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

特許第4786222号
(P4786222)

(45)発行日　平成23年10月5日(2011.10.5)　(24)登録日　平成23年7月22日(2011.7.22)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	520A
G06Q 50/00	(2006.01)	G06F	12/14	520F
G06Q 30/00	(2006.01)	G06F	12/14	560B
G10K 15/04	(2006.01)	G06F	17/60	142
		G06F	17/60	302E

請求項の数 6　(全 15 頁)　最終頁に続く

(21)出願番号　特願2005-138957 (P2005-138957)
(22)出願日　平成17年5月11日 (2005.5.11)
(65)公開番号　特開2006-318134 (P2006-318134A)
(43)公開日　平成18年11月24日 (2006.11.24)
審査請求日　平成20年3月6日 (2008.3.6)

(73)特許権者　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　上野　英俊
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　各務　健太郎
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　関野　公彦
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内

最終頁に続く

(54)【発明の名称】ディジタル権利管理システム、コンテンツサーバおよび携帯端末

(57)【特許請求の範囲】

【請求項１】

コンテンツ作成者により作成されたコンテンツを保存するコンテンツサーバと、

前記コンテンツサーバから任意のコンテンツを取得し利用する携帯端末と、

前記携帯端末により利用されたコンテンツをアップロードおよびダウンロード可能に保存するデータ保存サーバと

を含むディジタル権利管理システムであって、

前記コンテンツサーバは、前記コンテンツに関し、前記データ保存サーバへの前記コンテンツのバックアップ保存の可否を含む権利情報を作成し、前記携帯端末からのコンテンツ取得要求に応じて、前記コンテンツと前記権利情報とを配信し、

前記権利情報には、前記コンテンツ、前記権利情報、及び前記コンテンツの利用に関する状態情報の各々について個別にバックアップ保存の可否が設定されており、

前記携帯端末は、前記コンテンツを利用した場合に、前記バックアップ保存の可否情報に基づいて、前記コンテンツと前記権利情報と前記コンテンツの利用に関する状態情報のうちバックアップ保存が許可されている項目を含むバックアップデータを作成し、前記バックアップデータを前記データ保存サーバに送信し、

前記データ保存サーバで、前記バックアップデータを保存する

ことを特徴とするディジタル権利管理システム。

【請求項２】

前記権利情報は、前記コンテンツの使用制限に関する記述を含み、前記コンテンツの利

用に関する状態情報は、前記使用制限を前提とする現在の権利の状態を示す情報を含むことを特徴とする請求項１に記載のディジタル権利管理システム。
【請求項３】
前記携帯端末は、前記コンテンツを利用した結果生成される付属情報を前記バックアップデータに含めることを特徴とする請求項１に記載のディジタル権利管理システム。
【請求項４】
コンテンツ作成者により作成されたコンテンツを保存するコンテンツ保存部と、
前記コンテンツのバックアップ保存が前記コンテンツ作成者により許可されているか否かを判断するバックアップ保存可否判断部と、
前記コンテンツに関し、当該コンテンツのバックアップ保存可否の判断結果を含む権利情報を作成し、前記権利情報に、前記コンテンツ、前記権利情報、及び前記コンテンツの利用に関する状態情報の各々について個別にバックアップ保存の可否を設定する権利情報作成部と、
任意の端末装置からのコンテンツ取得要求に応じて、前記コンテンツと、前記権利情報とを配信するコンテンツ／権利情報配信部と
を備えるコンテンツサーバ。
【請求項５】
前記権利情報は、前記バックアップ保存が可能であるとの判断結果とともに、前記コンテンツをバックアップ保存するためのデータ保存サーバのアドレスを含むことを特徴とする請求項４に記載のコンテンツサーバ。
【請求項６】
コンテンツサーバにおいて、コンテンツ作成者により作成されたコンテンツを受付け、
前記コンテンツサーバにおいて、前記コンテンツのバックアップ保存が前記コンテンツ作成者により許可されているか否かを判断し、
前記コンテンツサーバにおいて、前記コンテンツに関し、前記コンテンツのバックアップ保存可否の判断結果を含む権利情報を作成し、前記権利情報に、前記コンテンツ、前記権利情報、及び前記コンテンツの利用に関する状態情報の各々について個別にバックアップ保存の可否を設定し、
前記コンテンツサーバにおいて、任意の端末装置からのコンテンツ取得要求に応じて、前記コンテンツと前記権利情報を配信するとともに、前記コンテンツおよび権利情報をネットワーク上で管理し、
前記携帯端末において、前記コンテンツサーバから前記コンテンツおよび前記コンテンツに関する権利情報を取得し、
前記携帯端末において前記コンテンツが利用されたときに、前記権利情報に基づいて、前記コンテンツ、前記権利情報、及び前記コンテンツの利用に関する状態情報のバックアップ保存の可否を判断し、
前記バックアップ保存が可能である場合に、前記携帯端末において、前記コンテンツと前記コンテンツの使用状況と前記権利情報のうちバックアップ保存が許可されている項目を含むバックアップデータを生成して、ネットワーク上のデータ保存サーバに保存することを特徴とするディジタル権利管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ディジタルコンテンツの著作権を管理する方法に関し、特に、移動通信網において、著作権およびこれに基づく権利情報の管理を行うディジタル権利管理システムと、システムで用いられるコンテンツサーバおよび携帯端末に関する。
【背景技術】
【０００２】
ディジタルコンテンツは、工業製品や食品などの有体物と異なり、同品質のものを複製することが容易であるという特徴を持つ。著作権法では、作成者の許諾を得ない不正なコ

ンテンツの複製を禁止しているが、実際には不法に複製され、使用される場合が多い。コンテンツの著作権を適切に保護することは、コンテンツ作成者にとって極めて重要であり、その要求も高い。

【０００３】

このような背景から、近年になってディジタルコンテンツの著作権管理技術であるＤＲＭ（Digital Rights Management）が注目を集めている。当初は、音楽ＣＤやＤＶＤ映画、ディジタル放送などに適用するＤＲＭ技術が注目されていたが、携帯端末を対象に提供されるコンテンツの多様化、高額化につれて、携帯端末に適用するＤＲＭ技術にも注目が集まっている。

【０００４】

これに応じて、モバイルアプリケーション要素技術の標準化団体であるＯＭＡ（Open Mobile Alliance）により、携帯端末向けのＤＲＭ技術であるＯＭＡ　ＤＲＭの標準化が行なわれている。ＯＭＡ　ＤＲＭでは、携帯端末に配信される任意のコンテンツを保護対象としており、著作権法で保護されるコンテンツの複製を制限可能とするだけではなく、コンテンツ使用に関する制限（使用回数、使用期限など）を指示することも可能である。また、ＯＭＡ　ＤＲＭはディジタルコンテンツと権利情報を分離することにより、ディジタルコンテンツの流通を促進する超流通機能を備えるなど、コンテンツプロバイダの要求に応える様々な機能を備えている。

【０００５】

ＯＭＡ　ＤＲＭには、低額コンテンツを主な対象とする簡易的なＯＭＡ　ＤＲＭバージョン１．０（DRMv1.0）（例えば、非特許文献１参照）と、高額コンテンツを主な対象とする高度なＯＭＡ　ＤＲＭバージョン２．０（DRMv2.0）（例えば、非特許文献２参照）の２種類が存在する。

【０００６】

図１は、ＯＭＡ　ＤＲＭが実現する超流通機能を説明するための図である。ＯＭＡ　ＤＲＭでは、コンテンツ１００２と権利情報１００３を分離して配信することにより、超流通を実現する。超流通とは、コンテンツ１００２の複製や再配布自体は自由とする代わりに、権利情報１００３に対して価値を与える方式である。コンテンツ１００２は暗号化を行い、権利情報１００３に含まれるコンテンツ鍵を取得しない限りコンテンツ１００２を利用できない仕組みである。超流通により、ユーザは友人に対して暗号化コンテンツ１００２をメールで転送し、友人が権利情報１００３を別途購入するといった新たなコンテンツの利用法の実現が可能である。

【０００７】

暗号化コンテンツ１００２は、ＤＲＭコンテンツフォーマット（ＤＣＦ:DRM Content Format）に従ってバイナリ化される。ＤＲＭコンテンツフォーマットには、権利情報１００３を保持する権利発行者（ＲＩ：Right Issuer）のＵＲＬが含まれており、モバイル端末１００１は権利発行者のＵＲＬにアクセスすることで、コンテンツ鍵を含む権利情報１００３の配信を要求する。以上の動作により、ディジタルコンテンツの普及を実現すると同時に、コンテンツの暗号化によってディジタル著作権の保護を実現することができる。

【０００８】

また、別の技術として、携帯電話端末用のデータ管理サービスシステムが公知となっている（例えば、特許文献１参照）。このデータ管理サービスシステムは、アプリケーション等のコンテンツの著作権を保護するとともに、携帯端末の変更により従来使用していた情報データが使用できなくなるという不具合を解消するために、携帯端末で使用するデータ情報をネットワーク上のデータ管理サーバに保存する。このとき、著作者識別情報を付与されたデータ情報については、著作権保護領域に格納され、他の保存領域への移動が制限される。また、著作権保護領域に格納されたデータ情報のダウンロードは、このデータ情報に対応付けられた利用者の携帯端末に対してのみ行えるようにする。このように、データ情報を管理サーバにアップロードしておき、必要なときにダウンロードして使用可能とすることで、携帯端末の機種変更時にも継続してコンテンツの利用が可能になる。

【０００９】
さらに別の技術として、携帯端末がネットワークからダウンロードしたコンテンツを利用した後、しばらく使用しない場合に、ネットワーク上のライセンス管理サーバに欄センスを預け、ライセンス管理サーバは、ライセンス引換券を携帯端末に対して発行することにより、携帯端末がコンテンツを再使用する場合に、ライセンス管理サーバからライセンスを再取得するシステムが提案されている（たとえば、特許文献２参照）。
【非特許文献１】Open Mobile Alliance, “OMA Digital Rights Management Enabler Release,”, Approved Version 1.0, OMA-DRM-V1_0-20040615-A, ２００４年６月、www.openmobilealliance.org.
【非特許文献２】Open Mobile Alliance, “OMA Digital Rights Management Enabler Release,”, Approved Version 2.0, OMA-DRM-V2_0-20040715-C, ２００４年７月、www.openmobilealliance.org.
【特許文献１】特開２００４－２００８４５号公報
【特許文献２】特開２００３－１７９５９０号公報
【発明の開示】
【発明が解決しようとする課題】
【００１０】
ＯＭＡ　ＤＲＭのディジタル著作権管理方式では、コンテンツについては転送等の自由な流通を認めるが、権利情報については携帯端末から転送するなどの自由な流通を認めない点に特徴がある。したがって、一度携帯端末にコンテンツ及び権利情報を取得した後、携帯端末の紛失や故障が生じた場合は、再度コンテンツと権利情報をコンテンツプロバイダから取得することが必要になり、場合によっては、権利取得のためにコンテンツに対する代金を再度支払う必要があった。
【００１１】
携帯端末の機種を変更する場合は、店頭などでメモリ転送装置や情報処理装置等を用い、メモリ転送装置を介して携帯電話端末を情報処理装置に接続して、携帯端末のメモリに記憶された電話番号等の個人情報データを電子的に吸い上げる（読み込む）処理や、逆にメモリにデータを書き込む処理を行ない、従前の携帯端末の個人情報データを新しい形態端末に書き込んでいた。このとき、著作権が存在するコンテンツを複製する場合には、別途コンテンツ作成者からの許諾が必要であるが、この許諾を得ることが容易ではなかったために、著作権が存在する権利情報に関しては、新しい携帯端末に書き込む処理はされていなかった。したがって、ユーザが購入済みのコンテンツを新しい携帯端末で継続的に利用することができないという問題があった。
【００１２】
また、上記特許文献１に記載のデータ管理サービスシステムでは、著作者が作成したコンテンツをユーザの判断でサーバにアップロードするか否かを決定できたため、著作権が存在するコンテンツをサーバへアップロードする場合、コンテンツの著作者からサーバへのアップロードのための複製権の許諾を別途得る必要がある。悪意のユーザの場合、コンテンツの著作者から複製の許諾を得ないコンテンツに関してもサーバにアップロードする、すなわち複製することが可能であり、著作者の複製権が容易に侵害される恐れがあるという問題があった。
【００１３】
さらに、このデータ管理サービスシステムでは、コンテンツの権利情報に着目した場合の問題点を解決していなかった。コンテンツの権利情報にはコンテンツの使用制限（使用回数、使用期限など）を指定することが可能であるが、これらコンテンツの使用制限は、コンテンツを使用する毎に状態が変化する状態情報である。しかし、従来のデータ管理サービスシステムでは、単にデータ情報をアップロード、ダウンロードすることについてのみ解決しており、コンテンツが利用されることにより状態情報が変化した場合の処理については、何ら考慮されていない。このため、携帯端末を紛失した場合に新しい携帯端末においてコンテンツの使用に関する使用制限を引き継ぐことができないという問題がある。

例えば、コンテンツの使用回数は５回までと権利情報に指定されており、携帯端末で３回使用した場合、ユーザは残り２回の使用が可能であるが、携帯端末であと２回使用可能であることを示す状態情報の処理については何ら示されておらず、携帯端末を変更した場合に状態情報を引き継ぐことができない。

【００１４】

特許文献２に記載のライセンス引換券を発行する方式では、携帯端末を紛失した場合、ライセンス引換券も紛失することになり、ライセンス管理サーバに預けたライセンスを再取得することができない。ライセンス引換券の再発行の手続きや、新しい携帯端末への引継ぎ処理については何ら開示されていないので、結局はライセンスを再取得しなければならない。

【００１５】

本発明は、上述した問題点に鑑みてなされたものであり、紛失や機種変更などにより携帯端末を変更する際に、それまで使用していたディジタルコンテンツと権利情報、コンテンツの使用制限に関する状態情報、その他関連する情報を、新たな携帯端末で継続して利用できるようにするディジタル権利管理システムと、このシステムで用いられるコンテンツサーバおよび携帯端末の提供を課題とする。

【課題を解決するための手段】

【００１６】

上記課題を達成するために、各コンテンツのバックアップ保存の可否に基づいて権利情報を作成し、携帯端末でコンテンツを利用するたびに、コンテンツの利用状態と権利情報とを含むバックアップデータを作成して、ネットワーク上のサーバで保存、管理する。

【００１７】

本発明の第１の側面では、コンテンツ作成者により作成されたコンテンツを保存するコンテンツサーバと、前記コンテンツサーバから任意のコンテンツを取得し利用する携帯端末と、前記携帯端末により利用されたコンテンツをアップロードおよびダウンロード可能に保存するデータ保存サーバとを含むディジタル権利管理システムを提供する。ディジタル権利管理システムにおいて、コンテンツサーバは、前記コンテンツに関し、データ保存サーバへのバックアップ保存の可否を含む権利情報を作成し、前記携帯端末からのコンテンツ取得要求に応じて、前記コンテンツと前記権利情報とを配信し、携帯端末は、前記コンテンツを利用した場合に、前記バックアップ保存の可否情報に基づいて作成したバックアップデータを、前記データ保存サーバに送信し、データ保存サーバにて、前記バックアップデータを保存する。

【００１８】

本発明の第２の側面では、携帯端末は、

（ａ）ネットワーク上のコンテンツサーバからコンテンツとその権利情報を取得して、前記コンテンツの使用状況と前記権利情報を管理し、前記権利情報に基づいて、前記コンテンツのバックアップ保存の可否を判断するディジタル権利管理手段と、

（ｂ）前記コンテンツが利用された場合に、当該コンテンツのバックアップ保存が可能であると判断されたならば、前記コンテンツの使用状況および権利情報を含むバックアップデータを生成して、ネットワーク上のデータ保存サーバに保存するバックアップ手段と、

を備える。

【００１９】

好ましくは、前記ディジタル権利管理手段は、前記バックアップデータの取得指示が入力された場合に、前記データ保存サーバから前記バックアップデータを取得する。

【００２０】

本発明の第３の側面では、コンテンツサーバは、

（ａ）コンテンツ作成者が作成したコンテンツと保存するコンテンツ保存部と、

前記コンテンツのバックアップ保存が前記コンテンツ作成者により許可されているか否かを判断するバックアップ保存可否判断部と、

（ｂ）前記コンテンツに関し、前記バックアップ保存可否の判断結果を含む権利情報を作

成する権利情報作成部と、
（ｃ）任意の端末装置からのコンテンツ取得要求に応じて、前記コンテンツと、前記権利情報とを配信するコンテンツ／権利情報配信部と
を備える。
【００２１】
好ましくは、前記権利情報は、バックアップ保存が可能であるとの判断結果とともに、前記コンテンツをバックアップ保存するデータ保存サーバのアドレスを含む。
【発明の効果】
【００２２】
携帯端末を変更した場合でも、それまで使用していたディジタルコンテンツ、権利情報、コンテンツの使用制限に関する状態情報、その他関連する情報を継続して利用することが可能になる。
【発明を実施するための最良の形態】
【００２３】
以下、本発明の実施の形態を、図面を参照して説明する。以下の説明で参照する各図において、同一の構成要素は同一の符号によって示されている。
（システム全体の構成）
図２は、本発明の実施形態に係るディジタル権利管理システム１の構成図である。ディジタル権利管理システム１は、ネットワーク１０に接続され互いに通信することが可能な携帯端末２１、２２、コンテンツサーバ３０、およびデータ保存サーバ４０を含む。携帯端末２１、２２、コンテンツサーバ３０、データ保存サーバ４０の各々は、ＣＰＵ、記憶装置、入出力装置等のハードウェア資源と、記憶装置に記憶されたソフトウェア資源とを備えている。
【００２４】
コンテンツサーバ３０は、コンテンツ作成者が作成した画像、動画像、音楽、プログラム等の任意のコンテンツと、そのコンテンツに対する権利情報を保持するサーバである。コンテンツサーバは、ＯＭＡ　ＤＲＭのように、コンテンツを保持するサーバと権利情報を保持するサーバの機能に応じて２つに分割してもよいし、一体としてもよい。本実施形態では、コンテンツサーバ３０において、コンテンツの保持と権利情報の保持を一体的に行なうものとする。
【００２５】
コンテンツサーバ３０は、携帯端末２１、２２からの要求に応じて、コンテンツを配信する際に、そのコンテンツが著作者によりバックアップ保存のための複製が許可されているか否かを示す情報を権利情報に含めて送信する。
【００２６】
携帯端末２１、２２は、バックアップ保存が許可されたコンテンツについて、その使用状態を示す状態情報とともに、データ保存サーバ４０に保存する。
【００２７】
データ保存サーバ４０は、携帯端末２１、２２から送信されたデータを保存し、保存したデータを携帯端末２１、２２に提供する。すなわち、携帯端末２１、２２に保存されるデータのアップロード及びダウンロードを行なうサーバである。
【００２８】
図３は、図２のディジタル権利管理システム１の動作を示すシーケンス図である。ユーザが携帯端末Ａから携帯端末Ｂへ切り換える場合を考える。
【００２９】
携帯端末Ａはコンテンツサーバ３０に対して任意のコンテンツに対するコンテンツ取得要求を送信する（Ｓ１０１）。コンテンツサーバ３０は、コンテンツ作成者の希望するコンテンツの使用方法の制限や、コンテンツの使用回数、使用期限などを含む権利情報を作成し、このコンテンツのデータ保存サーバ４０へのバックアップ保存の可否を示す情報（バックアップ保存可否フラグ）を追加する（Ｓ１０２）。そして、作成した権利情報を、

要求されたコンテンツとともに携帯端末Ａに配信する（Ｓ１０３）。

【００３０】

携帯端末Ａは、取得したコンテンツと権利情報を保存する（Ｓ１０４）。その後、このコンテンツの利用のたびに、このコンテンツの残り使用回数や残り使用期限などの状態情報を更新し（Ｓ１０５）、バックアップ保存用のデータを作成して（Ｓ１０６）、データ保存サーバ４０に対してバックアップデータの保存要求を送信する（Ｓ１０７）。データ保存サーバ４０は、バックアップデータを保存する（Ｓ１０８）。

【００３１】

携帯端末Ａの紛失または機種の変更により、ユーザが新たに携帯端末Ｂを取得する場合（Ｓ１０９、Ｓ１１０）、新たな携帯端末Ｂは、データ保存サーバ４０に対してバックアップデータの取得要求を送信する（Ｓ１１１）。データ保存サーバ４０は、携帯端末Ｂが携帯端末Ａと同一のユーザのものであることを認証し（Ｓ１１２）、バックアップデータを携帯端末Ｂに送信する（Ｓ１１３）。

【００３２】

携帯端末Ｂは、バックアップデータを取得し、コンテンツを保存するとともに、権利情報、状態情報を取り出して保存する（Ｓ１１４）。

【００３３】

このように、コンテンツサーバ３０は、各コンテンツについて、あらかじめ著作権者の決定に基づくデータ保存サーバ４０へのバックアップ保存の可否を示す情報を作成し、権利情報に追加する。各携帯端末２１、２２は、バックアップ保存可能なコンテンツについては、コンテンツの利用の都度、現在の権利状態を示す状態情報を含むバックアップデータを作成して、データ保存サーバ４０に保存する。これにより、携帯端末の紛失、機種変更などにより端末を切り換える場合でも、適正に取得したコンテンツとその権利情報をそのまま引き継ぐことができる。

【００３４】

図４は、携帯端末２１（または２２）の構成例を示すブロック図である。携帯端末２１、２２としては、携帯電話やＰＤＡ（Personal Digital Assistance）の他、持ち運び可能のノートパソコンも含む。

【００３５】

携帯端末２１は、ＤＭＡエージェント２０１、データ保存部２０２、バックアップエージェント２０３、コンテンツアプリケーション２０４を有する。

【００３６】

ＤＭＡエージェント２０１は、ＯＭＡ　ＤＲＭで定義されるＤＲＭエージェントとして動作する。具体的には、コンテンツサーバ３０からコンテンツと、このコンテンツに対する権利情報を取得し、権利情報に記述された内容に基づいて、コンテンツアプリケーション２０４によるコンテンツの利用状況を管理する。

【００３７】

コンテンツアプリケーション２０４は、コンテンツをユーザに提供する際に利用するアプリケーションであり、たとえば音楽プレイヤー、映像ビューワ、ゲームアプリケーション等である。ＤＲＭエージェント２０１は、コンテンツアプリケーション２０４を通じてコンテンツをユーザに提供する。

【００３８】

データ保存部２０２は、ＤＲＭエージェント２０１が取得したコンテンツを保存する。データ保存部２０２に保存されるデータは、ＤＲＭエージェント２０１以外からアクセスできないように実装される。

【００３９】

バックアップエージェント２０３は、コンテンツアプリケーション２０４によりコンテンツが利用され、ＤＲＭエージェント２０１からバックアップすべき情報を受け取ると、データ保存サーバ４０へのバックアップ保存が許可されているデータか否かを判断する。保存が許可されているデータに関してバックアップデータを作成し、データ保存サーバ４

０へ送信する。
【００４０】
このような携帯端末２１の詳細な動作については、後述する。
【００４１】
図５は、コンテンツサーバ３０の概略構成図である。コンテンツサーバ３０は、コンテンツ／権利情報配信部３０１と、コンテンツ保存部３０２と、権利情報保存部３０３と、バックアップ保存可否判断部３０４と、権利情報作成部３０５を有する。コンテンツ保存部３０２はコンテンツ作成者が作成したコンテンツを保存する。権利情報作成部３０５は、各コンテンツについてその権利情報を作成する。バックアップ保存可否判断部３０４は、各コンテンツについて、データ保存サーバ４０へのバックアップ保存がコンテンツ作成者によって許可されているか否かを判断し、バックアップ保存可否情報を権利情報作成部３０５に渡す。権利情報作成部３０５は、バックアップ保存可否情報を権利情報に追加する。権利情報保存部３０３は、作成された権利情報をコンテンツと関連付けて保存する。コンテンツ／権利情報配信部３０１は、ユーザの携帯端末２１、２２からの要求に応じて、要求されたコンテンツとその権利情報を配信する。
【００４２】
図６は、権利情報の一例として、ＯＭＡ　ＤＲＭの権利情報を示す。ＯＭＡ　ＤＲＭでは、ＯＤＲＬ（Open Digital Rights Language）に基づいてＸＭＬ（Extensible Markup Language）で権利情報を記述する。権利情報には、コンテンツ作成者の希望するコンテンツの使用方法の制限や、コンテンツの使用回数、使用期限などを記述することができる。
【００４３】
図７は、バックアップ保存可否情報を含む権利情報７０の構成例を示す。図７の例では、権利情報７０は使用許可情報７１と、使用制限情報７２と、バックアップ保存の可否を示す権利保存可否情報７３を含む。
【００４４】
使用許可情報７１は、再生、表示、実行、ハードコピーなど、コンテンツの使用方法に関する指定を示す情報である。使用制限情報７２は、コンテンツを使用する際の使用回数、使用開始可能時刻、使用終了時刻、使用開始からの有効期限などの情報を含む。
【００４５】
権利保存可否情報７３は、この権利情報が適用されるコンテンツをデータ保存サーバ４０に保存可能か否かを指定する権利保存可否識別子７４と、データ保存サーバ４０のアドレス情報７５を含む。
【００４６】
権利保存可否識別子７４は、コンテンツ、コンテンツの権利情報、権利情報の状態情報、附属情報等の各項目に分かれており、それぞれについて、データ保存サーバ４０に保存可能か否かの設定ができるようになっている。たとえば、それぞれの項目についてフラグを立てることによってバックアップ保存の可否を設定できる。付属情報については、さらにスクラッチパッドのようなメモリ情報等のサブ項目に分かれており、それぞれについてデータ保存サーバ４０への保存の可否が設定できる。ここでコンテンツとは、携帯端末２１，２２がコンテンツサーバ３０から取得するコンテンツそのものであり、権利情報とは、コンテンツに関する権利情報である。権利情報の状態情報と付属情報の詳細は後述する。
【００４７】
データ保存サーバアドレス７５には、携帯端末２１、２２が利用可能なデータ保存サーバ４０のアドレスが記述されており、携帯端末２１、２２は、データ保存サーバ４０に対してデータのアップロード、ダウンロードが可能である。
【００４８】
コンテンツサーバ３０は、例えばコンテンツの登録時に、著作権が存在するコンテンツに関して、バックアップを目的とするデータの複製を許諾するか否かをコンテンツ作成者に対して確認する。バックアップを目的とする複製、すなわちデータ保存サーバ４０への

保存が許諾されたならば、権利情報７０の権利保存可否識別子７４のコンテンツの項目を可（ＹＥＳ）に設定する。逆に、コンテンツ作成者がこのコンテンツのデータ保存サーバ４０への保存を望まない場合は、権利保存可否識別子７１のコンテンツの項目を不可（ＮＯ）に設定する。コンテンツ作成者は、データ保存サーバのアドレスを指定することによって、データの保存を許可するサーバを指定することもできる。

【００４９】

図８は、携帯端末２１（または２２）がコンテンツサーバ３０からコンテンツをダウンロードし、利用する場合の状態変更動作を示すフローチャートである。上述したように、携帯端末２１のＤＲＭエージェント２０１は、ユーザから任意のコンテンツを取得する指示を受け取ると、コンテンツサーバ３０からコンテンツと権利情報を取得し、取得したコンテンツと権利情報を、データ保存部２０２に保存し、ＤＲＭエージェント２０１以外からのアクセスが不可能になるように管理している。

【００５０】

ユーザからコンテンツの利用を指示されると（Ｓ１１でＹＥＳ）、ＤＲＭエージェント２０１はデータ保存部２０２からコンテンツ及び権利情報を取り出し、このコンテンツが利用可能となるようにコンテンツの復号に必要な処理を行ない、復号されたコンテンツをコンテンツアプリケーション２０４に渡す。

【００５１】

コンテンツアプリケーション２０４を介してコンテンツが利用されると、ＤＲＭエージェント２０１は、コンテンツの使用状況を監視するために、状態情報を更新する（Ｓ１２）。状態情報とは、コンテンツ使用の途中経過を示す情報であり、権利情報７０で指定されたコンテンツの使用制限を指定されたとおりに扱うために必要な情報である。状態情報には、このコンテンツの残りの利用可能回数を示す残存回数や、コンテンツの有効期限が含まれる。残存回数は、権利情報の中に当初記載されていた利用回数から、実際にコンテンツを利用した分を引いた残りの数値である。有効期限には、権利情報の中に含まれる終了時刻、使用開始時からの有効期限、絶対的な有効期限の中から、コンテンツが利用できる期限を日時で標記したものが含まれる。このような状態情報は、コンテンツが使用される毎に更新される。

【００５２】

ＤＲＭエージェント２０１は、状態情報が更新されると、コンテンツ、コンテンツの権利情報、権利情報の状態情報、付属情報をデータ保存サーバ４０に送信可能か否かの判断を行なう（Ｓ１３）。具体的には、ＤＲＭエージェント２０１は、権利保存可否識別子７４の記述を確認し、コンテンツ、コンテンツの権利情報、権利情報の状態情報、付属情報のうちのどのデータに関して、データ保存サーバ４０へのバックアップが許可されているかを確認する。例えば、権利保存可否識別子のコンテンツとコンテンツ権利情報の項目が「可（ＹＥＳ）」になっていれば、コンテンツの作成者がコンテンツと権利情報の双方についてバックアップを目的とする複製を許諾していると判断することができる。

【００５３】

権利保存可否識別子７４でデータ保存サーバ４０へのバックアップが許可されているものがある判断すると（Ｓ１３でＹＥＳ）、ＤＲＭエージェント２０１は、バックアップエージェント２０３にバックアップすべき情報を渡す（Ｓ１４）。

【００５４】

図９は、携帯端末２１（または２２）のバックアップエージェント２０３の動作を示すフローチャートである。バックアップエージェント２０３は、ＤＲＭエージェント２０１からバックアップする情報を受け取ると（Ｓ２１）、バックアップデータを作成する（Ｓ２２）。

【００５５】

図１０は、バックアップデータ８０の構成例である。図１０の例では、バックアップデータ８０は、バックアップデータを作成した端末を識別する携帯端末識別子を含む携帯端末情報８１と、該当するコンテンツを一意に識別するコンテンツＩＤとコンテンツのメデ

ィアタイプを記述するコンテンツタイプ等を含むコンテンツ基本フィールド８２と、コンテンツそのものを含むコンテンツフィールド８３と、コンテンツの権利情報を含む権利情報フィールド８４と、ＤＲＭエージェント２０１が管理するコンテンツの利用に関する状態情報を含む状態情報フィールド８５と、その他付随する情報を含む付属フィールド８６から構成されているが、データ保存サーバ４０に送信しない情報についてはバックアップデータ８０に含めなくてもよい。

【００５６】
付属フィールド８６には、当該コンテンツに関する付随的な情報を含むことが可能である。例えば、コンテンツが携帯電話におけるＪａｖａ（登録商標）アプリケーションである場合は、スクラッチパッド等が考えられる。スクラッチパッドは、ユーザがゲームを中断したい場合に、ゲームの途中経過を記録しておくメモリ領域であり、後にゲームを再開する場合は、スクラッチパッドに記述された情報を取り出すことで、ゲームを再開できる。

【００５７】
図９に戻って、バックアップエージェント２０３はバックアップデータを作成すると、データ保存サーバ４０に対して送信する（Ｓ２３）。バックアップデータを構成するフィールドのすべてを毎回作成し、データ保存サーバ４０に送信する必要はない。例えば、付属フィールド８６に含まれるスクラッチパッドについては、そのサイズが大きくなるため、毎回送信するとネットワーク資源の浪費になる。したがって、バックアップデータを生成する際に、データ保存サーバ４０に送信する必要のないデータについては、バックアップデータに含めないようにするのが望ましい。

【００５８】
データ保存サーバ４０は、携帯端末２１からバックアップデータを受信すると、送信元の携帯端末２１を認証する。認証方法としては、パスワード、携帯端末２１の識別子である電話番号、ＩＭＳＩ（International Mobile Subscriber Identity）、電子証明書などを利用する例が考えられる。データ保存サーバ４０は、携帯端末識別子ごとにデータを保存するデータ保存領域を保持しており、携帯端末２１に対応するデータ保存領域にバックアップデータを保存する。このデータ保存領域に対しては、対応する携帯端末以外からのアクセスは不可能とされる。

【００５９】
その後、ユーザが携帯端末２１から携帯端末２２に変更すると、データ保存サーバ４０からバックアップデータを取得する。

【００６０】
図１１は、新たな携帯端末２２がバックアップデータを取得するときの動作を示すフローチャートである。携帯端末２２のＤＲＭエージェント２０１は、ユーザから任意のコンテンツを取得する指示を受けると、コンテンツサーバ３０からコンテンツおよび権利情報を取得する（Ｓ３１）。ＤＲＭエージェント２０１は、コンテンツおよび権利情報をデータ保存部２０２に保存し、ＤＲＭエージェント２０１以外からのアクセスが不可能となるように管理する。

【００６１】
次に、ユーザからバックアップデータの取得指示を受けると（Ｓ３２）、データ保存サーバ４０に対して、先の携帯端末２１の識別子情報とともに、バックアップデータの取得要求を送信する（Ｓ３３）。

【００６２】
データ保存サーバ４０は、携帯端末２２からバックアップデータの取得要求を受け取ると、携帯端末２２を認証する。さらに、携帯端末２１の識別子に対応するデータ保存領域にバックアップデータが存在するか否かを判断する。この際、バックアップデータは複数存在することもある。対応するデータ保存領域にバックアップデータがあれば、データ保存サーバ４０は、そのバックアップデータを携帯端末２２に送信する

データ保存サーバ４０からバックアップデータを受信したＤＲＭエージェント２０１は、バックアップデータに含まれる情報を取り出す。コンテンツやコンテンツの権利情報はデータ保存部２０２に保存し、状態情報に関しては、ＤＲＭエージェント２０１が管理する状態情報として管理し、付属フィールドのメモリ情報に関しては、携帯端末２２のメモリデータとして設定する（Ｓ３４）。

【００６３】

以上の動作により、ユーザが携帯端末の機種変更を行った場合、もしくは携帯端末を紛失した後に別の携帯端末を購入した場合においても、それまで使用していたディジタルコンテンツ、権利情報、コンテンツの利用状況を示す状態情報、その他関連する情報を継続して新たな携帯端末で利用することが可能になる。

【００６４】

最後に、セキュリティに関する考察を述べる。

【００６５】

携帯端末２１，２２とデータ保存サーバ４０でやり取りされるバックアップデータについては、第三者に盗聴されないようにする必要がある。従って、携帯端末２１、２２とデータ保存サーバ４０との間の通信には、必要なデータ秘匿処理を施す必要がある。具体的な例として、ＩＰＳｅｃ（IP Security）やＳＳＬ（Secure Socket Layer）が考えられる。

【００６６】

データ保存サーバ４０は、アクセスする携帯端末２１、２２を認証する必要がある。認証方法としては、上述したように、パスワード、携帯端末の識別子である電話番号、ＩＭＳＩ（International Mobile Subscriber Identity）、電子証明書などを利用できる。

【００６７】

データ保存サーバ４０は、必要に応じて、コンテンツサーバ３０と連携し、携帯端末２１、２２がデータ保存サーバ４０を使用する権利があるか否かを確認する構成としてもよい。例えば、コンテンツサーバ３０は、権利情報を発行した携帯端末２１、２２を記録しておく。そして、データ保存サーバ４０は、アクセスのあった携帯端末の識別子をコンテンツサーバ３０に問い合わせ、コンテンツサーバ３０から、当該携帯端末に対して発行した権利情報のコピーを受信することによって、当該携帯端末がデータ保存サーバ４０を利用可能であるか否かを判断することができる。

【図面の簡単な説明】

【００６８】

【図１】ＯＭＡ　ＤＲＭの超流通を説明するための図である。

【図２】本発明の一実施形態に係るディジタル権利管理システムの概略図である。

【図３】図２のディジタル管理システムにおける処理シーケンスを示す図である。

【図４】本発明の一実施形態に係る携帯端末の構成例を示す図である。

【図５】本発明の一実施形態に係るコンテンツサーバの構成例を示す図である。

【図６】コンテンツサーバが発行するＯＭＡ　ＤＲＭ権利情報の記述例である。

【図７】権利情報の構成例を示す図である。

【図８】図４の携帯端末のＤＲＭエージェントにおける状態情報の更新処理のフローチャートである。

【図９】図４の携帯端末のバックアップエージェントにおけるバックアップデータ作成時のフローチャートである。

【図１０】バックアップエージェントが作成するバックアップデータの構成例を示す図である。

【図１１】新たな携帯端末のＤＲＭエージェントによるバックアップデータ取得時のフローチャートである。

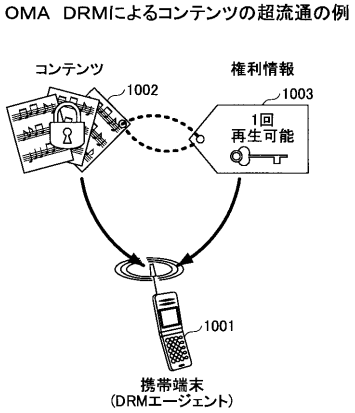
【符号の説明】

【００６９】

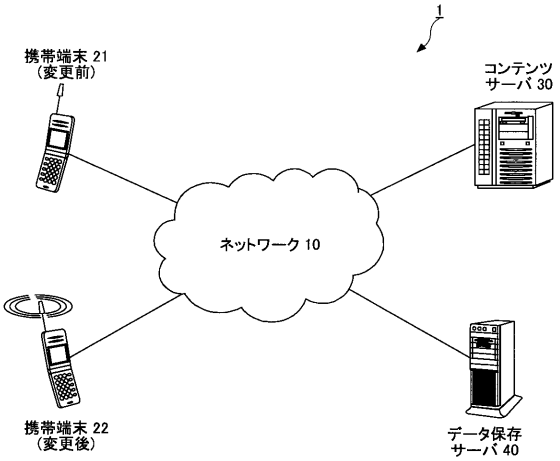
１　ディジタル権利管理システム

２１、２２　携帯端末
３０　コンテンツサーバ
４０　データ保存サーバ
７０　権利情報
７３　権利保存可否情報
８０　バックアップデータ
２０１　ＤＲＭエージェント
２０１　データ保存部
２０３　バックアップエージェント
２０４　コンテンツアプリケーション
３０１　コンテンツ／権利情報配信部
３０２　コンテンツ保存部
３０３　権利情報保存部
３０４　バックアップ保存可否判断部
３０５　権利情報作成部

【図１】

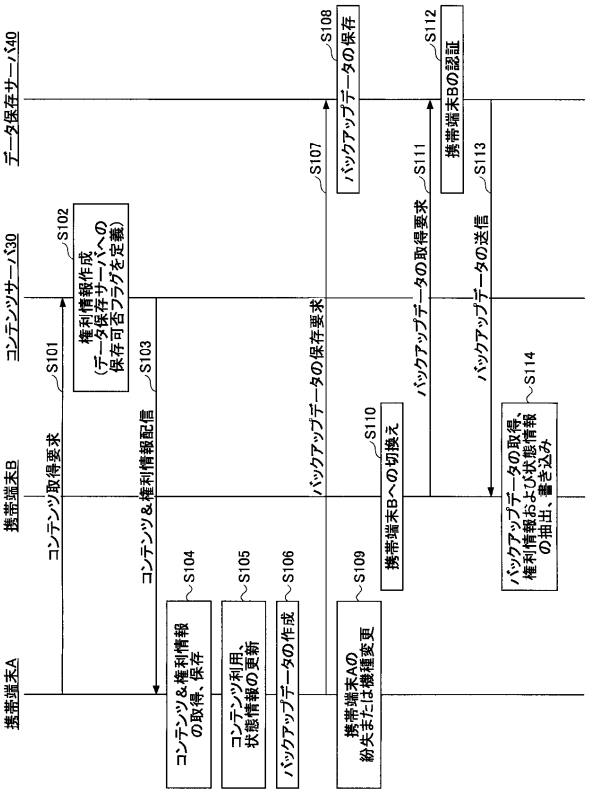


【図２】



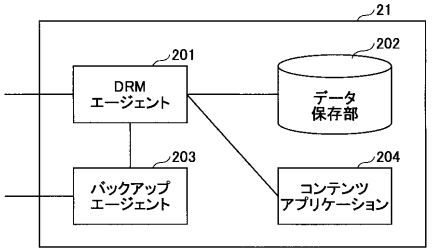
【図３】

ディジタル権利管理システムのシーケンス



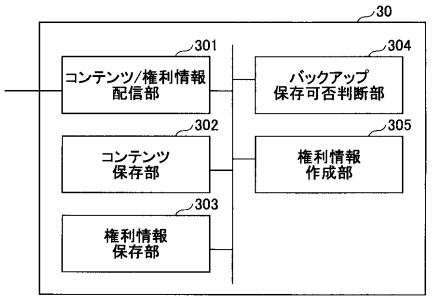
【図４】

携帯端末の構成例



【図５】

コンテンツサーバの構成例



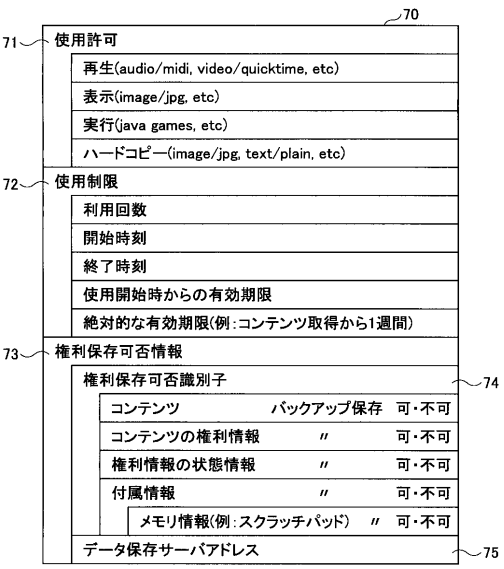
【図６】

権利情報の記述例

```
<o-ex: rights
  xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
  xmlns:o-dd="http://odrl.net/1.1/ODRL-DD">
  <o-ex:context>
    <o-dd:version>1.0</o-dd:version>
  <lo-ex:context>
  <o-ex:agreement>
    <o-ex :asset><o-ex : context>
        <o_dd:uid>cid:4567829547 @foo.bar</o-dd:uid>
    </o-ex:context></o-ex:asset>
    <o-ex:permission>
      <o-dd:display>
                <o-dd:constraint>
          <count><fixed> 1 </fixed></count>
          </ o-dd:constraint>
      </o-dd:display>
    </o-ex:permission>
  </o-ex:agreement>
</o-ex:rights>
```

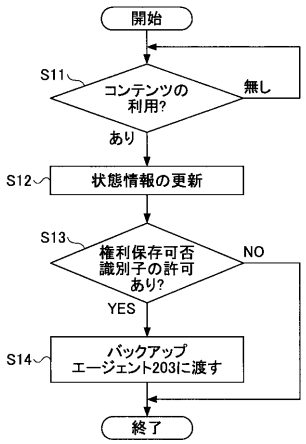
【図７】

権利情報の構成例



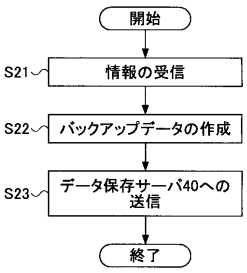
【図８】

DRMエージェントの動作フロー(状態情報の更新)



【図９】

バックアップエージェントの動作フロー



【図１０】

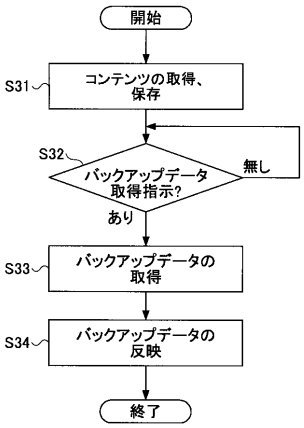
バックアップデータの構成例

80

81	携帯端末情報	
	携帯端末識別子	09012345678
82	コンテンツ基本フィールド	
	コンテンツID	uri:abcde.mode.xyz123
	コンテンツタイプ	audio/midi
83	コンテンツフィールド	
	コンテンツ	(バイナリデータ)
84	コンテンツ権利情報フィールド	
	権利情報	(ODRLのXMLデータ等)
85	状態情報フィールド	
	残存回数	3回
	有効期限	Wed, 9 Mar 2010 03:03:00:00 +0900
86	付属フィールド	
	メモリ情報	(バイナリデータ)

【図１１】

DRMエージェントの動作フロー(バックアップデータの取得)



フロントページの続き

(51)Int.Cl. FI
G10K 15/04 302D

(72)発明者 堀口 賞一
東京都千代田区永田町二丁目１１番１号 株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者 鈴木 偉元
東京都千代田区永田町二丁目１１番１号 株式会社エヌ・ティ・ティ・ドコモ内

審査官 宮司 卓佳

(56)参考文献 特開２００３－２８８２７７（ＪＰ，Ａ）
特開２００３－２９６４８４（ＪＰ，Ａ）
国際公開第０３／０８３７４６（WO，Ａ１）
特開２００３－０７６６５６（ＪＰ，Ａ）
特開２００４－１２６９０８（ＪＰ，Ａ）
特開２００４－０４６８０９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２４
Ｇ０６Ｑ ３０／００
Ｇ０６Ｑ ５０／００
Ｇ１０Ｋ １５／０４