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

特許第4496462号
(P4496462)

(45)発行日　平成22年7月7日(2010.7.7)　(24)登録日　平成22年4月23日(2010.4.23)

(51)Int.Cl.　F I
G06F 17/30 (2006.01)　G06F 17/30 １２０Ａ
G06F 21/24 (2006.01)　G06F 17/30 ２２０Ｃ
G06F 12/14 ５２０Ｐ
G06F 12/14 ５２０Ａ
G06F 12/14 ５４０Ａ

請求項の数 9　(全 37 頁)

(21)出願番号　特願2004-84014(P2004-84014)
(22)出願日　平成16年3月23日(2004.3.23)
(65)公開番号　特開2005-275504(P2005-275504A)
(43)公開日　平成17年10月6日(2005.10.6)
審査請求日　平成18年10月2日(2006.10.2)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100082131
弁理士　稲本　義雄
(72)発明者　山岸　靖明
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　橋本　勝憲
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　長　由紀子

最終頁に続く

(54)【発明の名称】情報処理システム、情報処理装置および方法、記録媒体、並びにプログラム

(57)【特許請求の範囲】
【請求項１】
第１の情報処理装置と第２の情報処理装置からなる情報処理システムにおいて、
前記第１の情報処理装置は、
コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件を、前記第２の情報処理装置に送信する送信手段を備え、
前記第２の情報処理装置は、
前記第１の情報処理装置から、前記メタデータ利用条件を受信する受信手段と、
暗号化されたメタデータを復号して、前記受信手段により受信された前記メタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号された前記メタデータを、前記セキュリティレベルに応じてそのまま、または再度暗号化して記憶させるメタデータ処理手段と、
前記コンテンツの検索要求に基づいて、前記メタデータ処理手段により前記所定の領域に記憶された前記メタデータを、前記セキュリティレベルに応じてそのまま、または復号して用いて、前記コンテンツの検索処理を実行する検索処理手段と、
前記検索処理手段による前記コンテンツの検索結果を出力する出力手段とを備える
情報処理システム。
【請求項２】
前記メタデータ利用条件は、前記セキュリティレベルの他に、前記メタデータの識別子、もしくは、前記メタデータを利用可能な、権利付与の対象者、または、操作に関する条

件を含む
請求項１に記載の情報処理システム。
【請求項３】
コンテンツを受信する情報処理装置において、
他の情報処理装置から、前記コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件を受信する受信手段と、
暗号化されたメタデータを復号して、前記受信手段により受信された前記メタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号された前記メタデータを、前記セキュリティレベルに応じてそのまま、または再度暗号化して記憶させるメタデータ処理手段と、
前記コンテンツの検索要求に基づいて、前記メタデータ処理手段により前記所定の領域に記憶された前記メタデータを、前記セキュリティレベルに応じてそのまま、または復号して用いて、前記コンテンツの検索処理を実行する検索処理手段と、
前記検索処理手段による前記コンテンツの検索結果を出力する出力手段と
を備える情報処理装置。
【請求項４】
前記メタデータ利用条件は、前記セキュリティレベルの他に、前記メタデータの識別子、もしくは、前記メタデータを利用可能な、権利付与の対象者、または、操作に関する条件を含む
請求項３に記載の情報処理装置。
【請求項５】
前記検索処理手段は、
前記コンテンツの検索要求に基づいて、前記メタデータ処理手段により前記所定の領域に記憶された前記メタデータを、前記セキュリティレベルに応じてそのまま読み出すか、または復号して読み出すメタデータ読み出し手段と、
前記メタデータ読み出し手段により読み出された前記メタデータを用いて、前記コンテンツを検索する検索手段とを備える
請求項３に記載の情報処理装置。
【請求項６】
前記コンテンツの再生要求があった場合、前記コンテンツを利用するために必要な権利情報を表すコンテンツ利用条件に基づいて、前記コンテンツが再生可能であるか否かを判定する再生判定手段と、
前記再生判定手段により前記コンテンツが再生可能であると判定された場合、前記コンテンツを復号し、再生する再生手段と
をさらに備える請求項３に記載の情報処理装置。
【請求項７】
コンテンツを受信する情報処理装置の情報処理方法において、
他の情報処理装置から、前記コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件を受信する受信ステップと、
暗号化されたメタデータを復号して、受信された前記メタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号された前記メタデータを、前記セキュリティレベルに応じてそのまま、または再度暗号化して記憶させるメタデータ処理ステップと、
前記コンテンツの検索要求に基づいて、前記所定の領域に記憶された前記メタデータを、前記セキュリティレベルに応じてそのまま、または復号して用いて、前記コンテンツの検索処理を実行する検索処理ステップと、
前記コンテンツの検索結果を出力する出力ステップと
を含む情報処理方法。
【請求項８】
コンテンツを受信する情報処理装置のコンピュータに、

他の情報処理装置から、前記コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件を受信する受信ステップと、
暗号化されたメタデータを復号して、受信された前記メタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号された前記メタデータを、前記セキュリティレベルに応じてそのまま、または再度暗号化して記憶させるメタデータ処理ステップと、
前記コンテンツの検索要求に基づいて、前記所定の領域に記憶された前記メタデータを、前記セキュリティレベルに応じてそのまま、または復号して用いて、前記コンテンツの検索処理を実行する検索処理ステップと、
前記コンテンツの検索結果を出力する出力ステップと
を含む処理を実行させるためのプログラムが記録されるプログラム記録媒体。
【請求項９】
コンテンツを受信する情報処理装置のコンピュータに、
他の情報処理装置から、前記コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件を受信する受信ステップと、
暗号化されたメタデータを復号して、受信された前記メタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号された前記メタデータを、前記セキュリティレベルに応じてそのまま、または再度暗号化して記憶させるメタデータ処理ステップと、
前記コンテンツの検索要求に基づいて、前記所定の領域に記憶された前記メタデータを、前記セキュリティレベルに応じてそのまま、または復号して用いて、前記コンテンツの検索処理を実行する検索処理ステップと、
前記コンテンツの検索結果を出力する出力ステップと
を含む処理を実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理システム、情報処理装置および方法、記録媒体、並びにプログラムに関し、特に、メタデータの内容に応じて、コンテンツに関するメタデータを利用する端末の処理を制御することができるようにした情報処理システム、情報処理装置および方法、記録媒体、並びにプログラムに関する。
【背景技術】
【０００２】
放送コンテンツ（放送波で配信されるコンテンツ、およびＩＰネットワーク上で配信されるコンテンツを含む）に関連するメタデータを利用する際に、メタデータの内容によっては、ユーザ端末での処理系に、高度なセキュリティを要するものと、セキュリティを要しないものを区別するようにすべきであるという要件が、放送コンテンツの事業者側から挙がっている。
【０００３】
これに対応して、従来、高度なセキュリティを要するメタデータは、コンテンツと同様に扱われ、高度なセキュリティを要するコンテンツと同じＤＲＭ(Digital Rights Management：著作権保護)システムで保護されて、伝送、蓄積、再生制御されていた。すなわち、高度なセキュリティを要するメタデータは、コンテンツを暗号化するコンテンツ鍵でコンテンツと同様に暗号化されたり、または、コンテンツ鍵を暗号化する鍵で暗号化され、保護されていた（特許文献１参照）。
【０００４】
【特許文献１】特開２００２－１０１０８６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】

しかしながら、実際には、メタデータは、コンテンツと異なる手順で扱われる場合が一般的である。例えば、ユーザ端末において、異なる複数のメタデータは、コンテンツより先に取得され、検索処理のため、予めデータベースに展開してから利用されることが多い。

【０００６】

すなわち、再生制御されるときにのみ暗号が解かれ、耐タンパなセキュアメモリ上で展開されて再生、表示制御されることにより、そのセキュリティが保護されるコンテンツとは異なり、メタデータの場合、コンテンツの検索要求が起こったときに初めてメタデータの暗号を解き、展開することは、ハードウェア的に困難である。したがって、メタデータは、予め暗号が解除され、データベースに展開されているほうがよい。

【０００７】

しかしながら、そのメタデータのセキュリティを保護するため、複数のメタデータが展開されるデータベースを、コンテンツの保護と同様に、高価なセキュアメモリ上に予め展開することは、コスト的に困難である。この場合、展開されたメタデータのデータベース領域として、耐タンパなセキュアメモリに加えて、セキュアハードディスクなどの２次記憶装置を併用して装置を構成することもできるが、一般に、セキュアハードディスクも、高価でコスト的に導入が難しく、たとえ、導入できたとしても、セキュアハードディスク等の２次記録装置は、セキュアメモリに比べ、データの保護に対するセキュリティが落ちてしまうことが多い。

【０００８】

以上のように、メタデータとコンテンツの、ユーザ端末における処理の利用条件そのものがそれぞれ分けて扱われる必要があるにもかかわらず、ユーザ端末において、高度なセキュリティを要するメタデータの保護が、高度なセキュリティを要するコンテンツと同様に扱われてしまうと、コストがかかりすぎてしまったり、あるいは、データの保護に対するセキュリティが低下してしまう課題があった。

【０００９】

また、放送コンテンツの事業者側においては、著作権保護に関して、コンテンツとメタデータの区別だけでなく、メタデータの種類によっても区別させたいという要件も挙がっている。その要件とは、具体的には、コンテンツを複数セグメントで分割してハイライトシーンのみをダイジェスト再生することが記述されているセグメントメタデータなどは、コンテンツ保護のセキュリティと同様なセキュリティを有する端末のみでしか処理させたくないというものである。しかしながら、上述したように、従来の方法では、メタデータは、セキュリティを要するか否かでしか区別されておらず、メタデータの種類に応じて、著作権保護に対するセキュリティの段階を細かく設定できない課題があった。

【００１０】

本発明は、このような状況に鑑みてなされたものであり、コンテンツの利用条件とは別に、メタデータに対する利用を制限することができるようにするものである。

【課題を解決するための手段】

【００１１】

本発明の情報処理システムは、第１の情報処理装置は、コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件を、第２の情報処理装置に送信する送信手段を備え、第２の情報処理装置は、第１の情報処理装置から、メタデータ利用条件を受信する受信手段と、暗号化されたメタデータを復号して、受信手段により受信されたメタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号されたメタデータを、セキュリティレベルに応じてそのまま、または再度暗号化して記憶させるメタデータ処理手段と、コンテンツの検索要求に基づいて、メタデータ処理手段により所定の領域に記憶されたメタデータを、セキュリティレベルに応じてそのまま、または復号して用いて、コンテンツの検索処理を実行する検索処理手段と、検索処理手段によるコンテンツの検索結果を出力する出力手段とを備える。

【００１２】

メタデータ利用条件は、セキュリティレベルの他に、メタデータの識別子、もしくは、メタデータを利用可能な、権利付与の対象者、または、操作に関する条件を含むことができる。

【００１３】

本発明の情報処理装置は、他の情報処理装置から、コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件を受信する受信手段と、暗号化されたメタデータを復号して、受信手段により受信されたメタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号されたメタデータを、セキュリティレベルに応じてそのまま、または再度暗号化して記憶させるメタデータ処理手段と、コンテンツの検索要求に基づいて、メタデータ処理手段により所定の領域に記憶されたメタデータを、セキュリティレベルに応じてそのまま、または復号して用いて、コンテンツの検索処理を実行する検索処理手段と、検索処理手段によるコンテンツの検索結果を出力する出力手段とを備える。

【００１４】

メタデータ利用条件は、セキュリティレベルの他に、メタデータの識別子、もしくは、メタデータを利用可能な、権利付与の対象者、または、操作に関する条件を含むことができる。

【００１５】

検索処理手段は、コンテンツの検索要求に基づいて、メタデータ処理手段により所定の領域に記憶されたメタデータを、セキュリティレベルに応じてそのまま読み出すか、または復号して読み出すメタデータ読み出し手段と、メタデータ読み出し手段により読み出されたメタデータを用いて、コンテンツを検索する検索手段とを備えることができる。

【００１６】

コンテンツの再生要求があった場合、コンテンツを利用するために必要な権利情報を表すコンテンツ利用条件に基づいて、コンテンツが再生可能であるか否かを判定する再生判定手段と、再生判定手段によりコンテンツが再生可能であると判定された場合、コンテンツを復号し、再生する再生手段とをさらに備えることができる。

【００１７】

本発明の情報処理方法は、他の情報処理装置から、コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件を受信する受信ステップと、暗号化されたメタデータを復号して、受信されたメタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号されたメタデータを、セキュリティレベルに応じてそのまま、または再度暗号化して記憶させるメタデータ処理ステップと、コンテンツの検索要求に基づいて、所定の領域に記憶されたメタデータを、セキュリティレベルに応じてそのまま、または復号して用いて、コンテンツの検索処理を実行する検索処理ステップと、コンテンツの検索結果を出力する出力ステップとを含む。

【００１８】

本発明の記録媒体に記録されるプログラムは、他の情報処理装置から、コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件を受信する受信ステップと、暗号化されたメタデータを復号して、受信されたメタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号されたメタデータを、セキュリティレベルに応じてそのまま、または再度暗号化して記憶させるメタデータ処理ステップと、コンテンツの検索要求に基づいて、所定の領域に記憶されたメタデータを、セキュリティレベルに応じてそのまま、または復号して用いて、コンテンツの検索処理を実行する検索処理ステップと、コンテンツの検索結果を出力する出力ステップとを含む。

【００１９】

本発明のプログラムは、他の情報処理装置から、コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件を受信する受信ステップと、暗号化されたメタデータを復号して、受信されたメタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号されたメタデータを、セキュリティレベルに応じてその

まま、または再度暗号化して記憶させるメタデータ処理ステップと、コンテンツの検索要求に基づいて、所定の領域に記憶されたメタデータを、セキュリティレベルに応じてそのまま、または復号して用いて、コンテンツの検索処理を実行する検索処理ステップと、コンテンツの検索結果を出力する出力ステップとを含む。

【００２０】

第１の本発明においては、第１の情報処理装置により、コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件が、第２の情報処理装置に送信される。第２の情報処理装置により、第１の情報処理装置から、コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件が受信され、暗号化されたメタデータが復号されて、受信されたメタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号されたメタデータが、セキュリティレベルに応じてそのまま、または再度暗号化されて記憶される。そして、コンテンツの検索要求に基づいて、所定の領域に記憶されたメタデータを、セキュリティレベルに応じてそのまま、または復号して用いて、コンテンツの検索処理が実行され、コンテンツの検索結果が出力される。

【００２１】

第２の本発明においては、情報処理装置から、コンテンツに関するメタデータを利用するために必要な権利情報を表すメタデータ利用条件が受信され、暗号化されたメタデータが復号されて、受信されたメタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号されたメタデータが、セキュリティレベルに応じてそのまま、または再度暗号化して記憶される。そして、コンテンツの検索要求に基づいて、所定の領域に記憶されたメタデータを、セキュリティレベルに応じてそのまま、または復号して用いて、コンテンツの検索処理が実行され、コンテンツの検索結果が出力される。

【発明の効果】

【００２２】

本発明によれば、メタデータのセキュリティレベルに応じて、端末側の処理を制御することができ、安全性が向上する。また、本発明によれば、メタデータの内容に応じて、処理可能な端末を制限することができる。

【発明を実施するための最良の形態】

【００２３】

以下に本発明の実施の形態を説明するが、請求項に記載の構成要件と、発明の実施の形態における具体例との対応関係を例示すると、次のようになる。この記載は、請求項に記載されている発明をサポートする具体例が、発明の実施の形態に記載されていることを確認するためのものである。したがって、発明の実施の形態中には記載されているが、構成要件に対応するものとして、ここには記載されていない具体例があったとしても、そのことは、その具体例が、その構成要件に対応するものではないことを意味するものではない。逆に、具体例が構成要件に対応するものとしてここに記載されていたとしても、そのことは、その具体例が、その構成要件以外の構成要件には対応しないものであることを意味するものでもない。

【００２４】

さらに、この記載は、発明の実施の形態に記載されている具体例に対応する発明が、請求項に全て記載されていることを意味するものではない。換言すれば、この記載は、発明の実施の形態に記載されている具体例に対応する発明であって、この出願の請求項には記載されていない発明の存在、すなわち、将来、分割出願されたり、補正により追加される発明の存在を否定するものではない。

【００２５】

請求項１に記載の情報処理システムは、第１の情報処理装置（例えば、図１のメタデータサーバ４）は、コンテンツ（例えば、図１のコンテンツ１１）に関するメタデータ（例えば、図１のメタデータ２１）を利用するために必要な権利情報を表すメタデータ利用条件（例えば、図１のメタデータライセンス２２）を、第２の情報処理装置に送信する送信

手段（例えば、図２の通信部３９）を備え、第２の情報処理装置（例えば、図１のユーザ端末１－１）は、第１の情報処理装置から、メタデータ利用条件を受信する受信手段と、暗号化されたメタデータを復号して、受信手段により受信されたメタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号されたメタデータを、セキュリティレベルに応じてそのまま、または再度暗号化して記憶させるメタデータ処理手段（例えば、図４のメタデータ復号部２１１）と、コンテンツの検索要求に基づいて、メタデータ処理手段により所定の領域に記憶されたメタデータを、セキュリティレベルに応じてそのまま、または復号して用いて、コンテンツの検索処理を実行する検索処理手段（例えば、図４のメタデータ検索部２１３）と、検索処理手段によるコンテンツの検索結果を出力する出力手段（例えば、図１９のステップＳ９０の処理を実行する図４のメタデータ表示制御部２１４）とを備えることを特徴とする。

【００２６】

請求項３に記載の情報処理装置は、他の情報処理装置（例えば、図１のメタデータサーバ４）から、コンテンツ（例えば、図１のコンテンツ１１）に関するメタデータ（例えば、図１のメタデータ２１）を利用するために必要な権利情報を表すメタデータ利用条件（例えば、図１のメタデータライセンス２２）を受信する受信手段（例えば、図３の受信部１０１）と、暗号化されたメタデータを復号して、受信手段により受信されたメタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号されたメタデータを、セキュリティレベルに応じてそのまま、または再度暗号化して記憶させるメタデータ処理手段（例えば、図４のメタデータ復号部２１１）と、コンテンツの検索要求に基づいて、メタデータ処理手段により所定の領域に記憶されたメタデータを、セキュリティレベルに応じてそのまま、または復号して用いて、コンテンツの検索処理を実行する検索処理手段（例えば、例えば、図１９のステップ８３の処理を制御する図４の利用条件判定処理部２０２）と、検索処理手段によるコンテンツの検索結果を出力する出力手段（例えば、図１９のステップＳ９０の処理を実行する図４のメタデータ出力制御部２１４）とを備えることを特徴とする。

【００２７】

請求項５に記載の情報処理装置は、検索処理手段は、コンテンツの検索要求に基づいて、メタデータ処理手段により所定の領域に記憶されたメタデータに、セキュリティレベルに応じた処理を実行するメタデータ読み出し手段（例えば、例えば、図２３のステップ１８１の処理を制御する図４の利用条件判定処理部２０２）と、メタデータ読み出し手段により読み出されたメタデータを用いて、コンテンツを検索する検索手段（例えば、図２３のステップＳ１８３の処理を実行する図４のメタデータ検索部２１３）とを備える。

【００２８】

請求項６に記載の情報処理装置は、コンテンツの再生要求があった場合、コンテンツ（例えば、図１のコンテンツ１１）を利用するために必要な権利情報を表すコンテンツ利用条件（例えば、図４のコンテンツ利用条件１５１）に基づいて、コンテンツが再生可能であるか否かを判定する再生判定手段（図４の利用条件判定処理部２２２）と、再生判定手段によりコンテンツが再生可能であると判定された場合、コンテンツを復号し、再生する再生手段（例えば、図４のコンテンツ復号部２３４）とをさらに備える。

【００２９】

請求項７に記載の情報処理方法は、他の情報処理装置（例えば、図１のメタデータサーバ４）から、コンテンツ（例えば、図１のコンテンツ１１）に関するメタデータ（例えば、図１のメタデータ２１）を利用するために必要な権利情報を表すメタデータ利用条件（例えば、図１のメタデータライセンス２２）を受信する受信ステップ（例えば、図１８のステップＳ４１）と、暗号化されたメタデータを復号して、受信されたメタデータ利用条件に含まれるセキュリティレベルに応じた所定の領域に、復号されたメタデータを、セキュリティレベルに応じてそのまま、または再度暗号化して記憶させるメタデータ処理ステップ（例えば、図１８のステップＳ４５）と、コンテンツの検索要求に基づいて、所定の領域に記憶されたメタデータを、セキュリティレベルに応じてそのまま、または復号して

用いて、コンテンツの検索処理を実行する検索処理ステップ（例えば、図１９のステップＳ８３）と、コンテンツの検索結果を出力する出力ステップと（例えば、図１９のステップＳ９０）を含む。

【００３０】

なお、請求項８に記載の記録媒体および請求項９に記載のプログラムは、上述した請求項７に記載の情報処理方法と基本的に同様の構成であるため、繰り返しになるのでその説明は省略する。

【００３１】

以下、図を参照して本発明の実施の形態について説明する。

【００３２】

図１は、本発明を適用したコンテンツ提供システムの構成例を表している。インターネットに代表されるネットワーク２には、パーソナルコンピュータなどにより構成されるユーザ端末１－１，１－２（以下、これらのユーザ端末を個々に区別する必要がない場合、単にユーザ端末１と称する）が接続されている。この例においては、ユーザ端末が２台のみ示されているが、ネットワーク２には、任意の台数のユーザ端末が接続される。

【００３３】

また、ネットワーク２には、コンテンツサーバ３およびメタデータサーバ４が接続されている。これらのコンテンツサーバ３およびメタデータサーバ４も、任意の台数、ネットワーク２に接続される。

【００３４】

コンテンツサーバ３には、図示せぬコンテンツプロバイダにより、著作権保護を必要とするコンテンツ１１、および、そのコンテンツ１１を利用するために必要なコンテンツ利用条件が含まれるコンテンツライセンス１２が記憶される。コンテンツサーバ３は、ユーザ端末１に対して、コンテンツ１１およびコンテンツライセンス１２を、ネットワーク２を介して提供する。コンテンツ利用条件は、例えば、対象となる対象コンテンツの「コンテンツＩＤ（識別子）」、対象コンテンツを利用するための「権利付与の対象者（ユーザ、グループ）」、並びに、対象コンテンツに対して許可される操作、期限、および回数などの「権利行使の条件」などからなる。

【００３５】

メタデータサーバ４には、図示せぬメタデータプロバイダにより、コンテンツサーバ３から提供されるコンテンツに関するメタデータ２１、および、そのメタデータを利用するために必要なメタデータ利用条件が含まれるメタデータライセンス２２が記憶される。メタデータサーバ４は、ユーザ端末１に対して、記憶されているメタデータ２１およびメタデータライセンス２２を、ネットワーク２を介して提供する。

【００３６】

メタデータ２１は、コンテンツのリリースや放送形態に依存しないコンテンツに関する一般的な情報（例えば、コンテンツのタイトルや内容、ジャンルなどの情報）であり、コンテンツの内容を検索するために用いられる。メタデータ利用条件は、例えば、対象となる対象メタデータの「メタデータＩＤ（識別子）」、対象メタデータを利用するための「権利付与の対象者（ユーザ、グループ）」、並びに、対象メタデータに対して許可される操作、期限、回数、および、対象メタデータを処理するユーザ端末１におけるセキュリティレベルなどの「権利行使の条件」などからなる。

【００３７】

ユーザ端末１は、メタデータサーバ４からのメタデータ２１およびメタデータライセンス２２を受信すると、メタデータライセンス２２のメタデータ利用条件に応じて、受信したメタデータ２１の暗号を解除し、展開する。また、ユーザ端末１は、ユーザよりコンテンツの検索要求があった場合、メタデータ利用条件に応じて、展開されているメタデータ２１を用いて、検索要求されたコンテンツ１１を検索する。そして、ユーザ端末１は、検索されたコンテンツ１１に対して、ユーザの再生要求があった場合、コンテンツライセンス１２のコンテンツ利用条件に応じて、要求されたコンテンツ１１の暗号を解除し、再生

する。
【００３８】
以上のように、図１のコンテンツ提供システムにおいては、ユーザ端末１には、コンテンツライセンス１２とは別に、メタデータ２１を利用するために必要なメタデータライセンス２２が提供され、メタデータ２１は、メタデータライセンス２２に基づいて処理され、コンテンツ１１は、コンテンツライセンス１２に基づいて処理される。
【００３９】
なお、図１の例においては、コンテンツ１１とコンテンツライセンス１２をコンテンツサーバ３から提供し、メタデータ２１とメタデータライセンス２２をメタデータサーバ４から提供するようにしたが、コンテンツ１１、コンテンツライセンス１２、メタデータ２１、およびメタデータライセンス２２の提供方法は、図１の例に限らず、すべてを同じサーバから提供するようにしてもよいし、それぞれ別のサーバから提供するようにしてもよい。
【００４０】
また、ユーザ端末１は、パーソナルコンピュータで構成することができることはもちろん、例えば、携帯電話機その他のPDA(Personal Digital Assistant)機器や、AV(Audio Visual)機器や家電（家庭用電化製品）などのCE（Consumer Electronics）機器などで構成することもできる。
【００４１】
図２は、ユーザ端末１のハードウェア構成例を表している。図２においては、ユーザ端末１は、例えばコンピュータをベースに構成されている。
【００４２】
ＣＰＵ（Central Processing Unit）３１は、ＲＯＭ（Read Only Memory）３２に記憶されているプログラム、または記憶部３８からＲＡＭ（Random Access Memory）３３にロードされたプログラムに従って各種の処理を実行する。ＲＡＭ３３にはまた、ＣＰＵ３１が各種の処理を実行する上において必要なデータなども適宜記憶される。
【００４３】
ＣＰＵ３１、ＲＯＭ３２、およびＲＡＭ３３は、バス３４を介して相互に接続されている。このバス３４にはまた、入出力インタフェース３５も接続されている。
【００４４】
入出力インタフェース３５には、キーボード、マウスなどよりなる入力部３６、ＣＲＴ（Cathode Ray Tube）、ＬＣＤ（Liquid Crystal Display）などよりなるディスプレイ、並びにスピーカなどよりなる出力部３７、ハードディスクなどより構成される記憶部３８、モデム、ターミナルアダプタなどより構成される通信部３９が接続されている。通信部３９は、ネットワーク２を介しての通信処理を行う。
【００４５】
入出力インタフェース３５にはまた、必要に応じてドライブ４０が接続され、磁気ディスク４１、光ディスク４２、光磁気ディスク４３、或いは半導体メモリ４４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部３８にインストールされる。
【００４６】
なお、図示は省略するが、コンテンツサーバ３、およびメタデータサーバ４も、図２に示したユーザ端末１と基本的に同様の構成を有するコンピュータにより構成される。そこで、以下の説明においては、図２の構成は、コンテンツサーバ３、またはメタデータサーバ４などの構成としても引用される。
【００４７】
ここで、ＣＰＵ３１が、各種のプログラムを実行することにより、図２のコンピュータは、ユーザ端末１、コンテンツサーバ３、またはメタデータサーバ４として機能することとなる。この場合、プログラムは、図２のコンピュータに内蔵されている記録媒体としてのROM３２や記憶部３８に予め記録しておくことができる。あるいはまた、プログラムは

、磁気ディスク４１や、光ディスク４２、光磁気ディスク４３、半導体メモリ４４などのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）し、いわゆるパッケージソフトウエアとして提供することができる。

【００４８】

なお、プログラムは、上述したようなリムーバブル記録媒体から図２のコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、図２のコンピュータに無線で転送したり、LAN(Local Area Network)、ネットワーク２を介して、図２のコンピュータに有線で転送してインストールすることもできる。

【００４９】

図３は、ユーザ端末１の機能構成例を示すブロック図である。図３に示される機能ブロックは、ユーザ端末１のＣＰＵ３１により所定の制御プログラムが実行されることで実現される。

【００５０】

受信部１０１は、コンテンツサーバ３またはメタデータサーバ４からネットワーク２を介して送信されてくるコンテンツ１１、コンテンツライセンス１２、メタデータ２１、または、メタデータライセンス２２を受信し、メタデータ２１をメタデータ処理部１０３に、コンテンツ１１をコンテンツ処理部１０４に、それぞれ供給し、コンテンツライセンス１２およびメタデータライセンス２２をＤＲＭ(Digital rights management)制御部１０２に供給する。

【００５１】

ＤＲＭ制御部１０２は、メタデータ利用条件判定部１１１およびコンテンツ利用条件判定部１１２により構成され、コンテンツ１１およびメタデータ２１の著作権を保護する処理を行う。メタデータ利用条件判定部１１１は、受信部１０１からメタデータライセンス２２を入力すると、メタデータライセンス２２のメタデータ利用条件に応じて、メタデータ処理部１０３を制御し、メタデータ２１に対して所定の処理をさせる。すなわち、メタデータ利用条件判定部１１１は、メタデータ利用条件に基づいて、ユーザ端末１がメタデータ２１を展開可能であるか（すなわち、メタデータ２１を用いて、コンテンツ検索処理が可能であるか）否かを判定し、ユーザ端末１がメタデータ２１を展開可能であると判定した場合、メタデータ処理部１０３を制御し、対応するメタデータ２１の暗号を解除させ、図４を参照して後述するメタデータＤＢ（データベース）２１２に蓄積させる。また、メタデータ利用条件判定部１１１は、入力部３６を介して、ユーザのコンテンツ検索の操作信号が入力されると、メタデータ利用条件に応じて、メタデータ処理部１０３に、メタデータＤＢ２１２に蓄積されているメタデータ２１を用いたコンテンツの検索処理を実行させる。

【００５２】

コンテンツ利用条件判定部１１２は、入力部３６を介して、ユーザのコンテンツ再生の操作信号が入力されると、受信部１０１より供給されるコンテンツライセンス１２のコンテンツ利用条件に基づいて、コンテンツ処理部１０４を制御し、コンテンツ１１に対して所定の処理をさせる。すなわち、コンテンツ利用条件判定部１１２は、入力部３６からコンテンツ１１の再生要求が指示されると、受信部１０１より供給されるコンテンツライセンス１２のコンテンツ利用条件に基づいて、ユーザ端末１がそのコンテンツ１１を再生可能であるか否かを判定し、ユーザ端末１がコンテンツ１１を再生可能であると判定した場合、コンテンツ処理部１０４を制御し、コンテンツ１１の暗号を解除させ、再生させる。また、コンテンツ利用条件判定部１１２は、入力部３６より指示されたコンテンツライセンス１２がユーザ端末１にない場合、コンテンツ処理部１０４を制御し、コンテンツライセンス１２の要求を、送信部１０５およびネットワーク２を介して、コンテンツサーバ３に送信させる。

【００５３】

メタデータ処理部１０３は、メタデータ利用条件判定部１１１の制御のもと、メタデータ２１に対して所定の処理を実行する。すなわち、メタデータ処理部１０３は、受信部１

０１より供給されるメタデータ２１の暗号の解除、または、メタデータ２１のメタデータＤＢ２１２への蓄積などを実行したり、メタデータＤＢ２１２に蓄積されているメタデータ２１の検索処理を実行し、その検索結果を、出力部３７を構成するモニタに表示させる。また、メタデータ処理部１０３は、メタデータ２１またはメタデータライセンス２２の要求を、送信部１０５およびネットワーク２を介して、メタデータサーバ４に送信する。

【００５４】

コンテンツ処理部１０４は、コンテンツ利用条件判定部１１２の制御のもと、コンテンツ１１またはコンテンツライセンス１２の要求を、送信部１０５およびネットワーク２を介して、コンテンツサーバ３に送信したり、コンテンツ記憶部２３２（図４）にコンテンツ１１を蓄積したり、コンテンツ１１の暗号を解除し、暗号が解除されたコンテンツ１１を再生し、出力部３７のモニタに表示させる。

【００５５】

送信部１０５は、コンテンツ処理部１０４からのコンテンツ取得の要求、または、メタデータ処理部１０３からのメタデータ取得の要求を、ネットワーク２を介して、コンテンツサーバ３またはメタデータサーバ４に送信する。

【００５６】

図４は、図３のユーザ端末１の詳細な機能構成例を表している。すなわち、図４は、図３のメタデータ処理部１０３、コンテンツ処理部１０４、メタデータ利用条件判定部１１１、およびコンテンツ利用条件判定部１１２の詳細な構成例を示すブロック図である。なお、図４において、太枠は、暗号化の状態を表している。

【００５７】

したがって、コンテンツ１１は、コンテンツサーバ３から、図示せぬコンテンツプロバイダによりコンテンツ暗号鍵１５２で暗号化された状態で、ネットワーク２および受信部１０１を介して、コンテンツ蓄積部２３１に供給される。コンテンツライセンス１２は、コンテンツサーバ３から、コンテンツプロバイダのＰＫＩ(Public Key Infrastructure)に基づいたコンテンツプロバイダ秘密鍵で暗号化された状態で、ネットワーク２および受信部１０１を介して、コンテンツライセンス復号部２２１に供給される。

【００５８】

コンテンツライセンス１２は、コンテンツ利用条件１５１、および、コンテンツ１１の暗号を解除するためのコンテンツ暗号鍵１５２により構成される。コンテンツ利用条件１５１は、例えば、対象となる対象コンテンツの「コンテンツＩＤ（識別子）例えば、ＵＲＬ（Uniform Resource Locator）」、対象コンテンツを利用するための「権利を行使する対象者（ユーザ、グループ）」、並びに、対象コンテンツに対して許可される操作（例えば、蓄積、再生、または複製など）、期限、および回数などの「権利行使の条件」などにより構成される。

【００５９】

メタデータ２１は、メタデータサーバ４から、図示せぬメタデータプロバイダによりメタデータ暗号鍵１６２で暗号化された状態で、ネットワーク２および受信部１０１を介して、メタデータ復号部２１１に供給される。メタデータライセンス２２は、メタデータサーバ４から、メタデータプロバイダのＰＫＩに基づいたメタデータプロバイダ秘密鍵で暗号化された状態で、ネットワーク２および受信部１０１を介して、メタデータライセンス復号部２０１に供給される。

【００６０】

メタデータ２１は、コンテンツに関連する情報などにより構成される。メタデータライセンス２２は、メタデータ利用条件１６１、および、メタデータ２１の暗号を解除するためのメタデータ暗号鍵１６２により構成される。メタデータ利用条件１６１は、図５に示されるように、例えば、「メタデータＩＤ（識別子）」、「権利付与の対象者（ユーザ名/ ユーザクラス名）」、「操作の対象要素（要素名）」、および「権利行使の条件」などにより構成される。

【００６１】

図５の例において、対象メタデータＩＤは、対象となるメタデータを識別する識別子であり、例えば、ＵＲＬで表される。権利付与の対象者は、権利が付与される対象を表すものであり、ユーザ名であってもよいし、ユーザが属するユーザクラス名であってもよい。具体的には、権利付与の対象者は、ユーザ端末のデバイス名や、ユーザによりメタデータを利用するために、メタデータプロバイダに予め契約される契約クラス名などからなる。操作の対象要素は、対象となるメタデータのうち、利用することが可能である部分（要素）を表す。権利行使の条件は、例えば、「デバイスセキュリティクラス」および「操作クラス」などからなる。

【００６２】

デバイスセキュリティクラスは、権利行使可能なデバイスのセキュリティレベル（例えば、レベル－Ｘ）を表すものである。デバイスのセキュリティレベルとは、デバイス（例えば、ユーザ端末１）が、著作権保護を必要とするデータに対して、どの程度のセキュリティで処理を実行することができるかということを定義したものである。

【００６３】

例えば、セキュリティレベルは、後述する図６の場合、メタデータを展開するメタデータＤＢ２１２の構成要素（メモリやハードディスクなど）がセキュリティ対策されているか否かで定義されている。この場合、メタデータＤＢ２１２の構成要素がメタデータ利用条件１６１のセキュリティレベルより低い場合、ユーザ端末１は、対象メタデータを展開することができないというように、メタデータＤＢ２１２の構成要素が、耐タンパ領域（セキュアな領域）に構成されているか（すなわち、メタデータが耐タンパ領域で処理されるか）否かに基づいて、メタデータプロバイダは、メタデータを処理するデバイスを制限することができる。すなわち、メタデータプロバイダは、セキュリティレベルが低いとされるデバイスに、メタデータの処理を禁止することができる。

【００６４】

操作クラスは、例えば、「ディスクに蓄積」などのように対象メタデータに対して許可される操作（例えば、蓄積、展開、または検索など）を示す。なお、ここには、期限、および回数なども記述することができる。

【００６５】

図４に戻って、点線で囲まれた領域は、ユーザ端末１における耐タンパ領域を表している。すなわち、ユーザ端末１において、メタデータ利用条件判定部１１１、コンテンツ利用条件判定部１１２、メタデータ処理部１０３のメタデータ復号部２１１およびメタデータＤＢ２１２の一部、並びに、コンテンツ処理部１０４のコンテンツ復号部２３４は、耐タンパ領域に構成されている。

【００６６】

メタデータ利用条件判定部１１１は、メタデータライセンス復号部２０１、利用条件判定処理部２０２により構成される。メタデータライセンス復号部２０１は、図示せぬ認証局（以下、ＣＡ(Certification Authority)と称する）より、メタデータプロバイダのＰＫＩに基づいたメタデータプロバイダ公開鍵１７１を予め取得し、記憶している。メタデータライセンス復号部２０１は、受信部１０１から供給されるメタデータライセンス２２の暗号を、メタデータプロバイダ公開鍵１７１で解除し、暗号が解除されたメタデータライセンス２２を、メタデータ利用条件１６１とメタデータ暗号鍵１６２に分け、利用条件判定処理部２０２に供給する。

【００６７】

利用条件判定処理部２０２は、ユーザ端末１が、メタデータライセンス復号部２０１により供給されたメタデータ利用条件１６１に該当する端末１であるか否かを判定し、その判定結果に基づいて、メタデータ暗号鍵１６２をメタデータ復号部２１１に供給し、メタデータ復号部２１１を制御し、対象メタデータに対して、メタデータ利用条件１６１に応じたメタデータ蓄積処理を実行させる。また、利用条件判定処理部２０２は、入力部３６を介してユーザのコンテンツ検索の操作信号が入力されると、メタデータＤＢ２１２に蓄積されているメタデータ２１のメタデータ利用条件１６１に応じて、メタデータ検索部２

１３を制御し、メタデータＤＢ２１２に蓄積されているメタデータ２１を用いたコンテンツの検索処理を実行させる。

【００６８】

メタデータ処理部１０３は、メタデータ復号部２１１、メタデータＤＢ２１２、メタデータ検索部２１３、およびメタデータ表示制御部２１４により構成される。メタデータ復号部２１１には、受信部１０１より暗号化されたメタデータ２１が供給され、利用条件判定処理部２０２よりメタデータ暗号鍵１６２が供給される。メタデータ復号部２１１は、利用条件判定処理部２０２の制御のもと、メタデータ暗号鍵１６２でメタデータ２１の暗号を解除し、暗号が解除されたメタデータ２１を、メタデータＤＢ２１２の耐タンパ領域に展開、蓄積したり、または、再度暗号化し、メタデータＤＢ２１２の耐タンパではない通常領域にメタデータ２１を蓄積する。また、メタデータ復号部２１１は、メタデータＤＢ２１２の通常領域に蓄積されるメタデータ２１がメタデータ検索部２１３により特定された場合、特定されたメタデータ２１の暗号を耐タンパ領域において解除し、メタデータ検索部２１３に供給する。

【００６９】

メタデータＤＢ２１２は、耐タンパ領域（例えば、セキュアメモリやセキュアハードディスクなど）と通常領域で構成され、例えば、図６を参照して後述するように、その構成要素に応じて、セキュリティレベルが定義されており、メタデータ復号部２１１によりメタデータ２１が展開、あるいは蓄積される。

【００７０】

メタデータ検索部２１３は、利用条件判定処理部２０２の制御のもと、メタデータＤＢ２１２に蓄積されているメタデータ２１を用いて、ユーザ指定のコンテンツの検索処理を実行し、ユーザ指定のコンテンツに対応するメタデータ２１を取得し、取得したメタデータ２１に応じて、コンテンツの検索結果情報を生成し、生成したコンテンツの検索結果情報を、メタデータ表示制御部２１４に供給する。また、メタデータ検索部２１３は、利用条件判定処理部２０２の制御のもと、送信部１０５およびネットワーク２を介して、メタデータサーバ４から所望のメタデータ２１およびメタデータライセンス２２を取得させる。

【００７１】

メタデータ表示制御部２１４は、メタデータ検索部２１３より供給される、メタデータ２１を用いて実行されたコンテンツの検索結果情報などに基づいた画像を、出力部３７を構成するモニタなどに出力する制御を行う。

【００７２】

コンテンツ利用条件判定部１１２は、コンテンツライセンス復号部２２１、および利用条件判定処理部２２２により構成される。コンテンツライセンス復号部２２１は、図示せぬＣＡより、コンテンツプロバイダのＰＫＩに基づいたコンテンツプロバイダ公開鍵１７２を予め取得し、記憶している。コンテンツライセンス復号部２０１は、受信部１０１から供給されるコンテンツライセンス１２の暗号を、コンテンツプロバイダ公開鍵１７２で解除し、暗号が解除されたコンテンツライセンス１２を、コンテンツ利用条件１５１とコンテンツ暗号鍵１５２に分け、利用条件判定処理部２２２に供給する。

【００７３】

利用条件判定処理部２２２は、ユーザの操作により、入力部３６を介して入力される操作信号に基づいて、ユーザ端末１が、コンテンツライセンス復号部２２１により供給されたコンテンツ利用条件１５１に該当する端末１であるか否かを判定し、その判定結果に基づいて、コンテンツ暗号鍵１５２をコンテンツ復号部２３４に供給するとともに、コンテンツ蓄積部２３１、コンテンツ検索部２３３、およびコンテンツ復号部２３４に、対象コンテンツに対して、コンテンツ利用条件１５１に応じた処理を実行させる。すなわち、利用条件判定処理部２２２は、入力部３６からコンテンツ１１の再生要求が指示されると、コンテンツ利用条件１５１に基づいて、ユーザ端末１がそのコンテンツ１１を再生可能であるか否かを判定し、ユーザ端末１がコンテンツ１１を再生可能であると判定した場合、

コンテンツ暗号鍵１５２を、コンテンツ復号部２３４に供給するとともに、コンテンツ検索部２３３およびコンテンツ復号部２３４を制御し、コンテンツ１１の暗号を解除させ、再生させる。

【００７４】

コンテンツ処理部１０４は、コンテンツ蓄積部２３１、コンテンツ記憶部２３２、コンテンツ検索部２３３、コンテンツ復号部２３４、および、コンテンツ表示制御部２３５により構成される。コンテンツ蓄積部２３１には、受信部１０１より暗号化されたコンテンツ１１が供給される。コンテンツ蓄積部２３１は、利用条件判定処理部２２２の制御のもと、供給されたコンテンツ１１を、コンテンツ記憶部２３２に蓄積する。

【００７５】

コンテンツ記憶部２３２は、メモリやハードディスクなどにより構成され、暗号化されたコンテンツ１１を、一旦蓄積したり、記憶する。コンテンツ検索部２３３は、利用条件判定処理部２２２の制御のもと、再生対象のコンテンツＩＤに対応するコンテンツをコンテンツ記憶部２３２から検索し、検索したコンテンツを、コンテンツ復号部２３４に復号させる。また、メタデータ検索部２１３は、再生対象のコンテンツＩＤに対応するコンテンツ１１が、コンテンツ記憶部２３２に蓄積されていない場合、送信部１０５を制御し、ネットワーク２を介して、コンテンツサーバ３から所望のコンテンツ１１を取得させる。

【００７６】

コンテンツ復号部２３４は、コンテンツ記憶部２３２において、コンテンツ検索部２３３により検索されたコンテンツ１１を入力し、コンテンツ暗号鍵１５２で、コンテンツ１１の暗号を耐タンパ領域において解除し、暗号が解除されたコンテンツ１１をコンテンツ表示制御部２３５に供給する。コンテンツ表示制御部２３５は、コンテンツ復号部２３４より供給されるコンテンツに基づいた画像を、出力部３７を構成するモニタなどに出力する制御を行う。

【００７７】

図６は、メタデータＤＢ２１２の構成要素とセキュリティレベルの対応関係の例を表している。ユーザ端末１においては、メタデータＤＢ２１２の構成要素のセキュリティの程度に応じて、セキュリティレベルが定義されている。

【００７８】

メタデータＤＢ２１２の構成要素が、耐タンパなメモリであるセキュアメモリで構成される場合、このユーザ端末１のセキュリティレベルは、レベル１とされる。メタデータＤＢ２１２の構成要素が、セキュアメモリと耐タンパなハードディスクであるセキュアハードディスクで構成される場合、このユーザ端末１のセキュリティレベルは、レベル２とされる。メタデータＤＢ２１２の構成要素が、セキュアメモリと耐タンパではないハードディスクである通常ハードディスクで構成される場合、このユーザ端末１のセキュリティレベルは、レベル３とされる。メタデータＤＢ２１２の構成要素が、耐タンパではないメモリである通常メモリと耐タンパなハードディスクであるセキュアハードディスクで構成される場合、このユーザ端末１のセキュリティレベルは、レベル４とされる。

【００７９】

なお、図６の例においては、ユーザ端末１におけるセキュリティレベルがメタデータＤＢ２１２の構成要素のセキュリティの程度により定義される場合を説明したが、メタデータＤＢ２１２だけでなく、メタデータの検索処理や、検索結果の応答処理を行うメタデータ検索部２１３のセキュリティの程度や、メタデータ検索部２１３からメタデータ検索結果が供給されるメタデータ表示制御部２１４のセキュリティの程度（すなわち、メタデータ検索部２１３またはメタデータ表示制御部２１４が耐タンパ領域上で処理可能か否か）などに応じて、ユーザ端末１のセキュリティレベルを定義するようにしてもよい。

【００８０】

図７を参照して、図６のセキュリティレベルで構成されるメタデータＤＢ２１２におけるメタデータの処理について説明する。図７の例においては、メタデータＤＢ２１２が、セキュリティレベル１であるメタデータＤＢ２１２－１、セキュリティレベル２であるメ

タデータＤＢ２１２－２、セキュリティレベル３であるメタデータＤＢ２１２－３、および、セキュリティレベル４であるメタデータＤＢ２１２－４である場合の構成例についてそれぞれ説明する。なお、ユーザ端末１において、メタデータＤＢの構成は、すべての構成を可能なように構成するようにしてもよいし、ユーザ端末１が有する機能の構成要素に応じて、これらの構成のうち、いずれか１つの構成などをとるようにしてもよい。

【００８１】

図７の例の場合、ユーザ端末１は、セキュアメモリ３０１、通常メモリ３０２、セキュアハードディスク３０３、通常ハードディスク３０４を有している。なお、各メモリおよびディスクにおいて、実線で示されるインデックステーブルまたはデータブロックは、常時展開（常駐）していることを表し、点線で示されるインデックステーブルまたはデータブロックは、逐次展開することを表し、太線で示されるインデックステーブルまたはデータブロックは、常時暗号化の状態であることを表す。

【００８２】

メタデータＤＢ２１２－１は、セキュリティレベル１であり、セキュアメモリ３０１により構成される。このメタデータＤＢ２１２－１の構成において、例えば、メタデータ２１のメタデータ利用条件１６１の「権利行使の条件」が、「セキュリティレベル１で検索許可」であった場合、メタデータ復号部２１１は、利用条件判定処理部２０２の制御のもと、メタデータ２１のデータ要素を効率よく検索するための索引としてのインデックステーブル３１１と、メタデータ２１のデータ要素であるデータブロック３１２に分けて、セキュアメモリ３０１に展開する。

【００８３】

メタデータＤＢ２１２－２は、セキュリティレベル２であり、セキュアメモリ３０１およびセキュアハードディスク３０３により構成される。このメタデータＤＢ２１２－２の構成において、例えば、メタデータ２１のメタデータ利用条件１６１の「権利行使の条件」が、「セキュリティレベル２で検索許可」であった場合、メタデータ復号部２１１は、利用条件判定処理部２０２の制御のもと、インデックステーブル３１１と、データブロック３１２に分け、インデックステーブル３１１をセキュアメモリ３０１に展開し、データブロック３１２を、セキュアハードディスク３０３に展開する。

【００８４】

メタデータＤＢ２１２－３は、セキュリティレベル３であり、セキュアメモリ３０１および通常ハードディスク３０４により構成される。このメタデータＤＢ２１２－３の構成において、例えば、メタデータ２１のメタデータ利用条件１６１の「権利行使の条件」が、「セキュリティレベル３で検索許可」であった場合、メタデータ復号部２１１は、利用条件判定処理部２０２の制御のもと、インデックステーブル３１１と、データブロック３１２に分け、インデックステーブル３１１をセキュアメモリ３０１に展開し、データブロック３１２を再度暗号化し、暗号化したデータブロック３１２を、通常ハードディスク３０４に展開する。

【００８５】

メタデータＤＢ２１２－４は、セキュリティレベル４であり、通常メモリ３０２およびセキュアハードディスク３０３により構成される。このメタデータＤＢ２１２－４の構成において、例えば、メタデータ２１のメタデータ利用条件１６１の「権利行使の条件」が、「セキュリティレベル４で検索許可」であった場合、メタデータ復号部２１１は、利用条件判定処理部２０２の制御のもと、インデックステーブル３１１と、データブロック３１２に分け、インデックステーブル３１１とデータブロック３１２を、セキュアハードディスク３０３に展開する。

【００８６】

なお、ユーザ端末１に、セキュリティレベル１のメタデータＤＢ２１２－１を構成する場合、インデックステーブル３１１およびデータブロック３１２を常時蓄積しておける容量の高価なセキュアメモリ３０１が必要になるが、インデックステーブル３１１も、データブロック３１２もセキュアメモリ３０１に展開されるため、メタデータの安全性は高く

、検索速度は速くなる。

【００８７】

ユーザ端末１に、セキュリティレベル２のメタデータＤＢ２１２－２を構成する場合、インデックステーブル３１１はセキュアメモリ３０１に展開され、データブロック３１２はセキュアハードディスク３０３に展開されるため、セキュリティレベル１よりは、安全性も検索速度も多少低くなるが、インデックステーブル３１１を常時蓄積しておけるだけのセキュアメモリ３０１と、データブロック３１２を蓄積する、セキュアメモリ３０１より安価なセキュアハードディスク３０３があればよく、セキュリティレベル１より安く構成できる。

【００８８】

ユーザ端末１に、セキュリティレベル３のメタデータＤＢ２１２－３を構成する場合、インデックステーブル３１１はセキュアメモリ３０１に展開され、データブロック３１２は通常ハードディスク３０３に暗号化されて蓄積されるため、通常ハードディスク３０４からの入出力時に暗号化復号処理が必要となり、検索速度が遅くなってしまうが、セキュアハードディスク３０３が必要ない分、コストを安く構成できる。

【００８９】

ユーザ端末１に、セキュリティレベル４のメタデータＤＢ２１２－４を構成する場合、インデックステーブル３１１およびデータブロック３１２はセキュアハードディスク３０３に展開、蓄積されているため、メタデータの検索の度に、通常メモリ３０２に、インデックステーブル３１１を展開する必要があり、検索速度も、安全性も高いとはいえないが、高価なセキュアメモリ３０１が必要ない分、コストを安く構成できる。

【００９０】

以上のように、メタデータ利用条件１６１に、「権利行使の条件」として、ユーザ端末１のデータベースＤＢ２１２のセキュリティレベルを記述することにより、ユーザ端末１において、メタデータを展開できるユーザ端末１や、ユーザ端末１内の処理方法（領域）を制限することができる。次に、このようにして、メタデータＤＢ２１２－１乃至メタデータＤＢ２１２－４に蓄積されたメタデータ２１を用いて実行されるコンテンツの検索処理について、それぞれ説明する。

【００９１】

メタデータＤＢ２１２－１に展開されているメタデータ２１を検索処理する場合、メタデータ検索部２１３は、利用条件判定処理部２０２から、ユーザ指定のコンテンツの検索要求が指示されると、利用条件判定処理部２０２のメタデータ利用条件１６１のセキュリティレベルに応じた制御のもと、セキュアメモリ３０１のインデックステーブル３１１を用いて、指定のコンテンツに対応するメタデータを検索し、セキュアメモリ３０１のデータブロック３１２から、検索されたメタデータに対応するデータブロック（データ要素）を特定し、特定されたデータブロックに基づいて、コンテンツの検索結果を求め、コンテンツの検索結果を、メタデータ表示制御部２１４に供給する。

【００９２】

メタデータＤＢ２１２－２に展開されているメタデータ２１を検索処理する場合、メタデータ検索部２１３は、利用条件判定処理部２０２から、ユーザ指定のコンテンツの検索要求が指示されると、利用条件判定処理部２０２のメタデータ利用条件１６１のセキュリティレベルに応じた制御のもと、セキュアメモリ３０１のインデックステーブル３１１を用いて、指定のコンテンツに対応するメタデータを検索し、セキュアハードディスク３０３のデータブロック３１２から、検索されたメタデータに対応するデータブロックを特定し、特定されたデータブロックに基づいて、コンテンツの検索結果を求め、コンテンツの検索結果を、メタデータ表示制御部２１４に供給する。

【００９３】

メタデータＤＢ２１２－３に蓄積されているメタデータ２１を検索処理する場合、メタデータ検索部２１３は、利用条件判定処理部２０２から、ユーザ指定のコンテンツの検索要求が指示されると、利用条件判定処理部２０２のメタデータ利用条件１６１のセキュリ

ティレベルに応じた制御のもと、セキュアメモリ３０１のインデックステーブル３１１を用いて、指定のコンテンツに対応するメタデータを検索し、通常ハードディスク３０４のデータブロック３１２から、検索されたメタデータに対応するデータブロックを特定し、メタデータ復号部２１１に、特定したデータブロックの暗号を解除させ、暗号が解除されたデータブロックに基づいて、コンテンツの検索結果を求め、コンテンツの検索結果を、メタデータ表示制御部２１４に供給する。

【００９４】

メタデータＤＢ２１２－４に蓄積されているメタデータ２１を検索処理する場合、メタデータ検索部２１３は、利用条件判定処理部２０２から、ユーザ指定のコンテンツの検索要求が指示されると、利用条件判定処理部２０２のメタデータ利用条件１６１のセキュリティレベルに応じた制御のもと、セキュアハードディスク３０３のインデックステーブル３１１を、通常メモリ３０２にインデックステーブル３１３として展開し、展開されたインデックステーブル３１３を用いて、指定のコンテンツに対応するメタデータを検索し、セキュアハードディスク３０３のデータブロック３１２から、検索されたメタデータに対応するデータブロックを特定し、特定したデータブロックに基づいて、コンテンツの検索結果を求め、コンテンツの検索結果を、メタデータ表示制御部２１４に供給する。そして、メタデータ検索部２１３は、メタデータ２１を用いて指定のコンテンツが検索された後、通常メモリ３０２に展開したインデックステーブル３１３を消去する。

【００９５】

以上のように、メタデータ検索部２１３は、メタデータ利用条件１６１のセキュリティレベルに応じて、検索処理を実行する。すなわち、メタデータ利用条件１６１に、ユーザ端末１のセキュリティレベルを記述することにより、メタデータの内容の重要性に応じて、ユーザ端末１における処理を制御することができ、セキュアメモリ３１１など、該当する機能を有していないユーザ端末１の処理を制限することができる。

【００９６】

図８は、コンテンツ利用条件１５１の構成例を表している。なお、図８において、各行頭の数字と、コロン記号（：）は、説明の便宜上付加したものであり、コードの一部ではなく、先頭行および最終行の「…」は、前後にもコードがあることを示している。後述する図９乃至図１１でも同様である。また、図８の例の場合、コンテンツ利用条件１５１は、XrML(eXtensible Rights Mark-up Language)（http://www.xrml.org/）より記述されている。

【００９７】

第１行目の<?xml version="1.0" encoding="UTF-8" ?>は、第２行目以下に記述されるコンテンツ利用条件１５１が、XML形式のバージョン"1.0"で記述されており、UTF-8でエンコードされていることを表している。そして、図８の例においては、第２行目乃至第５行目の<license xmlns="urn:abc:contentsLicense" xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance xsi:schemaLocation="urn:abc:contentsLicense http://www.abc.com/contentsLicense.xsd" >から、第３４行目の</license>までの間に、コンテンツ利用条件がXML形式で記述される。このライセンス<license>は、XrMLのアクセス制御表現形式のベースとなるもので、以下に説明する、主体（権利付与の対象者）<user>、資源（対象コンテンツ）<digitalResource>、条件<allConditions>、操作<Action>により規則が表される。

【００９８】

第６行目乃至第１０行目の「<inventory> <digitalResource licensePartId="targetContent"> <nonSecureIndirect URI="urn:xyz:contents1"/> </digitalResource> </inventory>」には、対象の資源（コンテンツ）が、コンテンツＩＤ「URI="urn:xyz:contents1」で特定されるコンテンツであることが記述される。

【００９９】

第１１行目の<grantGroup>から、第３３行目の</grantGroup>までの間に、対象のコンテンツに対する権利の範囲が記述される。第１２行目の<user deviceID="stb1.abc.co.jp

"/>には、主体（権利付与の対象者）<user>がデバイスＩＤ「stb1.abc.co.jp」（セットトップボックス等）で特定されるユーザであることが記述される。このユーザが許可される権利の内容は、第１３行目の<grant>乃至第２２行目の</grant>、および第２３行目の<grant>乃至第３２行目の</grant>に記述されている。

【０１００】

第１３行目の<grant>乃至第２２行目の</grant>において、第１４行目の<play/>は、操作<Action>が再生「play」であることを表し、第１５行目の<digitalResource licensePartIdRef="targetContent"/>は、対象の資源<digitalResource>が、第８行目の「targetContent」に記述されるコンテンツＩＤであることを表し、第１６行目乃至第２１行目の「<allConditions> <validityInterval> <notBefore>2003-11-15T04:03:02</notBefore> <notAfter>2003-12-06T04:03:02</notAfter> </validityInterval> </allConditions>」は、条件<allConditions>として、有効期限「validityInterval」が2003年11月15日の4時03分02秒「2003-11-15T04:03:02」から、2003年12月6日の4時03分02秒「2003-12-06T04:03:02」であることを表している。

【０１０１】

第２３行目の<grant>乃至第３２行目の</grant>において、第２４行目の<copy/>は、操作<Action>がコピー「copy」であることを表し、第２５行目の<digitalResource licensePartIdRef="targetContent"/>は、対象の資源<digitalResource>が、第８行目の「targetContent」に記述されるコンテンツＩＤであることを表し、第２６行目乃至第３１行目の「<allConditions> <count>1</count> <recordingMedia> <memoryStick/> </recordingMedia> </allConditions>」は、条件<allConditions>として、記録メディア「recordingMedia」がメモリスティック（商標）「memoryStick」で、記録回数「count」が１回であることを表している。

【０１０２】

すなわち、図８のコンテンツ利用条件１５１は、デバイスＩＤ「stb1.abc.co.jp」で特定されるセットトップボックス等のユーザ端末１が、コンテンツＩＤ「URI="urn:xyz:contents1」のコンテンツを、有効期間内「2003年11月15日の4時03分02秒から、2003年12月6日の4時03分02秒まで」に再生「play」でき、かつ、記録メディア「memoryStick」に１回のみコピー「copy」できることを表している。

【０１０３】

次に、図９乃至図１１を参照して、XACML(eXtensible Access Control Language)(http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml)より記述されるメタデータ利用条件１６１の例を説明する。

【０１０４】

第１行目の<?xml version="1.0" encoding="UTF-8" ?>は、第２行目以下に記述されるメタデータ利用条件１６１が、XML形式のバージョン"1.0"で記述されており、UTF-8でエンコードされていることを表している。そして、第２行目乃至第７行目の「<Policy xmlns="urn:oasis:names:tc:xacml:1.0:policy" xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance xsi:schemaLocation="urn:oasis:names:tc:xacml:1.0:policy http://www.oasis-open.org/tc/xacml/1.0/cs-xacml-schema-policy-01.xsd" PolicyId="urn:metadataAccessControlPolicy1" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">」から、第６２行目の</Policy>までの間に、メタデータを利用するためのルール<Rule>がXML形式で記述される。

【０１０５】

第８行目乃至第１２行目の「<Target> <Subjects> <AnySubject/> </Subjects> <Resources> <AnySubject/> </Resources> <Actions> <AnyAction/> </Actions> </Target>は、第１３行目の<Rule RuleId="urn:metadtaAccessControlRule1" Effect="Permit">」から、第６１行目の</Rule>までの間に記述される、XrMLのアクセス制御表現形式のベースとなるルール（利用条件）<Rule>が、主体（権利付与の対象者）<subjects>、資源（対象メタデータ）<Resources>、および動作（操作）<Actions>に対する規則により構成されるこ

とを示している。

【０１０６】

第１５行目の<Subjects>から、第３７行目の</Subjects>までの間には、複数の主体に関する規則を記述することができ、この場合、第１６行目の<Subject>から、第３６行目の</Subject>までの間に１つの主体に関する３つの規則が記述されている。

【０１０７】

第１７行目乃至第２３行目の「<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match"> <SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="rfc822Name" /> <AttributeValue DataType="rfc822Name">abc.co.jp</AttributeValue> </SubjectMatch>」は、主体のＩＤ（識別子）属性「subject-id」に、「abc.co.jp」の文字列が含まれることを表している。第２４行目乃至第２９行目の「<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"> <SubjectAttributeDesignator AttributeId="urn:abc:xacml:subject:group" DataType="http://www.w3.org/2001/XMLSchema#string" /> <AttributeValue>subscriberGroup1</AttributeValue> </SubjectMatch>」は、主体のグループ属性「subject-group」が、「ubscriberGroup1」であることを表している。第３０行目乃至第３５行目の「<SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"> <SubjectAttributeDesignator AttributeId="urn:abc:xacml:subject:deviceSecurityLevel" DataType="http://www.w3.org/2001/XMLSchema#string" /> <AttributeValue>level1</AttributeValue> </SubjectMatch>」は、主体のデバイスセキュリティレベル属性「deviceSecurityLevel」が、レベル１「level1」であることを表している。

【０１０８】

第３８行目の<Resources>から、第４９行目の</Resources>までの間には、メタデータ利用条件１６１において、複数の対象となる資源（メタデータ）を記述することができ、この場合、第３９行目の<Resource>から、第４８行目の</Resource>までの間に１つの資源（メタデータ）が記述されている。

【０１０９】

すなわち、第４０行目乃至第４７行目の「<ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"> <ResourceAttributeDesignator AttributeId="urn:abc:xacml:resource:resource-uri" DataType="http://www.w3.org/2001/XMLSchema#anyURI"/> <AttributeValue> file://localhost/metadataInstanceRepository/metadataInstance1.xml </AttributeValue> </ResourceMatch>」は、資源のＩＤ（識別子）属性「resource-uri」が、「file://localhost/metadataInstanceRepository/metadataInstance1.xml」であることを表している。

【０１１０】

第５０行目の<Actions>から、第５９行目の</ Actions>までの間には、メタデータ利用条件１６１において、主体が資源をアクセスする操作方法を複数記述することができ、この場合、第５１行目の<Action>から、第５８行目の</Action>までの間に１つの操作方法が記述されている。

【０１１１】

すなわち、第５２行目乃至第５７行目の「<ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"> <ActionAttributeDesignatorAttributeId="urn:abc:xacml:action" DataType=" http://www.w3.org/2001/XMLSchema#string" /> <AttributeValue>read</AttributeValue> </ActionMatch>」は、操作方法「Action」が、「read」であることを表している。

【０１１２】

すなわち、図９乃至図１１のメタデータ利用条件１６１は、「abc.co.jp」が含まれるデバイスＩＤ（識別属性）のセットトップボックス（例えば、「stb1.abc.co.jp」）で、メタデータ取得契約クラス「ubscriberGroup1」で、かつ、デバイスセキュリティレベル「level1」であれば、メタデータＩＤ「file://localhost/metadataInstanceRepository/

metadataInstance1.xml」のメタデータを、「read」できるというルール（利用条件）を表している。

【０１１３】

図１２乃至図１５は、メタデータ２１の構成例を表している。メタデータ２１は、コンテンツのリリースや放送形態に依存しないコンテンツに関する一般的な情報であり、記述される情報に応じて、図１２のプログラムメタデータ、図１３のプログラムロケーションメタデータ、図１４のセグメンテーションメタデータ、および図１５のプログラムグループメタデータなどに分類される。

【０１１４】

図１２は、プログラムメタデータとしてのメタデータ２１の構成例を示している。プログラムメタデータは、番組を構成するコンテンツの単位であるプログラムについての情報により構成されるメタデータであり、コンテンツを検索する場合や、コンテンツの内容を知りたい場合などに利用される。

【０１１５】

図１２の例の場合、プログラムメタデータは、コンテンツのタイトル「title」、概要「Synopsis」、検索のためのキーワード「Keyword」、ドラマ、ニュースなどのジャンル「Genre」、コンテンツへのアクセスするための規制レベルの値であるペアレンタル・レーティング「ParentalRating」、音声の言語「Language」、出演者一覧「CastList」、関連する他の情報への参照「ReltatedMaterial」、制作年「ProductionYear」、制作国「ProductionCountry」、および、レビューや評価「Review」などにより構成される。

【０１１６】

図１３は、プログラムロケーションメタデータとしてのメタデータ２１の構成例を示している。プログラムロケーションメタデータは、コンテンツが、ネットワーク２などで配信される場合と、デジタル放送波で配信される場合では、配信される時間帯、放送チャンネル、登録（アーカイブ）されているコンテンツサーバ３などのアドレス、配信プロトコルやフォーマットが異なるために必要となるメタデータである。

【０１１７】

図１３の例の場合、プログラムロケーションメタデータは、コンテンツが登録されている位置情報としてのＵＲＬ「LocationURL」、登録されている符号化フォーマット「Format」、および、コンテンツが配信（取得）可能な開始時刻と終了時刻「StartDate/EndDate」などにより構成される。なお、プログラムロケーションメタデータとしては、他に、コンテンツが放送される場合のチャンネル、時刻、および生放送であるかなどの情報も記述される。

【０１１８】

図１４は、セグメントメタデータとしてのメタデータ２１の構成例を示している。セグメントメタデータは、異なるプログラムから派生する複数のセグメントを、１つのセグメントグループとしてまとめることができ、例えば、コンテンツのダイジェスト版などのように、コンテンツのハイライトシーンのみを集めたり、好きな俳優の出演場面だけを集めてオリジナル番組を構成する際に利用されるメタデータである。

【０１１９】

図１４の例の場合、セグメントメタデータは、コンテンツのタイトル「title」、概要「Synopsis」、検索のためのキーワード「Keyword」、プログラムの中でのセグメントの位置を示すキーフレーム「KeyFrame」、および、必要なセグメント区間の開始時刻と終了時刻「SegmentLocation」などにより構成される。

【０１２０】

図１５は、プログラムグループメタデータとしてのメタデータ２１の構成例を示している。プログラムグループメタデータは、複数のプログラムをまとめたプログラムグループについての情報により構成されるメタデータであり、プログラムグループ、例えば、シリーズ単位でコンテンツを検索する場合などに利用される。なお、プログラムグループの種類としては、番組のシリーズ「series」（例えば、エピソード１番からＮ番など）、番組

のシリーズをまとめたもの「show」（例えば、すべてのエピソードなど）、プログラムコンセプト「programconcept」（例えば、ディレクターズカットなど）、あるいは、プログラムを編集したものであるプログラムコンピレーション「programCompilation」（例えば、戦争に関するニューズセグメントを編集したもの）などがある。

【０１２１】

図１５の例の場合、プログラムグループメタデータは、コンテンツのタイトル「title」、概要「Synopsis」、検索のためのキーワード「Keyword」、ドラマ、ニュースなどのジャンル「Genre」、コンテンツへのアクセスするための規制レベルの値であるペアレンタル・レーティング「ParentalRating」、音声の言語「Language」、出演者一覧「CastList」、シリーズものなど関連コンテンツ「ReltatedMaterial」、制作年「ProductionYear」、制作国「ProductionCountry」、レビューや評価「Review」、およびグループの要素「GroupElement」などにより構成される。

【０１２２】

次に、図１６のフローチャートを参照して、コンテンツサーバ３の送信処理を説明する。例えば、後述する図２４のステップＳ２０６において、ユーザ端末１よりネットワーク２を介して、コンテンツ１１のコンテンツライセンス１２が要求される。

【０１２３】

コンテンツサーバ３の通信部３９は、コンテンツライセンス１２の要求を受信し、受信したコンテンツライセンス１２の要求を、ＣＰＵ３１に供給する。ＣＰＵ３１は、ステップＳ１において、コンテンツライセンス１２が要求されたと判定するまで待機しており、コンテンツライセンス１２が要求されたと判定した場合、ステップＳ２に進み、要求されたコンテンツ１１のコンテンツライセンス１２を記憶部３８から読み出し、読み出したコンテンツライセンス１２を、通信部３９を制御して、ネットワーク２を介して、ユーザ端末１に送信させる。

【０１２４】

これに対応して、図２４のステップＳ２１０において、ユーザ端末１よりコンテンツ１１の要求が送信されてくる。コンテンツサーバ３の通信部３９は、コンテンツ１１の要求を受信し、受信したコンテンツ１１の要求を、ＣＰＵ３１に供給する。ＣＰＵ３１は、ステップＳ３において、ユーザ端末１により、コンテンツ１１が要求されたか否かを判定し、コンテンツ１１が要求されたと判定した場合、ステップＳ４に進み、要求されたコンテンツ１１を記憶部３８から読み出し、読み出したコンテンツ１１を、通信部３９を制御して、ネットワーク２を介して、ユーザ端末１に送信させ、コンテンツ送信処理を終了する。

【０１２５】

ＣＰＵ３１は、ステップＳ３において、ユーザ端末１により、コンテンツ１１が要求されていないと判定した場合、送信処理を終了する。

【０１２６】

以上のようにして、コンテンツサーバ３から、ユーザ端末１には、コンテンツライセンス１２が送信され、コンテンツ１１が送信、提供される。

【０１２７】

なお、図１６の例においては、ユーザ端末１の要求に応じて、コンテンツライセンス１２およびコンテンツ１１を送信するように説明したが、コンテンツライセンス１２およびコンテンツ１１の送信タイミングについては、図１６の例に限らず、コンテンツライセンス１２と同時にコンテンツ１１を送信するようにしてもよいし、コンテンツ１１を送信した後に、コンテンツライセンス１２を送信するようにしてもよい。

【０１２８】

次に、図１７のフローチャートを参照して、メタデータサーバ４の送信処理を説明する。例えば、図１７の例においては、メタデータプロバイダによりメタデータ２１およびメタデータライセンス２２の配信時刻が予め設定されている。

【０１２９】

メタデータサーバ４のＣＰＵ３１は、ステップＳ２１において、内蔵するクロックで計時動作を行って、所定の時刻になったと判定するまで待機しており、所定の時刻になったと判定した場合、ステップＳ２２に進み、対象のメタデータ２１のメタデータライセンス２２を記憶部３８から読み出し、読み出したメタデータライセンス２２を、通信部３９を制御して、ネットワーク２を介して、ユーザ端末１に送信させ、ステップＳ２３に進む。

【０１３０】

ＣＰＵ３１は、ステップＳ２３において、対象のメタデータ２１を記憶部３８から読み出し、読み出したメタデータ２１を、通信部３９を制御して、ネットワーク２を介して、ユーザ端末１に送信させ、送信処理を終了する。

【０１３１】

以上のようにして、メタデータサーバ４から、ユーザ端末１には、メタデータライセンス２２およびメタデータ２１が送信、提供される。

【０１３２】

なお、図１７の例においては、所定の時刻になった場合に、メタデータライセンス２２およびメタデータ２１を送信するように説明したが、メタデータライセンス２２およびメタデータ２１の送信タイミングについては、図１７の例に限らず、図１６のコンテンツと同様に、ユーザの要求に応じてメタデータライセンス２２およびメタデータ２１を順に送信するようにしてもよいし、メタデータ２１を送信した後に、メタデータライセンス２２を送信するようにしてもよい。

【０１３３】

次に、図１８のフローチャートを参照して、ユーザ端末１のメタデータ蓄積処理について説明する。例えば、図１７のステップＳ２２およびＳ２３において、メタデータサーバ４により、メタデータライセンス２２およびメタデータ２１がネットワーク２を介してユーザ端末１に送信される。メタデータライセンス２２は、メタデータプロバイダのＰＫＩに基づいたメタデータプロバイダ暗号鍵で暗号化されており、メタデータ２１は、メタデータ暗号鍵１６２で暗号化されている。

【０１３４】

ユーザ端末１の受信部１０１は、ステップＳ４１において、メタデータサーバ４からのメタデータライセンス２２を受信し、受信したメタデータライセンス２２を、メタデータライセンス復号部２０１に供給し、ステップＳ４２に進む。また、受信部１０１は、ステップＳ４２において、メタデータサーバ４からのメタデータ２１を受信し、受信したメタデータ２１を、メタデータ復号部２１１に供給し、ステップＳ４３に進む。

【０１３５】

ステップＳ４３において、メタデータライセンス復号部２０１は、予め取得しているメタデータプロバイダ公開鍵１７１を用いて、受信部１０１より供給されたメタデータライセンス２２の暗号を解除し、メタデータ利用条件１６１およびメタデータ暗号鍵１６２に分けて、メタデータ利用条件１６１およびメタデータ暗号鍵１６２を、利用条件判定処理部２０２に供給し、ステップＳ４４に進む。

【０１３６】

利用条件判定処理部２０２は、ステップＳ４４において、メタデータライセンス復号部２０１からのメタデータ利用条件１６１が、ユーザ端末１を権利付与の対象とするものであり、さらに、権利行使の条件として、セキュリティレベルがレベル１で、検索許可であるか否かを判定する。

【０１３７】

利用条件判定処理部２０２は、ステップＳ４４において、メタデータ利用条件１６１が、ユーザ端末１を権利付与の対象とするものであり、セキュリティレベルがレベル１で、検索許可であると判定した場合、ステップＳ４５に進み、メタデータ暗号鍵１６２をメタデータ復号部２１１に供給するとともに、メタデータ復号部２１１を制御し、受信部１０１より供給されたメタデータ２１の暗号を解除（復号）させ、ステップＳ４６に進み、メタデータ復号部２１１を制御し、暗号解除されたメタデータ２１を、メタデータＤＢ２１

２のセキュアメモリ３０１内に展開、蓄積させる。すなわち、メタデータ復号部２１１は、ステップＳ４６において、暗号解除されたメタデータ２１を、インデックステーブル３１１とデータブロック３１２に分けて、メタデータＤＢ２１２－１のセキュアメモリ３０１内に展開、蓄積し、メタデータ蓄積処理を終了する。

【０１３８】

利用条件判定処理部２０２は、ステップＳ４４において、メタデータ利用条件１６１が、ユーザ端末１を権利付与の対象とするものではない、セキュリティレベルがレベル１ではない、または検索許可ではないと判定した場合、ステップＳ４７に進み、メタデータ利用条件１６１が、ユーザ端末１を権利付与の対象とするものであり、セキュリティレベルがレベル２で、検索許可であるか否かを判定する。

【０１３９】

利用条件判定処理部２０２は、ステップＳ４７において、メタデータ利用条件１６１が、ユーザ端末１を権利付与の対象とするものであり、セキュリティレベルがレベル２で、検索許可であると判定した場合、ステップＳ４８に進み、メタデータ暗号鍵１６２をメタデータ復号部２１１に供給するとともに、メタデータ復号部２１１を制御し、受信部１０１より供給されたメタデータ２１の暗号を解除させ、ステップＳ４９に進み、メタデータ復号部２１１を制御し、暗号解除されたメタデータ２１を、メタデータＤＢ２１２のセキュアメモリ３０１およびセキュアハードディスク３０３内に展開、蓄積させる。すなわち、メタデータ復号部２１１は、ステップＳ４９において、暗号解除されたメタデータ２１を、インデックステーブル３１１とデータブロック３１２に分けて、インデックステーブル３１１をメタデータＤＢ２１２－２のセキュアメモリ３０１内に展開、蓄積し、データブロック３１２をメタデータＤＢ２１２－２のセキュアハードディスク３０３内に展開、蓄積し、メタデータ蓄積処理を終了する。

【０１４０】

利用条件判定処理部２０２は、ステップＳ４７において、メタデータ利用条件１６１が、ユーザ端末１を権利付与の対象とするものではない、セキュリティレベルがレベル２ではない、または、検索許可ではないと判定した場合、ステップＳ５０に進み、メタデータ利用条件１６１が、ユーザ端末１を権利付与の対象とするものであり、セキュリティレベルがレベル３で、検索許可であるか否かを判定する。

【０１４１】

利用条件判定処理部２０２は、ステップＳ５０において、メタデータ利用条件１６１が、ユーザ端末１を権利付与の対象とするものであり、セキュリティレベルがレベル３で、検索許可であると判定した場合、ステップＳ５１に進み、メタデータ暗号鍵１６２をメタデータ復号部２１１に供給するとともに、メタデータ復号部２１１を制御し、受信部１０１より供給されたメタデータ２１の暗号を解除させ、ステップＳ５２に進み、メタデータ復号部２１１を制御し、暗号解除されたメタデータ２１のインデックステーブル３１１を、メタデータＤＢ２１２のセキュアメモリ３０１内に展開させ、ステップＳ５３に進み、メタデータ２１のデータブロック３１２を再度暗号化させて、メタデータＤＢ２１２の通常ハードディスク３０４内に蓄積させる。

【０１４２】

すなわち、メタデータ復号部２１１は、ステップＳ５２において、暗号解除されたメタデータ２１を、インデックステーブル３１１とデータブロック３１２に分けて、インデックステーブル３１１をメタデータＤＢ２１２－３のセキュアメモリ３０１内に展開、蓄積し、ステップＳ５３に進み、データブロック３１２を再度暗号化して、暗号化されたデータブロック３１２を、メタデータＤＢ２１２－３の通常ハードディスク３０４内に蓄積し、メタデータ蓄積処理を終了する。

【０１４３】

利用条件判定処理部２０２は、ステップＳ５０において、メタデータ利用条件１６１が、ユーザ端末１を権利付与の対象とするものではない、セキュリティレベルがレベル３ではない、または、検索許可ではないと判定した場合、ステップＳ５４に進み、メタデータ

利用条件１６１が、ユーザ端末１を権利付与の対象とするものであり、セキュリティレベルがレベル４で、検索許可であるか否かを判定する。

【０１４４】

利用条件判定処理部２０２は、ステップＳ５４において、メタデータ利用条件１６１が、ユーザ端末１を権利付与の対象とするものであり、セキュリティレベルがレベル４で、検索許可であると判定した場合、ステップＳ５５に進み、メタデータ暗号鍵１６２をメタデータ復号部２１１に供給するとともに、メタデータ復号部２１１を制御し、受信部１０１より供給されたメタデータ２１の暗号を解除させ、ステップＳ５６に進み、メタデータ復号部２１１に、暗号解除されたメタデータ２１を、インデックステーブル３１１とデータブロック３１２に分けて、メタデータＤＢ２１２のセキュアハードディスク３０３内に展開、蓄積させる。

【０１４５】

すなわち、メタデータ復号部２１１は、ステップＳ５６において、暗号解除されたメタデータ２１を、インデックステーブル３１１とデータブロック３１２に分けて、インデックステーブル３１１およびデータブロック３１２を、メタデータＤＢ２１２－４のセキュアハードディスク３０３内に蓄積し、メタデータ蓄積処理を終了する。

【０１４６】

一方、利用条件判定処理部２０２は、ステップＳ５４において、メタデータ利用条件１６１が、ユーザ端末１を権利付与の対象とするものではない、セキュリティレベルがレベル４ではない、または、検索許可ではないと判定した場合、メタデータを復号すること、蓄積することなく、メタデータ蓄積処理を終了する。

【０１４７】

以上のように、ユーザ端末１において、メタデータ２１は、メタデータＤＢ２１２内の、メタデータ利用条件１６１のセキュリティレベルに応じた耐タンパな領域、または、耐タンパではない通常の領域に展開蓄積される。したがって、メタデータは、メタデータ利用条件１６１のセキュリティレベルに応じて、盗聴されることが抑制される。また、各セキュリティレベルの耐タンパ領域を有しないユーザ端末１の場合には、メタデータの展開、蓄積が禁止される。

【０１４８】

なお、図１８の例においては、検索許可が判定される場合のため、メタデータ２１を暗号解除、展開して蓄積するように説明したが、これに対して、蓄積許可の場合には、メタデータ２１は、暗号解除や展開されず、メタデータ利用条件１６１のセキュリティレベルに応じた所定の領域に暗号化された状態で蓄積されるようにしてもよい。

【０１４９】

次に、図１９のフローチャートを参照して、ユーザ端末１に蓄積されているメタデータ２１を用いて、コンテンツを検索するコンテンツ検索処理を説明する。ユーザは、入力部３６を構成するマウスまたはキーボードなどを操作することにより、所望のコンテンツを検索するためのキーワードなどを入力する。

【０１５０】

利用条件判定処理部２０２は、ステップＳ８１において、キーワード検索の要求があったと判定するまで待機しており、ユーザの操作により、入力部３６を介して入力される操作信号に基づいて、キーワード検索の要求があったと判定した場合、ステップＳ８２に進み、メタデータＤＢ２０２に蓄積（展開）されているメタデータ２１のメタデータ利用条件１６１がセキュリティレベル１であるか否かを判定し、メタデータ２１のメタデータ利用条件１６１がセキュリティレベル１であると判定した場合、ステップＳ８３に進み、メタデータ検索部２１３を制御し、セキュリティレベル１のメタデータＤＢ検索処理を実行させる。

【０１５１】

このメタデータＤＢの検索処理は、図２０を参照して説明するが、ステップＳ８３の処理により、メタデータＤＢ２１２－１のインデックステーブル３１１から、キーワードに

対応するメタデータが検索され、データブロック３１２から、検索されたメタデータに対応するデータブロックが特定され、特定されたデータブロックに基づいて、コンテンツの検索結果情報が生成され、処理は、ステップＳ８９に進む。

【０１５２】

利用条件判定処理部２０２は、ステップＳ８２において、メタデータ２１のメタデータ利用条件１６１がセキュリティレベル１ではないと判定した場合、ステップＳ８４に進み、メタデータＤＢ２０２に蓄積されているメタデータ２１のメタデータ利用条件１６１がセキュリティレベル２であるか否かを判定し、メタデータ２１のメタデータ利用条件１６１がセキュリティレベル２であると判定した場合、ステップＳ８５に進み、メタデータ検索部２１３を制御し、セキュリティレベル２のメタデータＤＢ検索処理を実行させる。

【０１５３】

このメタデータＤＢの検索処理は、図２１を参照して説明するが、ステップＳ８５の処理により、メタデータＤＢ２１２－２のインデックステーブル３１１から、キーワードに対応するメタデータが検索され、データブロック３１２から、検索されたメタデータに対応するデータブロックが特定され、特定されたデータブロックに基づいて、コンテンツの検索結果情報が生成され、処理は、ステップＳ８９に進む。

【０１５４】

利用条件判定処理部２０２は、ステップＳ８４において、メタデータ２１のメタデータ利用条件１６１がセキュリティレベル２ではないと判定した場合、ステップＳ８６に進み、メタデータＤＢ２０２に蓄積されているメタデータ２１のメタデータ利用条件１６１がセキュリティレベル３であるか否かを判定し、メタデータ２１のメタデータ利用条件１６１がセキュリティレベル３であると判定した場合、ステップＳ８７に進み、メタデータ検索部２１３を制御し、セキュリティレベル３のメタデータＤＢ検索処理を実行させる。

【０１５５】

このメタデータＤＢの検索処理は、図２２を参照して説明するが、ステップＳ８７の処理により、メタデータＤＢ２１２－３のインデックステーブル３１１から、キーワードに対応するメタデータが検索され、データブロック３１２から、検索されたメタデータに対応するデータブロックが特定され、特定されたデータブロックの暗号が解除され、暗号が解除されたデータブロックに基づいて、コンテンツの検索結果情報が生成され、処理は、ステップＳ８９に進む。

【０１５６】

利用条件判定処理部２０２は、ステップＳ８６において、メタデータ２１のメタデータ利用条件１６１がセキュリティレベル３ではない（すなわち、メタデータ２１のメタデータ利用条件１６１がセキュリティレベル４である）と判定した場合、ステップＳ８８に進み、メタデータ検索部２１３を制御し、セキュリティレベル４のメタデータＤＢ検索処理を実行させる。

【０１５７】

このメタデータＤＢの検索処理は、図２３を参照して説明するが、ステップＳ８７の処理により、メタデータＤＢ２１２－４のインデックステーブル３１１からインデックステーブル３１３が展開され、インデックステーブル３１３から、キーワードに対応するメタデータが検索され、データブロック３１２から、検索されたメタデータに対応するデータブロックが特定され、特定されたデータブロックに基づいて、コンテンツの検索結果情報が生成され、処理は、ステップＳ８９に進む。

【０１５８】

メタデータ検索部２１３は、ステップＳ８９において、コンテンツの検索結果を、メタデータ表示制御部２１４に供給し、ステップＳ９０に進む。メタデータ表示制御部２１４は、ステップＳ９０において、メタデータ検索部２１３からのコンテンツの検索結果に対応する画像を、出力部３７を構成するモニタに表示させ、メタデータ検索処理を終了する。

【０１５９】

なお、上述したコンテンツの検索処理において、キーワードに対応するメタデータ２１がユーザ端末１内にないとされた場合には、メタデータ表示制御部２１４に、キーワードに該当するものがないという情報を表示させたり、あるいは、ネットワーク２上より検索するか否かをユーザに選択させるような情報を表示させ、ユーザの操作に応じて、ネットワーク２上のメタデータサーバ４から該当するメタデータ２１を検索し、所望のメタデータ２１を取得するようにしてもよい。

【０１６０】

次に、図２０のフローチャートを参照して、図１９のステップＳ８３のセキュリティレベル１のメタデータＤＢ検索処理を説明する。セキュリティレベル１の場合、メタデータ２１のインデックステーブル３１１およびデータブロック３１２は、メタデータＤＢ２１２－１のセキュアメモリ３０１に展開されている。

【０１６１】

利用条件判定処理部２０２を介して、検索対象のキーワードが入力されると、メタデータ検索部２１３は、ステップＳ１２１において、メタデータＤＢ２１２－１のセキュアメモリ３０１に展開されているインデックステーブル３１１から、キーワードに対応するメタデータを検索し、ステップＳ１２２に進む。

【０１６２】

ステップＳ１２２において、メタデータ検索部２１３は、インデックステーブル３１１に、キーワードに対応するメタデータがあったか否かを判定し、インデックステーブル３１１に、キーワードに対応するメタデータがあったと判定した場合、ステップＳ１２３に進み、セキュアメモリ３０１から、検索されたメタデータに対応するデータブロック３１２を特定し、特定したデータブロック３１２を取得し、ステップＳ１２４に進む。

【０１６３】

一方、ステップＳ１２２において、メタデータ検索部２１３は、インデックステーブル３１１に、キーワードに対応するメタデータがないと判定した場合、ステップＳ１２３の処理をスキップし、ステップＳ１２４に進む。メタデータ検索部２１３は、ステップＳ１２４において、取得したデータブロック３１２、または、キーワードに対応するメタデータがないという判定結果に基づいて、コンテンツの検索結果情報を生成し、メタデータＤＢ検索処理を終了し、図１９のステップＳ８９に戻る。

【０１６４】

次に、図２１のフローチャートを参照して、図１９のステップＳ８５のセキュリティレベル２のメタデータＤＢ検索処理を説明する。セキュリティレベル２の場合、メタデータ２１のインデックステーブル３１１は、メタデータＤＢ２１２－２のセキュアメモリ３０１に展開されており、データブロック３１２は、セキュアハードディスク３０３に展開されている。

【０１６５】

利用条件判定処理部２０２を介して、検索対象のキーワードが入力されると、メタデータ検索部２１３は、ステップＳ１４１において、メタデータＤＢ２１２－２のセキュアメモリ３０１に展開されているインデックステーブル３１１から、キーワードに対応するメタデータを検索し、ステップＳ１４２に進む。

【０１６６】

ステップＳ１４２において、メタデータ検索部２１３は、インデックステーブル３１１に、キーワードに対応するメタデータがあったか否かを判定し、インデックステーブル３１１に、キーワードに対応するメタデータがあったと判定した場合、ステップＳ１４３に進み、セキュアハードディスク３０３から、検索されたメタデータに対応するデータブロック３１２を特定し、特定したデータブロック３１２を取得し、ステップＳ１４４に進む。

【０１６７】

一方、ステップＳ１４２において、メタデータ検索部２１３は、インデックステーブル３１１に、キーワードに対応するメタデータがないと判定した場合、ステップＳ１４３の

処理をスキップし、ステップＳ１４４に進む。メタデータ検索部２１３は、ステップＳ１４４において、取得したデータブロック３１２、または、キーワードに対応するメタデータがないという判定結果に基づいて、コンテンツの検索結果を生成し、メタデータＤＢ検索処理を終了し、図１９のステップＳ８９に戻る。

【０１６８】

次に、図２２のフローチャートを参照して、図１９のステップＳ８７のセキュリティレベル３のメタデータＤＢ検索処理を説明する。セキュリティレベル３の場合、メタデータ２１のインデックステーブル３１１は、メタデータＤＢ２１２－３のセキュアメモリ３０１に展開されており、データブロック３１２は、通常ハードディスク３０４に暗号化されて蓄積されている。

【０１６９】

利用条件判定処理部２０２を介して入力されるキーワード検索の操作信号に基づいて、メタデータ検索部２１３は、ステップＳ１６１において、メタデータＤＢ２１２のセキュアメモリ３０１に展開されているインデックステーブル３１１から、キーワードに対応するメタデータを検索し、ステップＳ１６２に進む。

【０１７０】

ステップＳ１６２において、メタデータ検索部２１３は、インデックステーブル３１１に、キーワードに対応するメタデータがあったか否かを判定し、インデックステーブル３１１に、キーワードに対応するメタデータがあったと判定した場合、ステップＳ１６３に進み、通常ハードディスク３０４から、検索されたメタデータに対応するデータブロック３１２を特定し、特定したデータブロック３１２を、データ復号部２１１に出力し、ステップＳ１６４に進む。

【０１７１】

データ復号部２１１は、ステップＳ１６４において、暗号化されたデータブロック３１２を入力すると、データブロック３１２の暗号を解除し、データ検索部２１３に供給し、ステップＳ１６５に進む。

【０１７２】

一方、ステップＳ１６２において、メタデータ検索部２１３は、インデックステーブル３１１に、キーワードに対応するメタデータがないと判定した場合、ステップＳ１４３の処理をスキップし、ステップＳ１６５に進む。メタデータ検索部２１３は、ステップＳ１６５において、データブロック３１２、または、キーワードに対応するメタデータがないという判定結果に基づいて、メタデータの検索結果情報を生成し、メタデータＤＢ検索処理を終了し、図１９のステップＳ８９に戻る。

【０１７３】

次に、図２３のフローチャートを参照して、図１９のステップＳ８８のセキュリティレベル４のメタデータＤＢ検索処理を説明する。セキュリティレベル４の場合、メタデータ２１のインデックステーブル３１１およびデータブロック３１２は、メタデータＤＢ２１２－４のセキュアハードディスク３０３に展開されている。

【０１７４】

利用条件判定処理部２０２を介して、検索対象のキーワードが入力されると、メタデータ検索部２１３は、ステップＳ１８１において、メタデータＤＢ２１２－４のセキュアハードディスク３０３のインデックステーブル３１１を、通常メモリ３０２にインデックステーブル３１３として展開させ、ステップＳ１８２に進み、メタデータＤＢ２１２－４の通常メモリ３０２に展開されているインデックステーブル３１３から、キーワードに対応するメタデータを検索し、ステップＳ１８３に進む。

【０１７５】

ステップＳ１８３において、メタデータ検索部２１３は、インデックステーブル３１１に、キーワードに対応するメタデータがあったか否かを判定し、インデックステーブル３１１に、キーワードに対応するメタデータがあったと判定した場合、ステップＳ１８４に進み、セキュアハードディスク３０３から、検索されたメタデータに対応するデータブロ

ック３１２を特定し、特定したデータブロック３１２を取得し、ステップＳ１８５に進む。

【０１７６】

一方、ステップＳ１８３において、メタデータ検索部２１３は、インデックステーブル３１１に、キーワードに対応するメタデータがないと判定した場合、ステップＳ１８４の処理をスキップし、ステップＳ１８５に進む。メタデータ検索部２１３は、ステップＳ１４４において、取得したデータブロック３１２、または、キーワードに対応するメタデータがないという判定結果に基づいて、メタデータの検索結果情報を生成し、ステップＳ１８６に進む。

【０１７７】

ステップＳ１８６において、メタデータ検索部２１３は、メタデータＤＢ２１２－４の通常メモリ３０２に展開したインデックステーブル３１３を消去し、メタデータＤＢ検索処理を終了し、図１９のステップＳ８９に戻る。

【０１７８】

以上のように、ユーザ端末１においては、コンテンツ１１の検索処理は、メタデータ利用条件１６１のセキュリティレベルに応じてメタデータＤＢに蓄積されているメタデータ２１を処理し、処理されたメタデータ２１を検索することにより実行される。したがって、ユーザ端末１は、メタデータＤＢ２１２のセキュリティレベルに応じた安全性および検索速度での処理を実行することができる。これにより、ユーザ端末１において、セキュリティを必要とするメタデータは、盗聴されるような安全ではない領域で処理されることが抑制され、メタデータの著作権保護を推進することができる。

【０１７９】

次に、図２４のフローチャートを参照して、コンテンツ再生処理を説明する。ユーザは、図１９のコンテンツ検索処理の結果を参照し、入力部３６を構成するマウスなどを操作することにより、所望のコンテンツを指定する。

【０１８０】

ステップＳ２０１において、利用条件判定処理部２２２は、コンテンツが要求されると判定するまで待機しており、ユーザの操作により、入力部３６を介して入力される操作信号に基づいて、コンテンツが要求されたと判定した場合、ステップＳ２０２に進み、コンテンツＩＤに基づいて、要求されたコンテンツ１１のコンテンツライセンス１２があるか否かを判定し、コンテンツライセンス１２があると判定した場合、ステップＳ２０３に進む。

【０１８１】

利用条件判定処理部２２２は、ステップＳ２０３において、コンテンツライセンス１２のコンテンツ利用条件１５１に基づいて、ユーザ端末１によるコンテンツの再生が許可されているか否かを判定し、ユーザ端末１によるコンテンツの再生が許可されていると判定した場合、ステップＳ２０４に進み、コンテンツ復号部２３４に、コンテンツ暗号鍵１５２を供給し、コンテンツ検索部２３３およびコンテンツ復号部２３４にコンテンツＩＤのコンテンツ再生を指示し、ステップＳ２０５に進む。

【０１８２】

コンテンツ検索部２３３は、ステップＳ２０５において、供給されたコンテンツＩＤのコンテンツがコンテンツ記憶部２３２にあると判定した場合、ステップＳ２１１に進む。コンテンツ検索部２３３は、ステップＳ２０５において、供給されたコンテンツＩＤのコンテンツがコンテンツ記憶部２３２にないと判定した場合、ステップＳ２１０に進む。

【０１８３】

一方、利用条件判定処理部２２２は、ステップＳ２０２において、コンテンツＩＤに基づいて、コンテンツライセンス２２がないと判定した場合、ステップＳ２０６において、コンテンツ検索部２３３を制御し、コンテンツＩＤに基づいて、送信部１０５に、ネットワーク２のコンテンツサーバ３に対して、コンテンツＩＤのコンテンツライセンス１２を取得させ、ステップＳ２０７に進む。

【０１８４】
これに対応して、コンテンツサーバ３は、図１６のステップＳ２において、コンテンツライセンス１２をネットワーク２を介して送信してくる。コンテンツライセンス１２は、コンテンツプロバイダのＰＫＩに基づいたコンテンツプロバイダ秘密鍵で暗号化されている。受信部１０１は、コンテンツサーバ３からのコンテンツライセンス１２を受信し、コンテンツライセンス復号部２２１に供給する。
【０１８５】
コンテンツライセンス復号部２２１は、ステップＳ２０７において、予め取得済みのコンテンツプロバイダ公開鍵１７２で、受信部１０１からのコンテンツライセンス１２の暗号を解除し、コンテンツ利用条件１５１とコンテンツ暗号鍵１５２に分けて、利用条件判定処理部２２２に供給する。利用条件判定処理部２２２は、ステップＳ２０８において、コンテンツ利用条件１５１に基づいて、ユーザ端末１によるコンテンツの再生が許可されているか否かを判定し、ユーザ端末１によるコンテンツの再生が許可されていると判定した場合、ステップＳ２０９において、コンテンツ復号部２３４に、コンテンツ暗号鍵１５２を供給し、コンテンツ検索部２３３およびコンテンツ復号部２３４にコンテンツＩＤのコンテンツ再生を指示し、ステップＳ２１０に進む。
【０１８６】
ステップＳ２１０において、コンテンツ検索部２３３は、再生が許可されているコンテンツＩＤに基づいて、送信部１０５に、ネットワーク２のコンテンツサーバ３に対して、コンテンツＩＤのコンテンツ１１を取得させ、ステップＳ２１１に進む。
【０１８７】
これに対応して、コンテンツサーバ３は、図１６のステップＳ４において、コンテンツ１１をネットワーク２を介して送信してくる。コンテンツライセンス１１は、コンテンツ暗号鍵１５２で暗号化されている。受信部１０１は、コンテンツサーバ３からのコンテンツライセンス１２を受信し、コンテンツ蓄積部２３１に供給する。コンテンツ蓄積部２３１は、利用条件判定処理部２２２のコンテンツ利用条件１５１に基づいた判定結果のもと、コンテンツＩＤのコンテンツ１１を、コンテンツ記憶部２３２に蓄積する。
【０１８８】
ステップＳ２１１において、コンテンツ復号部２３４は、利用条件判定処理部２２２からのコンテンツ暗号鍵１５２を用いて、耐タンパ領域で、コンテンツ記憶部２３２に蓄積されるコンテンツ１１の暗号を解除し、暗号が解除されたコンテンツ１１を、コンテンツ表示制御部２３５に出力し、ステップＳ２１２に進む。
【０１８９】
コンテンツ表示制御部２３５は、ステップＳ２１２において、コンテンツ復号部２３４からのコンテンツ１１を再生し、出力部３７を構成するモニタに表示させ、コンテンツ再生処理を終了する。
【０１９０】
ステップＳ２０３およびＳ２０８において、コンテンツＩＤの再生がユーザ端末１において許可されていないと判定された場合、利用条件判定処理部２２２は、コンテンツ再生処理を終了させる。
【０１９１】
以上のように、コンテンツ利用条件１５１とは別に、コンテンツとは異なるタイミングで、異なる処理を行うメタデータに、メタデータ利用条件１６１を設けて、メタデータ利用条件１６１に応じて、メタデータの蓄積、展開などの処理を制御するようにしたので、著作権保護の必要なメタデータを、コンテンツの検索時よりも先に展開するようにしても、コストに応じたセキュリティを維持することができる。すなわち、高価な耐タンパなメモリやハードディスクにかかるコストを、セキュリティに応じて最小限に抑えることができる。
【０１９２】
また、メタデータの内容に応じて、ユーザ端末１を制限するだけでなく、ユーザ端末１

における処理のセキュリティレベルを制限するようにしたので、それに応じた処理をユーザ端末１にさせたり、セキュリティレベル以下のユーザ端末１でのメタデータの処理を禁止することができる。したがって、メタデータの種類に応じた運用ができ、メタデータの流通および利用を促進させることができる。

【０１９３】

なお、上記説明においては、コンテンツ１１、コンテンツライセンス１２、メタデータ２１、およびメタデータライセンス２２を、ネットワーク２を介して提供する場合を説明したが、本発明は、ネットワーク２に限らず、地上波デジタルなどの放送波にも適用することができる。すなわち、コンテンツライセンス１２、メタデータ２１、およびメタデータライセンス２２は、放送波に多重されて送信されるようにしてもよい。なお、この場合、ユーザ端末１は、放送波を受信するためのチューナなどを有する。

【０１９４】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【０１９５】

コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図２に示されるように、磁気ディスク４１（フレキシブルディスクを含む）、光ディスク４２（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク４３（MD(Mini-Disc)（商標）を含む）、もしくは半導体メモリ４４などよりなるパッケージメディア、または、プログラムが一時的もしくは永続的に格納される記憶部３８などにより構成される。

【０１９６】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０１９７】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【図面の簡単な説明】

【０１９８】

【図１】本発明のコンテンツ提供システムの構成例を示す図である。

【図２】図１のユーザ端末の構成例を示すブロック図である。

【図３】図１のユーザ端末の機能構成例を示すブロック図である。

【図４】図３のユーザ端末の詳細な機能構成例を示すブロック図である。

【図５】メタデータ利用条件の構成例を示す図である。

【図６】メタデータＤＢの構成要素とセキュリティレベルの対応関係を説明する図である。

【図７】図６のセキュリティレベルに応じた図４のメタデータＤＢの構成例を示すブロックである。

【図８】コンテンツ利用条件の構成例を示す図である。

【図９】メタデータ利用条件の構成例を示す図である。

【図１０】メタデータ利用条件の構成例を示す図である。

【図１１】メタデータ利用条件の構成例を示す図である。

【図１２】プログラムメタデータの構成例を示す図である。

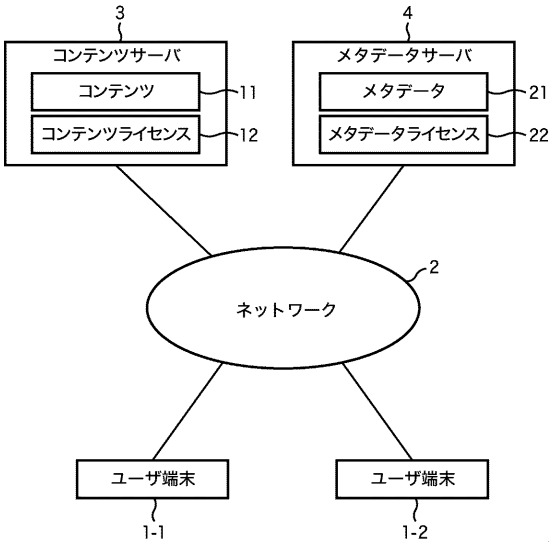
【図１３】プログラムロケーションメタデータの構成例を示す図である。

【図１４】セグメンテーションメタデータの構成例を示す図である。

【図１５】プログラムグループメタデータの構成例を示す図である。
【図１６】図１のコンテンツサーバの送信処理を説明するフローチャートである。
【図１７】図１のメタデータサーバの送信処理を説明するフローチャートである。
【図１８】図１のユーザ端末のメタデータ蓄積処理を説明するフローチャートである。
【図１９】図１のユーザ端末のコンテンツ検索処理を説明するフローチャートである。
【図２０】図１９のステップＳ８３のセキュリティレベル１のメタデータＤＢの検索処理を説明するフローチャートである。
【図２１】図１９のステップＳ８５のセキュリティレベル２のメタデータＤＢの検索処理を説明するフローチャートである。
【図２２】図１９のステップＳ８７のセキュリティレベル３のメタデータＤＢの検索処理を説明するフローチャートである。
【図２３】図１９のステップＳ８８のセキュリティレベル４のメタデータＤＢの検索処理を説明するフローチャートである。
【図２４】図１のユーザ端末のコンテンツ再生処理を説明するフローチャートである。
【符号の説明】
【０１９９】
１－１，１－２　ユーザ端末，２　ネットワーク，３　コンテンツサーバ，４　メタデータサーバ，１１　コンテンツ，１２　コンテンツライセンス１２　メタデータ，２２　メタデータライセンス，１０１　受信部，１０２　ＤＲＭ制御部，１０３　メタデータ処理部，１０４　コンテンツ処理部，１０５　送信部，１１１　メタデータ利用条件判定部，１１２　コンテンツ利用条件判定部，１５１　コンテンツ利用条件，１６１　メタデータ，２０１　メタデータライセンス復号部，２０２　利用条件判定処理部，２１１　メタデータ復号部，２１２　メタデータＤＢ，２１３　メタデータ検索部，２１４　メタデータ表示制御部，２２１　コンテンツライセンス復号部，２２２　利用条件判定処理部，２３１　コンテンツ蓄積部，２３２　コンテンツ記憶部，２３３　コンテンツ検索部，２３４　コンテンツ復号部，２３５　コンテンツ表示制御部

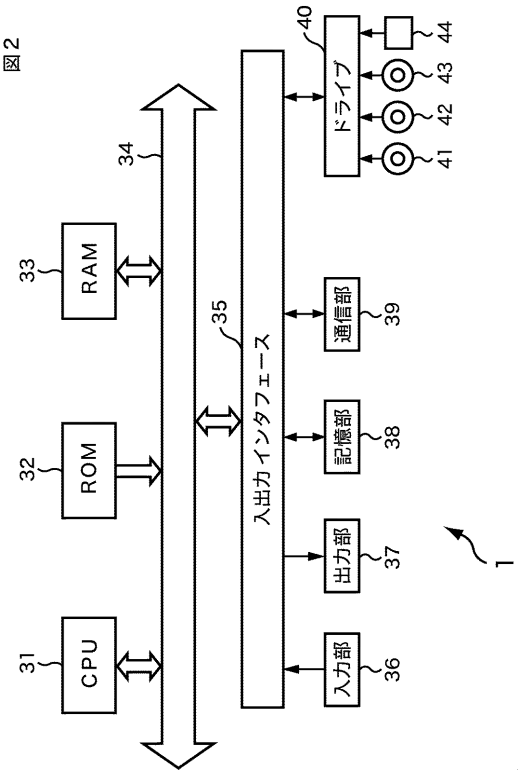
【図１】

図1



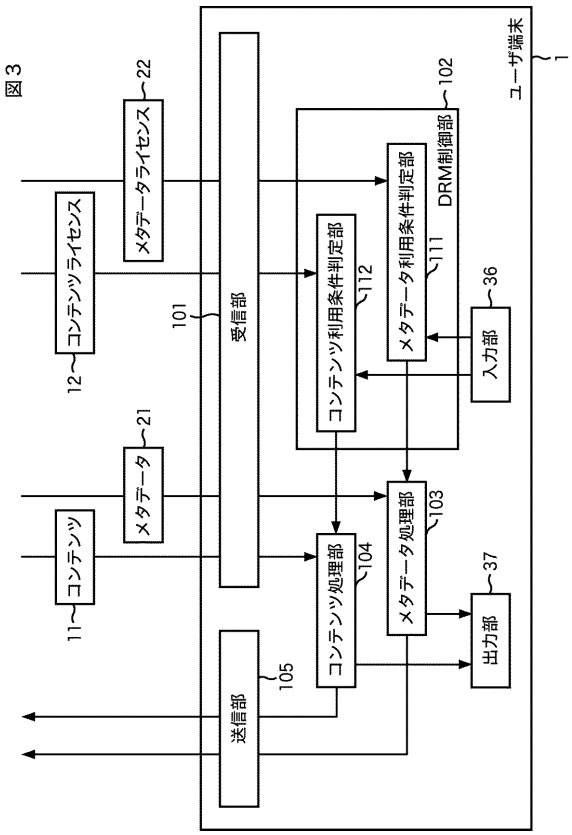
【図２】

図2



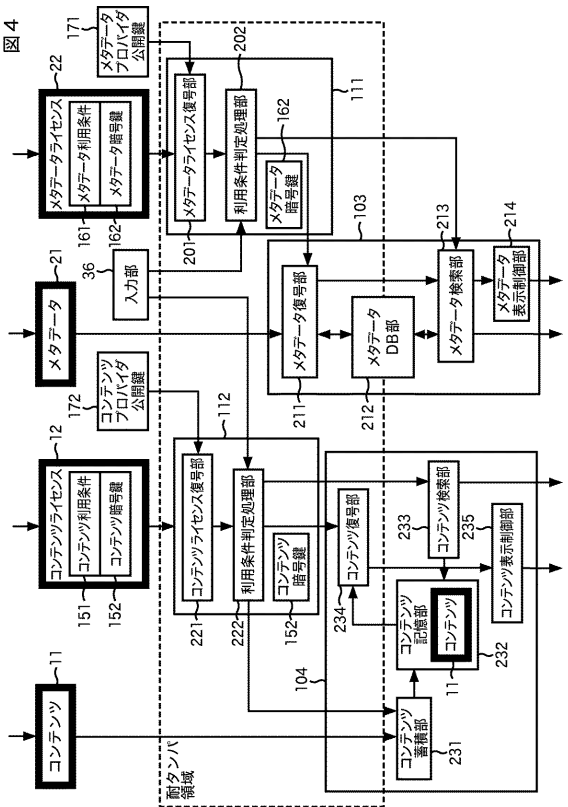
【図３】

図3



【図４】

図4



【図５】

図５

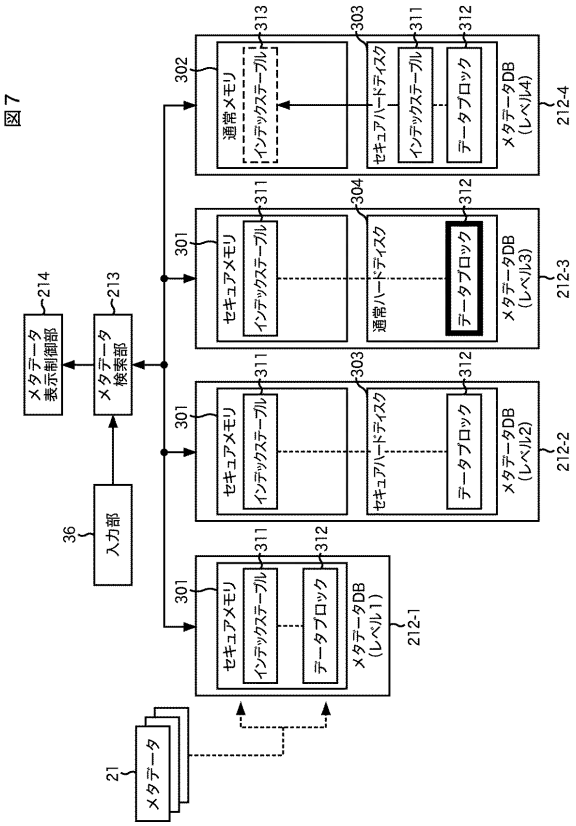
メタデータID
権利付与の対象者：(ユーザ名/ユーザクラス名)
操作の対象要素：(要素名)
権利行使の条件：
デバイスセキュリティクラス：レベル-X
操作クラス：ディスクに蓄積

【図６】

図６

セキュリティレベル	構成要素
レベル１	セキュアメモリ
レベル２	セキュアメモリ＋セキュアハードディスク
レベル３	セキュアメモリ＋通常ハードディスク
レベル４	通常メモリ＋セキュアハードディスク

【図７】



【図８】

図８

```
    ……
 1: <?xml version="1.0" encoding="UTF-8"?>
 2: <license xmlns="urn:abc:contentsLicense"
 3:          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 4:          xsi:schemaLocation="urn:abc:contentsLicense
 5:                  http://www.abc.com/contentsLicense.xsd" >
 6:          <inventory>
 7:                  <digitalResource licensePartId="targetContent">
 8:                          <nonSecureIndirect URI="urn:xyz:contents1"/>
 9:                  </digitalResource>
10:          </inventory>
11:          <grantGroup>
12:                  <user deviceID="stb1.abc.co.jp"/>
13:                  <grant>
14:                          <play/>
15:                          <digitalResource licensePartIdRef="targetContent"/>
16:                          <allConditions>
17:                                  <validityInterval>
18:                                          <notBefore>2003-11-15T04:03:02</notBefore>
19:                                          <notAfter>2003-12-06T04:03:02</notAfter>
20:                                  </validityInterval>
21:                          </allConditions>
22:                  </grant>
23:                  <grant>
24:                          <copy/>
25:                          <digitalResource licensePartIdRef="targetContent"/>
26:                          <allConditions>
27:                                  <count>1</count>
28:                                  <recordingMedia>
29:                                          <memoryStick/>
30:                                  </recordingMedia>
31:                          </allConditions>
32:                  </grant>
33:          </grantGroup>
34: </license>
    ……
```

【図９】

図９

```
    ……
 1: <?xml version="1.0" encoding="UTF-8" ?>
 2: <Policy xmlns="urn:oasis:names:tc:xacml:1.0:policy"
 3:      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 4:      xsi:schemaLocation="urn:oasis:names:tc:xacml:1.0:policy
 5:          http://www.oasis-open.org/tc/xacml/1.0/cs-xacml-schema-policy-01.xsd"
 6:      PolicyId="urn:metadataAccessControlPolicy1"
 7:      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
 8:    <Target>
 9:      <Subjects><AnySubject/></Subjects>
10:      <Resources><AnySubject/></Resources>
11:      <Actions><AnyAction/></Actions>
12:    </Target>
13:    <Rule RuleId="urn:metadtaAccessControlRule1" Effect="Permit">
14:    <Target>
15:      <Subjects>
16:        <Subject>
17:          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
18:            <SubjectAttributeDesignator
19:              AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
20:              DataType="rfc822Name" />
21:            <AttributeValue
22:              DataType="rfc822Name">abc.co.jp</AttributeValue>
23:          </SubjectMatch>
```

【図１０】

図10

```
24:     <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
25:       <SubjectAttributeDesignator
26:         AttributeId="urn:abc:xacml:subject:group"
27:         DataType="http://www.w3.org/2001/XMLSchema#string" />
28:       <AttributeValue>subscriberGroup1</AttributeValue>
29:     </SubjectMatch>
30:     <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
31:       <SubjectAttributeDesignator
32:         AttributeId="urn:abc:xacml:subject:deviceSecurityLevel"
33:         DataType="http://www.w3.org/2001/XMLSchema#string" />
34:       <AttributeValue>level1</AttributeValue>
35:   </SubjectMatch>
36: </Subject>
37: </Subjects>
38:     <Resources>
39:       <Resource>
40:         <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
41:           <ResourceAttributeDesignator
42:             AttributeId="urn:abc:xacml:resource:resource-uri"
43:             DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
44:           <AttributeValue>
45:             file://localhost/metadataInstanceRepository/metadataInstance1.xml
46:           </AttributeValue>
47:         </ResourceMatch>
48:       </Resource>
49:     </Resources>
```

【図１１】

図11

```
50:     <Actions>
51:       <Action>
52:         <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
53:           <ActionAttributeDesignator
54:             AttributeId="urn:abc:xacml:action"
55:             DataType=" http://www.w3.org/2001/XMLSchema#string" />
56:           <AttributeValue>read</AttributeValue>
57:         </ActionMatch>
58:       </Action>
59:     </Actions>
60:   </Target>
61: </Rule>
62: </Policy>
    ……
```

【図１２】

図12

Title: タイトル
Synopsis: 概要
Keyword: キーワード
Genre: ジャンル
ParentalRating: ペアレンタル・レーティング
Language: 言語
CastList: 出演者一覧
ReltatedMaterial: 関連コンテンツ
ProductionYear: 製作年
ProductionCountry: 製作国
Review: レビュー・評価

【図１３】

図13

LocationURL: URL
Format: 符号化フォーマット
StartDate/EndDate: 配信(取得)開始時刻/終了時刻

【図１４】

図14

Title: タイトル
Synopsis: 概要
Keyword: キーワード
KeyFrame: キーフレーム
SegmentLocation: セグメント区間開始時刻/終了時刻

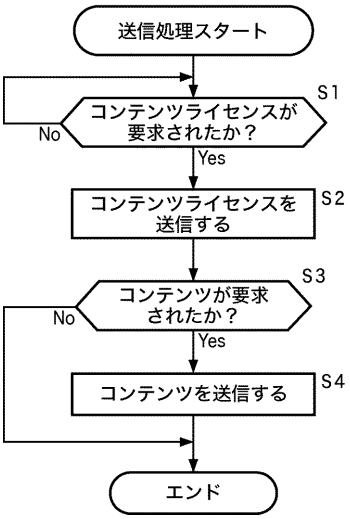
【図１５】

図15

Title: タイトル
Synopsis: 概要
Keyword: キーワード
Genre: ジャンル
ParentalRating: ペアレンタル・レーティング
Language: 言語
CastList: 出演者一覧
ReltatedMaterial: 関連コンテンツ
ProductionYear: 製作年
ProductionCountry: 製作国
Review: レビュー・評価
GroupElement: グループの要素

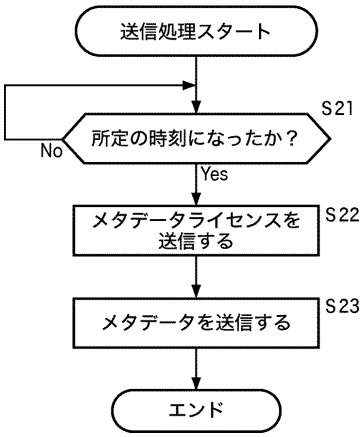
【図１６】

図16



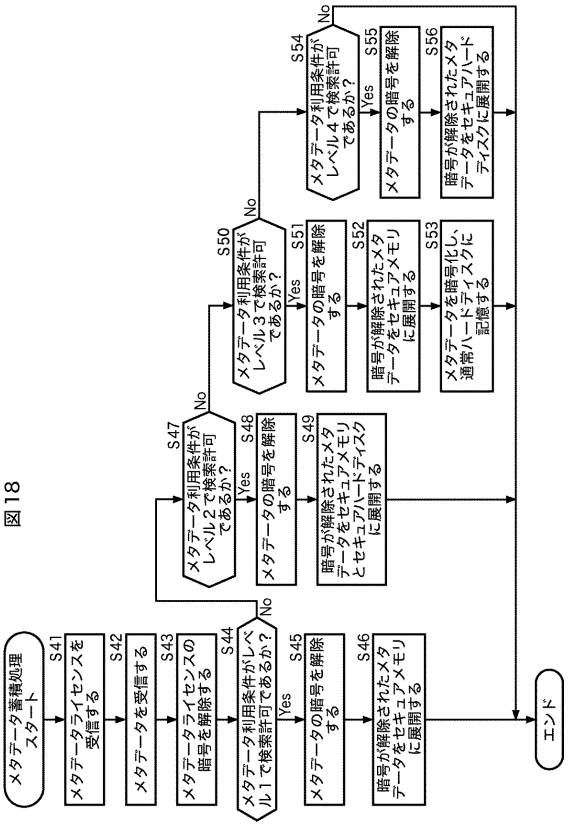
【図１７】

図17



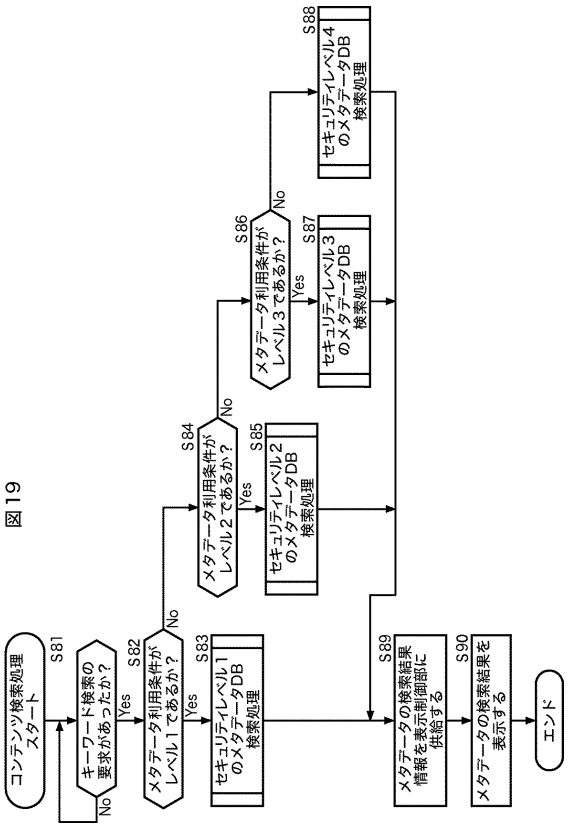
【図１８】

図18



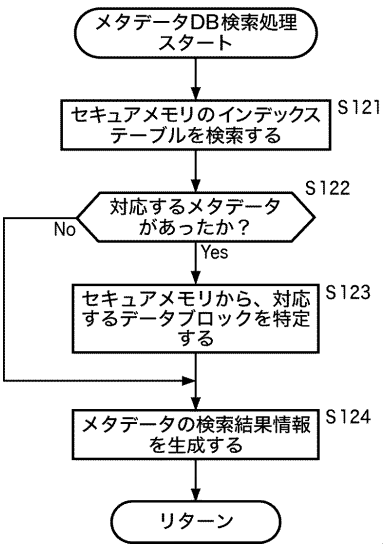
【図１９】

図19



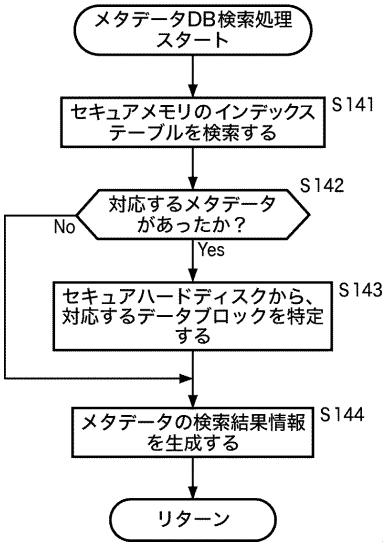
【図２０】

図20



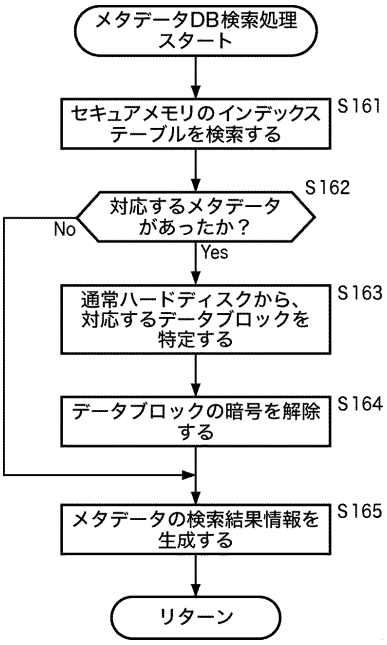
【図２１】

図21



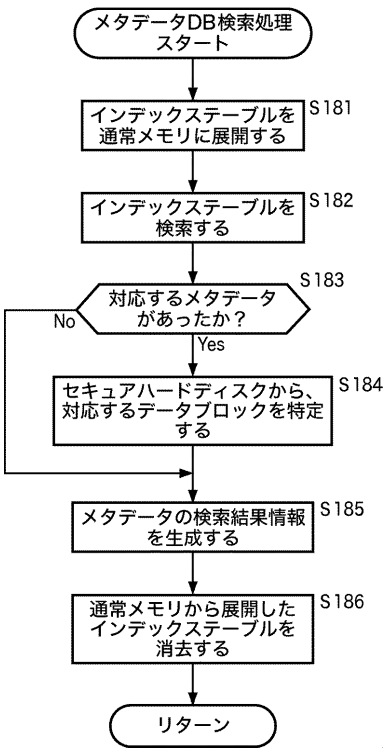
【図２２】

図22



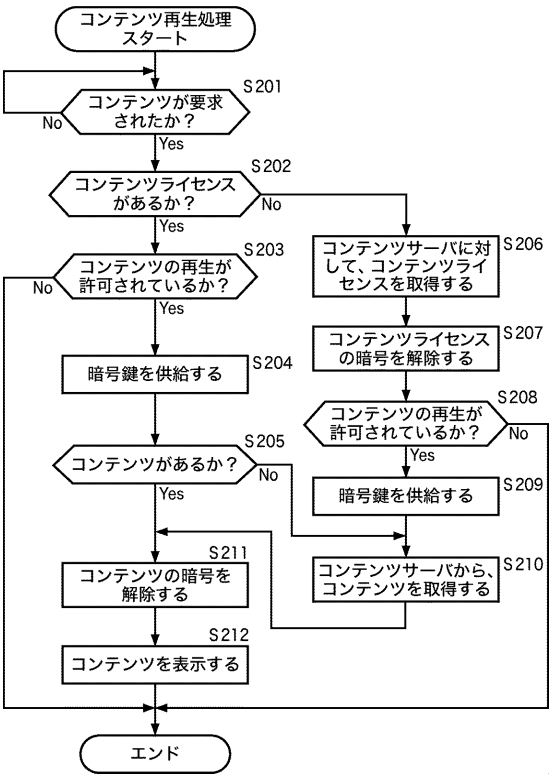
【図２３】

図23



【図２４】

図24



フロントページの続き

(56)参考文献 特開２００２－２０３０７０（ＪＰ，Ａ）
国際公開第０２／０９３３７０（WO，Ａ１）
特開２００２－１１８５４７（ＪＰ，Ａ）
特表２００３－５２０００８（ＪＰ，Ａ）
特開２００２－１７６４１９（ＪＰ，Ａ）
特開２００２－３００１５８（ＪＰ，Ａ）
特開２００２－２１７８９４（ＪＰ，Ａ）
鈴木 順一，ＩＰネットワークにおけるメタデータ交換サービスの実装と評価，情報処理学会研究報告，日本，社団法人情報処理学会，２００３年 3月 7日，第2003巻第24号，61-66

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １７／３０
Ｇ０６Ｆ ２１／２４