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

特許第5747758号
(P5747758)

(45)発行日　平成27年7月15日(2015.7.15)　(24)登録日　平成27年5月22日(2015.5.22)

(51)Int.Cl.		F I		
G06F 21/62	(2013.01)	G06F	21/62	309
G06F 21/60	(2013.01)	G06F	21/60	320
G06F 21/10	(2013.01)	G06F	21/10	350

請求項の数 20　(全 59 頁)

(21)出願番号　特願2011-202186(P2011-202186)
(22)出願日　平成23年9月15日(2011.9.15)
(65)公開番号　特開2013-65089(P2013-65089A)
(43)公開日　平成25年4月11日(2013.4.11)
審査請求日　平成26年8月7日(2014.8.7)

(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】
メディアに格納されたコンテンツを再生するデータ処理部を有し、
前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納した汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記データ処理部は、
コンテンツ再生処理に際して、前記コンテンツ初回再生時の日時情報に応じて決定されるコンテンツ利用許容期間である有効期限情報を前記暗号鍵格納ブロックから取得し、取得した有効期限情報と現在日時情報との比較により、コンテンツ再生の可否を判定する情報処理装置。
【請求項２】
前記暗号鍵格納ブロックに記録された有効期限情報は、前記ステータス格納ブロックに記録されたコンテンツ初回再生時の日時情報を基準日時として設定した有効期限情報である請求項１に記載の情報処理装置。

【請求項３】
前記利用制御情報は、
再生対象コンテンツの復号用の暗号鍵を格納した暗号鍵格納ブロックを識別可能とした暗号鍵格納ブロック識別子と、
前記再生対象コンテンツのコンテンツ対応ステータス情報を格納したステータス格納ブロックを識別可能としたステータス格納ブロック識別子を有し、
前記データ処理部は、
前記暗号鍵格納ブロック識別子に基づいて、前記保護領域から１つの暗号鍵格納ブロックを選択し、
前記ステータス格納ブロック識別子に基づいて、前記保護領域から１つのステータス格納ブロックを選択し、
各選択ブロックから前記再生対象コンテンツに対応する暗号鍵とステータス情報を取得する請求項１に記載の情報処理装置。
【請求項４】
前記暗号鍵格納ブロックには、前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である複数の有効期限情報が格納され、
前記データ処理部は、
前記汎用領域から再生対象コンテンツの利用制御情報を取得し、
前記ブロックに記録された複数の有効期限情報中、再生対象コンテンツに適用すべき有効期限情報の選択情報を、前記利用制御情報から抽出し、
該選択情報に従って、前記ブロックから選択した有効期限情報がコンテンツ初回再生時の日時情報に応じた有効期限情報である場合、前記コンテンツ対応ステータス情報として記録されたコンテンツ初回再生時の日時情報を基準日時とした有効期限情報に基づくコンテンツ再生可否判定を行う請求項１に記載の情報処理装置。
【請求項５】
前記データ処理部は、
前記利用制御情報、または前記ブロックから取得した有効期限情報と現在日時情報との比較処理を行う際に、信頼できる時間情報提供サーバから取得した現在日時情報を適用した処理を行う請求項１に記載の情報処理装置。
【請求項６】
前記暗号鍵格納ブロック、および前記ステータス格納ブロックは、前記メディアによるアクセス権判定に基づいてアクセスの認められるブロックであり、
前記データ処理部は、
前記暗号鍵格納ブロック、および前記ステータス格納ブロックからのデータ読み出し処理に際して、情報処理装置の証明書（Ｃｅｒｔｉｆｉｃａｔｅ）を前記メディアに送信し、前記メディアによるアクセス権判定処理によってデータ読み出し権利が確認されたことを条件として、データ読み出しを行う請求項１に記載の情報処理装置。
【請求項７】
前記ステータス格納ブロックは、前記メディアによるアクセス権判定に基づいてアクセスの認められるブロックであり、
前記データ処理部は、
前記ステータス格納ブロックに対するコンテンツ初回再生日時情報の記録処理に際して、情報処理装置の証明書（Ｃｅｒｔｉｆｉｃａｔｅ）を前記メディアに送信し、前記メディアによるアクセス権判定処理によってデータ書き込み処理の権利が確認されたことを条件として、データ記録を行う請求項１に記載の情報処理装置。
【請求項８】
前記暗号鍵格納ブロックは、前記メディアによるアクセス権判定に基づいてアクセスの認められるブロックであり、
前記ブロックに記録された有効期限情報は、前記暗号鍵格納ブロックに対するデータ書

き込み処理の権利を有するサーバによって書き込みおよび更新が行われる情報である請求項１に記載の情報処理装置。
【請求項９】
メディアに対するコンテンツ記録処理を行う情報処理装置であり、
前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納する汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記情報処理装置は、
前記汎用領域に対して、暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を記録する処理を行い、
前記暗号鍵格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの復号用の暗号鍵を記録し、
前記ステータス格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの初回再生時の日時情報を記録するためのコンテンツ対応ステータス情報記録領域を設定する処理を行う情報処理装置。
【請求項１０】
前記情報処理装置は、
前記利用制御情報に、前記暗号鍵格納ブロックの識別子と、前記ステータス格納ブロックの識別子を記録して前記メディアの汎用領域に記録する処理を行う請求項９に記載の情報処理装置。
【請求項１１】
前記暗号鍵を格納したブロックは、前記メディアによるアクセス権判定に基づいてアクセスの認められるブロックであり、
前記情報処理装置は、
前記ブロックに対するデータ記録処理に際して、情報処理装置の証明書（Ｃｅｒｔｉｆｉｃａｔｅ）を前記メディアに送信し、前記メディアによるアクセス権判定処理によってデータ記録処理の権利を有することが確認されたことを条件として、前記ブロックに対するデータ記録処理を行う請求項９に記載の情報処理装置。
【請求項１２】
前記情報処理装置は、
前記メディアに記録されたコンテンツを他の第２メディアに移動する処理に際して、
前記ステータス情報も併せて第２メディアに移動する処理を実行する請求項９に記載の情報処理装置。
【請求項１３】
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納した汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記暗号化コンテンツの再生処理を実行する再生装置に、前記暗号鍵格納ブロックに記録された有効期限情報と、前記ステータス格納ブロックに記録されたコンテンツ対応ステータス情報の参照処理に基づいて、コンテンツ初回再生時の日時情報に応じて設定されるコンテンツ利用許容期限に基づくコンテンツ再生可否判定を行わせることを可能とした情

報記憶装置。
【請求項１４】
前記利用制御情報は、
前記暗号鍵格納ブロックの識別子と、前記ステータス格納ブロックの識別子を記録した構成であり、
前記暗号化コンテンツの再生処理を実行する再生装置に、前記利用制御情報に記録された各ブロック識別子の参照処理に基づくブロック特定処理を行わせることを可能とした請求項１３に記載の情報記憶装置。
【請求項１５】
前記情報記憶装置は、
前記保護領域のブロックに対するアクセス要求装置の証明書を取得し、取得した証明書に基づいてアクセス許容判定処理を行うデータ処理部を有する請求項１３に記載の情報記憶装置。
【請求項１６】
データを記録するメディアと、
前記メディアに格納されたコンテンツを再生する再生装置と、
前記メディアに対するデータ記録を行うサーバを有し、
前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納する汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記サーバは、
前記汎用領域に対して、暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を記録する処理を行い、
前記暗号鍵格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの復号用の暗号鍵を記録し、
前記ステータス格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの初回再生時の日時情報を記録するためのコンテンツ対応ステータス情報記録領域を設定する処理を行い、
前記再生装置は、
コンテンツ再生処理に際して、前記コンテンツ初回再生時の日時情報に応じて決定されるコンテンツ利用許容期間である有効期限情報を前記暗号鍵格納ブロックから取得し、取得した有効期限情報と現在日時情報との比較により、コンテンツ再生の可否を判定する情報処理システム。
【請求項１７】
コンテンツ再生処理を実行する情報処理装置において実行する情報処理方法であり、
前記情報処理装置は、メディアに格納されたコンテンツを再生するデータ処理部を有し、
前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納した汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、

前記データ処理部は、
コンテンツ再生処理に際して、前記コンテンツ初回再生時の日時情報に応じて決定されるコンテンツ利用許容期間である有効期限情報を前記暗号鍵格納ブロックから取得し、取得した有効期限情報と現在日時情報との比較により、コンテンツ再生の可否を判定する情報処理方法。
【請求項１８】
メディアに対するコンテンツ記録処理を行う情報処理装置において実行する情報処理方法であり、
前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納する汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記情報処理装置は、
前記汎用領域に対して、暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を記録する処理を行い、
前記暗号鍵格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの復号用の暗号鍵を記録し、
前記ステータス格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの初回再生時の日時情報を記録するためのコンテンツ対応ステータス情報記録領域を設定する処理を行う情報処理方法。
【請求項１９】
コンテンツ再生処理を実行する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、
前記情報処理装置は、メディアに格納されたコンテンツを再生するデータ処理部を有し、
前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納した汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記プログラムは、データ処理部に、
コンテンツ再生処理に際して、前記コンテンツ初回再生時の日時情報に応じて決定されるコンテンツ利用許容期間である有効期限情報を前記暗号鍵格納ブロックから取得する処理と、取得した有効期限情報と現在日時情報との比較により、コンテンツ再生の可否を判定する処理を実行させるプログラム。
【請求項２０】
メディアに対するコンテンツ記録処理を行う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、
前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納する汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コン

テンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、

前記プログラムは、前記情報処理装置に、

前記汎用領域に対して、暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を記録する処理と、

前記暗号鍵格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの復号用の暗号鍵を記録する処理と、

前記ステータス格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの初回再生時の日時情報を記録するためのコンテンツ対応ステータス情報記録領域を設定する処理を実行させるプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本開示は、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するコンテンツの利用制御を行う情報処理装置、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ー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。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）等に記載がある。

【０００５】

コンテンツの利用制御構成として、コンテンツ暗号化の他、コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）を利用した構成がある。

例えば、ユーザにコンテンツを提供する際に、そのコンテンツの許容利用形態、例えば、コンテンツの利用期間に関する情報や、コピー処理の許可情報などを記録した利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）を併せて提供する。

ユーザの再生装置においてコンテンツを利用する場合、コンテンツに対応する利用制御情報を参照して、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に規定された範囲でコンテンツの利用を行わせるものである。

【０００６】

しかし、昨今、サーバ等からのコンテンツ取得処理が盛んになり、また、ユーザ装置に

おいて利用される記録メディアの容量が増大し、ユーザ装置が保持するコンテンツ数が急激に増大している。

【０００７】

このような多数のコンテンツを保持するユーザ装置には、

コンテンツとそのコンテンツに対応する利用制御情報のペア、

これらのデータペアが大量に保持される。

例えば利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）には、その利用制御情報に対応付けられたコンテンツの利用可能期間、すなわち有効期限情報が記録されている。

【０００８】

ユーザが、コンテンツの利用期限を延長したい場合、そのコンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）の有効期限を書き換える処理が必要となる。この書き換え処理は、ユーザ装置において勝手に実行することはできず、コンテンツ管理サーバ等によって行われる。

【０００９】

多数のコンテンツの有効期限を延長する場合、多数の利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）を１つ１つ書き換える処理が必要となり、ユーザ装置とサーバ間の通信処理や各装置における処理負荷が増大することになる。

【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】

本開示は、例えば上記問題点に鑑みてなされたものであり、利用管理対象となるコンテンツの利用許容期間の変更や更新処理を効率的に実行可能として、コンテンツ利用制御の利便性を向上させた情報処理装置、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】

本開示の第１の側面は、

メディアに格納されたコンテンツを再生するデータ処理部を有し、

前記メディアは、

暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納した汎用領域と、

前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、

前記データ処理部は、

コンテンツ再生処理に際して、前記コンテンツ初回再生時の日時情報に応じて決定されるコンテンツ利用許容期間である有効期限情報を前記暗号鍵格納ブロックから取得し、取得した有効期限情報と現在日時情報との比較により、コンテンツ再生の可否を判定する情報処理装置にある。

【００１３】

さらに、本開示の情報処理装置の一実施態様において、前記暗号鍵格納ブロックに記録された有効期限情報は、前記ステータス格納ブロックに記録されたコンテンツ初回再生時の日時情報を基準日時として設定した有効期限情報である。

【００１４】

さらに、本開示の情報処理装置の一実施態様において、前記利用制御情報は、再生対象コンテンツの復号用の暗号鍵を格納した暗号鍵格納ブロックを識別可能とした暗号鍵格納ブロック識別子と、前記再生対象コンテンツのコンテンツ対応ステータス情報を格納したステータス格納ブロックを識別可能としたステータス格納ブロック識別子を有し、前記データ処理部は、前記暗号鍵格納ブロック識別子に基づいて、前記保護領域から１つの暗号鍵格納ブロックを選択し、前記ステータス格納ブロック識別子に基づいて、前記保護領域から１つのステータス格納ブロックを選択し、各選択ブロックから前記再生対象コンテンツに対応する暗号鍵とステータス情報を取得する。

【００１５】

さらに、本開示の情報処理装置の一実施態様において、前記暗号鍵格納ブロックには、前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である複数の有効期限情報が格納され、前記データ処理部は、前記汎用領域から再生対象コンテンツの利用制御情報を取得し、前記ブロックに記録された複数の有効期限情報中、再生対象コンテンツに適用すべき有効期限情報の選択情報を、前記利用制御情報から抽出し、該選択情報に従って、前記ブロックから選択した有効期限情報がコンテンツ初回再生時の日時情報に応じた有効期限情報である場合、前記コンテンツ対応ステータス情報として記録されたコンテンツ初回再生時の日時情報を基準日時とした有効期限情報に基づくコンテンツ再生可否判定を行う。

【００１６】

さらに、本開示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、前記利用制御情報、または前記ブロックから取得した有効期限情報と現在日時情報との比較処理を行う際に、信頼できる時間情報提供サーバから取得した現在日時情報を適用した処理を行う。

【００１７】

さらに、本開示の情報処理装置の一実施態様において、前記暗号鍵格納ブロック、および前記ステータス格納ブロックは、前記メディアによるアクセス権判定に基づいてアクセスの認められるブロックであり、前記データ処理部は、前記暗号鍵格納ブロック、および前記ステータス格納ブロックからのデータ読み出し処理に際して、情報処理装置の証明書（Ｃｅｒｔｉｆｉｃａｔｅ）を前記メディアに送信し、前記メディアによるアクセス権判定処理によってデータ読み出し権利が確認されたことを条件として、データ読み出しを行う。

【００１８】

さらに、本開示の情報処理装置の一実施態様において、前記ステータス格納ブロックは、前記メディアによるアクセス権判定に基づいてアクセスの認められるブロックであり、前記データ処理部は、前記ステータス格納ブロックに対するコンテンツ初回再生日時情報の記録処理に際して、情報処理装置の証明書（Ｃｅｒｔｉｆｉｃａｔｅ）を前記メディアに送信し、前記メディアによるアクセス権判定処理によってデータ書き込み処理の権利が確認されたことを条件として、データ記録を行う。

【００１９】

さらに、本開示の情報処理装置の一実施態様において、前記暗号鍵格納ブロックは、前記メディアによるアクセス権判定に基づいてアクセスの認められるブロックであり、前記ブロックに記録された有効期限情報は、前記暗号鍵格納ブロックに対するデータ書き込み処理の権利を有するサーバによって書き込みおよび更新が行われる情報である。

【００２０】

さらに、本開示の第２の側面は、

メディアに対するコンテンツ記録処理を行う情報処理装置であり、

前記メディアは、

暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納する汎用領域と、

前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコ

ンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、

前記情報処理装置は、

前記汎用領域に対して、暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を記録する処理を行い、

前記暗号鍵格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの復号用の暗号鍵を記録し、

前記ステータス格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの初回再生時の日時情報を記録するためのコンテンツ対応ステータス情報記録領域を設定する処理を行う情報処理装置にある。

【００２１】

さらに、本開示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、前記利用制御情報に、前記暗号鍵格納ブロックの識別子と、前記ステータス格納ブロックの識別子を記録して前記メディアの汎用領域に記録する処理を行う。

【００２２】

さらに、本開示の情報処理装置の一実施態様において、前記暗号鍵を格納したブロックは、前記メディアによるアクセス権判定に基づいてアクセスの認められるブロックであり、前記情報処理装置は、前記ブロックに対するデータ記録処理に際して、情報処理装置の証明書（Ｃｅｒｔｉｆｉｃａｔｅ）を前記メディアに送信し、前記メディアによるアクセス権判定処理によってデータ記録処理の権利を有することが確認されたことを条件として、前記ブロックに対するデータ記録処理を行う。

【００２３】

さらに、本開示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、前記メディアに記録されたコンテンツを他の第２メディアに移動する処理に際して、前記ステータス情報も併せて第２メディアに移動する処理を実行する。

【００２４】

さらに、本開示の第３の側面は、

暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納した汎用領域と、

前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、

前記暗号化コンテンツの再生処理を実行する再生装置に、前記暗号鍵格納ブロックに記録された有効期限情報と、前記ステータス格納ブロックに記録されたコンテンツ対応ステータス情報の参照処理に基づいて、コンテンツ初回再生時の日時情報に応じて設定されるコンテンツ利用許容期限に基づくコンテンツ再生可否判定を行わせることを可能とした情報記憶装置にある。

【００２５】

さらに、本開示の情報記憶装置の一実施態様において、前記利用制御情報は、前記暗号鍵格納ブロックの識別子と、前記ステータス格納ブロックの識別子を記録した構成であり、前記暗号化コンテンツの再生処理を実行する再生装置に、前記利用制御情報に記録された各ブロック識別子の参照処理に基づくブロック特定処理を行わせることを可能とした。

【００２６】

さらに、本開示の情報記憶装置の一実施態様において、前記情報記憶装置は、前記保護領域のブロックに対するアクセス要求装置の証明書を取得し、取得した証明書に基づいてアクセス許容判定処理を行うデータ処理部を有する。

【００２７】
さらに、本開示の第４の側面は、
データを記録するメディアと、
前記メディアに格納されたコンテンツを再生する再生装置と、
前記メディアに対するデータ記録を行うサーバを有し、
前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納する汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記サーバは、
前記汎用領域に対して、暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を記録する処理を行い、
前記暗号鍵格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの復号用の暗号鍵を記録し、
前記ステータス格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの初回再生時の日時情報を記録するためのコンテンツ対応ステータス情報記録領域を設定する処理を行い、
前記再生装置は、
コンテンツ再生処理に際して、前記コンテンツ初回再生時の日時情報に応じて決定されるコンテンツ利用許容期間である有効期限情報を前記暗号鍵格納ブロックから取得し、取得した有効期限情報と現在日時情報との比較により、コンテンツ再生の可否を判定する情報処理システムにある。
【００２８】
さらに、本開示の第５の側面は、
コンテンツ再生処理を実行する情報処理装置において実行する情報処理方法であり、
前記情報処理装置は、メディアに格納されたコンテンツを再生するデータ処理部を有し、
前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納した汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記データ処理部は、
コンテンツ再生処理に際して、前記コンテンツ初回再生時の日時情報に応じて決定されるコンテンツ利用許容期間である有効期限情報を前記暗号鍵格納ブロックから取得し、取得した有効期限情報と現在日時情報との比較により、コンテンツ再生の可否を判定する情報処理方法にある。
【００２９】
さらに、本開示の第６の側面は、
メディアに対するコンテンツ記録処理を行う情報処理装置において実行する情報処理方法であり、
前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納する汎用領域

と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記情報処理装置は、
前記汎用領域に対して、暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を記録する処理を行い、
前記暗号鍵格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの復号用の暗号鍵を記録し、
前記ステータス格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの初回再生時の日時情報を記録するためのコンテンツ対応ステータス情報記録領域を設定する処理を行う情報処理方法にある。
【００３０】
さらに、本開示の第７の側面は、
コンテンツ再生処理を実行する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、
前記情報処理装置は、メディアに格納されたコンテンツを再生するデータ処理部を有し、
前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納した汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記プログラムは、データ処理部に、
コンテンツ再生処理に際して、前記コンテンツ初回再生時の日時情報に応じて決定されるコンテンツ利用許容期間である有効期限情報を前記暗号鍵格納ブロックから取得する処理と、取得した有効期限情報と現在日時情報との比較により、コンテンツ再生の可否を判定する処理を実行させるプログラムにある。
【００３１】
さらに、本開示の第８の側面は、
メディアに対するコンテンツ記録処理を行う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、
前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納する汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記プログラムは、前記情報処理装置に、
前記汎用領域に対して、暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を記録する処理と、
前記暗号鍵格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの復号用の暗号鍵を記録する処理と、

前記ステータス格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの初回再生時の日時情報を記録するためのコンテンツ対応ステータス情報記録領域を設定する処理を実行させるプログラムにある。

【００３２】

なお、本開示のプログラムは、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。

【００３３】

本開示のさらに他の目的、特徴や利点は、後述する本開示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】

【００３４】

本開示の一実施例の構成によれば、コンテンツ初回再生日時に応じた利用期限の設定を可能とした装置、方法が実現される。

具体的には、コンテンツと利用制御情報を格納した汎用領域と、コンテンツ復号用の暗号鍵と、コンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含む複数ブロックによって構成される保護領域を有するメディアに格納されたコンテンツを再生する。再生装置は、コンテンツ初回再生時の日時情報に応じて決定されるコンテンツ利用許容期間である有効期限情報を暗号鍵格納ブロックから取得し、取得した有効期限情報と現在日時情報との比較により、コンテンツ再生の可否を判定する。

これらの処理によって、コンテンツ初回再生日時に応じた利用期限の設定を可能とした装置、方法が実現される。

【図面の簡単な説明】

【００３５】

【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】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４】ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）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データの具体的構成例とアクセス制御処理の一例について説明する図である。

【図７】メモリカードの格納データの一例について説明する図である。

【図８】メモリカードに対するサーバのデータ記録処理の一例について説明する図である。

【図９】メモリカードの記録データに対するホストの読み取り処理の一例について説明する図である。

【図１０】コンテンツの有効期限情報の更新処理シーケンスについて説明する図である。

【図１１】ブロック対応の有効期限情報を設定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１２】ブロック対応の有効期限情報と利用制御情報の有効期限情報との共存構成について説明する図である。

【図１３】ブロック対応の有効期限情報と利用制御情報の有効期限情報との共存構成にお

いてサーバの実行する処理例について説明する図である。
【図１４】ブロック対応の有効期限情報と利用制御情報の有効期限情報との共存構成においてホストの実行する処理例について説明する図である。
【図１５】ブロック対応の有効期限情報と利用制御情報の有効期限情報との共存構成においてホストの実行するコンテンツ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１６】１つのブロックに複数のブロック対応の有効期限情報を設定する構成例について説明する図である。
【図１７】１つのブロックに複数のブロック対応の有効期限情報を設定する構成例について説明する図である。
【図１８】１つのブロックに複数のブロック対応の有効期限情報を設定する構成例において、１ブロックを複数サーバが利用する例について説明する図である。
【図１９】１つのブロックに複数のブロック対応の有効期限情報を設定する構成例において、１ブロックを複数サーバが利用する場合の記録データの例を説明する図である。
【図２０】コンテンツの初回再生日時等のステータス情報を記録し、ステータス情報に応じたコンテンツ利用期限を設定する例について説明する図である。
【図２１】コンテンツの初回再生日時等のステータス情報を記録し、ステータス情報に応じたコンテンツ利用期限を設定する例について説明する図である。
【図２２】コンテンツの初回再生日時等のステータス情報を記録し、ステータス情報に応じたコンテンツ利用期限を設定する例について説明する図である。
【図２３】コンテンツの初回再生日時等のステータス情報を記録し、ステータス情報に応じたコンテンツ利用期限を設定する例におけるサーバの処理について説明する図である。
【図２４】コンテンツの初回再生日時等のステータス情報を記録し、ステータス情報に応じたコンテンツ利用期限を設定する例におけるホストの処理について説明する図である。
【図２５】コンテンツの初回再生日時等のステータス情報を記録し、ステータス情報に応じたコンテンツ利用期限を設定する例におけるホストの処理について説明するフローチャートを示す図である。
【図２６】コンテンツの初回再生日時等のステータス情報を記録し、ステータス情報に応じたコンテンツ利用期限を設定する例におけるホストの処理について説明するフローチャートを示す図である。
【図２７】コンテンツのメディア間の移動（ムーブ）処理について説明する図である。
【図２８】コンテンツのメディア間の移動（ムーブ）処理について説明する図である。
【図２９】ホスト（再生装置）のハードウェア構成例について説明する図である。
【図３０】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】
【００３６】
以下、図面を参照しながら本開示の情報処理装置、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．メモリカードの構成例と利用例について
３．保護領域に対するアクセス許容情報を持つ証明書について
４．各装置の証明書を適用したメモリカードに対するアクセス処理例について
５．ブロック単位で有効期限情報を設定する処理例について
６．ブロック単位の有効期限情報と利用制御情報の有効期限情報の共存利用処理例について
７．複数の有効期限情報をブロックに設定してコンテンツに応じて選択適用する処理例について
８．コンテンツの初回利用情報を記録する処理例について
９．コンテンツのメディア間移動（ムーブ）処理について
１０．各装置のハードウェア構成例について

１１．本開示の構成のまとめ
【００３７】
［１．コンテンツ提供処理および利用処理の概要について］
以下、図面を参照しながら本開示の情報処理装置、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。
【００３８】
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）コンテンツ記録再生装置（ホスト）
（ｃ）コンテンツ記録メディア
これらの例を示している。
【００３９】
（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憶装置であるメモリカード３１を示している。
【００４０】
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には例えば著作権の管理対象となるコンテンツ等、利用制御対象となるコンテンツが含まれる。
【００４１】
利用制御対象となるコンテンツとは、例えば無秩序なコピーやコピーデータ配布等が禁止されたコンテンツや、利用期間が制限されたコンテンツ等である。なお、メモリカード３１に対して、利用制御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）が合わせて記録される。
利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）には、例えば許容されるコンテンツ利用期間や許容されるコピー回数などのコンテンツ利用に関する情報が記録される。
コンテンツ提供元は、コンテンツに併せてコンテンツ対応の利用制御情報を提供する。
【００４２】
（ａ）コンテンツ提供元は、音楽や映画等のコンテンツの提供元である。図１には、一例として、放送局１１と、コンテンツサーバ１２をコンテンツ提供元として示している。
放送局１１は、例えばテレビ局であり、様々な放送コンテンツを地上波や衛星を介した衛星波に載せてユーザ装置［（ｂ）コンテンツ記録再生装置（ホスト）］に提供する。
コンテンツサーバ１２は、音楽や映画等のコンテンツをインターネット等のネットワークを介して提供するサーバである。
【００４３】
ユーザは、例えば（ｃ）コンテンツ記録メディアであるメモリカード３１を（ｂ）コンテンツ記録再生装置（ホスト）に装着し、（ｂ）コンテンツ記録再生装置（ホスト）自体の受信部、あるいは、コンテンツ記録再生装置（ホスト）に接続された受信装置を介して、放送局１１やコンテンツサーバ１２の提供するコンテンツを受信してメモリカード３１に記録することができる。
【００４４】
（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放送局１１やコンテンツサーバ１２から受信したコンテンツをメモリカード３１に記録する。
【００４５】
（ｂ）コンテンツ記録再生装置（ホスト）としては、例えばＤＶＤプレーヤなど、ハードディスクやＤＶＤ，ＢＤ等のディスクを備えた記録再生専用器（ＣＥ機器：Ｃｏｎｓｕｍｅｒ　Ｅｌｅｃｔｒｏｎｉｃｓ機器）２１がある。さらに。ＰＣ２２や、スマートフォ

ン、携帯電話、携帯プレーヤ、タブレット端末などの携帯端末２３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。

【００４６】

ユーザは、記録再生専用器２１、ＰＣ２２、携帯端末２３などを利用して、放送局１１やコンテンツサーバ１２から音楽や映画等のコンテンツを受信し、メモリカード３１に記録する。

【００４７】

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。

情報記憶装置であるメモリカード３１は、例えばＰＣ等のコンテンツ再生器に対して着脱可能な記録メディアであり、コンテンツ記録を実行した機器から自由に取り外して、その他のユーザ機器に装着することが可能である。

【００４８】

すなわち、図２に示すように、

（１）記録処理

（２）再生処理

これらの処理を実行する。

なお、記録または再生の一方のみを実行する機器もある。

また、記録と再生各処理の実行機器は同一であることは必須ではなく、ユーザは自由に記録機器と再生機器を選択して利用することができる。

【００４９】

なお、多くの場合、メモリカード３１に記録された利用制御コンテンツは暗号化コンテンツとして記録されており、記録再生専用器２１やＰＣ２２、携帯端末２３等のコンテンツ再生装置は、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。

また、コンテンツに対応して設定される利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録された利用許容態様で再生処理などを行う。

（ｂ）コンテンツ記録再生装置（ホスト）には、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に従ったコンテンツ利用やコンテンツの復号処理を実行するためのプログラム（ホストアプリケーション）が格納されており、コンテンツ再生はこのプログラム（ホストアプリケーション）に従って実行する。

【００５０】

［２．メモリカードの構成例と利用例について］

次に、コンテンツの記録メディアとして利用されるフラッシュメモリ等のメモリカードの構成例と利用例について説明する。

メモリカード３１の記憶領域の具体的構成例を図３に示す。

メモリカード３１の記憶領域は、図３に示すように、

（ａ）保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１、

（ｂ）汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）５２、

これら２つの領域によって構成される。

【００５１】

（ｂ）汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）５２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、コンテンツやコンテンツ対応の利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）、その他の一般のコンテンツ管理データ等が記録される。

この汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）５２は、例えばサーバやユーザの記録再生装置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。

【００５２】

一方、（ａ）保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１は、自由なアクセスが許

容されない領域である。
保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１は複数の区分領域としてのブロック（＃０，＃１，＃２・・・）に分割され、各ブロック単位でアクセス権が設定される。
【００５３】
例えば、ユーザの利用する記録再生装置、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３１のデータ処理部が、メモリカード３１に予め格納されたプログラムに従って、各装置に応じてブロック単位で読み取り（Ｒｅａｄ）または書き込み（Ｗｒｉｔｅ）の可否を決定する。
【００５４】
メモリカード３１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３１は、まず、メモリカード３１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。
【００５５】
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を受信する。
たとえばアクセス要求装置がサーバである場合は、サーバの保有するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）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）５１の各ブロック（区分領域）単位でアクセスが許容されるか否かを判定する。
【００５６】
また、アクセス要求装置がホスト装置、例えばコンテンツ記録再生を実行するユーザ機器としての記録再生装置（ホスト）である場合は、記録再生装置（ホスト）の保有するホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）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）５１の各ブロック（区分領域）のアクセスが許容されるか否かを判定する。
【００５７】
このアクセス権判定処理は、図３に示す保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１内のブロック（図に示す領域＃０，＃１，＃２・・・）単位で行われる。メモリカード３１は、ブロック単位で許可された処理（データの読み取り／書き込み等の処理）のみをサーバやホストに実行させる。
【００５８】
メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）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　Ｃｅｒｔｉｆｉｃａｔｅ）や、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）に記録される。
なお、以下において「Ｃｅｒｔｉｆｉｃａｔｅ」は、簡略化して「Ｃｅｒｔ」として記載する。
【００５９】
このように、メモリカード３１は、メモリカード３１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。
【００６０】
［３．保護領域に対するアクセス許容情報を持つ証明書について］
次に、サーバやユーザ装置であるホスト機器（＝記録再生装置）が、上述したメモリカード３１の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１に対するアクセスを行う場合に、メモリカードに提示が必要となる証明書の構成例について図４、図５を参照して説明する。

【００６１】
上述したように、メモリカード３１は、メモリカード３１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。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）やホスト証明書（Ｈｏｓｔ　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）５１の各区分領域のアクセスを許容するか否かを判定する。
【００６２】
この認証処理に利用される装置証明書の一例として、図１に示す記録再生専用器２１、ＰＣ２２、携帯端末２３等のユーザ機器（ホスト機器）に格納されるホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）の構成例について図４を参照して説明する。
【００６３】
ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）は、例えば、公開鍵証明書発行主体である認証局によって各ユーザ機器（ホスト機器）に提供される。例えば、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）は、認証局がコンテンツ利用処理を認めたユーザ機器（ホスト機器）に対して発行するユーザ機器の証明書であり、公開鍵等を格納した証明書である。ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）は、認証局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。
【００６４】
なお、装置証明書は、例えば、装置製造時に装置の種類などの装置確認に基づいて予め装置内のメモリに格納することが可能である。ユーザの購入後、取得する場合は、装置と認証局あるいはその他の管理局との所定のシーケンスに従った装置種類や利用可能なコンテンツの種類等の確認処理を行って、各装置に対して発行し装置内のメモリに格納する構成としてもよい。
【００６５】
なお、メモリカード３１の保護領域に対するアクセスを行うサーバは、ホスト証明書と同様の構成を持つサーバ公開鍵とメモリカードのアクセス許容情報が記録されたサーバ証明書（Ｓｅｖｅｒ　Ｃｅｒｔ）を保持する。
【００６６】
図４に認証局が各ホスト機器（ユーザ機器）に提供するホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）の具体例を示す。
ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）には、図４に示すように、以下のデータが含まれる。
（１）タイプ情報
（２）ホストＩＤ（ユーザ機器ＩＤ）
（３）ホスト公開鍵（Ｈｏｓｔ　Ｐｕｂｌｉｃ　Ｋｅｙ）
（４）保護領域アクセス権情報（メディアの保護領域に対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤ　Ｗｒｉｔｅ））
（５）その他の情報
（６）署名（Ｓｉｇｎａｔｕｒｅ）
【００６７】
以下、上記（１）～（６）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、証明書のタイプやユーザ機器のタイプを示す情報であり、例えば本証明書がホスト証明書であることを示すデータや、機器の種類、例えばＰＣであるとか、音楽再生プレーヤであるといった機器の種類などを示す情報が記録される。
【００６８】
（２）ホストＩＤ
ホストＩＤは機器識別情報としての機器ＩＤを記録する領域である。
（３）ホスト公開鍵（Ｈｏｓｔ　Ｐｕｂｌｉｃ　Ｋｅｙ）

ホスト公開鍵（Ｈｏｓｔ　Ｐｕｂｌｉｃ　Ｋｅｙ）はホスト機器の公開鍵である。ホスト機器（ユーザ機器）に提供される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。

【００６９】

（４）保護領域アクセス権情報（メディアの保護領域に対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤ　Ｗｒｉｔｅ））

保護領域アクセス権情報は、コンテンツを記録するメディア、例えば図３に示すメモリカード３１の記憶領域中に設定される保護領域（ＰＤＡ：Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１内のデータ読み取り（Ｒｅａｄ）や、書き込み（Ｗｒｉｔｅ）が許容されたブロック（区分領域）単位の情報が記録される。

アクセス権は、保護領域内のブロック（区分領域）単位のアクセス権として記録される。

【００７０】

（５）その他の情報、（６）署名（Ｓｉｇｎａｔｕｒｅ）

ホスト証明書には、上記（１）～（４）の他、様々な情報が記録され、（１）～（５）の情報に対する署名データが記録される。

署名は、認証局の秘密鍵によって実行される。ホスト証明書に記録された情報、例えばホスト公開鍵を取り出して利用する場合には、まず認証局の公開鍵を適用した署名検証処理を実行して、ホスト証明書の改ざんがないことを確認し、その確認がなされたことを条件として、ホスト公開鍵等の証明書格納データの利用が行われることになる。

【００７１】

図４は、メモリカードの保護領域に対するユーザ機器（ホスト機器）のアクセス許容情報を記録したホスト証明書であるが、例えばメモリカードにコンテンツを提供するコンテンツ提供サーバなど、保護領域に対するアクセスが必要となるサーバに対しては、図４に示すホスト証明書と同様、メモリカードの保護領域に対するアクセス許容情報を記録した証明書［サーバ証明書（例えばサーバ公開鍵を格納した公開鍵証明書）］が提供される。

【００７２】

サーバに提供されるサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）の構成例について図５を参照して説明する。なお、以下ではサーバは、図１に示すコンテンツ提供元のすべて、すなわち放送局１１やコンテンツサーバ１２等、ユーザ装置に対してコンテンツを提供する装置を含むものとして説明する。

【００７３】

サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）は、例えば、公開鍵証明書発行主体である認証局によって例えば、コンテンツ提供を行うコンテンツサーバ等の装置に提供される。例えば、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）は、認証局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　Ｃｅｒｔ）は、認証局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。

【００７４】

図５に認証局が各コンテンツサーバに提供するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）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、図４を参照して説明したホスト証明書と同様、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）メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）

（５）その他の情報

（６）署名（Ｓｉｇｎａｕｒｅ）

【００７５】
これらの各情報は、図４を参照して説明した情報と同様の情報であり、詳細な説明は省略する。
なお、「（４）メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）」
は、各サーバ単位で、メモリカード３１の保護領域５１のブロック（区分領域）単位のアクセス権（データ読み取り（Ｒｅａｄ）／書き込み（Ｗｒｉｔｅ）許容情報）が記録される。
【００７６】
なお、サーバ証明書に記録された情報、例えばサーバ公開鍵を取り出して利用する場合には、まず認証局の公開鍵を適用した署名検証処理を実行して、サーバ証明書の改ざんがないことを確認し、その確認がなされたことを条件として、サーバ公開鍵等の証明書格納データの利用が行われることになる。
【００７７】
［４．各装置の証明書を適用したメモリカードに対するアクセス処理例について］
図４、図５を参照して説明したように、サーバやホスト機器（記録再生器等のユーザ機器）がメモリカード３１の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１のブロックに対してアクセスを行う場合には、図４や図５に示すような証明書をメモリカードに提示することが必要となる。
メモリカードは、図４や図５に示す証明書を確認して、図３に示すメモリカード３１の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）５１の各ブロック単位のアクセス可否を判定する。
【００７８】
ホスト機器は、例えば図４を参照して説明したホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）を保持し、コンテンツの提供等を行うサーバは、図５を参照して説明したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）を保持している。
【００７９】
これらの各装置が、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するアクセスを行う場合には、各装置が保有している証明書をメモリカードに提供してメモリカード側の検証に基づくアクセス可否の判定を受けることが必要となる。
【００８０】
図６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。
【００８１】
図６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Ａ６１、サーバＢ６２、ホスト機器６３、メモリカード７０を示している。
サーバＡ６１、サーバＢ６２は、例えば、メモリカード７０に対する記録コンテンツである暗号化コンテンツ（Ｃｏｎ１，Ｃｏｎ２，Ｃｏｎ３・・・）を提供する。
これらのサーバは、さらに、暗号化コンテンツの復号用に鍵であるタイトルキー（Ｋｔ１，Ｋｔ２・・・）、コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ：ＵＲ１，ＵＲ２・・・）を提供する。
【００８２】
ホスト機器６３は、メモリカード７０に格納されたコンテンツの再生処理を行う装置である。
ホスト機器６３は、メモリカード７０の汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０に記録された暗号化コンテンツ（Ｃｏｎ１，Ｃｏｎ２，Ｃｏｎ３・・・）と利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ：ＵＲ１，ＵＲ２・・・）を読み取る。さらに、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０のブロック（区分領域）８１，８２からコンテンツ復号処理に適用するタイトルキー（Ｋｔ１，Ｋｔ２・・・）を読み取って、タイトルキーによる復号処理を実行して利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に従ったコ

ンテンツ利用を行う。

【００８３】

メモリカード７０は、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０と、汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０を有し、暗号化コンテンツ、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）等は汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０に記録される。

コンテンツ再生に際して必要とする鍵であるタイトルキーは保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０に記録される。

【００８４】

先に図３を参照して説明したように、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０は、複数のブロック（区分領域）に区分されている。

図６に示す例では、

ブロック＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）８１、

ブロック＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）８２、

これらの２つのブロックのみを示している。

保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０には、この他にも多数のブロックが設定される。

【００８５】

ブロックの設定態様としては様々な設定が可能である。

図６に示す例では、

ブロック＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）８１は、サーバＡ６１専用のブロック、すなわち、サーバＡ６１の提供コンテンツの復号用のタイトルキーを格納する領域としている。

ブロック＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）８２は、サーバＢ６２専用のブロック、すなわち、サーバＢ６２の提供コンテンツの復号用のタイトルキーを格納する領域としている。

【００８６】

このような設定において、例えばコンテンツの提供サーバＡ６１は、提供コンテンツの復号に必要となるタイトルキーを、ブロック＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）８１に記録する。

この場合、サーバＡ６１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、ブロック＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）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）の許容されたブロックに対しては、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。

【００８７】

またサーバＢ６２は、提供コンテンツの復号に必要となるタイトルキーを、ブロック＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）８２に記録する。

この場合、サーバＢ６２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、ブロック＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）８２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。

【００８８】

また、ブロック＃０，＃１に記録されたタイトル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６３の保持するホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）は、ブロック＃０，＃１に対する読み取り（Ｒｅａｄ）許可が設定された証明書として構成される。

【００８９】

この例では、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）には、ブロック＃０

，＃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タイトル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。
また、その他の処理において、ホスト機器６３が保護領域に対するデータ書き込みが必要となる場合は、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）に書き込み（Ｗｒｉｔｅ）許可を設定してもよい。

【００９０】
メモリカード７０のデータ処理部は、コンテンツを提供するサーバや、コンテンツを利用するホストなどのアクセス要求装置から保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０に対するアクセス要求を受信すると、各装置の装置証明書を参照して、各ブロック単位のアクセス許容情報を確認して各ブロックに対するアクセスを許可するか否かを判定する。

【００９１】
メモリカード７０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ブロック（＃０，＃１，＃２・・・）を選別する。

【００９２】
アクセス制御情報は、図４、図５を参照して説明したように、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、証明書の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。

【００９３】
図６に示すサーバＡ６１とサーバＢ６２がメモリカード７０に対して書き込むデータの例を図７に示す。
各サーバはユーザ装置としてのホスト機器に装着されたメモリカード７０に対してコンテンツ他のデータを記録する。
サーバＡの提供コンテンツを、Ｃｏｎ（ａ１）、Ｃｏｎ（ａ２），Ｃｏｎ（ａ３）とする。
サーバＢの提供コンテンツを、Ｃｏｎ（ｂ１）、Ｃｏｎ（ｂ２）とする。

【００９４】
図７に示すように、
サーバＡは、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に、以下のデータを記録する。
コンテンツ：Ｃｏｎ（ａ１）、Ｃｏｎ（ａ２），Ｃｏｎ（ａ３）
上記コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）：ＵＲ（ａ１），ＵＲ（ａ２），ＵＲ（ａ３）
さらに、サーバＡは、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロック＃０に以下のデータを記録する。
上記コンテンツの復号に適用するタイトルキー：Ｋｔ（ａ１），Ｋｔ（ａ２），Ｋｔ（ａ３）、あるいはタイトルキーの変換データを記録する。

【００９５】
メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に記録するタイトルキーの変換データとは、具体的には、各タイトルキーと対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）のハッシュ値との排他的論理和（ＸＯＲ）演算結果である。
図に示す、Ｋｔ（ａ１）－ＵＲ（ａ１）ｈａｓｈ，Ｋｔ（ａ２）－ＵＲ（ａ２）ｈａｓｈ，Ｋｔ（ａ３）－ＵＲ（ａ３）ｈａｓｈ、

これらのデータである。

【００９６】

サーバＢは、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に、以下のデータを記録する。

コンテンツ：Ｃｏｎ（ｂ１）、Ｃｏｎ（ｂ２）

上記コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）：ＵＲ（ｂ１），ＵＲ（ｂ２）

さらに、サーバＢは、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロック＃１に以下のデータを記録する。

タイトルキーと対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）のハッシュ値との排他的論理和（ＸＯＲ）演算結果：Ｋｔ（ｂ１）－ＵＲ（ｂ１）ｈａｓｈ，Ｋｔ（ｂ２）－ＵＲ（ｂ２）ｈａｓｈ、

これらのデータを記録する。

【００９７】

各サーバが、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロック内にデータを記録する場合には、メモリカードは、前述したサーバ証明書の記録に基づくアクセス権確認を実行し、プロックに対する書き込み権の確認を行い、アクセス権が確認された場合にのみ、データ書き込みが実行される。

【００９８】

なお、ユーザ装置であるホスト機器においてコンテンツを利用する場合は、以下のシーケンスで処理が実行される。

まず、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）から利用対象コンテンツ：Ｃｏｎ（ｘｙ）と、対応する利用制御情報：ＵＲ（ｘｙ）を取得する。

さらに、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）から、対応するタイトルキーハッシュ値：Ｋｔ（ｘｙ）－ＵＲ（ｘｙ）ｈａｓｈを取得する。

【００９９】

次に、利用制御情報：ＵＲ（ｘｙ）のハッシュ値：ＵＲ（ｘｙ）ｈａｓｈを算出する。

次に、算出ハッシュ値ＵＲ（ｘｙ）ｈａｓｈと、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）から、読み取ったタイトルキーハッシュ値：Ｋｔ（ｘｙ）－ＵＲ（ｘｙ）ｈａｓｈとの排他的論理和演算（ＸＯＲ）を実行して、タイトルキー：Ｋｔ（ｘｙ）を取得する。

最後にタイトルキー：Ｋｔ（ｘｙ）を利用して暗号化コンテンツ：Ｃｏｎ（ｘｙ）の復号処理を実行してコンテンツの再生、利用を行う。

【０１００】

このようなシーケンスでコンテンツの再生等、コンテンツ利用が行われる。

なお、この処理に際しても、ホスト機器が保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロックからタイトルキーハッシュ値：Ｋｔ（ｘｙ）－ＵＲ（ｘｙ）ｈａｓｈを取得する際には、メモリカードによるホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）に基づくブロックに対するアクセス権（この場合は読み取り権）の確認が実行される。アクセス権の確認がなされた場合にのみタイトルキーハッシュ値：Ｋｔ（ｘｙ）－ＵＲ（ｘｙ）ｈａｓｈの読み取りが行われる。

【０１０１】

［５．ブロック単位で有効期限情報を設定する処理例について］

次に、ユーザに提供したコンテンツの利用許容期間であるコンテンツの有効期限情報をコンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ではなく、タイトルキーを格納したブロックに設定する処理例について説明する。

【０１０２】

従来、ユーザに提供したコンテンツに対して、利用許容期間を設定する場合、各コンテンツに対応して発行する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に利用許容期間を記録していた。

コンテンツ再生を実行するユーザ機器（ホスト機器）は、コンテンツ再生処理を行う前に利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）の記録を確認し、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に利用許容期間が記録されている場合には、現在日時が許容期間に該当するか否かを判定して該当する場合にのみ、コンテンツの利用を行うといった処理を行っていた。

【０１０３】

なお、ユーザ機器（ホスト機器）は、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）を参照してコンテンツの利用可否を判定する処理を含むコンテンツ再生プログラム（ホストアプリケーション）を保持しており、この再生プログラムに従ってコンテンツ再生が実行される。

【０１０４】

しかし、各コンテンツに対応して発行する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に利用許容期間を記録する設定では、以下のような問題が発生する。

先に説明したように、ユーザのコンテンツ記録メディアであるメモリカードに大量のコンテンツが記録され、その１つ１つに対応する利用制御情報に各コンテンツの利用許容期間を設定すると、利用期間の延長や更新などを行う場合に、多数の利用制御情報の記録情報の書き換えを行わなくてはならない。

この書き換え処理はサーバが行う必要があり、この処理のために、サーバ、ホスト、メモリカード間の通信が必要となり、各装置の処理負荷も大きなものとなってしまう。

【０１０５】

このような処理負荷を軽減するための一構成として、タイトルキーを格納した保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロック単位で有効期限情報を設定する処理例について、図８以下を参照して説明する。

【０１０６】

図８は、サーバＡ６１がメモリカード７０に、コンテンツを提供して記録する処理例を示している。このコンテンツ提供処理に際して、提供コンテンツの利用許容期間である有効期限情報を設定し、これを提供コンテンツのタイトルキーを格納した保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロックに記録する。

【０１０７】

すなわち、サーバＡ６１の提供コンテンツの復号に適用するタイトルキーを格納する保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０のブロック＃０，８１に、タイトルキーに併せて、有効期限情報を記録する。

図８に示す例では、サーバＡは、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０に、以下のコンテンツと利用制御情報を記録する。

コンテンツ：Ｃｏｎ（ａ１）、Ｃｏｎ（ａ２），Ｃｏｎ（ａ３）、

上記コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）：ＵＲ（ａ１），ＵＲ（ａ２），ＵＲ（ａ３）、

これらのコンテンツ利用制御情報のセットを記録する。

【０１０８】

さらに、サーバＡは、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０のブロック＃０，８１に以下のデータを記録する。

タイトルキーと対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）のハッシュ値との排他的論理和（ＸＯＲ）演算結果：Ｋｔ（ａ１）－ＵＲ（ａ１）ｈａｓｈ，Ｋｔ（ａ２）－ＵＲ（ａ２）ｈａｓｈ，Ｋｔ（ａ３）－ＵＲ（ａ３）ｈａｓｈ、

サーバＡの提供コンテンツ（Ｃｏｎ（ａ１）、Ｃｏｎ（ａ２），Ｃｏｎ（ａ３））の利用許容期間である有効期限情報、例えば、

２０１１／０９／１２～２０１１／１０／３１

この複数コンテンツに対して設定される有効期限情報をタイトルキーに対応付けて記録する。

【０１０９】

すなわち、サーバＡの提供コンテンツに対応する一括した有効期限を設定し、この有効期限情報をサーバＡの提供コンテンツに対応するタイトルキーを格納したブロックにタイトルキーに対応付けて記録する。

【０１１０】

このように、複数のタイトルキーを格納したブロック単位の有効期限情報の設定処理を実行することで、例えば以下のようなメリットが発生する。

例えばサーバＡの提供コンテンツの有効期限の更新を行う場合、サーバＡは、ブロックに記録した有効期限情報の書き換えを行うのみでよい。すなわち、提供コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）を１つ１つ書き換える処理を行う必要がなく、サーバとホストとメモリカード間の通信処理や処理負荷を軽減することが可能となる。

【０１１１】

なお、図８には、サーバＡ６１の処理例を示しているが、例えばサーバＢ６２は、サーバＢの提供コンテンツに対応するタイトルキーの格納領域である保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロック＃１にサーバＢの提供コンテンツに対応する一括した有効期限を記録することができる。

【０１１２】

なお、このブロック単位の有効期限情報の設定構成は、例えばサーバＡの提供コンテンツの利用許容期間を所定期間、例えば１か月単位で、逐次更新するコンテンツ利用形態を行う場合などに特に利便性が高い。

例えば、ユーザは月単位の会費を支払うことでサーバＡの提供コンテンツを月単位で自由に利用できるといった設定である。

なお、このようなコンテンツ利用サービスは、例えばサブスクリプション（Ｓｕｂｓｃｒｉｐｔｉｏｎ）サービスと呼ばれる。

【０１１３】

このサブスクリプション（Ｓｕｂｓｃｒｉｐｔｉｏｎ）サービスを提供するサーバは、各更新月にブロックに記録された有効期限情報を書き換えれば、そのブロックに記録されたタイトルキーに対応するコンテンツの利用許容期間を一括して更新することができる。

【０１１４】

なお、図８には、サーバＡの提供コンテンツに対する一括した有効期限を１つのブロックに１つのみ記録した設定例を示しているが、例えばサーバＡの書き込み許容ブロックを複数、設定して、各ブロックに異なる有効期限を設定する構成も可能である。

例えば、サーバＡの提供コンテンツを複数に区分して、各区分単位で利用ブロックを変更して、各ブロック単位で異なる有効期限を設定する構成としてもよい。

【０１１５】

このように、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロック単位の有効期限設定を行った場合のコンテンツの利用処理について、図９を参照して説明する。

【０１１６】

図９には、コンテンツを利用するユーザ装置であるホスト機器６３とコンテンツ等を格納したメモリカード７０を示している。

ホスト機器６３は、コンテンツの利用に際して以下の処理を実行する。

まず、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）から利用対象コンテンツ：Ｃｏｎ（ｘｙ）と、対応する利用制御情報：ＵＲ（ｘｙ）を取得する。

【０１１７】

次に、利用制御情報：ＵＲ（ｘｙ）を参照して、利用対象コンテンツ：Ｃｏｎ（ｘｙ）のタイトルキーの格納されたブロックがいずれのブロックであるかを確認する。

利用制御情報：ＵＲ（ｘｙ）には、利用対象コンテンツ：Ｃｏｎ（ｘｙ）のタイトルキーの格納されたブロックの識別子が記録されている。

【０１１８】

ブロックが特定されると、そのブロックの記録データの読み出し処理を行う。
まず、ブロック内データとして記録された有効期限情報を読み出す。この有効期限と現在日時とを比較して、現在日時が有効期限内であれば、そのブロックに記録されたタイトルキーハッシュ値：Ｋｔ（ｘｙ）－ＵＲ（ｘｙ）ｈａｓｈを取得する。
現在日時が有効期限内でない場合は、その時点で処理は中止される。すなわちコンテンツの復号、利用処理は実行されない。
【０１１９】
現在日時が有効期限内である場合に限り、ブロックに記録されたタイトルキーハッシュ値：Ｋｔ（ｘｙ）－ＵＲ（ｘｙ）ｈａｓｈを取得する。
次に、利用制御情報：ＵＲ（ｘｙ）のハッシュ値：ＵＲ（ｘｙ）ｈａｓｈを算出し、算出ハッシュ値ＵＲ（ｘｙ）ｈａｓｈと、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）から読み取ったタイトルキーハッシュ値：Ｋｔ（ｘｙ）－ＵＲ（ｘｙ）ｈａｓｈとの排他的論理和演算（ＸＯＲ）を実行して、タイトルキー：Ｋｔ（ｘｙ）を取得する。
最後にタイトルキー：Ｋｔ（ｘｙ）を利用して暗号化コンテンツ：Ｃｏｎ（ｘｙ）の復号処理を実行してコンテンツの再生、利用を行う。
【０１２０】
なお、ブロック内データとして記録された有効期限情報と現在日時情報との比較処理に際して利用する現在日時情報は、信頼できる時間情報提供サーバの提供する時間情報を利用する設定とすることが好ましい。
【０１２１】
また、ホスト機器６３がメモリカード７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０のブロックからタイトルキーハッシュ値：Ｋｔ（ｘｙ）－ＵＲ（ｘｙ）ｈａｓｈを取得する際には、メモリカード７０によるホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）に基づくブロックに対するアクセス権（この場合は読み取り権）の確認が実行される。アクセス権の確認がなされた場合にのみタイトルキーハッシュ値：Ｋｔ（ｘｙ）－ＵＲ（ｘｙ）ｈａｓｈの読み取りが行われる。
【０１２２】
次に、図１０を参照して、タイトルキーを格納したブロック単位で設定された有効期限の更新処理シーケンスについて説明する。
図１０には、コンテンツを提供、管理するコンテンツサーバと、タイトルキーを格納したブロック単位で有効期限のセッテイされたコンテンツを格納したメモリカードとの間で実行される有効期限の更新処理シーケンスを示している。
なお、メモリカードは例えばコンテンツ記録再生を実行するユーザ装置に装着され、ユーザ装置を介してサーバとメモリカード間の通信が実行される。
【０１２３】
まず、ステップＳ１０１において、コンテンツサーバとメモリカード間の認証処理を実行する。
例えば双方の有する公開鍵証明書（Ｃｅｒｔ）の交換処理などを伴う認証処理が実行される。
なお、この処理に際して、サーバは、先に図５を参照して説明したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）をメモリカードに提供する。
【０１２４】
認証処理が成立しなかった場合は、処理は中止される。すなわち有効期限の更新処理は実行されない。
認証処理が成立し、双方の機器が信頼できると判断されると、メモリカードは、ステップＳ１０２において、サーバ証明書に基づいて保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロック単位のアクセス権を確認する。サーバからの更新要求のあったブロックについてのアクセス権（書き込み（Ｗｒｉｔｅ））が確認された場合のみ、次の処理に移行する。
【０１２５】

ブロックアクセス権が確認されると、ステップＳ１０３において、サーバは、サーバ提供コンテンツのタイトルキーと、ブロック単位の有効期限情報の記録されたブロックの記録データを読み出す。

【０１２６】

ステップＳ１０４において、読み出したブロックデータ内の有効期限情報を更新する。例えば、

更新前有効期限情報：２０１１／０９／０１～２０１１／０９／３０を、

更新語有効期限情報：２０１１／１０／０１～２０１１／１０／３１

とする有効期限情報の書き換え処理を行う。

【０１２７】

最後に、ステップＳ１０５において、更新した有効期限情報を含むブロック記録データをメモリカードの同じブロックに書き込む（上書き）処理を実行する。

【０１２８】

次に、図１１に示すフローチャートを参照してコンテンツ利用を行うユーザ機器（ホスト機器）におけるコンテンツ再生処理シーケンスについて説明する。

図１１に示すフローに従った処理はユーザ機器に格納されたコンテンツ再生プログラム（ホストアプリケーション）に従ってユーザ機器のデータ処理部（ＣＰＵ等）において実行される。

【０１２９】

まず、ステップＳ１５１において、ユーザからの再生コンテンツ指定情報の入力を検出する。例えば再生装置の表示部に表示されたメニューとしてのコンテンツリストに対するユーザの入力であるコンテンツ指定情報の入力を検出する。

【０１３０】

次に、ステップＳ１５２において、再生指定コンテンツと利用制御情報をユーザ機器に装着されたメモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）から読み取る。すなわち、

利用対象コンテンツ：Ｃｏｎ（ｘｙ）と、

対応する利用制御情報：ＵＲ（ｘｙ）、

を取得する。

【０１３１】

次に、ステップＳ１５３において、読み取った利用制御情報：ＵＲ（ｘｙ）を参照して、利用対象コンテンツ：Ｃｏｎ（ｘｙ）のタイトルキーの格納されたブロックがいずれのブロックであるかを確認する。

【０１３２】

ブロックが特定されると、ステップＳ１５４において、そのブロックの記録データの読み出し処理を行い、ブロック内データとして記録された有効期限情報を確認する。

この有効期限と現在日時とを比較して、現在日時が有効期限内であるか否かを判定する。

【０１３３】

ステップＳ１５５において、現在日時が有効期限内でないと判定した場合は、ステップＳ１５７に進み、処理は中止される。すなわちコンテンツの復号、利用処理は実行されない。

【０１３４】

一方、ステップＳ１５５において、現在日時が有効期限内であると判定した場合は、ステップＳ１５６に進む。

ステップＳ１５６では、そのブロックに記録されたタイトルキーを取得して、タイトルキーを利用したコンテンツの復号処理を行い、コンテンツの再生、利用を行う。

【０１３５】

なお、ブロック内の格納タイトルキーは利用制御情報（ＵＲ：Ｕｓａｇｅ　Ｒｕｌｅ）とのハッシュ値との排他論理和（ＸＯＲ）演算結果として格納されており、前述したＵＲ

ハッシュの算出、ＵＲハッシュとのＸＯＲ演算処理などによるタイトルキーの取得を行う。

【０１３６】

このように、現在日時がブロックに記録された有効期限内でない場合は、その時点で処理は中止される。なお、前述したように、ブロック内データとして記録された有効期限情報と現在日時情報との比較処理に際して利用する現在日時情報は、信頼できる時間情報提供サーバの提供する時間情報を利用する設定とすることが好まししい。

【０１３７】

このように、本実施例では、複数のコンテンツに対応するタイトルキーを格納したブロック単位でコンテンツの有効期限情報を設定する構成としたので、複数コンテンツに対する有効期限の設定や更新処理に伴う通信処理やデータ処理の負荷を軽減することが可能となる。

【０１３８】

［６．ブロック単位の有効期限情報と利用制御情報の有効期限情報の共存利用処理例について］

次に、ブロック単位の有効期限情報と利用制御情報の有効期限情報の共存利用処理例について説明する。

先に説明した実施例では、サーバがユーザに提供する複数コンテンツの全体に対して１つのブロック対応有効期限を設定する例として説明した。

しかし、中には、１つのコンテンツに対応する独立した有効期限を設定したい場合もある。

【０１３９】

このような１つのコンテンツに対応する単独の有効期限は、従来と同様、例えばそのコンテンツに対する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録すればよい。

しかし、このような設定とすると、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）と、ブロックに記録された有効期限の２つの有効期限が混在することになり、どちらの有効期限を参照すべきかが不明確になる。

以下では、このような問題を解決した構成、すなわち、ブロック単位の有効期限情報と利用制御情報の有効期限情報を共存させて、各コンテンツについて、いずれか一方の有効期限情報を選択適用することを可能とした構成例について説明する。

【０１４０】

図１２を参照して本処理例の概要について説明する。

例えばサーバの提供するコンテンツはメモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に記録される。

また、このコンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）もサーバからメモリカードに提供され、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に記録される。この処理は従来と同様であり、また前述したブロック単位の利用期限情報を記録する構成でも同様の処理が実行される。

前述のブロック単位の利用期限情報を記録する構成では、コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）にはコンテンツの利用期限情報を記録していない設定であった。

【０１４１】

本処理例では、図１２に示すように、コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）は、図１２（ａ），（ｂ）に示す２つの設定のいずれかの設定となる。

（ａ）は、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）内にコンテンツの有効期限情報を記録し、かつブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）に無効を示すビット（０）を記録した設定。

（ｂ）は、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）内にコンテンツの有効期限情報を記録せず、かつブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）に有効を示すビット（１）を記録した設定。

これらの設定である。

【０１４２】

コンテンツを提供するサーバは、提供コンテンツの有効期限を、そのコンテンツ単独の設定とした有効期限を設定する場合は、上記（ａ）の設定に従った利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）を作成してコンテンツに併せてユーザ装置に提供してメモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に記録する。

【０１４３】

一方、提供コンテンツの有効期限を、そのコンテンツ単独の設定とせず、その他のコンテンツとともに、ブロック対応の有効期限を設定する場合は、上記（ｂ）の設定に従った利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）を作成してコンテンツに併せてユーザ装置に提供してメモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に記録する。

【０１４４】

サーバは、この２つの設定の利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）のいずれかを、コンテンツに応じて選択して提供する。

コンテンツの再生、利用を行うユーザ装置（ホスト機器）は、コンテンツ利用に際して、利用コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）を参照して、ブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定を確認する。

【０１４５】

ブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定が、無効を示すビット（０）である場合は、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）内の有効期限情報を参照する。

また、ブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定が、有効を示すビット（１）である場合は、コンテンツ対応のタイトルキーの格納された保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロックに記録された有効期限情報を参照する。

【０１４６】

このような処理により、利用制御情報に記録されたコンテンツ単独の有効期限と、複数のコンテンツに共通に設定されたブロック対応の有効期限とを共存させて、コンテンツに応じて誤りなく選択適用することが可能となる。

【０１４７】

次に、図１３を参照して、サーバＡ６１によるメモリカード７０に対する新たなコンテンツの記録処理シーケンスについて説明する。

図１３には、

（ａ１）ブロック対応の有効期限を利用するコンテンツ（ａ１）の提供処理、

（ａ２）コンテンツ単独の有効期限を利用制御情報に記録したコンテンツ（ａ２）の提供処理、

これらの２つのコンテンツの提供処理例を示している。

【０１４８】

まず、

（ａ１）ブロック対応の有効期限を利用するコンテンツ（ａ１）の提供処理、

について説明する。

サーバＡ６１がメモリカード７０に、他の提供コンテンツと共通するブロック対応の有効期限を設定したコンテンツを記録する場合には、このコンテンに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）のブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定を、有効を示すビット（１）とする。

この設定を持つ利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）を、コンテンツとともに、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に記録する。

【０１４９】

このコンテンツに対応するタイトルキーは、サーバＡ６１の書き込みの許容された保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロックに記録する。
図１３に示す例ではブロック＃０，８１がサーバＡ６１の書き込みの許容されたブロックであり、このブロックにタイトルキーを書き込む。なお、具体的には、タイトルキーに対する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）のハッシュ値とのＸＯＲ演算結果であるタイトルキーの変換データを記録する。

【０１５０】

このブロック＃０，８１には、サーバＡのその他の提供コンテンツに対応する有効期限が合わせて記録されている。コンテンツａ１については、このブロックに記録された有効期限が利用される。
ユーザ装置（ホスト機器）は、コンテンツ再生時に、コンテンツａ１に対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録されたブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定を確認して、この設定に基づいてブロックに記録された有効期限を参照して有効期限確認を行う。

【０１５１】

次に、
（ａ２）コンテンツ単独の有効期限を利用制御情報に記録したコンテンツ（ａ２）の提供処理、
について説明する。
サーバＡ６１がメモリカード７０に、コンテンツ単独の有効期限を設定したコンテンツを記録する場合には、このコンテンツ提供処理に際して、提供コンテンツの利用許容期間である有効期限情報を利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録する。
さらに、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）のブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定を、無効を示すビット（０）とした利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）を生成し、コンテンツとともに、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に記録する。

【０１５２】

このコンテンツに対応するタイトルキーは、サーバＡ６１の書き込みの許容された保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロックに記録する。
図１３に示す例はブロック＃０，８１がサーバＡ６１の書き込みの許容されたブロックであり、このブロックにタイトルキーを書き込む。なお、具体的には、タイトルキーに対する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）のハッシュ値とのＸＯＲ演算結果であるタイトルキーの変換データを記録する。

【０１５３】

なお、このブロック＃０，８１には、サーバＡのその他の提供コンテンツに対応するブロック対応の有効期限情報が記録されている。しかし、コンテンツａ２については、このブロック対応の有効期限は利用せず、コンテンツａ２に対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録された有効期限が利用される。

【０１５４】

すなわち、ユーザ装置（ホスト機器）は、コンテンツ再生時に、コンテンツａ２に対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録されたブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定を確認して、この設定に基づいて利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録された有効期限を参照して有効期限確認を行う。

【０１５５】

次に、図１４を参照してコンテンツの利用処理例について説明する。
図１４は、コンテンツを利用するユーザ装置であるホスト機器６３とコンテンツ等を格納したメモリカード７０を示している。
ホスト機器６３は、コンテンツの利用に際して以下の処理を実行する。
まず、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）から利

用対象コンテンツ：Ｃｏｎ（ｘｙ）と、対応する利用制御情報：ＵＲ（ｘｙ）を取得する。

【０１５６】

次に、利用制御情報：ＵＲ（ｘｙ）のブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定を確認する。

ビット設定が、無効を示すビット（０）である場合は、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）内の有効期限情報を参照する。

ビット設定が、有効を示すビット（１）である場合は、コンテンツ対応のタイトルキーの格納された保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロックに記録されたブロック対応の有効期限情報を参照する。

【０１５７】

このような処理により、利用制御情報に記録されたコンテンツ単独の有効期限と、複数のコンテンツに共通に設定されたブロック対応の有効期限とを共存させて、コンテンツに応じて誤りなく選択適用することが可能となる。

【０１５８】

図１５に示すフローチャートを参照して、コンテンツ利用を行うユーザ機器（ホスト機器）におけるコンテンツ再生処理シーケンスについて説明する。

図１５に示すフローに従った処理はユーザ機器に格納されたコンテンツ再生プログラム（ホストアプリケーション）に従ってユーザ機器のデータ処理部（ＣＰＵ等）において実行される。

【０１５９】

まず、ステップＳ２５１において、ユーザからの再生コンテンツ指定情報の入力を検出する。例えば再生装置の表示部に表示されたメニューとしてのコンテンツリストに対するユーザの入力であるコンテンツ指定情報の入力を検出する。

【０１６０】

次に、ステップＳ２５２において、再生指定コンテンツと利用制御情報をユーザ機器に装着されたメモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）から読み取る。すなわち、

利用対象コンテンツ：Ｃｏｎ（ｘｙ）と、

対応する利用制御情報：ＵＲ（ｘｙ）、

を取得する。

【０１６１】

次に、ステップＳ２５３において、読み取った利用制御情報：ＵＲ（ｘｙ）を参照して、利用制御情報：ＵＲ（ｘｙ）のブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定を確認する。

ビット設定が、無効を示すビット（０）である場合はステップＳ２５４に進む。有効を示すビット（１）である場合は、ステップＳ２５７に進む。

【０１６２】

ビット設定が、無効を示すビット（０）である場合はステップＳ２５４に進みステップＳ２５４において、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）内の有効期限情報を参照する。

【０１６３】

ステップＳ２５５において、現在日時が有効期限内であるか否かを判定し、有効期限内でないと判定した場合は、ステップＳ２７１に進み、処理は中止される。すなわちコンテンツの復号、利用処理は実行されない。

【０１６４】

一方、ステップＳ２５５において、現在日時が有効期限内であると判定した場合は、ステップＳ２５６に進む。

ステップＳ２５６では、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録されたタイトルキー格納ブロックを判別してそのブロックからデータを読み取る。

最後にステップＳ２６０においてブロックからの読み取りデータに含まれるタイトルキーを取得して、タイトルキーを利用したコンテンツの復号処理を行い、コンテンツの再生、利用を行う。

【０１６５】

一方、ステップＳ２５３において、利用制御情報：ＵＲ（ｘｙ）のブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定が、有効を示すビット（１）である場合は、ステップＳ２５７に進み、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録されたタイトルキー格納ブロックを判別してそのブロックからデータを読み取る。

【０１６６】

次に、ステップＳ２５８において、そのブロックの記録データの読み出し処理を行い、ブロック内データとして記録された有効期限情報を確認する。

このブロック対応有効期限と現在日時とを比較して、現在日時が有効期限内であるか否かを判定する。

【０１６７】

ステップＳ２５９において、現在日時が有効期限内でないと判定した場合は、ステップＳ２７２に進み、処理は中止される。すなわちコンテンツの復号、利用処理は実行されない。

【０１６８】

一方、ステップＳ２５９において、現在日時が有効期限内であると判定した場合は、ステップＳ２６０に進む。

ステップＳ２６０では、そのブロックに記録されたタイトルキーを取得して、タイトルキーを利用したコンテンツの復号処理を行い、コンテンツの再生、利用を行う。

【０１６９】

なお、ブロック内の格納タイトルキーは利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）とのハッシュ値との排他論理和（ＸＯＲ）演算結果として格納されており、前述したＵＲハッシュの算出、ＵＲハッシュとのＸＯＲ演算処理などによるタイトルキーの取得を行う。

【０１７０】

このように、現在日時がブロックに記録された有効期限内でない場合は、その時点で処理は中止される。なお、前述したように、ブロック内データとして記録された有効期限情報と現在日時情報との比較処理に際して利用する現在日時情報は、信頼できる時間情報提供サーバの提供する時間情報を利用する設定とすることが好ましい。

【０１７１】

このように、本実施例では、

利用制御情報に記録した有効期限情報、

ブロックに記録した有効期限情報、

これら２種類の有効期限情報を併存させ、

どちらを利用するかについての判別情報をコンテンツ対応の利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録する構成とした。

この設定により、

サーバは、コンテンツ単独の利用期限を設定することも可能でありまた、複数コンテンツに対応するブロック対応の期限をコンテンツに対応付けて利用させることも可能となる。

また、コンテンツ利用装置であるユーザ装置は、２つのタイプの有効期限をコンテンツに応じて誤りなく選択して適用することができる。

【０１７２】

［７．複数の有効期限情報をブロックに設定してコンテンツに応じて選択適用する処理例について］

次に、複数の有効期限情報をブロックに設定してコンテンツに応じて選択適用する処理例について説明する。

上述した実施例では、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の１つのブロックに、ブロック対応の有効期限を１つのみ設定した構成例を説明してきた。

【０１７３】

以下、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の１つのブロックに、複数の有効期限情報を記録し、コンテンツに応じてこれらの複数の有効期限から選択される１つの有効期限を参照して利用する構成例について説明する。

【０１７４】

図１６を参照して本実施例について説明する。

図１６には、コンテンツを記録したメモリカード７０の汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０の記録データと、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０の１つのブロック＃０，８１の記録データの例を示している。

【０１７５】

汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０には、以下のデータが記録されている。

コンテンツａ１、

コンテンツａ１に対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ａ１、

これらのデータが記録される。

なお、汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０には、この他にも多数のコンテンツとその利用制御情報のデータ組が記録されている。

【０１７６】

一方、コンテンツａ１を提供したサーバＡ専用の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０の１つのブロック＃０，８１には、図１６（ｂ）に示すように、タイトルキー格納領域に、サーバＡの提供コンテンツに対応するタイトルキーが記録されている。

図に示す、

Ｋｔ（ａ１）－ＵＲ（ａ１）ｈａｓｈ

Ｋｔ（ａ２）－ＵＲ（ａ２）ｈａｓｈ

：

Ｋｔ（ａｎ）－ＵＲ（ａｎ）ｈａｓｈ

これらのデータである。なお、前述したように、タイトルキーは利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ハッシュ値とのＸＯＲ演算結果として格納される。

【０１７７】

サーバＡ専用の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０の１つのブロック＃０，８１には、これらのタイトルキーに加えて、複数の有効期限データが記録された有効期限情報記録領域が設定されている。図に示す、

Ａｆｔｅｒ＃Ａｆ１，＃Ａｆ２，＃Ａｆ３・・・

Ｂｅｆｏｒｅ＃Ｂｆ１，Ｂｆ２，＃ｂｆ３・・・

これらのデータの記録領域である。

【０１７８】

Ａｆｔｅｒ＃Ａｆ１，＃Ａｆ２，＃Ａｆ３・・・は、具体的には、例えば、

Ａｆｔｅｒ＃Ａｆ１＝Ａｆｔｅｒ２０１１／０９／０１

Ａｆｔｅｒ＃Ａｆ２＝Ａｆｔｅｒ２０１１／１０／０１

Ａｆｔｅｒ＃Ａｆ３＝Ａｆｔｅｒ２０１１／１１／０１

このようなデータである。

Ａｆｔｅｒ＃Ａｆｎに設定された期日以降がコンテンツの利用が可能であることを示す。

このように、Ａｆｔｅｒ＃Ａｆ１，＃Ａｆ２，＃Ａｆ３・・・として、複数の異なる有効期限開始日時情報が記録されている。

【０１７９】

また、Ｂｅｆｏｒｅ＃Ｂｆ１，Ｂｆ２，＃Ｂｆ３・・・は、具体的には、例えば、

Ｂｅｆｏｒｅ＃Ｂｆ１＝Ｂｅｆｏｒｅ２０１１／０９／３０

Ｂｅｆｏｒｅ＃Ｂｆ２＝Ｂｅｆｏｒｅ２０１１／１０／３１
Ｂｅｆｏｒｅ＃Ｂｆ３＝Ｂｅｆｏｒｅ２０１１／１１／３０
このようなデータである。
Ｂｅｆｏｒｅ＃Ｂｆｎに設定された期日以前がコンテンツの利用が可能であることを示す。
すなわち、Ｂｅｆｏｒｅ＃Ｂｆ１，Ｂｆ２，＃Ｂｆ３・・・として、複数の異なる有効期限終了日時情報が記録されている。

【０１８０】
図１６（ａ）に、汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０に記録されたコンテンツａ１に対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ａ１の具体例を示す。

【０１８１】
利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）には、
（１）ブロック識別子
（２）タイトルキー識別子
（３）ブロック対応期限有効性判定ビット
（４）有効期限情報識別子
これらのデータが記録される。

【０１８２】
（１）ブロック識別子は、
この利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ＵＲ－（ａ１）の対応コンテンツ：Ｃｏｎ（ａ１）に対するタイトルキーＫｔ（ａ１）の格納ブロックを示す情報である。
本例ではブロック識別子＝＃０であり、
コンテンツ再生を実行するユーザ装置（ホスト機器）は、ブロック＃０を選択可能となる。

【０１８３】
（２）タイトルキー識別子は、
ブロック＃０に格納された多数のタイトルキーのどのタイトルキーが、この利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ＵＲ－（ａ１）の対応コンテンツ：Ｃｏｎ（ａ１）に対するタイトルキーであるかを示す情報である。
本例では、タイトルキー識別子＝ａ１であり、
タイトルキーＫｔ（ａ１）が選択可能となる。

【０１８４】
（３）ブロック対応期限有効性判定ビットは、
先の実施例において説明した情報である。
ブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定が、無効を示すビット（０）である場合は、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）内の有効期限情報を参照する。
また、ブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定が、有効を示すビット（１）である場合は、コンテンツ対応のタイトルキーの格納された保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のブロックに記録された有効期限情報を参照する。

【０１８５】
（４）有効期限情報識別子は、
上記の、ブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定が、有効を示すビット（１）である場合、すなわち、ブロックに記録された有効期限情報が有効である場合に記録される。
この有効期限情報識別子は、ブロックの有効期限情報記録領域に記録された多数の有効期限のいずれを利用するかを示す識別子である。

【０１８６】

図に示す例では、
有効期限情報識別子＝Ａｆ３，Ｂｆ３
これらの設定である。例えば、
Ａｆｔｅｒ＃Ａｆ３＝Ａｆｔｅｒ２０１１／１１／０１
Ｂｅｆｏｒｅ＃Ｂｆ３＝Ｂｅｆｏｒｅ２０１１／１１／３０
このようなデータであり、
この利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ＵＲ－（ａ１）の対応コンテンツ：Ｃｏｎ（ａ１）の有効利用期間は、
２０１１／１１／０１～２０１１／１１／３０
となる。

【０１８７】
コンテンツ再生を実行するユーザ装置（ホスト機器）は、このように、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録された、有効期限情報識別子に基づいて、ブロックに設定された多数の有効期限から、コンテンツ対応の有効期限を選択して利用することが可能となる。

【０１８８】
本例に従えば、１つのブロックに多数のコンテンツ対応のタイトルキーを記録する場合に、コンテンツ（およびタイトルキー）各々に対して個別の有効期限を記録することが可能となる。
なお、この設定でも、有効期限の更新処理は、ブロックに記録された有効期限情報を書き換える処理を行うことで実行でき、個別の利用制御情報の書き換えは不要となる。

【０１８９】
なお、この構成に従えば、１つのブロックを１つのコンテンツ提供主体、例えば１つのサーバ専用に設定することなく、複数の異なるコンテンツ提供サーバで共用するといった設定も可能である。
具体的には、図１７に示すように、１つのブロックのタイトルキー格納領域を区分して、サーバＡ用のタイトルキー格納領域とサーバＢ用のタイトルキー格納領域を設定する。
各コンテンツ提供サーバはそれぞれの領域にサーバの提供するコンテンツに対応するタイトルキーを格納する。
有効期限情報格納領域は、サーバＡ，Ｂに共通に利用する領域とする。

【０１９０】
各サーバは、コンテンツ提供時に利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に、図１６（ａ）を参照して説明した上述した各情報、すなわち、
（１）ブロック識別子
（２）タイトルキー識別子
（３）ブロック対応期限有効性判定ビット
（４）有効期限情報識別子
これらの各情報を記録してメモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に記録する。
このような設定とすることで、１つのブロックを複数のサーバが共用し、サーバ単位、コンテンツ単位の利用期限を自在に設定することが可能となる。

【０１９１】
このように、メモリカードの１つのブロックを複数のサーバのタイトルキー書き込み領域とした設定例における各サーバのアクセス権設定例を図１８に示す。
図１８にはサーバＡ６１、サーバＢ６２、サーバＣ６４、サーバＤ６５の４つのサーバを示している。

【０１９２】
サーバＡ６１、サーバＢ６２はメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０のブロック＃０，８１に対するアクセス権（Ｒｅａｄ／Ｗｒｉｔｅ）を有する。
サーバＣ６４、サーバＤ６５はメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅ

ａ）８０のブロック＃１，８２に対するアクセス権（Ｒｅａｄ／Ｗｒｉｔｅ）を有する。
【０１９３】
このような場合、各サーバの保持するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）は、図１８に示すように、
サーバＡ６１、サーバＢ６２の保持するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）はブロック＃０，８１に対するアクセス権（Ｒｅａｄ／Ｗｒｉｔｅ）許容情報が記録され、サーバＣ６４、サーバＤ６５の保持するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）はブロック＃１，８２に対するアクセス権（Ｒｅａｄ／Ｗｒｉｔｅ）許容情報が記録される。
【０１９４】
この設定において、メモリカードに記録されるデータの例を図１９に示す。
図１９に示すように、
メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　ａｒｅａ）には各サーバＡ～Ｄの提供するコンテンツと、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）が記録される。
【０１９５】
また、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の、
ブロック＃０には、サーバＡとサーバＢの提供コンテンツに対応するタイトルキーが格納され、
ブロック＃１にはサーバＣとサーバＤの提供コンテンツに対応するタイトルキーがそれぞれ格納される。
なお、タイトルキーは例えば利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ハッシュ値とのＸＯＲ演算結果として格納される。
【０１９６】
上述したように、本構成によれば、保護領域の１つのブロックに記録したタイトルキー対応のコンテンツ個別の有効期限の設定が可能であり、また１つのブロックを複数のサーバによって利用可能な共有ブロックとする設定も可能となる。
【０１９７】
［８．コンテンツの初回利用情報を記録する処理例について］
コンテンツの利用期限の設定態様としては、前述したように、例えば、
２０１１／１０／０１～２０１１／１０／３１
上記の利用期限ように絶対的な期限情報を設定することも可能であるが、このような設定の他、ユーザによるコンテンツの最初の利用開始日時から１ヶ月など、ユーザの初回利用時を起点として所定期間を利用可能期間として設定する態様も可能である。
【０１９８】
このような利用期限を設定する場合、利用可能期間はユーザの初回利用時によって変動することになり、サーバのコンテンツ提供日時からの期限設定ができない。また、予めサーバが利用期限を固定的に設定することができない。
以下では、このようなユーザ処理依存のコンテンツ利用期限の設定を可能とした処理例について説明する。
【０１９９】
この処理を実現するためのメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の記録データの設定例について、図２０を参照して説明する。
図２０には、メモリカード７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０に設定された２つのブロック、すなわち、ブロック＃０、ブロック＃１の記録データ例を示している。
【０２００】
ブロック＃０は、先の実施例の図１６を参照して説明したブロック＃０と同様のデータを記録する領域である。
すなわち、図２０（ｂ１）に示すように、タイトルキーと有効期限情報を記録した領域である。このブロックをタイトルキー格納ブロックとする。
本実施例では、このタイトルキー格納ブロックの他に保護領域（Ｐｒｏｔｅｃｔｅｄ

Ａｒｅａ）８０のもう１つのブロックを利用する。

【０２０１】

図２０に示すブロック＃１であり、図２０（ｂ２）に示すステータス格納ブロックである。

このステータス格納ブロックには、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　ＡＲｅａ）に記録した各コンテンツ（Ｃｏｎａ１，Ｃｏｎａ２，・・・）に対応する初回再生日時情報を記録する。

【０２０２】

例えば、図２０（ｂ２）に示す、

Ｓｔａｔｕｓ　ｆｏｒ　Ｃｏｎ（ａ１）は、コンテンツ：Ｃｏｎ（ａ１）の初回再生日時情報の記録領域である。

Ｓｔａｔｕｓ　ｆｏｒ　Ｃｏｎ（ａ２）は、コンテンツ：Ｃｏｎ（ａ２）の初回再生日時情報の記録領域である。

【０２０３】

なお、この各コンテンツの初回再生日時情報は、コンテンツ再生を実行するユーザ装置（ホスト機器）が記録する。

ユーザ装置（ホスト機器）は、ブロック＃１に対する書き込み許容情報が記録されたホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）を保持する。

ユーザ装置（ホスト機器）がコンテンツ、例えばコンテンツ：Ｃｏｎ（ａ１）を初めに再生する場合、その初回再生日時情報を、図２０（ｂ２）に示す［Ｓｔａｔｕｓ　ｆｏｒ　Ｃｏｎ（ａ１）］領域に記録する。

【０２０４】

図２１、図２２を参照して本実施例における利用制御情報（Ｕｓａｇｅ　Ｒｕｌ）の構成例について説明する。

図２１には、コンテンツを記録したメモリカード７０の汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０の記録データと、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０のタイトルキー格納ブロックであるブロック＃０，８１の記録データの例を示している。

図２２には、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０のステータス格納ブロックであるブロック＃１，８２の記録データの例を示している。

【０２０５】

図２１に示す汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０には、以下のデータが記録されている。

コンテンツａ１、

コンテンツａ１に対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ａ１、

これらのデータが記録される。

なお、汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０には、この他にも多数のコンテンツとその利用制御情報のデータ組が記録されている。

【０２０６】

一方、コンテンツａ１を提供したサーバＡ専用の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０のタイトルキー格納ブロックであるブロック＃０，８１には、図２１（ｂ１）に示すように、タイトルキー格納領域に、サーバＡの提供コンテンツに対応するタイトルキーが記録されている。

図に示す、

Ｋｔ（ａ１）－ＵＲ（ａ１）ｈａｓｈ

Ｋｔ（ａ２）－ＵＲ（ａ２）ｈａｓｈ

：

Ｋｔ（ａｎ）－ＵＲ（ａｎ）ｈａｓｈ

これらのデータである。なお、前述したように、タイトルキーは利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ハッシュ値とのＸＯＲ演算結果として格納される。

【０２０７】
サーバＡ専用の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０の１つのブロック＃０，８１には、これらのタイトルキーに加えて、複数の有効期限データが記録された有効期限情報記録領域が設定されている。図に示す、
Ａｆｔｅｒ＃Ａｆ１，＃Ａｆ２，＃Ａｆ３・・・
Ｂｅｆｏｒｅ＃Ｂｆ１，Ｂｆ２，＃Ｂｆ３・・・
これらのデータの記録領域である。
これらには、先に図１６を参照して説明したと同様のデータが含まれる。
【０２０８】
すなわち、例えば、
Ａｆｔｅｒ＃Ａｆ１，＃Ａｆ２，＃Ａｆ３・・・は、具体的には、
Ａｆｔｅｒ＃Ａｆ１＝Ａｆｔｅｒ２０１１／０９／０１
Ａｆｔｅｒ＃Ａｆ２＝Ａｆｔｅｒ２０１１／１０／０１
Ａｆｔｅｒ＃Ａｆ３＝Ａｆｔｅｒ２０１１／１１／０１
このようなデータであり、
Ａｆｔｅｒ＃Ａｆｎの各設定期日以降がコンテンツの利用が可能であることを示す。
【０２０９】
また、Ｂｅｆｏｒｅ＃Ｂｆ１，Ｂｆ２，＃Ｂｆ３・・・は、具体的には、例えば、
Ｂｅｆｏｒｅ＃Ｂｆ１＝Ｂｅｆｏｒｅ２０１１／０９／３０
Ｂｅｆｏｒｅ＃Ｂｆ２＝Ｂｅｆｏｒｅ２０１１／１０／３１
Ｂｅｆｏｒｅ＃Ｂｆ３＝Ｂｅｆｏｒｅ２０１１／１１／３０
このようなデータであり、
Ｂｅｆｏｒｅ＃Ｂｆｎの各設定期日以前がコンテンツの利用が可能であることを示す。
【０２１０】
本実施例では、これらの実際の日時情報の他、
Ａｆｔｅｒ＃Ａｆｐ＝Ａｆｔｅｒ（Ｓｔａｔｕｓ　ｆｏｒ　Ｃｏｎ（ｘｙ））、
あるいは、
Ｂｅｆｏｒｅ＃Ｂｆｑ＝Ｂｅｆｏｒｅ（Ｓｔａｔｕｓ　ｆｏｒ　Ｃｏｎ（ｘｙ）＋１ｍｏｎｔｈ）、
このような有効期限設定が可能な構成を持つ。
【０２１１】
Ａｆｔｅｒ＃Ａｆｐ＝Ａｆｔｅｒ（Ｓｔａｔｕｓ　ｆｏｒ　Ｃｏｎ（ｘｙ））は、
図２０（ｂ２）に示すステータス格納ブロックに記録されるコンテンツの初回再生日時以降がコンテンツの利用許容期間になることを示す。
Ｂｅｆｏｒｅ＃Ｂｆｑ＝Ｂｅｆｏｒｅ（Ｓｔａｔｕｓ　ｆｏｒ　Ｃｏｎ（ｘｙ）＋１ｍｏｎｔｈ）は、
図２０（ｂ２）に示すステータス格納ブロックに記録されるコンテンツの初回再生日時から１月経過までが、コンテンツの利用許容期間になることを示す。
このような設定を利用することで、図２０（ｂ２）に示すステータス格納ブロックに記録されるコンテンツの初回再生日時に対応したコンテンツ利用期限情報を設定することが可能となる。
【０２１２】
図２１（ａ）に、汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）９０に記録されたコンテンツａ１に対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ａ１の具体例を示す。
【０２１３】
利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）には、
（１）ブロック識別子
（２）タイトルキー識別子
（３）ブロック対応期限有効性判定ビット

（４）有効期限情報識別子
（５）ステータス格納ブロック識別子
（６）ステータス情報識別子
これらのデータが記録される。

【０２１４】

（１）ブロック識別子～（４）有効期限情報識別子は、先に図１６を参照して説明した情報と同様の情報であり説明を省略する。

これらの情報は、図２１（ｂ１）に示すタイトルキー格納ブロックに対応する情報である。

【０２１５】

（５）ステータス格納ブロック識別子
（６）ステータス情報識別子
これらのデータについて、図２２を参照して説明する。

これらのデータは、ステータス格納ブロック（ブロック＃１，８２）に対応する情報である。

【０２１６】

（５）ステータス格納ブロック識別子は、

この利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ＵＲ－（ａ１）の対応コンテンツ：Ｃｏｎ（ａ１）に対するステータス情報を格納したステータス格納ブロックを示す情報である。

本例ではステータス格納ブロック識別子＝＃１であり、

コンテンツ再生を実行するユーザ装置（ホスト機器）は、ステータス情報の格納ブロックが、ブロック＃１であることが判別できる。

【０２１７】

（６）ステータス情報識別子は、

ステータス格納ブロック（ブロック＃１）に格納された多数のステータス情報のどのステータス情報が、この利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）ＵＲ－（ａ１）の対応コンテンツ：Ｃｏｎ（ａ１）に対するステータスであるかを示す情報である。

本例では、ステータス情報識別子＝ａ１であり、

ステータス情報（ａ１）が選択可能となる。

【０２１８】

図２２（ｂ２）に示すメモリカード７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０に設定されるステータス格納ブロックであるブロック＃１，８２には、

コンテンツの利用開始日時を記録する。

コンテンツの利用開始日時は、コンテンツを利用するユーザ機器（ホスト機器）が記録する。

なお、サーバによるコンテンツ提供時には、

メモリカード７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０に設定されるステータス格納ブロックであるブロック＃１，８２には、コンテンツ利用開始日時データは記録されず、日時情報を記録するためのステータスデータ記録領域のみが設定される。

【０２１９】

各サーバは、コンテンツ提供時に利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に、図２２（ａ）に示す上述した各情報、すなわち、

（１）ブロック識別子
（２）タイトルキー識別子
（３）ブロック対応期限有効性判定ビット
（４）有効期限情報識別子
（５）ステータス格納ブロック識別子
（６）ステータス情報識別子
これらの各情報を記録してメモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）に記録する。

【０２２０】
　また、上述したようにメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のステータス情報格納ブロックには、ステータス情報としての「コンテンツの利用開始日時」の記録領域を設定する。
　コンテンツ再生を実行するユーザ装置（ホスト機器）が、コンテンツの初回再生を行う際に、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）のステータス情報格納ブロックに実際の初回再生日時データを記録する。
【０２２１】
　図２３を参照して、コンテンツ提供処理を実行するサーバの実行する処理について説明する。
　図２３には、コンテンツを提供するサーバＡ６１の実行するメモリカード７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０に対するデータ記録処理を示している。
　なお、サーバＡ６１は、この図２３に示す保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０に対するデータ記録処理に併せて、メモリカード７０の汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）にコンテンツと図２１、図２２を参照して説明した利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）の記録処理を実行する。
【０２２２】
　図２３に示すように、サーバＡ６１は、メモリカード７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０のタイトルキー格納ブロックであるブロック＃０，８１に提供コンテンツに対応するタイトルキーを記録する。
　さらに、このタイトルキーの記録処理に先立ち、メモリカード７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）８０のステータス格納ブロックであるブロック＃１，８２に提供コンテンツのステータス記録領域を設定し、
　各コンテンツの利用開始日時の記録領域を設定する。
【０２２３】
　サーバＡ６１は、ブロック＃０，８１、およびブロック＃１，８２に対する書き込み許容情報を記録したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）を保持し、この証明書をメモリカード７０に提示する。メモリカード７０のアクセス権判定処理の結果に応じて、各ブロックに対して、タイトルキーの書き込み処理、およびステータス情報の記録領域設定を行う。
【０２２４】
　次に、図２４を参照して、コンテンツ利用を行うホスト機器６３の処理について説明する。
　ホスト機器６３は、コンテンツを利用する場合に、利用コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）の記録情報に従って、タイトルキーの格納ブロックとステータスの格納ブロックを判別する。
　図２１、図２２を参照して説明した利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）の記録情報に従った処理である。
【０２２５】
　ホスト機器６３は、利用コンテンツに対応するタイトルキーをタイトルキーの格納ブロックであるブロック＃０，８１から取得する。
　さらに、コンテンツの初回再生時には、ステータス格納ブロックのステータス情報記録領域に初回再生日時情報を記録する。
　なお、この日時情報の記録に際しては、正確な日時情報を信頼できる時間情報提供サーバ等から取得して記録することが好ましい。
【０２２６】
　コンテンツの初回再生処理でなく、２回以降の再生処理である場合は、ステータス格納ブロックのステータス情報記録領域に記録された初回再生日時情報を参照し、さらに、ステータス格納ブロックのステータス情報記録領域に記録された有効期限情報を参照して、現在日時がコンテンツの利用期限内であるか否かを判定する。

【０２２７】
例えば、
あるコンテンツ：Ｃｏｎ（ｘｙ）に対してステータス情報記録領域に記録された初回再生日時情報が、
２０１１／０９／０１
であるとする。
【０２２８】
このコンテンツ：Ｃｏｎ（ｘｙ）に対応する利用制御情報（ＵＲ：Ｕｓａｇｅ　Ｒｕｌｅ）には、
ブロック識別子：＃０
有効期限情報識別子：＃Ａｆｐ，＃Ｂｆｑ
これらの有効期限情報識別子が記録されているとする。
【０２２９】
ユーザ機器（ホスト機器）は、保護領域のブロック＃０から有効期限情報識別子：＃Ａｆｐ，＃Ｂｆｑの有効期限情報を選択取得する。これらの有効期限情報は、以下の設定であるとする。
Ａｆｔｅｒ＃Ａｆｐ＝Ａｆｔｅｒ（Ｓｔａｔｕｓ　ｆｏｒ　Ｃｏｎ（ｘｙ））、
Ｂｅｆｏｒｅ＃Ｂｆｑ＝Ｂｅｆｏｒｅ（Ｓｔａｔｕｓ　ｆｏｒ　Ｃｏｎ（ｘｙ）＋１ｍｏｎｔｈ）、
この設定である場合、
コンテンツの利用許容期間は、
２０１１／０９／０１～２０１１／０９／３１
となる。
ユーザ機器は、現在日時が、このコンテンツ利用許容期間に該当している否かを判定して、該当している場合は、コンテンツの復号、再生を行う。該当していない場合は、コンテンツ利用を中止する。
【０２３０】
なお、現在日時情報については、信頼できる時間情報提供サーバ等から取得することが好ましい。
上記の説明では、有効期限情報や、ステータス情報として記録する初回再生日時を日までの設定として説明したが、時間単位、例えば時分秒単位の設定としてもよい。
【０２３１】
次に、図２５、図２６に示すフローチャートを参照して、コンテンツ利用を行うユーザ機器（ホスト機器）におけるコンテンツ再生処理シーケンスについて説明する。
図２５、図２６に示すフローに従った処理はユーザ機器に格納されたコンテンツ再生プログラム（ホストアプリケーション）に従ってユーザ機器のデータ処理部（ＣＰＵ等）において実行される。
【０２３２】
まず、ステップＳ３０１において、ユーザからの再生コンテンツ指定情報の入力を検出する。例えば再生装置の表示部に表示されたメニューとしてのコンテンツリストに対するユーザの入力であるコンテンツ指定情報の入力を検出する。
【０２３３】
次に、ステップＳ３０２において、再生指定コンテンツと利用制御情報をユーザ機器に装着されたメモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）から読み取る。すなわち、
利用対象コンテンツ：Ｃｏｎ（ｘｙ）と、
対応する利用制御情報：ＵＲ（ｘｙ）、
を取得する。
【０２３４】
次に、ステップＳ３０３において、読み取った利用制御情報：ＵＲ（ｘｙ）を参照して

、利用制御情報：ＵＲ（ｘｙ）のブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定を確認する。
ビット設定が、無効を示すビット（０）である場合はステップＳ３０４に進む。有効を示すビット（１）である場合は、ステップＳ３０７に進む。
【０２３５】
ビット設定が、無効を示すビット（０）である場合はステップＳ３０４に進みステップＳ３０４において、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）内の有効期限情報を参照する。
【０２３６】
ステップＳ３０５において、現在日時が有効期限内であるか否かを判定し、有効期限内でないと判定した場合は、ステップＳ３５１に進み、処理は中止される。すなわちコンテンツの復号、利用処理は実行されない。
【０２３７】
一方、ステップＳ３０５において、現在日時が有効期限内であると判定した場合は、ステップＳ３０６に進む。
ステップＳ３０６では、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録されたタイトルキー格納ブロックを判別してそのブロックからデータを読み取る。
最後にステップＳ３１１においてブロックからの読み取りデータに含まれるタイトルキーを取得して、タイトルキーを利用したコンテンツの復号処理を行い、コンテンツの再生、利用を行う。
【０２３８】
なお、ブロック内の格納タイトルキーは利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）とのハッシュ値との排他論理和（ＸＯＲ）演算結果として格納されており、前述したＵＲハッシュの算出、ＵＲハッシュとのＸＯＲ演算処理などによるタイトルキーの取得を行う。
【０２３９】
一方、ステップＳ３０３において、利用制御情報：ＵＲ（ｘｙ）のブロック対応期限有効性判定ビット（Ｓｕｂｓｃｒｉｐｔｉｏｎ　Ｅｎａｂｌｅ　ｂｉｔ）の設定が、有効を示すビット（１）である場合は、ステップＳ３０７に進み、利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）に記録されたタイトルキー格納ブロックを判別してそのブロックからデータを読み取る。
【０２４０】
次に、ステップＳ３０８において、そのブロックの記録データの読み出し処理を行い、ブロック内データとして記録された有効期限情報を確認する。
さらに、ステップＳ３０９において、ブロック内データとして記録された有効期限情報が、ステータス情報参照タイプであるか否かを判定する。
ステータス情報参照タイプとは、先に説明した、以下のような設定の有効期限情報である。
Ａｆｔｅｒ＃Ａｆｐ＝Ａｆｔｅｒ（Ｓｔａｔｕｓ　ｆｏｒ　Ｃｏｎ（ｘｙ））、
Ｂｅｆｏｒｅ＃Ｂｆｑ＝Ｂｅｆｏｒｅ（Ｓｔａｔｕｓ　ｆｏｒ　Ｃｏｎ（ｘｙ）＋１ｍｏｎｔｈ）、
このような設定である場合、ステータス情報参照タイプである場合は、ステップＳ３２１に進む。
【０２４１】
上記のようなステータス情報参照タイプでない場合は、ステップＳ３１０に進む。
ステップＳ３１０では、ブロックから取得した有効期限情報と現在日時とを比較して、現在日時が有効期限内であるか否かを判定する。
ステップＳ３１０において、現在日時が有効期限内でないと判定した場合は、ステップＳ３５２に進み、処理は中止される。すなわちコンテンツの復号、利用処理は実行されない。
【０２４２】

一方、ステップＳ３１０において、現在日時が有効期限内であると判定した場合は、ステップＳ３１１に進む。
ステップＳ３１１では、そのブロックに記録されたタイトルキーを取得して、タイトルキーを利用したコンテンツの復号処理を行い、コンテンツの再生、利用を行う。
【０２４３】
一方、ステップＳ３０９において、ブロック内データとして記録された有効期限情報が、ステータス情報参照タイプであると判定した場合はステップＳ３２１に進む。
この場合は、図２６に示すステップＳ３２１において、利用制御情報ファイルの記録に従ってステータス情報格納ブロックから指定されたステータス情報を取得する。
【０２４４】
次に、ステップＳ３２２において、取得したステータス情報に初回再生日時情報が記録されているか否かを判定する。
ステータス情報に初回再生日時情報が記録されている場合は、ステップＳ３２３に進む。
ステータス情報に初回再生日時情報が記録されていない場合は、ステップＳ３２４に進む。
【０２４５】
ステータス情報に初回再生日時情報が記録されていない場合は、ステップＳ３２４に進み、ステータス情報として初回再生日時情報を記録する。なお、この初回再生日時情報記録処理に際しては、信頼できる時間情報提供サーバ等から正確な時間情報を取得して記録する処理を行うことが好ましい。
この初回再生日時情報の記録処理の後、ステップＳ３２５に進み、タイトルキー格納ブロックに記録されたタイトルキーを取得して、タイトルキーを利用したコンテンツの復号処理を行い、コンテンツの再生、利用を行う。
【０２４６】
一方、ステップＳ３２２において、取得したステータス情報に初回再生日時情報が記録されていると判定した場合は、ステップＳ３２３に進む。
ステップＳ３２３では、
ステータス情報に記録された初回再生日時情報と、
ステップＳ３０８において取得したステータス情報参照タイプの有効期限情報に基づいて、現在日時が有効期限内であるか否かを判定する。
【０２４７】
ステップＳ３２３において、現在日時が有効期限内でないと判定した場合は、ステップＳ３５３に進み、処理は中止される。すなわちコンテンツの復号、利用処理は実行されない。
【０２４８】
一方、ステップＳ３２３において、現在日時が有効期限内であると判定した場合は、ステップＳ３２５に進む。
ステップＳ３２５では、そのブロックに記録されたタイトルキーを取得して、タイトルキーを利用したコンテンツの復号処理を行い、コンテンツの再生、利用を行う。
【０２４９】
このように、本実施例では、
ブロックに記録した有効期限情報を、ユーザ装置において記録可能なステータス情報参照タイプとして構成することで、
ユーザのコンテンツ再生処理に依存してコンテンツの利用許容期間が設定される構成において、その有効期限の設定範囲でのコンテンツ利用を許容する構成を実現する。
【０２５０】
［９．コンテンツのメディア間移動（ムーブ）処理について］
次に、上述したステータス情報を記録する構成において、コンテンツを異なるメディア間で移動する場合の処理について説明する。

【０２５１】
あるメモリカードである第１メディアに記録されたコンテンツを他のメモリカードである第２メディアに移動（ムーブ）する場合の処理について説明する。
ムーブ対象となるコンテンツに対して、ステータス参照タイプの利用期限情報が設定されている場合には、このステータス情報についても併せて移動することが必要となる。
【０２５２】
例えば、ステータス参照タイプの利用期限情報が設定されたコンテンツＣｏｎ（ｘｙ）のメディア間の移動（ムーブ）処理を行う場合、
コンテンツ：Ｃｏｎ（ｘｙ）
コンテンツＣｏｎ（ｘｙ）に対応する利用制御情報：ＵＲ（ｘｙ）
コンテンツＣｏｎ（ｘｙ）に対応するタイトルキー：Ｋｔ（ｘｙ）
タイトルキー：Ｋｔ（ｘｙ）格納ブロックの利用期限情報、
利用制御情報：ＵＲ（ｘｙ）に記録されたステータス格納ブロックの対応ステータス情報、
これらの各情報を併せて移動（ムーブ）する処理が必要となる。
【０２５３】
これらのデータ移動に際しては、ムーブ元メディアである第１のメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の各ブロックからのデータ読み取りと、ムーブ先メディアである第２のメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の各ブロックへのデータ記録処理を行うことが必要となる。
従って、これらのブロックに対するアクセス権を有するサーバによる処理を行うことが必要となる。
【０２５４】
図２７、図２８を参照してコンテンツのムーブ処理におけるサーバの処理について説明する。
図２７は、ムーブ元メディアに対する処理、
図２８は、ムーブ先メディアに対する処理、
これらの各処理を示している。
なお、図２７、図２８は、サーバＡ６１の提供コンテンツのムーブ処理を実行する際のメモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の記録データに対する処理のみを示している。
汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）のデータ移動はユーザ装置において実行できる。
【０２５５】
まず、図２７を参照して、ムーブ元メディアに対する処理について説明する。
サーバＡ６１は、ムーブ元メディア３０１のタイトルキー格納ブロックであるブロック＃０からムーブ対象コンテンツに対応するタイトルキーを読み出して取得し、さらにブロック＃０からタイトルキーデータを削除する。
【０２５６】
また、サーバＡ６１は、ムーブ元メディア３０１のステータス格納ブロックであるブロック＃１からムーブ対象コンテンツに対応するステータス情報を読み出して取得し、さらにブロック＃１からステータス情報を削除する。
この処理によって、ムーブ元メディア３０１には、ムーブ対象コンテンツに対応するタイトルキーとステータス情報が削除される。
【０２５７】
次に、図２８を参照して、ムーブ先メディアに対する処理について説明する。
サーバＡ６１は、ムーブ先メディア３０２のタイトルキー格納ブロックであるブロック＃０に対して、ムーブ元メディアから取得したムーブ対象コンテンツに対応するタイトルキーを記録する。
【０２５８】

さらに、サーバＡ６１は、ムーブ先メディア３０２のステータス格納ブロックであるブロック＃１に対して、ムーブ元メディアから取得したムーブ対象コンテンツに対応するステータス情報を記録する。

この処理によって、ムーブ先メディア３０２には、ムーブ対象コンテンツに対応するタイトルキーとステータス情報が記録される。

【０２５９】

なお、図２７を参照して説明したサーバＡ６１とムーブ元メディア３０１間の処理に際しては、サーバとムーブ元メディア３０１間の相互認証処理を実行し、さらに、ムーブ元メディア３０１はサーバＡ６１から受信したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）に基づく各ブロックのアクセス権確認を実行する。

認証の成立とアクセス権の確認がなされたことを条件として、上記の図２７を参照して説明した処理が行われる。

【０２６０】

同様に、図２８を参照して説明したサーバＡ６１とムーブ先メディア３０２間の処理に際しては、サーバとムーブ先メディア３０２間の相互認証処理を実行し、さらに、ムーブ先メディア３０２はサーバＡ６１から受信したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）に基づく各ブロックのアクセス権確認を実行する。

認証の成立とアクセス権の確認がなされたことを条件として、上記の図２８を参照して説明した処理が行われる。

【０２６１】

［１０．各装置のハードウェア構成例について］

最後に、図２９、図３０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２９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。

【０２６２】

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、放送局やサーバからのコンテンツ受信処理や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。

【０２６３】

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。

【０２６４】

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。

【０２６５】

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、あるいはメモリカード等の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。

【０２６６】

図３０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。

【０２６７】

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。

【０２６８】

入出力インタフェース８０５に接続されている通信部８０６は、例えばサーバやホスト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　Ａｒｅａ）８１１、自由にデータ記録読み取りができる汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）８１２を有する。

【０２６９】

なお、サーバは、例えば図２９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。

【０２７０】

［１１．本開示の構成のまとめ］

以上、特定の実施例を参照しながら、本開示の実施例について詳解してきた。しかしながら、本開示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。本開示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。

【０２７１】

なお、本明細書において開示した技術は、以下のような構成をとることができる。

（１）　メディアに格納されたコンテンツを再生するデータ処理部を有し、

前記メディアは、

暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納した汎用領域と、

前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、

前記データ処理部は、

コンテンツ再生処理に際して、前記コンテンツ初回再生時の日時情報に応じて決定されるコンテンツ利用許容期間である有効期限情報を前記暗号鍵格納ブロックから取得し、取得した有効期限情報と現在日時情報との比較により、コンテンツ再生の可否を判定する情報処理装置。

【０２７２】

（２）前記暗号鍵格納ブロックに記録された有効期限情報は、前記ステータス格納ブロ

ックに記録されたコンテンツ初回再生時の日時情報を基準日時として設定した有効期限情報である前記（１）に記載の情報処理装置。

（３）前記利用制御情報は、再生対象コンテンツの復号用の暗号鍵を格納した暗号鍵格納ブロックを識別可能とした暗号鍵格納ブロック識別子と、前記再生対象コンテンツのコンテンツ対応ステータス情報を格納したステータス格納ブロックを識別可能としたステータス格納ブロック識別子を有し、前記データ処理部は、前記暗号鍵格納ブロック識別子に基づいて、前記保護領域から１つの暗号鍵格納ブロックを選択し、前記ステータス格納ブロック識別子に基づいて、前記保護領域から１つのステータス格納ブロックを選択し、各選択ブロックから前記再生対象コンテンツに対応する暗号鍵とステータス情報を取得する前記（１）または（２）に記載の情報処理装置。

【０２７３】

（４）前記暗号鍵格納ブロックには、前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である複数の有効期限情報が格納され、前記データ処理部は、前記汎用領域から再生対象コンテンツの利用制御情報を取得し、前記ブロックに記録された複数の有効期限情報中、再生対象コンテンツに適用すべき有効期限情報の選択情報を、前記利用制御情報から抽出し、該選択情報に従って、前記ブロックから選択した有効期限情報がコンテンツ初回再生時の日時情報に応じた有効期限情報である場合、前記コンテンツ対応ステータス情報として記録されたコンテンツ初回再生時の日時情報を基準日時とした有効期限情報に基づくコンテンツ再生可否判定を行う前記（１）～（３）いずれかに記載の情報処理装置。

【０２７４】

（５）前記データ処理部は、前記利用制御情報、または前記ブロックから取得した有効期限情報と現在日時情報との比較処理を行う際に、信頼できる時間情報提供サーバから取得した現在日時情報を適用した処理を行う前記（１）～（４）いずれかに記載の情報処理装置。

（６）前記暗号鍵格納ブロック、および前記ステータス格納ブロックは、前記メディアによるアクセス権判定に基づいてアクセスの認められるブロックであり、前記データ処理部は、前記暗号鍵格納ブロック、および前記ステータス格納ブロックからのデータ読み出し処理に際して、情報処理装置の証明書（Ｃｅｒｔｉｆｉｃａｔｅ）を前記メディアに送信し、前記メディアによるアクセス権判定処理によってデータ読み出し権利が確認されたことを条件として、データ読み出しを行う前記（１）～（５）いずれかに記載の情報処理装置。

【０２７５】

（７）前記ステータス格納ブロックは、前記メディアによるアクセス権判定に基づいてアクセスの認められるブロックであり、前記データ処理部は、前記ステータス格納ブロックに対するコンテンツ初回再生日時情報の記録処理に際して、情報処理装置の証明書（Ｃｅｒｔｉｆｉｃａｔｅ）を前記メディアに送信し、前記メディアによるアクセス権判定処理によってデータ書き込み処理の権利が確認されたことを条件として、データ記録を行う前記（１）～（６）いずれかに記載の情報処理装置。

（８）前記暗号鍵格納ブロックは、前記メディアによるアクセス権判定に基づいてアクセスの認められるブロックであり、前記ブロックに記録された有効期限情報は、前記暗号鍵格納ブロックに対するデータ書き込み処理の権利を有するサーバによって書き込みおよび更新が行われる情報である前記（１）～（７）いずれかに記載の情報処理装置。

【０２７６】

（９）　メディアに対するコンテンツ記録処理を行う情報処理装置であり、

前記メディアは、

暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納する汎用領域と、

前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コン

テンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記情報処理装置は、
前記汎用領域に対して、暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を記録する処理を行い、
前記暗号鍵格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの復号用の暗号鍵を記録し、
前記ステータス格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの初回再生時の日時情報を記録するためのコンテンツ対応ステータス情報記録領域を設定する処理を行う情報処理装置。

【０２７７】

（１０）前記情報処理装置は、前記利用制御情報に、前記暗号鍵格納ブロックの識別子と、前記ステータス格納ブロックの識別子を記録して前記メディアの汎用領域に記録する処理を行う前記（９）に記載の情報処理装置。
（１１）　前記暗号鍵を格納したブロックは、前記メディアによるアクセス権判定に基づいてアクセスの認められるブロックであり、
前記情報処理装置は、
前記ブロックに対するデータ記録処理に際して、情報処理装置の証明書（Ｃｅｒｔｉｆｉｃａｔｅ）を前記メディアに送信し、前記メディアによるアクセス権判定処理によってデータ記録処理の権利を有することが確認されたことを条件として、前記ブロックに対するデータ記録処理を行う前記（９）または（１０）に記載の情報処理装置。
（１２）前記情報処理装置は、前記メディアに記録されたコンテンツを他の第２メディアに移動する処理に際して、前記ステータス情報も併せて第２メディアに移動する処理を実行する前記（９）～（１１）いずれかに記載の情報処理装置。

【０２７８】

（１３）　暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納した汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記暗号化コンテンツの再生処理を実行する再生装置に、前記暗号鍵格納ブロックに記録された有効期限情報と、前記ステータス格納ブロックに記録されたコンテンツ対応ステータス情報の参照処理に基づいて、コンテンツ初回再生時の日時情報に応じて設定されるコンテンツ利用許容期限に基づくコンテンツ再生可否判定を行わせることを可能とした情報記憶装置。

【０２７９】

（１４）前記利用制御情報は、前記暗号鍵格納ブロックの識別子と、前記ステータス格納ブロックの識別子を記録した構成であり、前記暗号化コンテンツの再生処理を実行する再生装置に、前記利用制御情報に記録された各ブロック識別子の参照処理に基づくブロック特定処理を行わせることを可能とした前記（１３）に記載の情報記憶装置。
（１５）前記情報記憶装置は、前記保護領域のブロックに対するアクセス要求装置の証明書を取得し、取得した証明書に基づいてアクセス許容判定処理を行うデータ処理部を有する前記（１３）または（１４）に記載の情報記憶装置。

【０２８０】

（１６）　データを記録するメディアと、
前記メディアに格納されたコンテンツを再生する再生装置と、
前記メディアに対するデータ記録を行うサーバを有し、

前記メディアは、
暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を格納する汎用領域と、
前記暗号化コンテンツの復号用の暗号鍵と、該暗号鍵の適用コンテンツに適用されるコンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含むアクセス制限の設定された複数のブロックによって構成される保護領域を有し、
前記サーバは、
前記汎用領域に対して、暗号化コンテンツ、および該暗号化コンテンツ対応の利用制御情報を記録する処理を行い、
前記暗号鍵格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの復号用の暗号鍵を記録し、
前記ステータス格納ブロックに対して、前記汎用領域に記録した暗号化コンテンツの初回再生時の日時情報を記録するためのコンテンツ対応ステータス情報記録領域を設定する処理を行い、
前記再生装置は、
コンテンツ再生処理に際して、前記コンテンツ初回再生時の日時情報に応じて決定されるコンテンツ利用許容期間である有効期限情報を前記暗号鍵格納ブロックから取得し、取得した有効期限情報と現在日時情報との比較により、コンテンツ再生の可否を判定する情報処理システム。

【０２８１】
さらに、上記した装置およびシステムにおいて実行する処理の方法や、処理を実行させるプログラムも本開示の構成に含まれる。

【０２８２】
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。

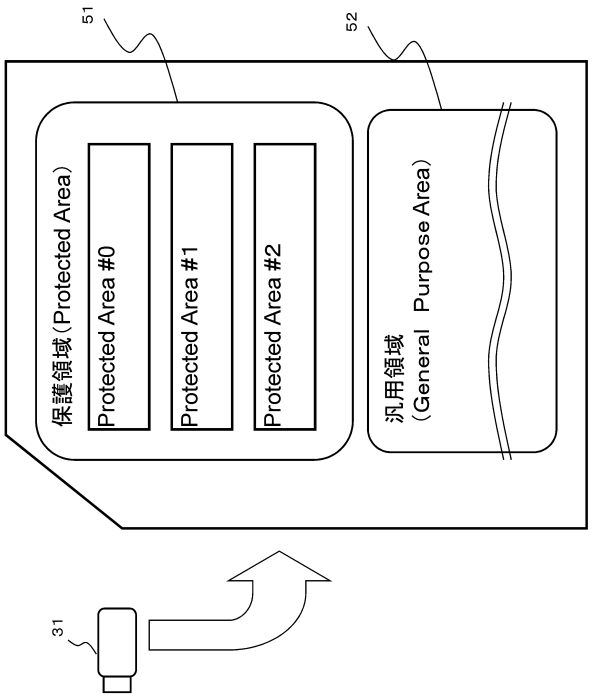
【０２８３】
なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【産業上の利用可能性】

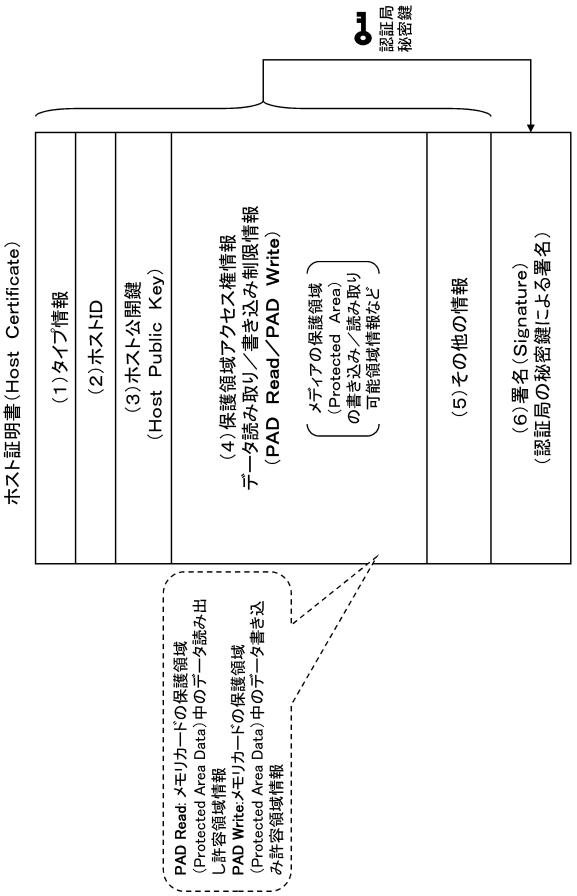
【０２８４】
以上、説明したように、本開示の一実施例の構成によれば、コンテンツ初回再生日時に応じた利用期限の設定を可能とした装置、方法が実現される。
具体的には、コンテンツと利用制御情報を格納した汎用領域と、コンテンツ復号用の暗号鍵と、コンテンツ利用許容期間である有効期限情報を格納した暗号鍵格納ブロック、および、コンテンツ初回再生時の日時情報をコンテンツ対応ステータス情報として格納するステータス格納ブロックを含む複数ブロックによって構成される保護領域を有するメディアに格納されたコンテンツを再生する。再生装置は、コンテンツ初回再生時の日時情報に応じて決定されるコンテンツ利用許容期間である有効期限情報を暗号鍵格納ブロックから取得し、取得した有効期限情報と現在日時情報との比較により、コンテンツ再生の可否を

判定する。
　これらの処理によって、コンテンツ初回再生日時に応じた利用期限の設定を可能とした装置、方法が実現される。
【符号の説明】
【０２８５】
　１１　放送局
　１２　コンテンツサーバ
　２１　記録再生専用器
　２２　ＰＣ
　２３　携帯端末
　３１　メモリカード
　５１　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
　５２　汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）
　６１　サーバＡ
　６２　サーバＢ
　６３　ホスト
　６４　サーバＣ
　６５　サーバＤ
　８１　ブロック＃０
　８２　ブロック＃１
　９０　汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）
３０１　ムーブ元メディア
３０２　ムーブ先メディア
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　汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）

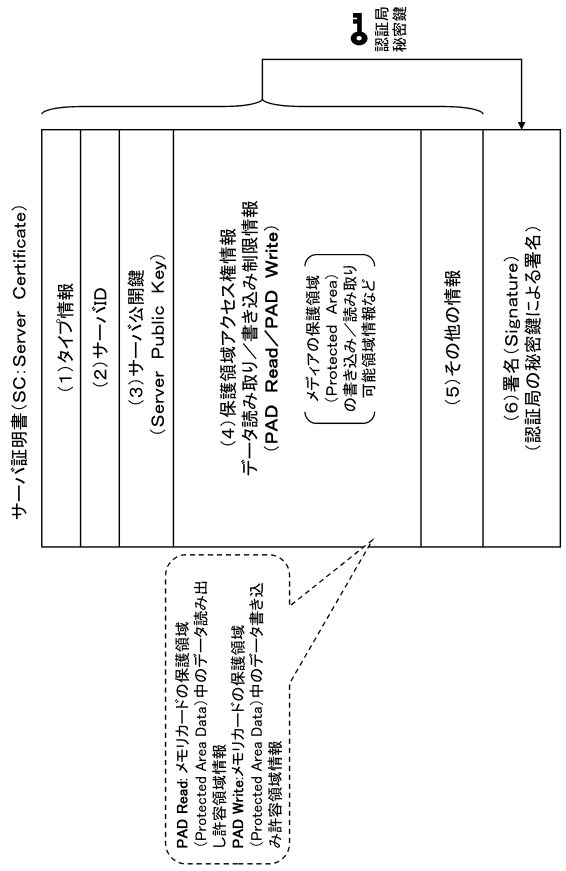
【図３】


保護領域(Protected Area)
Protected Area #0
Protected Area #1
Protected Area #2
汎用領域
(General Purpose Area)
51
52
31

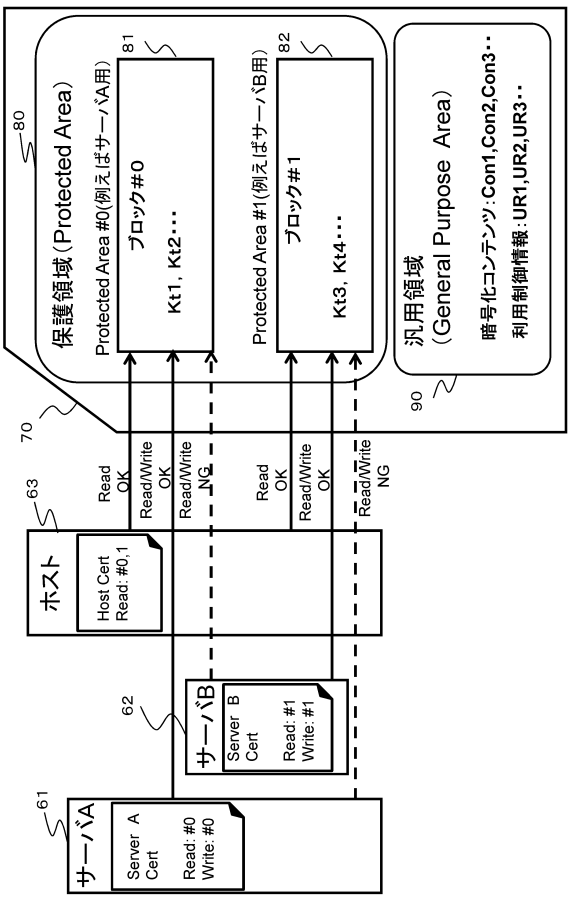
【図４】


ホスト証明書(Host Certificate)
(1)タイプ情報
(2)ホストID
(3)ホスト公開鍵
(Host Public Key)
(4)保護領域アクセス権情報
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
(5)その他の情報
(6)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

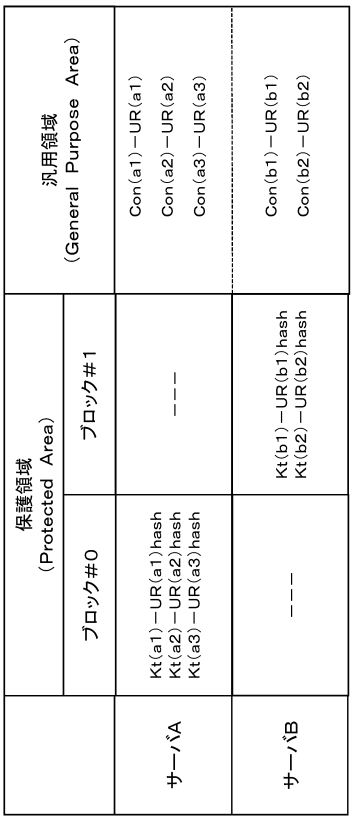
【図５】


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)保護領域アクセス権情報
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
(5)その他の情報
(6)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】

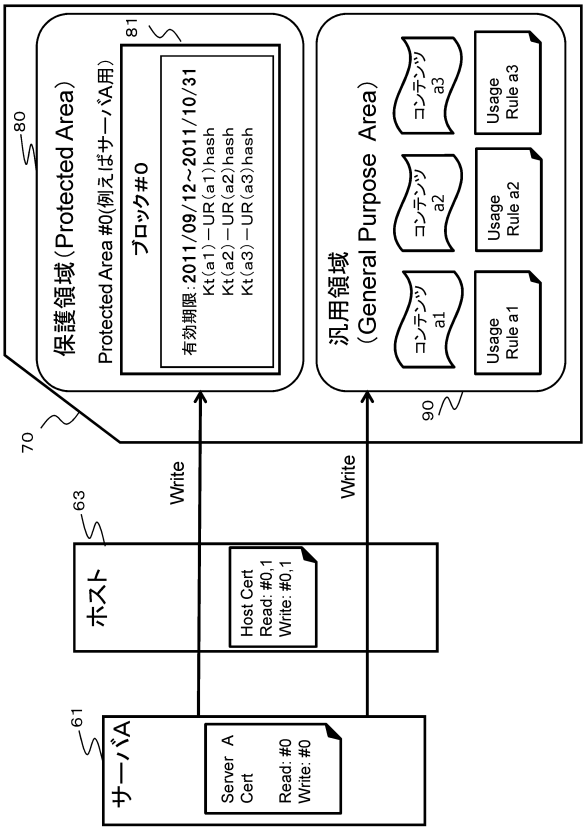

保護領域(Protected Area)
Protected Area #0(例えばサーバA用)
ブロック#0
Kt1, Kt2・・・
Protected Area #1(例えばサーバB用)
ブロック#1
Kt3, Kt4・・・
汎用領域
(General Purpose Area)
暗号化コンテンツ:Con1,Con2,Con3・・
利用制御情報:UR1,UR2,UR3・・
80
81
82
90
70
ホスト
Host Cert
Read: #0,1
63
サーバB
Server B
Cert
Read: #1
Write: #1
62
サーバA
Server A
Cert
Read: #0
Write: #0
61
Read
OK
Read/Write
OK
Read/Write
NG
Read
OK
Read/Write
OK
Read/Write
NG

【図７】

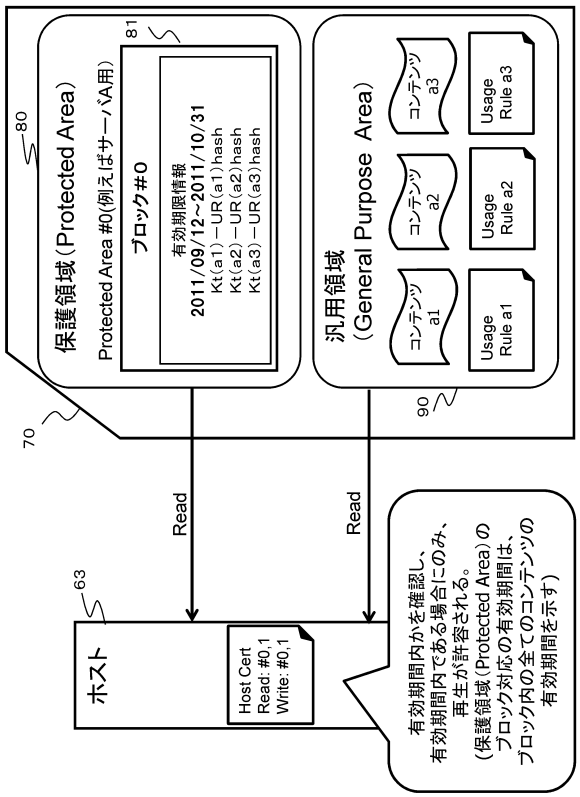


	保護領域 (Protected Area)		汎用領域 (General Purpose Area)
	ブロック#0	ブロック#1	
サーバA	Kt(a1)－UR(a1)hash Kt(a2)－UR(a2)hash Kt(a3)－UR(a3)hash	－ － －	Con(a1)－UR(a1) Con(a2)－UR(a2) Con(a3)－UR(a3)
サーバB	－ － －	Kt(b1)－UR(b1)hash Kt(b2)－UR(b2)hash	Con(b1)－UR(b1) Con(b2)－UR(b2)

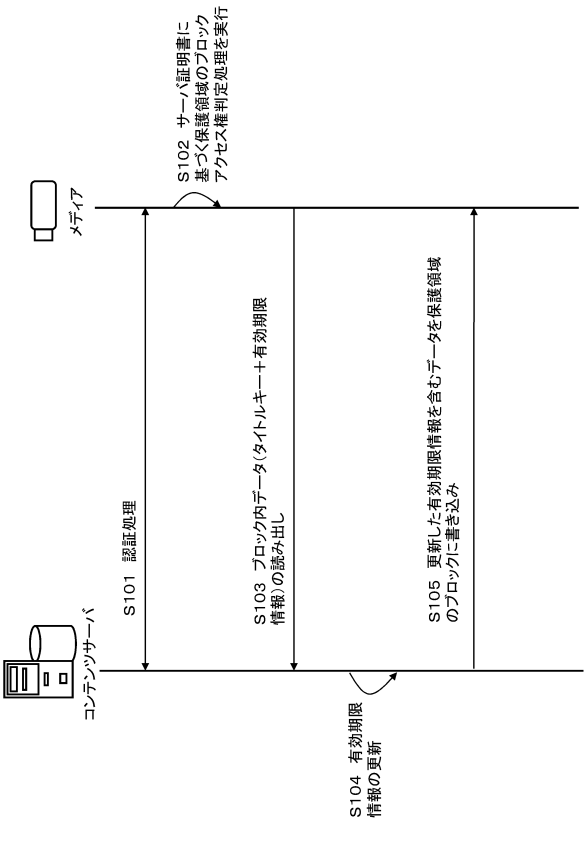
【図８】



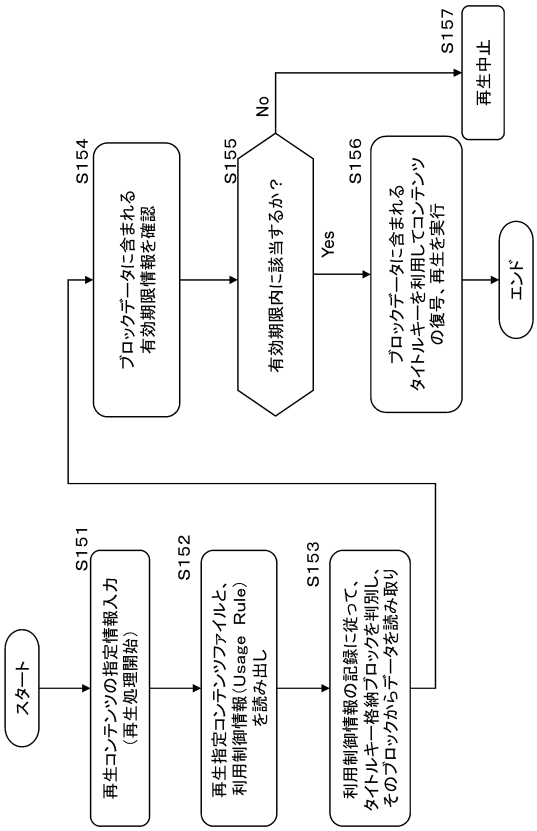
【図９】



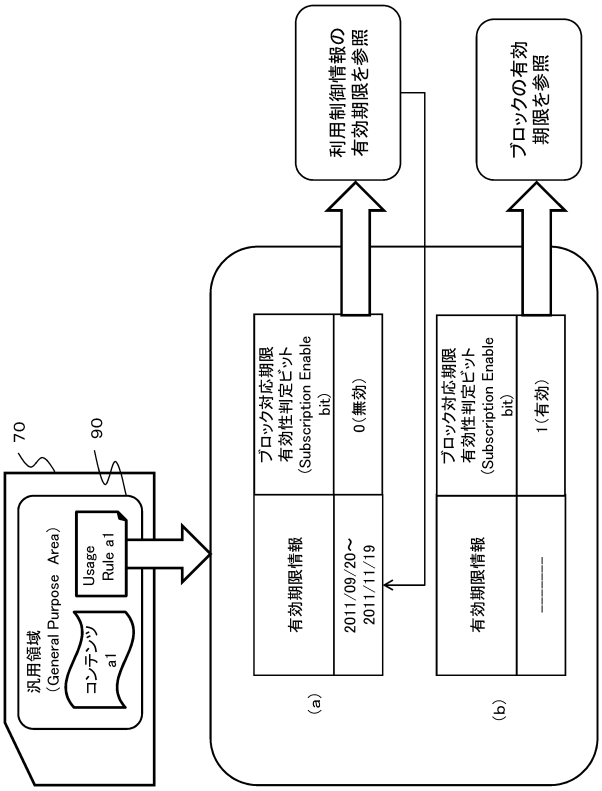
【図１０】



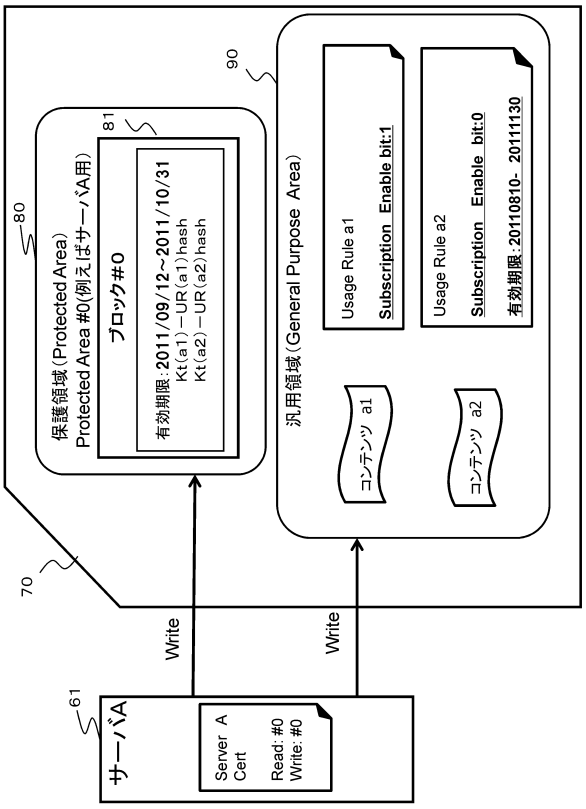
【図１１】



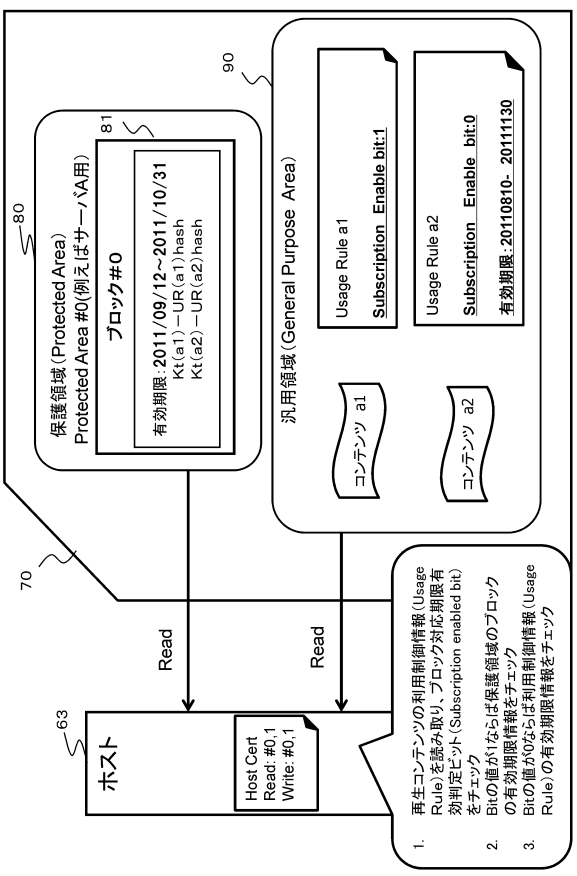
【図１２】



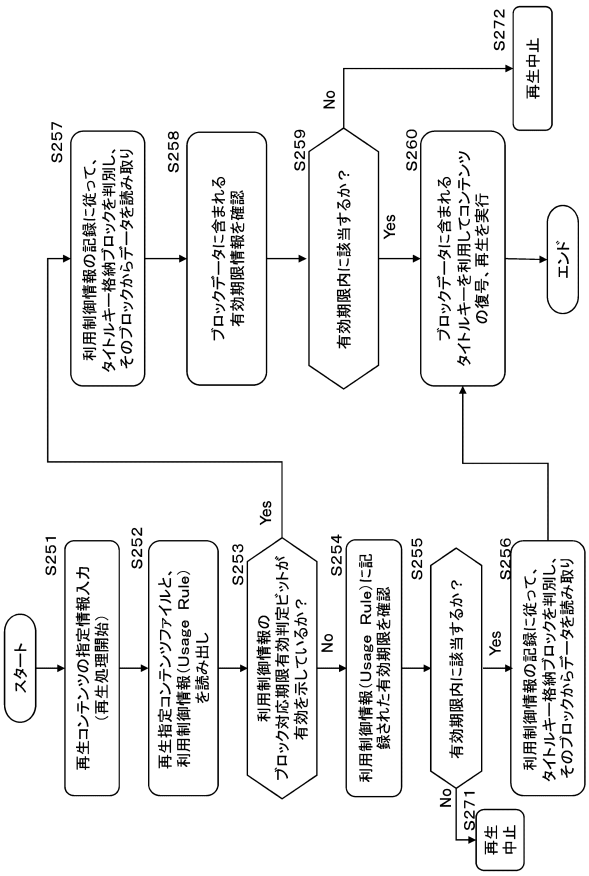
【図１３】



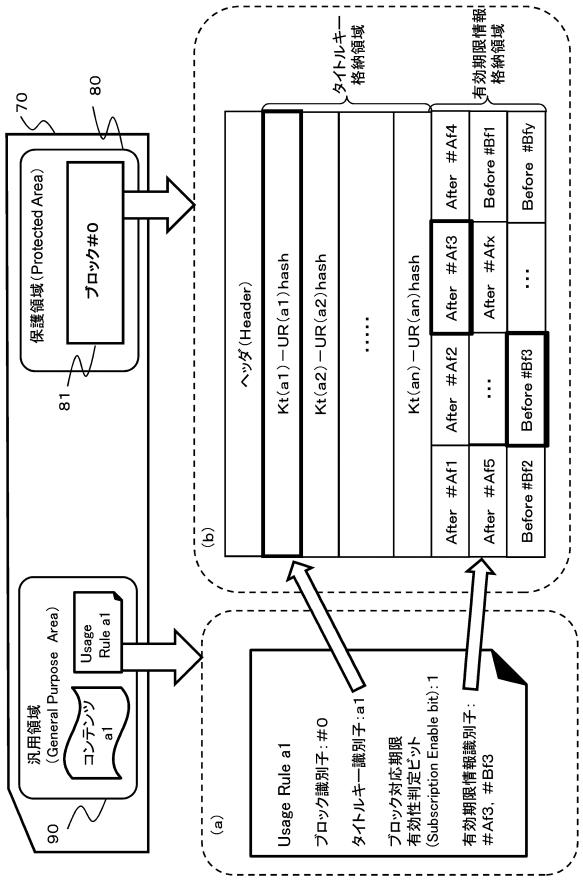
【図１４】



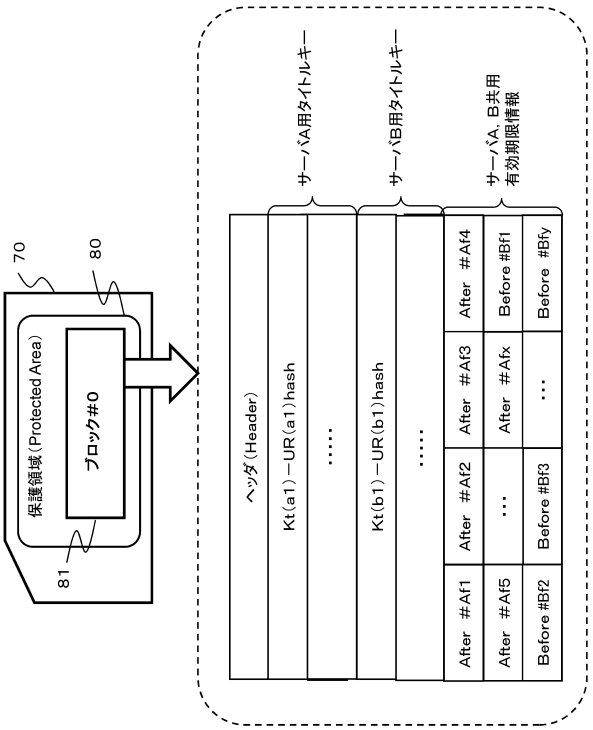
【図１５】



【図１６】



【図１７】

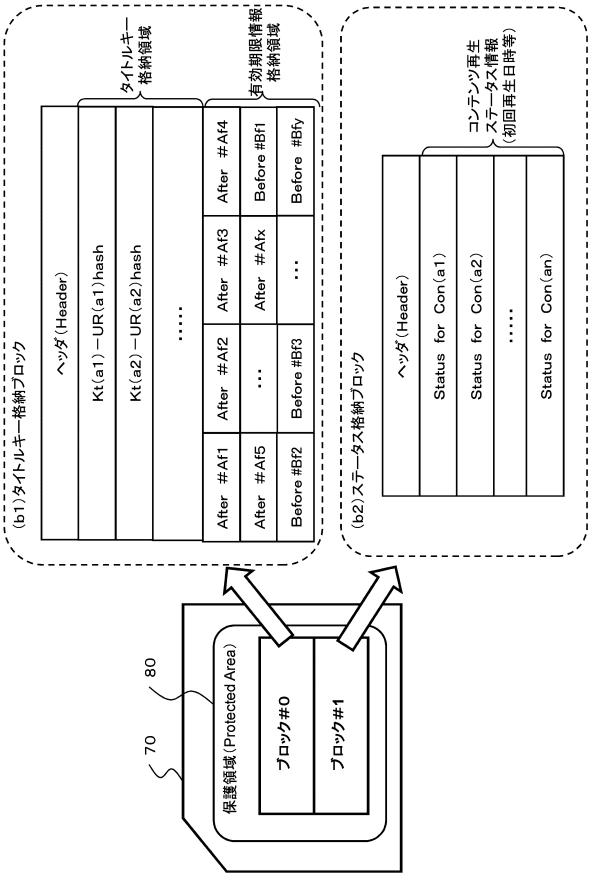


【図１８】

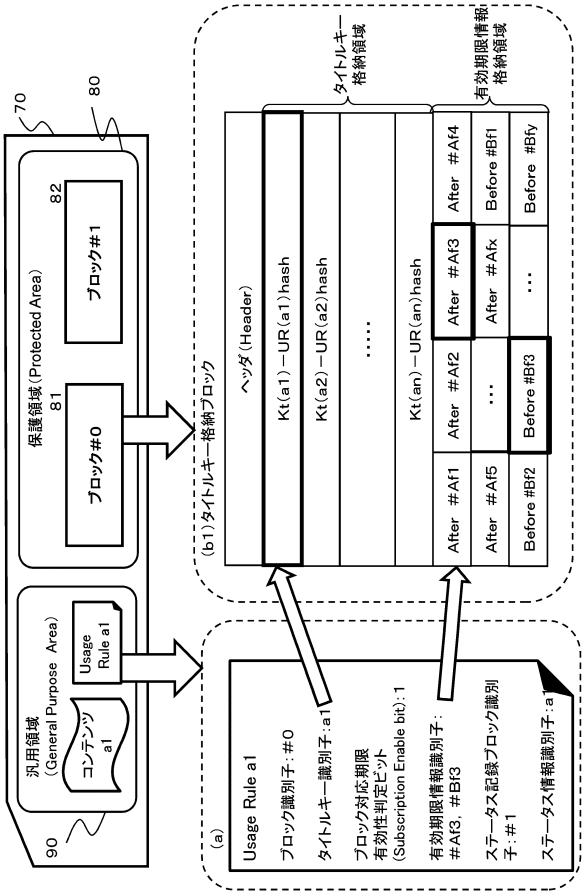
【図１９】

	保護領域 (Protected Area)		汎用領域 (General Purpose Area)
	ブロック#0	ブロック#1	
サーバA	Kt(a1)−UR(a1)hash Kt(a2)−UR(a2)hash Kt(a3)−UR(a3)hash	− − −	Con(a1)−UR(a1) Con(a2)−UR(a2) Con(a3)−UR(a3)
サーバB	Kt(b1)−UR(b1)hash Kt(b2)−UR(b2)hash	− − −	Con(b1)−UR(b1) Con(b2)−UR(b2)
サーバC	− − −	Kt(c1)−UR(c1)hash	Con(c1)−UR(c1)
サーバD	− − −	Kt(d1)−UR(d1)hash Kt(d2)−UR(d2)hash	Con(d1)−UR(d1) Con(d2)−UR(d2)

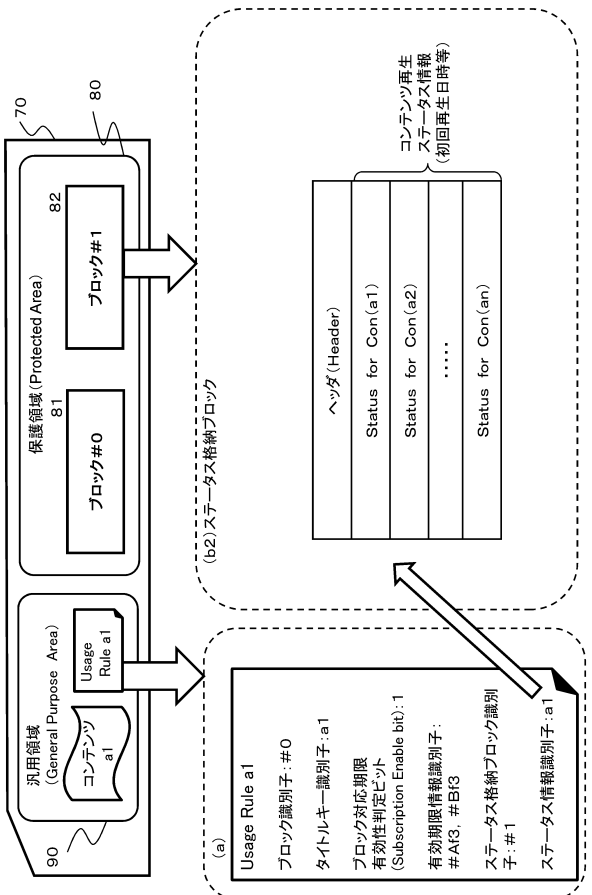
【図２０】



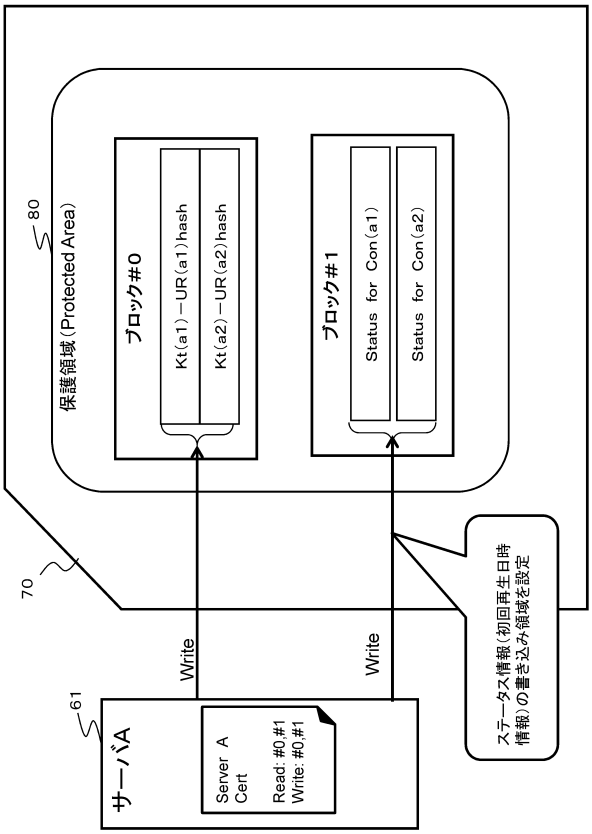
【図２１】



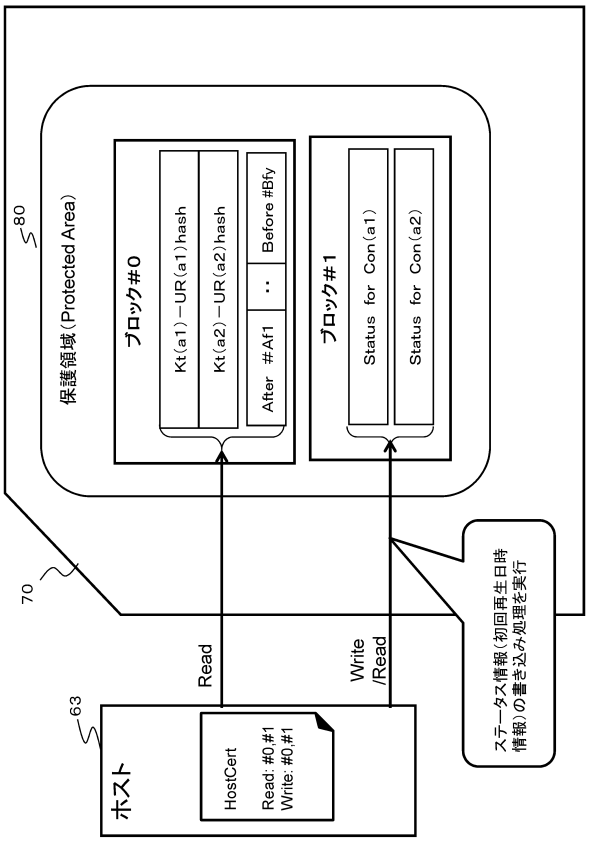
【図２２】



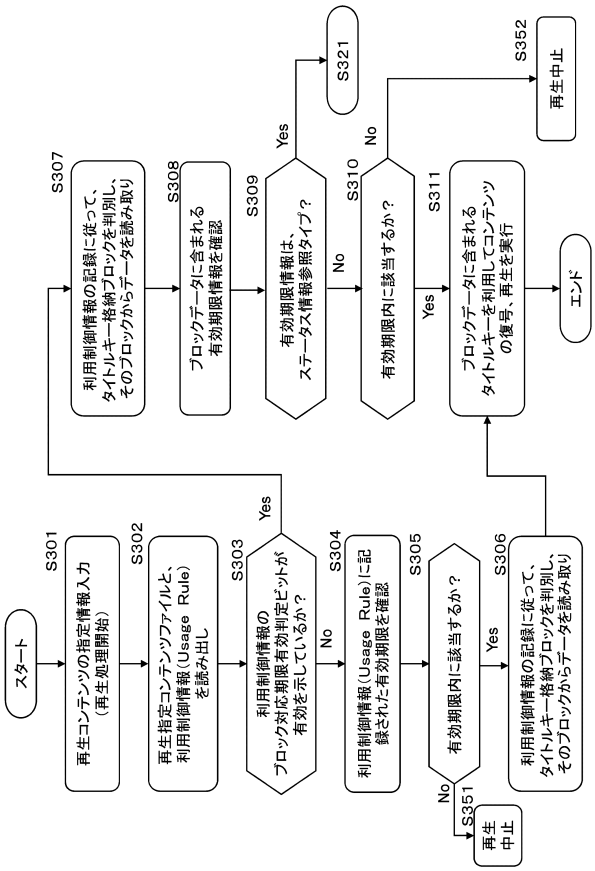
【図２３】



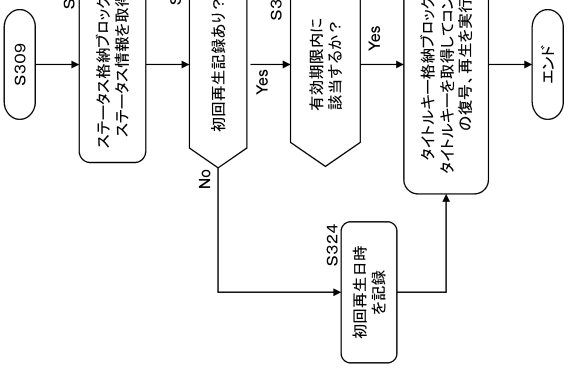
【図２４】



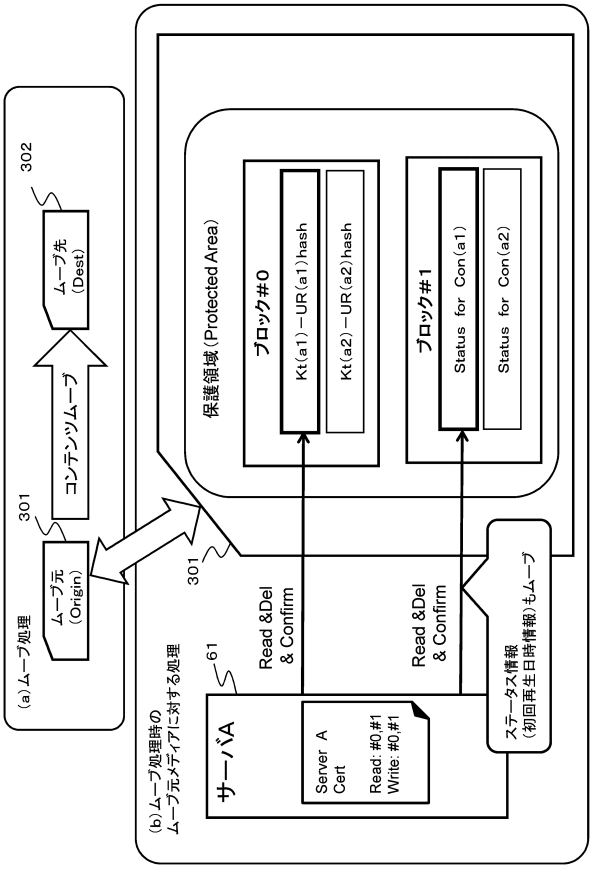
【図２５】



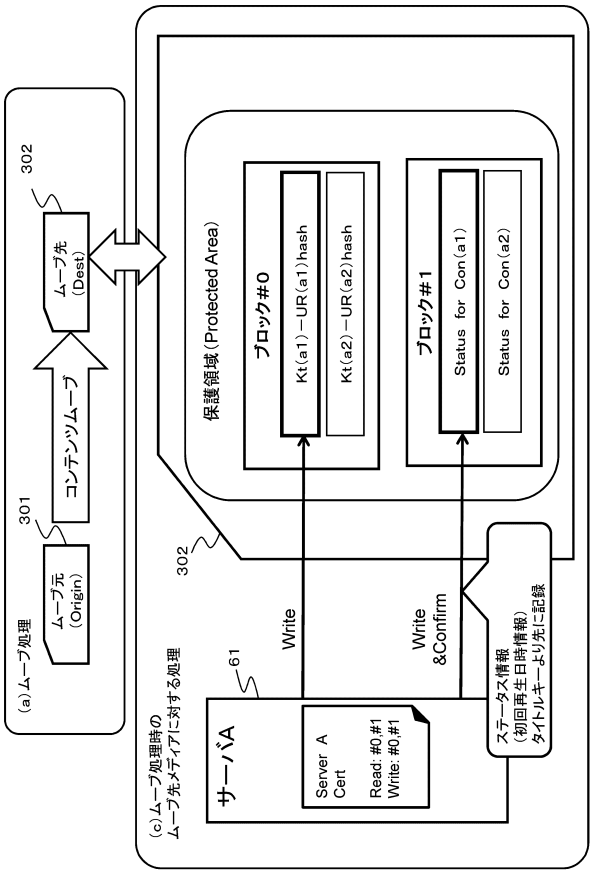
【図２６】



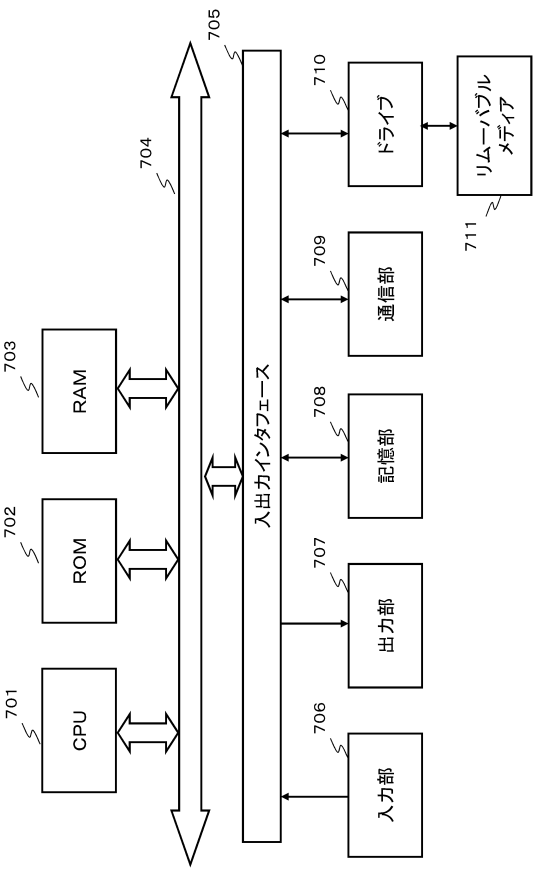
【図２７】



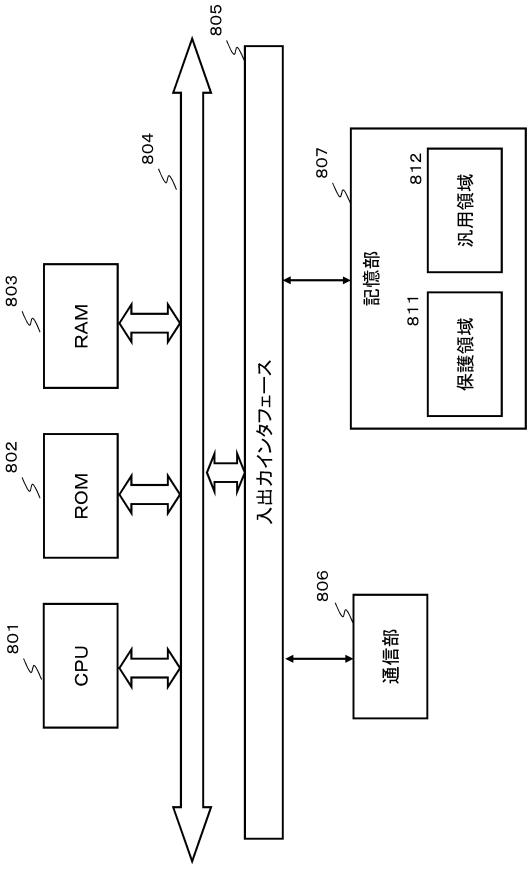
【図２８】



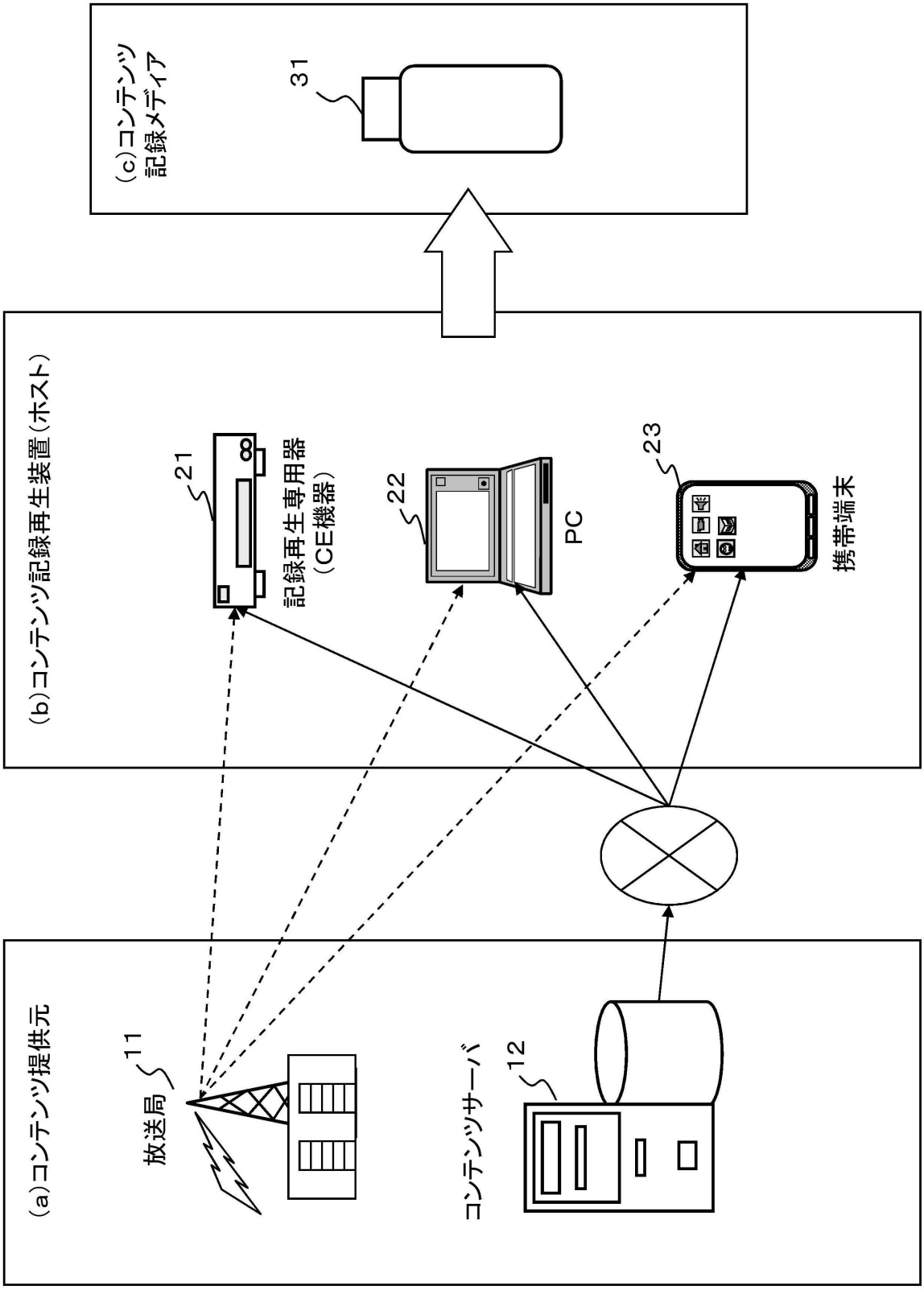
【図２９】



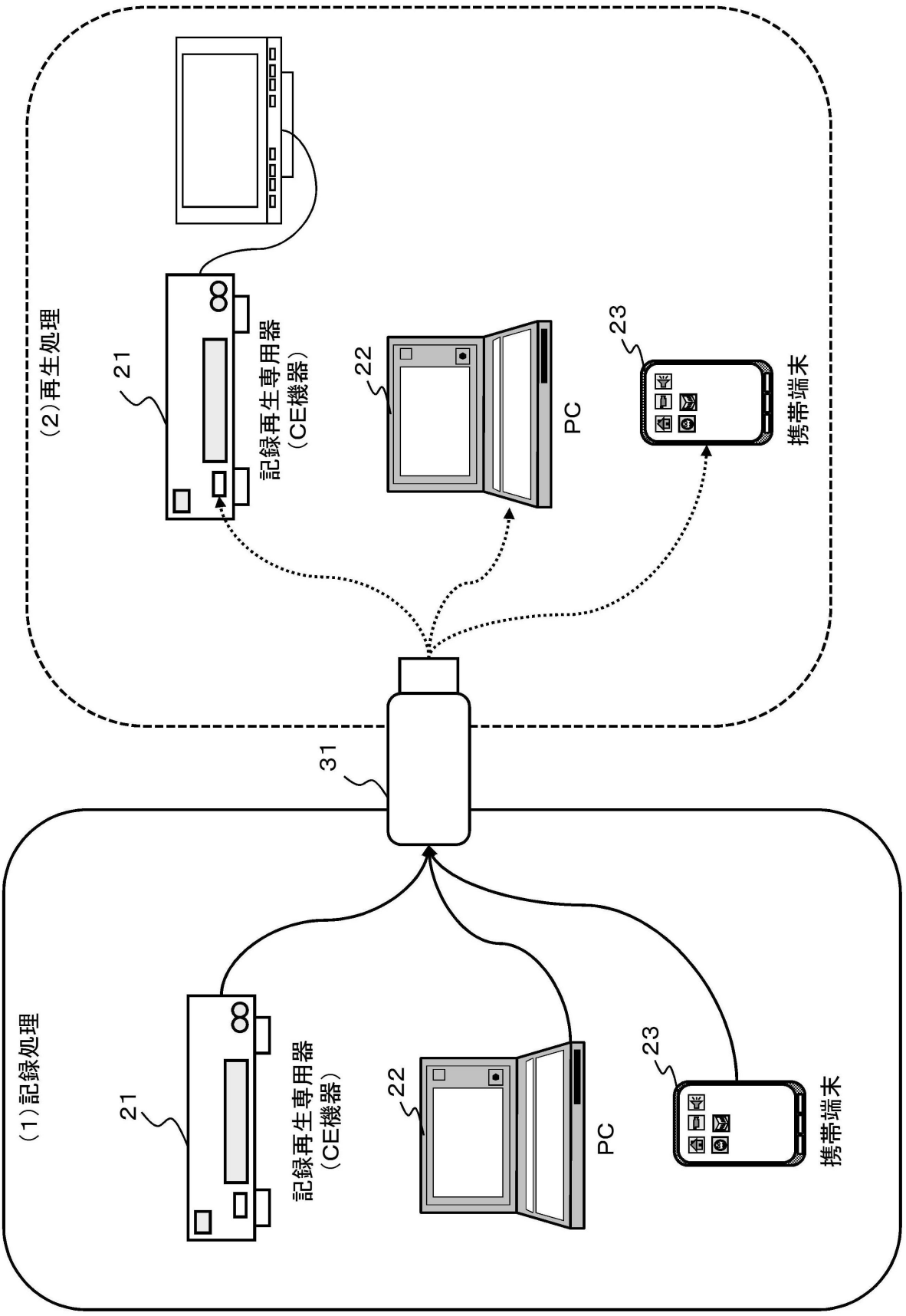
【図３０】



【図１】


(c)コンテンツ
記録メディア
31
(b)コンテンツ記録再生装置(ホスト)
21
記録再生専用器
(CE機器)
22
PC
23
携帯端末
(a)コンテンツ提供元
放送局
11
コンテンツサーバ
12

【図２】


(1)記録処理
21
記録再生専用器
(CE機器)
22
PC
23
携帯端末
31
(2)再生処理
21
記録再生専用器
(CE機器)
22
PC
23
携帯端末

フロントページの続き

(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　小林　義行
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　村松　克美
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　宮司　卓佳

(56)参考文献　特開２００３－１１４８３０（ＪＰ，Ａ）
特開２００９－３０３１８７（ＪＰ，Ａ）
特表２００９－５４３２１２（ＪＰ，Ａ）
特開２０１０－２３８３３４（ＪＰ，Ａ）
特開２００７－２５７６１６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／００－２１／８８
Ｇ０６Ｆ１２／１４