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

特許第5573489号
(P5573489)

(45)発行日　平成26年8月20日(2014.8.20)　(24)登録日　平成26年7月11日(2014.7.11)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601B
H04L	9/14	(2006.01)	H04L	9/00	641
G06F	21/16	(2013.01)	H04L	9/00	601E
G06F	21/62	(2013.01)	G06F	21/22	116
			G06F	21/24	166A

請求項の数 15　(全 44 頁)

(21)出願番号　特願2010-185833(P2010-185833)
(22)出願日　平成22年8月23日(2010.8.23)
(65)公開番号　特開2012-44577(P2012-44577A)
(43)公開日　平成24年3月1日(2012.3.1)
審査請求日　平成25年7月29日(2013.7.29)

(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】
コンテンツ記録装置における記録メディアに対するコンテンツ記録処理に適用する暗号鍵であり、コンテンツ記録装置およびコンテンツに対応する固有の暗号鍵を生成するデータ処理部と、
前記データ処理部の生成した暗号鍵を送信する通信部を有し、
前記データ処理部は、
前記暗号鍵として、コンテンツ記録装置における記録メディアに対する新たなコンテンツ記録処理ごと異なる個別鍵であり、コンテンツ記録装置および暗号化対象とするコンテンツ固有の個別鍵を生成して前記通信部を介して送信し、
前記通信部を介して送信した個別鍵と、該個別鍵の暗号化対象となるコンテンツと、該個別鍵の送信先情報を対応付けた管理情報を生成して記憶部に格納する情報処理装置。
【請求項２】
前記記録メディアは、アクセス制限のある保護領域を有する記録メディアであり、
前記データ処理部は、
前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域に対する書き込みを実行する構成である請求項１に記載の情報処理装置。
【請求項３】
前記データ処理部は、

前記コンテンツ記録装置に対して、前記個別鍵による暗号化処理を行うコンテンツを送信する請求項１または２に記載の情報処理装置。
【請求項４】
前記データ処理部は、
前記コンテンツ記録装置が、既にコンテンツが記録された情報記録媒体から、前記記録メディアに対してコンテンツのコピー処理を実行する際に、コピー対象となるコンテンツの暗号化処理用の鍵として前記個別鍵を送信する請求項１または２に記載の情報処理装置。
【請求項５】
前記データ処理部は、
前記個別鍵を乱数生成処理により生成する請求項１に記載の情報処理装置。
【請求項６】
前記データ処理部は、
前記個別鍵を、前記コンテンツ記録装置または記録メディアと対応付けた管理情報を生成して記憶部に格納する処理を行う請求項１に記載の情報処理装置。
【請求項７】
記録メディアに対するコンテンツ記録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、
前記記録メディアに設定されたアクセス制限領域である保護領域に記録された個別鍵であり、コンテンツ記録装置および暗号化対象とするコンテンツ固有の個別鍵を読み出し、前記個別鍵を適用してサーバからの受信コンテンツまたは情報記録媒体からの読み出しコンテンツの暗号化処理を実行して前記記録メディアに対する記録処理を実行する構成であり、
前記個別鍵の読み出し処理に際して、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域からの読み出しを実行する情報処理装置。
【請求項８】
記録メディアに記録された暗号化コンテンツの復号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、
前記記録メディアに設定されたアクセス制限領域である保護領域に記録された個別鍵であり、コンテンツ記録装置およびコンテンツ固有の個別鍵を読み出し、前記個別鍵を適用して前記暗号化コンテンツの復号処理を実行する構成であり、
前記個別鍵の読み出し処理に際して、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域からの読み出しを実行する情報処理装置。
【請求項９】
記録メディアと、
前記記録メディアに対するコンテンツ記録処理を実行する記録装置と、
前記コンテンツの暗号鍵を提供するサーバからなるコンテンツ管理システムであり、
前記サーバは、前記コンテンツ記録装置における記録メディアに対する新たなコンテンツ記録処理ごと異なる個別鍵であり、記録装置および暗号化対象とするコンテンツ固有の個別鍵を生成して前記記録メディアのアクセス制限のある保護領域に記録し、
前記通信部を介して送信した個別鍵と、該個別鍵の暗号化対象となるコンテンツと、該個別鍵の送信先情報を対応付けた管理情報を生成して記憶部に格納し、
前記記録装置は、前記保護領域に記録された個別鍵であり、記録装置および暗号化対象とするコンテンツ固有の個別鍵を読み出し、前記個別鍵を適用してサーバからの受信コンテンツまたは情報記録媒体からの読み出しコンテンツの暗号化処理を実行して前記記録メディアに対する記録処理を実行する構成であり、
前記記録メディアは、前記サーバおよび前記記録装置からの保護領域に対するアクセス

要求に応じて各装置のアクセス許容情報を記録した証明書の記録情報を確認し、アクセス権限があることを確認した場合にアクセスを許容する処理を行うコンテンツ管理システム。

【請求項１０】
サーバにおいて実行する情報処理方法であり、
データ処理部が、コンテンツ記録装置における記録メディアに対するコンテンツ記録処理に適用する暗号鍵であり、コンテンツ記録装置およびコンテンツに対応する固有の暗号鍵を生成するデータ処理ステップと、
通信部が、前記データ処理部の生成した暗号鍵を送信する通信ステップを実行し、
前記データ処理ステップは、
前記暗号鍵として、コンテンツ記録装置における記録メディアに対する新たなコンテンツ記録処理ごと異なる個別鍵であり、コンテンツ記録装置および暗号化対象とするコンテンツ固有の個別鍵を生成して前記通信部を介して送信し、
前記通信部を介して送信した個別鍵と、該個別鍵の暗号化対象となるコンテンツと、該個別鍵の送信先情報を対応付けた管理情報を生成して記憶部に格納する情報処理方法。

【請求項１１】
情報記録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、記録メディアに対するコンテンツ記録処理を実行するデータ処理ステップを有し、
前記データ処理ステップは、
前記記録メディアに設定されたアクセス制限領域である保護領域に記録された個別鍵であり、コンテンツ記録装置および暗号化対象とするコンテンツ固有の個別鍵を読み出し、前記個別鍵を適用してサーバからの受信コンテンツまたは情報記録媒体からの読み出しコンテンツの暗号化処理を実行して前記記録メディアに対する記録処理を実行するステップであり、
前記個別鍵の読み出し処理に際して、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域からの読み出しを実行する情報処理方法。

【請求項１２】
情報記再生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、記録メディアに記録された暗号化コンテンツの復号処理を実行するデータ処理ステップを有し、
前記データ処理ステップは、
前記記録メディアに設定されたアクセス制限領域である保護領域に記録された個別鍵であり、コンテンツ記録装置およびコンテンツ固有の個別鍵を読み出し、前記個別鍵を適用して前記暗号化コンテンツの復号処理を実行するステップであり、
前記個別鍵の読み出し処理に際して、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域からの読み出しを実行する情報処理方法。

【請求項１３】
サーバ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、コンテンツ記録装置における記録メディアに対するコンテンツ記録処理に適用する暗号鍵であり、コンテンツ記録装置およびコンテンツに対応する固有の暗号鍵を生成させるデータ処理ステップと、
通信部に、前記データ処理部の生成した暗号鍵を送信させる通信ステップを実行させ、
前記データ処理ステップにおいては、
前記暗号鍵として、コンテンツ記録装置における記録メディアに対する新たなコンテンツ記録処理ごと異なる個別鍵であり、コンテンツ記録装置および暗号化対象とするコンテンツ固有の個別鍵を生成して前記通信部を介して送信させ、
前記通信部を介して送信した個別鍵と、該個別鍵の暗号化対象となるコンテンツと、該

個別鍵の送信先情報を対応付けた管理情報を生成して記憶部に格納させるプログラム。
【請求項１４】
情報記録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、記録メディアに対するコンテンツ記録処理を実行させるデータ処理ステップを有し、
前記データ処理ステップは、
前記記録メディアに設定されたアクセス制限領域である保護領域に記録された個別鍵であり、コンテンツ記録装置および暗号化対象とするコンテンツ固有の個別鍵を読み出し、前記個別鍵を適用してサーバからの受信コンテンツまたは情報記録媒体からの読み出しコンテンツの暗号化処理を実行して前記記録メディアに対する記録処理を実行させるステップであり、
前記個別鍵の読み出し処理に際して、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域からの読み出しを実行させるプログラム。
【請求項１５】
情報記再生置において情報処理を実行させるプログラムであり、
データ処理部にが、記録メディアに記録された暗号化コンテンツの復号処理を実行させるデータ処理ステップを有し、
前記データ処理ステップは、
前記記録メディアに設定されたアクセス制限領域である保護領域に記録された個別鍵であり、コンテンツ記録装置およびコンテンツ固有の個別鍵を読み出し、前記個別鍵を適用して前記暗号化コンテンツの復号処理を実行させるステップであり、
前記個別鍵の読み出し処理に際して、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域からの読み出し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、コンテンツの不正利用の防止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】
また、近年、ネットワークを介したコンテンツの流通が盛んになり、ユーザによるコンテンツ購入処理の形態は、コンテンツを予め記録したディスクの購入処理から、ネットワーク接続したサーバからダウンロードする処理に次第にシフトしている。
【０００４】
具体的なコンテンツ購入形態としては、ＲＯＭディスク等のメディアの購入を行う処理の他、例えば、以下のようなコンテンツ購入形態がある。
（ａ）ネットワーク接続可能な端末やＰＣ等のユーザ装置を利用してコンテンツ提供サーバに接続して、コンテンツをダウンロードして購入するＥＳＴ（Ｅｌｅｃｔｒｉｃ　Ｓｅｌｌ　Ｔｈｒｏｕｇｈ）。
（ｂ）コンビニや、駅等の公共スペースに設置された共用端末を利用して、ユーザのメ

ディア（メモリカード等）にコンテンツを記録するＭｏＤ（Ｍａｎｕｆａｃｔｕｒｉｎｇ　ｏｎ　Ｄｅｍａｎｄ）。

【０００５】

このように、ユーザは、コンテンツ記録用のメモリカードなどのメディアを有していれば、様々なコンテンツ提供プロバイダ等のコンテンツソースから自由に様々なコンテンツを選択購入し、自分のメディアに記録することができる。

なお、ＥＳＴ、ＭｏＤ等の処理については、例えば特許文献１（特開２００８－９８７６５号公報）に記載されている。

【０００６】

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。

【０００７】

具体的には、ユーザが映画等のコンテンツをサーバからダウンロードしてユーザのメモリカード等の記録メディアに記録する場合、例えば以下のような処理が行われる。

サーバはコンテンツを暗号化コンテンツとしてクライアント（ユーザ装置）に提供する。

さらに、正規なコンテンツ購入処理を行ったユーザにのみ、暗号化コンテンツを復号するための鍵を提供する。

このようなコンテンツ提供処理を行うことで、コンテンツの利用制御を実現しようとしている。

【０００８】

しかし、上述の処理を行っても、例えば、正規なコンテンツ購入処理を行ったユーザが、サーバから取得したコンテンツ復号用の鍵を、他人に提供してしまうことを防止することは難しい。具体的には、サーバから取得した鍵をネット上で公開するなどして、不特定多数のユーザが利用可能な状態に設定されることも想定される。このような行為が行われると、この流出鍵を用いて誰でも暗号化コンテンツの復号、再生、利用を行うことが可能となり、コンテンツの不正利用が蔓延するといった事態が発生する。

【先行技術文献】

【特許文献】

【０００９】

【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】

【００１０】

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、暗号化コンテンツの復号に利用される鍵の流出によるコンテンツ不正利用を効果的に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】

【００１１】

本発明の第１の側面は、

コンテンツの暗号鍵を生成するデータ処理部と、

前記データ処理部の生成した暗号鍵を送信する通信部を有し、

前記データ処理部は、

前記暗号鍵として、コンテンツ記録装置における記録メディアに対する新たなコンテンツ記録処理ごと異なる個別鍵を生成して前記通信部を介して送信する情報処理装置にある。

【００１２】

さらに、本発明の情報処理装置の一実施態様において、前記記録メディアは、アクセス制限のある保護領域を有する記録メディアであり、前記データ処理部は、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域に対する書き込みを実行する構成である。

【００１３】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記コンテンツ記録装置に対して、前記個別鍵による暗号化処理を行うコンテンツを送信する。

【００１４】

さらに、本発明の情報処理装置の一実施態様において、前記データ処理部は、前記コンテンツ記録装置が、既にコンテンツが記録された情報記録媒体から、前記記録メディアに対してコンテンツのコピー処理を実行する際に、コピー対象となるコンテンツの暗号化処理用の鍵として前記個別鍵を送信する。

【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、前記個別鍵を乱数生成処理により生成する。

【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、前記個別鍵を、前記コンテンツ記録装置または記録メディアと対応付けた管理情報を生成して記憶部に格納する処理を行う。

【００１７】

さらに、本発明の第２の側面は、

記録メディアに対するコンテンツ記録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、

前記記録メディアに設定されたアクセス制限領域である保護領域に記録された個別鍵を読み出し、前記個別鍵を適用してサーバからの受信コンテンツまたは情報記録媒体からの読み出しコンテンツの暗号化処理を実行して前記記録メディアに対する記録処理を実行する構成であり、

前記個別鍵の読み出し処理に際して、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域からの読み出しを実行する情報処理装置にある。

【００１８】

さらに、本発明の第３の側面は、

記録メディアに記録された暗号化コンテンツの復号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、

前記記録メディアに設定されたアクセス制限領域である保護領域に記録された個別鍵を読み出し、前記個別鍵を適用して前記暗号化コンテンツの復号処理を実行する構成であり、

前記個別鍵の読み出し処理に際して、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域からの読み出しを実行する情報処理装置にある。

【００１９】

さらに、本発明の第４の側面は、

記録メディアと、

前記記録メディアに対するコンテンツ記録処理を実行する記録装置と、

前記コンテンツの暗号鍵を提供するサーバからなるコンテンツ管理システムであり、

前記サーバは、前記コンテンツ記録装置における記録メディアに対する新たなコンテン

ツ記録処理ごと異なる個別鍵を生成して前記記録メディアのアクセス制限のある保護領域に記録し、
前記記録装置は、前記保護領域に記録された個別鍵を読み出し、前記個別鍵を適用してサーバからの受信コンテンツまたは情報記録媒体からの読み出しコンテンツの暗号化処理を実行して前記記録メディアに対する記録処理を実行する構成であり、
前記記録メディアは、前記サーバおよび前記記録装置からの保護領域に対するアクセス要求に応じて各装置のアクセス許容情報を記録した証明書の記録情報を確認し、アクセス権限があることを確認した場合にアクセスを許容する処理を行うコンテンツ管理システムにある。

【００２０】
さらに、本発明の第５の側面は、
サーバにおいて実行する情報処理方法であり、
データ処理部が、コンテンツの暗号鍵を生成するデータ処理ステップと、
通信部が、前記データ処理部の生成した暗号鍵を送信する通信ステップを実行し、
前記データ処理ステップは、
前記暗号鍵として、コンテンツ記録装置における記録メディアに対する新たなコンテンツ記録処理ごと異なる個別鍵を生成して前記通信部を介して送信する情報処理方法にある。

【００２１】
さらに、本発明の第６の側面は、
情報記録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、記録メディアに対するコンテンツ記録処理を実行するデータ処理ステップを有し、
前記データ処理ステップは、
前記記録メディアに設定されたアクセス制限領域である保護領域に記録された個別鍵を読み出し、前記個別鍵を適用してサーバからの受信コンテンツまたは情報記録媒体からの読み出しコンテンツの暗号化処理を実行して前記記録メディアに対する記録処理を実行するステップであり、
前記個別鍵の読み出し処理に際して、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域からの読み出しを実行する情報処理方法にある。

【００２２】
さらに、本発明の第７の側面は、
情報記再生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、記録メディアに記録された暗号化コンテンツの復号処理を実行するデータ処理ステップを有し、
前記データ処理ステップは、
前記記録メディアに設定されたアクセス制限領域である保護領域に記録された個別鍵を読み出し、前記個別鍵を適用して前記暗号化コンテンツの復号処理を実行するステップであり、
前記個別鍵の読み出し処理に際して、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域からの読み出しを実行する情報処理方法にある。

【００２３】
さらに、本発明の第８の側面は、
サーバ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、コンテンツの暗号鍵を生成させるデータ処理ステップと、
通信部に、前記データ処理部の生成した暗号鍵を送信させる通信ステップを実行させ、

前記データ処理ステップにおいては、
前記暗号鍵として、コンテンツ記録装置における記録メディアに対する新たなコンテンツ記録処理ごと異なる個別鍵を生成して前記通信部を介して送信させるプログラムにある。

【００２４】
さらに、本発明の第９の側面は、
情報記録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、記録メディアに対するコンテンツ記録処理を実行させるデータ処理ステップを有し、
前記データ処理ステップは、
前記記録メディアに設定されたアクセス制限領域である保護領域に記録された個別鍵を読み出し、前記個別鍵を適用してサーバからの受信コンテンツまたは情報記録媒体からの読み出しコンテンツの暗号化処理を実行して前記記録メディアに対する記録処理を実行させるステップであり、
前記個別鍵の読み出し処理に際して、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域からの読み出しを実行させるプログラムにある。

【００２５】
さらに、本発明の第１０の側面は、
情報記再生置において情報処理を実行させるプログラムであり、
データ処理部にが、記録メディアに記録された暗号化コンテンツの復号処理を実行させるデータ処理ステップを有し、
前記データ処理ステップは、
前記記録メディアに設定されたアクセス制限領域である保護領域に記録された個別鍵を読み出し、前記個別鍵を適用して前記暗号化コンテンツの復号処理を実行させるステップであり、
前記個別鍵の読み出し処理に際して、前記記録メディアに対してアクセス許容情報を記録した証明書を提示し、前記記録メディアにおける証明書の記録情報確認処理がなされたことを条件として、前記個別鍵の保護領域からの読み出しを実行させるプログラムにある。

【００２６】
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。

【００２７】
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】

【００２８】
本発明の一実施例の構成によれば、コンテンツの暗号鍵の漏洩に基づくコンテンツの不正利用を防止する構成が実現される。具体的には、記録装置がメモリカード等の記録メディアに対してサーバから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を記録する際、記録コンテンツ用の暗号鍵としてメディアに対する記録処理単位で異なる個別鍵を適用して暗号化を行い記録する。個別鍵は、サーバが記録メディアのアクセス制限領域である保護領域に書き込み、記録装置は、記録メディアの保護領域に書き込まれた

個別鍵を読み出して暗号化処理を実行する。個別鍵はサーバにおいて生成され、個別鍵データは、コンテンツ記録処理を実行した装置情報等とともに管理情報としてサーバにおいて管理され、個別鍵が漏洩した場合は管理情報に基づいて個別鍵の漏洩元を追求することが可能となる。

【図面の簡単な説明】

【００２９】

【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】従来の一般的なユーザに対する提供コンテンツとデータの基本構成例について説明する図である。

【図４】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５】サーバ証明書のデータ構成例について説明する図である。

【図６】装置証明書を適用したメモリカードの記憶領域へのアクセス処理の具体例について説明する図である。

【図７】本発明の一実施例に従ったサーバクライアント間のコンテンツ提供シーケンスについて説明するシーケンス図である。

【図８】本発明の一実施例に従った記録装置における個別鍵を適用したコンテンツの暗号化処理例について説明する図である。

【図９】本発明の一実施例に従った記録装置における個別鍵を適用したコンテンツの暗号化処理例について説明する図である。

【図１０】本発明の一実施例に従った再生装置における個別鍵を適用したコンテンツ復号、再生処理例について説明する図である。

【図１１】本発明の一実施例に従ったサーバからの提供データの構成について説明するシーケンス図である。

【図１２】サーバにおける管理情報に記録されるデータ例について説明する図である。

【図１３】サーバにおけるコンテンツのクライアントに対する提供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】記録装置におけるコンテンツ記録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】再生装置におけるコンテンツ再生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】個別鍵（Ｋｉｎｄ）のみで暗号化したコンテンツを記録メディアに記録する場合の処理例について説明する図である。

【図１７】個別鍵（Ｋｉｎｄ）に加え、さらにコンテンツ配信単位で異なる鍵として設定されるバインド鍵（Ｋｂｉｎｄ）を利用した処理例について説明する図である。

【図１８】サーバおよびクライアントとしての情報処理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１９】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】

【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。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．ユーザに対する提供コンテンツとデータの従来の基本構成例について

３．コンテンツ記録メディアとしてのメモリカードの構成例について

４．本発明に従ったユーザへの提供データおよびコンテンツの記録再生処理例について

５．サーバとクライアントにおいて実行する処理の処理シーケンスについて

（５－１）サーバにおけるデータ処理シーケンス

（５－２）記録装置および記録メディアにおけるコンテンツ記録シーケンス

（５－３）再生装置におけるコンテンツ再生シーケンス
６．タイトル鍵を利用する場合と利用しない場合のコンテンツ提供処理シーケンスについて
（６－１）タイトル鍵を利用しない場合の処理例
（６－２）タイトル鍵を利用する場合の処理例
７．各装置のハードウェア構成例について

【００３１】

［１．コンテンツ提供処理および利用処理の概要について］

【００３２】

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。

【００３３】

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。

【００３４】

（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。図１には、例えばフラッシュメモリ等からなる記録部を持つメモリカード３１を示している。

【００３５】

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、メモリカード３１にコンテンツを記録する場合、その記録コンテンツの許容コピー回数などのコピー制限情報や、他機器への出力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場合が多い。

【００３６】

図１に示す（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。

【００３７】

ユーザは、図１に示す（ｃ）コンテンツ記録メディアである例えばメモリカード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。

【００３８】

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、暗号化コンテンツの復号に適用する鍵情報等コンテンツ再生に必要な情報をクライアントに提供する。さらに、コンテンツに対する利用制御情報、コンテンツＩＤ他のコンテンツ管理情報を記録したトークン等のコンテンツ関連情報を提供する場合もある。

【００３９】

コンテンツサーバ１１からのダウンロード処理の他、ユーザは、図１（ａ）に示すコンテンツ記録ディスク１２からコンテンツをコピーして（ｃ）コンテンツ記録メディアであるメモリカード３１等に記録することもできる。

【００４０】

例えば、ユーザは、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にコピーを行う。ただし、このコピー処理が無秩序に実行されると、コピーコンテンツが無制限に増加することになる。このような事態を防止するため、例えばＡＡＣＳ（Ａｄｖａｎｃｅｄ Ａｃｃｅｓｓ Ｃｏｎｔｅｎｔ Ｓｙｓｔｅｍ）規格に従った暗号化コンテンツを記録したメディアからのコンテンツコピー処理に際しては、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須とされている。このコピー処理は、マネージドコピー（ＭＣ：Ｍａｎａｇｅｄ Ｃｏｐｙ）と呼ばれる。なお、ＡＡＣＳはコンテンツの著作権保護のための様々な規格を規定している。

【００４１】

マネージドコピー（ＭＣ：Ｍａｎａｇｅｄ Ｃｏｐｙ）に従ったコンテンツコピーを行う場合、図１（ｂ）に示すコンテンツ記録装置（ホスト）としての記録再生装置２２や、ＰＣ２３はコンテンツサーバ１１に接続し、コンテンツサーバ１１から、コピーコンテンツに対応する利用制御情報やトークン、さらにさらに暗号化コンテンツの復号に適用する鍵情報等のコンテンツ管理情報を受信し、コピー先メディアに記録する。

【００４２】

ユーザは、このように、

サーバからのコンテンツのダウンロード処理、あるいは、

コンテンツが記録されたディスクからのコンテンツコピー処理、

これらのいずれかの形態で、ユーザの所有する図１（ｃ）に示すメモリカード３１等のコンテンツ記録メディアにコンテンツを記録して利用することができる。

【００４３】

なお、ユーザのメディアにコンテンツを記録する装置としては、図１（ｂ）コンテンツ記録装置（ホスト）に示すように、

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、

これらの様々な機器がある。

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通信部を備えていることが必要であり、コンテンツ記録ディスク１２を利用する構成である場合は、ディスク再生可能な装置であることが必要である。

【００４４】

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。

【００４５】

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。

【００４６】

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。

【００４７】

［２．ユーザに対する提供コンテンツとデータの従来の基本構成例について］

次に、図３を参照して、従来の一般的なユーザに対する提供コンテンツとデータの基本構成例について説明する。

【００４８】

図３に示す構成は、例えばＢｌｕ－ｒａｙ（登録商標）ディスク等に記録されるＡＡＣＳ（Ａｄｖａｎｃｅｄ　Ａｃｃｅｓｓ　Ｃｏｎｔｅｎｔ　Ｓｙｓｔｅｍ）規格に従った暗号化コンテンツの基本的な構成例である。なお、前述したようにＡＡＣＳはコンテンツの著作権保護のための様々な規格を規定している。ＡＡＣＳ規格の代表的な暗号化構成として、コンテンツをユニット単位に区分してユニット毎に異なる暗号化鍵を適用する構成がある。このような暗号化構成を採用することで、ユニット単位のコンテンツの利用制御が可能となり、厳格で多様なコンテンツ利用制御が実現される。

【００４９】

図３には、以下の各データを示している。

（ａ）暗号化コンテンツ

（ｂ）暗号化コンテンツを構成する各ユニットの暗号化フォーマット

（ｃ）ユーザに対する提供データ（従来）

【００５０】

図３（ａ）暗号化コンテンツは、例えば映画等のコンテンツであり、例えばＢＤ（Ｂｌｕ－ｒａｙ（登録商標）ディスク）等に記録されるコンテンツの構成に対応する。

図３（ａ）に示すようにコンテンツはユニット（Ｕｎｉｔ）単位に区分されている。

１ユニットは、６１４４バイト単位のデータから構成される。

【００５１】

図３（ｂ）には、ユニット単位の暗号化フォーマットを示している。

（ｂ１）にはユニット１（Ｕｎｉｔ１）、（ｂｎ）にはユニットｎ（Ｕｎｉｔｎ）に対する暗号化フォーマットを示している。

ユニット１～ユニットｎは、それぞれ共通の構成、すなわち、

１６バイトのシード（ＳＥＥＤ）、

６１２８バイトのブロック（Ｂｌｏｃｋ）データ、

を有している。

【００５２】

シードは暗号鍵生成用データとして用いられ、ブロックはシードを適用して生成した暗号鍵によって暗号化されるデータ領域である。

具体的には、各ユニットｘ（ｘ＝１～ｎ）において、コンテンツ対応の暗号鍵であるタイトル鍵（Ｋｔ）と、各ユニットのシード（ＳＥＥＤｘ）を利用してブロックに対する暗号鍵であるブロック鍵（Ｋｂｘ）が生成され、生成したブロック鍵（Ｋｂｘ）でブロック（Ｂｌｏｃｋ＿ｘ）が暗号化される。

すなわち図に示す例ではｎ個のユニット１～ｎの各ユニットのブロック１～ｎは、それぞれ異なるシード１～ｎを用いて生成された異なるブロック鍵（Ｋｂ１～Ｋｂｎ）によって暗号化されることになる。

図３（ｃ１）暗号化コンテンツに示すような構成を持つ暗号化コンテンツである。

【００５３】

なお、ブロック鍵（Ｋｂｘ）は、例えば、以下の演算処理によって生成される。

Ｋｂｘ＝（ＡＥＳ＿Ｅ（Ｋｔ，ＳＥＥＤｘ））（ＸＯＲ）（ＳＥＥＤｘ）

上記式において、

ＡＥＳ＿Ｅ（Ｋｔ，ＳＥＥＤｘ）は、タイトル鍵によるシードｘ（ＳＥＥＤｘ）の暗号化処理（ＡＥＳ　Ｅｎｃｒｙｐｔｉｏｎ）、

（ＸＯＲ）は、排他論理和演算、

を示している。

すなわち、各ユニットにおけるブロック鍵は、そのユニットｘのシード（ＳＥＥＤｘ）をタイトル鍵（Ｋｔ）で暗号化したデータ（ＡＥＳ＿Ｅ（Ｋｔ，ＳＥＥＤｘ））と、シード（ＳＥＥＤｘ）との排他論理和（ＸＯＲ）演算結果として算出される。

【００５４】

このように生成されたユニット対応のブロック鍵（Ｋｂｘ）を利用して各ユニットのブロック（ブロックｘ）の暗号化がなされる。

【００５５】

このようにユニット単位で異なるブロック鍵を適用した暗号化ブロックを持つ複数ユニットからなる暗号化コンテンツがディスク、あるいはサーバを介してユーザに提供される。

図３（ｃ）が、ユーザに対する提供データの例を示している。ユーザに提供されるデータには、以下のデータが含まれる。

（ｃ１）暗号化コンテンツ

（ｃ２）タイトル鍵（Ｋｔ）

【００５６】

（ｃ１）暗号化コンテンツは、上述した説明に従って生成される暗号化コミンテンツであり、ユニット単位で、シードとタイトル鍵で生成されブロック鍵を適用した暗号化ブロックを連結したデータである。

（ｃ２）タイトル鍵（Ｋｔ）は、コンテンツ対応のタイトル鍵（Ｋｔ）である。

【００５７】

これらの

（ｃ１）暗号化コンテンツ

（ｃ２）タイトル鍵（Ｋｔ）

が、ディスクなどに記録され、あるいはサーバからユーザに提供されるというのがこれまでの一般的なコンテンツの提供形態である。

【００５８】

ユーザは、暗号化コンテンツの復号処理を行う場合は、各ユニット単位で、ブロック鍵を生成して生成したブロック鍵を利用して各ユニットのブロックの復号を実行する。すなわち、前述のブロック鍵の生成式、

Ｋｂｘ＝（ＡＥＳ＿Ｅ（Ｋｔ，ＳＥＥＤｘ））（ＸＯＲ）（ＳＥＥＤｘ）

上記式を適用して、タイトル鍵（Ｋｔ）と各ブロックのシードデータ（ＳＥＥＤｘ）を利用して、各ユニットｘのブロック鍵ｘ（Ｋｂｘ）を生成して、ユニット単位でブロックの復号を実行してコンテンツ再生を実行する。

なおシードデータは暗号化されていない平文データとしてユーザに提供されることになる。

【００５９】

しかし、このように、ユーザに対して、

（ｃ１）暗号化コンテンツ

（ｃ２）タイトル鍵（Ｋｔ）
を提供した場合、
その後、ユーザがタイトル鍵（Ｋｔ）を漏洩してしまうと、例えば不正なコピーコンテンツを持つユーザがコピーコンテンツを復号することが可能となり、コンテンツの利用制御が不可能になる。
特に、昨今は個人がネットワーク上で様々な情報を公開しており、このような情報の１つとしてタイトル鍵を公開してしまうと、即座にそのタイトル鍵は誰でも利用可能な状態になってしまう。このような場合、コンテンツの利用制御は不可能となる。
本発明は、このような事態を防止するため、ユーザに提供するデータの構成を変更した。

【００６０】
［３．コンテンツ記録メディアとしてのメモリカードの構成例について］
次に、コンテンツの記録先として利用されるフラッシュメモリ等によって構成されるメモリカードの構成例について説明する。

【００６１】
メモリカード１００の記憶領域の具体的構成例を図４に示す。
メモリカード１００の記憶領域は、図４に示すように、
（ａ）保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１、
（ｂ）非保護領域（Ｕｓｅｒ　Ａｒｅａ）１０２、
これら２つの領域によって構成される。

【００６２】
（ｂ）非保護領域（Ｕｓｅｒ　Ａｒｅａ）１０２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。

【００６３】
一方、（ａ）保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１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１００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。

【００６４】
メモリカード１００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１００は、まず、メモリカード１００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。

【００６５】
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）１０１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４に示す保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１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。

【００６６】
メモリカードに対するデータ書き込みを実行する装置であるサーバのサーバ証明書のデータ例を図５に示す。図５は、認証局がサーバに提供するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）のデータ構成例を示す図である。
サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）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　Ｃｅｒｔｉｆｉｃａｔｅ）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。

【００６７】

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）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）

【００６８】

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。

【００６９】

（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。

【００７０】

（４）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４に示すメモリカード１００の記憶領域中に設定される保護領域（ＰＤＡ：Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１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。

【００７１】

メモリカードは、例えばサーバから認証処理の段階で受領する図５に示すサーバ証明書のこの記録フィールドを参照して、例えば、図４に示す保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１内の区分領域（図に示す領域＃０，＃１，＃２・・・）単位で書き込み、読み取りの許可判定処理を行い、許可された区分領域で許可された処理のみの実行を許容する。

【００７２】

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、［（５）その他の情報］が記録され、さらに、（１）～（５）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（６）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。

【００７３】

メモリカードの保護領域に対するアクセス要求を行うサーバ以外の装置、例えば記録装置、再生装置等もホスト公開鍵を格納し、図５（４）に示すメディアに対する読み取り／

書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）を記録したホスト証明書を保持し、このホスト証明書をメモリカードに提示する。

【００７４】

メモリカードはアクセス要求を行う装置から提示された証明書の署名検証を行い、証明書の正当性を確認した上で、証明書内の読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）の記録を参照して図４に示す保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１内の区分領域（図に示す領域＃０，＃１，＃２・・・）単位で書き込み、読み取りの許可判定処理を行い、許可された区分領域で許可された処理のみの実行を許容する。

【００７５】

上述したように、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　Ｃｅｒｔ）や、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）に記録される。

【００７６】

メモリカード１００は、メモリカード１００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。

【００７７】

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。

【００７８】

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１２０、ホスト機器１４０、メモリカード１００を示している。

サーバ１２０は、例えばコンテンツの提供処理や、コンテンツ復号に適用する暗号鍵の書き込み処理を実行するサーバである。

ホスト機器１４０は、メモリカード１００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暗号鍵を取得する必要がある機器である。

【００７９】

メモリカード１００は、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１と、非保護領域（Ｕｓｅｒ　Ａｒｅａ）１０２を有し、暗号化コンテンツ等は非保護領域（Ｕｓｅｒ　Ａｒｅａ）１０２に記録される。

暗号化コンテンツの復号に適用する暗号鍵は保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１に記録される。なお、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１に記録される暗号鍵には例えばコンテンツ記録処理ごとに異なる個別鍵（Ｋｉｎｄ）が含まれる。個別鍵（Ｋｉｎｄ）の利用処理については後段で詳細に説明する。

【００８０】

先に図４を参照して説明したように、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１は、複数の領域に区分されている。

図６に示す例では、

区分領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）１１１、

区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）１１２、

これらの２つの区分領域を持つ例を示している。

【００８１】

メモリカード１００はアクセス要求装置と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（Ｐｒｏｔｅ

ｃｔｅｄ　Ａｒｅａ）１０１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。この判定処理の結果、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。

【００８２】

例えば、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）１１２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。すなわち、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

このような設定で構成される。

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。

【００８３】

また、例えば区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）１１２に記録された暗号鍵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１４０の保持するホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）は、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）１１２に対する読み取り（Ｒｅａｄ）許可のみが設定された証明書、すなわち、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

このような設定で構成される。

【００８４】

ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）には、区分領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）１１２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暗号鍵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。

【００８５】

このように、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）１０１に対するデータ書き込みとデータ読み取りについて、装置証明書に基づいて許可するか否かを判定する。

【００８６】

［４．本発明に従ったユーザへの提供データおよびコンテンツの記録再生処理例について］

図６以下を参照して本発明の一実施例に従ったユーザに対する提供データおよび記録再生処理例について説明する。

【００８７】

図６には、左から、

（１）コンテンツ提供処理を実行するサーバ１５０、

（２）コンテンツを受信しメディアに対する記録処理を実行する記録装置１６０、

（３）コンテンツ記録用のメモリカード等の記録メディア１７０

（４）コンテンツを記録したディスク１８０

これらを示している。

記録メディア１７０は、図４を参照して説明したメモリカード１００に対応し、機器に応じたアクセス制限のなされる保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１７１と、アクセス制限のない非保護領域（Ｕｓｅｒ　Ａｒｅａ）１７２を有する。

【００８８】

図６に示す例は、以下の２つの処理例を併せて示している。

（ａ）サーバ１５０から提供されたコンテンツを記録装置１６０が受信して記録メディア１７０に記録する処理、

（ｂ）ディスク１８０に記録されたコンテンツを記録装置１６０が読み取って記録メデ

ィア１７０に記録する処理、
これら２つの処理例を示している。
（ａ），（ｂ）いずれの処理においても、記録装置１６０は、サーバ１５０と通信を実行して、個別鍵１５１を取得し、記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）に記録する処理を行う。

【００８９】
なお、個別鍵１５１は、記録メディア１７０に対する新たなコンテンツの記録処理ごとにサーバ１５０が生成する鍵である。例えばサーバ１５０は、乱数生成処理によって逐次異なる個別鍵（Ｋｉｎｄ）を生成して送信し、記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）に記録する処理を行う。

【００９０】
（ａ）サーバ１５０から提供されたコンテンツを記録装置１６０が受信して記録メディア１７０に記録する処理においては、図６に示すステップＳ１１、Ｓ１２、Ｓ１３ａ、Ｓ１４、Ｓ１５の順番で処理が行われる。
（ｂ）ディスク１８０に記録されたコンテンツを記録装置１６０が読み取って記録メディア１７０に記録する処理においては、図６に示すステップＳ１１、Ｓ１２、Ｓ１３ｂ、Ｓ１４、Ｓ１５の順番で処理が行われる。

【００９１】
まず、（ａ）サーバ１５０から提供されたコンテンツを記録装置１６０が受信して記録メディア１７０に記録する処理について説明する。

【００９２】
ステップＳ１１において、サーバ１５０は、個別鍵（Ｋｉｎｄ）１５１を記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）１７１に記録する処理を行う。
この処理の開始前に、サーバ１５０と、記録メディア１７０は相互認証を実行する。この認証処理の段階で、記録メディア１７０はアクセス要求装置としてのサーバ１５０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）１７１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４、図６を参照して説明したように保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）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許容される。

【００９３】
サーバ１５０は、記録メディア１７０の許容を条件として、個別鍵（Ｋｉｎｄ）１５１を記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）１７１に記録する処理を行う。
保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）１７１に記録された結果が、図６に示す個別鍵（Ｋｉｎｄ）１７３である。

【００９４】
次に、ステップＳ１２において、記録装置１６０は、記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）１７１に記録された個別鍵（Ｋｉｎｄ）１７３を読み出す。

【００９５】
なお、この読み出し処理の前に、記録装置１６０と、記録メディア１７０は相互認証を実行する。この認証処理の段階で、記録メディア１７０はアクセス要求装置としての記録装置１６０から公開鍵証明書等の装置証明書（たとえばホスト証明書（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）１７１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４、図６を参照して説明したように保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）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許容される。

【００９６】
記録装置１６０は、記録メディア１７０の許容を条件として、個別鍵（Ｋｉｎｄ）１７３を記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１７１から読み出す処理を行う。
【００９７】
次に、ステップＳ１３ａにおいて、記録装置１６０は、サーバ１５０からコンテンツ１５２を受信する。なお、このコンテンツは、暗号化されていない平文コンテンツ、あるいはコンテンツ対応のタイトル鍵等によって暗号化された暗号化コンテンツ、すなわち、先に図３（ｃ１）を参照して説明した暗号化コンテンツのいずれかの態様である。
【００９８】
なお、サーバ１５０は、タイトル鍵によって暗号化された暗号化コンテンツを提供する場合は、タイトル鍵を記録メディア１７０に暗号化して記録する。さらに前述の個別鍵の記録メディアに対する記録処理と同様、タイトル鍵の暗号鍵であるバインド鍵を記録メディア１７０の保護領域１７１に記録する処理を実行する。なお、この具体的な処理例については後段で説明する。
【００９９】
なお、サーバ１５０と記録装置１６０との間でもデータの送受信前に相互認証処理が実行され、認証処理においてセッション鍵の共有を行い、送受信データは必要に応じてセッション鍵で暗号化されて転送される。平文コンテンツを送受信する場合は、サーバ１５０は、このセッション鍵で暗号化して記録装置１６０に送信する。記録装置１６０は、セッション鍵で暗号化されたデータを受信した場合は、共有するセッション鍵で復号して次のステップに進む。
【０１００】
ステップＳ１４は、記録装置１６０において実行するコンテンツの暗号化処理である。このコンテンツ暗号化処理は、ステップＳ１２において記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１７１から読み出した個別鍵（Ｋｉｎｄ）１７３による暗号化処理である。
【０１０１】
なお、サーバから受信したコンテンツが平文コンテンツである場合は、個別鍵で暗号化した暗号化コンテンツを生成する。
一方、サーバから受信したコンテンツがタイトル鍵等によって暗号化された暗号化コンテンツ（例えば図３（ｃ１）に示す暗号化コンテンツ）である場合は、この暗号化コンテンツをさらに個別鍵で再暗号化した暗号化コンテンツを生成する。
【０１０２】
ステップＳ１４において記録装置１６０が実行するコンテンツの暗号化処理は、サーバ１５０から受信したコンテンツの全体を個別鍵（Ｋｉｎｄ）を用いて暗号化する設定としてもよいし、その一部のみを個別鍵を適用して暗号化する構成としてもよい。
この一部の暗号化処理例について図８、図９を参照して説明する。
【０１０３】
図８は、サーバから受信したコンテンツが平文コンテンツである場合の処理例である。図８には、
（ａ）サーバからの受信コンテンツ（平文コンテンツ）
（ｂ）記録装置の生成した暗号化コンテンツ（一部ユニットのみ個別鍵で暗号化した暗号化コンテンツ）
これらのコンテンツ例を示している。
記録装置１６０は、このようにサーバからの受信コンテンツの一部のみを個別鍵を適用して暗号化する構成としてもよい。
【０１０４】
ただし、このように一部のみを個別鍵（Ｋｉｎｄ）で選択的に暗号化した場合は、暗号化部分（例えばユニット識別子）を暗号化コンテンツに対応する暗号化領域識別情報とし

て作成し、暗号化コンテンツとともに記録メディアに記録する。
再生時には、この暗号化領域識別情報を参照して復号処理を実行する。
【０１０５】
図９は、サーバから受信したコンテンツがタイトル鍵とシードを用いて生成したブロック鍵で暗号化した暗号化コンテンツである場合の処理例である。図９には、
（ａ）サーバからの受信コミンテンツ（タイトル鍵（Ｋｔ）を適用した暗号化コンテンツ）
（ｂ）記録装置の生成した暗号化コンテンツ（一部ユニットのみ個別鍵で再暗号化した暗号化コンテンツ）
これらのコンテンツ例を示している。
記録装置１６０は、このようにサーバからの受信コンテンツの一部のみを個別鍵を適用して暗号化する構成としてもよい。
【０１０６】
この図９の設定でも、暗号化部分（例えばユニット識別子）を暗号化コンテンツに対応する暗号化領域識別情報として作成し、暗号化コンテンツとともに記録メディアに記録する。再生時には、この暗号化領域識別情報を参照して復号処理を実行する。
【０１０７】
次に、ステップＳ１５において、記録装置１６０は、生成した暗号化コンテンツを記録メディア１７０の非保護領域（Ｕｓｅｒ　ａｒｅａ）１７２に記録する。図に示す暗号化コンテンツ１７４が記録されることになる。
【０１０８】
この処理においては、サーバ１５０は、個別鍵のみを、コンテンツ提供処理ごとに逐次生成して送信することになるが、提供するコンテンツについては、すべての記録装置に対して共通のコンテンツとして提供することが可能となる。従って、サーバの処理負担は大きく増大することはない。
なお、サーバ１５０は、生成し送信した個別鍵の情報を個別鍵やコンテンツを提供した装置情報（クライアント情報）やユーザ情報に対応付けて記録した管理情報を生成して記憶部に格納する。
【０１０９】
例えば個別鍵が漏洩した場合には、管理情報に基づいて、個別鍵や個別鍵に併せてコンテンツを配信した装置（クライアント）やユーザを特定し、流出元を追及することができる。なお、管理情報の詳細については後段で説明する。
【０１１０】
次に、（ｂ）ディスク１８０に記録されたコンテンツを記録装置１６０が読み取って記録メディア１７０に記録する処理について説明する。
この処理は、ディスク１８０に記録されたコンテンツをサーバ管理の下で他の記録メディアに記録する処理であり、マネージドコピー（ＭＣ：Ｍａｎａｇｅｄ　Ｃｏｐｙ）とよばれる処理である。
【０１１１】
ステップＳ１１～Ｓ１２の処理は、サーバ１５０からのコンテンツダウンロード処理の実行時と同様の処理が行われる。
すなわち、ステップＳ１１において、サーバ１５０は、個別鍵（Ｋｉｎｄ）１５１を記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１７１に記録する処理を行う。
なおこのステップＳ１１の処理以前に、記録装置１６０は、ディスク１８０からコピーするコンテンツの情報、例えばディスクＩＤやコンテンツＩＤをサーバ１５０に送信する。サーバ１５０はこれらの情報に基づいてコピーを許容するか否かを判定し、許容する場合に、個別鍵の送信、記録処理を実行する。
【０１１２】
なお、個別鍵の記録処理の開始前に、サーバ１５０と、記録メディア１７０は相互認証

を実行する。この認証処理の段階で、記録メディア１７０はアクセス要求装置としてのサーバ１５０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）１７１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４、図６を参照して説明したように保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）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許容される。

【０１１３】

サーバ１５０は、記録メディア１７０の許容を条件として、個別鍵（Ｋｉｎｄ）１５１を記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）１７１に記録する処理を行う。

保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）１７１に記録された結果が、図６に示す個別鍵（Ｋｉｎｄ）１７３である。

【０１１４】

次に、ステップＳ１２において、記録装置１６０は、記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）１７１に記録された個別鍵（Ｋｉｎｄ）１７３を読み出す。

【０１１５】

なお、この読み出し処理の前に、記録装置１６０と、記録メディア１７０は相互認証を実行する。この認証処理の段階で、記録メディア１７０はアクセス要求装置としての記録装置１６０から公開鍵証明書等の装置証明書（たとえばホスト証明書（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）１７１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４、図６を参照して説明したように保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）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許容される。

【０１１６】

記録装置１６０は、記録メディア１７０の許容を条件として、個別鍵（Ｋｉｎｄ）１７３を記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）１７１から読み出す処理を行う。

【０１１７】

次に、ステップＳ１３ｂにおいて、記録装置１６０は、ディスク１８０からコンテンツ１８１を読み取る。なお、このコンテンツは、暗号化されていない平文コンテンツ、あるいはコンテンツ対応のタイトル鍵等によって暗号化された暗号化コンテンツ、すなわち、先に図３（ｃ１）を参照して説明した暗号化コンテンツのいずれかの態様である。

【０１１８】

なお、タイトル鍵によって暗号化された暗号化コンテンツの処理を行う場合は、タイトル鍵をサーバ１５０から受信、またはディスク１８０から読み出して記録メディア１７０に記録する処理を実行する。

【０１１９】

ステップＳ１４は、記録装置１６０において実行するコンテンツの暗号化処理である。このコンテンツ暗号化処理は、ステップＳ１２において記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）１７１から読み出した個別鍵（Ｋｉｎｄ）１７３による暗号化処理である。

なお、ディスク１８０から読み取ったコンテンツが平文コンテンツである場合は、個別鍵でのみ暗号化した暗号化コンテンツを生成する。

【０１２０】

一方、ディスク１８０から読み取ったコンテンツがタイトル鍵等によって暗号化された暗号化コンテンツ（例えば図３（ｃ１）に示す暗号化コンテンツ）である場合は、この暗号化コンテンツをさらに個別鍵で再暗号化した暗号化コンテンツを生成する。

【０１２１】
なお、ステップＳ１４において記録装置１６０が実行するコンテンツの暗号化処理は、先に図８、図９を参照して説明したようにコンテンツの全体を個別鍵（Ｋｉｎｄ）を用いて暗号化する設定としてもよいし、その一部のみを個別鍵を適用して暗号化する構成としてもよい。
【０１２２】
次に、ステップＳ１５において、記録装置１６０は、生成した暗号化コンテンツを記録メディア１７０の非保護領域（Ｕｓｅｒ　ａｒｅａ）１７２に記録する。図に示す暗号化コンテンツ１７４が記録されることになる。
【０１２３】
この処理においては、サーバ１５０は、個別鍵のみを、コンテンツコピー処理ごとに逐次生成して送信する。
なお、サーバ１５０は、生成し送信した個別鍵の情報を個別鍵を提供した装置情報（クライアント情報）やユーザ情報に対応付けて記録した管理情報を生成して記憶部に格納する。
【０１２４】
例えば個別鍵が漏洩した場合には、管理情報に基づいて、個別鍵や個別鍵に併せてコンテンツを配信した装置（クライアント）やユーザを特定し、流出元を追及することができる。なお、管理情報の詳細については後段で説明する。
【０１２５】
次に、図１０を参照して、記録メディア１７０に記録したコンテンツの復号再生処理について説明する。
図１０には、
記録メディア１７０
再生装置１９０、
これらを示している。
【０１２６】
記録メディア１７０は、図７に示す記録メディア１７０であり、図７を参照して説明したシーケンス（ステップＳ１１～Ｓ１５）に従って、サーバ１５０から取得した個別鍵１７３と、サーバ１５０からのダウンロードコンテンツ、またはディスク１８０からのコピーコンテンツを個別鍵で暗号化した暗号化コンテンツ１７４を記録したメディアである。
再生装置１９０は、ユーザのＰＣや再生機器等の再生装置である。
【０１２７】
再生処理は、図１０に示すステップＳ２１～Ｓ２３の順で実行される。
まず、ステップＳ２１において、再生装置１９０は、記録メディア１７０の保護領域１７１から個別鍵（Ｋｉｎｄ）１７３を読み出す。
【０１２８】
なお、この読み出し処理の前に、再生装置１９０と、記録メディア１７０は相互認証を実行する。この認証処理の段階で、記録メディア１７０はアクセス要求装置としての再生装置１９０から公開鍵証明書等の装置証明書（たとえばホスト証明書（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）１７１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４、図６を参照して説明したように保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）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許容される。
【０１２９】
再生装置１９０は、記録メディア１７０の許容を条件として、個別鍵（Ｋｉｎｄ）１７３を記録メディア１７０の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１７１から読み出す処理を行う。
【０１３０】

次に、ステップＳ２２において、再生装置１９０は、記録メディア１７０の非保護領域１７２から個別鍵（Ｋｉｎｄ）で暗号化された暗号化コンテンツ１７４を読み出す。

【０１３１】

次に、ステップＳ２３において、再生装置１９０は、記録メディア１７０の非保護領域１７２から読み出した個別鍵（Ｋｉｎｄ）を適用して暗号化コンテンツ１７４の復号処理を実行して、コンテンツ１９１を再生する。

なお、個別鍵による復号結果が、平文コンテンツではなくタイトル鍵とうによって暗号化されたコンテンツ（図３（ｃ１）に示す暗号化コンテンツ）である場合は、さらにタイトル鍵を利用した復号処理を実行してコンテンツの復号を行ってコンテンツ１９１を再生する。

【０１３２】

本発明において、サーバは、コンテンツの提供処理単位、あるいはコンテンツのディスクからのコピー処理単位で異なる個別鍵（Ｋｉｎｄ）を生成し、生成した個別鍵（Ｋｉｎｄ）を記録メディアに提供する。

【０１３３】

図１１にサーバから各クライアントに提供するデータの概念図を示す。

図１１に示すように、コンテンツのダウンロード処理に際しては、

サーバ１５０は、例えば同じタイトルのコンテンツを提供するクライアント１，２に対して、

（ａ）コンテンツ（平文または暗号化コンテンツ）

を各クライアントに共通するデータとして提供する。

なお、コンテンツをタイトル鍵を用いた暗号化コンテンツとして提供する場合は、

（ｂ）タイトル鍵（Ｋｔ）

も、共通データとして各クライアントに提供する。

サーバ１５０は、各クライアント単位で異なるデータとして、

（ｃ）個別鍵（Ｋｉｎｄ）

を提供する。

【０１３４】

コンテンツをディスクからコピーして記録する処理に際しては、

サーバ１５０は、例えば同じタイトルのコンテンツのコピーを行うクライアント１，２に対して、各クライアント単位で異なるデータとして、

（ａ）個別鍵（Ｋｉｎｄ）

のみを提供する。

ただし、コンテンツが、タイトル鍵を用いた暗号化コンテンツとしてコピーされる場合は、

（ｂ）タイトル鍵（Ｋｔ）

を、共通データとして各クライアントに提供する。

【０１３５】

クライアント１，２・・の記録メディアには、例えばタイトル鍵で暗号化されたコンテンツのダウンロードまたはコピー処理が実行される場合でも、個別鍵によって暗号化された異なる暗号化コンテンツが記録される。

従って、例えばタイトル鍵が漏洩し、不特定多数のユーザによって利用可能な状況となっても、個別鍵は、クライアント単位（配信コンテンツ単位）で異なるデータであり、これらの個別データが不特定多数が利用可能な状況にならない限り、コンテンツの不正利用が広がることはない。

【０１３６】

また、個別鍵はサーバによって、配信先情報とともに管理されるので、万が一、不正に広まった個別鍵や暗号化シードが発見された場合は、その個別鍵の配送先を特定することが可能となる。

図１２にサーバの記憶手段に保持される管理情報のデータ構成例を示す。

図１２に示すように、管理情報には、
配信コンテンツに対応する固有ＩＤ、
配信コンテンツ情報、
個別鍵（Ｋｉｎｄ）情報
配信先情報、
配信ユーザ情報、
配信日時情報、
例えばこれらの情報が含まれる。
タイトル鍵で暗号化されたコンテンツのダウンロードまたはコピー処理が実行される場合には、タイトル鍵（Ｋｔ）情報も登録される。

【０１３７】
なお、配信先情報としては、図７を参照して説明した記録装置１６０と、記録メディア１７０を個別に登録する設定としてもよい。あるいはいずれかのみを登録する設定としてもよい。
個別鍵（Ｋｉｎｄ）情報は、全てのエントリに対して異なるデータが記録される。なお、配信先のユーザが同じ場合には、同じ個別鍵を利用する構成としてもよい。この場合、個別鍵は配信処理単位ではなく配信先ユーザ単位で異なる鍵として設定されることになる。
この場合でも、不正なデータ流出があった場合には個別鍵の照合によって流出元としてのユーザの特定は可能となる。
なお、図１２に示す管理情報の例は一例であり、これらの情報の全てが必須ではなく、また、これらの情報以外の情報を管理情報として保持してもよい。

【０１３８】
このように、本発明の構成では、コンテンツ配信、あるいはコンテンツコピー処理管理を行うサーバが、コンテンツ記録先としての記録メディアの保護領域にコンテンツの暗号鍵として適用される個別鍵（Ｋｉｎｄ）を記録する処理を行う構成とした、
この個別鍵（Ｋｉｎｄ）は、新たなコンテンツのダウンロード処理またはコンテンツのコピー処理ごとにサーバが異なる鍵として生成して提供するものであり、個別鍵情報は、提供先情報とともに管理情報としてサーバにおいて記録、管理される。

【０１３９】
これらの処理により、例えばコンテンツ対応のタイトル鍵が漏洩してもタイトル鍵のみではコンテンツ復号ができずコンテンツの不正利用が防止される。また、個別鍵が漏洩した場合は管理情報に基づいて配信先を特定可能であり、個別鍵の漏洩元を追求することが可能となる。

【０１４０】
［５．サーバとクライアントにおいて実行する処理の処理シーケンスについて］
次に図１３以下のフローチャートを参照してサーバとクライアントにおいて実行する処理の処理シーケンスについて説明する。

【０１４１】
（５－１）サーバにおけるデータ処理シーケンス
まず、図１３に示すフローチャートを参照してサーバにおけるコンテンツのクライアントに対する提供処理シーケンスについて説明する。
図１３に示す処理はサーバのデータ処理部の制御の下に実行される処理である。

【０１４２】
ステップＳ１２１において、個別鍵（Ｋｉｎｄ）を生成する。この個別鍵生成処理は、例えば乱数生成処理によって実行される。

【０１４３】
次にステップＳ１２３において、個別鍵を記録メディアに送信し、記録処理を行う。なお、サーバは、個別鍵（Ｋｉｎｄ）を記録メディアの保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）１７１に記録する処理を行う。

【０１４４】
なお、この処理の開始前に、サーバと記録メディアは相互認証を実行する。この認証処理の段階で、記録メディアはアクセス要求装置としてのサーバ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）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４、図６を参照して説明したように保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）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許容される。
サーバは、記録メディアの許容を条件として、個別鍵（Ｋｉｎｄ）を記録メディアの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に記録する処理を行う。
【０１４５】
次に、ステップＳ１２４において、コンテンツの生成または取得を行う。このコンテンツは、暗号化のなされていない平文コンテンツ、または、タイトル鍵等を適用して暗号化された暗号化コンテンツ、すなわち、図３（ｃ）に示す暗号化コンテンツである。図３（ｃ）に示す暗号化コンテンツである場合は、ユニット単位のブロックデータがユニットのシードとタイトル鍵で生成されたブロック鍵（Ｋｂ）を適用して暗号化されたコンテンツである。
【０１４６】
次に、ステップＳ１２５において、ステップＳ１２４で生成または取得したコンテンツを記録装置に送信する。なお、例えば提供コンテンツが平文コンテンツである場合は、サーバと記録装置間で実行した認証処理において生成したセッション鍵で暗号化を行って送信することが好ましい。
【０１４７】
最後に、ステップＳ１２６において、個別鍵（Ｋｉｎｄとコンテンツ提供先クライアント情報とを対応づけた管理情報エントリを生成して記憶部に格納する。
この管理情報は、先に図１２を参照して説明した管理情報である。
【０１４８】
なお、ステップＳ１２４において記録装置に提供するコンテンツがタイトル鍵を用いて暗号化されたコンテンツである場合は、タイトル鍵についても記録メディアに記録する処理を行う。この処理の具体例については後段で説明する。
【０１４９】
（５－２）記録装置および記録メディアにおけるコンテンツ記録シーケンス
次に、図１４に示すフローチャートを参照して、サーバから受信したコンテンツ、またはディスクから読み取ったコンテンツをメモリカード等の記録メディアに記録する処理シーケンスについて説明する。
図１４に示す処理はメモリカード等を装着した記録装置およびメモリカード等の記録メディア自体のデータ処理部の制御の下に実行される処理である。
【０１５０】
まず、ステップＳ１３１においてコンテンツを記録するメディアを記録装置にセットする。例えば図１に示すメモリカード３１を記録装置としてのＰＣ等にセットする。
【０１５１】
ステップＳ１３２において、サーバから個別鍵（Ｋｉｎｄ）を受信してメディアの保護領域に記録する。なお、この処理の前提として、サーバと記録メディア間で相互認証を実行し、記録メディアがサーバから受領したサーバ証明書に記録された保護領域のアクセス権を確認し、サーバの書き込み権限が確認された区分領域に対して個別鍵（Ｋｉｎｄ）が書き込まれる。
【０１５２】
次に、ステップＳ１３３において記録装置は、記録メディアの保護領域に書き込まれた個別鍵（Ｋｉｎｄ）を読み取る。なお、この処理の前提として、記録装置と記録メディア

間で相互認証を実行し、記録メディアが記録装置から受領したホスト証明書に記録された保護領域のアクセス権を確認し、記録装置の読み取り権限が確認された区分領域からのみ読み取り処理が実行される。

【０１５３】

次に、ステップＳ１３４において、記録装置はサーバから

タイトル鍵等で暗号化されたコンテンツ、または、

セッション鍵で暗号化されたコンテンツ、

を受信しセッション鍵で暗号化されている場合は、セッション鍵で復号を行った後、個別鍵（Ｋｉｎｄ）で暗号化を行う。

この暗号化処理の例を図１４の（ａ），（ｂ１），（ｂ２）として示してある。

（ａ）は、サーバからの受信コンテンツを示している。

（ｂ１）は、受信コンテンツ全体を個別鍵（Ｋｉｎｄ）で暗号化した例である。

（ｂ２）は、受信コンテンツの一部を選択的に暗号化した例である。

【０１５４】

（ｂ２）に示す暗号化の例は、先に図８、図９を参照して説明した部分暗号化の例に対応する。

なお、（ｂ２）のように一部のみを個別鍵（Ｋｉｎｄ）で選択的に暗号化した場合は、暗号化部分（例えばユニット識別子）を暗号化コンテンツに対応する暗号化領域識別情報として作成し、暗号化コンテンツとともに記録メディアに記録する。

再生時には、この暗号化領域識別情報を参照して復号処理を実行する。

【０１５５】

最後にステップＳ１３５において、記録装置は暗号化コンテンツを記録メディアに記録する。なお、この記録処理は記録メディアの非保護領域（Ｕｓｅｒ　Ａｒｅａ）に対する書き込み処理として実行する。

また、（ｂ２）に示す部分暗号化を行った場合は、暗号化部分（例えばユニット識別子）を暗号化コンテンツに対応する暗号化領域識別情報として作成し、暗号化コンテンツとともに記録メディアに記録する。

【０１５６】

（５－３）再生装置におけるコンテンツ再生シーケンス

次に、図１５に示すフローチャートを参照して、再生装置におけるコンテンツ再生シーケンスについて説明する。

図１５に示す処理は再生装置のデータ処理部の制御の下に実行される処理である。

【０１５７】

ステップＳ１５１においてコンテンツを記録したメディアを再生装置にセットする。例えば図１に示すメモリカード３１を再生装置としての記録再生器２２や、ＰＣ２３等にセットする。

【０１５８】

次に、ステップＳ１５２において、記録メディアの保護領域に書き込まれた個別鍵（Ｋｉｎｄ）を読み取る。なお、この処理の前提として、再生装置と記録メディア間で相互認証を実行し、記録メディアが再生装置から受領したホスト証明書に記録された保護領域のアクセス権を確認し、再生装置の読み取り権限が確認された区分領域からのみ読み取り処理が実行される。

【０１５９】

次にステップＳ１５３において、暗号化コンテンツを記録メディアから読み取り、個別鍵（Ｋｉｎｄ）を適用して復号する。

なお、先に説明した図１４（ｂ２）のように一部のみを個別鍵（Ｋｉｎｄ）で選択的に暗号化したコンテンツである場合は、暗号化部分（例えばユニット識別子）の領域情報を記録した暗号化領域識別情報を記録メディアから読み出して、この暗号化領域識別情報を参照して復号処理を実行する。

【０１６０】

次に、ステップＳ１５４において、個別鍵（Ｋｉｎｄ）で復号したコンテンツがさらにタイトル鍵等によって暗号化されているか否かを判定する。
個別鍵（Ｋｉｎｄ）による復号コンテンツが平文コンテンツである場合は、ステップＳ１５４の判定はＮｏとなり、ステップＳ１５６に進み、再生処理に移行する。
【０１６１】
個別鍵（Ｋｉｎｄ）による復号コンテンツが平文コンテンツでない場合は、ステップＳ１５４の判定はＹｅｓとなり、ステップＳ１５５に進む。
【０１６２】
ステップＳ１５５では、暗号化コンテンツのユニット単位で、シードとタイトル鍵に基づくブロック鍵を生成し暗号化ブロックを復号する。
ブロック鍵の生成は、先に説明したように以下の式によって行われる。
Ｋｂｘ＝（ＡＥＳ＿Ｅ（Ｋｔ，ＳＥＥＤｘ））（ＸＯＲ）（ＳＥＥＤｘ）
上記式において、
ｘはブロック識別子
ＡＥＳ＿Ｅ（Ｋｔ，ＳＥＥＤｘ）は、タイトル鍵によるシードｘ（ＳＥＥＤｘ）の暗号化処理（ＡＥＳ　Ｅｎｃｒｙｐｔｉｏｎ）、
（ＸＯＲ）は、排他論理和演算、
を示している。
すなわち、各ユニットにおけるブロック鍵は、そのユニットのシードをタイトル鍵（Ｋｔ）で暗号化したデータ（ＡＥＳ＿Ｅ（Ｋｔ，ＳＥＥＤｘ））と、シードとの排他論理和演算結果として取得される。
【０１６３】
このように、ステップＳ１５５においてブロック鍵による各ブロックの復号を行って、ステップＳ１５６においてコンテンツ再生処理が実行される。
【０１６４】
本発明の処理では、サーバは、コンテンツダウンロード処理やコンテンツコピー処理ごとに異なる設定とした個別鍵（Ｋｉｎｄ）を提供し、記録装置は、個別鍵を適用してダウンロードコンテンツやコピーコンテンツを暗号化してキロクメディアに記録する設定とした。
この設定により、例えばコンテンツに対応するタイトル鍵を漏洩や公開するなどの行為を行ったとしても、個別鍵が得られない限り、復号が不可能となる。
【０１６５】
また、個別鍵を漏洩した場合には、個別鍵データの構成を解析して、サーバの管理情報（図１２参照）の登録情報と照合することでデータの漏洩元を突き止め、特定することが可能となる。
【０１６６】
［６．タイトル鍵を利用する場合と利用しない場合のコンテンツ提供処理シーケンスについて］
上述した説明において、サーバが提供するコンテンツ、あるいはディスクから読み取るコンテンツは、タイトル鍵を用いて暗号化されている暗号化コンテンツである場合とヒラブンコンテンツである場合の２通りがあると説明した。以下では、これらの２つの処理例について、サーバからコンテンツを提供する場合の処理例として具体的なシーケンス例を個別に説明する。以下の処理例について順次説明する。
（６－１）タイトル鍵を利用しない場合の処理例（図１６）
（６－２）タイトル鍵を利用する場合の処理例（図１７）
【０１６７】
（６－１）タイトル鍵を利用しない場合の処理例
まず、図１６を参照して、タイトル鍵を利用した暗号化処理を実行しないコンテンツをユーザの記録装置に提供する処理シーケンスについて説明する。
【０１６８】

図１６には、左から、
（Ａ）コンテンツサーバ２００
（Ｂ）コンテンツ記録装置（ホスト）３００
（Ｃ）メモリカード４００
これらを示している。
（Ａ）コンテンツサーバ２００は、図１（ａ）に示すコンテンツサーバ１１に対応し、
（Ｂ）コンテンツ記録装置は、図１（ｂ）に示すコンテンツ記録装置（ホスト）としての記録再生器２２やＰＣ２３に対応し、
（Ｃ）メモリカードは図１（ｃ）に示すメモリカード３１に対応する。

【０１６９】
図１６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１に示すディスク１２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、その他の個別鍵や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。

【０１７０】
なお、図１６に示す（Ｃ）メモリカード４００は、（Ｂ）コンテンツ記録装置（ホスト）３００に装着し、（Ｂ）コンテンツ記録装置（ホスト）３００の通信部を介して（Ａ）コンテンサーバ２００との通信を実行し、（Ａ）コンテンツサーバ２００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）３００を介して受信してメモリカード４００に記録する。

【０１７１】
図１６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Ｓ２０１において、コンテンツサーバ２００とメモリカード４００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２００は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４００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。

【０１７２】
なお、メモリカードは相互認証処理や、先に図４等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。

【０１７３】
コンテンツサーバ２００とメモリカード４００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２００はメモリカード４００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２００からのデータ提供処理は行われない。

【０１７４】
相互認証の成立後、コンテンツサーバ２００は、データベース２１１に記録された特定のコンテンツ集合に対応する識別子であるボリュームＩＤやコンテンツ識別子としてのコンテンツＩＤ等のデータを取得して、これらのＩＤやその他のコンテンツ管理情報を記録したトークン２１３を生成し、ステップＳ２０２においてトークン２１３に対する署名を実行して、コンテンツ記録装置（ホスト）３００に対して送信、すなわちメモリカード４００に対する書き込みデータとして送信する。

【０１７５】
なお、トークン２１３は、提供コンテンツの識別子としてのコンテンツＩＤや、コンテンツに対する利用規則を定めたデータとしてクライアントに提供される利用制御情報の正当性を検証するためのハッシュ値等を記録したデータである。トークンにはサーバの署名が設定され、改ざんの検証が可能な設定となっている。

クライアントではコンテンツ再生時にトークンの署名を検証してトークンの正当性を検証しさらにトークンに記録された利用制御情報のハッシュ値に基づいてさーばから受信する利用制御情報ファイルの正当性を検証し、正当性の確認された利用制御情報ファイルに記録された利用制御情報に従ってコンテンツの利用（再生やコピー）を行う。

【０１７６】

トークンは、（Ａ）コンテンツサーバ２００から（Ｂ）コンテンツ記録装置（ホスト）３００を介して（Ｃ）メモリカード４００に送信され、メモリカード４００に記録される。この記録データが図１６の（Ｃ）メモリカード４００中に示すトークン（Ｔｏｋｅｎ）４１５である。

【０１７７】

なお、メモリカード４００は、図４等を参照して説明したように機器に応じたアクセス制限のなされる保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）と、アクセス制限のない非保護領域（Ｕｓｅｒ　Ａｒｅａ）に分割されている。

【０１７８】

また、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。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４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。

【０１７９】

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　Ｃｅｒｔ）や、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）に記録される。

【０１８０】

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。

【０１８１】

図１６に示す（Ｃ）メモリカード４００には保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）４１２を示している。保護領域４１２以外の領域は非保護領域である。保護領域（ｐｏｔｅｃｔｅｄ　Ａｒｅａ）４１２は、図に示すように個別鍵（Ｋｉｎｄ）４１３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。

【０１８２】

なお、個別鍵（Ｋｉｎｄ）４１３はコンテンツの暗号化および復号に適用する鍵であり、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。

【０１８３】

図１６（Ａ）コンテンツサーバ２００のステップＳ２０３の処理として示すように、個別鍵（Ｋｉｎｄ）は、コンテンツサーバにおいて生成される。この鍵は、コンテンツのサーバからの提供処理、あるいはディスクからのコ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個別鍵（Ｋｉｎｄ）が生成されることになる。

【０１８４】

サーバ２００の生成した個別鍵（Ｋｉｎｄ）は、メモリカード４００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に書き込まれる。

なお、メモリカード４００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、および保護領域に設定される区分領域（＃１，＃２・・・）単位で書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の可否が設定される。

【０１８５】

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個別鍵（Ｋｉｎｄ）を記録する。図１６に示す個別鍵（Ｋｉｎｄ）４１３である。なお、図１６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個別鍵（Ｋｉｎｄ）４１３が記録される。

【０１８６】

なお、コンテンツサーバ２００からメモリカード４００への個別鍵の送信は、セッション鍵で暗号化したデータとして送信が行われる。

セッション鍵は、サーバ２００とメモリカード４００間の相互認証処理（ステップＳ２０１）時に生成され、双方で共有する鍵である。メモリカード４００は、暗号化された個別鍵をセッション鍵で復号してメモリカード４００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）４１２の所定の区分領域に記録する。

【０１８７】

さらに、コンテンツサーバ２００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Ｓ２０４でコンテンツサーバ２００の秘密鍵で署名処理を実行してメモリカード４００に提供する。

書き込み結果が、図１６に示す利用制御情報４１７である。

【０１８８】

また、コンテンツサーバ２００は、コンテンツ２１８をコンテンツ記録装置（ホスト）３００に提供する。

なお、サーバ２００とコンテンツ記録装置（ホスト）３００との間では相互認証が実行され、この認証処理に際してサーバ２００とコンテンツ記録装置（ホスト）３００が共有した秘密鍵であるセッション鍵で暗号化を行ってコンテンツ送信を行うのが好ましい。

【０１８９】

コンテンツ記録装置（ホスト）３００は、受信コンテンツをセッション鍵で復号した後、メモリカード４００の保護領域から読み出した個別鍵（Ｋｉｎｄ）で暗号化を実行する。

なお、個別鍵の読み出し処理に際しては、コンテンツ記録装置（ホスト）３００とメモリカード４００との間の相互認証の成立、およびコンテンツ記録装置（ホスト）３００の証明書（ホスト証明書）に基づくアクセス権限の確認がメモリカード４００において実行される。

【０１９０】

アクセス権限が確認された場合にのみ個別鍵の読み出しが実行され、ステップＳ２０５において、コンテンツ記録装置（ホスト）３００がコンテンツの暗号化を実行してメモリカード４００にか書き込む処理が行われる。

書き込み結果が、図１６に示す暗号化コンテンツ４１８である。

【０１９１】

（６－２）タイトル鍵を利用する場合の処理例（図１７）

次に、図１７を参照して、タイトル鍵を利用した暗号化処理を実行した暗号化コンテンツをユーザの記録装置に提供する処理シーケンスについて説明する。

【０１９２】
図１７には、左から、
（Ａ）コンテンツサーバ２００
（Ｂ）コンテンツ記録装置（ホスト）３００
（Ｃ）メモリカード４００
これらを示している。
（Ａ）コンテンツサーバ２００は、図１（ａ）に示すコンテンツサーバ１１に対応し、
（Ｂ）コンテンツ記録装置は、図１（ｂ）に示すコンテンツ記録装置（ホスト）としての記録再生器２２やＰＣ２３に対応し、
（Ｃ）メモリカードは図１（ｃ）に示すメモリカード３１に対応する。
【０１９３】
図１７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１に示すディスク１２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、その他の個別鍵や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。
【０１９４】
なお、図１７に示す（Ｃ）メモリカード４００は、（Ｂ）コンテンツ記録装置（ホスト）３００に装着し、（Ｂ）コンテンツ記録装置（ホスト）３００の通信部を介して（Ａ）コンテンサーバ２００との通信を実行し、（Ａ）コンテンツサーバ２００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）３００を介して受信してメモリカード４００に記録する。
【０１９５】
図１７を参照して処理シーケンスについて説明する。
ステップＳ２０１～Ｓ２０３の処理は、先に図１６を参照して説明したと同様の処理である。
ステップＳ２０１において、コンテンツサーバ２００とメモリカード４００間で相互認証処理を実行し、相互認証の成立後、コンテンツサーバ２００は、コンテンツＩＤ等のＩＤやその他のコンテンツ管理情報を記録したトークン２１３を生成し、ステップＳ２０２においてトークン２１３に対する署名を実行して、コンテンツ記録装置（ホスト）３００に対して送信、すなわちメモリカード４００に対する書き込みデータとして送信する。
【０１９６】
トークンは、（Ａ）コンテンツサーバ２００から（Ｂ）コンテンツ記録装置（ホスト）３００を介して（Ｃ）メモリカード４００に送信され、メモリカード４００に記録される。この記録データが図１７の（Ｃ）メモリカード４００中に示すトークン（Ｔｏｋｅｎ）４１５である。
【０１９７】
次に、図１６（Ａ）コンテンツサーバ２００のステップＳ２０３の処理として、個別鍵（Ｋｉｎｄ）がコンテンツサーバにおいて生成される。この鍵は、コンテンツのサーバからの提供処理、あるいはディスクからのコ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個別鍵（Ｋｉｎｄ）が生成されることになる。
【０１９８】
サーバ２００の生成した個別鍵（Ｋｉｎｄ）は、メモリカード４００の保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に書き込まれる。
なお、メモリカード４００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、および保護領域に設定される区分領域（＃１，＃２・・・）単

位で書き込み（Ｗｒｉｔｅ）、読み取り（Ｒｅａｄ）の可否が設定される。

【０１９９】

ステップＳ３０１以下の処理は、図１６を参照して説明した処理と異なる処理となる。

ステップＳ３０１において、コンテンツサーバ２００はバインド鍵（Ｂｉｎｄｉｎｇ Ｋｅｙ（Ｋｂｉｎｄ））を例えば乱数生成処理によって生成する。バインド鍵（Ｂｉｎｄｉｎｇ Ｋｅｙ（Ｋｂｉｎｄ））は暗号化コンテンツの復号に適用するタイトル鍵の暗号化処理に利用される鍵である。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コ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鍵が生成されることになる。

【０２００】

サーバ２００の生成したバインド鍵（Ｂｉｎｄｉｎｇ Ｋｅｙ（Ｋｂｉｎｄ））は、メモリカード４００の保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）に書き込まれる。個別鍵（Ｋｉｎｄ）の書き込み処理と同様、メモリカードにおけるサーバ証明書の記録確認処理によってアクセス権限が確認された後に書き込み処理が行われることになる。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鍵（Ｂｉｎｄｉｎｇ Ｋｅｙ（Ｋｂｉｎｄ））４１４が記録される。

【０２０１】

なお、コンテンツサーバ２００からメモリカード４００へのバインド鍵の送信は、セッション鍵で暗号化したデータとして送信が行われる。

セッション鍵は、サーバ２００とメモリカード４００間の相互認証処理（ステップＳ２０１）時に生成され、双方で共有する鍵である。メモリカード４００は、暗号化されたバインド鍵をセッション鍵で復号してメモリカード４００の保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）４１２の所定の区分領域に記録する。

【０２０２】

図１７に示す（Ａ）コンテンツサーバ２００は、次に、生成したバインド鍵（Ｋｂｉｎｄ）と、（Ｃ）メモリカード４００から受領したメディアＩＤを利用して、ステップＳ３０２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鍵と呼ばれる。

なお、メディアＩＤは、メモリカード４００の識別情報としてメモリカード４００内のメモリに予め記録されたＩＤである。

【０２０３】

次に、コンテンツサーバ２００は、ステップＳ３０３において、コンテンツの暗号化鍵であるタイトル鍵（例えばＣＰＳユニット鍵）２１５をボリュームユニーク鍵で暗号化して暗号化タイトル鍵を生成する。

【０２０４】

コンテンツサーバ２００は生成した暗号化タイトル鍵をコンテンツ記録装置（ホスト）３００を介してメモリカード４００に送信する。メモリカード４００は、受信した暗号化タイトル鍵をメモリカード４００に記録する。この記録データが図１７のメモリカード４００中に示す暗号化タイトル鍵４１６である。なお、タイトル鍵はＣＰＳユニット鍵とも呼ばれる。

【０２０５】

さらに、コンテンツサーバ２００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Ｓ３０４でコンテンツサーバ２００の秘密鍵で署名処理を実行してメモリカード４００に提供する。

また、コンテンツサーバ２００は、ステップＳ３０５において、コンテンツ２１８をタイトル鍵２１５で暗号化する。

ここで生成する暗号化コンテンツは、例えば図３（ｃ１）に示す暗号化コンテンツである。各ユニットのブロックが、それぞれ各ユニットのシードを用いて生成された異なるブロック鍵（Ｋｂ１～Ｋｂｎ）によって暗号化された暗号化コンテンツである。

【０２０６】
メモリカード４００には、これらのサーバからの提供データが記録される。この記録データが図１７のメモリカード４００中に示す利用制御情報４１７、暗号化コンテンツ４１８である。
【０２０７】
［７．各装置のハードウェア構成例について］
最後に、図１８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１８を参照して、コンテンツ提供処理を実行するサーバ、および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クライアントとしての情報記録装置や情報再生装置のハードウェア構成例について説明する。
【０２０８】
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クライアント間の通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。
【０２０９】
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。
【０２１０】
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。
【０２１１】
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、プログラム等の各種データを取得する。例えば、取得されたプログラムに従ったデータ処理、あるいはコンテンツや鍵データを用いて、ＣＰＵによって実行するデータ処理、記録再生プログラムに従って鍵生成、コンテンツの暗号化、記録処理、復号、再生処理などが行われる。
【０２１２】
図１９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記録装置や再生装置等の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。

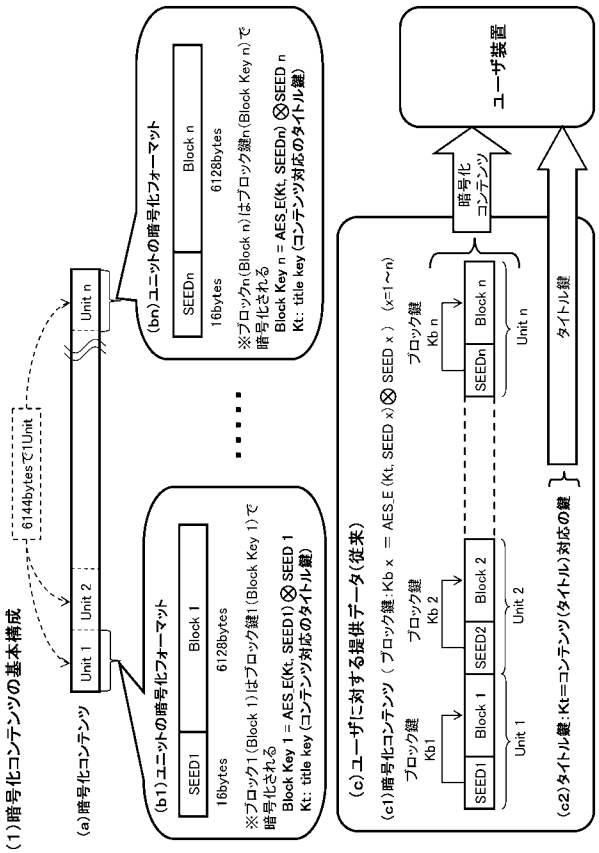
【０２１３】
ＣＰＵ８０１はバス８０４を介して入出力インタフェース８０５に接続され、入出力インタフェース８０５には、通信部８０６、記憶部８０７が接続されている。
【０２１４】
入出力インタフェース８０５に接続されている通信部８０６は、例えばサーバ、ホスト機器との通信を実行する。記憶部８０７は、データの記憶領域であり、先に説明したようにアクセス制限のある保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｅａ）８１１、自由にデータ記録読み取りができる非保護領域８１２を有する。

【０２１５】
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。
【０２１６】
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。
【０２１７】
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】
【０２１８】
以上、説明したように、本発明の一実施例の構成によれば、コンテンツの暗号鍵の漏洩に基づくコンテンツの不正利用を防止する構成が実現される。具体的には、記録装置がメモリカード等の記録メディアに対してサーバから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を記録する際、記録コンテンツ用の暗号鍵としてメディアに対する記録処理単位で異なる個別鍵を適用して暗号化を行い記録する。個別鍵は、サーバが記録メディアのアクセス制限領域である保護領域に書き込み、記録装置は、記録メディアの保護領域に書き込まれた個別鍵を読み出して暗号化処理を実行する。個別鍵はサーバにおいて生成され、個別鍵データは、コンテンツ記録処理を実行した装置情報等とともに管理情報としてサーバにおいて管理され、個別鍵が漏洩した場合は管理情報に基づいて個別鍵の漏洩元を追求することが可能となる。
【符号の説明】
【０２１９】
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　メモリカード

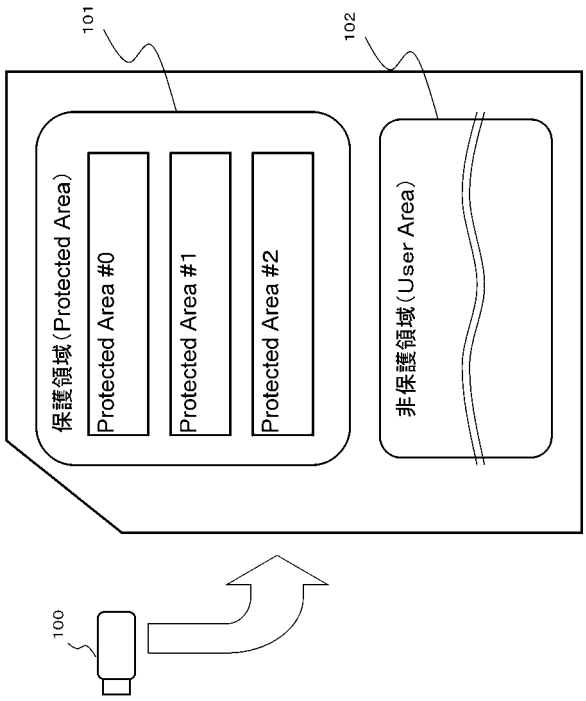
１０１　保護領域
１０２　非保護領域
１１１，１１２　区分領域
１２０　サーバ
１４０　ホスト装置
１５０　サーバ
１５１　個別鍵（Ｋｉｎｄ）
１５２　コンテンツ
１６０　記録装置
１７０　記録メディア
１７１　保護領域
１７２　非保護領域
１７３　個別鍵（Ｋｉｎｄ）
１７４　暗号化コンテンツ
１８０　ディスク
１８１　コンテンツ
２００　コンテンツサーバ
２１１　データベース（ＤＢ）
２１２　ボリュームＩＤ
２１３　トークン
２１４　ボリュームユニーク鍵
２１５　タイトル鍵（例えばＣＰＳユニット鍵）
２１６　利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）
２１７　コンテンツ
２１８　変換暗号化コンテンツ
２１９　暗号化シードファイル
３００　コンテンツ記録装置（ホスト）
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
４１３　個別鍵（Ｋｉｎｄ）
４１４　バインド鍵
４１５　トークン
４１６　暗号化タイトル鍵
４１７　利用制御情報
４１８　変換暗号化コンテンツ
４１９　暗号化シードファイル
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）

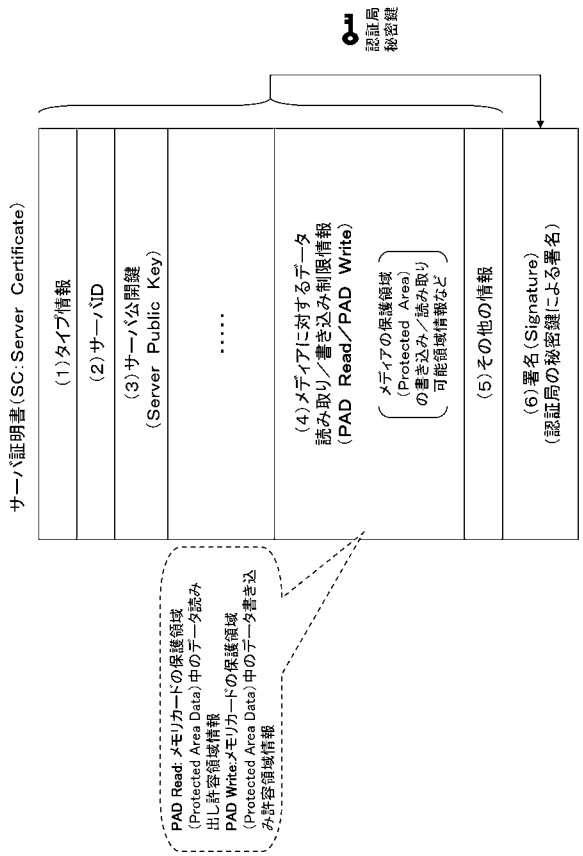
【図３】



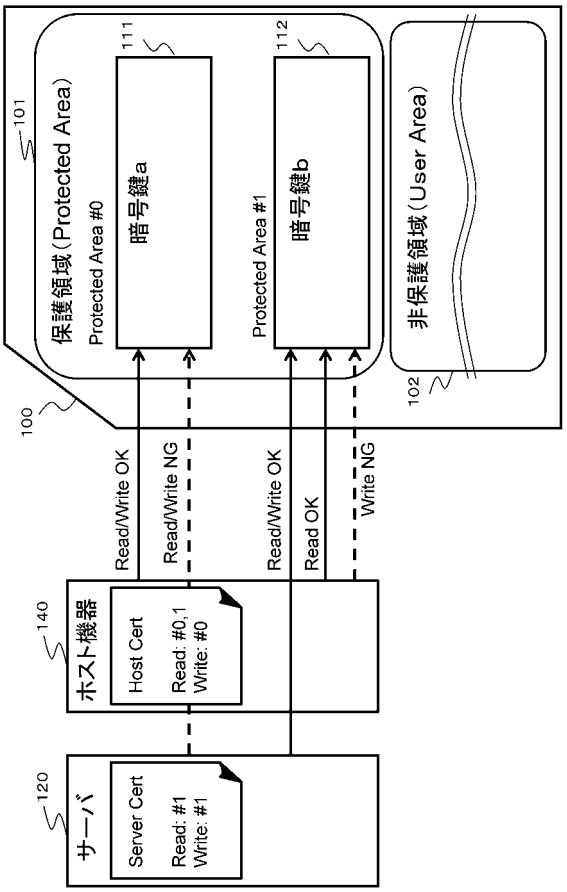
【図４】



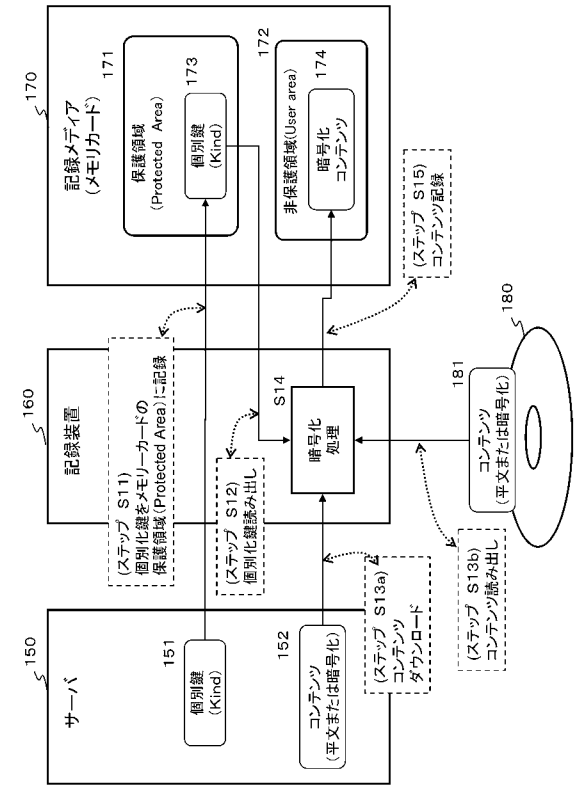
【図５】


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)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)
(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

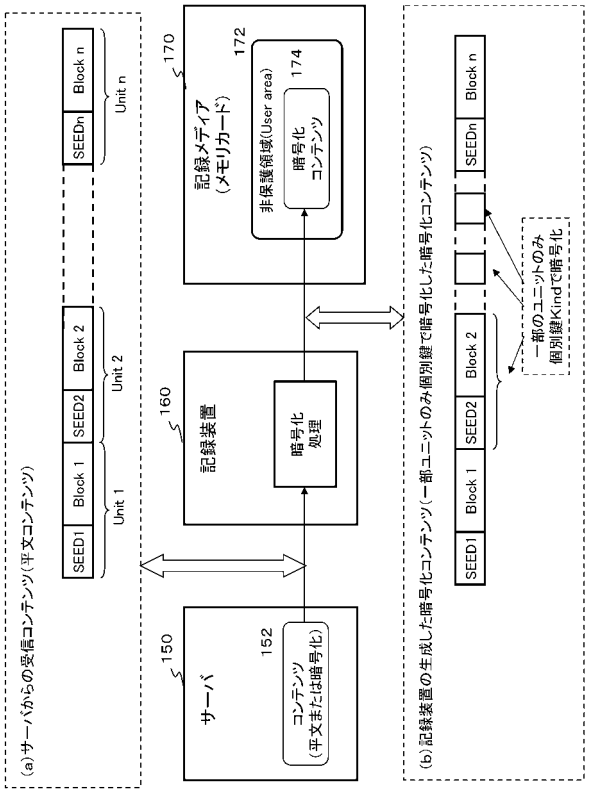
【図６】


101
保護領域(Protected Area)
Protected Area #0
111
暗号鍵a
Protected Area #1
112
暗号鍵b
非保護領域(User Area)
102
100
Read/Write OK
Read/Write NG
Read/Write OK
Read OK
Write NG
140
ホスト機器
Host Cert
Read: #0,1
Write: #0
120
サーバ
Server Cert
Read: #1
Write: #1

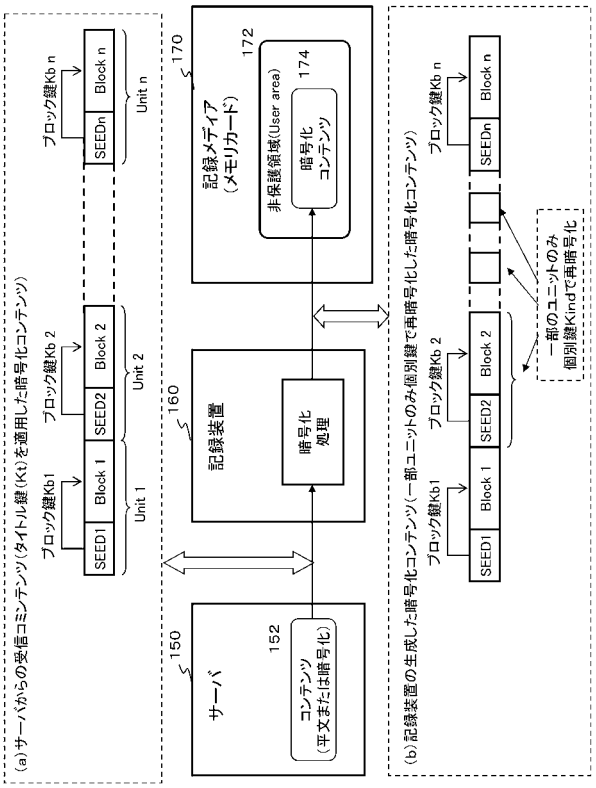
【図７】


150
サーバ
151
個別鍵
(Kind)
152
コンテンツ
(平文または暗号化)
160
記録装置
170
記録メディア
(メモリカード)
171
保護領域
(Protected Area)
173
個別鍵
(Kind)
172
非保護領域(User area)
174
暗号化
コンテンツ
(ステップ S11)
個別化鍵をメモリーカードの
保護領域(Protected Area)に記録
(ステップ S12)
個別化鍵読み出し
S14
暗号化
処理
(ステップ S13a)
コンテンツ
ダウンロード
(ステップ S13b)
コンテンツ読み出し
(ステップ S15)
コンテンツ記録
180
181
コンテンツ
(平文または暗号化)

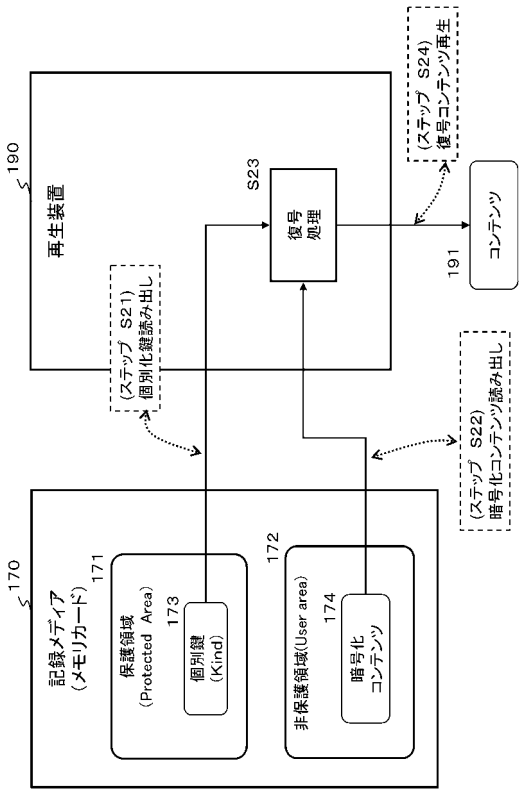
【図８】


(a)サーバからの受信コンテンツ(平文コンテンツ)
SEED1
Block 1
SEED2
Block 2
SEEDn
Block n
Unit 1
Unit 2
Unit n
150
サーバ
152
コンテンツ
(平文または暗号化)
160
記録装置
暗号化
処理
170
記録メディア
(メモリカード)
172
非保護領域(User area)
174
暗号化
コンテンツ
(b)記録装置の生成した暗号化コンテンツ(一部ユニットのみ個別鍵で暗号化した暗号化コンテンツ)
SEED1
Block 1
SEED2
Block 2
SEEDn
Block n
一部のユニットのみ
個別鍵Kindで暗号化

【図９】



【図１０】



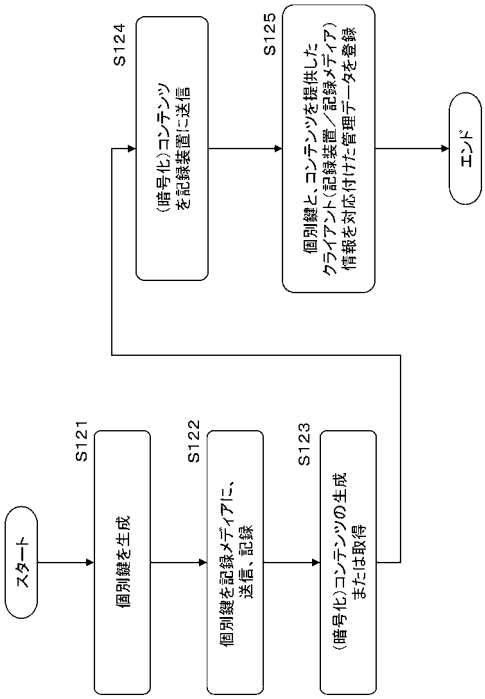
【図１２】

(サーバからタイトル鍵を用いた暗号化コンテンツとして提供する場合)

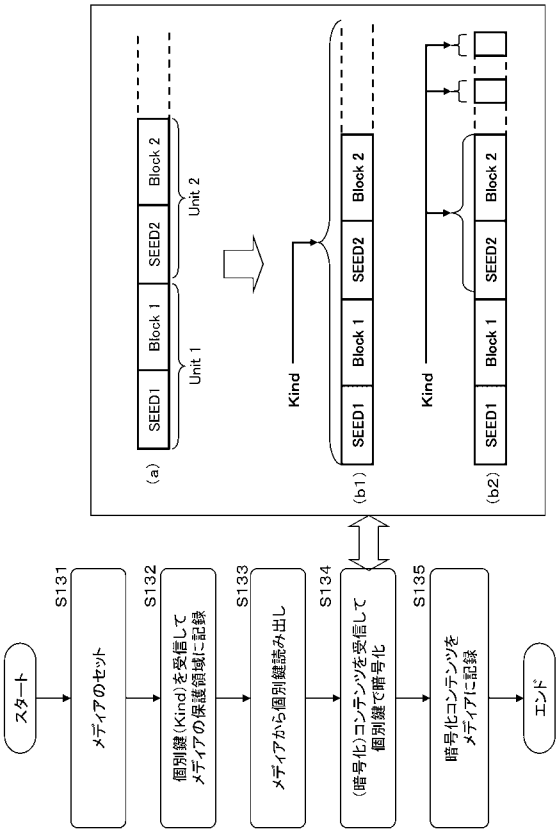
記録装置と記録メディアを個別に登録してもよい

配信処理固有ID	配信コンテンツ情報	個別鍵(Kind)情報	配信先情報	配信ユーザ	配信日時情報	タイトル鍵(Kt)情報
5784102578	ABCストーリー	2317cad･･･31	xyz@patnet.co.jp	スズキイチロウ	2010.07.22	154366･･･a21
2354711245	ABCストーリー	012ea765･･･22	jkl@ynos.ne.jp	タナカカオル	2010.09.15	154366･･･a21
･･	･･	･･	･･	･･	･･	･･

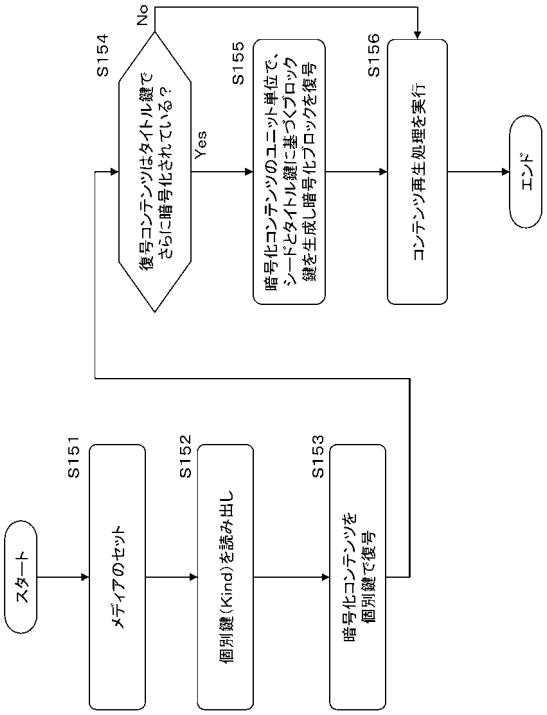
【図１３】



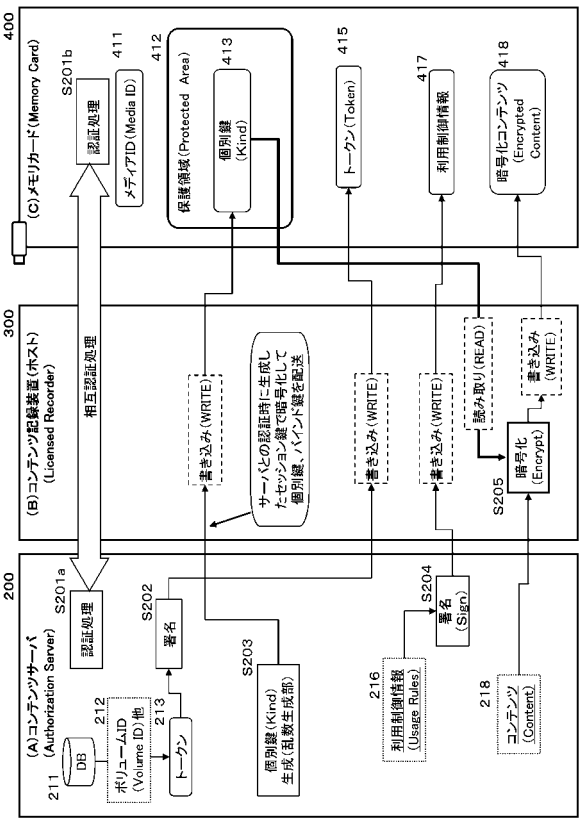
【図１４】



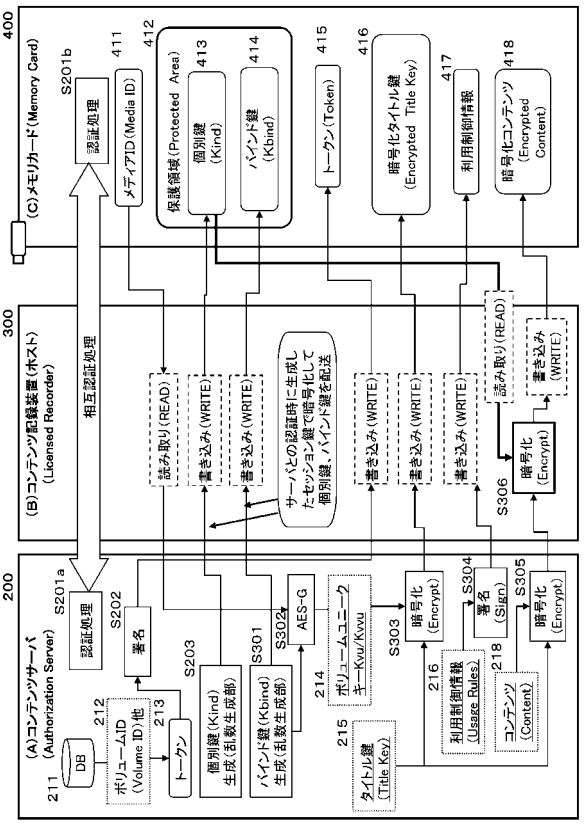
【図１５】



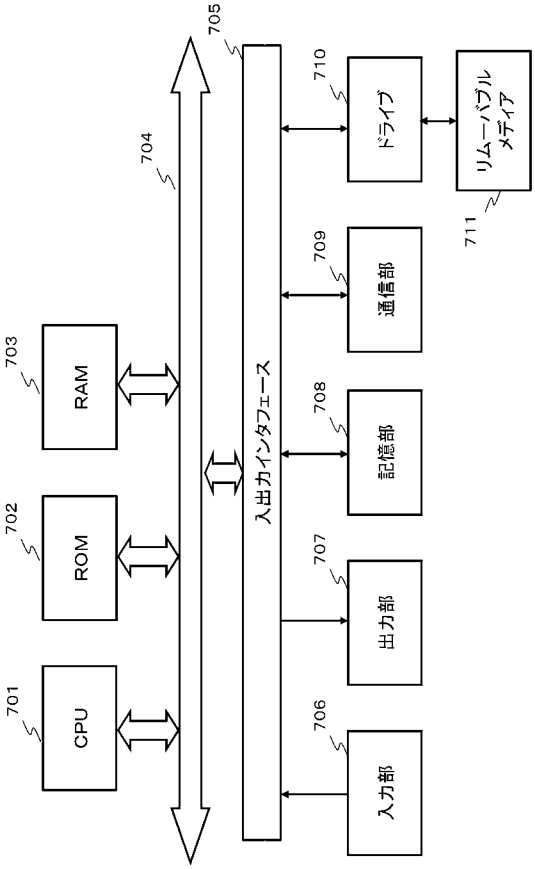
【図１６】



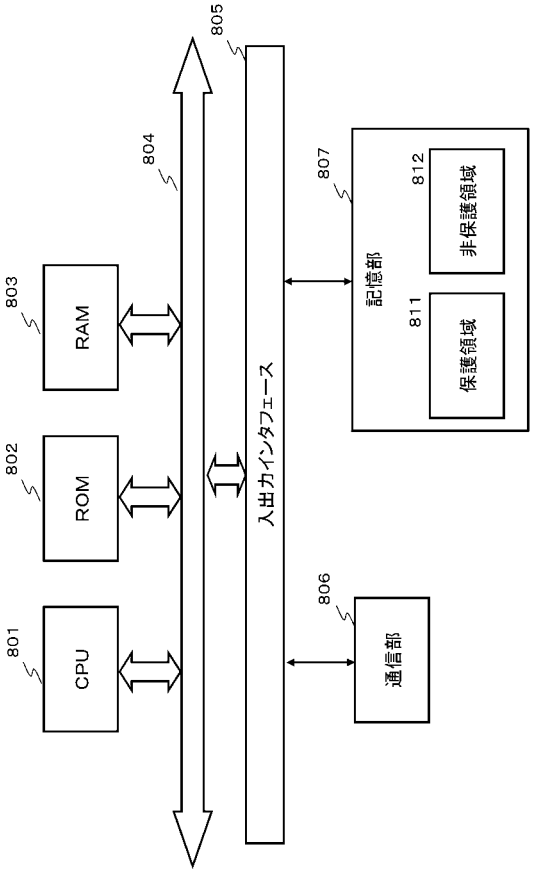
【図１７】



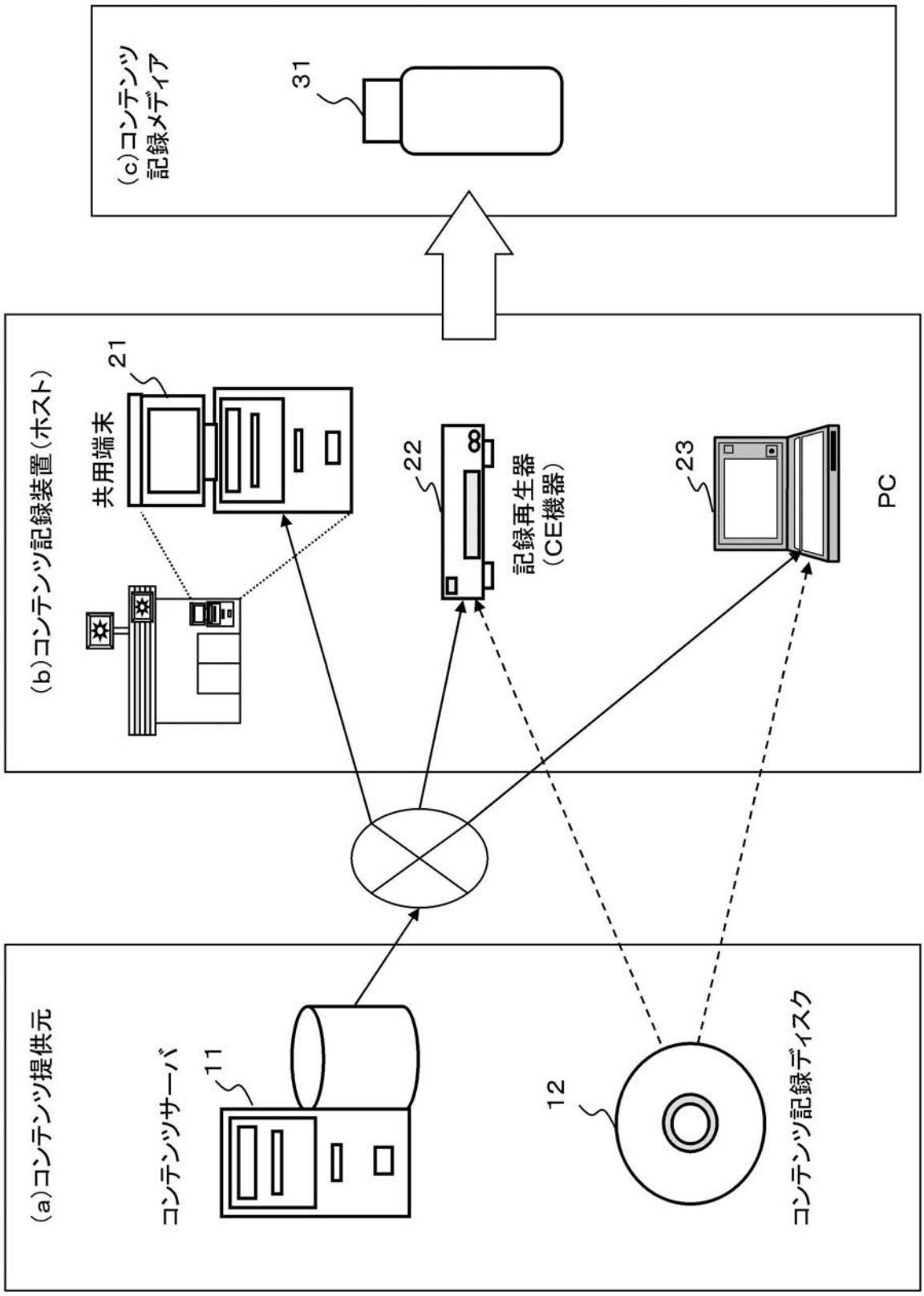
【図１８】


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

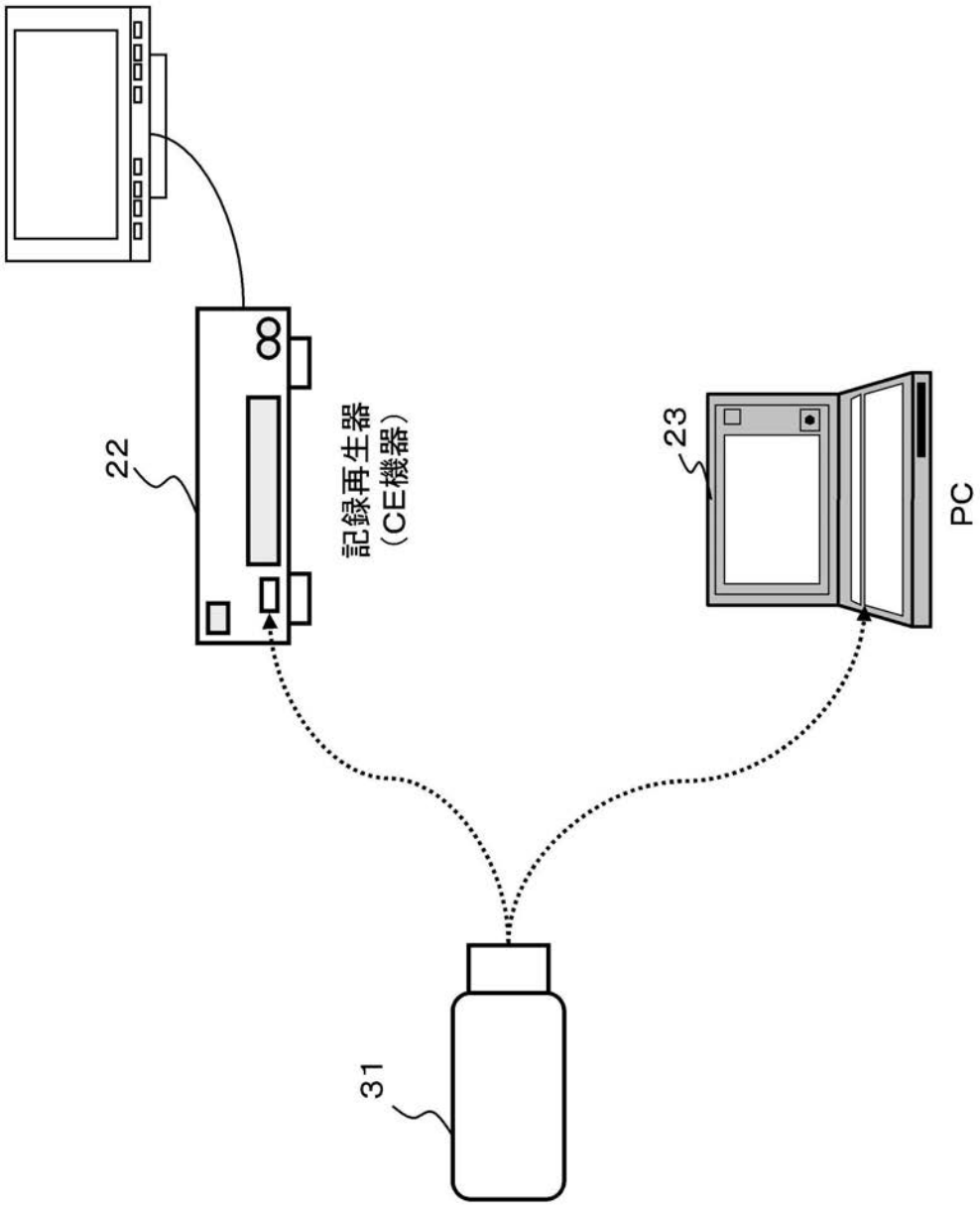
【図１９】


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

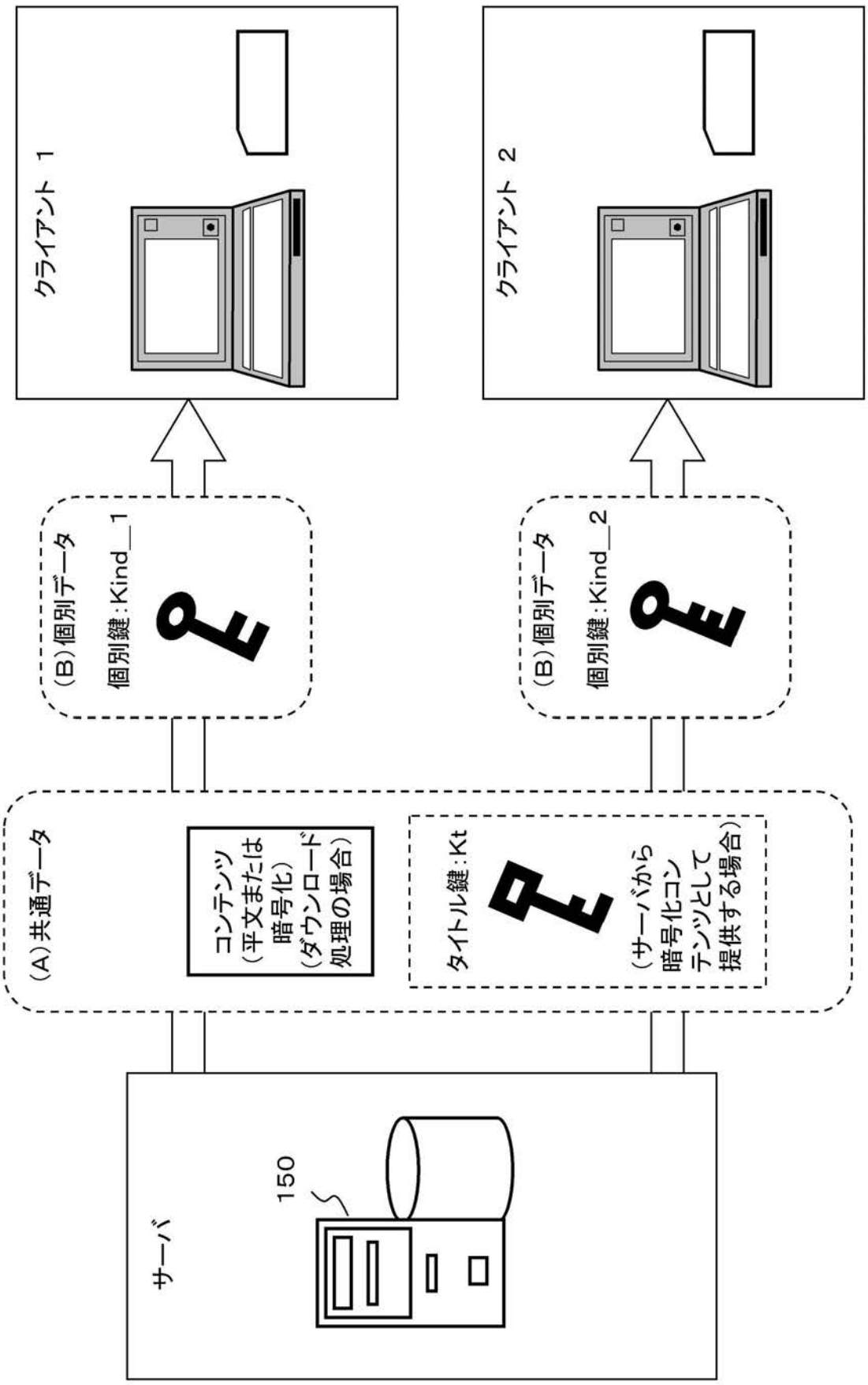
【図１】


(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
(b)コンテンツ記録装置(ホスト)
共用端末
21
22
記録再生器
(CE機器)
23
PC
(c)コンテンツ
記録メディア
31

【図２】



【図１１】


クライアント 1
クライアント 2
(B)個別データ
個別鍵:Kind_1
(B)個別データ
個別鍵:Kind_2
(A)共通データ
コンテンツ
(平文または
暗号化)
(ダウンロード
処理の場合)
タイトル鍵:Kt
(サーバから
暗号化コン
テンツとして
提供する場合)
サーバ
150

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　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　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
(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　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

審査官　石田　信行

(56)参考文献　特開２０１０－１４０２９８（ＪＰ，Ａ）
特開２００７－３３６０５９（ＪＰ，Ａ）
特開２００４－３２６２７７（ＪＰ，Ａ）
特開平０９－１７９７６８（ＪＰ，Ａ）
特開２０１０－００９７１４（ＪＰ，Ａ）
国際公開第２００６／０１３９２４（WO，Ａ１）
特開２００３－１１４８３０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／１４
Ｇ０６Ｆ　２１／１６
Ｇ０６Ｆ　２１／６２