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

特許第5598115号
(P5598115)

(45)発行日　平成26年10月1日(2014.10.1)　(24)登録日　平成26年8月22日(2014.8.22)

(51)Int.Cl.		F I		
G06F 21/62	(2013.01)	G06F	21/24	165D
G06F 21/64	(2013.01)	G06F	21/24	167A
H04L 9/32	(2006.01)	H04L	9/00	673B
G06K 17/00	(2006.01)	G06K	17/00	B
		G06K	17/00	T

請求項の数 11　(全 65 頁)　最終頁に続く

(21)出願番号　特願2010-143362(P2010-143362)
(22)出願日　平成22年6月24日(2010.6.24)
(65)公開番号　特開2012-8757(P2012-8757A)
(43)公開日　平成24年1月12日(2012.1.12)
審査請求日　平成25年6月12日(2013.6.12)

(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　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(74)代理人　100095496
弁理士　佐々木　榮二
(74)代理人　110000763
特許業務法人大同特許事務所

最終頁に続く

(54)【発明の名称】情報処理装置、および情報処理方法、並びにプログラム

(57)【特許請求の範囲】

【請求項１】

メディアに記録されたコンテンツの再生処理を実行するデータ処理部を有し、

前記データ処理部は、

前記メディアの記録コンテンツに対応する管理データであり、コンテンツ管理データを提供するサーバが生成したトークンを前記メディアから取得し、取得したトークンに記録されたサーバＩＤであり、トークンの記録情報として設定されたコンテンツＩＤの構成ビットに含まれるサーバＩＤと、前記管理データの取得元であるサーバから取得したサーバ証明書に記録されたサーバＩＤとを比較し、両サーバＩＤが一致しない場合、または、前記コンテンツＩＤが、無効化コンテンツの識別子（ＩＤ）を記録したコンテンツリボケーションリストに記録されている場合は、コンテンツ再生を中止する情報処理装置。

【請求項２】

前記情報処理装置は、

無効化コンテンツの識別子（ＩＤ）を記録したコンテンツリボケーションリストを格納した記憶部を有し、

前記データ処理部は、

前記トークンに記録されたサーバＩＤと、前記サーバ証明書に記録されたサーバＩＤとが一致することを確認した場合に、再生予定のコンテンツＩＤが前記コンテンツリボケーションリストに記録されているか否かを検証し、記録されている場合には、コンテンツ再生を中止する処理を実行する請求項１に記載の情報処理装置。

【請求項３】
前記データ処理部は、
前記サーバ証明書に設定された署名の検証処理により、サーバ証明書の正当性を確認する処理を実行し、サーバ証明書の正当性が確認されたことを条件として、該サーバ証明書からサーバＩＤを取得する処理を行う請求項１に記載の情報処理装置。
【請求項４】
前記データ処理部は、
前記サーバ証明書に設定された署名の検証処理により、サーバ証明書の正当性を確認する処理を実行し、サーバ証明書の正当性が確認されたことを条件として、該サーバ証明書からサーバ公開鍵を取得し、
取得したサーバ公開鍵を適用して前記トークンに設定された署名の検証処理を実行して、トークンの正当性を確認する処理を実行し、トークンの正当性が確認されたことを条件として、該トークンからサーバＩＤを取得する処理を実行する請求項１に記載の情報処理装置。
【請求項５】
前記データ処理部は、
前記コンテンツリボケーションリストに設定された署名の検証処理により、コンテンツリボケーションリストの正当性を確認する処理を実行し、コンテンツリボケーションリストの正当性が確認されたことを条件として、再生予定のコンテンツＩＤが前記コンテンツリボケーションリストに記録されているか否かを検証する処理を実行する請求項２に記載の情報処理装置。
【請求項６】
前記メディアはフラッシュメモリタイプのメモリカードであり、
前記データ処理部は、
再生対象コンテンツおよび前記管理データを前記メモリカードから読み出す処理を実行する請求項１～５いずれかに記載の情報処理装置。
【請求項７】
コンテンツ管理データを提供するサーバと、
前記サーバの提供データを受信してメディアに記録するホスト装置を有し、
前記サーバは、
前記コンテンツ管理データとして、サーバＩＤを記録したトークンであり、前記サーバが生成したトークンと、
サーバＩＤを記録情報として含み、認証局署名を有する認証局発行のサーバ証明書を前記ホスト装置に提供し、
前記ホスト装置は、
前記トークンに記録されたサーバＩＤであり、トークンの記録情報として設定されたコンテンツＩＤの構成ビットに含まれるサーバＩＤが、前記サーバ証明書に記録されたサーバＩＤと一致するか否かを判定し、
両サーバＩＤが一致しない場合、または、前記コンテンツＩＤが、無効化コンテンツの識別子（ＩＤ）を記録したコンテンツリボケーションリストに記録されている場合は、コンテンツ再生を中止するコンテンツ利用制御システム。
【請求項８】
前記ホスト装置は、
無効化コンテンツの識別子（ＩＤ）を記録したコンテンツリボケーションリストを格納した記憶部を有し、
前記トークンに記録されたサーバＩＤと、前記サーバ証明書に記録されたサーバＩＤとが一致することを確認した場合に、再生予定のコンテンツＩＤが前記コンテンツリボケーションリストに記録されているか否かを検証し、記録されている場合には、コンテンツ再生を中止する処理を実行する請求項７に記載のコンテンツ利用制御システム。
【請求項９】

コンテンツおよびコンテンツの管理データを記録した情報記録媒体であり、
前記管理データには、該管理データを提供したサーバのサーバＩＤを記録データとして含むトークンであり、前記サーバが生成したトークンと、
前記サーバに対応する証明書であり、サーバＩＤを記録情報として含み認証局の署名を有する認証局が発行したサーバ証明書を含み、
コンテンツ再生を実行する再生装置において、前記トークンに記録されたサーバＩＤであり、トークンの記録情報として設定されたコンテンツＩＤの構成ビットに含まれるサーバＩＤが前記サーバ証明書に記録されたサーバＩＤと一致するか否かを判定させ、さらに、前記コンテンツＩＤが、無効化コンテンツの識別子（ＩＤ）を記録したコンテンツリボケーションリストに記録されているか否かを確認させ、
サーバＩＤが一致しない場合、または、前記コンテンツＩＤがコンテンツリボケーションリストに記録されている場合は、コンテンツ再生を中止させることを可能とした情報記録媒体。
【請求項１０】
情報処理装置において実行する情報処理方法であり、
データ処理部が、メディアに記録されたコンテンツの管理データを取得するステップと、
前記データ処理部が、前記管理データに含まれ、該管理データを提供するサーバが生成したトークンに記録されたサーバＩＤであり、トークンの記録情報として設定されたコンテンツＩＤの構成ビットに含まれるサーバＩＤと、前記管理データの取得元であるサーバから取得したサーバ証明書に記録されたサーバＩＤとを比較し、両サーバＩＤが一致しない場合、または、前記コンテンツＩＤが、無効化コンテンツの識別子（ＩＤ）を記録したコンテンツリボケーションリストに記録されている場合は、コンテンツ再生を中止する情報処理方法。
【請求項１１】
情報処理装置において情報処理を実行させるプログラムであり、
データ処理部に、メディアに記録されたコンテンツの管理データを取得させるステップと、
前記データ処理部に、前記管理データに含まれ、該管理データを提供するサーバが生成したトークンに記録されたサーバＩＤであり、トークンの記録情報として設定されたコンテンツＩＤの構成ビットに含まれるサーバＩＤと、前記管理データの取得元であるサーバから取得したサーバ証明書に記録されたサーバＩＤとを比較させて、両サーバＩＤが一致しない場合、または、前記コンテンツＩＤが、無効化コンテンツの識別子（ＩＤ）を記録したコンテンツリボケーションリストに記録されている場合は、コンテンツ再生を中止させるステップと、
を実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、および情報処理方法、並びにプログラムに関する。特に、例えばメモリカード等の記録メディアに記録したコンテンツの利用制御等を実行する情報処理装置、および情報処理方法、並びにプログラムに関する。
【背景技術】
【０００２】
昨今、情報記録媒体として、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）や、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）、あるいはフラッシュメモリなど、様々なメディアが利用されている。特に、昨今は、大容量のフラッシュメモリを搭載したＵＳＢメモリなどのメモリカードの利用が盛んになっている。ユーザは、このような様々な情報記録媒体（メディア）に音楽や映画などのコンテンツを記録して再生装置（プレーヤ）に装着してコンテンツの再生を行うことができる。

【０００３】
しかし、音楽データ、画像データ等の多くのコンテンツは、その作成者あるいは販売者に著作権、頒布権等が保有されている。従って、ユーザにコンテンツを提供する場合には、一定の利用制限、すなわち正規な利用権を持つユーザのみにコンテンツの利用を許諾し、許可のないコピー等の無秩序な利用が行われないような制御を行うのが一般的となっている。
【０００４】
例えば、コンテンツの利用制御に関する規格としてＡＡＣＳ（Ａｄｖａｎｃｅｄ Ａｃｃｅｓｓ Ｃｏｎｔｅｎｔ Ｓｙｓｔｅｍ）が知られている。ＡＡＣＳの規格は、例えばＢｌｕ－ｒａｙ Ｄｉｓｃ（登録商標）の記録コンテンツに対する利用制御構成を定義している。具体的には例えばＢｌｕ－ｒａｙ Ｄｉｓｃ（登録商標）に記録するコンテンツを暗号化コンテンツとして、その暗号鍵を取得できるユーザを正規ユザにのみ限定することを可能とするアルゴリズムなどを規定している。
【０００５】
しかし、現行のＡＡＣＳ規定には、Ｂｌｕ－ｒａｙ Ｄｉｓｃ（登録商標）等のディスク記録コンテンツに対する利用制御構成についての規定は存在するが、例えばメモリカードなどのフラッシュメモリに記録されるコンテンツ等については、十分な規定がない。従って、このようなメモリカードの記録コンテンツについては、著作権の保護が不十分になる恐れがあり、これらメモリカード等のメディアを利用したコンテンツ利用に対する利用制御構成を構築することが要請されている。
【０００６】
例えばＡＡＣＳ規定では、Ｂｌｕ－ｒａｙ Ｄｉｓｃ（登録商標）等のディスク記録コンテンツに対する利用制御構成として以下のような規定がある。
（ａ）既にコンテンツの記録されたメディア（例えばＲＯＭディスク）からＢｌｕ－ｒａｙ Ｄｉｓｃ（登録商標）等のディスクにコピーされたコンテンツに対する利用規定、
（ｂ）サーバからダウンロードしてＢｌｕ－ｒａｙ Ｄｉｓｃ（登録商標）等のディスクに記録されたコンテンツの利用規定、
例えば、このようなコンテンツの利用制御について規定している。
【０００７】
ＡＡＣＳでは、例えば上記（ａ）のメディア間のコンテンツコピーを実行する場合、管理サーバからコピー許可情報を取得することを条件としたマネージドコピー（ＭＣ：Ｍａｎａｇｅｄ Ｃｏｐｙ）について規定している。
【０００８】
また、上記の（ｂ）のサーバからのコンテンツのダウンロード処理として、ＡＡＣＳでは、
ＰＣ等のユーザ装置を利用したＥＳＴ（Ｅｌｅｃｔｒｉｃ Ｓｅｌｌ Ｔｈｒｏｕｇｈ）や、
コンビニ等に設置された共用端末を利用したＭｏＤ（Ｍａｎｕｆａｃｔｕｒｉｎｇ ｏｎ Ｄｅｍａｎｄ）、
これらの各種のダウンロード形態を規定して、これらの各ダウンロード処理によりディスクにコンテンツを記録して利用する場合についても、所定のルールに従った処理を行うことを義務付けている。
なお、これらの処理については、例えば特許文献１（特開２００８－９８７６５号公報）に記載されている。
【０００９】
しかし、前述したように、ＡＡＣＳの規定は、Ｂｌｕ－ｒａｙ Ｄｉｓｃ（登録商標）等のディスク記録コンテンツを利用制御対象として想定しているものであり、ＵＳＢルモリなどを含むフラッシュメモリタイプ等のメモリカードに記録されるコンテンツについては十分な利用制御に関する規定がないという問題がある。
【先行技術文献】

【特許文献】
【００１０】
【特許文献１】特開２００８－９８７６５号公報
【発明の概要】
【発明が解決しようとする課題】
【００１１】
本発明は、例えば上記問題点に鑑みてなされたものであり、フラッシュメモリ等のディスク以外の情報記録媒体（メディア）にコンテンツを記録して利用する場合の利用制御構成を確立して不正なコンテンツ利用を防止する構成を実現する情報処理装置、および情報処理方法、並びにプログラムを提供することを目的とする。
【課題を解決するための手段】
【００１２】
本発明の第１の側面は、
メディアに記録されたコンテンツの再生処理を実行するデータ処理部を有し、
前記データ処理部は、
前記メディアの記録コンテンツに対応する管理データであるトークンを前記メディアから取得し、取得したトークンに記録されたサーバＩＤと、前記管理データの取得元であるサーバから取得したサーバ証明書に記録されたサーバＩＤとを比較し、両サーバＩＤが一致しない場合は、コンテンツ再生を中止する処理を実行する情報処理装置にある。
【００１３】
さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、無効化コンテンツの識別子（ＩＤ）を記録したコンテンツリボケーションリストを格納した記憶部を有し、前記データ処理部は、前記トークンに記録されたサーバＩＤと、前記サーバ証明書に記録されたサーバＩＤとが一致することを確認した場合に、再生予定のコンテンツＩＤが前記コンテンツリボケーションリストに記録されているか否かを検証し、記録されている場合には、コンテンツ再生を中止する処理を実行する。
【００１４】
さらに、本発明の情報処理装置の一実施態様において、前記トークンに記録されたサーバＩＤは、トークンの記録情報として設定されたコンテンツＩＤの構成ビットに含まれ、前記データ処理部は、トークンに含まれるコンテンツＩＤからサーバＩＤの構成ビットを抽出して、前記サーバ証明書に記録されたサーバＩＤとの比較処理を実行する。
【００１５】
さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記サーバ証明書に設定された署名の検証処理により、サーバ証明書の正当性を確認する処理を実行し、サーバ証明書の正当性が確認されたことを条件として、該サーバ証明書からサーバＩＤを取得する処理を行う。
【００１６】
さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記サーバ証明書に設定された署名の検証処理により、サーバ証明書の正当性を確認する処理を実行し、サーバ証明書の正当性が確認されたことを条件として、該サーバ証明書からサーバ公開鍵を取得し、取得したサーバ公開鍵を適用して前記トークンに設定された署名の検証処理を実行して、トークンの正当性を確認する処理を実行し、トークンの正当性が確認されたことを条件として、該トークンからサーバＩＤを取得する処理を実行する。
【００１７】
さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記コンテンツリボケーションリストに設定された署名の検証処理により、コンテンツリボケーションリストの正当性を確認する処理を実行し、コンテンツリボケーションリストの正当性が確認されたことを条件として、再生予定のコンテンツＩＤが前記コンテンツリボケーションリストに記録されているか否かを検証する処理を実行する。
【００１８】

さらに、本発明の情報処理装置の一実施態様において、前記メディアはフラッシュメモリタイプのメモリカードであり、前記データ処理部は、再生対象コンテンツおよび前記管理データを前記メモリカードから読み出す処理を実行する。

【００１９】

さらに、本発明の第２の側面は、

コンテンツ管理データを提供するサーバと、

前記サーバの提供データを受信してメディアに記録するホスト装置を有し、

前記サーバは、

前記コンテンツ管理データとして、サーバＩＤを記録したトークンと、

サーバＩＤを記録情報として含み、認証局署名を有する認証局発行のサーバ証明書を前記ホスト装置に提供し、

前記ホスト装置は、

前記トークンに記録されたサーバＩＤが、前記サーバ証明書に記録されたサーバＩＤと一致するか否かを判定し、一致の確認がなされたことを条件としてコンテンツ再生を行うコンテンツ利用制御システムにある。

【００２０】

さらに、本発明のコンテンツ利用制御システムの一実施態様において、前記ホスト装置は、無効化コンテンツの識別子（ＩＤ）を記録したコンテンツリボケーションリストを格納した記憶部を有し、前記トークンに記録されたサーバＩＤと、前記サーバ証明書に記録されたサーバＩＤとが一致することを確認した場合に、再生予定のコンテンツＩＤが前記コンテンツリボケーションリストに記録されているか否かを検証し、記録されている場合には、コンテンツ再生を中止する処理を実行する。

【００２１】

さらに、本発明の第３の側面は、

コンテンツおよびコンテンツの管理データを記録した情報記録媒体であり、

前記管理データには、該管理データを提供したサーバのサーバＩＤを記録データとして含むトークンと、

前記サーバに対応する証明書であり、サーバＩＤを記録情報として含み認証局の署名を有する認証局が発行したサーバ証明書を含み、

コンテンツ再生を実行する再生装置において、前記トークンに記録されたサーバＩＤが前記サーバ証明書に記録されたサーバＩＤと一致するか否かを判定させて、一致の確認がなされたことを条件としてコンテンツ再生を許容することを可能とした情報記録媒体にある。

【００２２】

さらに、本発明の第４の側面は、

情報処理装置において実行する情報処理方法であり、

データ処理部が、メディアに記録されたコンテンツの管理データを取得するステップと、

前記データ処理部が、前記管理データに含まれるトークンに記録されたサーバＩＤと、前記管理データの取得元であるサーバから取得したサーバ証明書に記録されたサーバＩＤとを比較し、両サーバＩＤが一致しない場合は、コンテンツ再生を中止する処理を実行するステップと、

を実行する情報処理方法にある。

【００２３】

さらに、本発明の第５の側面は、

情報処理装置において情報処理を実行させるプログラムであり、

データ処理部に、メディアに記録されたコンテンツの管理データを取得させるステップと、

前記データ処理部に、前記管理データに含まれるトークンに記録されたサーバＩＤと、前記管理データの取得元であるサーバから取得したサーバ証明書に記録されたサーバＩＤ

とを比較させて、両サーバＩＤが一致しない場合は、コンテンツ再生を中止させるステップと、

を実行させるプログラムにある。

【００２４】

なお、本発明のプログラムは、例えば、様々なプログラム・コードを実行可能な情報処理装置やコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体によって提供可能なプログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、情報処理装置やコンピュータ・システム上でプログラムに応じた処理が実現される。

【００２５】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【発明の効果】

【００２６】

本発明の一実施例の構成によれば、メディアに記録されたコンテンツの不正利用を防止する再生制御が実現される。メディアの記録コンテンツに対応する管理データであるトークンをメディアから取得し、取得したトークンに記録されたサーバＩＤと、管理データの取得元であるサーバから取得したサーバ証明書に記録されたサーバＩＤとを比較し、両サーバＩＤが一致しない場合は、コンテンツ再生を中止させる。両ＩＤの一致が確認された場合には、再生予定のコンテンツＩＤがコンテンツリボケーションリストに記録されているか否かを検証し、記録されている場合には、コンテンツ再生を中止する。本処理により、メディア記録コンテンツの不正利用を防止した再生制御が実現される。

【図面の簡単な説明】

【００２７】

【図１】コンテンツ提供処理および利用処理の概要について説明する図である。

【図２】メモリカードに記録されたコンテンツの利用形態について説明する図である。

【図３】サーバ管理構成とサーバからの提供データについて説明する図である。

【図４】サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）と、コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）について説明する図である。

【図５】サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）について説明する図である。

【図６】メモリカードの記憶領域の具体的構成例について説明する図である。

【図７】コンテンツサーバが生成して提供するトークンの具体的なデータ構成例について説明する図である。

【図８】サーバとメモリカード間の処理とメモリカードの格納データについて説明する図である。

【図９】メモリカード内に記録されるデータを示すディレクトリ構造と、コンテンツ再生処理を実行する再生装置内に記録されるデータの例について説明する図である。

【図１０】コンテンツサーバからコンテンツをダウンロードしてメモリカードに記録する場合の処理シーケンスについて説明するフローチャートを示す図である。

【図１１】図１０に示すフロー中のステップＳ１０３の詳細シーケンスについて説明するフローチャートを示す図である。

【図１２】コンテンツサーバからコンテンツをダウンロードしてメモリカードに記録する場合の処理シーケンスについて説明するフローチャートを示す図である。

【図１３】コンテンツサーバからコンテンツをダウンロードしてメモリカードに記録する場合の処理シーケンスについて説明するフローチャートを示す図である。

【図１４】サーバからダウンロードしてメディア（メモリカード）に記録したコンテンツ

と管理情報（ダウンロードコンテンツ対応の管理データ）を適用したコンテンツの再生処理シーケンスについて説明するフローチャートを示す図である。
【図１５】図１４に示すフロー中のステップＳ３０３の詳細シーケンスについて説明するフローチャートを示す図である。
【図１６】サーバからダウンロードしてメディア（メモリカード）に記録したコンテンツと管理情報（ダウンロードコンテンツ対応の管理データ）を適用したコンテンツの再生処理シーケンスについて説明するフローチャートを示す図である。
【図１７】サーバからダウンロードしてメディア（メモリカード）に記録したコンテンツと管理情報（ダウンロードコンテンツ対応の管理データ）を適用したコンテンツの再生処理シーケンスについて説明するフローチャートを示す図である。
【図１８】記録再生装置（ホスト）の所有するホスト証明書の例について説明する図である。
【図１９】メモリカードに対するアクセス要求装置がサーバである場合と、記録再生装置等のホスト機器である場合のアクセス制限の設定例について説明する図である。
【図２０】メモリカードに対するアクセス要求装置がＰＣである場合と、ＣＥ機器である場合のアクセス制限の設定例について説明する図である。
【図２１】メモリカードを装着してデータの記録や再生処理を行うホスト機器のハードウェア構成例について説明する図である。
【図２２】メモリカードのハードウェア構成例について説明する図である。
【発明を実施するための形態】
【００２８】
以下、図面を参照しながら本発明の情報処理装置、および情報処理方法、並びにプログラムの詳細について説明する。なお、説明は以下の項目に従って行う。
１．コンテンツ提供処理および利用処理の概要について
２．サーバ管理構成とサーバからの提供データについて
３．サーバがコンテンツ管理情報として提供するトークンについて
４．サーバとメモリカード間の処理とメモリカードの格納データについて
５．サーバからのコンテンツダウンロード処理シーケンスについて
６．コンテンツ再生処理シーケンスについて
７．メモリカードの保護領域のアクセス制限構成と処理について
８．各装置のハードウェア構成例について
【００２９】
［１．コンテンツ提供処理および利用処理の概要について］
【００３０】
以下、図面を参照しながら本発明の情報処理装置、および情報処理方法、並びにプログラムの詳細について説明する。
【００３１】
まず、図１以下を参照して、コンテンツ提供処理および利用処理の概要について説明する。
図１には、左から、
（ａ）コンテンツ提供元
（ｂ）コンテンツ記録装置（ホスト）
（ｃ）コンテンツ記録メディア
これらを示している。
【００３２】
（ｃ）コンテンツ記録メディアはユーザがコンテンツを記録して、コンテンツの再生処理に利用するメディアである。ここでは例えばフラッシュメモリ等の情報記録装置であるメモリカード３１を示している。
【００３３】
ユーザは、例えば音楽や映画などの様々なコンテンツをメモリカード３１に記録して利

用する。これらのコンテンツは例えば著作権管理コンテンツ等、利用制御対象となるコンテンツである。所定の利用条件下での利用のみが許容され、基本的に無秩序なコピー処理やコピーデータの無制限な配布等は禁止される。なお、後述するがメモリカード３１に対して、コンテンツを記録する場合、そのコンテンツに対応する利用制御情報（Ｕｓａｇｅ Ｒｕｌｅ）、具体的には、許容されるコピー回数などのコピー制限情報などを規定した利用制御情報（Ｕｓａｇｅ Ｒｕｌｅ）も併せて記録される。

【００３４】

（ａ）コンテンツ提供元は、利用制限のなされた音楽や映画等のコンテンツの提供元である。図１には、コンテンツサーバ１１と、予めコンテンツの記録されたＲＯＭディスク等のコンテンツ記録ディスク１２を示している。

コンテンツサーバ１１は、音楽や映画等のコンテンツを提供するサーバである。コンテンツ記録ディスク１２は予め音楽や映画等のコンテンツを記録したＲＯＭディスク等のディスクである。

【００３５】

ユーザは、（ｃ）コンテンツ記録メディアであるメモリカード３１を（ｂ）コンテンツ記録装置（ホスト）に装着し、（ｂ）コンテンツ記録装置（ホスト）を介してコンテンツサーバ１１に接続して、コンテンツを受信（ダウンロード）してメモリカード３１に記録することができる。

【００３６】

なお、コンテンツサーバ１１は、このダウンロード処理に際して、所定のシーケンスに従った処理を行い、暗号化コンテンツの他、利用制御情報やトークン、さらに鍵情報（バインドキー）等のコンテンツ管理情報を提供する。これらの処理、および提供データについては、後段で詳細に説明する。

【００３７】

あるいは、（ｃ）コンテンツ記録メディアであるメモリカード３１を装着した（ｂ）コンテンツ記録装置（ホスト）に、予めコンテンツの記録されたＲＯＭディスク等のコンテンツ記録ディスク１２を装着してコンテンツ記録ディスク１２の記録コンテンツをメモリカード３１にコピーすることができる。ただし、このコピー処理を実行する場合にも、コンテンツサーバ１１に接続して所定のシーケンスに従った処理が必要となる。コンテンツサーバ１１は、このディスクからのコンテンツコピー処理に際して、コピーコンテンツに対応する利用制御情報やトークン、さらに鍵情報（バインドキー）等のコンテンツ管理情報を提供する。

【００３８】

（ｂ）コンテンツ記録装置（ホスト）は、（ｃ）コンテンツ記録メディアであるメモリカード３１を装着して、（ａ）コンテンツ提供元であるコンテンツサーバ１１からネットワークを介して受信（ダウンロード）したコンテンツ、あるいは、コンテンツ記録ディスク１２から読み取ったコンテンツをメモリカード３１に記録する。

【００３９】

（ｂ）コンテンツ記録装置（ホスト）としては、不特定多数のユーザが利用可能な公共スペース、例えば駅やコンビニ等に設置された共用端末２１、ユーザ機器としての記録再生器（ＣＥ（Ｃｏｎｓｕｍｅｒ Ｅｌｅｃｔｒｏｎｉｃｓ）機器）２２、ＰＣ２３などがある。これらはすべて（ｃ）コンテンツ記録メディアであるメモリカード３１を装着可能な装置である。

また、これらの（ｂ）コンテンツ記録装置（ホスト）は、コンテンツサーバ１１からのダウンロード処理を実行する構成である場合は、ネットワークを介したデータ送受信処理を実行することが可能な構成である。

コンテンツ記録ディスク１２を利用する構成の場合は、ディスクの再生可能な装置であることが必要である。

【００４０】

図１に示すように、ユーザは、

（ａ）コンテンツ提供元であるコンテンツサーバ１１からのダウンロードコンテンツ、あるいはＲＯＭディスク等のコンテンツ記録ディスク１２に記録されたコンテンツを（ｂ）コンテンツ記録装置（ホスト）を介して、（ｃ）コンテンツ記録メディアとしてのメモリカード３１に記録する。

【００４１】

このメモリカード３１に記録されたコンテンツの利用形態について図２を参照して説明する。

ユーザは、コンテンツを記録したメモリカード３１を、例えば、図１（ｂ）を参照して説明した（ｂ）コンテンツ記録装置（ホスト）としてのユーザ機器である記録再生器（ＣＥ機器）２２やＰＣ２３等に装着してメモリカード３１に記録されたコンテンツを読み取り、再生する。

【００４２】

なお、多くの場合、これらのコンテンツは暗号化コンテンツとして記録されており、記録再生器（ＣＥ機器）２２やＰＣ２３等の再生装置は、所定のシーケンスに従った復号処理を実行した後、コンテンツ再生を行う。

なお、メモリカード３１に記録されたコンテンツを再生する機器は、図１（ｂ）を参照して説明した（ｂ）コンテンツ記録装置（ホスト）に限られず、その他の再生装置（プレーヤ）であってもよい。ただし、例えば予め規定されたシーケンスに従った暗号化コンテンツの復号処理等を実行可能な機器、すなわち予め規定された再生処理シーケンスを実行するプログラムを格納した機器であることが必要となる。なお、コンテンツ再生シーケンスの詳細については、後段で説明する。

【００４３】

［２．サーバ管理構成とサーバからの提供データについて］

次に、図３以下を参照して、サーバ管理構成とサーバからの提供データについて説明する。

図３には、コンテンツの記録先であるユーザのメモリカード４００、
コンテンツ記録処理を実行するコンテンツ記録装置（ホスト）３００、
コンテンツやコンテンツ管理データを提供するコンテンツサーバ２００、
コンテンツサーバ２００の管理局として設定される認証局（認証サーバ）１００、
さらにコンテンツを記録したディスク２５０、
これらを示している。

【００４４】

なお、図３に示すメモリカード４００は、図１、図２に示すメモリカード３１に相当し、図３に示すコンテンツ記録装置（ホスト）３００は、図１に示す（ｂ）コンテンツ記録装置（ホスト）に相当する装置である。

また、図３に示すコンテンツサーバ２００は、図１に示すコンテンツサーバ１１に相当し、図３に示すディスク２５０は、図１に示すディスク１２に相当する。

【００４５】

なお、コンテンツサーバ２００は、図３にコンテンツサーバ＃１～コンテンツサーバ＃ｎとして示すように、複数存在している。これらの様々なコンテンツサーバに対して、メモリカード４００を装着したコンテンツ記録装置（ホスト）３００が接続し、コンテンツやコンテンツ管理データを取得してメモリカード４００に記録する。

【００４６】

図３に示す認証局（認証サーバ）１００は、コンテンツやコンテンツ管理データを提供する各コンテンツサーバ＃１～＃ｎに対して、

（ａ）サーバ公開鍵を格納したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）、

（ｂ）サーバ秘密鍵、

（ｃ）無効化したサーバのサーバＩＤを記録したリストであるサーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、

（ｄ）無効化したコンテンツのコンテンツＩＤを記録したリストであるコンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、
たとえば、これらのデータを提供する。

【００４７】

コンテンツサーバ＃１～＃ｎの各々は、これらのデータを認証局１００から受信し、サーバ内の記憶部に格納する。以下、コンテンツサーバ＃１～＃ｎの処理は共通するので代表してコテンツサーバ＃１の処理について説明する。以下コンテンツサーバ＃１をコンテンツサーバ２００として説明する。

【００４８】

コンテンツサーバ２００は、メモリカード４００に対するコンテンツの提供処理を実行する際に、コンテンツ２０２を暗号化して暗号化コンテンツとして提供するとともに、コンテンツ管理情報として、トークン２０１や、サーバリボケーションリスト（ＳＲＬ）２０３、コンテンツリボケーションリスト（ＣＲＬ）２０４、さらに図には示していないが、コンテンツの復号に適用する暗号鍵（バインドキー）等をコンテンツ記録装置（ホスト）３００に提供して、コンテンツと共にメモリカード４００に記録させる。

【００４９】

なお、ユーザが、コンテンツ記録装置（ホスト）３００にディスク２５０を装着し、ディスク２５０に格納されたコンテンツをメモリカード４００に記録する（コピー）場合には、コンテンツ記録装置（ホスト）３００は、コピー許可をコンテンツサーバ２００から得て、コンテンツのコピーを実行する。この処理のために、コンテンツ記録装置（ホスト）３００は、例えばコピー予定のコンテンツの識別子であるコンテンツＩＤをディスク２５０から取得してコンテンツサーバ２００に送信する。

【００５０】

なお、ディスク２５０に格納されたコンテンツも暗号化コンテンツであり、その復号に適用する鍵の他、図３に示すコンテンツ管理データとしてのトークン２０１や、サーバリボケーションリスト（ＳＲＬ）２０３、コンテンツリボケーションリスト（ＣＲＬ）２０４などがコンテンツサーバ２００からコンテンツ記録装置（ホスト）３００に提供され、ディスク２５０から提供されたコンテンツに対応する管理データとしてコンテンツと共にメモリカード４００に記録する処理が行われる。

【００５１】

先に、説明したように、認証局１００は、図３に示すように、
サーバリボケーションリスト（ＳＲＬ）１０２、
コンテンツリボケーションリスト（ＣＲＬ）１０３、
サーバ証明書（ＳＥｒｖｅｒ　Ｃｅｒｔ）１０１、
これらの各データを各コンテンツサーバに提供する。
図４以下を参照して、これらのデータの詳細構成例について説明する。

【００５２】

まず、図４を参照して、
サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）と、
コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、
これらの各リストについて説明する。

【００５３】

図４には、
（ａ）サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）
（ｂ）コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、
これらのデータ構成例を示している。

【００５４】
（ａ）サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）は、無効化（リボーク）されたサーバ（コンテンツサーバ）の識別子（ＩＤ）を記録したリストであり、認証局１００が発行するリストである。
サーバリボケーションリスト（ＳＲＬ）は、例えば不正なコンテンツの配信など、不正処理が発覚したコンテンツサーバのサーバＩＤを記録したリストである。新たな不正サーバの発覚等により、逐次更新される。
【００５５】
サーバリボケーションリスト（ＳＲＬ）には、図４（ａ）に示すようにバージョン番号が設定される。例えば００１→００２→００３等、新たなリスト発行処理ごとに、バージョン番号は増加する。すなわち、より新しいサーバリボケーションリスト（ＳＲＬ）のバージョン番号は、古いサーバリボケーションリスト（ＳＲＬ）のバージョン番号より大きな番号が設定される。
【００５６】
サーバリボケーションリスト（ＳＲＬ）は、バージョン番号と、無効化されたサーバのサーバＩＤが記録され、これらのデータに対して、認証局の秘密鍵に基づく署名（Ｓｉｇｎａｔｕｒｅ）が生成されて記録される。この署名処理により、データ改ざんが防止される。
【００５７】
サーバリボケーションリスト（ＳＲＬ）を利用する場合は、署名検証を実行して、サーバリボケーションリスト（ＳＲＬ）の正当性を確認した上で利用が行われる。なお、署名検証は、認証局の公開鍵を利用して実行される。
【００５８】
コンテンツを記録するメモリカードや、コンテンツを再生する再生装置、例えば図２に示す記録再生器２２やＰＣ２３等の再生装置の記憶部（メモリ）にもサーバリボケーションリスト（ＳＲＬ）が記録される。
【００５９】
再生装置は、コンテンツ再生時に再生コンテンツやコンテンツ管理データを受領したサーバのサーバＩＤを取得し、取得したサーバＩＤが、再生装置の記憶部に格納されたサーバリボケーションリスト（ＳＲＬ）に無効サーバとして記録されているか否かを検証する。なお、サーバＩＤは、例えばコンテンツに関する管理データとしてサーバから受信するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）などから取得できる。
【００６０】
サーバリボケーションリスト（ＳＲＬ）に再生予定のコンテンツやコンテンツ管理データを受領したサーバのサーバＩＤが記録されている場合は、そのコンテンツは不正なサーバの提供コンテンツである可能性があるため、再生が禁止される。
【００６１】
なお、このような処理を実行するための再生処理プログラムは、予め再生装置に提供され、コンテンツの再生処理においては、再生処理プログラムに従った処理が実行される。すなわち、再生装置では、コンテンツ再生処理に先立って、再生装置が利用するサーバリボケーションリスト（ＳＲＬ）のバージョン番号の確認や、サーバリボケーションリスト（ＳＲＬ）に基づいて利用コンテンツやコンテンツ管理データを提供したサーバが無効化（リボーク）されていないことを確認する処理を実行する。なお、コンテンツ再生シーケンスについては後段でフローチャートを参照して説明する。
【００６２】
（ｂ）コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）は、無効化（リボーク）されたコンテンツの識別子（ＩＤ）を記録したリストであり、認証局１００が発行するリストである。コンテンツリボケーションリスト（ＣＲＬ）は、例えば不正なコピーコンテンツの流通が発覚した場合など、その不正流通コンテンツのコンテンツＩＤを記録して生成されるリストであり、新たな不正コンテンツ

の発覚等により、逐次更新される。

【００６３】

コンテンツリボケーションリスト（ＣＲＬ）には、図４（ｂ）に示すようにバージョン番号が設定される。例えば００１→００２→００３等、新たな発行処理ごとに、バージョン番号は増加する。すなわち、より新しいコンテンツリボケーションリスト（ＣＲＬ）のバージョン番号は、古いコンテンツリボケーションリスト（ＣＲＬ）のバージョン番号より大きな番号が設定される。

【００６４】

コンテンツリボケーションリスト（ＣＲＬ）は、バージョン番号と、無効化コンテンツのコンテンツＩＤが記録され、これらのデータに対して、認証局の秘密鍵に基づく署名（Ｓｉｇｎａｔｕｒｅ）が生成されて記録される。この署名処理により、データ改ざんが防止される。

【００６５】

コンテンツリボケーションリスト（ＣＲＬ）を利用する場合は、署名検証を実行して、コンテンツリボケーションリスト（ＣＲＬ）の正当性を確認した上で利用が行われる。なお、署名検証は、認証局の公開鍵を利用して実行される。

【００６６】

コンテンツを記録するメモリカードや、コンテンツを再生する再生装置、例えば図２に示す記録再生器２２やＰＣ２３等の再生装置の記憶部（メモリ）にもコンテンツリボケーションリスト（ＣＲＬ）が記録される。

【００６７】

再生装置は、コンテンツ再生時に再生コンテンツのコンテンツＩＤを取得し、取得したコンテンツＩＤが、再生装置の記憶部に格納されたコンテンツリボケーションリスト（ＣＲＬ）にリボーク（無効化）コンテンツとして記録されているか否かを検証する。なお、コンテンツＩＤは、例えばコンテンツに関する管理データとしてサーバから受信する（あるいはディスクから読み取る）コンテンツ証明書などから取得できる。

【００６８】

コンテンツリボケーションリスト（ＣＲＬ）に再生予定のコンテンツのコンテンツＩＤが記録されている場合は、そのコンテンツは無効化コンテンツであるため、再生が禁止される。

【００６９】

なお、このような処理を実行するための再生処理プログラムは、予め再生装置に提供され、コンテンツの再生処理においては、再生処理プログラムに従った処理が実行される。すなわち、再生装置では、コンテンツ再生処理に先立って、再生装置が利用するコンテンツリボケーションリスト（ＣＲＬ）のバージョン番号の確認や、コンテンツリボケーションリスト（ＣＲＬ）に基づいて利用コンテンツが無効化されていないことを確認する処理が実行される。なお、コンテンツ再生シーケンスについては後段でフローチャートを参照して説明する。

【００７０】

次に、図５を参照して認証局１００が各コンテンツサーバに提供するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）１０１について説明する。

認証局１００が各コンテンツサーバに提供するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）１０１は、認証局１００がコンテンツ提供処理を認めたサーバに対して発行するサーバの証明書であり、サーバ公開鍵等を格納した証明書である。サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）１０１は、認証局１００秘密鍵によって署名が設定され、改ざんの防止されたデータとして構成される。

【００７１】

図５に認証局１００が各コンテンツサーバに提供するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）１０１の具体例を示す。

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）には、図５に示すように、以

下のデータが含まれる。
（１）タイプ情報
（２）サーバＩＤ
（３）サーバ公開鍵（Ｓｅｒｖｅｒ　Ｐｕｂｌｉｃ　Ｋｅｙ）
（４）コンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）
（５）サーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）
（６）メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）
（７）その他の情報
（８）署名（Ｓｉｇｎａｕｒｅ）

【００７２】

以下、上記（１）～（８）の各データについて説明する。
（１）タイプ情報
タイプ情報は、証明書のタイプやコンテンツサーバのタイプを示す情報であり、例えば本証明書がサーバ証明書であることを示すデータや、サーバの種類、例えば音楽コンテンツの提供サーバであるとか、映画コンテンツの提供サーバであるといったサーバの種類などを示す情報が記録される。

【００７３】

（２）サーバＩＤ
サーバＩＤはサーバ識別情報としてのサーバＩＤを記録する領域である。
（３）サーバ公開鍵（Ｓｅｒｖｅｒ　Ｐｕｂｌｉｃ　Ｋｅｙ）
サーバ公開鍵（Ｓｅｒｖｅｒ　Ｐｕｂｌｉｃ　Ｋｅｙ）はサーバの公開鍵である。サーバに提供されるサーバ秘密鍵とともに公開鍵暗号方式に従った鍵ペアを構成する。

【００７４】

（４）コンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）
コンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）は、先に図４（ｂ）を参照して説明した無効化（リボーク）されたコンテンツを記録したリストであるコンテンツリボケーションリスト（ＣＲＬ）に設定されたバージョン番号中、再生装置における利用が許容されるバージョン番号の最小値である。すなわち、再生装置において、コンテンツ再生の前処理として実行が義務付けられるコンテンツのリボーク検証の際に利用が許容される最小のバージョン番号を記録した領域である。

【００７５】

前述したように、コンテンツリボケーションリスト（ＣＲＬ）には、図４（ｂ）に示すようにバージョン番号が設定され、例えば００１→００２→００３等、新たな発行処理ごとに、バージョン番号は増加する。すなわち、より新しいコンテンツリボケーションリスト（ＣＲＬ）のバージョン番号は、古いコンテンツリボケーションリスト（ＣＲＬ）のバージョン番号より大きな番号が設定される。

【００７６】

再生装置は、コンテンツ再生時に再生コンテンツのコンテンツＩＤを取得し、取得したコンテンツＩＤが、再生装置の記憶部に格納されたコンテンツリボケーションリスト（ＣＲＬ）に無効コンテンツとして記録されているか否かを検証する。コンテンツリボケーションリスト（ＣＲＬ）に再生予定のコンテンツのコンテンツＩＤが記録されている場合は、そのコンテンツは例えば不正にコピーされたコンテンツ等、不正コンテンツである可能性があるため、再生が禁止される。

【００７７】

しかし、再生装置が古いバージョンのコンテンツリボケーションリスト（ＣＲＬ）を参

照してコンテンツ再生可否を判定してしまうと、その古いＣＲＬの発行後に無効化されたコンテンツの再生がいつまでも許容されてしまう場合がある。

【００７８】

このような事態を防止するため、再生装置の利用を許容するコンテンツリボケーションリスト（ＣＲＬ）の最小のバージョン番号を設定する。このデータが、図５に示すサーバ証明書に記録されるコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）である。なお、このコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）は、後述するトークン（Ｔｏｋｅｎ）にも記録される。

【００７９】

再生装置は、コンテンツ再生処理に際して、コンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）より小さいバージョン番号の設定されたコンテンツリボケーションリスト（ＣＲＬ）、すなわち古いコンテンツリボケーションリスト（ＣＲＬ）を利用することは許容されない。なお、このような処理を実行する再生処理プログラムは、予め再生装置に提供され、コンテンツの再生処理においては、再生処理プログラムに従った処理が実行される。コンテンツ再生シーケンスについては後段でフローチャートを参照して説明する。

【００８０】

（５）サーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）

サーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）は、先に図４（ａ）を参照して説明した無効化（リボーク）されたサーバ（コンテンツサーバ）を記録したリストであるサーバリボケーションリスト（ＳＲＬ）に設定されたバージョン番号中、再生装置における利用が許容されるバージョン番号の最小値である。すなわち、再生装置において、コンテンツ再生の前処理として実行が義務付けられるサーバのリボーク検証の際に利用が許容される最小のバージョン番号を記録した領域である。

【００８１】

前述したように、サーバリボケーションリスト（ＳＲＬ）には、図４（ａ）に示すようにバージョン番号が設定される。例えば００１→００２→００３等、新たな発行処理ごとに、バージョン番号は増加する。すなわち、より新しいサーバリボケーションリスト（ＳＲＬ）のバージョン番号は、古いサーバリボケーションリスト（ＳＲＬ）のバージョン番号より大きな番号が設定される。

【００８２】

再生装置は、コンテンツ再生時に再生コンテンツやコンテンツ管理データを受領したサーバのサーバＩＤを取得し、取得したサーバＩＤが、再生装置の記憶部に格納されたサーバリボケーションリスト（ＳＲＬ）に無効サーバとして記録されているか否かを検証する。サーバリボケーションリスト（ＳＲＬ）に再生予定のコンテンツやコンテンツ管理データを受領したサーバのサーバＩＤが記録されている場合は、そのコンテンツは不正なサーバの提供コンテンツである可能性があるため、再生が禁止される。

【００８３】

しかし、再生装置が古いバージョンのサーバリボケーションリスト（ＳＲＬ）を参照してコンテンツ再生可否を判定してしまうと、その古いＳＲＬの発行後に無効化されたサーバ（コンテンツサーバ）の提供コンテンツの再生がいつまでも許容されてしまう場合がある。

【００８４】

このような事態を防止するため、再生装置の利用を許容するサーバリボケーションリスト（ＳＲＬ）の最小のバージョン番号を設定している。このデータが、図５に示すサーバ証明書に記録されるサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）である。なお、このサーバリボケーションリスト

（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）は、後述するトークン（Ｔｏｋｅｎ）にも記録される。

【００８５】

再生装置は、コンテンツ再生処理に際して、サーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）より小さいバージョン番号の設定されたサーバリボケーションリスト（ＳＲＬ）、すなわち古いサーバリボケーションリスト（ＳＲＬ）を利用することは許容されない。なお、このような処理を実行するための再生処理プログラムは、予め再生装置に提供され、コンテンツの再生処理においては、再生処理プログラムに従った処理が実行される。コンテンツ再生シーケンスについては後段でフローチャートを参照して説明する。

【００８６】

（６）メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）

メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）は、コンテンツを記録するメディア、例えば図１、図２に示すメモリカード３１、あるいは図３に示すメモリカード４００の記憶領域中に設定される保護領域（ＰＤＡ：Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）内のデータ読み取り（Ｒｅａｄ）や、書き込み（Ｗｒｉｔｅ）が許容された区分領域についての情報が記録される。

【００８７】

メモリカード４００の記憶領域の具体的構成例を図６に示す。

メモリカード４００の記憶領域は、図６に示すように、

（ａ）保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）４０１、

（ｂ）非保護領域（Ｕｓｅｒ　Ａｒｅａ）４０２、

これら２つの領域によって構成される。

【００８８】

（ｂ）非保護領域（Ｕｓｅｒ　Ａｒｅａ）４０２はユーザの利用する記録再生装置によって、自由にアクセス可能な領域であり、コンテンツや一般のコンテンツ管理データ等が記録される。ユーザによって自由にデータの書き込みや読み取りを行うことか可能な領域である。

【００８９】

一方、（ａ）保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）４０１は、自由なアクセスが許容されない領域である。

例えば、ユーザの利用する記録再生装置、再生装置、あるいはネットワークを介して接続されるサーバ等によってデータの書き込みあるいは読み取りを行おうとする場合、メモリカード４００に予め格納されたプログラムに従って、各装置に応じて読み取り（Ｒｅａｄ）または書き込み（Ｗｒｉｔｅ）の可否が決定される。

【００９０】

メモリカード４００は、予め格納されたプログラムを実行するためのデータ処理部や認証処理を実行する認証処理部を備えており、メモリカード４００は、まず、メモリカード４００に対してデータの書き込みまたは読み取りを実行しようとする装置との認証処理を行う。

【００９１】

この認証処理の段階で、相手装置、すなわちアクセス要求装置から公開鍵証明書等の装置証明書（たとえばサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ））を受信し、その証明書に記載された情報を用いて、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）４０１の各区分領域のアクセスが許容されるか否かを判定する。この判定処理は、図６に示す保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）４０１内の区分領域（図に示す領域＃０，＃１，＃２・・・）単位で判定処理が行われ、許可された区分領域で許可された処理のみが実行される。

【００９２】

このメディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉ

ｔｅ）は、例えば、アクセスしようとする装置、例えばコンテンツサーバ、あるいは記録再生装置（ホスト）単位で設定される。これらの情報は各装置対応のサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）や、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）に記録される。

【００９３】

メモリカード４００は、メモリカード４００に予め格納された規定のプログラムに従って、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）や、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）の記録データを検証して、アクセス許可のなされた領域についてのみアクセスを許容する処理を行う。

【００９４】

このサーバに対するアクセス許容情報が、図５に示す（６）メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）に相当する。

図５に示す（６）メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）には、例えば以下のような情報が記録される。

図６に示す保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）４０１中の、

領域（＃１）については、データの読み取り（Ｒｅａｄ）のみを許容、

領域（＃２）については、データの読み取り（Ｒｅａｄ）と書き込み（Ｗｒｉｔｅ）を許容、

領域（＃３）については、データの読み取り（Ｒｅａｄ）と書き込み（Ｗｒｉｔｅ）のいずれも許容しない、

このような区分領域単位のアクセス許容情報が記録される。

【００９５】

メモリカード４００のデータ処理部は、この情報を用いて各区分領域に対するアクセスの可否を判定する。なお、このアクセス判定の前処理としてアクセス要求装置と、メモリカード４００との間で相互認証処理が実行される。この相互認証が成立したことを条件としてアクセス要求装置から受領した証明書、例えばサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）を検証してアクセス許容領域の判定が行われる。

【００９６】

図５に示すように、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）には、上述したデータの他、［（７）その他の情報］が記録され、さらに、（１）～（７）の各データに対して認証局の秘密鍵によって生成された（８）署名（Ｓｉｇｎａｔｕｒｅ）が記録される。この署名により改ざんの防止構成が実現される。

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）を利用する場合は、署名検証を実行して、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）の正当性を確認した上で利用が行われる。なお、署名検証は、認証局の公開鍵を利用して実行される。

【００９７】

［３．サーバがコンテンツ管理情報として提供するトークンについて］

先に図３を参照して説明したように、コンテンツサーバ２００は、メモリカード４００に対するコンテンツの提供処理を実行する際に、コンテンツ２０２を暗号化して提供するとともに、コンテンツ管理情報としてのトークン２０１や、サーバリボケーションリスト（ＳＲＬ）２０３、コンテンツリボケーションリスト（ＣＲＬ）２０４、さらに図には示していないが、コンテンツの復号に適用する暗号鍵（バインドキー）等をコンテンツ記録装置（ホスト）３００に提供して、コンテンツと共にメモリカード４００に記録させる。

【００９８】

なお、コンテンツ記録装置（ホスト）３００にディスク２５０を装着し、ディスク２５０に格納されたコンテンツをメモリカード４００に記録する（コピー）場合には、コンテンツ記録装置（ホスト）３００は、コピー許可をコンテンツサーバ２００から得て、コンテンツのコピーを実行する。この処理のために、コンテンツ記録装置（ホスト）３００はコピー予定のコンテンツの識別子であるコンテンツＩＤをディスク２５０から取得してコンテンツサーバ２００に送信する。

【００９９】

なお、ディスク２５０に格納されたコンテンツも暗号化コンテンツであり、その復号に適用する鍵の他、図３に示すコンテンツ管理情報としてのトークン２０１や、サーバリボケーションリスト（ＳＲＬ）２０３、コンテンツリボケーションリスト（ＣＲＬ）２０４などがコンテンツサーバ２００からコンテンツ記録装置（ホスト）３００に提供され、ディスク２５０から提供されたコンテンツに対応する管理データとしてコンテンツと共にメモリカード４００に記録する処理が行われる。

【０１００】

コンテンツサーバ２００が生成して提供するトークン２０１の具体的なデータ構成例について図７を参照して説明する。

トークンは、図７に示すように、以下のデータを記録データとして有する。

（１）コンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）

（２）サーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）

（３）ボリュームＩＤ（ＰＶ　Ｖｏｌｕｍｅ　ＩＤ）

（４）コンテンツＩＤ（Ｃｏｎｔｅｎｔ　ＩＤ）

（５）コンテンツハッシュテーブルダイジェスト（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ　Ｄｉｇｅｓｔ（Ｓ））

（６）利用制御情報ハッシュ値（Ｕｓａｇｅ　Ｒｕｌｅ　Ｈａｓｈ）

（７）タイムスタンプ（Ｔｉｍｅ　ｓｔａｍｐ）

（８）その他の情報

（９）署名（Ｓｉｇｎａｔｕｒｅ）

【０１０１】

以下、上記（１）～（９）の各データについて説明する。

（１）コンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）

（２）サーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）

【０１０２】

これらのデータは、先に図５を参照して説明したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）に格納されたデータと同じデータである。

すなわち、再生装置においてコンテンツ再生時の前処理として実行されるコンテンツおよびサーバの有効性確認処理において利用の許容されるコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）の最小のバージョン番号を記録した領域である。

【０１０３】

再生装置は、トークンを参照して、これらの値を取得し、再生装置内のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）のバージョンがこのトークンに記録された最小値以上の値である場合にのみ、そのリボケーションリスト（ＣＲＬ／ＳＲＬ）を利用してコンテンツとサーバのリボーク（無効化）確認を行うことができる。再生装置がトークンに記録された最小値未満のバージョンの古いＣＲＬ／ＳＲＬのみしか保持していない場合には、コンテンツ再生処理は禁止されることになる。

なお、コンテンツ再生処理の詳細シーケンスについては後段でフローチャートを参照して説明する。

【０１０４】

（３）ボリュームＩＤ（ＰＶ　Ｖｏｌｕｍｅ　ＩＤ）

ボリュームＩＤ（ＰＶ　Ｖｏｌｕｍｅ　ＩＤ）は、所定単位（例えばタイトル単位）のコンテンツに対応する識別子（ＩＤ）である。このＩＤは、例えばコンテンツ再生時に利用可能性のあるＪａｖａ（登録商標）アプリケーションであるＢＤ－Ｊ／ＡＰＩやＢＤ＋

ＡＰＩ等によって参照される場合があるデータである。

【０１０５】

（４）コンテンツＩＤ（Ｃｏｎｔｅｎｔ　ＩＤ）

コンテンツＩＤ（Ｃｏｎｔｅｎｔ　ＩＤ）はコンテンツを識別する識別子であるが、トークンに記録されるコンテンツＩＤは、コンテンツまたはコンテンツ管理データ（トークンを含む）を提供したサーバＩＤを含むデータとして設定される。すなわち、

コンテンツＩＤ＝サーバＩＤ（Ｓｅｒｖｅｒ　ＩＤ）＋コンテンツ固有ＩＤ（Ｕｎｉｑｕｅ　Ｃｏｎｔｅｎｔ　ＩＤ）

上記のようにサーバＩＤを含むデータとしてコンテンツＩＤが記録される。

【０１０６】

サーバＩＤは、認証局が各コンテンツサーバに設定したＩＤである。先に図５を参照して説明したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）に記録されたサーバＩＤと同じＩＤである。

コンテンツ固有ＩＤは、コンテンツサーバが独自に設定するコンテンツ対応の識別子（ＩＤ）である。

トークンに記録されるコンテンツＩＤは、このように認証局の設定したサーバＩＤとコンテンツサーバの設定したコンテンツ固有ＩＤの組み合わせとして構成される。

【０１０７】

なお、コンテンツＩＤの構成ビット数や、サーバＩＤのビット数、コンテンツ固有ＩＤのビット数は予め規定されており、コンテンツを再生する再生装置は、トークンに記録されたコンテンツＩＤから所定ビット数の上位ビットを取得してサーバＩＤを取得し、コンテンツＩＤから所定の下位ビットを取得することでコンテンツ固有ＩＤを得ることが可能となる。

【０１０８】

（５）コンテンツハッシュテーブルダイジェスト（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ　Ｄｉｇｅｓｔ（Ｓ））

コンテンツハッシュテーブルダイジェスト（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ　Ｄｉｇｅｓｔ（Ｓ））は、メモリカードに格納されるコンテンツのハッシュ値を記録したデータである。このデータは、コンテンツが改ざん検証処理に利用される。

【０１０９】

コンテンツを再生する再生装置は、メモリカードに記録された再生予定のコンテンツのハッシュ値を計算し、トークンに記録されたコンテンツハッシュテーブルダイジェスト（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ　Ｄｉｇｅｓｔ（Ｓ））の記録値との比較を実行する。計算データと登録データとが一致としていればコンテンツの改ざんはないと判定されコンテンツ再生が可能となる。一致しない場合は、コンテンツは改ざんされている可能性があると判定され、再生は禁止される。

【０１１０】

（６）利用制御情報ハッシュ値（Ｕｓａｇｅ　Ｒｕｌｅ　Ｈａｓｈ）

利用制御情報ハッシュ値（Ｕｓａｇｅ　Ｒｕｌｅ　Ｈａｓｈ）はサーバがコンテンツの管理データとしてユーザに提供しメモリカードに記録させる利用制御情報のハッシュ値である。

利用制御情報は、例えばコンテンツのコピーを許容するか否か、コピーの許容回数、他機器への出力可否などのコンテンツの利用形態の許容情報などを記録したデータであり、コンテンツとともにメモリカードに記録される情報である。

利用制御情報ハッシュ値は、この利用制御情報の改ざん検証用のデータとして利用されるハッシュ値である。

【０１１１】

コンテンツを再生する再生装置は、メモリカードに記録された再生予定のコンテンツに対応する利用制御情報のハッシュ値を計算し、トークンに記録された利用制御情報ハッシュ値（Ｕｓａｇｅ　Ｒｕｌｅ　Ｈａｓｈ）の記録値との比較を実行する。計算データと登

録データとが一致としていれば利用制御情報の改ざんはないと判定され、利用制御情報に従ったコンテンツ利用が可能となる。一致しない場合は、利用制御情報は改ざんされている可能性があると判定され、コンテンツの再生等の利用処理は禁止される。

【０１１２】

（７）タイムスタンプ（Ｔｉｍｅ　ｓｔａｍｐ）

タイムスタンプ（Ｔｉｍｅ　ｓｔａｍｐ）は、このトークンの作成日時、例えば図７の（９）に示す署名の作成日時情報である。

【０１１３】

トークン（Ｔｏｋｅｎ）には、上述したデータの他、図７に示すように［（８）その他の情報］が記録され、さらに、（１）～（８）の各データに対してサーバの秘密鍵によって生成された（９）署名（Ｓｉｇｎａｔｕｒｅ）が記録される。この署名によりトークンの改ざん防止構成が実現される。

【０１１４】

トークン（Ｔｏｋｅｎ）を利用する場合は、署名検証を実行して、トークン（Ｔｏｋｅｎ）が改ざんのない正当なトークンであることを確認した上で利用が行われる。なお、署名検証は、サーバの公開鍵を利用して実行される。サーバの公開鍵は、先に図５を参照して説明したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）から取得可能である。

【０１１５】

［４．サーバとメモリカード間の処理とメモリカードの格納データについて］

次に、図８以下を参照してサーバとメモリカード間の処理とメモリカードの格納データについて説明する。

【０１１６】

図８には、左から、

（Ａ）コンテンツサーバ

（Ｂ）コンテンツ記録装置（ホスト）

（Ｃ）メモリカード

これらを示している。

（Ａ）コンテンツサーバは、図３に示すコンテンツサーバ２００に対応し、

（Ｂ）コンテンツ記録装置は、図３に示すコンテンツ記録装置（ホスト）３００に対応し、

（Ｃ）メモリカードは図３に示すメモリカード４００に対応する。

【０１１７】

図８には、コンテンツサーバがメモリカードに対して、コンテンツと、コンテンツ以外のコンテンツ管理情報を提供して記録させる場合の処理シーケンスを示している。

なお、コンテンツを図３に示すディスク２５０からコピーしてメモリカードに記録する場合は、コンテンツはディスクからメモリカードに記録されるが、その他のトークンを含む管理データについては、コンテンツサーバからメモリカードに送信されて記録される。

【０１１８】

なお、図８に示す（Ｃ）メモリカードは、（Ｂ）コンテンツ記録装置（ホスト）に装着し、（Ｂ）コンテンツ記録装置（ホスト）の通信部を介して（Ａ）コンテンサーバとの通信を実行し、（Ａ）コンテンツサーバから受信する各種のデータを（Ｂ）コンテンツ記録装置（ホスト）を介して受信してメモリカードに記録する。

【０１１９】

図８を参照して処理シーケンスについて説明する。

まず、ステップＳ２１において、コンテンツサーバとメモリカード間で相互認証処理を実行する。例えば公開鍵暗号方式に従って、双方の公開鍵証明書の交換処理等を含む相互認証処理を行う。コンテンツサーバは先に説明したように、認証局の発行した公開鍵を格納したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）と秘密鍵を保持している。メモリカードも予め認証局から公開鍵証明書と秘密鍵のペアを受信し自己の記憶部に格

納している。
【０１２０】
なお、メモリカードは相互認証処理や、図６を参照して説明した保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するアクセス可否判定を行うプログラムを格納し、これらのプログラムを実行するデータ処理部を有する。
【０１２１】
コンテンツサーバとメモリカード間の相互認証が成立し、双方の正当性が確認されると、サーバはメモリカードに対して様々なデータを提供する。相互認証が成立しない場合は、サーバからのデータ提供処理は行われない。
【０１２２】
相互認証の成立後、コンテンツサーバは、データベース２１１に記録されたボリュームＩＤ等のデータを取得して、トークン２１３を生成し、ステップＳ２２においてトークンに対する署名を実行して、コンテンツ記録装置（ホスト）に対してメモリカードに対する書き込みデータとして送信する。
【０１２３】
トークン２１３は、先に図７を参照して説明したように、以下のデータを含む。
（１）コンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）
（２）サーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（ＭｉｎｉｍｕｍＳＲＬ　Ｖｅｒｓｉｏｎ）
（３）ボリュームＩＤ（ＰＶ　Ｖｏｌｕｍｅ　ＩＤ）
（４）コンテンツＩＤ（Ｃｏｎｔｅｎｔ　ＩＤ）
（５）コンテンツハッシュテーブルダイジェスト（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ　Ｄｉｇｅｓｔ（Ｓ））
（６）利用制御情報ハッシュ値（Ｕｓａｇｅ　Ｒｕｌｅ　Ｈａｓｈ）
（７）タイムスタンプ（Ｔｉｍｅ　ｓｔａｍｐ）
（８）その他の情報
（９）署名（Ｓｉｇｎａｔｕｒｅ）
【０１２４】
これらのデータを含むトークンが、（Ａ）コンテンツサーバから（Ｂ）コンテンツ記録装置（ホスト）を介して（Ｃ）メモリカードに送信され、メモリカードに記録される。この記録データが図８の（Ｃ）メモリカード中に示すトークン（Ｔｏｋｅｎ）４１５である。
【０１２５】
なお、メモリカードは、先に図６を参照して説明したように保護領域（ｐｏｔｅｃｔｅｄ　Ａｒｅａ）と非保護領域（Ｕｓｅｒ　Ａｒｅａ）に分割されている。
図８に示す（Ｃ）メモリカードには保護領域（ｐｏｔｅｃｔｅｄ　Ａｒｅａ）４１２を示している。保護領域（ｐｏｔｅｃｔｅｄ　Ａｒｅａ）４１２は、図に示すようにバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））４１４が記録される。その他のデータは、非保護領域（Ｕｓｅｒ　Ａｒｅａ）に記録される。
【０１２６】
なお、バインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））４１４は暗号化コンテンツの復号に適用するタイトルキー（ＣＰＳユニットキーとも呼ばれる）の暗号化処理に利用される鍵であり、コンテンツサーバにおいて乱数生成処理等によって生成される。
【０１２７】
図８（Ａ）コンテンツサーバのステップＳ２３の処理として示すように、バインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））は、コンテンツサーバにおいて生成される。この鍵は、コンテンツのメモリカードに対する提供処理、あるいはディスクからのヒンテンツのコピー処理が実行される毎に、サーバが、逐次、乱数生成等を実行して生成してメモリカードに提供する。従って、コンテンツの提供あるいはコピー処理ごとに異なるバインドキ

ーが生成されることになる。

【０１２８】

サーバの生成したバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））は、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に書き込まれる。

なお、先に図６を参照して説明したように、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するデータの書き込み（Ｗｒｉｔｅ）、あるいは保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）からのデータ読み込み（Ｒｅａｄ）処理は制限された処理である。アクセス要求装置（サーバや、記録再生装置（ホスト））単位、および各区分領域（＃１，＃２・・・）単位で書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の可否が設定されている。この設定情報はサーバであればサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）、記録再生装置（ホスト）であればホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）に記録されている。

【０１２９】

メモリカードは、アクセス要求装置から受領した証明書、本例ではサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）を参照して、書き込みの許容された保護領域内の区分領域にバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））を記録する。図８に示すバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））４１４である。なお、図８では、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）４１２の内部を詳細に示していないが、この保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）は図６を参照して説明したように複数の区分領域（＃０，＃１，＃２・・・）に区分されており、サーバ証明書に書き込み許容領域として記録された区分領域にバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ（Ｋｂ））４１４が記録される。

【０１３０】

なお、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）はステップＳ２１の認証処理に際して、メモリカードがコンテンツサーバから受領した証明書を参照することができる。なお、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）には認証局の署名が設定され、メモリカードは認証局の公開鍵を適用して署名検証を実行し、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）の正当性を確認していることが前提となる。

【０１３１】

なお、コンテンツサーバからメモリカードへのバインドキーの送信は、セッションキーで暗号化したデータとして送信が行われる。

セッションキーは、サーバとメモリカード間の相互認証処理（ステップＳ２１）時に生成され、双方で共有する鍵である。メモリカードは、暗号化されたバインドキーをセッションキーで復号してメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の所定の区分領域に記録する。

【０１３２】

図８に示す（Ａ）コンテンツサーバは、次に、生成したバインドキー（Ｋｂ）と、（Ｃ）メモリカードから受領したメディアＩＤを利用して、ステップＳ２４において、鍵生成処理（ＡＥＳ－Ｇ）を行う。ここで生成する鍵はボリュームユニークキーと呼ばれる。

なお、メディアＩＤは、メモリカードの識別情報としてメモリカード内のメモリに予め記録されたＩＤである。

【０１３３】

次に、コンテンツサーバは、ステップＳ２５において、コンテンツの暗号化キーであるタイトルキー（ＣＰＳユニットキー）２１５をボリュームユニークキーで暗号化して暗号化タイトルキーを生成する。

【０１３４】

（Ａ）コンテンツサーバは生成した暗号化タイトルキーを（Ｂ）コンテンツ記録装置（ホスト）を介して（Ｃ）メモリカードに送信する。メモリカードは、受信した暗号化タイトルキーをメモリカードに記録する。この記録データが図８の（Ｃ）メモリカード中に示す暗号化タイトルキー４１６である。なお、タイトルキーはＣＰＳユニットキーとも呼ばれる。

【０１３５】
さらに、コンテンツサーバは、コンテンツに対応する利用制御情報２１６を生成して、ステップＳ２７でコンテンツサーバの秘密鍵で署名処理を実行してメモリカードに提供する。
また、コンテンツサーバは、ステップＳ２８において、コンテンツ２１８をタイトルキー２１５で暗号化してメモリカードに提供する。
【０１３６】
メモリカードは、これらのサーバからの提供データを記録する。この記録データが図８の（Ｃ）メモリカード中に示す利用制御情報４１７、暗号化コンテンツ４１８である。
【０１３７】
なお、図８に示す処理シーケンス中には示していないが、コンテンツサーバは、これらのデータの他、例えば、
（１）コンテンツリボケーションリスト（ＣＲＬ）
（２）サーバリボケーションリスト（ＳＲＬ）
これらのデータをメモリカードに提供し、メモリカードはこれらのデータをメモリカードに記録する。
【０１３８】
図９にメモリカード内に記録されるデータを示すディレクトリ構造と、コンテンツ再生処理を実行する再生装置内に記録されるデータの例を示す。
【０１３９】
図９の左側がメモリカードのディレクトリ構成であり、
ルート［ｒｏｏｔ］ディレクトリ以下に設定される主にＢＤ関連コンテンツを設定するディレクトリである［ＢＤＭＶ］ディレトトリの下位にサーバからのダウンロードまたはディスクからのコピーコンテンツやその管理情報を記録するディレクトリ［ＤＥＬＴＡ］が設定され、ディレクトリ［ＤＥＬＴＡ］以下に、サーバから提供されるコンテンツやコンテンツ管理データが記録される。
なお、図に示すディレクトリ構成は一例であり、メモリカードに対する記録構成は、この例に限らず、様々な構成とすることができる。ただし、コンテンツとコンテンツに対応するトークン等を含む管理情報はその対応関係を識別可能とする設定で記録されることが必要である。
【０１４０】
図９に示すメモリカードのディレクトリ［ＤＥＬＴＡ］以下の設定データについて説明する。
ＣＰＳユニットキーファイル（ＣＰＳ　Ｕｎｉｔ　Ｋｅｙ　Ｆｉｌｅ）４２１は、図８に示す暗号化タイトルキー４１６に対応する。
トークン（Ｔｏｋｅｎ）４２２は、図８に示すトークン４１５に対応する。
コンテンツハッシュテーブル４２３は、図８には示していないが、コンテンツのハッシュ値としてコンテンツサーバから提供され記録される。
【０１４１】
利用制御情報（ＣＰＳユニットＵｓａｇｅ　Ｆｉｌｅ＃１～＃ｎ）４２４＃１～＃ｎは、図８に示す利用制御情報４１７に対応する。なお、ＣＰＳユニットはコンテンツの利用単位（再生単位）として設定されるユニットであり、各ユニット単位で利用制御情報が設定される。
【０１４２】
サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）４２５は、図８に示す認証処理（ステップＳ２１）において、サーバから受領する証明書であり、先に図５を参照して説明したようにサーバＩＤやサーバの公開鍵等が格納された構成を持つ。
【０１４３】
コンテンツリボケーションリスト（ＣＲＬ）４２６は無効化（リボーク）されたコンテンツの識別子（ＩＤ）を記録したリストであり、先に図４（ｂ）を参照して説明したデー

タ構成を持つ。
サーバリボケーションリスト（ＳＲＬ）４２７は無効化（リボーク）されたサーバの識別子（ＩＤ）を記録したリストであり、先に図４（ａ）を参照して説明したデータ構成を持つ。
メモリカードには、このようなコンテンツやコンテンツ管理データが記録される。
【０１４４】
なお、図には示していないが、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）にはバインドキーが記録される。
暗号化コンテンツの復号処理にはタイトルキー（ＣＰＳユニットキー）を取得することが必要であり、このタイトルキーは、前述したように、バインドキーとメディアＩＤを利用して生成されるボリュームユニークキーで暗号化されている。
【０１４５】
従って、再生装置においてタイトルキーを取得するためには、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に記録されたバインドキーを取り出して、さらにメディアＩＤを利用してボリュームユニークキーを生成して、生成したボリュームユニークキーを適用して暗号タイトルキー（暗号化ＣＰＳユニットキー）を復号してタイトルキー（ＣＰＳユニットキー）取得する処理を行うことが必要となる。
【０１４６】
図９の右側には、メモリカードに記録されたコンテンツの再生処理を実行する再生装置のメモリに格納されるデータ例を示している。コンテンツの再生処理を実行する再生装置は、例えば、図１、図２に示す記録再生器２２、ＰＣ２３、あるいは再生機能のみを持つ再生装置などである。これら、コンテンツの再生処理を実行する再生装置は、
サーバリボケーションリスト（ＳＲＬ）３１１、
コンテンツリボケーションリスト（ＣＲＬ）３１２、
これらのリストをメモリに記録している。
【０１４７】
なお、コンテンツの再生処理を実行する再生装置では、コンテンツ再生処理に際して再生装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）３１１と、コンテンツリボケーションリスト（ＣＲＬ）３１２のバージョンと、その時点で再生装置が取得可能なサーバリボケーションリスト（ＳＲＬ）と、コンテンツリボケーションリスト（ＣＲＬ）のバージョン比較を実行し、自装置のメモリに格納された各リストのバージョンより新しいバージョンのリストが取得できる場合は、メモリに格納された古いバージョンのリストを新しいバージョンのリストに置き換えるリストの更新処理を実行する。
【０１４８】
例えば再生装置がメモリカードに記録されたコンテンツを再生する場合には、メモリカードに記録されているサーバリボケーションリスト（ＳＲＬ）４２６と、コンテンツリボケーションリスト（ＣＲＬ）４２７の各リストのバージョンと、再生装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）３１１と、コンテンツリボケーションリスト（ＣＲＬ）３１２のバージョンを比較する。
【０１４９】
例えば、メモリカードに記録されているサーバリボケーションリスト（ＳＲＬ）４２６と、コンテンツリボケーションリスト（ＣＲＬ）４２７の各リストのバージョンが、再生装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）３１１と、コンテンツリボケーションリスト（ＣＲＬ）３１２のバージョンが新しい（例えばバージョン値が大きい値である）場合には、再生装置は再生装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）３１１と、コンテンツリボケーションリスト（ＣＲＬ）３１２を、メモリカードに記録されているサーバリボケーションリスト（ＳＲＬ）４２６と、コンテンツリボケーションリスト（ＣＲＬ）４２７の各リストに置き換える処理を行う。
【０１５０】
さらに、ディスクからコンテンツ再生を行う場合に、ディスクからより新しいリボケー

ジョンリストが得られる場合には、メモリに格納されたリストをディスクから読み取られるリストによる更新を行う。
このように、再生装置は、より新しいリボケーションリストに置き換える処理を実行する。この処理の実行シーケンスは例えば再生装置が保持する再生処理プログラム中の一部に記録されており、再生装置はプログラムにしたがって各リボケーションリストの更新を実行する。
【０１５１】
再生装置に予め記録されたコンテンツ再生プログラムを実行すると、再生装置に記録された、
サーバリボケーションリスト（ＳＲＬ）３１１、
コンテンツリボケーションリスト（ＣＲＬ）３１２、
これらの各リストのバージョンと、その時点で利用可能なリスト、例えばサーバから受信、あるいはディスク等から読み取ったリストのバージョン比較を実行して、新しいバージョンのリストが得られた場合は、装置のメモリに記録された古いリストを更新する処理が行われる。
【０１５２】
［５．サーバからのコンテンツダウンロード処理シーケンスについて］
次に、図１０以下のフローチャートを参照してサーバからのコンテンツダウンロード処理シーケンスについて説明する。
【０１５３】
図１０に示すフローチャートは、例えば図１に示すコンテンツサーバ１１からコンテンツをダウンロードして図１に示すメモリカード３１に記録する場合の処理である。
図１０に示すフローは、図１に示す（ｂ）コンテンツ記録装置（共用端末２１、記録再生装置２２、ＰＣ２３等）のデータ処理部において実行する処理である。ただし、メモリカードに対するデータ書き込み、読み取り等の処理に際してはメモリカードのデータ処理部においても処理が実行される場合がある。
例えば、ステップＳ１０９のバインドキーの書き込み処理に際しては、メモリカードのデータ処理部において、先に図６を参照して説明した保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対する書き込み可否の判定が行われる。
【０１５４】
図１０に示すフローチャートの各ステップについて説明する。
ステップＳ１０１において、装置にメモリカードを装着し、サーバに対するアクセスを行う。なお、この時点で、先に図８のステップＳ２１の処理として説明したサーバとメモリカードとの相互認証処理が実行される。ステップＳ１０２以下の処理はこの相互認証処理が成立した場合に実行される。相互認証が成立しなかった場合にはコンテンツダウンロード処理は実行されない。なお、記録再生装置とサーバ間、さらに記録再生装置とメモリカード間の相互認証処理も必要に応じて行う構成としてよい。
【０１５５】
少なくともサーバとメモリカードとの相互認証が成立した後、様々なデータがメモリカードに提供され、メモリカードに格納される。なお、サーバとの通信はメモリカードを装着した装置、例えば図１に示す（ｂ）コンテンツ記録装置（共用端末２１、記録再生装置２２、ＰＣ２３等）を介して行われる。
【０１５６】
ステップＳ１０２では、
トークン（Ｔｏｋｅｎ）、
コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ），
サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、
サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）、

これらの各データのダウンロード処理、読み取り処理、メモリカードに対する書き込み処理を行う。

【０１５７】

トークン（Ｔｏｋｅｎ）は、先に図７を参照して説明したデータを持つ。

コンテンツリボケーションリスト（ＣＲＬ）は、先に図４（ｂ）を参照して説明した無効化（リボーク）コンテンツの識別子（ＩＤ）を記録したリストである。

サーバリボケーションリスト（ＳＲＬ）は、先に図４（ａ）を参照して説明した無効化（リボーク）サーバの識別子（ＩＤ）を記録したリストである。

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）は、先に図５を参照して説明したサーバ公開鍵を格納したデータである。

【０１５８】

なお、コンテンツリボケーションリスト（ＣＲＬ）と、サーバリボケーションリスト（ＳＲＬ）と、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）は図３に示す認証局１００が発行し、認証局の秘密鍵による署名が設定されている。

トークン（Ｔｏｋｅｎ）は、サーバ（例えば図３に示すコンテンツサーバ２００）が発行し、サーバの秘密鍵による署名が設定されている。

【０１５９】

ステップＳ１０３では、ステップＳ１０２においてサーバから取得したコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）の検証処理と再生器のメモリへの取り込み処理を実行する。

このステップＳ１０３の詳細シーケンスについて、図１１に示すフローチャートを参照して説明する。

【０１６０】

図１１のステップＳ１５１において処理を開始する。この処理は、図１０に示すフローのステップＳ１０１～Ｓ１０２の処理の完了後に行われる。すなわちメモリカードを装着し、装着したメモリカードに以下のデータ、すなわち、

トークン（Ｔｏｋｅｎ）、

コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ），

サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ），

これらのデータの記録が完了した後に行われる。

【０１６１】

ステップＳ１５２において、

メモリカードに記録した、

コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ），

サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）

これらのデータを読み取る。

これらはサーバからダウンロードしたデータである。

【０１６２】

ステップＳ１５３において、コンテンツリボケーションリスト（ＣＲＬ）の署名検証を実行する。

前述したようにコンテンツリボケーションリスト（ＣＲＬ）は、図３を参照して説明したように認証局（認証サーバ）１００の発行するリストであり、認証局の秘密鍵による署名が付与されている。ステップＳ１５３では、この署名の検証を実行する。なお、署名に必要となる認証局公開鍵は、認証局公開鍵証明書から取得可能であり、この処理を実行する機器（例えば図１（ｂ）コンテンツ記録装置（共用端末２１、記録再生装置２２、ＰＣ

２３等））に格納されている。格納されていない場合は必要に応じて取得する。
【０１６３】
ステップＳ１５３において、コンテンツリボケーションリスト（ＣＲＬ）の署名検証が成立し、コンテンツリボケーションリスト（ＣＲＬ）が改ざんのない正当なリストであることが確認された場合は、ステップＳ１５４に進む。
【０１６４】
一方、ステップＳ１５３において、コンテンツリボケーションリスト（ＣＲＬ）の署名検証が成立せず、コンテンツリボケーションリスト（ＣＲＬ）が改ざんのない正当なリストであることが確認されなかった場合は、ステップＳ１６０に進み、その後の処理を中止する。この場合は、図１０のフローのステップＳ１０４以下の処理がすべて中止されることになり、コンテンツのダウンロード（Ｓ１０６）も行われない。
【０１６５】
ステップＳ１５３において、コンテンツリボケーションリスト（ＣＲＬ）の署名検証が成立し、コンテンツリボケーションリスト（ＣＲＬ）が改ざんのない正当なリストであることが確認された場合は、ステップＳ１５４に進む。
【０１６６】
ステップＳ１５４では、
メディア（メモリカード）にダウンロードして記録したコンテンツリボケーションリスト（ＣＲＬ）のバージョンと、この処理を実行中の装置、例えば図１（ｂ）コンテンツ記録装置（共用端末２１、記録再生装置２２、ＰＣ２３等））のメモリに格納されているコンテンツリボケーションリスト（ＣＲＬ）のバージョンとの比較処理を実行する。
【０１６７】
この処理は、先に図９を参照して説明した２つのコンテンツリボケーションリスト（ＣＲＬ）、すなわち、
（１）サーバからダウンロードして、メモリカード内に記録したコンテンツリボケーションリスト（ＣＲＬ）４２７、
（２）再生器内のメモリに格納済みのコンテンツリボケーションリスト（ＣＲＬ）３１２、
これら２つのＣＲＬのバージョン比較処理に相当する。
再生器は、ダウンロード処理を実行中の機器（例えば図１（ｂ）コンテンツ記録装置（共用端末２１、記録再生装置２２、ＰＣ２３等））に対応する。
【０１６８】
ステップＳ１５４において、
メディア（メモリカード）にダウンロード記録したコンテンツリボケーションリスト（ＣＲＬ）のバージョン値＞再生器のメモリに記録されたコンテンツリボケーションリスト（ＣＲＬ）のバージョン値
上記式が成立する場合は、ステップＳ１５５に進む。
【０１６９】
上記式が成立する場合とは、メディア（メモリカード）にダウンロード記録したコンテンツリボケーションリスト（ＣＲＬ）が、再生器（例えば図１（ｂ）コンテンツ記録装置（共用端末２１、記録再生装置２２、ＰＣ２３等））のメモリに記録されたコンテンツリボケーションリスト（ＣＲＬ）より新しいことを意味する。
この場合は、ステップＳ１５５において、メディア（メモリカード）にダウンロード記録した新しいコンテンツリボケーションリスト（ＣＲＬ）を、再生器（例えば図１（ｂ）コンテンツ記録装置（共用端末２１、記録再生装置２２、ＰＣ２３等））のメモリに記録されている古いコンテンツリボケーションリスト（ＣＲＬ）に置き換える更新処理を実行する。
【０１７０】
コンテンツの再生処理を行う再生装置は、コンテンツ再生処理に際して、自装置のメモリに格納されたリボケーションリストを参照してコンテンツやサーバのリボーク（無効化

）状況を判定するので、このような更新処理を行うことで、より新しいリストを適用した適正な判断が可能となる。なお、コンテンツ再生処理シーケンスについては後段で説明する。

【０１７１】

ステップＳ１５５におけるコンテンツリボケーションリスト（ＣＲＬ）の更新処理が完了した場合、および、ステップＳ１５４において、メディア（メモリカード）にダウンロード記録したコンテンツリボケーションリスト（ＣＲＬ）が装置内のメモリに記録済みのコンテンツリボケーションリスト（ＣＲＬ）より新しくないと判定された場合（ステップＳ１５４の判定がＮｏ）は、ステップＳ１５６に進む。

【０１７２】

ステップＳ１５６では、サーバリボケーションリスト（ＳＲＬ）の署名検証を実行する。

前述したようにサーバリボケーションリスト（ＳＲＬ）は、図３を参照して説明した認証局（認証サーバ）１００の発行するリストであり、認証局の秘密鍵による署名が付与されている。ステップＳ１５６では、この署名の検証を実行する。なお、署名に必要となる認証局公開鍵は、認証局公開鍵証明書から取得可能であり、この処理を実行する装置（例えば図１（ｂ）コンテンツ記録装置（共用端末２１、記録再生装置２２、ＰＣ２３等））に格納されている。格納されていない場合は必要に応じて取得する。

【０１７３】

ステップＳ１５６において、サーバリボケーションリスト（ＳＲＬ）の署名検証が成立し、サーバリボケーションリスト（ＳＲＬ）が改ざんのない正当なリストであることが確認された場合は、ステップＳ１５７に進む。

【０１７４】

一方、ステップＳ１５６において、サーバリボケーションリスト（ＳＲＬ）の署名検証が成立せず、サーバリボケーションリスト（ＳＲＬ）が改ざんのない正当なリストであることが確認されなかった場合は、ステップＳ１６０に進み、その後の処理を中止する。この場合は、図１０のフローのステップＳ１０４以下の処理がすべて中止されることになり、コンテンツのダウンロード（Ｓ１０６）も行われない。

【０１７５】

ステップＳ１５６において、サーバリボケーションリスト（ＳＲＬ）の署名検証が成立し、サーバリボケーションリスト（ＳＲＬ）が改ざんのない正当なリストであることが確認された場合は、ステップＳ１５７に進み、メディア（メモリカード）にダウンロードして記録したサーバリボケーションリスト（ＳＲＬ）のバージョンと、この処理を実行中の装置、例えば図１（ｂ）コンテンツ記録装置（共用端末２１、記録再生装置２２、ＰＣ２３等））のメモリに格納されているサーバリボケーションリスト（ＳＲＬ）のバージョンとの比較処理を実行する。

【０１７６】

この処理は、先に図９を参照して説明した２つのサーバリボケーションリスト（ＳＲＬ）、すなわち、

（１）サーバからダウンロードして、メモリカード内に記録したサーバリボケーションリスト（ＳＲＬ）４２６、

（２）再生器内のメモリに格納済みのサーバリボケーションリスト（ＳＲＬ）３１１、

これら２つのＳＲＬのバージョン比較処理に相当する。

再生器は、ダウンロード処理を実行中の機器（例えば図１（ｂ）コンテンツ記録装置（共用端末２１、記録再生装置２２、ＰＣ２３等））に対応する。

【０１７７】

ステップＳ１５７において、

メディア（メモリカード）にダウンロード記録したサーバリボケーションリスト（ＳＲＬ）のバージョン値＞再生器のメモリに記録されたサーバリボケーションリスト（ＳＲＬ）のバージョン値、

上記式が成立する場合は、ステップＳ１５８に進む。

【０１７８】

上記式が成立する場合とは、メディア（メモリカード）にダウンロード記録したサーバリボケーションリスト（ＳＲＬ）が、再生器（例えば図１（ｂ）コンテンツ記録装置（共用端末２１、記録再生装置２２、ＰＣ２３等））のメモリに記録されたサーバリボケーションリスト（ＳＲＬ）より新しいことを意味する。

この場合は、ステップＳ１５８において、メディア（メモリカード）にダウンロード記録した新しいサーバリボケーションリスト（ＳＲＬ）を、再生器（例えば図１（ｂ）コンテンツ記録装置（共用端末２１、記録再生装置２２、ＰＣ２３等））のメモリに記録されている古いサーバリボケーションリスト（ＳＲＬ）に置き換える更新処理を実行する。

【０１７９】

前述したように、再生装置はコンテンツ再生処理に際して、自装置のメモリに格納されたリボケーションリストを参照してコンテンツやサーバのリボーク（無効化）状況を判定するので、このような更新処理を行うことで、より新しいリストを適用した適正な判断が可能となる。なお、コンテンツ再生処理シーケンスについては後段で説明する。

【０１８０】

ステップＳ１５８におけるサーバリボケーションリスト（ＳＲＬ）の更新処理が完了した場合、および、ステップＳ１５７において、メディア（メモリカード）にたダウンロード記録したサーバリボケーションリスト（ＳＲＬ）が装置内のメモリに記録済みのサーバリボケーションリスト（ＳＲＬ）より新しくないと判定された場合（ステップＳ１５７の判定がＮｏ）は、この処理を終了し、図１０のフローのステップＳ１０４に進む。

【０１８１】

図１０に示すフローチャートに戻り、ステップＳ１０４以下の処理について説明する。

ステップＳ１０４では、

（１）ダウンロード予定のコンテンツがリボーク（無効化）されているか否か、

（２）トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）のバージョンより大きいか否か、

これらの判定処理を実行する。

各判定処理について説明する。

【０１８２】

（１）ダウンロード予定のコンテンツがリボーク（無効化）されているか否か、

この処理は、ダウンロード予定のコンテンツのコンテンツＩＤが、装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）に記録されているか否かの判定処理として行われる。なお、コンテンツＩＤはサーバに対するダウンロード要求時にサーバから受領したコンテンツＩＤを用いてもよいし、トークン中に記録されたコンテンツＩＤ中のコンテンツ固有ＩＤを用いてもよい。あるいはサーバから別途、コンテンツＩＤを記録したコンテンツ証明書を受信してその証明書に記載されたコンテンツＩＤを用いてもよい。

【０１８３】

ダウンロード予定のコンテンツのコンテンツＩＤが、装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）に記録されている場合、そのコンテンツはリボーク（無効化）コンテンツであり、ステップＳ１０４の判定はＹｅｓとなり、以下の処理は実行されず、ステップＳ１１０に進み、他ダウンロード処理は中止される。この場合、コンテンツのダウンロード（Ｓ１０６）は実行されない。

【０１８４】

また、ステップＳ１０４のもう１つの判定処理である、

（２）トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）の

バージョンより大きいか否かの判定において大きいと判定された場合には、装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）は利用できないことになり、この場合もステップＳ１０４の判定はＹｅｓとなり、以下の処理は実行されず、ステップＳ１１０に進み、他ダウンロード処理は中止される。この場合、コンテンツのダウンロード（Ｓ１０６）は実行されない。

【０１８５】

ステップＳ１０４において、

（１）ダウンロード予定のコンテンツがリボーク（無効化）されていないと判定され、

かつ、

（２）トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）のバージョンより大きくないと判定された場合にのみ、

ステップＳ１０４の判定がＮｏとなり、次のステップＳ１０５の処理に進む。

【０１８６】

ステップＳ１０５では、

（１）ダウンロード処理を行っているサーバがリボーク（無効化）されているか否か、

（２）トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）のバージョンより大きいか否か、

これらの判定処理を実行する。

各判定処理について説明する。

【０１８７】

（１）ダウンロード処理を行っているサーバがリボーク（無効化）されているか否か、

この処理は、ダウンロード処理を行っているサーバのサーバＩＤが、装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）に記録されているか否かの判定処理として行われる。なお、サーバＩＤは例えばステップＳ１０２において取得したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）から取得できる。なお、この処理の前提としてサーバ証明書に付与された認証局の署名検証処理によって、サーバ証明書の正当性の確認を行う。

【０１８８】

ダウンロード処理を行っているサーバのサーバＩＤが、装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）に記録されている場合、そのサーバはリボーク（無効化）されたサーバであり、ステップＳ１０５の判定はＹｅｓとなり、以下の処理は実行されず、ステップＳ１１０に進み、他ダウンロード処理は中止される。この場合、コンテンツのダウンロード（Ｓ１０６）は実行されない。

【０１８９】

また、ステップＳ１０５のもう１つの判定処理である、

（２）トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）のバージョンより大きいか否かの判定において大きいと判定された場合には、装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）は利用できないことになり、この場合もステップＳ１０５の判定はＹｅｓとなり、以下の処理は実行されず、ステップＳ１１０に進み、他ダウンロード処理は中止される。この場合、コンテンツのダウンロード（Ｓ１０６）は実行されない。

【０１９０】

ステップＳ１０５において、

（１）ダウンロード処理を行っているサーバがリボーク（無効化）されていないと判定

され、
（２）トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）のバージョンより大きくないと判定された場合にのみ、
ステップＳ１０５の判定がＮｏとなり、次のステップＳ１０６の処理に進む。
【０１９１】
ステップＳ１０６では、接続サーバから以下のデータをダウンロードしてメディア（メモリカード）に対して書き込む処理を実行する。
暗号化コンテンツ（Ｅｎｃｒｙｐｔｅｄ　ｃｏｎｔｅｎｔ）、
ＣＰＳユニットキーファイル（ＣＰＳ　Ｕｎｉｔ　Ｋｅｙ　Ｆｉｌｅ）、
コンテンツハッシュテーブル（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ）、
利用制御情報（ＣＰＳ　Ｕｎｉｔ　Ｕｓａｇｅ　Ｆｉｌｅ）
【０１９２】
暗号化コンテンツは、ＣＰＳユニットキーファイル（ＣＰＳ　Ｕｎｉｔ　Ｋｅｙ　Ｆｉｌｅ）に含まれるＣＰＳユニットキー（タイトルキー）で暗号化されたコンテンツである。
ＣＰＳユニットキーファイル（ＣＰＳ　Ｕｎｉｔ　Ｋｅｙ　Ｆｉｌｅ）は、コンテンツ復号用の鍵であるＣＰＳユニットキー（タイトルキー）を記録したファイルである。なお、先に図８を参照して説明したように、ＣＰＳユニットキー（タイトルキー）自身もバインドキーとメディアＩＤを用いて生成されるボリュームユニークキーを用いて暗号化されている。
【０１９３】
コンテンツハッシュテーブルは、コンテンツのハッシュ値を格納したテーブルである。コンテンツの再生時にコンテンツの正当性を確認するために利用される。
利用制御情報は、コンテンツの再生処理やコピー処理等のコンテンツ利用時の制限情報等を記録したデータである。
【０１９４】
ステップＳ１０６におけるダウンロード、記録処理が完了すると、ステップＳ１０７において課金処理を行う。
なお、課金処理に際しては、例えば決済サーバ等の別のサーバとの接続を伴う処理として実行してもよい。
【０１９５】
ステップＳ１０８において課金処理の完了が確認されない場合は、ステップＳ１１０で処理を中止する。この場合、ステップＳ１０９のバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）のダウンロードが実行されないので、コンテンツの復号、利用は不可能となる。
【０１９６】
ステップＳ１０８において課金処理の完了が確認されると、ステップＳ１０９に進む。
ステップＳ１０９では、サーバから提供されるバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）のダウンロードを実行して、メディア（メモリカード）に記録して、ステップＳ１１０において処理を終了する。
【０１９７】
なお、バインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）は、メモリカードの識別子としてメモリカードの不揮発性メモリに予め記録されたメディアＩＤとの暗号処理によってボリュームユニークキーを生成する際に必須となる鍵データである。
ボリュームユニークキーはＣＰＳユニットキー（タイトルキー）の復号に適用され、ＣＰＳユニットキー（タイトルキー）は暗号化コンテンツの復号に必要となる。
従って、バインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）が得られなければ、暗号化コンテンツの復号、再生は不可能となる。
【０１９８】

また、ステップＳ１０９におけるバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）のメモリカードへの書き込み処理は、先に、図６を参照して説明したように、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の所定の区分領域（図６に示すＰｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１，＃２，＃３・・・）に対して実行されることになる。

【０１９９】

サーバのメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対する記録許容領域については、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）に記録されている。メモリカードのデータ処理部が、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）に記録された情報を参照してバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）の記録先を決定して記録する処理を行う。

【０２００】

なお、メモリカードを装着した装置が、メモリカードの取得した記録先許容情報を受領して、記録先を決定する処理を行う構成としてもよい。また、メモリカードを装着した装置自身が、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）に記録された記録許容領域情報を取得して記録先を決定する処理を行う構成としてもよい。

なお、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するデータ書き込み／読み取り制御処理についての詳細については、後段で説明する。

【０２０１】

図１０を参照して説明したコンテンツダウンロード処理は、ダウンロード処理時に、再生装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）のバージョンの値が、トークンに記録された許容最小値以上であるか否かを検証して、トークンに記録された許容最小値以上でない場合は、処理を中止する設定として説明した。

しかし、このバージョンチェックはダウンロード処理においては行わず、コンテンツの再生処理時に実行する構成としてもよい。

【０２０２】

次に、図１２、図１３に示すフローチャートを参照して、コンテンツダウンロード処理のもう１つの例について説明する。

図１０のフローチャートを参照して説明した処理では、再生装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）のバージョンの値と、トークンに記録されたバージョン許容最小値のみを比較する処理例として説明した。

【０２０３】

図１２、図１３に示す処理は、このバージョン比較に加え、さらに、

メデイア（メモリカード）に記録したコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）のバージョンの値と、トークンに記録されたバージョン許容最小値についての比較処理も実行する処理例である。

【０２０４】

メデイア（メモリカード）に記録したコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）のバージョンの値が、トークンに記録されたバージョン許容最小値未満である場合は処理を中止する。

【０２０５】

図１２、図１３に示すフローチャートの各ステップの処理について説明する。

ステップＳ２０１～ステップＳ２０３の処理は、図１０参照して説明したステップＳ１０１～Ｓ１０３の処理と同様の処理である。

すなわち、ステップＳ２０１において、装置にメモリカードを装着し、サーバに対するアクセスを行う。なお、ステップＳ２０１の時点で、先に図８のステップＳ２１の処理として説明したサーバとメモリカードとの相互認証処理が実行され、ステップＳ２０２以下の処理はこの相互認証処理が成立した場合に実行される。

【０２０６】

ステップＳ２０２では、
トークン（Ｔｏｋｅｎ）、
コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ），
サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）
サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ），
これらの各データのダウンロード処理、読み取り処理、、メモリカードに対する書き込み処理を行う。

【０２０７】

ステップＳ２０３では、ステップＳ２０２においてサーバから取得したコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）の検証処理と再生器のメモリへの取り込み処理を実行する。
このステップＳ２０３の詳細シーケンスについては、先に図１１に示すフローチャートを参照して説明した通りである。

【０２０８】

すなわち、サーバからダウンロードし、メモリカードに記録した
コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ），
サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）
これらリボケーションリストの署名検証により正当性を確認する処理と、ダウンロードリストと、記録再生装置のメモリに格納されたリストのバージョン比較処理による装置格納リストの更新処理が行われる。

【０２０９】

すなわち、ダウンロードしたコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）が装置のメモリに格納された各リボケーションリストより新しいものである場合には、装置のメモリに格納されたリストをダウンロードした新しいリストに置き換えるリボケーションリスト更新処理を実行する。

【０２１０】

これらの処理の完了後、ステップＳ２０４に進む。
ステップＳ２０４は、図１０に示すフローのステップＳ１０４の処理に対応する。
ステップＳ２０４では、
（１）ダウンロード予定のコンテンツがリボーク（無効化）されているか否か、
（２）トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）のバージョンより大きいか否か、
これらの判定処理を実行する。
この判定処理は図１０に示すフローのステップＳ１０４の処理と同様の処理である。

【０２１１】

ステップＳ２０４において、
（１）ダウンロード予定のコンテンツがリボーク（無効化）されていないと判定され、
かつ、
（２）トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）のバージョンより大きくないと判定された場合にのみ、
ステップＳ２０４の判定がＮｏとなり、次のステップＳ２０５の処理に進む。
この場合以外は、ステップＳ２０４の判定はＹｅｓとなり、ステップＳ２１２に進み、

その後の処理は中止される。この場合は、コンテンツのダウンロードは（ステップＳ２０８）行われない。

【０２１２】

ステップＳ２０４の判定がＮｏとなり、次のステップＳ２０５の処理に進むと、ステップＳ２０５では、

トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）と、ステップＳ２０２において新たにサーバからダウンロードし、メディア（メモリカード）に記録したコンテンツリボケーションリスト（ＣＲＬ）のバージョンの比較を行う。

【０２１３】

このステップＳ２０５の処理は、図１０を参照して説明した処理には含まれない処理である。

ステップＳ２０５において、

トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、ステップＳ２０２において新たにサーバからダウンロードし、メディア（メモリカード）に記録したコンテンツリボケーションリスト（ＣＲＬ）のバージョンより大きい場合、このダウンロードにより新たに記録したコンテンツリボケーションリスト（ＣＲＬ）は、トークンの記録に従って使用できないリストとなる。この場合、ステップＳ２０５の判定はＹｅｓとなり、以下の処理は実行されず、ステップＳ２１２に進み、他ダウンロード処理は中止される。この場合、コンテンツのダウンロード（Ｓ２０８）は実行されない。

【０２１４】

ステップＳ２０５において、

トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、ステップＳ２０２において新たにサーバからダウンロードし、メディア（メモリカード）に記録したコンテンツリボケーションリスト（ＣＲＬ）のバージョンより大きくないと判定した場合には、ステップＳ２０５の判定がＮｏとなり、次のステップＳ２０６の処理に進む。

【０２１５】

ステップＳ２０６は、図１０に示すフローのステップＳ１０５の処理に対応する。

ステップＳ２０６では、

（１）ダウンロード処理の実行先のサーバがリボーク（無効化）されているか否か、

（２）トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）のバージョンより大きいか否か、

これらの判定処理を実行する。

この判定処理は図１０に示すフローのステップＳ１０５の処理と同様の処理である。

【０２１６】

ステップＳ２０６において、

（１）ダウンロード処理の実行先のサーバがリボーク（無効化）されていないと判定され、

かつ、

（２）トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）のバージョンより大きくないと判定された場合にのみ、

ステップＳ２０６の判定がＮｏとなり、次のステップＳ２０７の処理に進む。

この場合以外は、ステップＳ２０６の判定はＹｅｓとなり、ステップＳ２１２に進み、その後の処理は中止される。この場合は、コンテンツのダウンロードは（ステップＳ２０

８）行われない。
【０２１７】
ステップＳ２０６の判定がＮｏとなり、次のステップＳ２０７の処理に進むと、ステップＳ２０７では、
トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）と、ステップＳ２０２において新たにサーバからダウンロードし、メディア（メモリカード）に記録したサーバリボケーションリスト（ＳＲＬ）のバージョンの比較を行う。
【０２１８】
このステップＳ２０７の処理は、図１０を参照して説明した処理には含まれない処理である。
ステップＳ２０７において、
トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、ステップＳ２０２において新たにサーバからダウンロードし、メディア（メモリカード）に記録したサーバリボケーションリスト（ＳＲＬ）のバージョンより大きい場合、このダウンロードにより新たに記録したサーバリボケーションリスト（ＳＲＬ）は、トークンの記録に従って使用できないリストとなる。この場合、ステップＳ２０７の判定はＹｅｓとなり、以下の処理は実行されず、ステップＳ２１２に進み、他ダウンロード処理は中止される。この場合、コンテンツのダウンロード（Ｓ２０８）は実行されない。
【０２１９】
ステップＳ２０７において、
トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、ステップＳ２０２において新たにサーバからダウンロードし、メディア（メモリカード）に記録したサーバリボケーションリスト（ＳＲＬ）のバージョンより大きくないと判定した場合には、ステップＳ２０７の判定がＮｏとなり、次のステップＳ２０８の処理に進む。
【０２２０】
ステップＳ２０８～ステップＳ２１２の処理は、図１０に示すフローチャートのステップＳ１０６～Ｓ１１０の処理に対応する。
ステップＳ２０８では、接続サーバから以下のデータをダウンロードしてメディア（メモリカード）に対して書き込む処理を実行する。
暗号化コンテンツ（Ｅｎｃｒｙｐｔｅｄ　ｃｏｎｔｅｎｔ）、
ＣＰＳユニットキーファイル（ＣＰＳ　Ｕｎｉｔ　Ｋｅｙ　Ｆｉｌｅ）、
コンテンツハッシュテーブル（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ）、
利用制御情報（ＣＰＳ　Ｕｎｉｔ　Ｕｓａｇｅ　Ｆｉｌｅ）
【０２２１】
暗号化コンテンツは、ＣＰＳユニットキーファイル（ＣＰＳ　Ｕｎｉｔ　Ｋｅｙ　Ｆｉｌｅ）に含まれるＣＰＳユニットキー（タイトルキー）で暗号化されたコンテンツである。
ＣＰＳユニットキーファイル（ＣＰＳ　Ｕｎｉｔ　Ｋｅｙ　Ｆｉｌｅ）は、コンテンツ復号用の鍵であるＣＰＳユニットキー（タイトルキー）を記録したファイルである。なお、先に図８を参照して説明したように、ＣＰＳユニットキー（タイトルキー）自身もバインドキーとメディアＩＤを用いて生成されるボリュームユニークキーを用いて暗号化されている。
【０２２２】
コンテンツハッシュテーブルは、コンテンツのハッシュ値を格納したテーブルである。コンテンツの再生時にコンテンツの正当性を確認するために利用される。
利用制御情報は、コンテンツの再生処理やコピー処理等のコンテンツ利用時の制限情報等を記録したデータである。

【０２２３】
ステップＳ２０８におけるダウンロード、記録処理が完了すると、ステップＳ２０９において課金処理を行う。
なお、課金処理に際しては、例えば決済サーバ等の別のサーバとの接続を伴う処理として実行してもよい。
【０２２４】
ステップＳ２１０において課金処理の完了が確認されない場合は、ステップＳ２１２で処理を中止する。この場合、ステップＳ２１１のバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）のダウンロードが実行されないので、コンテンツの復号、利用は不可能となる。
【０２２５】
ステップＳ２１０において課金処理の完了が確認されると、ステップＳ２１１に進む。
ステップＳ２１１では、サーバから提供されるバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）のダウンロードを実行して、メディア（メモリカード）に記録する。
【０２２６】
なお、前述したようにバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）は、メモリカードの識別子としてメモリカードの不揮発性メモリに予め記録されたメディアＩＤとの暗号処理によってボリュームユニークキーを生成する際に必須となる鍵データである。
ボリュームユニークキーはＣＰＳユニットキー（タイトルキー）の復号に適用され、ＣＰＳユニットキー（タイトルキー）は暗号化コンテンツの復号に必要となる。
従って、バインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）が得られなければ、暗号化コンテンツの復号、再生は不可能となる。
【０２２７】
なお、ステップＳ２１１におけるバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）のメモリカードへの書き込み処理は、先に、図６を参照して説明したように、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の所定の区分領域（図６に示すＰｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１，＃２，＃３・・・）に対して実行されることになる。
【０２２８】
サーバの記録許容領域については、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）に記録されており、メモリカードの書き込み処理プログラムがサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）に記録された情報を参照してバインドキー（Ｂｉｎｄｉｎｇ　Ｋｅｙ）の記録先を決定して記録する処理を行う。あるいはダウンロード実行装置が代わりに行ってもよい。
なお、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するデータ書き込み／読み取り制御処理についての詳細については、後段で説明する。
【０２２９】
なお、図１２を参照して説明したコンテンツダウンロード処理においては、
ダウンロード処理時に、再生装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）、さらにダウンロードしてルモリカードに新たに記録したコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）、これらのバージョンの値が、トークンに記録された許容最小値以上であるか否かを検証して、トークンに記録された許容最小値以上でない場合は、処理を中止する設定として説明した。
【０２３０】
しかし、これらのバージョンチェックはダウンロード処理においては行わず、コンテンツの再生処理時に実行する構成としてもよい。
【０２３１】
なお、図１０～図１３に示すフローチャートでは、コンテンツ自体をサーバからダウンロードする場合の処理例として説明したが、コンテンツ自体をディスクからメモリカードにコピーする場合は、コンテンツ以外のデータをサーバから取得することになる。この場合、図１０～図１３に示すフロー中のコンテンツのダウンロード処理がディスクからのコンテンツコピー処理に置き換えられることになる。その他のトークン、ＣＲＬ、ＳＲＬ等

を含むコンテンツ管理情報については、サーバからダウンロードしてメモリカードに記録され、この際に、コンテンツ記録以外の図１０～図１３のフローに示す処理が実行される。

【０２３２】

［６．コンテンツ再生処理シーケンスについて］

次に、図１４以下のフローチャートを参照して、サーバからダウンロードしてメディア（メモリカード）に記録したコンテンツと管理情報（ダウンロードコンテンツ対応の管理データ）を適用したコンテンツの再生処理シーケンスについて説明する。

【０２３３】

このコンテンツ再生処理は、メモリカードを装着した再生装置によって行われる。再生装置は、例えば図２に示す記録再生器２２、ＰＣ２３、あるいは再生処理のみを行う再生装置等の様々な装置である。なお、これらの再生装置には、以下に説明するフローに従った再生シーケンスを実行するためのプログラムが格納されており、そのプログラムに従って再生伴う様々な処理、例えばコンテンツの復号処理や、管理データの検証、管理データを適用したコンテンツやサーバ検証等を実行する。

【０２３４】

図１４に示すフローチャートについて説明する。

ステップＳ３０１において、再生対象となるコンテンツと管理データを格納したメデイア（メモリカード）を装着し、再生対象コンテンツのユーザ指定等により再生コンテンツが選択される。

【０２３５】

ステップＳ３０２において、再生対象コンテンツに対応する以下の管理データがメモリカードから読み取られる。

トークン（Ｔｏｋｅｎ）、

コンテンツハッシュテーブル（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ）、

コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）、

サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、

これらのデータの読み取りを行う。

【０２３６】

トークン（Ｔｏｋｅｎ）は、先に図７を参照して説明したデータを持つ。

コンテンツハッシュテーブル（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ）はコンテンツのハッシュ値を格納したデータであり、コンテンツの正当性（改ざんの有無）を判定するために利用される。

コンテンツリボケーションリスト（ＣＲＬ）は、先に図４（ｂ）を参照して説明した無効化（リボーク）コンテンツの識別子（ＩＤ）を記録したリストである。

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）は、先に図５を参照して説明したサーバ公開鍵を格納したデータである。

サーバリボケーションリスト（ＳＲＬ）は、先に図４（ａ）を参照して説明した無効化（リボーク）サーバの識別子（ＩＤ）を記録したリストである。

【０２３７】

なお、コンテンツリボケーションリスト（ＣＲＬ）と、サーバリボケーションリスト（ＳＲＬ）と、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）は図３に示す認証局１００が発行し、認証局の秘密鍵による署名が設定されている。

トークン（Ｔｏｋｅｎ）とコンテンツハッシュテーブル（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ）は、サーバ（例えば図３に示すコンテンツサーバ２００）が発行し、サーバの秘密鍵による署名が設定されている。

【０２３８】

ステップＳ３０３では、ステップＳ３０２においてサーバから取得したコンテンツリボケーションリスト（ＣＲＬ）に基づくコンテンツのリボーク（無効化）状況の検証処理を実行する。

このステップＳ３０３の詳細シーケンスについて、図１５に示すフローチャートを参照して説明する。

【０２３９】

図１５のステップＳ３３１は、図１４のステップＳ３０１と同様の処理を示しており、コンテンツリボケーションリスト（ＣＲＬ）に基づくコンテンツのリボーク（無効化）状況の検証処理の開始条件として行われる処理である。

ステップＳ３３２において、

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）、

トークン（Ｔｏｋｅｎ）、

コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、

これらのデータを取得する。

なお、これらは再生対象コンテンツに対応してメモリカードに記録された管理データである。

【０２４０】

ステップＳ３３３において、

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）、

トークン（Ｔｏｋｅｎ）、

コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、

これらの各データに設定された署名検証処理を実行して各データの正当性を確認する。

【０２４１】

前述したように、コンテンツリボケーションリスト（ＣＲＬ）と、サーバリボケーションリスト（ＳＲＬ）と、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）は図３に示す認証局１００が発行し、認証局の秘密鍵による署名が設定されている。これらのデータに対しては、認証局の公開鍵を適用した署名検証を実行する。

再生装置は、予め認証局の公開鍵を格納した公開鍵証明書を自装置のメモリに格納している。あるいは必要に応じて取得するものとする。

【０２４２】

また、トークン（Ｔｏｋｅｎ）は、サーバ（例えば図３に示すコンテンツサーバ２００）が発行し、サーバの秘密鍵による署名が設定されている。この署名検証は、サーバ証明書に格納されたサーハバの公開鍵を適用して実行される。ただし、サーバ証明書の署名検証により正当性の確認されたサーバ証明書であることが条件である。

【０２４３】

ステップＳ３３３において、

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）、

トークン（Ｔｏｋｅｎ）、

コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、

これらの各データに設定された署名検証処理を実行して全てのデータの正当性が確認された場合は、ステップＳ３３３の判定はＹｅｓとなり、ステップＳ３３４に進む。

一方、上記のいずれかのデータの署名検証が成立しなかった場合は、ステップＳ３３３の判定はＮｏとなり、ステップＳ３２０（図１４参照）に進み、再生処理は中止される。

【０２４４】

ステップＳ３３３において、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）、トークン（Ｔｏｋｅｎ）、コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、これら全てのデータの正当性が確認された場合は

、ステップＳ３３４に進む。ステップＳ３３４では、正当性の確認されたトークン内に記録されたコンテンツＩＤが、正当性の確認されたコンテンツリボケーションリスト（ＣＲＬ）にリボーク（無効化）コンテンツとして記録されているか否かを判定する。

【０２４５】

なお、トークンには、先に図７を参照して説明したように、コンテンツＩＤとして、サーバＩＤと、コンテンツ固有ＩＤとの組み合わせデータが記録されている。

コンテンツリボケーションリスト（ＣＲＬ）に記録されるコンテンツＩＤは、「コンテンツ固有ＩＤ」あるいは「コンテンツＩＤ＝サーバＩＤ＋コンテンツ固有ＩＤ」、これらいずれのパターンとしてもよく、再生装置は、これらのパターンに応じて、トークンに記録されたコンテンツＩＤ（またはコンテンツ固有ＩＤ）と、コンテンツリボケーションリスト（ＣＲＬ）に記録されたコンテンツＩＤ（またはコンテンツ固有ＩＤ）とを比較する。

【０２４６】

トークンに記録されたコンテンツＩＤ（またはコンテンツ固有ＩＤ）がコンテンツリボケーションリスト（ＣＲＬ）に記録されている場合は、そのコンテンツ、すなわち再生予定のコンテンツはリボーク（無効化）されていることになり、ステップＳ３３４の判定はＮｏとなり、ステップＳ３２０に進みコンテンツ再生は中止される。

【０２４７】

一方、トークンに記録されたコンテンツＩＤ（またはコンテンツ固有ＩＤ）がコンテンツリボケーションリスト（ＣＲＬ）に記録されていない場合は、そのコンテンツ、すなわち再生予定のコンテンツはリボーク（無効化）されていないことになり、ステップＳ３３４の判定はＹｅｓとなり、ステップＳ３３５に進む。

【０２４８】

ステップＳ３３５では、トークンに記録されたコンテンツＩＤ中の上位ビットとして設定されているサーバＩＤを取得する。このサーバＩＤが、正当性の確認されたサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）に記録されたサーバＩＤと一致するか否かを確認する。

【０２４９】

一致すれば、トークンは、認証局によって認められた正当なサーバによって、自己のサーバＩＤを設定したコンテンツＩＤを記録した正しい記録データを持つトークンであると判定し、ステップＳ３３５の判定がＹｅｓとなり、図１４のステップＳ３０４に進む。

【０２５０】

一致しない場合は、トークンが、認証局によって認められた正当なサーバではあるが、自己のサーバＩＤと異なるサーバＩＤを設定した不正なコンテンツＩＤを記録した不正データを持つトークンであると判定し、ステップＳ３３５の判定はＮｏとなり、ステップＳ３２０（図１４）に進みコンテンツ再生は中止される。

【０２５１】

このステップＳ３３５の判定処理は、トークンが認証局の監視外で、サーバが自由に作成できるという問題点を補う処理として行われる。

認証局によって認められたサーバであっても、不正なトークンを作成する可能性がある。

しかし、トークン内に記録されるコンテンツＩＤは、先に図７を参照して説明したように、

コンテンツＩＤ＝［サーバＩＤ］＋［コンテンツ固有ＩＤ］

の構成を有しているため、トークンに記録されたコンテンツＩＤを参照すれば不正なトークンを作成したサーバを特定できる。

【０２５２】

不正を行おうとするサーバは、この特定を不可能にするため、トークン中に記録されるコンテンツＩＤに含まれるサーバＩＤを、本来の自サーバのＩＤではなく、他のサーバＩＤや実在しないサーバＩＤ等に設定してトークンを作成することが考えられる。

【０２５３】

このような不正を防止し判定する処理がステップＳ３３５の処理である。ステップＳ３３５において、トークン中のコンテンツＩＤに含まれるサーバＩＤと、サーバ証明書に記録されたサーバＩＤが一致することを確認することで、トークンに記録されたコンテンツＩＤ中のサーバＩＤが間違いなくトークンの発行主体であることが確認され、不正な記録を含むトークンでないことが確認される。

【０２５４】

図１５に示す、

サーバ証明書とコンテンツリボケーションリスト（ＣＲＬ）の署名検証の成立（Ｓ３３３）、

トークンに記録されたコンテンツＩＤがコンテンツリボケーションリスト（ＣＲＬ）に記録されていないことの確認（Ｓ３３４）、

トークンに記録されたサーバＩＤとサーバ証明書のサーバＩＤが一致することの確認（Ｓ３３５）、

これらすべてが確認された場合に図１４のフローのステップＳ３０４に進む。

【０２５５】

図１４のフローチャートのステップＳ３０４では、ステップＳ３０２において読み取ったコンテンツハッシュテーブルの正当性確認処理を実行する。

コンテンツハッシュテーブル（ＣＨＴ）はコンテンツのハッシュ値を登録したテーブルであり、コンテンツの正当性（改ざんの有無）を検証するために利用されるデータであり、例えばサーバの秘密鍵による署名が付与されている。この署名検証を実行する。署名検証はサーバ証明書から取得するサーバ公開鍵によって行われる。

【０２５６】

ステップＳ３０４において、コンテンツハッシュテーブル（ＣＨＴ）の正当性が確認されなかった場合は、ステップＳ３０４の判定はＮｏとなり、ステップＳ３２０に進み、コンテンツ再生は中止される。

【０２５７】

ステップＳ３０４において、コンテンツハッシュテーブル（ＣＨＴ）の正当性が確認された場合は、ステップＳ３０４の判定はＹｅｓとなり、ステップＳ３０５に進む。

【０２５８】

ステップＳ３０５では、コンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）の検証処理と再生器のメモリへの取り込み処理を実行する。

この処理は、先に、図１１に示すフローチャートを参照して説明した処理に相当する。

すなわち、サーバからダウンロードし、メモリカードに記録した、

コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ），

サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）

これらリボケーションリストの署名検証により正当性を確認する処理と、ダウンロードリストと、記録再生装置のメモリに格納されたリストのバージョン比較処理による装置格納リストの更新処理が行われる。

リボケーションリストの署名検証により正当性が確認されなかった場合は、コンテンツ再生は中止（Ｓ３２０）される。

【０２５９】

また、バージョン比較処理において、ダウンロードしたコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）が装置のメモリに格納された各リボケーションリストより新しいものである場合には、装置のメモリに格納されたリストをダウンロードした新しいリストに置き換えるリボケーションリスト更新処理を実行する。

【０２６０】

これらの処理の完了後、ステップ３０６に進む。

ステップＳ３０６では、

（１）再生予定のコンテンツがリボーク（無効化）されているか否か、
（２）トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）のバージョンより大きいか否か、
これらの判定処理を実行する。
この判定処理は図１０に示すフローのステップＳ１０４の処理と同様の処理である。

【０２６１】

ステップＳ３０６において、
（１）再生予定のコンテンツがリボーク（無効化）されていないと判定され、
かつ、
（２）トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）のバージョンより大きくないと判定された場合にのみ、
ステップＳ３０６の判定がＮｏとなり、次のステップＳ３０７の処理に進む。
この場合以外は、ステップＳ３０６の判定はＹｅｓとなり、ステップＳ３２０に進み、その後の処理は中止される。この場合は、コンテンツ再生は行われない。

【０２６２】

ステップＳ３０６の判定がＮｏとなり、次のステップＳ３０７の処理に進むと、ステップＳ３０７では、
（１）再生予定コンテンツまたは再生予定コンテンツの管理データを取得したサーバがリボーク（無効化）されているか否か、
（２）トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）のバージョンより大きいか否か、
これらの判定処理を実行する。
この判定処理は図１０に示すフローのステップＳ１０５の処理と同様の処理である。

【０２６３】

ステップＳ３０７において、
（１）再生予定コンテンツまたは再生予定コンテンツの管理データを取得したサーバがリボーク（無効化）されていないと判定され、
かつ、
（２）トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）のバージョンより大きくないと判定された場合にのみ、
ステップＳ３０７の判定がＮｏとなり、次のステップＳ３０８の処理に進む。
この場合以外は、ステップＳ３０７の判定はＹｅｓとなり、ステップＳ３２０に進み、その後の処理は中止される。この場合は、コンテンツ再生は行われない。

【０２６４】

ステップＳ３０７の判定がＮｏとなり、次のステップＳ３０８の処理に進むと、ステップＳ３０８では、
トークンと利用制御情報の検証処理を実行する。
トークンは、先に図７参照して説明したデータ構成を有し、サーバの秘密鍵による署名が付与されている。
利用制御情報は、コンテンツの再生条件やコピー許容回数等のコンテンツの利用条件を記録したデータであり、サーバの秘密鍵による署名が付与されている。
ステップＳ３０８では、これらの各データの署名検証によりデータの正当性を確認する

。署名検証は、サーバ証明書から取得されるサーバ公開鍵を用いて行われる。
【０２６５】
ステップＳ３０９では、これらの各データの署名検証が成立しデータの正当性が確認されたか否かを判定する。
ステップＳ３０９において、トークンと利用制御情報の正当性が確認されなかった場合は、ステップＳ３０９の判定はＮｏとなり、ステップＳ３２０に進み、その後の処理は中止される。この場合は、コンテンツ再生は行われない。
【０２６６】
ステップＳ３０９において、トークンと利用制御情報の正当性が確認された場合は、ステップＳ３０９の判定はＹｅｓとなり、次のステップＳ３１０に進む。
【０２６７】
ステップＳ３１０では、コンテンツの復号に適用するＣＰＳユニットキー（タイトルキー）を取得する。
なお、先に図８等を参照して説明したように、再生装置においてＣＰＳユニットキー（タイトルキー）を取得するためには、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に記録されたバインドキーを取り出して、さらにメディアＩＤを利用してボリュームユニークキーを生成して、生成したボリュームユニークキーを適用して暗号化ＣＰＳユニットキー（暗号化タイトルキー）を復号してＣＰＳユニットキー（タイトルキー）を取得する処理を行う。
【０２６８】
その後、ステップＳ３１１において、取得したＣＰＳユニットキー（タイトルキー）を適用して暗号化コンテンツの復号処理を行いコンテンツ再生を実行する。
【０２６９】
このように、コンテンツ再生を実行するためには、サーバから受領したトークン他のコンテンツ管理データを検証し、各管理データの正当性を確認した後、管理データに基づいて、コンテンツと、サーバの正当性を検証し、さらにサーバから受信したバインドキーを適用してコンテンツ復号用のＣＰＳユニットキー（タイトルキー）を取得して暗号化コンテンツの復号を行うという一連の処理が必要となる。
【０２７０】
また、コンテンツと、サーバの正当性を検証するために適用するコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）は、トークンに記録されたバージョンの最小許容値以上のバージョンのものに制限される。すなわちトークンに記録されたバージョンの最小許容値未満のバージョンの古いリストを適用してコンテンツやサーバの有効性を判定して再生処理に移行することが禁止される。
【０２７１】
なお、これらの再生処理シーケンスは、再生装置が保持する再生処理プログラムに従って実行される。
また、図１４を参照して説明した処理は、コンテンツとコンテンツ管理データの双方をサーバからダウンロードした場合に適用されるのみではなく、他のメデイア、例えば図１に示すコンテンツ記録ディスクからメモリカードにコンテンツをコピーし、そのコンテンツに対応する管理データをサーバから取得した場合にも実行される。
【０２７２】
次に、図１６、図１７に示すフローチャートを参照して、コンテンツ再生処理のもう１つの例について説明する。
図１４のフローチャートを参照して説明した処理では、再生装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）のバージョンの値と、トークンに記録されたバージョン許容最小値のみを比較する処理例として説明した。
【０２７３】
図１６、図１７に示す処理は、このバージョン比較に加え、さらに、

メデイア（メモリカード）に記録したコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）のバージョンの値と、トークンに記録されたバージョン許容最小値の比較処理も実行する処理例である。

【０２７４】

メデイア（メモリカード）に記録したコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）のバージョンの値が、トークンに記録されたバージョン許容最小値未満である場合は再生処理を中止する。

【０２７５】

図１６、図１７に示すフローチャートの各ステップの処理について説明する。

ステップＳ３８１～ステップＳ３８５の処理は、図１４、図１５参照して説明したステップＳ３０１～Ｓ３０５の処理と同様の処理である。

【０２７６】

ステップＳ３８１において、再生対象となるコンテンツと管理データを格納したメデイア（メモリカード）を装着し、再生対象コンテンツのユーザ指定等により再生コンテンツが選択される。

【０２７７】

ステップＳ３８２において、再生対象コンテンツに対応する以下の管理データがメモリカードから読み取られる。

トークン（Ｔｏｋｅｎ）、

コンテンツハッシュテーブル（Ｃｏｎｔｅｎｔ　Ｈａｓｈ　Ｔａｂｌｅ）、

コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）、

サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）、

これらのデータの読み取りを行う。

【０２７８】

ステップＳ３８３では、ステップＳ３８２においてサーバから取得したコンテンツリボケーションリスト（ＣＲＬ）に基づくコンテンツのリボーク（無効化）状況の検証処理を実行する。

このステップＳ３８３の詳細シーケンスは、先に図１５に示すフローチャートを参照して説明したとおりである。

【０２７９】

図１５に示す、

サーバ証明書とコンテンツリボケーションリスト（ＣＲＬ）の署名検証の成立（Ｓ３３３）、

トークンに記録されたコンテンツＩＤがコンテンツリボケーションリスト（ＣＲＬ）に記録されていないことの確認（Ｓ３３４）、

トークンに記録されたサーバＩＤとサーバ証明書のサーバＩＤが一致することの確認（Ｓ３３５）、

これらのいずれかが確認されない場合は、ステップＳ３９５に進み、コンテンツ再生は中止される。

これらすべてが確認された場合に図１６のフローのステップＳ３８４に進む。

【０２８０】

図１６のフローチャートのステップＳ３８４では、ステップＳ３８２において読み取ったコンテンツハッシュテーブルの正当性確認処理を実行する。

コンテンツハッシュテーブル（ＣＨＴ）はコンテンツのハッシュ値を登録したテーブルであり、コンテンツの正当性（改ざんの有無）を検証するために利用されるデータであり、例えばサーバの秘密鍵による署名が付与されている。この署名検証を実行する。署名検証はサーバ証明書から取得するサーバ公開鍵によって行われる。

【０２８１】
ステップＳ３８４において、コンテンツハッシュテーブル（ＣＨＴ）の正当性が確認されなかった場合は、ステップＳ３８４の判定はＮｏとなり、ステップＳ３９５に進み、コンテンツ再生は中止される。
【０２８２】
ステップＳ３８４において、コンテンツハッシュテーブル（ＣＨＴ）の正当性が確認された場合は、ステップＳ３８４の判定はＹｅｓとなり、ステップＳ３８５に進む。
【０２８３】
ステップＳ３８５では、コンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）の検証処理と再生器のメモリへの取り込み処理を実行する。
この処理は、先に、図１１に示すフローチャートを参照して説明した処理に相当する。
すなわち、サーバからダウンロードし、メモリカードに記録した、
コンテンツリボケーションリスト（ＣＲＬ：Ｃｏｎｔｅｎｔ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ），
サーバリボケーションリスト（ＳＲＬ：Ｓｅｒｖｅｒ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）
これらリボケーションリストの署名検証により正当性を確認する処理と、ダウンロードリストと、記録再生装置のメモリに格納されたリストのバージョン比較処理による装置格納リストの更新処理が行われる。
リボケーションリストの署名検証により正当性が確認されなかった場合は、コンテンツ再生は中止（Ｓ３９５）される。
【０２８４】
また、バージョン比較処理において、ダウンロードしたコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）が装置のメモリに格納された各リボケーションリストより新しいものである場合には、装置のメモリに格納されたリストをダウンロードした新しいリストに置き換えるリボケーションリスト更新処理を実行する。
【０２８５】
これらの処理の完了後、ステップ３８６に進む。ステップＳ３８６では、
（１）再生予定のコンテンツがリボーク（無効化）されているか否か、
（２）トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）のバージョンより大きいか否か、
これらの判定処理を実行する。
この判定処理は図１４に示すステップＳ３０６の処理と同様であり、また図１０に示すフローのステップＳ１０４の処理と同様の処理である。
【０２８６】
ステップＳ３８６において、
（１）再生予定のコンテンツがリボーク（無効化）されていないと判定され、
かつ、
（２）トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）のバージョンより大きくないと判定された場合にのみ、
ステップＳ３８６の判定がＮｏとなり、次のステップＳ３８７の処理に進む。
この場合以外は、ステップＳ３８６の判定はＹｅｓとなり、ステップＳ３９５に進み、その後の処理は中止される。この場合は、コンテンツ再生は行われない。
【０２８７】
ステップＳ３８６の判定がＮｏとなり、次のステップＳ３８７の処理に進むと、ステップＳ３８７では、

トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）と、再生予定のコンテンツに対応する管理データとしてサーバからダウンロードして、メディア（メモリカード）に記録したコンテンツリボケーションリスト（ＣＲＬ）のバージョンの比較を行う。

【０２８８】

このステップＳ３８７の処理は、図１４を参照して説明した処理には含まれない処理である。

ステップＳ３８７において、

トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、サーバからダウンロードし、メディア（メモリカード）に記録したコンテンツリボケーションリスト（ＣＲＬ）のバージョンより大きい場合、このダウンロードにより新たに記録したコンテンツリボケーションリスト（ＣＲＬ）は、トークンの記録に従って使用できないリストとなる。この場合、ステップＳ３８７の判定はＹｅｓとなり、以下の処理は実行されず、ステップＳ３９５に進み、以下の処理は中止される。この場合、コンテンツの再生処理は実行されない。

【０２８９】

ステップＳ３８７において、

トークン（Ｔｏｋｅｎ）に記録されているコンテンツリボケーションリスト（ＣＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＣＲＬ　Ｖｅｒｓｉｏｎ）が、再生予定のコンテンツ対応の管理データとしてサーバからダウンロードし、メディア（メモリカード）に記録したコンテンツリボケーションリスト（ＣＲＬ）のバージョンより大きくないと判定した場合には、ステップＳ３８７の判定がＮｏとなり、次のステップＳ３８８の処理に進む。

【０２９０】

ステップＳ３８８では、

（１）再生予定のコンテンツあるいは再生予定コンテンツに対応するコンテンツ管理データをダウンロードしたサーバがリボーク（無効化）されているか否か、

（２）トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）のバージョンより大きいか否か、

これらの判定処理を実行する。

この判定処理は図１４に示すステップＳ３０７の処理と同様であり、また図１０に示すフローのステップＳ１０５の処理と同様の処理である。

【０２９１】

ステップＳ３８８において、

（１））再生予定のコンテンツあるいは再生予定コンテンツに対応するコンテンツ管理データをダウンロードしたサーバがリボーク（無効化）されていないと判定され、

かつ、

（２）トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、この処理を実行している装置のメモリに格納されたサーバリボケーションリスト（ＳＲＬ）のバージョンより大きくないと判定された場合にのみ、

ステップＳ３８８の判定がＮｏとなり、次のステップＳ３８９の処理に進む。

この場合以外は、ステップＳ３８８の判定はＹｅｓとなり、ステップＳ３９５に進み、その後の処理は中止される。この場合は、コンテンツ再生は行われない。

【０２９２】

ステップＳ３８８の判定がＮｏとなり、次のステップＳ３８９の処理に進むと、ステップＳ３８９では、

トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）と、再生予定のコンテンツに対応する管理データとしてサーバからダウンロードして、メディア（メモリカード）に記録したサーバリボケーションリスト（ＳＲＬ）のバージョンの比較を行う。

【０２９３】

このステップＳ３８９の処理は、図１４を参照して説明した処理には含まれない処理である。

ステップＳ３８９において、

トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、サーバからダウンロードし、メディア（メモリカード）に記録したサーバリボケーションリスト（ＳＲＬ）のバージョンより大きい場合、このダウンロードにより新たに記録したサーバリボケーションリスト（ＳＲＬ）は、トークンの記録に従って使用できないリストとなる。この場合、ステップＳ３８９の判定はＹｅｓとなり、以下の処理は実行されず、ステップＳ３９５に進み、以下の処理は中止される。この場合、コンテンツの再生処理は実行されない。

【０２９４】

ステップＳ３８９において、

トークン（Ｔｏｋｅｎ）に記録されているサーバリボケーションリスト（ＳＲＬ）バージョン許容最小値（Ｍｉｎｉｍｕｍ　ＳＲＬ　Ｖｅｒｓｉｏｎ）が、再生予定のコンテンツ対応の管理データとしてサーバからダウンロードし、メディア（メモリカード）に記録したサーバリボケーションリスト（ＳＲＬ）のバージョンより大きくないと判定した場合には、ステップＳ３８９の判定がＮｏとなり、次のステップＳ３９０の処理に進む。

【０２９５】

ステップＳ３９０～Ｓ３９３は、図１４を参照して説明したフローのステップＳ３０８～Ｓ３１１の処理に対応する処理である。

ステップＳ３９０では、

トークンと利用制御情報の検証処理を実行する。

トークンは、先に図７参照して説明したデータ構成を有し、サーバの秘密鍵による署名が付与されている。

利用制御情報は、コンテンツの再生条件やコピー許容回数等のコンテンツの利用条件を記録したデータであり、サーバの秘密鍵による署名が付与されている。

ステップＳ３９０では、これらの各データの署名検証によりデータの正当性を確認する。署名検証は、サーバ証明書から取得されるサーバ公開鍵を用いて行われる。

【０２９６】

ステップＳ３９１では、これらの各データの署名検証が成立しデータの正当性が確認されたか否かを判定する。

ステップＳ３９１において、トークンと利用制御情報の正当性が確認されなかった場合は、ステップＳ３９１の判定はＮｏとなり、ステップＳ３９５に進み、その後の処理は中止される。この場合は、コンテンツ再生は行われない。

【０２９７】

ステップＳ３９１において、トークンと利用制御情報の正当性が確認された場合は、ステップＳ３９１の判定はＹｅｓとなり、次のステップＳ３９２に進む。

【０２９８】

ステップＳ３９２では、コンテンツの復号に適用するＣＰＳユニットキー（タイトルキー）を取得する。

なお、先に図８等を参照して説明したように、再生装置においてＣＰＳユニットキー（タイトルキー）を取得するためには、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に記録されたバインドキーを取り出して、さらにメディアＩＤを利用してボリュームユニークキーを生成して、生成したボリュームユニークキーを適用して暗号化ＣＰＳユニットキー（暗号化タイトルキー）を復号してＣＰＳユニットキー（タイトルキー）を

取得する処理を行う。

【０２９９】

その後、ステップＳ３９３において、取得したＣＰＳユニットキー（タイトルキー）を適用して暗号化コンテンツの復号処理を行いコンテンツ再生を実行する。

【０３００】

このように、本処理例では、コンテンツ再生を実行するためには、サーバから受領したトークン他のコンテンツ管理データを検証し、各管理データの正当性を確認した後、管理データに基づいて、コンテンツと、サーバの正当性を検証し、さらにサーバから受信したバインドキーを適用してコンテンツ復号用のＣＰＳユニットキー（タイトルキー）を取得して暗号化コンテンツの復号を行うという一連の処理が必要となる。

【０３０１】

また、コンテンツと、サーバの正当性を検証するために適用するコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）については、

（ａ）再生装置のメモリに格納されたコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）のバージョン、

（ｂ）再生予定のコンテンツ対応の管理データとしてサーバからダウンロードしてメモリカードに格納されたコンテンツリボケーションリスト（ＣＲＬ）とサーバリボケーションリスト（ＳＲＬ）のバージョン、

これらの各リストのバージョンが、いずれも、トークンに記録されたバージョンの最小許容値以上のバージョンのものに制限される。すなわちトークンに記録されたバージョンの最小許容値未満のバージョンの古いリストを適用してコンテンツやサーバの有効性を判定して再生処理に移行することが禁止される。

【０３０２】

なお、これらの再生処理シーケンスは、再生装置が保持する再生処理プログラムに従って実行される。

また、図１６～図１７を参照して説明した処理は、コンテンツとコンテンツ管理データの双方をサーバからダウンロードした場合に適用されるのみではなく、他のメディア、例えば図１に示すコンテンツ記録ディスクからメモリカードにコンテンツをコピーし、そのコンテンツに対応する管理データをサーバから取得した場合にも実行される。

【０３０３】

［７．メモリカードの保護領域のアクセス制限構成と処理について］

先に、図６を参照して説明したように、メモリカードは、自由なアクセスの許容される非保護領域（Ｕｓｅｒ　Ａｒｅａ）と、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）を有している。

以下では、メモリカードの保護領域のアクセス制限構成と具体的な処理例について説明する。

【０３０４】

メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するデータの書き込み（Ｗｒｉｔｅ）、あるいは保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）からのデータ読み込み（Ｒｅａｄ）は制限されている。

【０３０５】

具体的には、

アクセス要求装置（サーバや、記録再生装置（ホスト）等）単位、および、

各区分領域（＃１，＃２・・・）単位、

で、書き込み（Ｗｒｉｔｅ）処理と、読み取り（Ｒｅａｄ）処理の可否をアクセス制御情報として設定している。

【０３０６】

この設定情報は、各装置の装置証明書に記録されている。装置証明書は認証局の署名を持つ認証局発行の証明書である。

具体的には、サーバであれば先に図５を参照して説明したサーバ証明書（Ｓｅｒｖｅｒ

Ｃｅｒｔ）である。記録再生装置（ホスト）も、認証局の発行したホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）を有し、この証明書にアクセス制御情報が記録されている。
これらの証明書は認証局の署名が設定されており、改ざん防止構成がとられている。すなわち、署名検証により、正当性（改ざんの有無）を確認可能な構成を有している。
【０３０７】
メモリカードは、アクセス要求装置から受領した証明書、例えばサーバであれば図５を参照して説明したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）、記録再生装置（ホスト）であれば記録再生装置（ホスト）の証明書であるホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）を参照して、各装置に対して許容されている書き込み領域や読み取り領域を確認する。
【０３０８】
例えばデータ書き込み（Ｗｒｉｔｅ）処理の場合は、メモリカードがアクセス要求装置から受領した証明書の記録データに基づいて、メモリカードのデータ処理部が書き込み許容領域を確認し、確認された書き込み許容領域に対してデータの書き込みを実行する。例えば先に図６を参照して説明したバインドキーの書き込み等が行われる。
【０３０９】
データの読み取り（Ｒｅａｄ）処理の場合も同様であり、アクセス要求装置の証明書の記録データに基づいて、読み取り許容領域を確認し、確認された読み取り許容領域からデータの読み取りが実行される。
【０３１０】
例えば先に図６を参照して説明したバインドキーは、サーバによるアクセス要求に基づいて、サーバに対して書き込みの許容された区分領域に書き込みが実行される。
このバインドキーは、記録再生装置（ホスト）において、コンテンツ再生処理を実行する場合に必要なデータであり、記録再生装置（ホスト）は、バインドキーの書き込みが行われた区分領域の読み取り許可のなされた証明書（ホスト証明書）を保持していることが必要となる。
【０３１１】
記録再生装置（ホスト）において、コンテンツ再生処理を実行する場合、記録再生装置（ホスト）はメモリカードに対してホスト証明書を提供する。メモリカードのデータ処理部は、ホスト証明書の署名検証により、正当性を確認した後、ホスト証明書に記録された保護領域に対するアクセス許容情報を参照して、バインドキーの書き込まれた区分領域に対する読み取り（Ｒｅａｄ）の許可情報が記録されていることの確認を条件として、バインドキーを読み取り、記録再生装置（ホスト）に提供する。
【０３１２】
記録再生装置（ホスト）の所有するホスト証明書の例を図１８に示す。
図１８は、コンテンツ再生を実行する記録再生装置（ホスト）の所有するホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）の例である。図１８に示すように、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）には以下のデータが記録される。
【０３１３】
Ｔｙｐｅ：タイプ情報（Ｔｙｐｅ）５０１は、証明書の種類情報や、ホスト情報等を記録する。たとえばホストがＰＣであるか、ホストが記録再生装置であるか、記録装置であるか、再生装置であるかの情報等が記録される。
ＰＡＤ　Ｒｅａｄ：読み取り許容領域情報（ＰＡＤ　Ｒｅａｄ）５０２は、メモリカードの保護領域（ＰＡ：Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の読み取り（Ｒｅａｄ）の許容された区分領域を示す情報である。
ＰＡＤ　Ｗｒｉｔｅ：書き込み許容領域情報（ＰＡＤ　Ｗｒｉｔｅ）５０３は、メモリカードの保護領域（ＰＡ：Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の書き込み（Ｗｒｉｔｅ）の許容された区分領域を示す情報である。
Ｈｏｓｔ　ＩＤ：ホストＩＤ(Ｈｏｓｔ　ＩＤ)５０４は、ホストの識別子であるホストＩＤの記録領域である。
Ｈｏｓｔ　Ｐｕｂｌｉｃ　Ｋｅｙ：ホスト公開鍵（Ｈｏｓｔ　Ｐｕｂｌｉｃ　Ｋｅｙ）

５０５は、ホストの公開鍵を格納した領域である。
Ｓｉｇｎａｔｕｒｅ：署名（Ｓｉｇｎａｔｕｒｅ）５０６は、ホスト証明書の構成データに対する認証局の秘密鍵による署名データである。
これらのデータが記録される。

【０３１４】
なお、これらのデータは、先に図５を参照して説明したサーバ証明書（Ｓｅｒｖｅｒ Ｃｅｒｔｉｆｉｃａｔｅ）にも記録されている。

【０３１５】
図１９を参照して、メモリカードに対するアクセス要求装置がサーバである場合と、記録再生装置等のホスト機器である場合のアクセス制限の設定例について説明する。

【０３１６】
図１９には、左から、メモリカードに対するアクセス要求装置であるサーバ５２１、ホスト機器５２２、メモリカード５３０を示している。
サーバ５２１は、前述のダウンロードコンテンツや、ディスクからのコピーコンテンツの再生時に必要となるバインドキーの書き込み処理を実行するサーバである。
ホスト機器５２２は、メモリカードに格納されたコンテンツの再生処理を行う装置であり、コンテンツの復号処理のために、メモリカードに記録されたバインドキーを取得する必要がある機器である。

【０３１７】
メモリカード５３０は、保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）５４０と、非保護領域（Ｕｓｅｒ Ａｒｅａ）５５０を有し、暗号化コンテンツ等は非保護領域（Ｕｓｅｒ Ａｒｅａ）５５０に記録される。
バインドキー（Ｂｉｎｄｉｎｇ Ｋｅｙ）は保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）５４０に記録される。

【０３１８】
先に図６を参照して説明したように、保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）５４０は、複数の領域に区分されている。
図１９に示す例では、
区分領域＃０（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ＃０）５４１、
区分領域＃１（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ＃１）５４２、
これらの２つの区分領域を持つ例を示している。

【０３１９】
区分領域＃０（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ＃０）５４１は、放送コンテンツの鍵データとしてのバインドキー記録領域として設定され、
区分領域＃１（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ＃１）５４２は、ダウンロード、コピーコンテンツの鍵データとしてのバインドキー記録領域として設定された例である。

【０３２０】
このような設定では、先に図８を参照して説明したサーバの提供するバインドキーは、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ＃１）５４２に記録される。
この場合、サーバのサーバ証明書（Ｓｅｒｖｅｒ Ｃｅｒｔｉｆｉｃａｔｅ）に記録される書き込み許容領域情報（ＰＡＤ Ｗｒｉｔｅ）は、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ＃１）に対する書き込み（Ｗｒｉｔｅ）許可が設定された証明書として構成される。
なお、図に示す例では、書き込み（Ｗｒｉｔｅ）の許容された区分領域に対しては、読み取り（Ｒｅａｄ）についても許容された設定として示している。

【０３２１】
また、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ＃１）５４２に記録されたバインドキーを読み取ってコンテンツ再生を実行する再生装置であるホスト機器５２２の保持するホスト証明書（Ｈｏｓｔ Ｃｅｒｔｉｆｉｃａｔｅ）は、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ＃１）に対する読み取り（Ｒｅａｄ）許可のみが設定された証明書とし

て構成される。
【０３２２】
ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）には、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）に対する書き込み（Ｗｒｉｔｅ）許可は設定されない。
ただし、コンテンツ削除時に、削除コンテンツに対応するバインドキーの削除が可能な設定とするため、削除処理については許可する設定としてもよい。
【０３２３】
すなわち、メモリカードのデータ処理部は、アクセス要求装置からの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５４０に対するデータ書き込みとデータ読み取りについては、書く装置の装置証明書に基づいて許可するか否かを判定するが、削除要求についてはすべて許可する設定としてもよい。
【０３２４】
あるいは、アクセス要求装置の証明書に、区分領域単位の書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の各処理についての許容情報に加えて、削除（ｄｅｌｅｔｅ）についての許容情報を記録して、この記録情報に基づいて削除の可否を判定する構成としてもよい。
【０３２５】
図１９に示すメモリカード５３０の区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）５４１は、放送コンテンツの鍵データとしてのバインドキー記録領域として設定された例を示している。
放送コンテンツは、例えば、レコーダ、あるいはＰＣ等、放送データの受信、記録機能を持つホスト機器５２２が放送局からのコンテンツを受信してメディアに記録する。
【０３２６】
この場合、放送コンテンツの復号のために適用する鍵情報であるバインドキーは、放送局が提供し、ホスト機器５２２が受信する。ホスト機器５２２はメモリカード５３０にアクセスを行い、メモリカード５３０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５４０に放送コンテンツ用の鍵データを記録する。
【０３２７】
この例では、放送コンテンツ用の鍵データを記録する領域は、区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）５４１として予め規定されている。
メモリカード５３０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５４０は、このように、区分領域（＃０，＃１，＃２・・・）単位で、記録するデータの種類を予め規定することが可能である。
【０３２８】
メモリカードは、アクセス要求装置からのデータ書き込みや読み取り要求の入力に応じて、書き込みあるいは読み取り要求データの種類を判別し、データ書き込み先あるいは読み取り先としての区分領域（＃０，＃１，＃２・・・）を選別する。
【０３２９】
放送コンテンツの復号のために適用する鍵情報であるバインドキーは、ホスト機器５２２が書き込み処理を実行し、再生処理においても、ホスト機器５２２が読み取り処理を実行する。
【０３３０】
従って、ホスト機器５２２の保持するホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）は、放送コンテンツ用の鍵データの記録領域として規定された区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）５４１については、書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の双方の処理許可が設定された証明書として構成される。
【０３３１】
図１９に示すホスト５２２の保持するホスト証明書（Ｈｏｓｔ　Ｃｅｒ）は、図に示すように、
読み取り（Ｒｅａｄ）許容領域：＃０，＃１

書き込み（Ｗｒｉｔｅ）許容領域：＃０
これらの設定のなされた証明書となる。
【０３３２】
一方、サーバ５２１はこの放送コンテンツ用の鍵データの記録領域として規定された区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）５４１に対しては、データ書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）のいずれも許可されておらず、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）にはデータ書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の非許可情報が記録される。
【０３３３】
図１９に示すサーバ５２１の保持するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒ）は、図に示すように、
読み取り（Ｒｅａｄ）許容領域：＃１
書き込み（Ｗｒｉｔｅ）許容領域：＃１
これらの設定のなされた証明書となる。
【０３３４】
このように、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）は、アクセス要求装置単位、かつ区分領域（＃０，＃１，＃２・・・）単位で、データの書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の許容、非許容がアクセス制御情報として設定される。
【０３３５】
このアクセス制御情報は、各アクセス要求装置の証明書（サーバ証明書、ホスト証明書など）に記録され、メモリカードは、アクセス要求装置から受領した証明書について、まず署名検証を行い、正当性を確認した後、証明書に記載されたアクセス制御情報、すなわち、以下の情報を読み取る。
読み取り許容領域情報（ＰＡＤ　Ｒｅａｄ）、
書き込み許容領域情報（ＰＡＤ　Ｗｒｉｔｅ）、
これらの情報に基づいて、アクセス要求装置に対して認められた処理のみを許容して実行する。
【０３３６】
なお、ホスト機器にも、例えばレコーダ、プレーヤ等のＣＥ機器や、ＰＣ等、様々な機器の種類がある。
装置証明書は、これらの各装置が個別に保持する証明書であり、これらの装置の種類に応じて異なる設定とすることができる。
また、メモリカードのデータ処理部は、装置証明書に記録された以下の情報、すなわち、
読み取り許容領域情報（ＰＡＤ　Ｒｅａｄ）、
書き込み許容領域情報（ＰＡＤ　Ｗｒｉｔｅ）、
これらの情報のみならず、
図１８を参照して説明したタイプ情報（Ｔｙｐｅ）５０１に基づいて、保護領域の区分領域単位のアクセスの許容判定を行ってもよい。
【０３３７】
図２０には、メモリカード５３０に対するデータの記録や、メモリカード５３０に記録されたデータの読み出しを実行するホスト機器としてＰＣ５２３と、レコーダやプレーヤ等のＣＥ（Ｃｏｎｓｕｍｅｒ　Ｅｌｅｃｔｒｏｎｉｃｓ）機器５２４を示している。
【０３３８】
また、図２０に示すメモリカード５３０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５４０は、以下の設定のなされた区分領域を持つ。
区分領域＃２（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃２）５４５は、ＳＤ（Ｓｔａｎｄａｒｄ　Ｄｅｆｉｎｉｔｉｏｎ（標準画質））画像のデータに対応するコンテンツの鍵データとしてのバインドキー記録領域として設定され、

区分領域＃３（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃３）５４６は、ＨＤ（Ｈｉｇｈ　Ｄｅｆｉｎｉｔｉｏｎ（高画質））画像のデータに対応するコンテンツの鍵データとしてのバインドキー記録領域として設定されている。

【０３３９】

図２０に示すＰＣ５２３の保持するホスト証明書（Ｈｏｓｔ　Ｃｅｒ）は、図に示すように、

タイプ：ＰＣ

読み取り（Ｒｅａｄ）許容領域：＃２

書き込み（Ｗｒｉｔｅ）許容領域：＃２

これらの設定のなされた証明書である。

【０３４０】

また、ＣＥ機器５２４の保持するホスト証明書（Ｈｏｓｔ　Ｃｅｒ）は、図に示すように、

タイプ：ＣＥ

読み取り（Ｒｅａｄ）許容領域：＃２，３

書き込み（Ｗｒｉｔｅ）許容領域：＃２，３

これらの設定のなされた証明書である。

【０３４１】

すなわち、ＰＣ５２３は、ＳＤ（Ｓｔａｎｄａｒｄ　Ｄｅｆｉｎｉｔｉｏｎ（標準画質））画像のデータに対応するコンテンツの鍵データとしてのバインドキー記録領域である区分領域＃２（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃２）５４５に対するデータ書き込み（Ｗｒｉｔｅ）と読み取り（Ｒｅａｄ）のみが許容されている。ＰＣ５２３は、ＨＤ（Ｈｉｇｈ　Ｄｅｆｉｎｉｔｉｏｎ（高画質））画像のデータに対応するコンテンツの鍵データとしてのバインドキー記録領域である区分領域＃３（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃３）５４６に対するデータ書き込み（Ｗｒｉｔｅ）と読み取り（Ｒｅａｄ）は許可されていない。

【０３４２】

また、ＣＥ機器５２４は、ＳＤ（Ｓｔａｎｄａｒｄ　Ｄｅｆｉｎｉｔｉｏｎ（標準画質））画像のデータに対応するコンテンツの鍵データとしてのバインドキー記録領域である区分領域＃２（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃２）５４５に対するデータ書き込み（Ｗｒｉｔｅ）と読み取り（Ｒｅａｄ）のみが許容されている。また、ＨＤ（Ｈｉｇｈ　Ｄｅｆｉｎｉｔｉｏｎ（高画質））画像のデータに対応するコンテンツの鍵データとしてのバインドキー記録領域である区分領域＃３（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃３）５４６に対するデータ書き込み（Ｗｒｉｔｅ）と読み取り（Ｒｅａｄ）も許可されている。

【０３４３】

このように、ホスト機器であってもその装置の種類に応じたアクセス制御情報を設定できる。

なお。ホスト証明書のタイプ情報にはＰＣであるかＣＥ機器であるかを識別する情報が含まれており、メモリカードのデータ処理部は、装置証明書に記録されたアクセス制御情報、すなわち、

読み取り許容領域情報（ＰＡＤ　Ｒｅａｄ）、

書き込み許容領域情報（ＰＡＤ　Ｗｒｉｔｅ）、

これらの情報に基づいて、核区分領域のアクセス（Ｒｅａｄ／Ｗｒｉｔｅ）可否の判定を行ってもよいが、タイプ情報（Ｔｙｐｅ）に基づいて、保護領域の区分領域単位のアクセスの許容判定を行ってもよい。

【０３４４】

図１９、図２０を参照して説明したように、メモリカード５３０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５４０に設定する複数の区分領域については、例えば、

プレミアムコンテンツと放送録画コンテンツ、あるいは、

ＳＤ画サイズのコンテンツとＨＤ画サイズのコンテンツ、

このように、要求されるセキュリティレベルが異なるコンテンツを格納領域として設定する構成が可能である。
また、
サーバやクライアント、
ＰＣやＣＥ機器、
このように、セキュリティレベルの異なる機器に応じてそれぞれ記録もしくは再生のいずれかを許容するといった設定とすることで、各区分領域の利用形態を柔軟に制御できる。

【０３４５】

さらに、例えば、サーバやホスト機器等の特定の機器のアクセス権限を変更したい場合には、証明書に属性を追加するといった処理も可能である。
この権限変更の方法の具体的な手法として、例えばあるホスト機器に権限を追加する場合の処理としては、以下のような方法がある。
（１）権限変更を行うホスト機器に対して新たな鍵と属性を追加した証明書を合わせて発行し、古いホスト機器の鍵と証明書を無効化して、鍵と証明書の更新を行う。
あるいは、１つのホスト機器が有効な２つ以上の鍵と証明書を持つ構成としてもよい。
（２）属性を追加した証明書のみを追加発行して、ホスト機器の証明書のみを更新する。
（３）追加したい属性のみ記述した証明書のみを追加発行する。
ただし、この場合、ホスト機器は１つの鍵に対して複数の証明書を持つことになる。
例えば、上記の（１）～（３）の方法で特定の機器のアクセス権限を変更する処理が可能となる。

【０３４６】

［８．各装置のハードウェア構成例について］
最後に、図２１以下を参照して、上述した処理を実行する各装置のハードウェア構成例について説明する。
まず、図２１を参照して、メモリカードを装着してデータの記録や再生処理を行うホスト機器のハードウェア構成例について説明する。

【０３４７】

ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）７０１は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）７０２、または記憶部７０８に記憶されているプログラムに従って各種の処理を実行するデータ処理部として機能する。例えば、上述の各実施例において説明したサーバとの通信処理やサーバからの受信データのメモリカード(図中のリムーバブルメディア７１１)に対する記録処理、メモリカード(図中のリムーバブルメディア７１１)からのデータ再生処理等を実行する。ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）７０３には、ＣＰＵ７０１が実行するプログラムやデータなどが適宜記憶される。これらのＣＰＵ７０１、ＲＯＭ７０２、およびＲＡＭ７０３は、バス７０４により相互に接続されている。

【０３４８】

ＣＰＵ７０１はバス７０４を介して入出力インタフェース７０５に接続され、入出力インタフェース７０５には、各種スイッチ、キーボード、マウス、マイクロホンなどよりなる入力部７０６、ディスプレイ、スピーカなどよりなる出力部７０７が接続されている。ＣＰＵ７０１は、入力部７０６から入力される指令に対応して各種の処理を実行し、処理結果を例えば出力部７０７に出力する。

【０３４９】

入出力インタフェース７０５に接続されている記憶部７０８は、例えばハードディスク等からなり、ＣＰＵ７０１が実行するプログラムや各種のデータを記憶する。通信部７０９は、インターネットやローカルエリアネットワークなどのネットワークを介して外部の装置と通信する。

【０３５０】

入出力インタフェース７０５に接続されているドライブ７１０は、磁気ディスク、光ディスク、光磁気ディスク、或いは半導体メモリなどのリムーバブルメディア７１１を駆動し、記録されているコンテンツや鍵情報等の各種データを取得する例えば、。取得されたコンテンツや鍵データを用いて、ＣＰＵによって実行する再生プログラムに従ってコンテンツの復号、再生処理などが行われる。

【０３５１】

図２２は、メモリカードのハードウェア構成例を示している。

ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）８０１は、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）８０２、または記憶部８０７に記憶されているプログラムに従って各種の処理を実行するデータ処理部として機能する。例えば、上述の各実施例において説明したサーバやホスト機器との通信処理やデータの記憶部８０７に対する書き込み、読み取り等の処理、記憶部８０７の保護領域８１１の区分領域単位のアクセス可否判定処理等を実行する。ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）８０３には、ＣＰＵ８０１が実行するプログラムやデータなどが適宜記憶される。これらのＣＰＵ８０１、ＲＯＭ８０２、およびＲＡＭ８０３は、バス８０４により相互に接続されている。

【０３５２】

ＣＰＵ８０１はバス８０４を介して入出力インタフェース８０５に接続され、入出力インタフェース８０５には、通信部８０６、記憶部８０７が接続されている。

【０３５３】

入出力インタフェース８０５に接続されている通信部８０４は、例えばサーバ、ホスト機器との通信を実行する。記憶部８０７は、データの記憶領域であり、先に説明したようにアクセス制限のある保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｅａ）８１１、自由にデータ記録読み取りができる非保護領域８１２を有する。

【０３５４】

なお、サーバは、例えば図２１に示すホスト機器と同様のハードウェア構成を持つ装置によって実現可能である。

【０３５５】

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

【０３５６】

また、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。例えば、プログラムは記録媒体に予め記録しておくことができる。記録媒体からコンピュータにインストールする他、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、インターネットといったネットワークを介してプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０３５７】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【産業上の利用可能性】

【０３５８】

以上、説明したように、本発明の一実施例の構成によれば、メディアに記録されたコン

テンツの不正利用を防止する再生制御が実現される。メディアの記録コンテンツに対応する管理データであるトークンをメディアから取得し、取得したトークンに記録されたサーバＩＤと、管理データの取得元であるサーバから取得したサーバ証明書に記録されたサーバＩＤとを比較し、両サーバＩＤが一致しない場合は、コンテンツ再生を中止させる。両ＩＤの一致が確認された場合には、再生予定のコンテンツＩＤがコンテンツリボケーションリストに記録されているか否かを検証し、記録されている場合には、コンテンツ再生を中止する。本処理により、メディア記録コンテンツの不正利用を防止した再生制御が実現される。

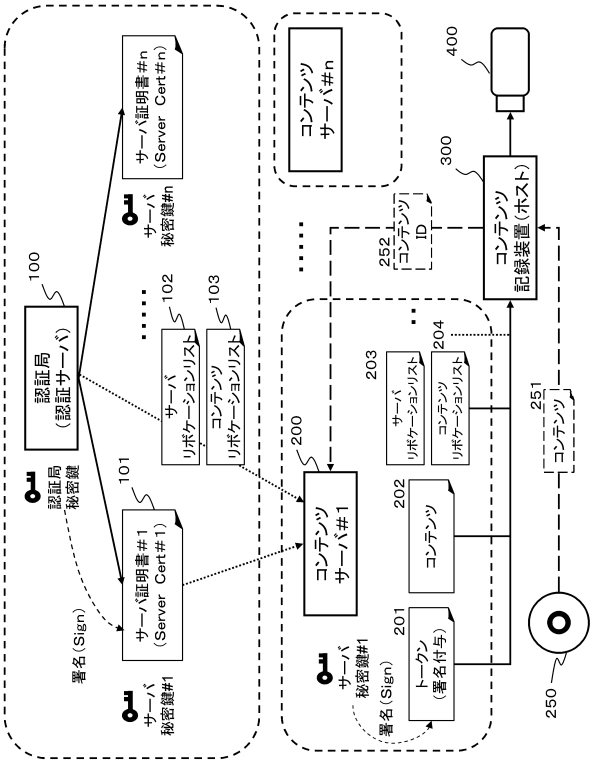
【符号の説明】

【０３５９】

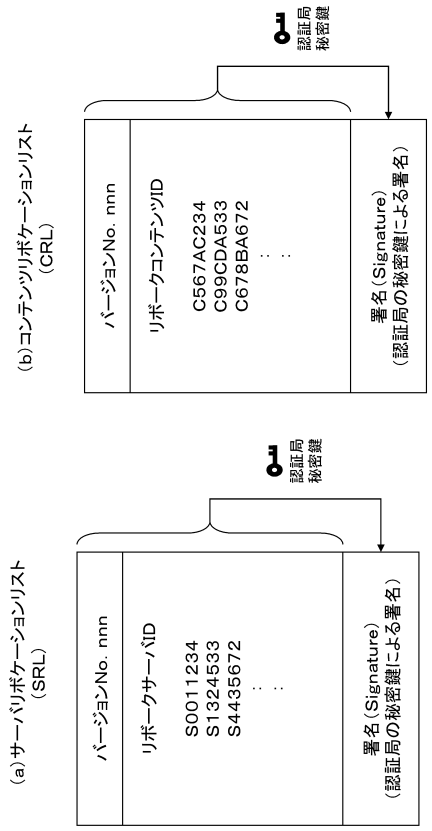
１１　コンテンツサーバ
１２　コンテンツ記録ディスク
２１　共用端末
２２　記録再生器（ＣＥ機器）
２３　ＰＣ
３１　メモリカード
１００　認証局（認証サーバ）
１０１　サーバ生類所（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）
１０２　サーバリボケーションリスト(ＳＲＬ)
１０３　コンテンツリボケーションリスト（ＣＲＬ）
２００　コンテンツサーバ
２０１　トークン
２０２　コンテンツ
２０３　サーバリボケーションリスト(ＳＲＬ)
２０４　コンテンツリボケーションリスト（ＣＲＬ）
２１１　データベース（ＤＢ）
２１２　ボリュームＩＤ
２１３　トークン
２１４　ボリュームユニークキー
２１５　タイトルキー（ＣＰＳユニットキー）
２１６　利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）
２１８　コンテンツ
２５０　ディスク
２５１　コンテンツ
２５２　コンテンツＩＤ
３００　コンテンツ記録装置（ホスト）
３１１　サーバリボケーションリスト(ＳＲＬ)
３１２４　コンテンツリボケーションリスト（ＣＲＬ）
４００　メモリカード
４０１　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
４０２　非保護領域
４１１　メディアＩＤ
４１２　保護領域
４１４　バインドキー
４１５　トークン
４１６暗号化タイトルキー
４１７　利用制御情報
４１８　暗号化コンテンツ
５０１　タイプ情報（Ｔｙｐｅ）
５０２　読み取り許容領域情報（ＰＡＤ　Ｒｅａｄ）

５０３　書き込み許容領域情報（ＰＡＤ　Ｗｒｉｔｅ）
５０４　ホストＩＤ(Ｈｏｓｔ　ＩＤ)
５０５　ホスト公開鍵（Ｈｏｓｔ　Ｐｕｂｌｉｃ　Ｋｅｙ）
５０６　署名（Ｓｉｇｎａｔｕｒｅ）
５２１　サーバ
５２２　ホスト機器
５２３　ＰＣ
５２４　ＣＥ機器
５３０　メモリカード
５４０　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
５４１　区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）
５４２　区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）
５４５　区分領域＃２（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃２）
５４６　区分領域＃３（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃３）
５５０　非保護領域（Ｕｓｅｒ　Ａｒｅａ）
７０１　ＣＰＵ
７０２　ＲＯＭ
７０３　ＲＡＭ
７０４　バス
７０５　入出力インタフェース
７０６　入力部
７０７　出力部
７０８　記憶部
７０９　通信部
７１０　ドライブ
７１１　リムーバブルメディア
８０１　ＣＰＵ
８０２　ＲＯＭ
８０３　ＲＡＭ
８０４　バス
８０５　入出力インタフェース
８０６　通信部
８０７　記憶部
８１１　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
８１２　非保護領域（Ｕｓｅｒ　Ａｒｅａ）

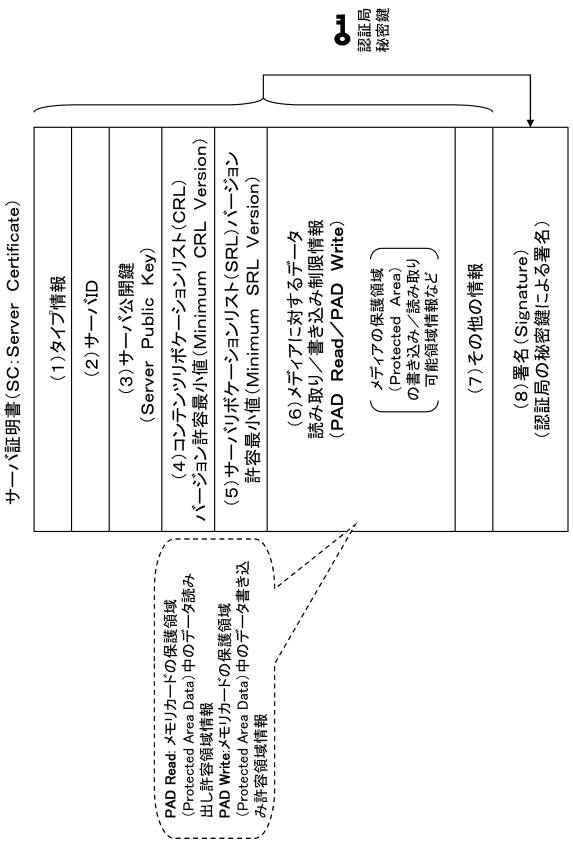
【図３】


認証局
(認証サーバ)
100
認証局
秘密鍵
署名(Sign)
サーバ証明書#1
(Server Cert#1)
101
サーバ
秘密鍵#1
サーバ証明書#n
(Server Cert#n)
サーバ
秘密鍵#n
サーバ
リポケーションリスト
102
コンテンツ
リポケーションリスト
103
コンテンツ
サーバ#1
200
コンテンツ
202
トークン
(署名付与)
201
サーバ
秘密鍵#1
署名(Sign)
サーバ
リポケーションリスト
203
コンテンツ
リポケーションリスト
204
コンテンツ
サーバ#n
252
コンテンツ
ID
300
コンテンツ
記録装置(ホスト)
400
251
コンテンツ
250

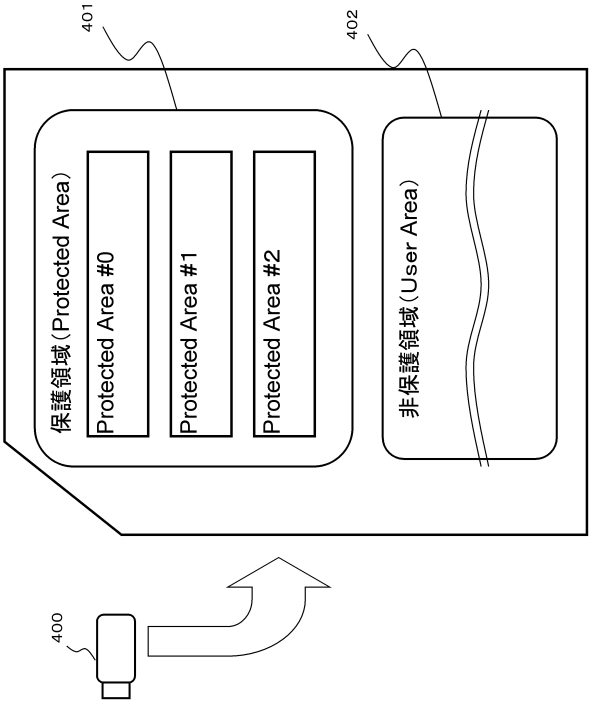
【図４】


(a)サーバリポケーションリスト
(SRL)
バージョンNo. nnn
リポークサーバID
S0011234
S1324533
S4435672
署名(Signature)
(認証局の秘密鍵による署名)
認証局
秘密鍵
(b)コンテンツリポケーションリスト
(CRL)
バージョンNo. nnn
リポークコンテンツID
C567AC234
C99CDA533
C678BA672
署名(Signature)
(認証局の秘密鍵による署名)
認証局
秘密鍵

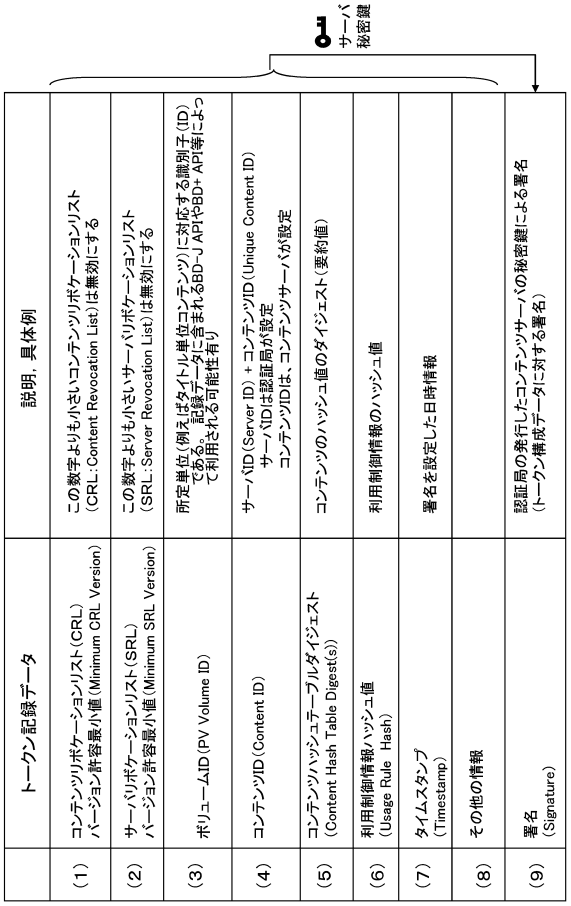
【図５】


サーバ証明書(SC:Server Certificate)
(1)タイプ情報
(2)サーバID
(3)サーバ公開鍵
(Server Public Key)
(4)コンテンツリポケーションリスト(CRL)
バージョン許容最小値(Minimum CRL Version)
(5)サーバリポケーションリスト(SRL)バージョン
許容最小値(Minimum SRL Version)
(6)メディアに対するデータ
読み取り／書き込み制限情報
(PAD Read／PAD Write)
メディアの保護領域
(Protected Area)
の書き込み／読み取り
可能領域情報など
(7)その他の情報
(8)署名(Signature)
(認証局の秘密鍵による署名)
認証局
秘密鍵
PAD Read:メモリカードの保護領域
(Protected Area Data)中のデータ読み
出し許容領域情報
PAD Write:メモリカードの保護領域
(Protected Area Data)中のデータ書き込
み許容領域情報

【図６】

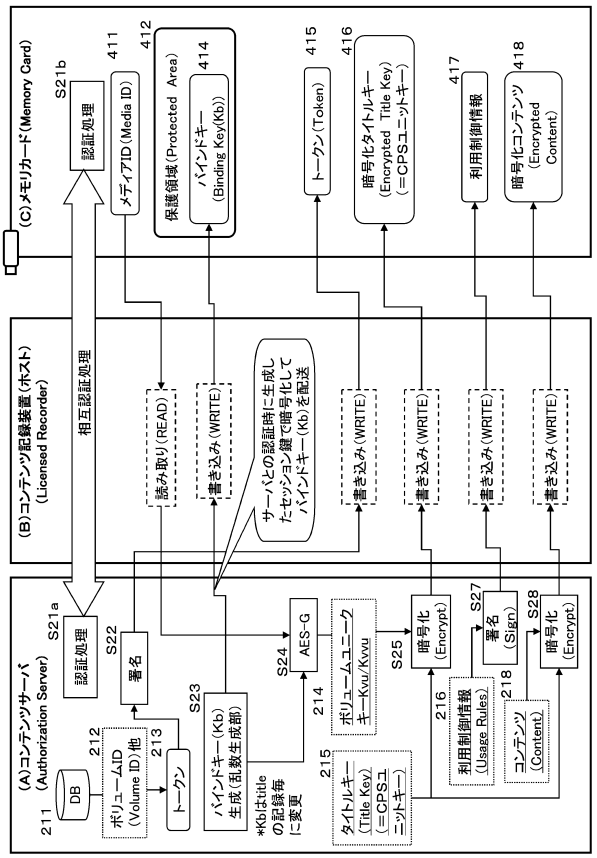

401
402
保護領域(Protected Area)
Protected Area #0
Protected Area #1
Protected Area #2
非保護領域(User Area)
400

【図７】

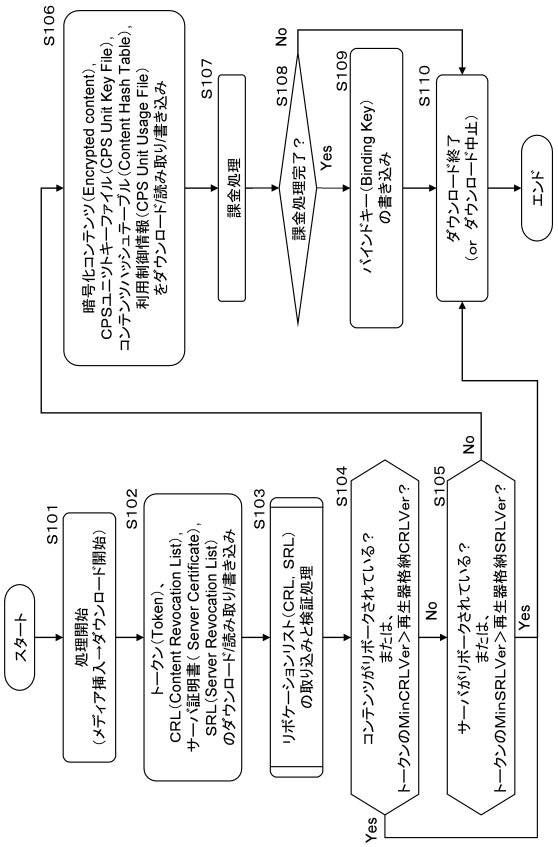


	トークン記録データ	説明，具体例
(1)	コンテンツリボケーションリスト(CRL) バージョン許容最小値(Minimum CRL Version)	この数字よりも小さいコンテンツリボケーションリスト (CRL:Content Revocation List)は無効にする
(2)	サーバリボケーションリスト(SRL) バージョン許容最小値(Minimum SRL Version)	この数字よりも小さいサーバリボケーションリスト (SRL:Server Revocation List)は無効にする
(3)	ボリュームID (PV Volume ID)	所定単位(例えばタイトル単位コンテンツ)に対応する識別子(ID) である。記録データに含まれるBD-J APIやBD+ API等によって利用される可能性有り
(4)	コンテンツID (Content ID)	サーバID (Server ID) + コンテンツID (Unique Content ID) サーバIDは認証局が設定 コンテンツIDは、コンテンツサーバが設定
(5)	コンテンツハッシュテーブルダイジェスト (Content Hash Table Digest(s))	コンテンツのハッシュ値のダイジェスト(要約値)
(6)	利用制御情報ハッシュ値 (Usage Rule Hash)	利用制御情報のハッシュ値
(7)	タイムスタンプ (Timestamp)	署名を設定した日時情報
(8)	その他の情報	
(9)	署名 (Signature)	認証局の発行したコンテンツサーバの秘密鍵による署名 (トークン構成データに対する署名)

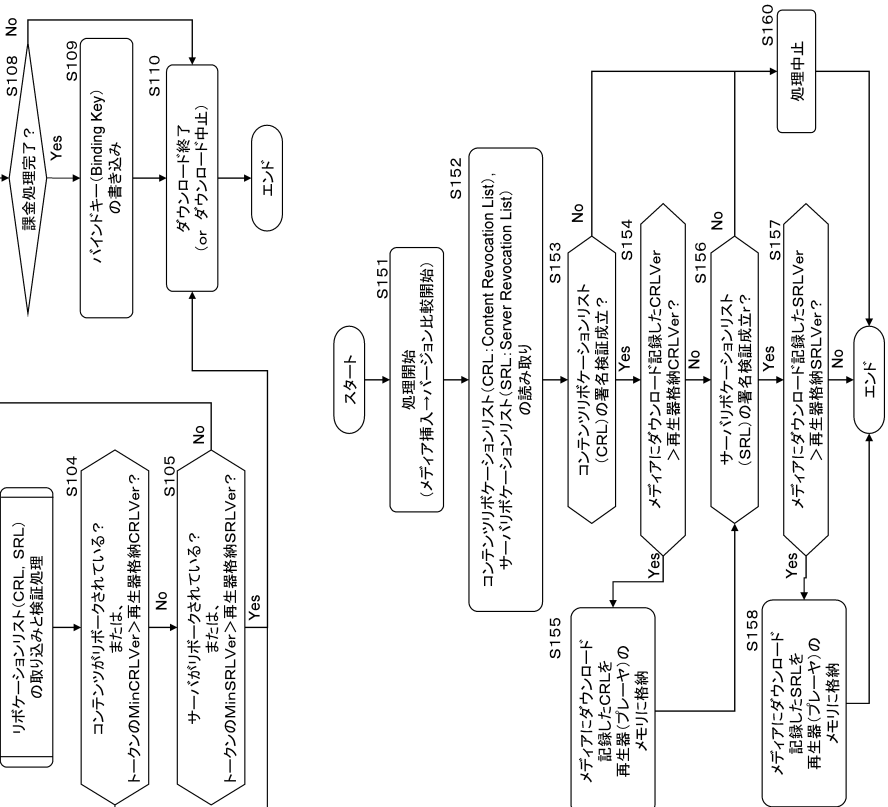
【図８】



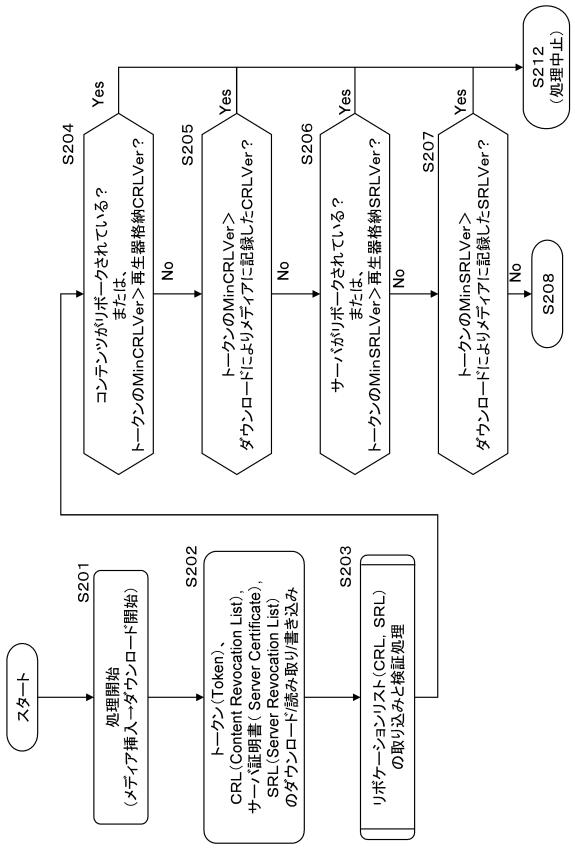
【図１０】



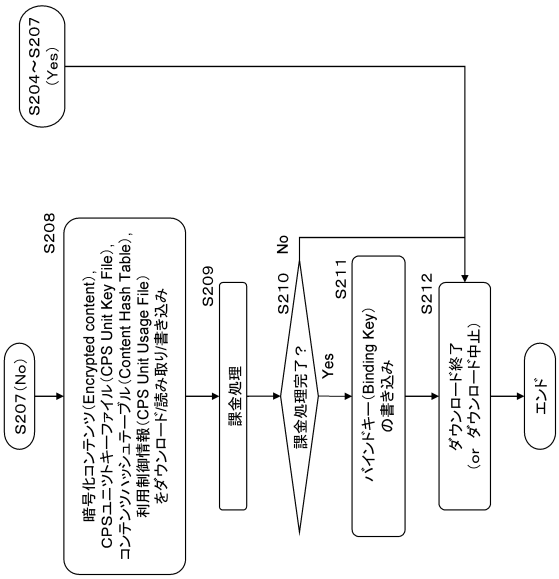
【図１１】



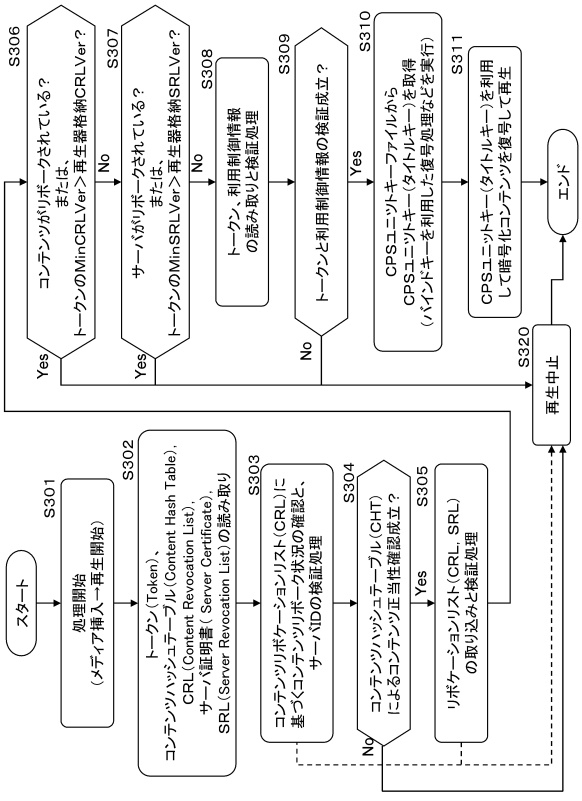
【図１２】



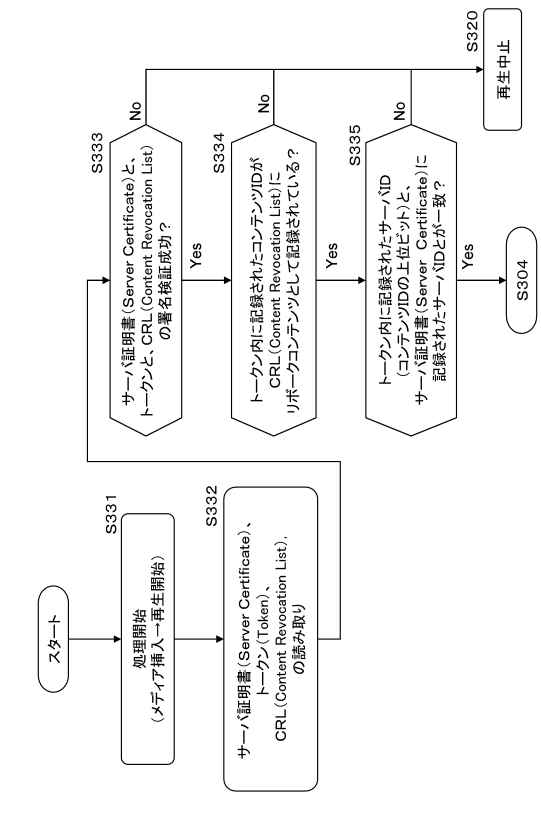
【図１３】



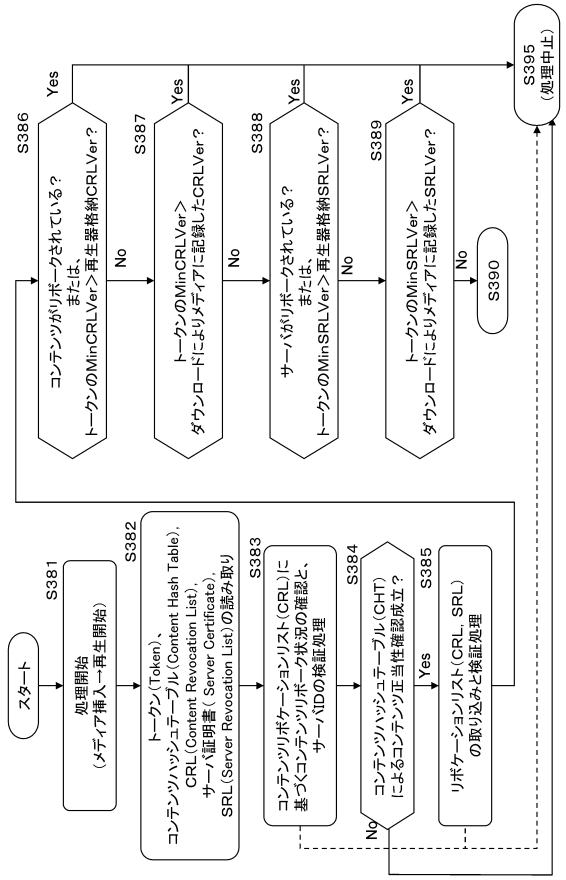
【図１４】



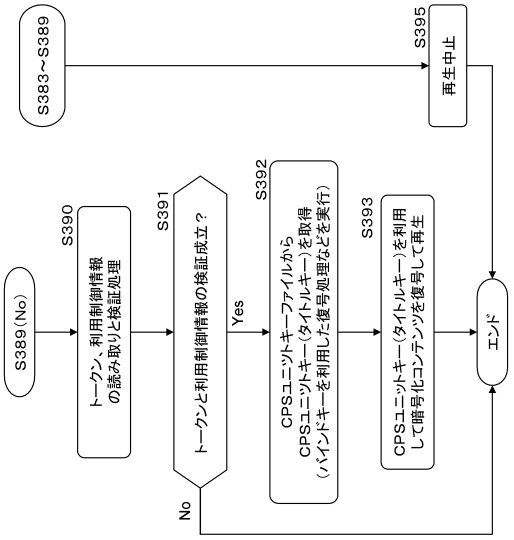
【図１５】



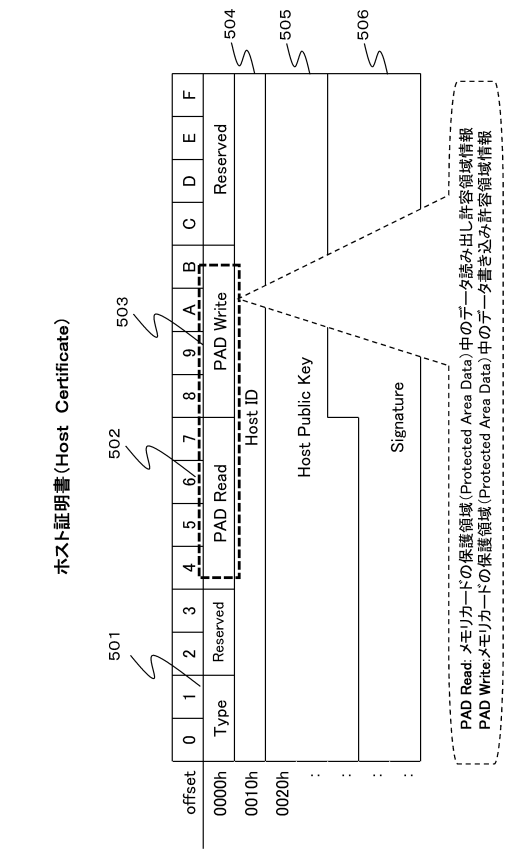
【図１６】



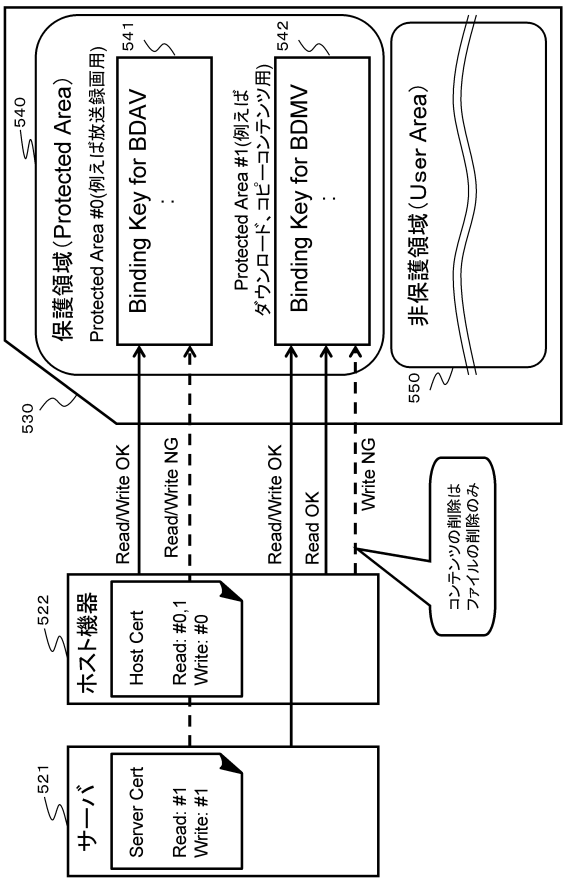
【図１７】



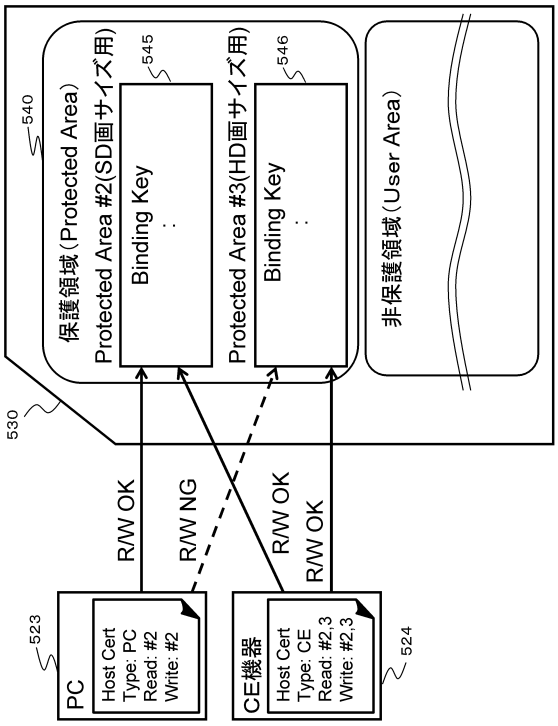
【図１８】



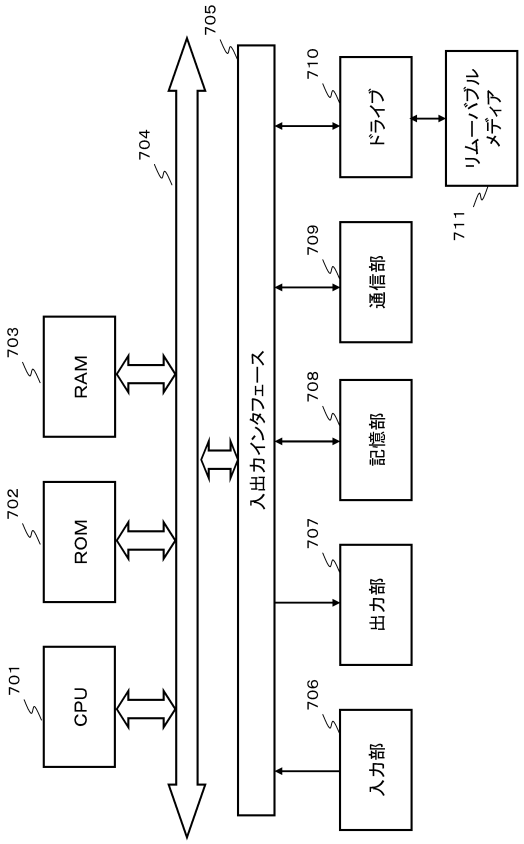
【図１９】



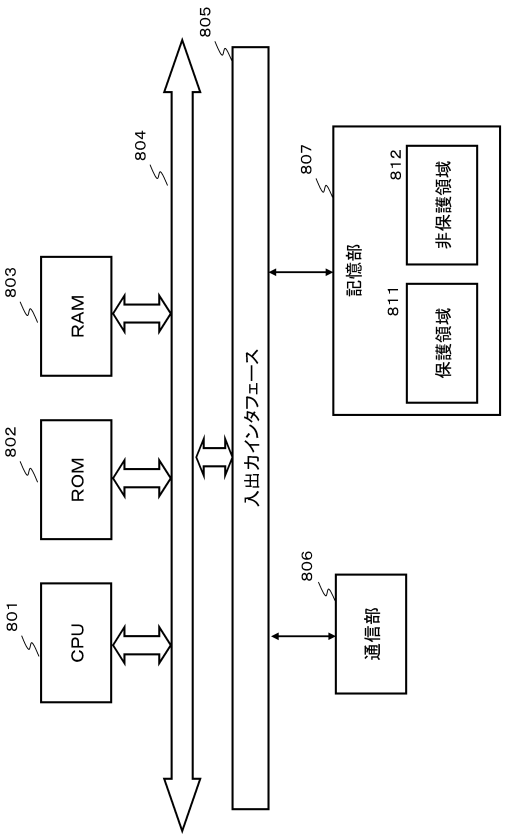
【図２０】


530
保護領域(Protected Area)
Protected Area #2(SD画サイズ用)
Binding Key
545
Protected Area #3(HD画サイズ用)
Binding Key
546
540
非保護領域(User Area)
R/W OK
R/W NG
R/W OK
R/W OK
PC
Host Cert
Type: PC
Read: #2
Write: #2
523
CE機器
Host Cert
Type: CE
Read: #2,3
Write: #2,3
524

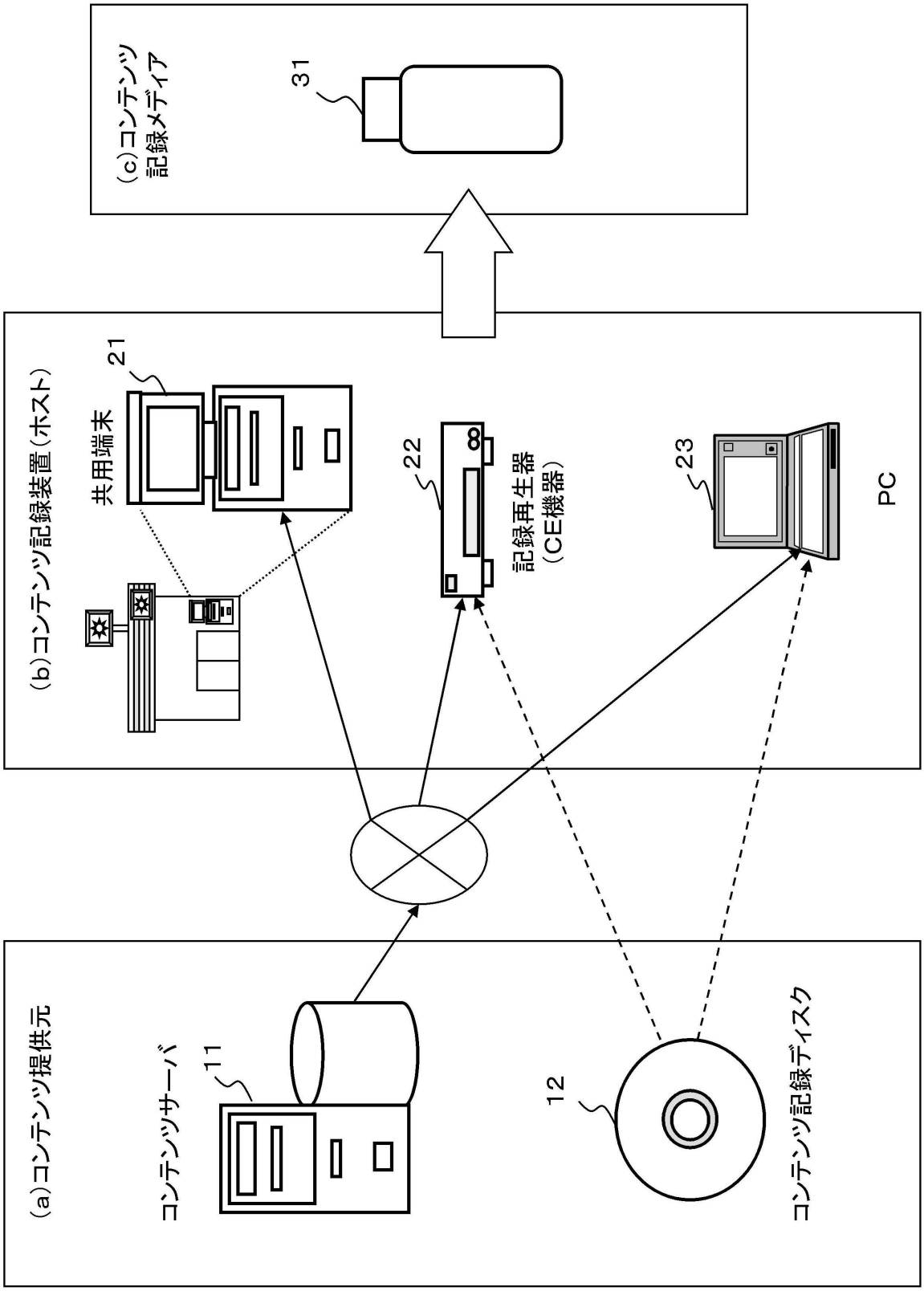
【図２１】


705
704
710
ドライブ
リムーバブル
メディア
711
703
RAM
709
通信部
入出力インタフェース
702
ROM
708
記憶部
707
出力部
701
CPU
706
入力部

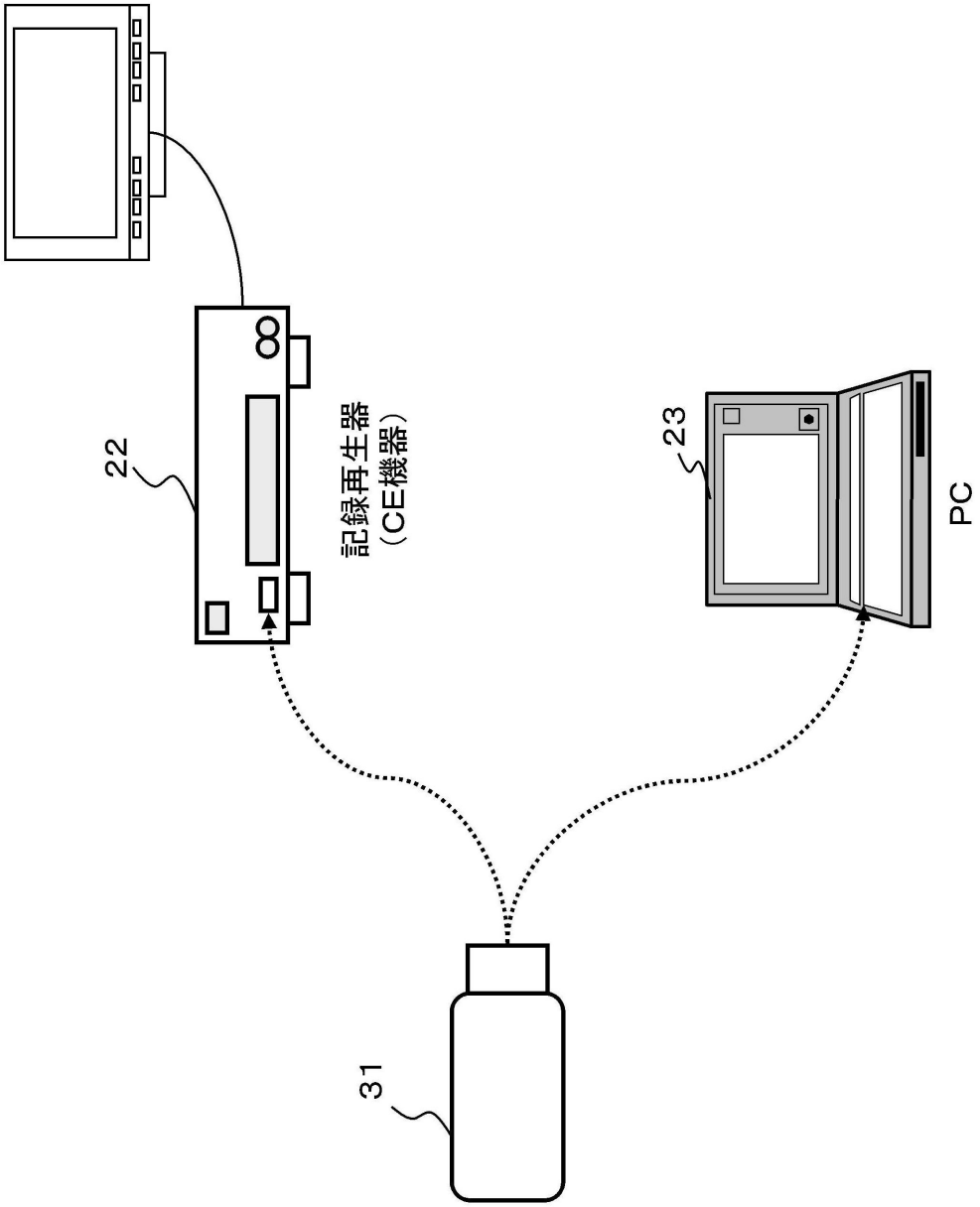
【図２２】


805
804
807
812
非保護領域
803
RAM
811
保護領域
記憶部
802
ROM
入出力インタフェース
801
CPU
806
通信部

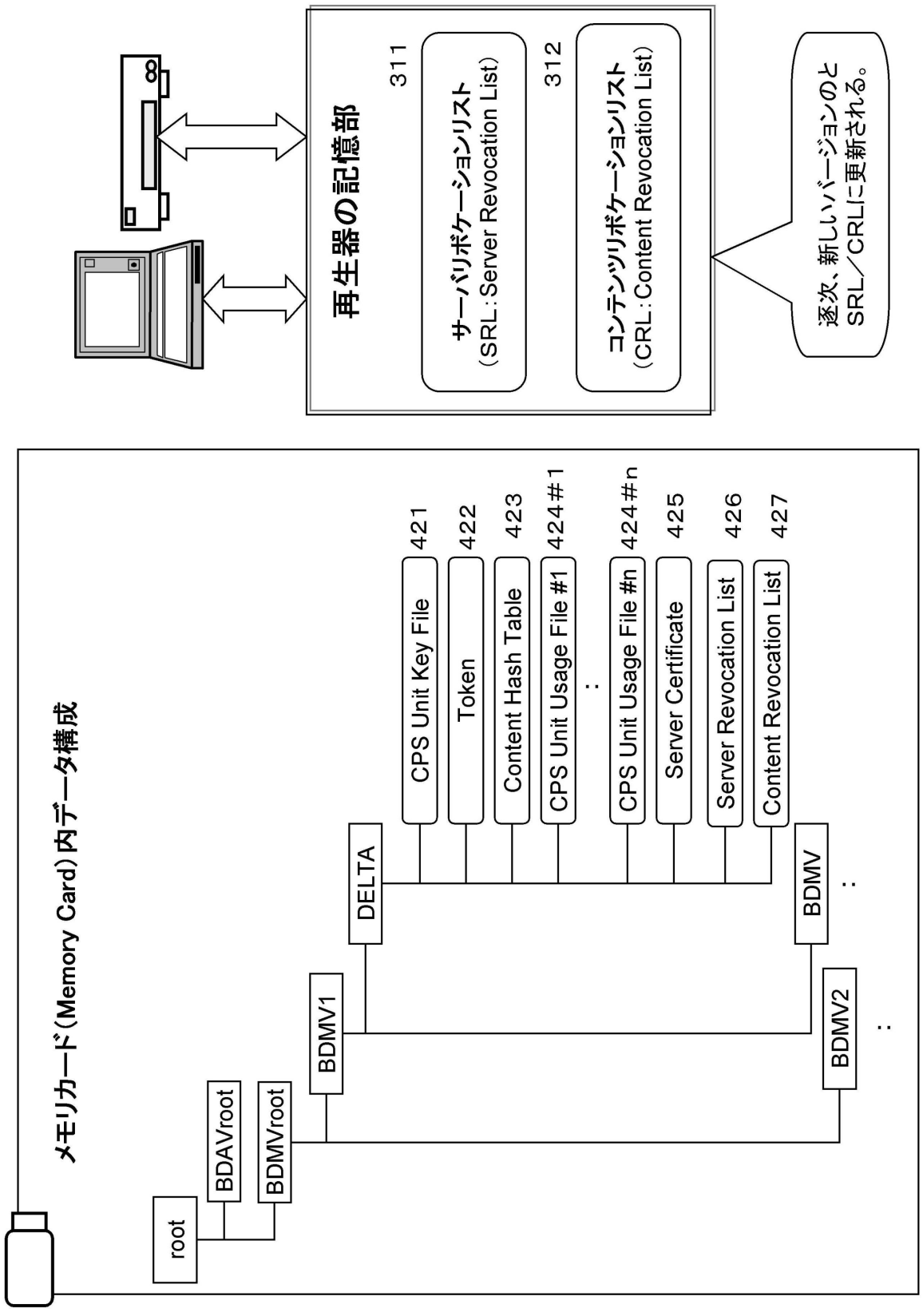
【図１】


(c)コンテンツ
記録メディア
31
(b)コンテンツ記録装置(ホスト)
21
共用端末
22
記録再生器
(CE機器)
23
PC
(a)コンテンツ提供元
コンテンツサーバ
11
12
コンテンツ記録ディスク

【図２】



【図９】


メモリカード(Memory Card)内データ構成
root
BDAVroot
BDMVroot
BDMV1
DELTA
CPS Unit Key File
421
Token
422
Content Hash Table
423
CPS Unit Usage File #1
424#1
CPS Unit Usage File #n
424#n
Server Certificate
425
Server Revocation List
426
Content Revocation List
427
BDMV
BDMV2
再生器の記憶部
311
サーバリボケーションリスト
(SRL:Server Revocation List)
312
コンテンツリボケーションリスト
(CRL:Content Revocation List)
逐次、新しいバージョンのと
SRL／CRLに更新される。

フロントページの続き

(51)Int.Cl. F I
H04L 9/00 675B

(72)発明者 上田 健二朗
東京都港区港南１丁目７番１号 ソニー株式会社内
(72)発明者 吉村 光司
東京都港区港南１丁目７番１号 ソニー株式会社内
(72)発明者 久野 浩
東京都港区港南１丁目７番１号 ソニー株式会社内
(72)発明者 林 隆道
東京都港区港南１丁目７番１号 ソニー株式会社内
(72)発明者 海老原 宗毅
東京都港区港南１丁目７番１号 ソニー株式会社内

審査官 脇岡 剛

(56)参考文献 特開２００４－１５７７０３（ＪＰ，Ａ）
特開２００８－１４０４４０（ＪＰ，Ａ）
特開２００５－１２２５６７（ＪＰ，Ａ）
特開２００２－１３５２４３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ ２１／６２
Ｇ０６Ｆ ２１／６４
Ｇ０６Ｋ １７／００
Ｈ０４Ｌ ９／３２