって暗号化されたメディアファイルを中央メディア記憶に記憶することによって、メディアファイルは暗号化されて記憶され、ほとんどまたは全く追加の処理なしでダウンロードされるべく用意ができている。その結果、サーバはより効率的であり、メディアファイルのダウンロードに対するより多くの要求を扱うことができる。

【００３６】

図４Ａおよび４Ｂは、本発明のある実施形態によるメディア購入およびダウンロード処理４００のフロー図である。メディア購入およびダウンロード処理４００は例えば、図１に示されるメディアサーバ１０２または図２に示されるメディアサーバ２００のメディア購入マネージャ２０４およびメディアダウンロードマネージャ２０６によって実行される。

【００３７】

メディア購入およびダウンロード処理４００は最初に、購入可能であるメディアファイルをユーザがブラウズすることを許可する（４０２）。ここでは、メディアファイルのうちの１つ以上を購入するかどうかをユーザが決定するのを助けるために、ユーザはメディアファイルをブラウズすることができる。しばしばユーザは、メディアファイルについてのメタデータの少なくとも一部を見て、メディアファイルに関連付けられたテキストを見て、および／またはメディアファイルに関するオーディオ、グラフィックスまたはビデオを試すことができる。

【００３８】

ブラウズ（４０２）した後、ユーザは購入のためのメディアファイルを選択する（４０４）。それから、ユーザはそのメディアファイルを購入し（４０６）、関連付けられたダウンロードキーを受け取る。ユーザはまた、メディアファイルが購入されるときにグローバルキーを受け取りえる。ここで、メディアファイルの購入は、クレジットカード、デビットカード、または支払い支援（例えば、PayPal、Neteller、プリペイドATMなど）のようなさまざまな金融送金手段の任意のものを通して、ユーザがメディアファイルへのアクセスのために支払いをする電子商取引のトランザクションでありえる。

【００３９】

次に、メディアファイルはユーザへダウンロードされる（４０８）。ある実施形態において、メディアファイルのダウンロード４０８は、データネットワークを通してユーザへ、すなわちユーザのクライアントマシンへメディアファイルをストリーミングすることによって実行されえる。ここで、メディアファイルのダウンロード４０８は効率的であるが、それはメディアファイルが記憶されている方法のために、処理が重い変換なしでその迅速なダウンロードが促進されるからである。

【００４０】

いったんメディアファイルがダウンロードされる（４０８）と、メディアファイルはそれからユーザのローカルマシンにおいてダウンロードキーを用いて復号される（４１０）。さらにこの時点で、もしメディアファイルそのもののメタデータが暗号化されているなら、そのメタデータもメディアファイルへのアクセス権を購入したユーザへ前に提供されたグローバルキーを用いて復号されえる。

【００４１】

メディアアイテムの購入４０６に続いて、ユーザに関連付けられたユーザキーが取り出される（４１２）。ユーザキーのうちの一つが選択される（４１４）。ユーザキーは、セキュリティを改善するために回転（例えば循環）されえる。ある実施形態において、許可されえる異なるクライアントマシンの個数は制限されえ、それにより所定の制限された個数のクライアントマシンより多いマシン上で、ダウンロードされたメディアファイルを利用するユーザの能力が制限される。

【００４２】

ユーザがユーザキーのうちの一つを選択（４１４）した後、ランダムコンテンツキーが生成される（４１６）。ランダムコンテンツキーは、実質的にランダムに生成されるか、または疑似ランダムに生成されるキーである。それから、メディアファイルのメディア部がランダムコンテンツキーで暗号化される（４１８）。ランダムコンテンツキーはそれから、選択されたユーザキーでそれ自身が暗号化される（４２０）。

【００４３】

次に、メディアファイルは、ユーザキー参照および暗号化されたランダムコンテンツキーをさらに含むように変更される（４２２）。オプションとして、メディアファイルは、メディアファイルへのアクセス権を購入したユーザを識別する情報を含むようにさらに変更されえる。例えば、メディアファイルは、グローバルキー（アクセス権を購入したユーザに関連付けられる）の暗号化されたバージョンをメディアファイル内に格納することによってユーザ識別情報を含むように変更されえる。オプションとして、メディアファイルのメディア部は、ユーザ識別可能な情報でディジタル的に透かしが入れられることによって変更されえる。

【００４４】

クライアントマシン上でメディアファイルを利用するためには、適切なユーザキーが必要とされ、このユーザキー参照はユーザキーが位置特定されることを可能にする（もしそれが存在するなら）。ある実施形態において、もしユーザキーが存在するなら、ユーザキーは、ユーザのクライアントマシンのローカルデータ記憶内に記憶される。同様に、変更されたメディアファイルは、ローカルデータ記憶に記憶される（４２４）。例えば、ローカルデータ記憶は、ディスクドライブ、ランダムアクセスメモリ、取り外し可能な媒体などでありえる。また、ある実施形態においては、ローカルデータ記憶内の変更されたメデ

ィアファイルの記憶を管理するためにデータベースが利用されえる。操作４２４に続いて、メディア購入およびダウンロード処理４００は完了し終了する。

【００４５】

メディアファイルは、暗号化されていようといまいと、さまざまなファイルフォーマットを有しえる。例えば、ある適切なファイルフォーマットはＭＰＥＧ４フォーマットである。他の適切なフォーマットには、QuickTimeムービー、ＭＰＥＧ－１フォーマットおよびＭＰＥＧ－２フォーマットが含まれる。

【００４６】

図５Ａおよび５Ｂは、本発明の他の実施形態によるメディア購入およびダウンロード処理５００のフロー図である。メディア購入およびダウンロード処理５００は例えば、図１に示されるメディアサーバ１０２によってまたは図２に示されるメディアサーバ２００のメディア購入マネージャ２０４およびメディアダウンロードマネージャ２０６によって実行される。

【００４７】

メディア購入およびダウンロード処理５００は最初に、購入可能であるメディアファイルをユーザがブラウズすることを許可する（５０２）。ここでは、メディアファイルのうちの１つ以上を購入するかどうかをユーザが決定するのを助けるために、ユーザはメディアファイルをブラウズすることができる。しばしばユーザは、メディアファイルについてのメタデータの少なくとも一部を見て、メディアファイルに関連付けられたテキストを見て、および／またはメディアファイルに関するオーディオ、グラフィックスまたはビデオを試すことができる。

【００４８】

ブラウズ（５０２）した後、ユーザは購入のためのメディアファイルを選択する（５０４）。それから、ユーザはそのメディアファイルを購入し（５０６）、関連付けられたダウンロードキーを受け取る。ユーザはまた、メディアファイルが購入されるときにグローバルキーを受け取りえる。ここで、メディアファイルの購入は、クレジットカード、デビットカード、または支払い支援（例えば、PayPal、Neteller、プリペイドATMなど）のようなさまざまな金融送金手段の任意のものを通して、ユーザがメディアファイルへのアクセスのために支払いをする電子商取引のトランザクションでありえる。

【００４９】

次に、メディアファイルはユーザへダウンロードされる（５０８）。ある実施形態において、メディアファイルのダウンロード５０８は、データネットワークを通してユーザへ、すなわちユーザのクライアントマシンへメディアファイルをストリーミングすることによって実行されえる。ここで、メディアファイルのダウンロード５０８は効率的であるが、それはメディアファイルが記憶されている方法のために、処理が重い変換なしでその迅速なダウンロードが促進されるからである。

【００５０】

メディアアイテムの購入５０６に続いて、ユーザに関連付けられたユーザキーが取り出される（５１０）。それから、ユーザキーのうちの一つが選択される（５１２）。ユーザキーは、セキュリティを改善するために回転（例えば循環）されえる。ある実施形態において、許可されえる異なるクライアントマシンの個数は制限されえ、それにより所定の制限された個数のクライアントマシンより多いマシン上で、ダウンロードされたメディアファイルを利用するユーザの能力が制限される。

【００５１】

ユーザがユーザキーのうちの一つを選択（５１２）した後、ランダムコンテンツキーが生成される（５１４）。ランダムコンテンツキーは、実質的にランダムに生成されるか、または疑似ランダムに生成されるキーである。それから、メディアファイルのメディア部がダウンロードキーおよびランダムコンテンツキーを用いて転写される（５１６）。ランダムコンテンツキーはそれから、選択されたユーザキーでそれ自身が暗号化される（５１８）。

【００５２】
次に、メディアファイルは、ユーザキー参照および暗号化されたランダムコンテンツキーをさらに含むように変更される（５２０）。オプションとして、メディアファイルは、メディアファイルへのアクセス権を購入したユーザを識別する情報を含むようにさらに変更されえる。例えば、メディアファイルは、グローバルキー（アクセス権を購入したユーザに関連付けられる）の暗号化されたバージョンをメディアファイル内に格納することによってユーザ識別情報を含むように変更されえる。
【００５３】
クライアントマシン上でメディアファイルを利用するためには、適切なユーザキーが必要とされ、このユーザキー参照はユーザキーが位置特定されることを可能にする（もしそれが存在するなら）。ある実施形態において、もしユーザキーが存在するなら、ユーザキーは、ユーザのクライアントマシンのローカルデータ記憶内に記憶される。同様に、変更されたメディアファイルは、ローカルデータ記憶に記憶される（５２２）。例えば、ローカルデータ記憶は、ディスクドライブ、ランダムアクセスメモリ、取り外し可能な媒体などでありえる。また、ある実施形態においては、ローカルデータ記憶内の変更されたメディアファイルの記憶を管理するためにデータベースが利用されえる。操作５２２に続いて、メディア購入およびダウンロード処理５００は完了し終了する。
【００５４】
図６Ａおよび６Ｂは、本発明のさらに他の実施形態によるメディア購入およびダウンロード処理６００のフロー図である。メディア購入およびダウンロード処理６００は例えば、図１に示されるメディアサーバ１０２によってまたは図２に示されるメディアサーバ２００のメディア購入マネージャ２０４およびメディアダウンロードマネージャ２０６によって実行される。
【００５５】
メディア購入およびダウンロード処理６００は最初に、購入可能であるメディアファイルをユーザがブラウズすることを許可する（６０２）。ここでは、メディアファイルのうちの１つ以上を購入するかどうかをユーザが決定するのを助けるために、ユーザはメディアファイルをブラウズすることができる。しばしばユーザは、メディアファイルについてのメタデータの少なくとも一部を見て、メディアファイルに関連付けられたテキストを見て、および／またはメディアファイルに関するオーディオ、グラフィックスまたはビデオを試すことができる。
【００５６】
ブラウズ（６０２）した後、ユーザは購入のためのメディアファイルを選択する（６０４）。それから、ユーザはそのメディアファイルを購入する（６０６）。ここで、メディアファイルの購入は、クレジットカード、デビットカード、または支払い支援（例えば、PayPal、Neteller、プリペイドATMなど）のようなさまざまな金融送金手段の任意のものを通して、ユーザがメディアファイルへのアクセスのために支払いをする電子商取引のトランザクションでありえる。
【００５７】
メディアアイテムの購入６０６に続いて、ユーザに関連付けられたユーザキーが取り出される（６０８）。それから、ユーザキーのうちの一つが選択される（６１０）。ユーザキーは、セキュリティを改善するために回転（例えば循環）されえる。ある実施形態において、許可されえる異なるクライアントマシンの個数は制限されえ、それにより所定の制限された個数のクライアントマシンより多いマシン上で、ダウンロードされたメディアファイルを利用するユーザの能力が制限される。
【００５８】
ユーザがユーザキーのうちの一つを選択（６１０）した後、ランダムコンテンツキーが生成される（６１２）。ランダムコンテンツキーは、実質的にランダムに生成されるか、または疑似ランダムに生成されるキーである。それから、メディアファイルのメディア部がランダムコンテンツキーで暗号化される（６１４）。ランダムコンテンツキーはそれか

ら、選択されたユーザキーでそれ自身が暗号化される（６１６）。

【００５９】

次に、メディアファイルは、ユーザキー参照および暗号化されたランダムコンテンツキーをさらに含むように変更される（６１８）。オプションとして、メディアファイルは、メディアファイルへのアクセス権を購入したユーザを識別する情報を含むようにさらに変更されえる。例えば、メディアファイルは、グローバルキー（アクセス権を購入したユーザに関連付けられる）の暗号化されたバージョンをメディアファイル内に格納することによってユーザ識別情報を含むように変更されえる。オプションとして、メディアファイルのメディア部は、ユーザ識別可能な情報でディジタル的に透かしが入れられることによって変更されえる。

【００６０】

メディアファイルがそれからユーザにダウンロードされる（６２０）。この実施形態において、メディアファイルのダウンロード６２０は、メディアファイルをデータネットワークを通してユーザに、すなわちユーザのクライアントマシンにストリーミングすることによって実行されえる。

【００６１】

クライアントマシン上でメディアファイルを利用するためには、適切なユーザキーが必要とされ、このユーザキー参照はユーザキーが位置特定されることを可能にする（もしそれが存在するなら）。ある実施形態において、もしユーザキーが存在するなら、ユーザキーは、ユーザのクライアントマシンのローカルデータ記憶内に記憶される。同様に、変更されたメディアファイルは、ローカルデータ記憶に記憶される（６２２）。例えば、ローカルデータ記憶は、ディスクドライブ、ランダムアクセスメモリ、取り外し可能な媒体などでありえる。また、ある実施形態においては、ローカルデータ記憶内の変更されたメディアファイルの記憶を管理するためにデータベースが利用されえる。操作６２２に続いて、メディア購入およびダウンロード処理６００は完了し終了する。

【００６２】

図７は、本発明のある実施形態による再生処理７００のフロー図である。再生処理７００は、図１に示されるクライアントマシン１１２またはクライアント１１４のようなクライアントマシン（ユーザマシン）において実行される。クライアントマシンは、デスクトップコンピュータ、ノートブックコンピュータ、ハンドヘルドコンピュータ、パーソナルディジタルアシスタント、メディアプレーヤー、およびさまざまな他のデバイスでありえる。

【００６３】

再生処理７００は、クライアントマシンのユーザが再生のためにローカルデータ記憶内のメディアファイルをブラウズすること（７０２）を可能にする。換言すれば、再生のために利用可能であるメディアファイルがユーザによって検索され、スキャンされ、またはレビュー（例えばブレビュー）されえる。典型的には、ユーザはメディアファイルを通してメディアファイルについてのメタデータを用いてブラウズするか、またはおそらくはメディアファイルのサンプルを試す。次は、再生されるべきメディアファイルが選択される（７０４）。それから、ユーザキー参照が選択されたメディアファイルから得られる（７０６）。前述のように、ローカルメディア記憶に記憶されているメディアファイルは、メディアファイル内に含まれたユーザキー参照を有する。したがって、ユーザキー参照は、選択されたメディアファイルから獲得されえる（７０６）。ユーザキーはそれから、選択されたメディアファイルから得られた（７０６）ユーザキー参照に基づいてクライアントマシン（例えばローカルデータ記憶）内で位置特定される（７０８）。

【００６４】

次に、判定７１０は、ユーザキーが見つかったかを決定する。判定７１０が、ユーザキーが見つけられないと決定するなら、ユーザはクライアントマシンをメディアファイルにアクセスするのに適切に設定されておらず、したがって、ユーザアカウントがメディアサーバでセットアップ（７１２）されなければならない。これは、ユーザがメディアサーバ

とクライアントマシンを介してやりとりして、クライアントマシンに特定のユーザアカウントをセットアップすることを要求する。ユーザアカウントのセットアップ７１２に続いて、再生処理７００は、ユーザキーが位置特定されえるよう、操作７０８および後続の操作を反復するために元に戻る。

【００６５】

一方、判定７１０が、ユーザキーが見つかったと決定するとき、暗号化されたランダムコンテンツキーは選択されたメディアファイルから得られる（７１４）。再び、選択されたメディアファイルの性質から、それは暗号化されたランダムコンテンツキーを含む。それから、暗号化されたランダムコンテンツキーは、ユーザキーで復号される（７１６）。復号７１６から生じるランダムコンテンツキーは、それからメディアファイルの暗号化されたメディア部を復号する（７１８）のに用いられえる。この時点で、メディアファイルのメディア部は「嫌疑が晴れて」いる。最後に、メディアファイルのメディア部はクライアントマシンにおいて再生される（７２０）。操作７２０に続いて、再生処理７００は、完了し終了する。

【００６６】

本発明の上述のさまざまな局面、特徴、実施形態または実現例は、単独で、またはさまざまな組み合わせにおいて用いられえる。

【００６７】

メディアファイルは、オーディオアイテム（例えば、音楽のようなオーディオファイルまたはソング）、ビデオアイテム（例えば、ビデオファイルまたはムービー）、または画像アイテム（例えば、写真）に関しえる。

【００６８】

本発明は好ましくはソフトウェアによって実現されるが、ハードウェアにおいても、またはハードウェアおよびソフトウェアの組み合わせにおいても実現されえる。本発明はまた、コンピュータで読み取り可能な媒体上のコンピュータによって読み取り可能なコードとして実現されえる。コンピュータで読み取り可能な媒体は、その後にコンピュータシステムによって読み取られえる任意のデータ記憶デバイスである。コンピュータで読み取り可能な媒体の例には、読み出し専用メモリ、ランダムアクセスメモリ、ＣＤ－ＲＯＭ、ＤＶＤ、磁気テープ、光データ記憶デバイス、および搬送波が含まれる。コンピュータで読み取り可能な媒体は、コンピュータによって読み取り可能なコードが分散化されたやり方で記憶され実行されるようにネットワークで結合されたコンピュータシステム上にも配信されえる。

【００６９】

本発明の効果は数多くある。異なる実施形態または実現例は、以下の効果の１つ以上を生みえるが、必ずしも生まなくてもよい。本発明のある効果は、暗号化およびユーザアカウントが用いられて、コンテンツのコントロールされた配信を提供することである。コントロールされた配信は、コンテンツへの無許可のアクセスを制限するだけでなく、無許可ユーザによるコンテンツに対する使用権限を制限する。本発明の他の効果は、メディアファイルに特定の暗号化がサーバ側において利用されえ、一方、ユーザに特定の暗号化がクライアント側において使用されえることである。本発明の他の効果は、メディアファイルがおいて記憶および許可された（例えば、そのような権利を購入することによって）任意のユーザへのダウンロードのためにサーバ側において共通して暗号化されえることである。本発明の他の効果は、クライアント側における全てのメディアファイルが異なるキーで暗号化されるように、メディアファイルがクライアント側においてランダムな基準を用いて再暗号化されえることである。本発明のさらに他の効果は、もし所望であれば、購入されたメディアファイルは、メディアファイル内のコンテンツが制限された個数のクライアント（ユーザマシン）上でだけ再生されるように制限された使用権を有しえることである。本発明のさらに他の効果は、クライアント側におけるメディアファイルがメタデータ（暗号化されずに記憶されている）についてブラウズされえ、一方、メディアコンテンツデータへのアクセスは暗号化を通して保護されていることである。

【００７０】
本発明の多くの特徴および優位性は、記載された説明から明らかであり、よって添付の特許請求の範囲によって、本発明のそのような特徴および優位性の全てをカバーすることが意図される。さらに、多くの変更および改変が当業者には容易に可能であるので、本発明は、図示され記載されたものと全く同じ構成および動作に限定されるべきではない。したがって、全ての適切な改変物および等価物は本発明の範囲に入るものとされる。

【図面の簡単な説明】

【００７１】
【図１】本発明のある実施形態によるメディア配信システムのブロック図である。
【図２】本発明のある実施形態によるメディアサーバのブロック図である。
【図３】本発明のある実施形態によるメディア記憶処理のフロー図である。
【図４Ａ】本発明のある実施形態によるメディア購入およびダウンロード処理のフロー図である。
【図４Ｂ】本発明のある実施形態によるメディア購入およびダウンロード処理のフロー図である。
【図５Ａ】本発明の他の実施形態によるメディア購入およびダウンロード処理のフロー図である。
【図５Ｂ】本発明の他の実施形態によるメディア購入およびダウンロード処理のフロー図である。
【図６Ａ】本発明のさらに他の実施形態によるメディア購入およびダウンロード処理のフロー図である。
【図６Ｂ】本発明のさらに他の実施形態によるメディア購入およびダウンロード処理のフロー図である。
【図７】本発明のある実施形態による再生処理のフロー図である。

【図１】

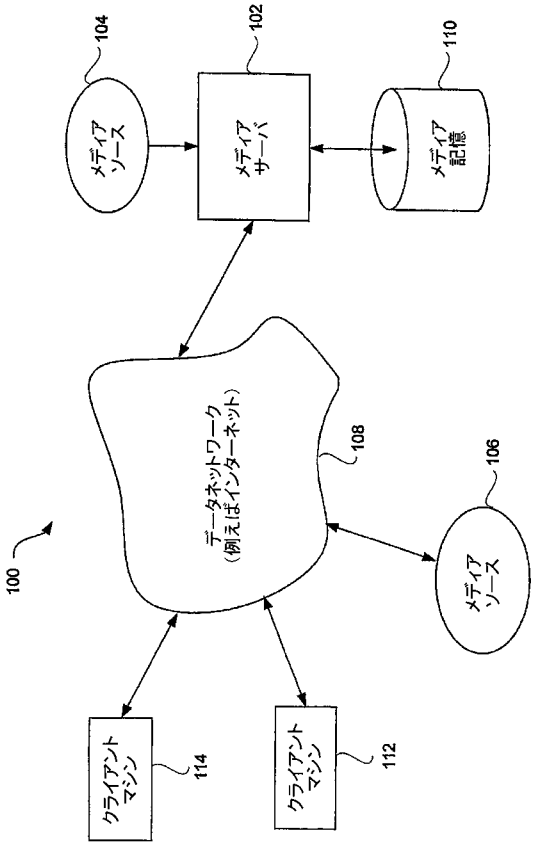



FIG. 1

【図２】

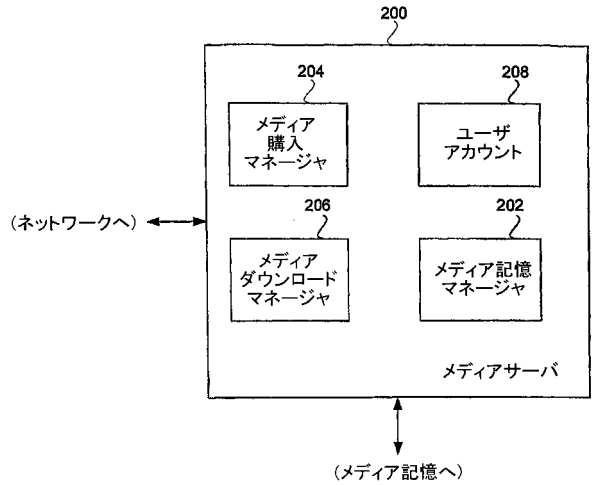



FIG. 2

【図３】

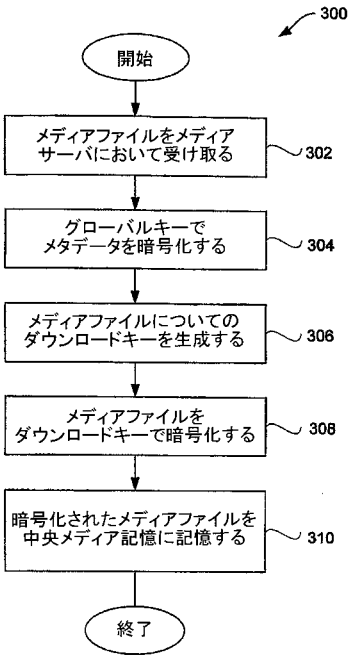



FIG. 3

【図４Ａ】

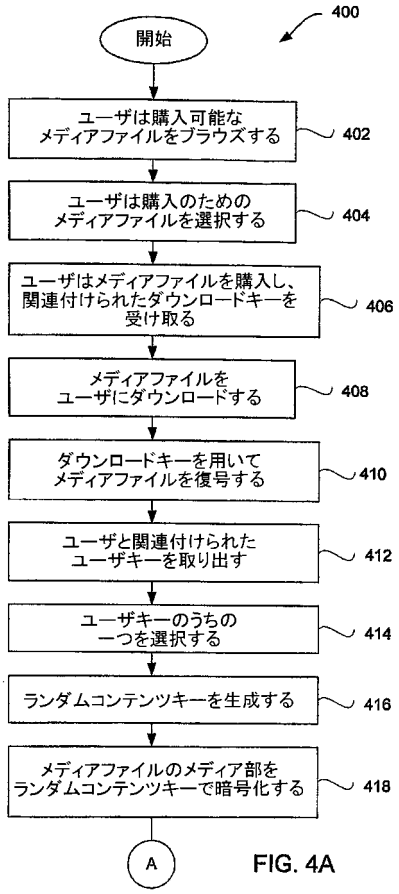



FIG. 4A

【図４Ｂ】

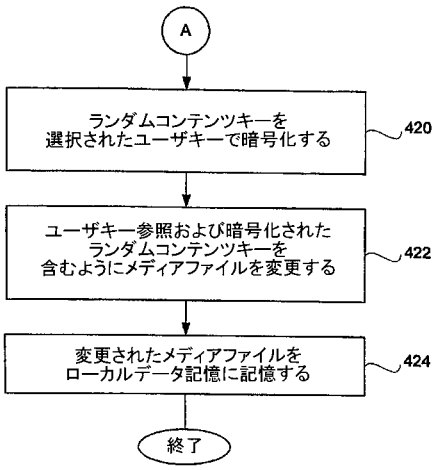



FIG. 4B

【図５Ａ】

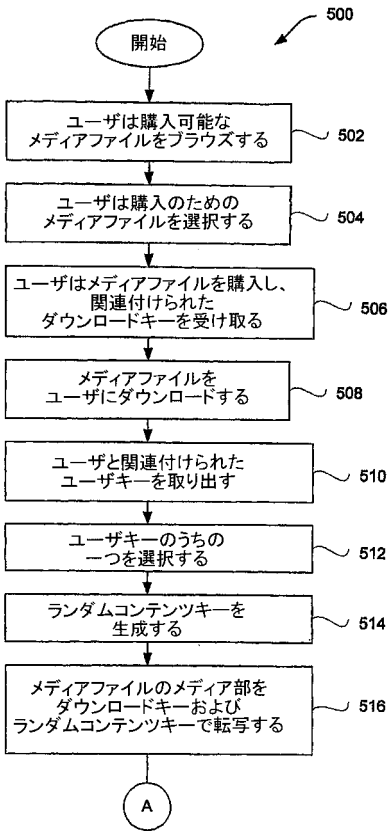



FIG. 5A

【図５Ｂ】

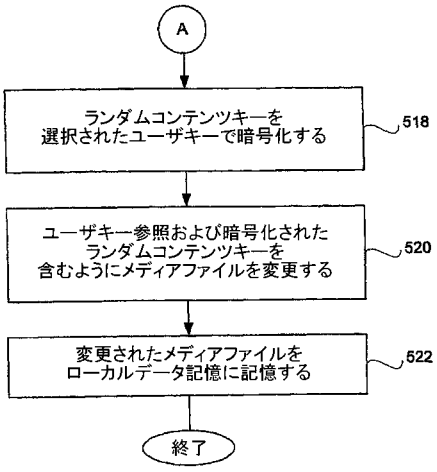



FIG. 5B

【図６Ａ】

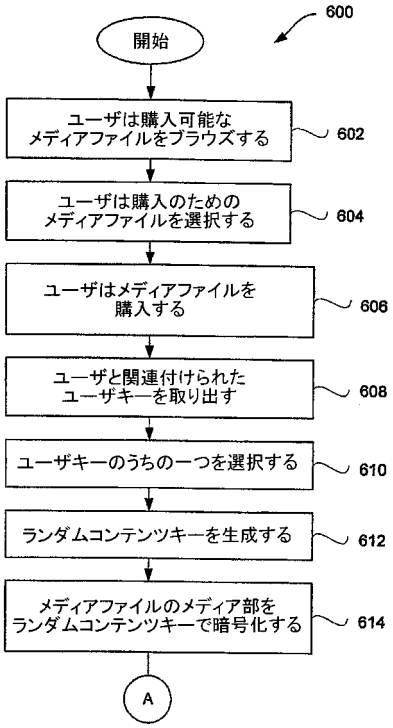



FIG. 6A

【図６Ｂ】

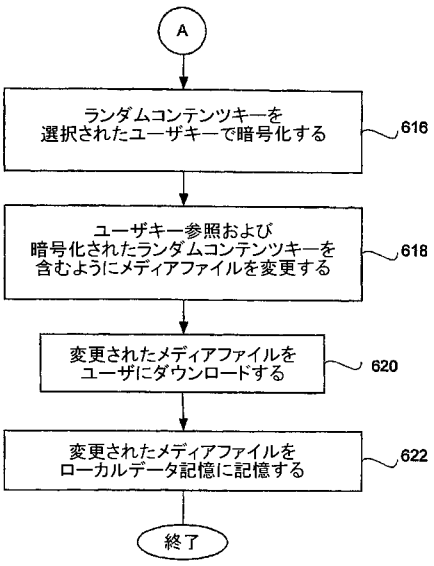



FIG. 6B

【図７】

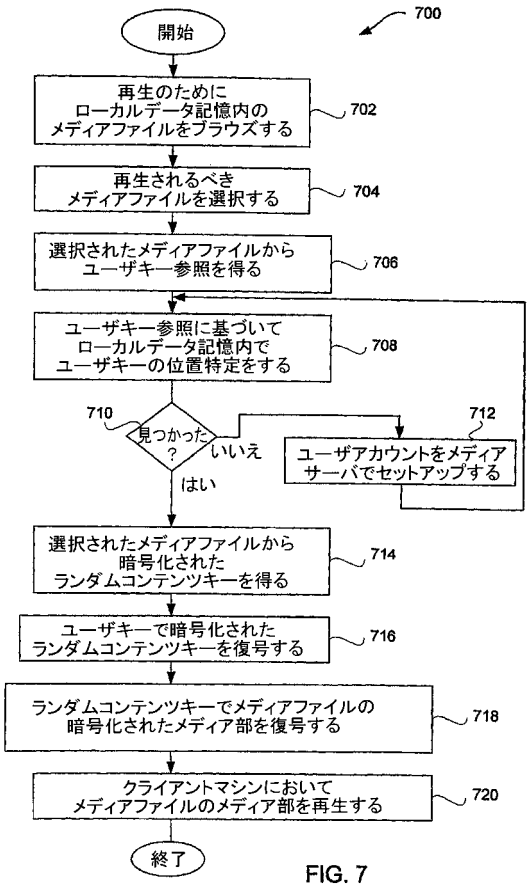



FIG. 7

【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/012848

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

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)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 2002/002468 A1 (GEISLER DOUGLAS R ET AL) 3 January 2002 (2002-01-03) | 1-5,45, 51-54, 58-60 |
| Y | page 5, paragraph 52<br>page 7, paragraphs 71,72<br>page 8, paragraph 76<br>page 11, paragraph 152 - page 13, paragraph 182<br>page 14, paragraphs 201,206<br>page 14, paragraph 211 - page 15, paragraph 225<br>page 35, paragraph 664 | 6-32, 46-50, 55-57 |

-/--

[X] Further documents are listed in the continuation of box C

[X] Patent family members are listed in 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 |
|---|---|
| 12 October 2004 | 20/10/2004 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Arbutina, L |

Form PCT/ISA/210 (second sheet) (January 2004)

## INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/012848

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No |
|---|---|---|
| X | WO 01/46786 A (LIQUID AUDIO INC)<br>28 June 2001 (2001-06-28)<br>page 3, paragraph 2 - page 4, paragraph 2 | 33-44,<br>60,69-71 |
| Y | page 6, last line - page 8, line 4<br><br>page 9, paragraph 2 - page 10, paragraph 3<br>page 14, paragraph 2 - page 17, paragraph 4<br>page 21, paragraph 4 - page 26, line 4 | 6-32,<br>46-50,<br>55-57 |
| X | WO 01/44908 A (MICROSOFT CORP)<br>21 June 2001 (2001-06-21)<br>page 9, line 6 - line 30<br>page 30, line 20 - page 37, line 14<br>page 14, line 22 - page 21, line 2<br>page 26, line 4 - line 21 | 1,60-68 |
| X | US 6 385 596 B1 (ANSELL STEVEN T ET AL)<br>7 May 2002 (2002-05-07)<br>column 3, line 51 - column 4, line 12<br>column 6, line 48 - column 8, line 17<br>column 9, line 40 - line 67<br>column 12, line 55 - column 14, line 35<br>column 16, line 26 - column 19, line 43<br>figure 2 | 1,45,51,<br>60 |

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2004/012848

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2002002468 A1 | 03-01-2002 | US 2003105718 A1 | 05-06-2003 |
| | | US 6389538 B1 | 14-05-2002 |
| | | US 6226618 B1 | 01-05-2001 |
| | | EP 1077398 A1 | 21-02-2001 |
| | | US 2002107803 A1 | 08-08-2002 |
| | | AU 763380 B2 | 24-07-2003 |
| | | AU 5481899 A | 06-03-2000 |
| | | CA 2338414 A1 | 24-02-2000 |
| | | CA 2467974 A1 | 24-02-2000 |
| | | CA 2467998 A1 | 24-02-2000 |
| | | CN 1320232 T | 31-10-2001 |
| | | EP 1104555 A2 | 06-06-2001 |
| | | JP 2002522995 T | 23-07-2002 |
| | | TW 454132 B | 11-09-2001 |
| | | WO 0008909 A2 | 24-02-2000 |
| | | US 6263313 B1 | 17-07-2001 |
| | | US 6345256 B1 | 05-02-2002 |
| | | US 6398245 B1 | 04-06-2002 |
| | | US 6587837 B1 | 01-07-2003 |
| | | US 6418421 B1 | 09-07-2002 |
| | | US 6389403 B1 | 14-05-2002 |
| | | US 6574609 B1 | 03-06-2003 |
| WO 0146786 A | 28-06-2001 | US 6792113 B1 | 14-09-2004 |
| | | AU 1432301 A | 03-07-2001 |
| | | EP 1240568 A1 | 18-09-2002 |
| | | JP 2003518351 T | 03-06-2003 |
| | | WO 0146786 A1 | 28-06-2001 |
| WO 0144908 A | 21-06-2001 | AU 2259901 A | 25-06-2001 |
| | | AU 2260001 A | 25-06-2001 |
| | | AU 4717501 A | 03-07-2001 |
| | | EP 1242854 A1 | 25-09-2002 |
| | | EP 1242855 A1 | 25-09-2002 |
| | | EP 1242858 A2 | 25-09-2002 |
| | | JP 2003517767 T | 27-05-2003 |
| | | JP 2003518282 T | 03-06-2003 |
| | | WO 0144907 A1 | 21-06-2001 |
| | | WO 0144908 A1 | 21-06-2001 |
| | | WO 0146783 A2 | 28-06-2001 |
| US 6385596 B1 | 07-05-2002 | NONE | |

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 トリブル・ガイ・エル.
アメリカ合衆国 カリフォルニア州９４０１０ ヒルズバーロウ, ダウニー・ウェイ, ２５
(72)発明者 ヘラー・デイブ
アメリカ合衆国 カリフォルニア州９５１２５ サン・ホセ, ジョナサン・アベニュー, ２０１６
(72)発明者 ロビン・ジェフリィ・エル.
アメリカ合衆国 カリフォルニア州９４０２４ ロス・アルトス, ベンベニュー・アベニュー, ７０５

Ｆターム(参考) 5J104 AA12 PA07

【要約の続き】
ンピューティングデバイスである。