(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6242036号
(P6242036)
(45)発行日　平成29年12月6日(2017.12.6)　(24)登録日　平成29年11月17日(2017.11.17)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601A
H04L 9/00 601E

請求項の数 14　(全 71 頁)

(21)出願番号　特願2011-251734(P2011-251734)
(22)出願日　平成23年11月17日(2011.11.17)
(65)公開番号　特開2013-110460(P2013-110460A)
(43)公開日　平成25年6月6日(2013.6.6)
審査請求日　平成26年10月20日(2014.10.20)
審判番号　不服2016-7426(P2016-7426/J1)
審判請求日　平成28年5月20日(2016.5.20)

(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
(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　久野　浩
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　林　隆道
東京都港区港南１丁目７番１号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、情報記憶装置、情報処理システム、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】
アクセス制限の設定された保護領域と、アクセス制限のない汎用領域を有する記憶部と、
外部装置からの前記保護領域に対するアクセス要求に応じて、アクセス可否を判定するデータ処理部を有し、
前記記憶部の前記汎用領域には、
前記暗号化コンテンツと、
前記暗号化コンテンツの復号、再生開始前に、署名検証成立の確認が要求される電子署名を格納した暗号化コンテンツ署名ファイルを格納し、
前記記憶部の前記保護領域には、
前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データであり、前記暗号化コンテンツの構成データおよび暗号鍵を含むデータに対する電子署名と前記暗号化コンテンツに対応して設定される利用制御情報を連結した連結データのハッシュ値と、前記暗号鍵との演算によって生成された変換暗号鍵を格納し、
前記データ処理部は、前記保護領域に対するアクセス要求装置から受領した証明書に基づいて、前記保護領域に対するアクセス可否を判定して、アクセス可の判定がなされたことを条件として、前記アクセス要求装置に対して、前記変換暗号鍵の読み出しを許容し、
前記記憶部から前記暗号化コンテンツを読み出して復号処理を実行する前記アクセス要求装置に、前記変換暗号鍵に対する前記電子署名と前記利用制御情報とを適用した演算で

あり、前記変換暗号鍵の生成時に用いた値を適用した演算による暗号鍵取得を行わせることを可能とした情報記憶装置。

【請求項２】

前記変換暗号鍵は、

前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算結果である請求項１に記載の情報記憶装置。

【請求項３】

前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵、さらに、前記暗号化コンテンツ署名ファイルの構成データを含むデータに対する電子署名である請求項１に記載の情報記憶装置。

【請求項４】

前記電子署名は、前記暗号化コンテンツ署名ファイルの構成データである前記暗号化コンテンツ署名ファイルの発行日時情報を含むデータに対する電子署名である請求項３に記載の情報記憶装置。

【請求項５】

メディアに記録された暗号化コンテンツの復号および再生処理を実行するデータ処理部を有し、

前記データ処理部は、

前記暗号化コンテンツの復号処理に際して、前記メディアに記録された前記暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を前記メディアから読み出し、該変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を実行し、

前記変換暗号鍵は、

前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データであり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と前記暗号化コンテンツに対応して設定される利用制御情報を連結した連結データのハッシュ値と、前記暗号鍵との演算によって生成された変換暗号鍵であり、

前記データ処理部は、

前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名と、

前記メディアに記録された利用制御情報を取得し、取得したデータの双方を適用した演算であり、前記変換暗号鍵の生成時に用いた値を適用した演算処理を実行して暗号鍵の取得処理を実行する情報処理装置。

【請求項６】

前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名である請求項５に記載の情報処理装置。

【請求項７】

前記変換暗号鍵は、

前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算結果であり、

前記データ処理部は、

前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名と、

前記メディアに記録された利用制御情報を取得し、取得したデータを適用した演算処理を実行して暗号鍵の取得処理を実行する請求項５に記載の情報処理装置。

【請求項８】

前記データ処理部は、

前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名に対する署名検証処理を実行し、

該署名検証処理に成功し、前記暗号化コンテンツ署名ファイルの正当性を確認したこと

を条件として、前記暗号鍵の取得処理を行う請求項５に記載の情報処理装置。
【請求項９】
メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理部を有し、
前記データ処理部は、
前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データであり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と前記暗号化コンテンツに対応して設定される利用制御情報を連結した連結データのハッシュ値と、前記暗号鍵の演算処理により、前記変換暗号鍵を生成する情報処理装置。
【請求項１０】
前記データ処理部は、
前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算を実行して前記変換暗号鍵を生成する請求項９に記載の情報処理装置。
【請求項１１】
情報処理装置において実行する情報処理方法であり、
データ処理部が、メディアに記録された暗号化コンテンツの復号処理に際して、復号に適用する暗号鍵の変換データである変換暗号鍵を前記メディアから読み出し、該変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を行うデータ処理ステップを実行し、
前記変換暗号鍵は、
前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データであり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と前記暗号化コンテンツに対応して設定される利用制御情報を連結した連結データのハッシュ値と、前記暗号鍵との演算によって生成された変換暗号鍵であり、
前記データ処理部は、前記データ処理部ステップにおいて、
前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名と、
前記メディアに記録された利用制御情報を取得し、取得したデータの双方を適用した演算であり、前記変換暗号鍵の生成時に用いた値を適用した演算処理を実行して暗号鍵の取得処理を実行する情報処理方法。
【請求項１２】
情報処理装置において実行する情報処理方法であり、
データ処理部が、メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理ステップを実行し、
前記データ処理ステップにおいて、
前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データであり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と前記暗号化コンテンツに対応して設定される利用制御情報を連結した連結データのハッシュ値と、前記暗号鍵の演算処理により、前記変換暗号鍵を生成する情報処理方法。
【請求項１３】
情報処理装置において情報処理を実行させるプログラムであり、
データ処理部に、メディアに記録された暗号化コンテンツの復号処理に際して、復号に適用する暗号鍵の変換データである変換暗号鍵を前記メディアから読み出す処理と、該変換暗号鍵に対する演算処理による暗号鍵の取得処理を行うデータ処理ステップを実行させ、
前記変換暗号鍵は、
前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成デー

タであり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と前記暗号化コンテンツに対応して設定される利用制御情報を連結した連結データのハッシュ値と、前記暗号鍵との演算によって生成された変換暗号鍵であり、

前記データ処理部ステップにおいて、

前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名と、

前記メディアに記録された利用制御情報を取得し、取得したデータの双方を適用した演算であり、前記変換暗号鍵の生成時に用いた値を適用した演算処理による暗号鍵の取得処理を実行させるプログラム。

【請求項１４】

情報処理装置において情報処理を実行させるプログラムであり、

データ処理部に、メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理ステップを実行させ、

前記データ処理ステップにおいて、

前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データであり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と前記暗号化コンテンツに対応して設定される利用制御情報を連結した連結データのハッシュ値と、前記暗号鍵の演算処理により、前記変換暗号鍵を生成させるプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本開示は、情報処理装置、情報記憶装置、情報処理システム、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を防止する情報処理装置、情報記憶装置、情報処理システム、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】

例えば映画や音楽などのコンテンツは、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、あるいはインターネット等のネットワーク、あるいは放送波などを介してユーザに提供される。ユーザは、例えばＰＣ、携帯端末、ＢＤプレーヤ等の記録再生装置、テレビなど様々な情報処理装置を利用して、コンテンツの再生を行うことができる。

【０００３】

しかし、これらユーザに提供される音楽データ、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、コンテンツ提供者は、ユーザにコンテンツを提供する場合、所定のコンテンツ利用制限が行う場合が多い。

【０００４】

デジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーコンテンツのインターネットを介した配信や、いわゆる海賊版ディスクの流通など不正コピーコンテンツの利用が蔓延しているといった問題が発生している。

このようなデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。

【０００５】

例えば、コンテンツ暗号化処理はその１つの態様である。暗号化データを復号するために用いる鍵が、コンテンツ利用権であるライセンスを受けた再生装置のみに与えられる。ライセンスは、例えば不正コピーを行わない等の所定の動作規定に従うように設計された

再生装置に対して与えられる。一方、ライセンスを受けていない再生装置は、暗号化されたデータを復号するための鍵を有していないため、暗号化データの復号を行うことができない。

【０００６】

しかしながら、このようなコンテンツの暗号化を実行しても、不正なコンテンツ利用が行われてしまうという現状がある。

具体的なコンテンツの不正利用の一例について説明する。

コンテンツサーバが、ユーザ機器、例えば記録再生機器や、ＰＣ、あるいは携帯端末等のユーザ機器に対して暗号化コンテンツを配信する構成を想定する。

【０００７】

コンテンツサーバが、ユーザ機器に対して暗号化コンテンツを配信する場合、コンテンツサーバは、

（ａ）暗号化コンテンツ

（ｂ）暗号化コンテンツの暗号化および復号に適用する暗号鍵

これらの各データを例えばネットワークを介してユーザ機器に配信する。

【０００８】

例えば同じ映画等の同一コンテンツを多数のユーザ機器に提供する場合、コンテンツサーバの実行する処理態様としては、例えば以下の２つの処理態様がある。

（Ａ）ユーザ機器各々に対して、個別の異なる暗号鍵を適用して異なる暗号化コンテンツを生成して提供する。

（Ｂ）複数のユーザ機器に対して、同一の暗号鍵で暗号化した同じ暗号化コンテンツを生成して提供する。

【０００９】

コンテンツの不正利用を防止するための安全性を考慮した場合、上記（Ａ）の処理は有効である。

しかし、上記（Ａ）の処理を行うためには、多数のユーザ各々に対して、個別の暗号鍵を設定して個別の暗号化コンテンツを生成する処理が必要となり、暗号鍵の生成、管理、暗号化コンテンツの生成処理等、コンテンツを配信するユーザ数に応じてサーバの処理負荷が増大するという問題が発生する。

【００１０】

従って、多くの場合上記（Ｂ）の処理、すなわち、同一コンテンツについては、同一の暗号鍵で暗号化した同じ暗号化コンテンツを生成して、複数のユーザに提供する処理が行われることが多い。

例えば、あるタイトルのコンテンツに対して、１つの暗号鍵（＝タイトルキー）を設定し、この１つのタイトルキーを適用して同一の暗号化コンテンツを生成して、

（ａ）暗号化コンテンツ、

（ｂ）タイトルキー

これらのデータセットを、多数のユーザに配信するものである。

このような処理を行うことで。コンテンツサーバの処理負荷は削減される。

【００１１】

なお、以下、コンテンツのタイトル単位で設定される暗号鍵を「タイトルキー」として説明する。

なお、タイトルキーは、そのタイトルの暗号化コンテンツの暗号化と復号処理に適用される。

【００１２】

しかし、このように、多数のユーザに同一のデータセット、すなわち、

（ａ）暗号化コンテンツ

（ｂ）タイトルキー

これらの同一のデータの組み合わせを配信すると、一部の「不正ユーザ」によって以下のような処理が行われる可能性がある。

【００１３】
（１）「不正ユーザ」が、サーバから受信したタイトルキーを読み出して、読み出したタイトルキーを不特定多数のユーザに対して公開する。
あるいは、
（２）「不正ユーザ」が、ある暗号化コンテンツＡに対応するタイトルキーＡを使用して、全く別のコンテンツＢを暗号化して、
（Ｘ）タイトルキーＡ、
（Ｙ）タイトルキーＡで暗号化した暗号化コンテンツＢ、
これらの組み合わせデータを不特定多数のユーザに配信する。
このような不正が実行される可能性がある。
【００１４】
例えば上記（１）の処理が行われると、不正公開されたタイトルキーを取得した多数のユーザによって、そのタイトルキーを利用して暗号化されたコンテンツが不正に利用される。
また、上記（２）の処理が行われると、上記の「不正ユーザ」の生成した不正なデータセット、すなわち、
（Ｘ）タイトルキーＡ、
（Ｙ）タイトルキーＡで暗号化した暗号化コンテンツＢ、
これらを「不正ユーザ」から取得することで、多数のユーザによって、暗号化コンテンツＢが不正に利用されてしまうことになる。
結果として、本来の正規なデータセット、すなわち、
暗号化コンテンツＢ、
暗号化コンテンツＢに対応するタイトルキーＢ、
これらのデータセットを正規に購入するユーザが減少し、著作権者や頒布権者の利益が著しく損なわれることになる。
【００１５】
さらに、具体的な不正処理例について説明する。
コンテンツサーバが、以下の（１）～（３）の暗号化コンテンツ（Ｃ）とタイトルキー（Ｋｔ）のデータセットを保持しているものとする。
（１）　（Ｋｔ１１，Ｃ１１）
（２）　（Ｋｔ１２，Ｃ１２）
（３）　（Ｋｔ１３，Ｃ１３）
ただし、
Ｃｎｎは、コンテンツファイル
Ｋｔｎｎは、コンテンツの暗号化に使用したタイトルキー
である。
（Ｋｔ１１，Ｃ１１）は、タイトルキー（Ｋｔ１１）と、タイトルキー（Ｋｔ１１）よって暗号化されたコンテンツ（Ｃ１１）のデータセットである。
【００１６】
例えば、ある「不正ユーザＵｘ」が、上記の３つのデータセット
（１）　（Ｋｔ１１，Ｃ１１）
（２）　（Ｋｔ１２，Ｃ１２）
（３）　（Ｋｔ１３，Ｃ１３）
これらを総て購入したとする。
この購入処理自体は、「不正ユーザＵｘ」の持つユーザ機器、例えばＰＣとコンテンツサーバとの所定の正当な購入手続に従って行われたものとする。
「不正ユーザＵｘ」は、ユーザ機器であるＰＣの例えばハードディスク等のメディアに上記の（１）～（３）のデータセットを記録する。
【００１７】
「不正ユーザＵｘ」は、ＰＣ等のユーザ機器ＰＣのハードディスク等のメディアから上

記の（１）～（３）のデータセットを読み出し、一旦、すべての暗号化コンテンツをそれぞれのタイトルキーで復号し、以下のデータを得る。
タイトルキー：Ｋｔ１１，Ｋｔ１２，Ｋｔ１３
復号コンテンツ：Ｃ１１，Ｃ１２，Ｃ１３
なお、正当な再生機器において、正規のコンテンツ再生プログラムを利用する場合にはタイトルキーを外部に読み出すことはできないが、ＰＣ等の装置に不正プログラムをインストールするなどの方法によって、タイトルキー自体が読み出されてしまう可能性があり、タイトルキーの読み出しを完全に防止することは困難であるというのが現状である。

【００１８】
さらに、「不正ユーザＵｘ」は、
復号コンテンツ：Ｃ１１～Ｃ１３を連結したデータ、
Ｃ１１｜｜Ｃ１２｜｜Ｃ１３
を生成し、
この連結データをタイトルキー：Ｋｔ１１で暗号化する。
すなわち、以下のデータセット、
（Ｋｔ１１，Ｃ１１｜｜Ｃ１２｜｜Ｃ１３）
を生成し、このデータセットを、ネットワークを介して不正に流通、例えば安い価格で販売、あるいは無償で多くのユーザに提供するといったことを行う。

【００１９】
このような処理が行われると、
多くの一般ユーザは、上記の「不正ユーザＵｘ」から、上記の不正作成データセット、すなわち、
（Ｋｔ１１，Ｃ１１｜｜Ｃ１２｜｜Ｃ１３）
上記の不正データセットを取得することが可能となる。
このデータセットは、
（ａ）タイトルキーＫｔ１１で暗号化された暗号化コンテンツ
（ｂ）タイトルキーＫｔ１１、
これらのデータセットによって構成されており、
正規のコンテンツ提供者からユーザに提供されるデータセットコンテンツと同一のデータ構成を有している。

【００２０】
そのため、ライセンスを持つ正当なコンテンツ再生プログラムを持つ正当な再生機器は、タイトルキーＫｔ１１を利用して、何ら問題なく暗号化コンテンツ［Ｃ１１｜｜Ｃ１２｜｜Ｃ１３］を復号、再生してしまうことができる。
結果として、正規なコンテンツ購入が行われることなく、不正利用が蔓延し、Ｃ１１～Ｃ１３等のコンテンツを正規に購入するユーザが減少により、正当権利者の利益が損なわれることになる。

【００２１】
さらに具体化して説明する。例えば、あるドラマなど、１話～１２話の１２タイトルからなるシリーズコンテンツにおいて、
１話＝（Ｋｔ０１，Ｃ０１）
２話＝（Ｋｔ０２，Ｃ０２）
３話＝（Ｋｔ０３，Ｃ０３）
：　　：
１２話＝（Ｋｔ１２，Ｃ１２）
上記のように各話単位で、コンテンツの購入単位を設定としているとする。

【００２２】
このような場合に、ある１人の「不正ユーザ」が１話～１２話の１２タイトルのシリーズ全てを購入して、１話～１２話のコンテンツ：Ｃ０１～Ｃ１２を連結して、１話対応のタイトルキー：Ｋｔ０１で再暗号化したデータセット、すなわち、

（Ｋｔ０１，Ｃ０１｜｜Ｃ０２｜｜Ｃ０３・・・｜｜Ｃ１２）
を生成して、ネットワーク上で公開してしまう。あるいは不正に販売するといった処理を行う。

【００２３】
このような場合、多数のユーザ機器において、「不正ユーザ」の生成した不正データセット、
（Ｋｔ０１，Ｃ０１｜｜Ｃ０２｜｜Ｃ０３・・・｜｜Ｃ１２）
を取得して再生、利用してしまうといったことが可能となる。
例えば、上記の１２話の各々の１話単位の正規価格が￥２，０００であるとする。
この場合、１２話全話を購入すると、
１２×￥２，０００＝￥２４，０００
である。

【００２４】
上記の「不正ユーザ」は、上記の不正データセット、
（Ｋｔ０１，Ｃ０１｜｜Ｃ０２｜｜Ｃ０３・・・｜｜Ｃ１２）
を、例えば￥６，０００で販売する。この場合、多くのユーザがこの安いコンテンツを購入してしまい、結果として、正規なコンテンツ販売が阻害され、本来の著作権者や販売権者の利益、権利が侵害されることになる。

【００２５】
上記の例の他、ある１つのコンテンツＣ１１に対応して設定されたタイトルキーＫｔ１１を、その他の無関係の様々なコンテンツＣｘｘの暗号化に利用して、
（Ｋｔ１１，Ｃｘｘ）
コンテンツ、Ｃｘｘを様々なコンテンツとすることが可能であり、無制限にすべてのコンテンツを１つのタイトルキーで復号、再生することが可能となるという問題が発生する。
すなわち、平文コンテンツの再生を禁止した再生機器を作成したとしても、上記の不正なデータセットの利用により、正規購入コンテンツと同様の復号、再生が可能になってしまう。

【００２６】
さらに「不正ユーザ」は、タイトルキーのすげかえ、再暗号化をサービスとして立ち上げることも可能となり、あたかもオーソライズされたサーバかのごとく振舞える。

【００２７】
このように、コンテンツの暗号化処理という対策のみでは、コンテンツの不正利用を防止することが困難になっている。

【００２８】
暗号化処理と異なるコンテンツ不正利用排除手法として、再生装置にコンテンツの改ざん検証を実行させる手法がある。この手法を適用することで、例えば不正コンテンツの流通過程において、コンテンツに何等かの変更（改ざん）が行われた場合にその改ざんコンテンツの利用を停止させることができる。

【００２９】
具体的には、コンテンツ再生を実行するユーザ装置において、コンテンツの改ざんの有無検証処理を実行させて、コンテンツに改ざんがないことが確認された場合にのみコンテンツ再生を許容し、改ざんがあることが判明した場合には、コンテンツの再生を実行しない構成とする制御構成である。

【００３０】
例えば、特許文献１（特開２００２－３５８０１１号公報）には、再生予定のコンテンツファイルからハッシュ値を計算し、予め用意された照合用ハッシュ値、すなわち正当なコンテンツデータに基づいて予め計算済みの照合用ハッシュ値との比較を実行し、新たに算出したハッシュ値が照合用ハッシュ値と一致した場合には、コンテンツの改ざんは無いと判定して、コンテンツの再生処理に移行する制御構成を開示している。

【００３１】
しかし、このようにハッシュ値をコンテンツに基づいて算出する処理を実行する場合、ハッシュ値算出の元データとしてのコンテンツデータの容量が大きい場合、計算に要する処理負荷、処理時間が多大なものとなる。昨今では動画像データの高品質化が進み、１コンテンツあたり、数ＧＢ～数十ＧＢのデータ量を持つ場合が多くなっている。このような大容量データに基づくコンテンツのハッシュ値算出処理を、コンテンツ再生を実行するユーザ機器に行わせることは、ユーザ機器に求められるデータ処理能力が過大になるという問題、さらに、コンテンツの検証に要する時間が長くなり、コンテンツ再生処理が効率的に行われないという問題が発生する。
【００３２】
また、特許文献２（特許第４５７６９３６号）には、情報記録媒体の格納コンテンツの細分化データとして設定されたハッシュユニット各々についてのハッシュ値をコンテンツハッシュテーブルに記録してコンテンツとともに情報記録媒体に格納した構成を開示している。
【００３３】
この開示構成によれば、コンテンツ再生を実行する情報処理装置は、ランダムに選択した１つ以上のハッシュユニットに基づいてハッシュ値照合処理を実行する。本構成によりコンテンツのデータ量にかかわらず、少ないデータ量のハッシュユニットに基づくハッシュ値の算出、照合処理が可能となり、コンテンツ再生を実行するユーザ機器における効率的なコンテンツ検証が可能となる。
【００３４】
しかし、特許文献２に記載の構成は、情報記録媒体の格納コンテンツに対する処理を前提としている。この開示構成は、例えば情報記録媒体の製造時にコンテンツとともにハッシュ値も併せて記録できる場合には利用可能であるが、例えばサーバからのダウンロードコンテンツに対して適用することは困難であるという問題がある。
【００３５】
また、上記の特許文献１、特許文献２は、いずれもコンテンツの改ざん検証に重点をおいており、改ざんのない不正コピーコンテンツの流通に対しては、何ら制御することができないという問題がある。
このように、従来技術としてのコンテンツの暗号化や、改ざん検証処理は、不正コピーコンテンツの流通や、コンテンツ暗号鍵の漏えいに対して、十分な防止効果を奏していないというのが現状である。
【先行技術文献】
【特許文献】
【００３６】
【特許文献１】特開２００２－３５８０１１号公報
【特許文献２】特許第４５７６９３６号
【発明の概要】
【発明が解決しようとする課題】
【００３７】
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、コンテンツの不正利用の効果的な防止を実現する情報処理装置、情報記憶装置、情報処理システム、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】
【００３８】
本開示の第１の側面は、
暗号化コンテンツおよび暗号化コンテンツの復号に適用する暗号鍵を格納する記憶部を有し、
前記記憶部は、前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵を

格納し、
前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名であり、
前記記憶部から前記暗号化コンテンツを読み出して復号処理を実行する再生装置に、前記変換暗号鍵に対する電子署名の適用演算による暗号鍵取得を行わせることを可能とした情報記憶装置にある。
【００３９】
さらに、本開示の情報記憶装置の一実施態様において、前記変換暗号鍵は、前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算結果である。
【００４０】
さらに、本開示の情報記憶装置の一実施態様において、前記記憶部は、アクセス制限の設定された保護領域を有し、前記変換暗号鍵を、前記保護領域に格納した構成である。
【００４１】
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、前記保護領域に対するアクセス要求装置から受領した証明書に基づいて、前記保護領域に対するアクセス可否を判定するデータ処理部を有する。
【００４２】
さらに、本開示の情報記憶装置の一実施態様において、前記記憶部は、アクセス制限の設定された保護領域と、アクセス制限のない汎用領域を有し、前記変換暗号鍵を、前記保護領域に格納し、前記暗号化コンテンツと、前記暗号化コンテンツ署名ファイルを、前記汎用領域に格納した構成である。
【００４３】
さらに、本開示の情報記憶装置の一実施態様において、前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵、さらに、前記暗号化コンテンツ署名ファイルの構成データを含むデータに対する電子署名である。
【００４４】
さらに、本開示の情報記憶装置の一実施態様において、前記電子署名は、前記暗号化コンテンツ署名ファイルの構成データである前記暗号化コンテンツ署名ファイルの発行日時情報を含むデータに対する電子署名である。
【００４５】
さらに、本開示の第２の側面は、
メディアに記録された暗号化コンテンツの復号および再生処理を実行するデータ処理部を有し、
前記データ処理部は、
前記暗号化コンテンツの復号処理に際して、前記メディアに記録された前記暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を読み出し、該変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を実行し、
前記変換暗号鍵は、
前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、
前記データ処理部は、
前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する情報処理装置にある。
【００４６】
さらに、本開示の情報処理装置の一実施態様において、前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名である。
【００４７】
さらに、本開示の情報処理装置の一実施態様において、前記変換暗号鍵は、前記暗号化

コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算結果であり、前記データ処理部は、前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名と、前記メディアに記録された利用制御情報を取得し、取得したデータを適用した演算処理を実行して暗号鍵の取得処理を実行する。

【００４８】

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、前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名に対する署名検証処理を実行し、該署名検証処理に成功し、前記暗号化コンテンツ署名ファイルの正当性を確認したことを条件として、前記暗号鍵の取得処理を行う。

【００４９】

さらに、本開示の第３の側面は、

メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理部を有し、

前記データ処理部は、

前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名であり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と、前記暗号鍵の演算処理により、前記変換暗号鍵を生成する情報処理装置にある。

【００５０】

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、前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算を実行して前記変換暗号鍵を生成する。

【００５１】

さらに、本開示の第４の側面は、

情報処理装置において実行する情報処理方法であり、

データ処理部が、メディアに記録された暗号化コンテンツの復号処理に際して、復号に適用する暗号鍵の変換データである変換暗号鍵を読み出し、該変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を行うデータ処理ステップを実行し、

前記変換暗号鍵は、

前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、

前記データ処理部は、前記データ処理部ステップにおいて、

前記メディアに記録された暗号化コンテンツ署名ファイルから前記電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する情報処理方法にある。

【００５２】

さらに、本開示の第５の側面は、

情報処理装置において実行する情報処理方法であり、

データ処理部が、メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理ステップを実行し、

前記データ処理ステップにおいて、

前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名であり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と、前記暗号鍵の演算処理により、前記変換暗号鍵を生成する情報処理方法にある。

【００５３】

さらに、本開示の第６の側面は、

情報処理装置において情報処理を実行させるプログラムであり、
データ処理部に、メディアに記録された暗号化コンテンツの復号処理に際して、復号に適用する暗号鍵の変換データである変換暗号鍵の読み出し処理と、該変換暗号鍵に対する演算処理による暗号鍵の取得処理を行うデータ処理ステップを実行させ、
前記変換暗号鍵は、
前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、
前記データ処理部ステップにおいて、
前記メディアに記録された暗号化コンテンツ署名ファイルから前記電子署名の取得処理と、取得した電子署名を適用した演算処理による暗号鍵の取得処理を実行させるプログラムにある。

【００５４】

さらに、本開示の第７の側面は、
情報処理装置において情報処理を実行させるプログラムであり、
データ処理部に、メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理ステップを実行させ、
前記データ処理ステップにおいて、
前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名であり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と、前記暗号鍵の演算処理により、前記変換暗号鍵を生成させるプログラムにある。

【００５５】

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。

【００５６】

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】

【００５７】

本開示の一実施例の構成によれば、コンテンツの不正利用を効果的に防止する装置、方法が実現される。

具体的には、暗号化コンテンツの復号処理に際して、メディアに記録された暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を読み出し、変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を実行する。変換暗号鍵は、暗号鍵と、暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、再生装置は、メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する。電子署名は、暗号化コンテンツの構成データおよび暗号鍵を含むデータに対する電子署名として設定される。

この暗号化コンテンツ署名ファイルの署名データを変換暗号鍵の構成データとすることで、鍵の掛け替え処理などによるコンテンツ不正利用を防止することが可能となる。

【図面の簡単な説明】

【００５８】

【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】コンテンツの不正利用を防止するための本開示の情報処理システムの全体構成について説明する図である。
【図８】コンテンツの不正利用を防止するために適用するデータの各装置間の流れについて説明する図である。
【図９】暗号化コンテンツ署名ファイル（ＥＣＳファイル）の構成例について説明する図である。
【図１０】暗号化コンテンツ署名ファイル（ＥＣＳファイル）の構成例について説明する図である。
【図１１】暗号化コンテンツ署名ファイル（ＥＣＳファイル）に含まれるＥＣＳ発行装置証明書の構成例について説明する図である。
【図１２】ＥＣＳ発行装置証明書リボケーションリストの構成例について説明する図である。
【図１３】暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成処理とデータ構成の概要について説明する図である。
【図１４】暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成とコンテンツ提供、利用処理シーケンスについて説明するシーケンス図である。
【図１５】暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成とコンテンツ提供、利用処理シーケンスについて説明するシーケンス図である。
【図１６】暗号化コンテンツ署名ファイル（ＥＣＳファイル）に記録された日時データを適用したコンテンツ提供可否判定処理のシーケンスについて説明するフローチャートを示す図である。
【図１７】暗号化コンテンツ署名ファイル（ＥＣＳファイル）に記録された日時データを適用したコンテンツ提供可否判定処理のシーケンスについて説明するフローチャートを示す図である。
【図１８】暗号化コンテンツ署名ファイル（ＥＣＳファイル）に記録された日時データを適用したコンテンツ再生可否判定処理の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１９】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２０】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２１】メモリカードに対する記録データの構成例について説明する図である。
【図２２】メモリカードに対する記録データの構成例について説明する図である。
【図２３】メモリカードの汎用領域に記録される利用制御情報の記録データの構成例について説明する図である。
【図２４】すげ替え処理による不正なコンテンツ利用例について説明する図である。
【図２５】すげ替え処理による不正なコンテンツの記録処理例について説明するフローチャートを示す図である。
【図２６】すげ替え処理によって記録した不正コンテンツの再生が実行できないことを説明するフローチャートを示す図である。
【図２７】すげ替え処理による不正なコンテンツ利用例について説明する図である。
【図２８】すげ替え処理による不正なコンテンツの記録処理例について説明するフローチ

ャートを示す図である。
【図２９】すげ替え処理によって記録した不正コンテンツの再生が実行できないことを説明するフローチャートを示す図である。
【図３０】暗号化コンテンツ署名ファイル（ＥＣＳファイル）に記録されたブロック識別子と利用制御情報ファイルに記録されたブロック識別子について説明する図である。
【図３１】暗号化コンテンツ署名ファイル（ＥＣＳファイル）に記録されたブロック識別子と利用制御情報ファイルに記録されたブロック識別子を適用したコンテンツ提供可否判定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３２】ＥＣＳ発行装置証明書からのブロック識別子読み出し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３３】暗号化コンテンツ署名ファイル（ＥＣＳファイル）に記録されたブロック識別子と利用制御情報ファイルに記録されたブロック識別子を適用したコンテンツ再生可否判定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３４】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３５】メモリカード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。
【発明を実施するための形態】
【００５９】
以下、図面を参照しながら本開示の情報処理装置、情報記憶装置、情報処理システム、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．暗号化コンテンツ署名（ＥＣＳ）発行装置を利用したコンテンツ提供システムについて
６．ＥＣＳファイルの構成例について
７．ＥＣＳ発行装置証明書リボケーションリストの構成について
８．暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成処理について
９．ＥＣＳファイル、ＥＣＳ発行装置証明書の日時情報を適用した処理について
１０．暗号鍵とＥＣＳ発行装置署名との関連づけ構成について
１１．暗号化コンテンツ署名（ＥＣＳ）ファイルに記録したブロック識別子の適用処理について
１２．各装置のハードウェア構成例について
１３．本開示の構成のまとめ
【００６０】
［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。
【００６１】
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）コンテンツ提供装置
（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。
【００６２】
（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。

なお、以下の実施例では、コンテンツ提供装置が提供するコンテンツは暗号化コンテンツである例を代表例として説明するが、本開示の構成は、提供コンテンツが暗号化コンテンツである場合に限らず、暗号化されていない平文コンテンツである場合にも適用可能である。

【００６３】

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。

【００６４】

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。

コンテンツ提供装置は、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。

【００６５】

（ａ）コンテンツ提供装置は、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をコンテンツ提供装置として示している。

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。

【００６６】

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。

【００６７】

（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）コンテンツ提供装置である放送局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。

【００６８】

（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。

【００６９】

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。

【００７０】

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。

【００７１】

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。

【００７２】

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。

【００７３】

［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。

【００７４】

（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。

【００７５】

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。

【００７６】

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。

【００７７】
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。
【００７８】
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。
【００７９】
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。
【００８０】
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。
【００８１】
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。
【００８２】
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。
【００８３】
［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。
【００８４】
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。
【００８５】
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。

【００８６】

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。

【００８７】

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。

【００８８】

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。

【００８９】

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（Ｓｉｇｎａｕｒｅ）

【００９０】

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。

【００９１】

（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。

【００９２】

（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。
【００９３】
（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。
【００９４】
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。
【００９５】
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装置のすべて、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。
【００９６】
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。
【００９７】
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）
【００９８】
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。
【００９９】

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。

【０１００】

［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。

【０１０１】

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。

【０１０２】

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。

【０１０３】

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。

【０１０４】

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の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。

【０１０５】

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。

【０１０６】

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。

【０１０７】

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。

【０１０８】
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。

【０１０９】
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。

【０１１０】
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。

【０１１１】
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。

【０１１２】
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。

【０１１３】
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）８

０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。

【０１１４】

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。

【０１１５】

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。

【０１１６】

［５．暗号化コンテンツ署名（ＥＣＳ）発行装置を利用したコンテンツ提供システムについて］

先に図１を参照して説明したように、ユーザ装置に提供されるコンテンツはコンテンツ提供装置から提供される。しかし、このコンテンツ提供装置自身が、不正なコピーコンテンツを配信する場合もある。以下では、このようなサーバの不正処理など、ユーザ装置以外の構成による不正についても防止可能とした構成について説明する。

【０１１７】

図７を参照して、コンテンツの不正利用を防止するための本開示の情報処理システムの全体構成について説明する。

図７には、情報処理システムの全体構成例を示している。図７には以下の４種類の装置を階層構成として示している。

（Ａ）ライセンス発行装置（ＬＡ）１０１

（Ｂ）暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２－１～ｎ

（Ｃ）コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３－１～ｍ

（Ｄ）ユーザ装置（コンテンツ再生装置）１０４－１～ｆ

【０１１８】

図７に示す（Ｃ）コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３－１～ｍは、図１に示す放送局１１、コンテンツサーバ１２等に対応する。

また、図７に示す（Ｄ）ユーザ装置（コンテンツ再生装置）１０４－１～ｆは、図１に示す記録再生専用器２１、ＰＣ２２、携帯端末２３等のユーザ装置に対応する。

【０１１９】

（Ｃ）コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３－１～ｍは、コンテンツサーバや放送局、さらにはコンテンツを格納したディスク等のメディアを提供するメディア提供会社などコンテンツを送信する装置や、メディアに対するコンテンツ記録を実行する装置など、様々な情報処理装置を含む。これらは多数存在する。

【０１２０】

（Ｄ）ユーザ装置（コンテンツ再生装置）１０４－１～ｆは、コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３－１～ｍからコンテンツ、例えば映画、音楽、その他の様々なコンテンツをインターネットや放送波、あるいはディスク等のメディアを介して受信、または読み出して再生処理を実行する装置である。具体的にはＰＣ、携帯端末、ＤＶＤプレーヤ、ＢＤプレーヤ、テレビなどコンテンツ再生可能な様々な種類の情報処理装置が含まれる。

【０１２１】
（Ｂ）暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２－１～ｎは、（Ｃ）コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３－１～ｍの提供するコンテンツに対応する暗号化コンテンツ署名ファイル（ＥＣＳファイル：Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｆｉｌｅ）を生成する。
【０１２２】
（Ｃ）コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３－１～ｍは、例えば、新たな映画コンテンツなどのコンテンツをユーザ装置１０４に提供する場合、そのコンテンツに対応する暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成依頼を、暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２に対して行う。
【０１２３】
（Ｂ）暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２－１～ｎは、この依頼に応じて、暗号化コンテンツ署名ファイル（ＥＣＳファイル）を生成して、（Ｃ）コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３に提供する。
なお、この暗号化コンテンツ署名ファイル（ＥＣＳファイル）の具体的な構成と生成処理については後段で詳細に説明する。
【０１２４】
（Ｃ）コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３は、（Ｂ）暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２から暗号化コンテンツ署名ファイル（ＥＣＳファイル）を受領し、これを、暗号化コンテンツに併せて（Ｄ）ユーザ装置（コンテンツ再生装置）１０４に提供する。
【０１２５】
（Ｄ）ユーザ装置（コンテンツ再生装置）１０４は、コンテンツの再生を行う前に、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の署名検証処理を行い、この署名検証処理の成立が確認された場合にのみ、コンテンツの復号、再生が許容される。
なお、ユーザ装置（コンテンツ再生装置）１０４には、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の署名検証を条件としてコンテンツの復号、再生を実行するシーケンスに従った再生処理プログラムが格納されており、この再生処理プログラムに従って暗号化コンテンツ署名ファイル（ＥＣＳファイル）の署名検証等のコンテンツ再生可否判定処理と、コンテンツ再生が実行されることになる。
例えば、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の署名検証が成功しなかった場合は、コンテンツの再生は禁止される。
【０１２６】
（Ａ）ライセンス発行装置（ＬＡ）１０１は、（Ｂ）暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２－１～ｎに対して、ＥＣＳファイルの発行許可証としてのライセンスを提供する。
【０１２７】
（Ａ）ライセンス発行装置（ＬＡ）１０１は、予め既定したライセンス発行シーケンスにしたがって、（Ｂ）暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２－１～ｎの正当性を確認し、正当であると確認された場合に、暗号化コンテンツ署名（ＥＣＳ）発行装置に対して、ライセンスを発行する。
【０１２８】
なお、ライセンスは、具体的には、例えばライセンス発行装置（ＬＡ）１０１の秘密鍵による署名が付与された公開鍵証明書である。公開鍵証明書には、暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓ

ｓｕｅｒ）１０２の公開鍵が格納される。なお、この公開鍵証明書に格納される公開鍵に対応する秘密鍵も併せて（Ａ）ライセンス発行装置（ＬＡ）１０１から、暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２に提供される。

【０１２９】

次に、図８を参照して、

（Ａ）ライセンス発行装置（ＬＡ）１０１、

（Ｂ）暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２、

（Ｃ）コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３、

これらの３者間で実行される処理について説明する。

【０１３０】

図８には、

（Ａ）ライセンス発行装置（ＬＡ）１０１、

（Ｂ）暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２、

（Ｃ）コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３、

これらの３つの装置と、各装置において実行する代表的な処理を示す図である。

【０１３１】

ライセンス発行装置（ＬＡ）１０１の実行する処理は、処理（Ａ１）、（Ａ２）として示している。

ライセンス発行装置（ＬＡ）１０１は以下の処理を実行する。

処理（Ａ１）暗号化コンテンツ署名（ＥＣＳ）発行装置１０２に対して、使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）付のＥＣＳ発行装置証明書（ＥＣＳ　Ｉｓｓｕｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）を提供する。

処理（Ａ２）コンテンツ提供装置１０３に対して、ＥＣＳ発行装置証明書リボケーションリスト（ＥＣＳ　Ｉｓｓｕｅｒ　Ｋｅｙ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）を提供する。

【０１３２】

暗号化コンテンツ署名（ＥＣＳ）発行装置１０２の実行する処理は、処理（Ｂ１）、（Ｂ２）として示している。

暗号化コンテンツ署名（ＥＣＳ）発行装置１０２は以下の処理を実行する。

処理（Ｂ１）暗号化コンテンツ署名ファイル（ＥＣＳファイル：Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｆｉｌｅ）を生成、

処理（Ｂ２）コンテンツ提供装置１０３に対して、暗号化コンテンツ署名ファイル（ＥＣＳファイル：Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｆｉｌｅ）を提供、

【０１３３】

コンテンツ提供装置１０３の実行する処理は、処理（Ｃ１）、（Ｃ２）として示している。

コンテンツ提供装置１０３は以下の処理を実行する。

処理（Ｃ１）暗号化コンテンツ署名（ＥＣＳ）発行装置１０２に対して、ＥＣＳファイル生成用データを提供する。例えば、コンテンツハッシュリスト集合、タイトルキーのハッシュ値、ブロック識別子等を提供する。

処理（Ｃ２）ＥＣＳファイルを利用したコンテンツ提供可否判定処理、

【０１３４】

［６．ＥＣＳファイルの構成例について］

次に、暗号化コンテンツ署名（ＥＣＳ）発行装置１０２の生成するＥＣＳファイルの構成例について説明する。

図９にＥＣＳファイルと、ＥＣＳファイルの構成データとしても設定されるＥＣＳ発行装置証明書のデータ構成例を示す。

ＥＣＳファィルは、暗号化コンテンツ署名（ＥＣＳ）発行装置１０２において生成するファイルであり、コンテンツ提供装置１０３から受領するコンテンツハッシュリスト集合、タイトルキーのハッシュ値、ブロック識別子等を構成データとして格納したファイルである。

【０１３５】

図９（Ａ）に示すように、ＥＣＳファイルは、

（１）コンテンツハッシュリスト集合（Ｈａｓｈ　Ｌｉｓｔ　Ｃｏｌｌｅｃｔｉｏｎｓ）

（２）ＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）

（３）ブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）

（４）ＥＣＳ発行装置署名（Ｓｉｇｎａｔｕｒｅ　ｂｙ　ＥＣＳ　Ｉｓｓｕｅｒ）

（５）ＥＣＳ発行装置証明書（ＥＣＳ　Ｉｓｓｕｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）

（６）コンテンツブロックテーブル（Ｓｔｏｒｅｄ　Ｃｏｎｔｅｎｔ　Ｂｌｏｃｋ　Ｔａｂｌｅ）

これらのデータを含むファイルである。

【０１３６】

（１）コンテンツハッシュリスト集合（Ｈａｓｈ　Ｌｉｓｔ　Ｃｏｌｌｅｃｔｉｏｎｓ）は、コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３が生成して、暗号化コンテンツ署名（ＥＣＳ）発行装置１０２が受領するデータである。ユーザ装置に提供するコンテンツ、具体的にはユーザ装置において再生される例えば映画等のコンテンツに基づいて生成されるコンテンツの構成データに基づいて生成されるハッシュ値とその属性情報（ハッシュ値生成元のコンテンツブロックの位置等を示すオフセット、レングスなどの情報）を含むデータである。

【０１３７】

（２）ＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）は、暗号化コンテンツ署名（ＥＣＳ）発行装置１０２においてＥＣＳファイルを生成した日時情報である。

この日時情報は、例えば、（４）ＥＣＳ発行装置署名（ＥＣＳ　Ｓｉｇｎａｔｕｒｅ）の生成日時に対応する。

【０１３８】

（３）ブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）は、コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３から、暗号化コンテンツ署名（ＥＣＳ）発行装置１０２に通知されるデータであり、コンテンツ提供装置１０３がユーザ装置１０４に対して提供したコンテンツに対応する暗号鍵であるタイトルキーを格納したメディアの保護領域のブロックの識別子である。これは、コンテンツ提供装置１０３が利用可能なメディアの保護領域におけるブロックの識別子である。

先に、図３、図６等を参照して説明したように、コンテンツ提供装置の利用可能なメディアの保護領域のブロックは予め設定されており、これらのアクセス許容ブロック情報が記録される。

【０１３９】

（４）ＥＣＳ発行装置署名（ＥＣＳ　Ｓｉｇｎａｔｕｒｅ）

ＥＣＳ発行装置署名（ＥＣＳ　Ｓｉｇｎａｔｕｒｅ）は、ＥＣＳ発行装置の電子署名である。

署名対象データは、コンテンツハッシュリスト集合、ＥＣＳ発行日時、ブロック識別子、さらに、タイトルキー（ハッシュ値）等の構成データとなる。

【０１４０】

（５）ＥＣＳ発行装置証明書（ＥＣＳ　Ｉｓｓｕｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）

ＥＣＳ発行装置証明書（ＥＣＳ　Ｉｓｓｕｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）は、ＥＣＳ発行装置１０２に対応する公開鍵証明書であり、図９（Ｂ）に示すように、ＥＣＳ発行装

置１０２の公開鍵等が格納されている。この構成については後述する。
【０１４１】
（６）コンテンツブロックテーブル（Ｓｔｏｒｅｄ Ｃｏｎｔｅｎｔ Ｂｌｏｃｋ Ｔａｂｌｅ）
コンテンツブロックテーブル（Ｓｔｏｒｅｄ Ｃｏｎｔｅｎｔ Ｂｌｏｃｋ Ｔａｂｌｅ）は、上記のコンテンツハッシュリスト集合（Ｈａｓｈ Ｌｉｓｔ Ｃｏｌｌｅｃｔｉｏｎｓ）に、複数のコンテンツに対応するハッシュリストが記録されている場合に、各ハッシュリストとコンテンツの対応情報を記録したフィールドとして設定される。
【０１４２】
次に、図９（Ｂ）に示すＥＣＳ発行装置証明書（ＥＣＳ Ｉｓｓｕｅｒ Ｃｅｒｔｉｆｉｃａｔｅ）のデータ構成について説明する。
ＥＣＳ発行装置証明書（ＥＣＳ Ｉｓｓｕｅｒ Ｃｅｒｔｉｆｉｃａｔｅ）は、ライセンス発行装置（ＬＡ）１０１が生成し、ＥＣＳ発行装置１０２に提供される。ＥＣＳ発行装置１０２は、ＥＣＳ発行装置証明書（ＥＣＳ Ｉｓｓｕｅｒ Ｃｅｒｔｉｆｉｃａｔｅ）の生成に必要となるデータをライセンス発行装置（ＬＡ）１０１に提供して、ＥＣＳ発行装置証明書（ＥＣＳ Ｉｓｓｕｅｒ Ｃｅｒｔｉｆｉｃａｔｅ）の生成を依頼する。
【０１４３】
ライセンス発行装置（ＬＡ）１０１は、この依頼に応じてＥＣＳ発行装置証明書（ＥＣＳ Ｉｓｓｕｅｒ Ｃｅｒｔｉｆｉｃａｔｅ）を生成する。
図９（Ｂ）に示すように、ＥＣＳ発行装置証明書は、
（１）ＥＣＳ証明書識別子（ＥＣＳ Ｃｅｒｔｉｆｉｃａｔｅ ＩＤ）
（２）ブロック識別子開始番号（Ｓｔａｒｔ ＰＡＤ Ｂｌｏｃｋ Ｎｕｍｂｅｒ）
（３）ブロック識別子範囲（ＰＡＤ Ｂｌｏｃｋ Ｎｕｍｂｅｒ Ｃｏｕｎｔｅｒ）
（４）発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ Ｄａｔｅ）
（５）ＥＣＳ発行装置公開鍵（ＥＣＳ Ｉｓｓｕｅｒ Ｐｕｂｌｉｃ Ｋｅｙ）
（６）ＬＡ署名（Ｓｉｇｎａｔｕｒｅ ｂｙ ＬＡ）
これらのデータを含むファイルである。
【０１４４】
（１）ＥＣＳ証明書識別子（ＥＣＳ Ｃｅｒｔｉｆｉｃａｔｅ ＩＤ）は。このＥＣＳ証明書の識別子である。
（２）ブロック識別子開始番号（Ｓｔａｒｔ ＰＡＤ Ｂｌｏｃｋ Ｎｕｍｂｅｒ）は、ＥＣＳ発行装置１０２が、コンテンツ提供装置１０３に対して許容可能なメディアの保護領域のアクセス許容ブロックの開始番号である。
（３）ブロック識別子範囲（ＰＡＤ Ｂｌｏｃｋ Ｎｕｍｂｅｒ Ｃｏｕｎｔｅｒ）は、ＥＣＳ発行装置１０２が、コンテンツ提供装置１０３に対して許容可能なメディアの保護領域のアクセス許容ブロックの開始番号からの範囲を示す情報である。
【０１４５】
（４）発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ Ｄａｔｅ）は、この発行装置証明書の使用期限情報である。
（５）ＥＣＳ発行装置公開鍵（ＥＣＳ Ｉｓｓｕｅｒ Ｐｕｂｌｉｃ Ｋｅｙ）は、ＥＣＳ発行装置の公開鍵である。
（６）ＬＡ署名（Ｓｉｇｎａｔｕｒｅ ｂｙ ＬＡ）は、図７、図８に示すライセンス発行装置（ＬＡ）の電子署名である。ＥＣＳ発行装置証明書の上記構成データ（１）～（５）に基づいて生成される電子署名である。
【０１４６】
図１０は、ＥＣＳファイルのシンタックス、
図１１は、ＥＣＳ発行装置証明書のシンタックス、
を示す図である。
なお、ＥＣＳ発行装置証明書に記録される、
（２）ブロック識別子開始番号（Ｓｔａｒｔ ＰＡＤ Ｂｌｏｃｋ Ｎｕｍｂｅｒ）

（３）ブロック識別子範囲（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ　Ｃｏｕｎｔｅｒ）
これらの２つのデータは、前述したように、ＥＣＳ発行装置１０２が、コンテンツ提供装置１０３に対して許容可能なメディアの保護領域のアクセス許容ブロックを示す情報である。
具体的には、例えば、
ブロック識別子開始番号≦Ｎ≦ブロック識別子開始番号＋ブロック識別子範囲
を満たす、すべてをブロック識別子として設定したのと同等である。
【０１４７】
また、
ブロック識別子開始番号＝０ｘＦＦＦＦＦＦＦＦ
と設定されていた場合は、
メディアの保護領域の全ブロックがアクセス許容ブロックであることを示す。
【０１４８】
なお、図９～図１１を参照して説明した例は、ＥＣＳファイルがＥＣＳ発行装置証明書を含む構成として説明したが、ＥＣＳファイルにＥＣＳ発行装置証明書を含めず、ＥＣＳファイルと、ＥＣＳ発行装置証明書を個別のファイルとして構成してもよい。
【０１４９】
［７．ＥＣＳ発行装置証明書リボケーションリストの構成について］
次に、図１２を参照して、ＥＣＳ発行装置証明書リボケーションリストの構成について説明する。
【０１５０】
ＥＣＳ発行装置証明書リボケーションリスト（ＥＣＳ　Ｉｓｓｕｅｒ　Ｋｅｙ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）は、先に図８を参照して説明したように、ライセンス発行装置（ＬＡ）１０１が発行するリストである。このリストは、例えばコンテンツ提供装置１０３において利用される。
【０１５１】
ライセンス発行装置（ＬＡ）１０１は、不正であると判定されたＥＣＳ発行装置の公開鍵を格納したＥＣＳ発行装置証明書（図９（Ｂ）参照）を無効化し、無効化したＥＣＳ発行装置（具体的には、ＥＣＳ発行装置証明書）の識別子（ＩＤ）を登録したリストとして、ＥＣＳ発行装置証明書リボケーションリストを生成する。
図１２に示すように、ＥＣＳ発行装置証明書リボケーションリストは、以下のデータを格納している。
（１）バージョン（Ｖｅｒｓｉｏｎ）
（２）エントリ数（Ｎｕｍｂｅｒ　ｏｆ　ｅｎｔｒｉｅｓ）
（３）リボーク（無効化）されたＥＣＳ発行装置証明書のＩＤ
（４）リボーク（無効化）されたＥＣＳ発行装置証明書のリボーク日時
（５）ライセンス発行装置（ＬＡ）１０１の電子署名
これらのデータを格納している。
【０１５２】
（５）ライセンス発行装置（ＬＡ）１０１の電子署名は（１）～（４）のデータに対する署名である。
なお、ＥＣＳ発行装置証明書リボケーションリストは、不正なＥＣＳ発行装置が新たに発見された場合には、そのＥＣＳ発行装置のＩＤを追加して更新した新しいバージョンのリストが逐次、発行され、コンテンツ提供装置１０３に提供される。
【０１５３】
［８．暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成処理について］
次に、図１３を参照して暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成処理について説明する。
【０１５４】
暗号化コンテンツ署名ファイル（ＥＣＳファイル）は、コンテンツ提供装置（Ｃｏｎｔ

ｅｎｔ　Ｓｅｒｖｅｒ）１０３からの生成依頼に基づいて、暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２が生成する。

【０１５５】

コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３が、例えば、新たな映画コンテンツなどのコンテンツをユーザ装置１０４に提供する場合、そのコンテンツに対応する暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成依頼を、暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２に対して行う。

【０１５６】

暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２は、この依頼に応じて、暗号化コンテンツ署名ファイル（ＥＣＳファイル）を生成して、コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３に提供する。

【０１５７】

図１３は、この暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成処理において、コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３と暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２の実行する処理を説明する図である。

【０１５８】

コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３は、新たな暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成依頼を行う場合、図１３に示すように、

コンテンツ１８１の構成データ（コンテンツブロック）に基づいて生成したハッシュ値を含むコンテンツハッシュリスト集合（Ｈａｓｈ　Ｌｉｓｔ　Ｃｏｌｌｅｃｔｉｏｎｓ）１８３を生成する。

【０１５９】

なお、コンテンツハッシュリスト集合（Ｈａｓｈ　Ｌｉｓｔ　Ｃｏｌｌｅｃｔｉｏｎｓ）１８３は、ユーザ装置１０４に提供する暗号化コンテンツの構成データ（コンテンツブロック）に基づいて生成したハッシュ値を格納したコンテンツハッシュリスト集合として生成される。

【０１６０】

コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３は、生成したコンテンツハッシュリスト集合（Ｈａｓｈ　Ｌｉｓｔ　Ｃｏｌｌｅｃｔｉｏｎｓ）１８３を暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２に提供する。

【０１６１】

さらに、コンテンツ１８１の暗号化に適用する暗号鍵であるタイトルキー１８２、またはタイトルキーのハッシュ値も暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２に提供する。

【０１６２】

コンテンツハッシュリスト集合（Ｈａｓｈ　Ｌｉｓｔ　Ｃｏｌｌｅｃｔｉｏｎｓ）１８３は、ユーザ装置に提供するコンテンツ、具体的にはユーザ装置において再生される例えば映画等のコンテンツに基づいて生成されるコンテンツの構成データに基づいて生成されるハッシュ値とその属性情報を含むデータである。

なお、属性情報には、例えばハッシュ値を算出したコンテンツブロックの位置情報等の属性情報などが含まれる。

【０１６３】

暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ　Ｃｏｎｔｅｎｔ　Ｓｉｇｎａｔｕｒｅ　Ｉｓｓｕｅｒ）１０２は、図１３に示すステップＳ１１において、コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３から受信したデータと、ＥＣ

Ｓファイルの構成データ、具体的には、例えば、
コンテンツハッシュリスト集合、
ＥＣＳ発行日時、
ブロック識別子、
タイトルキー（ハッシュ）、
これらのデータに対する署名を生成する。

【０１６４】

署名データの生成は、暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ Ｃｏｎｔｅｎｔ Ｓｉｇｎａｔｕｒｅ Ｉｓｓｕｅｒ）１０２の保持する秘密鍵を適用して署名を生成する。例えばＥＣＤＳＡアルゴリズムに従った署名生成を行う。

【０１６５】

生成した署名は、図１３に示すように、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の構成データとして設定される。

先に図９を参照して説明したように、暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ Ｃｏｎｔｅｎｔ Ｓｉｇｎａｔｕｒｅ Ｉｓｓｕｅｒ）１０２の生成する暗号化コンテンツ署名ファイル（ＥＣＳファイル）２００は、以下のデータを構成データとして有する。

（１）コンテンツハッシュリスト集合（Ｈａｓｈ Ｌｉｓｔ Ｃｏｌｌｅｃｔｉｏｎｓ）
（２）ＥＣＳ発行日時（ＥＣＳ Ｉｓｓｕｅ Ｄａｔｅ）
（３）ブロック識別子（ＰＡＤ Ｂｌｏｃｋ Ｎｕｍｂｅｒ）
（４）ＥＣＳ発行装置署名（Ｓｉｇｎａｔｕｒｅ ｂｙ ＥＣＳ Ｉｓｓｕｅｒ）
（５）ＥＣＳ発行装置証明書（ＥＣＳ Ｉｓｓｕｅｒ Ｃｅｒｔｉｆｉｃａｔｅ）
（６）コンテンツブロックテーブル（Ｓｔｏｒｅｄ Ｃｏｎｔｅｎｔ Ｂｌｏｃｋ Ｔａｂｌｅ）
これらのデータを含むファイルである。

【０１６６】

［９．ＥＣＳファイル、ＥＣＳ発行装置証明書の日時情報を適用した処理について］

次に、ＥＣＳファイル、ＥＣＳ発行装置証明書の日時情報を適用した処理について説明する。

（１）ＥＣＳ発行装置１０２が生成し、コンテンツ提供装置に提供されるＥＣＳファイル、
（２）ライセンス発行装置（ＬＡ）１０１が生成し、ＥＣＳ発行装置１０２に提供されるＥＣＳ発行装置証明書、
これらには、図９を参照して説明したように、様々な日時情報が記録される。

【０１６７】

例えば、ＥＣＳファイルには、
ＥＣＳ発行日時（ＥＣＳ Ｉｓｓｕｅ Ｄａｔｅ）
が記録される。
また、ＥＣＳ発行装置証明書には、
発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ Ｄａｔｅ）
が記録される。

【０１６８】

コンテンツ提供装置１０３は、これらのＥＣＳファイルとＥＣＳ発行装置証明書に記録された日時情報や、先に図１２を参照して説明したＥＣＳ発行装置証明書リボケーションリストを適用して、ユーザ装置１０４に対するコンテンツ提供処理の可否判定処理を実行する。

【０１６９】

また、コンテンツ提供装置１０３からコンテンツを受領するユーザ装置においても、ＥＣＳファイルとＥＣＳ発行装置証明書に記録された日時情報や、先に図１２を参照して説

明したＥＣＳ発行装置証明書リボケーションリストを適用して、ユーザ装置１０４におけるコンテンツ再生の可否判定処理を実行する。
以下、これらの処理について説明する。
【０１７０】
まず、図１４、図１５に示すシーケンス図を参照して、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成とコンテンツ提供、利用処理シーケンスについて説明する。
図１４には、左から、
ライセンス発行装置１０１、
暗号化コンテンツ署名（ＥＣＳ）発行装置１０２、
コンテンツ提供装置１０３、
これらの各装置を示し、ステップＳ１１１、Ｓ１２１～Ｓ１２８の各処理を時系列処理として示している。
これらの各処理ステップについて説明する。
【０１７１】
ステップＳ１１１
ステップＳ１１１は、ライセンス発行装置１０１が、暗号化コンテンツ署名（ＥＣＳ）発行装置１０２に対してライセンス（ＥＣＳ発行装置証明書）を発行する処理である。
【０１７２】
先に図８他を参照して説明したように、ライセンス発行装置１０１は、暗号化コンテンツ署名（ＥＣＳ）発行装置１０２に対して、ＥＣＳファイルの発行許可証としてのライセンス、すなわちＥＣＳ発行装置証明書を提供する。
ライセンス発行装置（ＬＡ）１０１は、予め既定したライセンス発行シーケンスにしたがって、暗号化コンテンツ署名（ＥＣＳ）発行装置１０２の正当性を確認し、正当であると確認された場合に、暗号化コンテンツ署名（ＥＣＳ）発行装置に対して、ＥＣＳ発行装置証明書を発行する。
【０１７３】
ＥＣＳ発行装置証明書は、図９（Ｂ）を参照して説明したデータ構成を有する公開鍵証明書である。ＥＣＳ発行装置証明書には、暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ Ｃｏｎｔｅｎｔ Ｓｉｇｎａｔｕｒｅ Ｉｓｓｕｅｒ）１０２の公開鍵が格納される。なお、このＥＣＳ発行装置証明書に格納される公開鍵に対応する秘密鍵も併せて（Ａ）ライセンス発行装置（ＬＡ）１０１から、暗号化コンテンツ署名（ＥＣＳ）発行装置（Ｅｎｃｒｙｐｔｅｄ Ｃｏｎｔｅｎｔ Ｓｉｇｎａｔｕｒｅ Ｉｓｓｕｅｒ）１０２に提供される。
【０１７４】
ステップＳ１２１～Ｓ１２４は、図１３を参照して説明した暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成処理のシーケンスである。
この処理は、コンテンツ提供装置１０３が、例えば新たなコンテンツをユーザ装置に提供する場合に、その新たなコンテンツに対応する暗号化コンテンツ署名ファイル（ＥＣＳファイル）を取得するために、各提供コンテンツに応じて逐次実行される。
この処理は、暗号化コンテンツ署名（ＥＣＳ）発行装置１０２と、コンテンツ提供装置１０３との間で実行される。
【０１７５】
まず、ステップＳ１２１において、コンテンツ提供装置１０３は、暗号化コンテンツ署名ファイル（ＥＣＳファイル）作成に必要となるデータを生成する。
具体的には、図１３を参照して説明した、
コンテンツハッシュリスト集合（Ｈａｓｈ Ｌｉｓｔ Ｃｏｌｌｅｃｔｉｏｎｓ）１８３の生成処理などを実行する。
【０１７６】
前述したように、コンテンツハッシュリスト集合（Ｈａｓｈ Ｌｉｓｔ Ｃｏｌｌｅｃｔｉｏｎｓ）は、ユーザ装置に提供するコンテンツ、具体的にはユーザ装置において再生

される例えば映画等のコンテンツに基づいて生成されるコンテンツの構成データに基づいて生成されるハッシュ値とその属性情報を含むデータである。
属性情報には、例えばハッシュ値を算出したコンテンツブロックの位置情報等の属性情報などが含まれる。
【０１７７】
なお、コンテンツ提供装置１０３は、コンテンツの暗号化および復号処理に適用するタイトルキー、あるいはタイトルキーのハッシュ値も、暗号化コンテンツ署名（ＥＣＳ）発行装置１０２への提供データとして生成する。
【０１７８】
次に、コンテンツ提供装置１０３は、ステップＳ１２２において、生成データを暗号化コンテンツ署名（ＥＣＳ）発行装置１０２に送信して、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の生成および送信要求を行う。
【０１７９】
次に、ステップＳ１２３において、暗号化コンテンツ署名（ＥＣＳ）発行装置１０２は、コンテンツ提供装置１０３から受信したデータに対する署名生成処理を行う。
すなわち、図１３を参照して説明したステップＳ１１の署名生成処理を実行する。
【０１８０】
さらに、先に図９（Ａ）を説明したデータ構成を持つ暗号化コンテンツ署名ファイル（ＥＣＳファイル）を生成し、ステップＳ１２４において、生成した暗号化コンテンツ署名ファイル（ＥＣＳファイル）をコンテンツ提供装置１０３に送信する。
【０１８１】
先に図９（Ａ）を参照して説明したように、暗号化コンテンツ署名ファイル（ＥＣＳファイル）には、
ＥＣＳファイルは、
（１）コンテンツハッシュリスト集合（Ｈａｓｈ　Ｌｉｓｔ　Ｃｏｌｌｅｃｔｉｏｎｓ）
（２）ＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）
（３）ブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）
（４）ＥＣＳ発行装置署名（Ｓｉｇｎａｔｕｒｅ　ｂｙ　ＥＣＳ　Ｉｓｓｕｅｒ）
（５）ＥＣＳ発行装置証明書（ＥＣＳ　Ｉｓｓｕｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）
（６）コンテンツブロックテーブル（Ｓｔｏｒｅｄ　Ｃｏｎｔｅｎｔ　Ｂｌｏｃｋ　Ｔａｂｌｅ）
これらのデータが含まれる。
【０１８２】
暗号化コンテンツ署名ファイル（ＥＣＳファイル）を受信したコンテンツ提供装置１０３は、ステップＳ１２５において、暗号化コンテンツ署名ファイル（ＥＣＳファイル）を適用したコンテンツ提供が許容されるか否かのコンテンツ提供可否判定処理を実行する。
ステップＳ１２６において、コンテンツ提供が許容されると判定した場合は、ステップＳ１２７においてユーザ装置に対するコンテンツ提供処理を実行する。
ステップＳ１２６において、コンテンツ提供が許容されないと判定した場合は、ステップＳ１２８に進み、コンテンツ提供処理を中止する。
なお、ステップＳ１２５～Ｓ１２８の処理については、図１６以下を参照して、後段でさらに詳細に説明する。
【０１８３】
次に、図１５を参照して、コンテンツ提供装置１０３からユーザ装置１０４に対するコンテンツの提供と、ユーザ装置１０４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には、左から、
コンテンツ提供装置１０３、
ユーザ装置１０４、

これらを示している。

【０１８４】

まず、コンテンツ提供装置１０３は、ステップＳ１３１において、ユーザ装置に、

（１）暗号化コンテンツ

（２）暗号化コンテンツ署名ファイル（ＥＣＳファイル）

（３）タイトルキー

これらのデータを送信する。

【０１８５】

なお、ステップＳ１３１の処理の前処理として、例えばユーザ装置１０４からコンテンツ提供装置１０３に対するコンテンツ送信要求が実行されているものとする。コンテンツ提供装置１０３は、ユーザ装置からのリクエストに応じたコンテンツを提供する。

【０１８６】

なお、ステップＳ１３１においてコンテンツ提供装置１０３の送信する、

（１）暗号化コンテンツ

は、コンテンツに対応して設定される上記の「（３）タイトルキー」で暗号化されたコンテンツである。

また、

（２）暗号化コンテンツ署名ファイル（ＥＣＳファイル）

は、上記の（１）暗号化コンテンツに対応して生成されたファイルであり、先に図９を参照して説明した暗号化コンテンツ署名ファイル（ＥＣＳファイル）の構成データを格納している。

【０１８７】

ユーザ装置１０４は、これらのデータを受信し、例えばハードディスク等のメディアに格納する。

その後、コンテンツの再生処理を実行する際に、図１５に示すステップＳ１３２以下の処理を実行する。

【０１８８】

ユーザ装置１０４は、ステップＳ１３２において、再生対象コンテンツに対応する暗号化コンテンツ署名ファイル（ＥＣＳファイル）を読み出して、暗号化コンテンツ署名ファイル（ＥＣＳファイル）を適用してコンテンツ再生が許容されるか否かのコンテンツ再生可否判定処理を実行する。

ステップＳ１３３において、コンテンツ再生が許容されると判定した場合は、ステップＳ１３４においてコンテンツ再生処理を実行する。

ステップＳ１３３において、コンテンツ再生が許容されないと判定した場合は、ステップＳ１３５に進み、コンテンツ再生処理を中止する。

なお、ステップＳ１３２～Ｓ１３５の処理については、図１８を参照して、後段でさらに詳細に説明する。

【０１８９】

次に、図１４を参照して説明したコンテンツ提供装置におけるステップＳ１２５｜Ｓ１２８の処理、すなわち、暗号化コンテンツ署名ファイル（ＥＣＳファイル）を適用したコンテンツ提供可否判定処理の詳細シーケンスについて図１６、図１７に示すフローチャートを参照して説明する。

【０１９０】

図１６に示すフローチャートのステップＳ１５１の前処理として、コンテンツ提供装置は、暗号化コンテンツ署名ファイル（ＥＣＳファイル）発行装置から受信した暗号化コンテンツ署名ファイル（ＥＣＳファイル）に設定されたＥＣＳ発行装置署名を適用した署名検証を実行する。

この署名検証が成立し、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の正当性が確認され場合は、さらに、暗号化コンテンツ署名ファイル（ＥＣＳファイル）に格納されたＥＣＳ発行装置証明書の署名検証を実行する。これらの２つの署名検証が成立したこと

を条件としてステップＳ１５１以下の処理を行う。

【０１９１】

上記２つの署名検証の少なくともいずれかが成立しなかった場合は、暗号化コンテンツ署名ファイル（ＥＣＳファイル）またはＥＣＳ発行装置証明書の正当性が確認されないので、ステップＳ１５１以下の処理は実行されない。この場合はコンテンツ提供処理も実行しないことになる。

【０１９２】

暗号化コンテンツ署名ファイル（ＥＣＳファイル）と、ＥＣＳ発行装置証明書の２つの署名検証が成立し、暗号化コンテンツ署名ファイル（ＥＣＳファイル）とＥＣＳ発行装置証明書の正当性が確認された場合、コンテンツ提供装置は、ステップＳ１５１の処理を実行する。

【０１９３】

コンテンツ提供装置は、

暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）を読み出す。さらに、

ＥＣＳ発行装置証明書の記録データであるＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）を読み出す。

さらに、これらの日時情報を比較し、

ＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）がＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）より前であるか否かを判定する。

ＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）がＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）より前である場合（Ｙｅｓ）は、ステップＳ１５６に進み、暗号化コンテンツの配布を停止する。

【０１９４】

ＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）がＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）より前でない場合（Ｎｏ）は、ステップＳ１５２に進み、ステップＳ１５３以下において暗号化コンテンツ署名ファイル（ＥＣＳファイル）とＥＣＳ発行装置証明書に記録された日時情報（タイムスタンプ）を適用したコンテンツ提供可否判定処理を開始する。

【０１９５】

ステップＳ１５３では、ＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）と、コンテンツ提供装置の持つ時間クロックあるいは信頼できる時間情報提供サーバから取得した実時間とを比較する。

ＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）が、実時間より１日以上前であれば、ステップＳ１５６に進み、コンテンツ提供処理を中止する。

【０１９６】

一方、ＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）が、実時間より１日以上前でなければ、ステップＳ１５４に進む。

ステップＳ１５４では、ＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）と、コンテンツ提供装置の持つ時間クロックあるいは信頼できる時間情報提供サーバから取得した実時間とを比較する。

ＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）が、実時間より１日以上前であれば、ステップＳ１５６に進み、コンテンツ提供処理を中止する。

【０１９７】

一方、ＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）が、実時間より１日以上前でなければ、ステップＳ１５５に進む。

【０１９８】

次に、ステップＳ１５５以下において実行するリボケーションリストを適用したコンテンツ提供可否判定処理について、図１７に示すフローチャートを参照して説明する。

なお、コンテンツ提供装置は、予め図１２を参照して説明したＥＣＳ発行装置公開鍵リ

ボケーションリストを取得しているものとする。例えばライセンス発行装置（ＬＡ）１０１から取得可能である。

【０１９９】

コンテンツ提供装置は、ステップＳ１６１において、ＥＣＳ発行装置証明書からＥＣＳ証明書識別子を取得し、この識別子（ＩＤ）がＥＣＳ発行装置公開鍵リボケーションリストに登録されているか否かを判定する。

登録されていない場合（Ｎｏ）は、ＥＣＳ発行装置証明書は無効化（リボーク）されておらず有効であることが確認され、この場合は、ステップＳ１６４に進み、コンテンツ提供処理を実行する。

【０２００】

一方、ステップＳ１６１において、ＥＣＳ証明書識別子（ＩＤ）がＥＣＳ発行装置公開鍵リボケーションリストに登録されていると判定した場合（Ｙｅｓ）、この場合は、ステップＳ１６２に進む。

【０２０１】

ステップＳ１６２では、ＥＣＳ発行装置公開鍵リボケーションリストに登録されているそのＥＣＳ発行装置証明書が無効化（リボーク）された日時、すなわち、

リボーク日時と、

暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）と、

これらの２つの日時データを比較する。

【０２０２】

暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）がリボーク日時より前である場合（Ｙｅｓ）は、ステップＳ１６４に進み、コンテンツの提供処理を実行する。

これは、リボーク以前の正当なＥＣＳ発行装置証明書に基づく処理であると判断できるためである。

【０２０３】

一方、ステップＳ１６２において、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）がリボーク日時より前でない場合（Ｎｏ）は、ステップＳ１６３に進み、コンテンツの提供処理を停止する。

これは、リボーク後の不当なＥＣＳ発行装置証明書に基づく処理であると判断できるためである。

【０２０４】

次に、図１８に示すフローチャートを参照して、先に図１５のステップＳ１３２～Ｓ１３５を参照して説明したユーザ装置１０４における暗号化コンテンツ署名ファイル（ＥＣＳファイル）を適用したコンテンツ再生許容判定処理の詳細について説明する。

【０２０５】

なお、ユーザ装置は、図１８に示すステップＳ１７１以前に、コンテンツ提供装置から受信した暗号化コンテンツ署名ファイル（ＥＣＳファイル）に設定されたＥＣＳ発行装置署名を適用した署名検証を実行する。

この署名検証が成立し、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の正当性が確認され場合は、さらに、暗号化コンテンツ署名ファイル（ＥＣＳファイル）に格納されたＥＣＳ発行装置証明書の署名検証を実行する。これらの２つの署名検証が成立したことを条件としてステップＳ１７１以下の処理を行う。

【０２０６】

上記２つの署名検証の少なくともいずれかが成立しなかった場合は、暗号化コンテンツ署名ファイル（ＥＣＳファイル）またはＥＣＳ発行装置証明書の正当性が確認されないので、ステップＳ１７１以下の処理は実行されない。この場合はコンテンツ再生処理も実行しないことになる。

【０２０７】
暗号化コンテンツ署名ファイル（ＥＣＳファイル）と、ＥＣＳ発行装置証明書の２つの署名検証が成立し、暗号化コンテンツ署名ファイル（ＥＣＳファイル）とＥＣＳ発行装置証明書の正当性が確認された場合、ユーザ装置は、ステップＳ１７１の処理を実行する。
【０２０８】
ステップＳ１７１において、ユーザ装置は、
暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）を読み出す。さらに、
ＥＣＳ発行装置証明書の記録データであるＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）を読み出す。
さらに、これらの日時情報を比較し、
ＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）がＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）より前であるか否かを判定する。
前である場合（Ｙｅｓ）は、ステップＳ１７５に進み、コンテンツの復号、再生処理を実行しない。
これは、すでに有効期限の切れたＥＣＳ発行装置証明書であることが確認されたからである。
【０２０９】
一方、ステップＳ１７１において、ＥＣＳ発行装置証明書使用期限（Ｅｘｐｉｒａｔｉｏｎ　Ｄａｔｅ）がＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）より前でない場合（Ｎｏ）は、ステップＳ１７２に進み、ステップＳ１７３以下においてリボケーションリストを適用したコンテンツ提供可否判定処理を実効する。
【０２１０】
なお、ユーザ装置は、予め図１２を参照して説明したＥＣＳ発行装置公開鍵リボケーションリストを取得しているものとする。例えばライセンス発行装置（ＬＡ）１０１から取得可能である。
【０２１１】
ユーザ装置は、ステップＳ１７３において、ＥＣＳ発行装置証明書からＥＣＳ証明書識別子を取得し、この識別子（ＩＤ）がＥＣＳ発行装置公開鍵リボケーションリストに登録されているか否かを判定する。
登録されていない場合（Ｎｏ）は、ＥＣＳ発行装置証明書は無効化（リボーク）されておらず有効であることが確認され、この場合は、ステップＳ１７６に進み、コンテンツ再生処理を実行する。
【０２１２】
なお、コンテンツ再生処理の開始前に、さらに、暗号化コンテンツの復号に適用するタイトルキーの取得や生成処理、さらに、暗号化コンテンツ署名ファイルに含まれるコンテンツハッシュリストを適用したハッシュ値照合処理を実行する。ハッシュ値照合において照合が成立し、コンテンツの改ざんのないことが確認された場合にコンテンツの再生が許容されることになる。
【０２１３】
一方、ステップＳ１７３において、ＥＣＳ証明書識別子（ＩＤ）がＥＣＳ発行装置公開鍵リボケーションリストに登録されていると判定した場合（Ｙｅｓ）、この場合は、ステップＳ１７４に進む。
【０２１４】
ステップＳ１７４では、ＥＣＳ発行装置公開鍵リボケーションリストに登録されているそのＥＣＳ発行装置証明書が無効化（リボーク）された日時、すなわち、
リボーク日時と、
暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）と、
これらの２つの日時データを比較する。

【０２１５】
暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）がリボーク日時より前である場合（Ｙｅｓ）は、ステップＳ１７６に進み、コンテンツの再生処理を実行する。
これは、リボーク以前の正当なＥＣＳ発行装置証明書に基づく処理であると判断できるためである。
【０２１６】
一方、ステップＳ１７３において、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の記録データであるＥＣＳ発行日時（ＥＣＳ　Ｉｓｓｕｅ　Ｄａｔｅ）がリボーク日時より前でない場合（Ｎｏ）は、ステップＳ１７５に進み、コンテンツの再生処理を停止する。
これは、リボーク後の不当なＥＣＳ発行装置証明書に基づく処理であると判断できるためである。
【０２１７】
［１０．暗号鍵とＥＣＳ発行装置署名との関連づけ構成について］
次に、暗号鍵とＥＣＳ発行装置署名との関連づけ構成について説明する。
先に、図３、図６を参照して説明したように、ユーザ装置１０４では、例えばフラッシュメモリから構成されるメモリカード等にコンテンツ等を記録して利用する。
【０２１８】
図３を参照して説明したように、メモリカード３１の記憶領域は、
（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。
【０２１９】
（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。
【０２２０】
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。
【０２２１】
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。
【０２２２】
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。
【０２２３】
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、図５を参照して説明したサーバの保

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。

【０２２４】

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装置としての記録再生装置（ホスト）である場合は、図４を参照して説明した記録再生装置（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。

【０２２５】

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。

【０２２６】

ユーザ装置１０４がメディアを装着してコンテンツ提供装置１０３から受信するコンテンツを記録する場合のデータ記録構成例について、図１９を参照して説明する。

図１９には、コンテンツ提供装置としてのサーバＡ２０１がユーザ装置としてのホスト２０２に装着されたメモリカード２１０に、暗号化コンテンツを提供して記録する処理例を示している。

メモリカード２１０は、

保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１１、

汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）２１２、

これらを有している。

【０２２７】

コンテンツ提供装置としてのサーバＡ２０１は、暗号化コンテンツ提供処理に際して、提供コンテンツの暗号化および復号に適用するタイトルキーを保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の所定ブロックに記録する。

【０２２８】

サーバＡ２０１は、先に図５を参照したサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）を保有している。

まず、サーバＡ２０１は、メモリカード２１０との相互認証処理を実行する。その際にメモリカード２１０に対してサーバ証明書を出力する。

メモリカード２１０は、サーバＡ２０１から受信したサーバ証明書に記録された保護領域アクセス権情報を確認する。

この確認処理において、サーバＡ２０１がブロック＃０のアクセス権（書き込みの権利）を有していることが判定された場合にのみ、サーバＡ２０１はメモリカード２１０に設定された保護領域２１１のブロック＃０に対するデータ書き込みが可能となる。

【０２２９】

図に示すように、サーバＡ２０１は、提供コンテンツの復号に適用するタイトルキーを保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１１のブロック＃０，２２１に格納する。

なお、保護領域には、タイトルキー自体をそのまま格納せず、

（ａ）利用制御情報（ＵＲ：Ｕｓａｇｅ　Ｒｕｌｅ）と、

（ｂ）図９を参照して説明したＥＣＳファイルの構成データであるＥＣＳ発行装置署名（Ｓｉｇｎａｔｕｒｅ　ｂｙ　ＥＣＳ　Ｉｓｓｕｅｒ）

これら（ａ）、（ｂ）の連結データのハッシュ値と、

タイトルキーＫｔとの排他的論理和演算結果を格納する。

【０２３０】

例えばコンテンツ（ａ１）に対するタイトルキー：Ｋｔ（ａ１）は、以下のタイトルキー変換データとして保護領域に格納する。

Ｋｔ（ａ１）（＋）（ＵＲ（ａ１）｜｜ＥＣＳＳｉｇ（ａ１））ｈａｓｈ
ただし、
ＵＲ（ａ１）：コンテンツａ１に対応する利用制御情報
ＥＣＳＳｉｇ（ａ１）：コンテンツａ１に対応するＥＣＳファイルの構成データであるＥＣＳ発行装置署名（Ｓｉｇｎａｔｕｒｅ　ｂｙ　ＥＣＳ　Ｉｓｓｕｅｒ）
また、演算子としての記号、
（＋）：排他的論理和演算
｜｜：データの連結を意味し、ａ｜｜ｂはデータａとデータｂの連結データを意味する。
ｈａｓｈ：ハッシュ値を意味し、（ａ｜｜ｂ）ｈａｓｈは、データａとデータｂの連結データのハッシュ値を意味する。

【０２３１】
図１９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）２１２に、以下のコンテンツと利用制御情報とＥＣＳファイルを記録する。
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）、
上記コンテンツに対応するＥＣＳファイル（ＥＣＳ　Ｆｉｌｅ）：ＥＣＳ（ａ１）、ＥＣＳ（ａ２）、ＥＣＳ（ａ３）、
これらのコンテンツと利用制御情報とＥＣＳファィルのセットを記録する。

【０２３２】
さらに、サーバＡは、メモリカードの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）２１１のブロック＃０，２２１に以下のデータを記録する。
コンテンツ対応のタイトルキーと、
コンテンツ対応の利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）とＥＣＳ発行装置署名（ＥＣＳＳｉｇ）の連結データのハッシュ値との排他的論理和（ＸＯＲ）演算結果
Ｋｔ（ａ１）（＋）（ＵＲ（ａ１）｜｜ＥＣＳＳｉｇ（ａ１））ｈａｓｈ
Ｋｔ（ａ２）（＋）（ＵＲ（ａ２）｜｜ＥＣＳＳｉｇ（ａ２））ｈａｓｈ
Ｋｔ（ａ３）（＋）（ＵＲ（ａ３）｜｜ＥＣＳＳｉｇ（ａ３））ｈａｓｈ

【０２３３】
なお、図１９には、サーバＡ２０１の処理例を示しているが、例えば異なるサーバＢは、サーバＢの提供コンテンツ（ｂｘ）に対応するタイトルキーの格納領域として許容された保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）の所定ブロック、例えば、ブロック＃１にサーバＢの提供コンテンツに同様のタイトルキー変換データ、例えば、
Ｋｔ（ｂｘ）（＋）（ＵＲ（ｂｘ）｜｜ＥＣＳＳｉｇ（ｂｘ））ｈａｓｈ
上記データを格納する。

【０２３４】
図２０には、コンテンツを利用するユーザ装置（ホスト）２０２とコンテンツ等を格納したメモリカード２１０を示している。

【０２３５】
ユーザ装置（ホスト）２０２は、先に図４を参照したホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）を保有している。
まず、ユーザ装置（ホスト）２０２は、メモリカード２１０との相互認証処理を実行する。その際にメモリカード２１０に対してホスト証明書を出力する。
メモリカード２１０は、ユーザ装置（ホスト）２０２から受信したホスト証明書に記録された保護領域アクセス権情報を確認する。
この確認処理において、ユーザ装置（ホスト）２０２がブロック＃０のアクセス権（読み取りの権利）を有していることが判定された場合にのみ、ユーザ装置（ホスト）２０２はメモリカード２１０に設定された保護領域２１１のブロック＃０からのデータ読み取り

が可能となる。
【０２３６】
これらの相互認証およびアクセス権が確認された後、ユーザ装置（ホスト）２０２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）２１２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）、ＥＣＳファイル：ＥＣＳ（ｘｙ）取得する。
【０２３７】
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保護領域の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。
【０２３８】
保護領域２１１のタイトルキー格納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。
例えば、選択ブロックから、以下のデータを読み出す。
Ｋｔ（ｘｙ）（＋）（ＵＲ（ｘｙ）｜｜ＥＣＳＳｉｇ（ｘｙ））ｈａｓｈ
【０２３９】
次に、汎用領域２１２から読み出した
利用制御情報：ＵＲ（ｘｙ）と、
ＥＣＳファイル：ＥＣＳ（ｘｙ）に格納されたＥＣＳ発行装置署名（ＥＣＳＳｉｇ（ｘｙ））
これらの連結処理とハッシュ値算出処理を行う。
すなわち、
（ＵＲ（ｘｙ）｜｜ＥＣＳＳｉｇ（ｘｙ））ｈａｓｈ
上記を算出する。
この算出結果を、
Ｐ（ｘｙ）とする。
【０２４０】
その後、以下の計算を行うことでタイトルキーＫｔ（ｘｙ）を得る。
［ブロックからの読み出しデータ（タイトルキー変換データ）］（＋）Ｐ（ｘｙ）
＝（Ｋｔ（ｘｙ）（＋）（ＵＲ（ｘｙ）｜｜ＥＣＳＳｉｇ（ｘｙ））ｈａｓｈ）（＋）Ｐ（ｘｙ）
＝（Ｋｔ（ｘｙ）（＋）（ＵＲ（ｘｙ）｜｜ＥＣＳＳｉｇ（ｘｙ））ｈａｓｈ）（＋）（ＵＲ（ｘｙ）｜｜ＥＣＳＳｉｇ（ｘｙ））ｈａｓｈ）
＝Ｋｔ（ｘｙ）
このような計算処理によってタイトルキーＫｔ（ｘｙ）を取得し、取得したタイトルキーによって暗号化コンテンツを復号して利用する。
【０２４１】
メモリカードの記録データの例について図２１を参照して説明する。
図２１には、２つの異なるサーバ、サーバＡとサーバＢがメモリカードに対して書き込むデータの例を示している。
サーバＡは、メモリカードの保護領域のブロック＃０に対するアクセス権を有している。
サーバＢは、メモリカードの保護領域のブロック＃１に対するアクセス権を有している。
【０２４２】
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。
【０２４３】
図２１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）、
上記コンテンツに対応するＥＣＳファイル（ＥＣＳ　Ｆｉｌｅ）：ＥＣＳ（ａ１）、ＥＣＳ（ａ２）、ＥＣＳ（ａ３）、
【０２４４】
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）の変換データ、
　Ｋｔ（ａ１）（＋）（ＵＲ（ａ１）｜｜ＥＣＳＳｉｇ（ａ１））ｈａｓｈ
　Ｋｔ（ａ２）（＋）（ＵＲ（ａ２）｜｜ＥＣＳＳｉｇ（ａ２））ｈａｓｈ
　Ｋｔ（ａ３）（＋）（ＵＲ（ａ３）｜｜ＥＣＳＳｉｇ（ａ３））ｈａｓｈ
これらのデータを記録する。
【０２４５】
一方、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）、
上記コンテンツに対応するＥＣＳファイル（ＥＣＳ　Ｆｉｌｅ）：ＥＣＳ（ｂ１）、ＥＣＳ（ｂ２）、
【０２４６】
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。
上記コンテンツの復号に適用するタイトルキー：Ｋｔ（ｂ１）、Ｋｔ（ｂ２）の変換データ、
　Ｋｔ（ｂ１）（＋）（ＵＲ（ｂ１）｜｜ＥＣＳＳｉｇ（ｂ１））ｈａｓｈ
　Ｋｔ（ｂ２）（＋）（ＵＲ（ｂ２）｜｜ＥＣＳＳｉｇ（ｂ２））ｈａｓｈ
これらのデータを記録する。
【０２４７】
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。
【０２４８】
図２２には、
サーバＡとサーバＢが、メモリカードの保護領域のブロック＃０に対するアクセス権を有し、
サーバＣとサーバＤが、メモリカードの保護領域のブロック＃１に対するアクセス権を有する場合におけるデータ記録例を示している。
【０２４９】
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）、
上記コンテンツに対応するＥＣＳファイル（ＥＣＳ　Ｆｉｌｅ）：ＥＣＳ（ａ１）、ＥＣＳ（ａ２）、ＥＣＳ（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）の変換データ、
Ｋｔ（ａ１）（＋）（ＵＲ（ａ１）｜｜ＥＣＳＳｉｇ（ａ１））ｈａｓｈ
Ｋｔ（ａ２）（＋）（ＵＲ（ａ２）｜｜ＥＣＳＳｉｇ（ａ２））ｈａｓｈ
Ｋｔ（ａ３）（＋）（ＵＲ（ａ３）｜｜ＥＣＳＳｉｇ（ａ３））ｈａｓｈ
これらのデータを記録する。

【０２５０】
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）、
上記コンテンツに対応するＥＣＳファイル（ＥＣＳ　Ｆｉｌｅ）：ＥＣＳ（ｂ１）、ＥＣＳ（ｂ２）、

【０２５１】
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＃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（ｂ１）、Ｋｔ（ｂ２）の変換データ、
Ｋｔ（ｂ１）（＋）（ＵＲ（ｂ１）｜｜ＥＣＳＳｉｇ（ｂ１））ｈａｓｈ
Ｋｔ（ｂ２）（＋）（ＵＲ（ｂ２）｜｜ＥＣＳＳｉｇ（ｂ２））ｈａｓｈ
これらのデータを記録する。

【０２５２】
サーバＣ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（ｃ１）
上記コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）：ＵＲ（ｃ１）、
上記コンテンツに対応するＥＣＳファイル（ＥＣＳ　Ｆｉｌｅ）：ＥＣＳ（ｃ１）、

【０２５３】
さらに、サーバＣ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。
上記コンテンツの復号に適用するタイトルキー：Ｋｔ（ｃ１）の変換データ、
Ｋｔ（ｃ１）（＋）（ＵＲ（ｃ１）｜｜ＥＣＳＳｉｇ（ｃ１））ｈａｓｈ
これらのデータを記録する。

【０２５４】
サーバＤ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（ｄ１）、Ｃｏｎ（ｄ２）
上記コンテンツに対応する利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）：ＵＲ（ｄ１）、ＵＲ（ｄ２）、
上記コンテンツに対応するＥＣＳファイル（ＥＣＳ　Ｆｉｌｅ）：ＥＣＳ（ｄ１）、ＥＣＳ（ｄ２）、

【０２５５】
さらに、サーバＤ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。
上記コンテンツの復号に適用するタイトルキー：Ｋｔ（ｄ１）、Ｋｔ（ｄ２）の変換データ、
Ｋｔ（ｄ１）（＋）（ＵＲ（ｄ１）｜｜ＥＣＳＳｉｇ（ｄ１））ｈａｓｈ
Ｋｔ（ｄ２）（＋）（ＵＲ（ｄ２）｜｜ＥＣＳＳｉｇ（ｄ２））ｈａｓｈ
これらのデータを記録する。
【０２５６】
なお、コンテンツ再生を実行するユーザ装置（ホスト）は、再生対象コンテンツを汎用領域から選択した場合、そのタイトルキーの格納されている保護領域のブロックを特定するこが必要となる。
このブロック特定情報は、各コンテンツに対応する利用制御情報（ＵＲ）から取得する。
【０２５７】
図２３を参照して利用制御情報の利用例について説明する。図２３（ａ）に、メモリカードの汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）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。
【０２５８】
利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）には、
（１）ブロック識別子（＃０）
（２）タイトルキー識別子（ａ１）
（３）ＥＣＳファイル識別子（ａ１）
これらのデータが記録される。
【０２５９】
（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。
【０２６０】
（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。
【０２６１】
（３）ＥＣＳファイル識別子（ａ１）は、
コンテンツ（ａ１）に対応するＥＣＳファイルを識別するための情報である。
【０２６２】
ユーザ装置（ホスト）は、利用制御情報：ＵＲ（ａ１）を参照して、利用対象コンテンツ：Ｃｏｎ（ａ１）のタイトルキーの格納された保護領域のブロックがいずれのブロックであるかを確認し、そのブロックから、以下のデータを読み出す。
Ｋｔ（ａ１）（＋）（ＵＲ（ａ１）｜｜ＥＣＳＳｉｇ（ａ１））ｈａｓｈ
【０２６３】
次に、汎用領域から読み出した
利用制御情報：ＵＲ（ａ１）と、
ＥＣＳファイル：ＥＣＳ（ａ１）に格納されたＥＣＳ発行装置署名（ＥＣＳＳｉｇ（ｘ

ｙ））
これらの連結処理とハッシュ値算出処理を行う。
すなわち、
Ｐ（ａ１）＝（ＵＲ（ａ１）｜｜ＥＣＳＳｉｇ（ａ１））ｈａｓｈ
上記を算出する。
その後、以下の計算を行うことでタイトルキーＫｔ（ｘｙ）を得る。
［ブロックからの読み出しデータ（タイトルキー変換データ）］（＋）Ｐ（ｘｙ）
＝（Ｋｔ（ａ１）（＋）（ＵＲ（ａ１）｜｜ＥＣＳＳｉｇ（ａ１））ｈａｓｈ）（＋）Ｐ（ａ１）
＝（Ｋｔ（ａ１）（＋）（ＵＲ（ａ１）｜｜ＥＣＳＳｉｇ（ａ１））ｈａｓｈ）（＋）（ＵＲ（ａ１）｜｜ＥＣＳＳｉｇ（ａ１））ｈａｓｈ）
＝Ｋｔ（ａ１）
このような計算処理によってタイトルキーＫｔ（ａ１）を取得し、取得したタイトルキーによって暗号化コンテンツを復号して利用する。

【０２６４】
このように、メモリカードの保護領域に記録するタイトルキーは、
利用制御情報（ＵＲ）とＥＣＳ発行装置署名（ＥＣＳＳｉｇ）との連結データのハッシュ値との排他的論理和（ＸＯＲ）演算結果として格納される。
このような処理を行うことで、ＥＣＳ発行装置署名（ＥＣＳＳｉｇ）に適用するＥＣＳ発行装置の署名鍵（秘密鍵）の漏えいが発生した場合にもコンテンツの不正利用を防止することが可能となる。

【０２６５】
例えば、コンテンツ提供サーバやユーザ装置が、漏えいしたＥＣＳ発行装置の署名鍵（秘密鍵）を適用した不正処理、具体的には、暗号化コンテンツのすげ替え処理などによるコンテンツ不正利用を防止可能となる。

【０２６６】
なお、すげ替えとは、例えば、あるコンテンツ（Ｃ１）に対応するタイトルキー（Ｋｔ１）を利用して他のコンテンツ（Ｃ２）、（Ｃ３）、（Ｃ４）・・・の暗号化を施してユーザに提供する処理などである。
このような処理を行うと、タイトルキー（Ｋｔ１）を有するユーザ装置では、その他のコンテンツ（Ｃ２）、（Ｃ３）、（Ｃ４）・・・を正規購入することなく、復号、再生することが可能となる。

【０２６７】
メモリカードの保護領域に記録するタイトルキーを、利用制御情報（ＵＲ）とＥＣＳ発行装置署名（ＥＣＳＳｉｇ）との連結データのハッシュ値との排他的論理和（ＸＯＲ）演算結果として格納することで、上記のようなすげ替えを防止することができる。

【０２６８】
このすげ替え防止効果について図２４以下を参照して説明する。
図２４は、
（ａ）コンテンツ（Ｃ１）に対応する正当なデータ格納構成
（ｂ）コンテンツ（Ｃ１）に対応するタイトルキー（Ｋｔ１）を利用してコンテンツ（Ｃ２）を暗号化したすげ替えデータのデータ格納構成を示している。

【０２６９】
図２４（ａ）に示す正当データ格納構成では、
メモリカードの汎用領域に、以下のデータが格納される。
（ａ１）コンテンツ（Ｃ１）に対する正当なタイトルキー（Ｋｔ１）で暗号化された暗号化コンテンツ（Ｃ１（Ｋｔ１））
（ａ２）コンテンツ（Ｃ１）に対する正当な利用制御情報（ＵＲ１）
（ａ３）コンテンツ（Ｃ１）に対する正当な暗号化コンテンツ署名ファイル（ＥＣＳファイル：ＥＣＳ１（Ｃ１，Ｋｔ１））

【０２７０】
なお、ＥＣＳファイルには、ＥＣＳ発行装置署名（ＥＣＳＳｉｇ）が格納されており、このＥＣＳ発行装置署名（ＥＣＳＳｉｇ）は、先に、図１３を参照して説明したように、コンテンツ（Ｃ１）のハッシュリスト集合と、タイトルキー（Ｋｔ１）のハッシュ値を含むデータに基づいて生成された電子署名を含む。この署名データの生成元データを明示するため、ＥＣＳファイルは、ＥＣＳ１（Ｃ１，Ｋｔ１）として記載している。
【０２７１】
また、図２４（ａ）に示す正当データ格納構成では、
メモリカードの保護領域のブロックＮに、タイトルキー（Ｋｔ１）の変換データ、すなわち、以下のデータが記録される。
Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ
ただし、
ＵＲ１：コンテンツ１に対応する利用制御情報
ＥＣＳ１Ｓｉｇ：コンテンツ１に対応するＥＣＳファイルの構成データであるＥＣＳ発行装置署名（Ｓｉｇｎａｔｕｒｅ　ｂｙ　ＥＣＳ　Ｉｓｓｕｅｒ）
また、演算子としての記号、
（＋）：排他的論理和演算
｜｜：データの連結を意味し、ａ｜｜ｂはデータａとデータｂの連結データを意味する。
ｈａｓｈ：ハッシュ値を意味し、（ａ｜｜ｂ）ｈａｓｈは、データａとデータｂの連結データのハッシュ値を意味する。
【０２７２】
例えば、悪意のあるコンテンツ提供サーバは、このコンテンツ（Ｃ１）のタイトルキー（Ｋｔ１）を他のコンテンツ（Ｃ２）に対する暗号鍵として利用して、ユーザに提供する。
この不正コンテンツ配信の結果、メモリカードには、図２４（ｂ）に示す「すげ替えデータ」が格納される。
【０２７３】
図２４（ｂ）に示す「すげ替えデータ」格納構成では、
メモリカードの汎用領域に、以下のデータが格納される。
（ｂ１）コンテンツ（Ｃ２）に対する不正なタイトルキー（Ｋｔ１）で暗号化された不正暗号化コンテンツ（Ｃ２（Ｋｔ１））
（ｂ２）コンテンツ（Ｃ２）に不正に対応付けた利用制御情報（ＵＲ１）［＝コンテン（Ｃ１）対応の利用制御情報（ＵＲ１）］
（ｂ３）コンテンツ（Ｃ２）に対応させて不正に生成した暗号化コンテンツ署名ファイル（ＥＣＳ２［＝ＥＣＳ２（Ｃ２，Ｋｔ１）］
【０２７４】
なお、不正なＥＣＳファイル：ＥＣＳ２に格納されるＥＣＳ発行装置署名（ＥＣＳＳｉｇ）は、コンテンツ（Ｃ２）のハッシュリスト集合と、コンテンツ（Ｃ１）対応のタイトルキー（Ｋｔ１）のハッシュ値を含むデータに基づいて、漏えいしたＥＣＳ発行装置の署名鍵（秘密鍵）によって生成した電子署名を含む。この署名データの生成元データを明示するため、ＥＣＳファイルは、ＥＣＳ２（Ｃ２，Ｋｔ１）として記載している。
【０２７５】
また、図２４（ｂ）に示す「すげ替えデータ」格納構成では、
メモリカードの保護領域のブロックＮに、タイトルキー（Ｋｔ１）の変換データ、すなわち、以下のデータが記録される。
Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ
【０２７６】
この図２４（ｂ）に示す「すげ替えデータ」の記録処理シーケンスについて図２５に示すフローチャートを参照して説明する。

なお、この図２５に示す処理は、既に、図２４（ａ）に示すコンテンツ（Ｃ１）に対応する正当なデータセットを格納したメモリカードを利用して実行され、メモリカードの保護領域のブロックＮに対するアクセス権としてデータ読み取り処理の権利を有する装置、例えばコンテンツ提供サーバやユーザ装置によって実行される処理である。

【０２７７】

まず、ステップＳ２０１において、新たなコンテンツＣ２を用意する。

次に、ステップＳ２０２において、メモリカードの汎用領域に記録されたコンテンツ（Ｃ１）の利用制御情報（ＵＲ１）から、「ブロック識別子」及び「タイトルキー識別子」を取得し、これらの取得情報に基づいて、保護領域の所定ブロック、すなわちタイトルキー格納ブロックから、正当なコンテンツ（Ｃ１）に対応する以下のタイトルキー変換データを読み出す。

Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ

なお、ＥＣＳ１Ｓｉｇ＝Ｓｉｇｎ（ＥＣＳ署名鍵，Ｍ）

Ｍ＝コンテンツＣ１のコンテンツハッシュリスト集合｜｜Ｋｔ１ハッシュ値

である。

【０２７８】

次に、ステップＳ２０３において、汎用領域から読み出した正当なコンテンツ（Ｃ１）に対応する利用制御情報（ＵＲ１）とＥＣＳファイル（ＥＣＳ１（Ｃ１，Ｋｔ１））の連結データのハッシュ値を算出し、算出結果と、保護領域から読み出した上記のタイトルキー変換データとの排他的論理和演算（ＸＯＲ）を実行してコンテンツ（Ｃ１）に対応する正当なタイトルキー（Ｋｔ１）を取得する。

すなわち、

Ｋｔ１＝（保護領域からの読み出しデータ）（＋）（汎用領域からの読み出しデータ）

＝Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ

上記式に従ってタイトルキー（Ｋｔ１）を取得する。

なお、（＋）は排他的論理和演算（ＸＯＲ）を意味する。

【０２７９】

次に、ステップＳ２０４において、ステップＳ２０３で取得したタイトルキー（Ｋｔ１）を適用して新たなコンテンツＣ２の暗号化を実行する。

暗号化コンテンツＣ２（Ｋｔ１）を生成する。

【０２８０】

次に、ステップＳ２０５において、暗号化コンテンツＣ２（Ｋｔ１）をメモリカードの汎用領域に記録する。

【０２８１】

次に、ステップＳ２０６において、コンテンツＣ２から生成したコンテンツハッシュリスト集合及びＫｔ１ハッシュ値に対する暗号化コンテンツ署名ＥＣＳ２Ｓｉｇを生成する。以下の署名データである。

ＥＣＳ２Ｓｉｇ＝Ｓｉｇｎ（ＥＣＳ署名鍵，Ｍ）

ただし、

Ｍ＝コンテンツＣ２のコンテンツハッシュリスト集合｜｜Ｋｔ１ハッシュ値

である。

なお、署名生成には漏えいした暗号化コンテンツ署名発行装置の署名鍵（秘密鍵）を適用する。

【０２８２】

最後にステップＳ２０７において、ステップＳ２０６で不正に生成したＥＣＳ署名（ＥＣＳ２Ｓｉｇ（Ｃ２，Ｋｔ１））を含むＥＣＳファイルを生成してメモリカードの汎用領域に記録する。

【０２８３】

この図２５に示す一連の処理によって図２４（ｂ）に示す「すげ替えデータ」の記録処

理が終了する。
このようなすげ替え処理によって、コンテンツＣ２を、異なるコンテンツ（Ｃ１）のタイトルキー（Ｋｔ１）を適用して暗号化されたコンテンツＣ２（Ｋｔ１）が生成される。
なお、本例では、不正記録コンテンツＣ２（Ｋｔ１）に対応する利用制御情報として、コンテンツＣ１の利用制御情報（ＵＲ１）をそのまま利用するものとする。
【０２８４】
次に、図２４（ｂ）に示す「すげ替えデータ」を利用してコンテンツＣ２を再生するユーザ装置の処理について、図２６に示すフローチャートを参照して説明する。
まず、ステップＳ２２１において、ユーザ装置は、メモリカードの汎用領域から再生予定の暗号化コンテンツＣ２（Ｋｔ１）と、このコンテンツに対して生成されたＥＣＳファイル（ＥＣＳ２（Ｃ２，Ｋｔ１））を読み出す。
【０２８５】
次にステップＳ２２２において、メモリカードの汎用領域からコンテンツＣ２に対応付けて記録されている利用制御情報（ＵＲ１）からタイトルキーの格納ブロックを示すブロック識別子を読み取る。
前述したように、本例では、不正記録コンテンツＣ２（Ｋｔ１）に対応する利用制御情報として、コンテンツＣ１の利用制御情報（ＵＲ１）をそのまま利用する。
【０２８６】
先に図２３を参照して説明したように、利用制御情報（ＵＲ）には、タイトルキーを格納したブロック識別子、タイトルキー識別子等が記録されている。
ステップＳ２２２では、コンテンツＣ１の利用制御情報（ＵＲ１）からブロック識別子、タイトルキー識別子を読み取る。
このブロック識別子、タイトルキー識別子は、コンテンツＣ１に対する正当なタイトルキーＫｔ１の格納されたブロックと、そのブロックに格納されたタイトルキーに対応する識別子である。
したがって、読み取りデータは、コンテンツＣ１に対するタイトルキー変換データ、すなわち、
Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ
となる。
【０２８７】
次に、ステップＳ２２３において、汎用領域から読み出した利用制御情報（ＵＲ１）とコンテンツＣ２に対応して不正に生成したＥＣＳファイル（ＥＣＳ２（Ｃ２，Ｋｔ１））の連結データのハッシュ値を算出し、算出結果と、保護領域から読み出した上記のタイトルキー変換データとの排他的論理和演算（ＸＯＲ）を実行してコンテンツＣ２に対応する復号用のタイトルキーＫｔ２の取得を試みる。
ここでは、Ｋｔ２＝Ｋｔ１となるタイトルキーＫｔ２が得られればタイトルキーの取得に成功したことになる。
【０２８８】
すなわち、以下の式に従ってタイトルキー算出処理を試みる。
Ｋｔ２＝（保護領域からの読み出しデータ）（＋）（汎用領域からの読み出しデータ）
＝Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ２Ｓｉｇ）ｈａｓｈ（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ
上記タイトルキー算出式に従ってタイトルキー（Ｋｔ２）の取得を試みる。
なお、（＋）は排他的論理和演算（ＸＯＲ）を意味する。
【０２８９】
しかし、上記タイトルキー算出式において、
ＥＣＳ２Ｓｉｇ≠ＥＣＳ１Ｓｉｇ
であるため、
上記算出式によってえられる値：Ｋｔ２は、Ｋｔ１とは異なる値、すなわち、
Ｋｔ２≠Ｋｔ１

となる。

【０２９０】

この結果、ユーザ装置は、コンテンツＣ２の暗号化に適用したタイトルキーＫｔ１を取得することはできず、コンテンツＣ２の復号、再生は失敗する。ステップＳ２２４の処理である。

【０２９１】

また、ステップＳ２２５において、ユーザ装置は、予め規定された再生シーケンスに従って、汎用領域から読み出したＥＣＳファイルに含まれるＥＣＳ発行装置署名（ＥＣＳＳｉｇ）の検証処理を実行する。

以下の式に従って署名検証処理を行う。

Ｖｅｒｉｆｙ（ＥＣＳ発行装置公開鍵，ＥＣＳ２Ｓｉｇ，Ｍ）

ただし、

Ｖｅｒｉｆｙ（ｋ，Ｓ，Ｍ）は、データＭに対する電子署名Ｓを検証鍵ｋを用いて検証する処理を示す。

Ｍ＝コンテンツＣ２のコンテンツハッシュリスト集合｜｜Ｋｔ２ハッシュである。

Ｋｔ２は、ステップＳ２２３で算出した値を利用することになる。

【０２９２】

ＥＣＳファイルに格納したＥＣＳ２Ｓｉｇは、図２５に示すフローのステップＳ２０６において生成した不正な署名であり、以下のデータである。

ＥＣＳ２Ｓｉｇ＝Ｓｉｇｎ（ＥＣＳ署名鍵，Ｍ）

ただし、

Ｍ＝コンテンツＣ２のコンテンツハッシュリスト集合｜｜Ｋｔ１ハッシュ値

である。

【０２９３】

このように、

署名検証に適用するデータＭは、Ｋｔ２ハッシュ値を含むデータであるのに対して、

ＥＣＳファイルに格納された署名データＥＣＳ２Ｓｉｇは、Ｋｔ１ハッシュを含むＭに対して生成されている。

従って、このステップＳ２２５における署名検証は失敗する。図２６のステップＳ２２６に記載の通りである。

【０２９４】

このように、ユーザ装置は、図２４（ｂ）に示す「すげ替えデータ」を適用してコンテンツＣ２の復号、再生を行おうとしても、

コンテンツＣ２の復号に失敗、

ＥＣＳファイルの署名検証に失敗、

これらの結果となり、結果としてコンテンツＣ２を利用することはできない。

【０２９５】

図２４～図２６を参照して説明した処理例は、コンテンツＣ１のタイトルキーＫｔ１を適用して、新たなコンテンツＣ２の暗号化と復号を試みた処理例であった。

次に、図２７以下を参照して、コンテンツＣ１に対応する正しい利用制御情報（ＵＲ１）を不正に改ざんして、新たな利用制御情報（ＵＲ２）を生成した不正処理を行う場合の例について説明する。

利用制御情報には、例えば、コンテンツの利用期間情報やコピー制限情報などが記録されており、この利用制御情報の書き換えによって、利用可能期限を延長するといった不正が行われる可能性がある。

【０２９６】

図２７は、先に説明した図２４と同様、

（ａ）コンテンツ（Ｃ１）に対応する正当なデータ格納構成

（ｂ）コンテンツ（Ｃ１）に対応するタイトルキー（Ｋｔ１）を利用してコンテンツ（Ｃ２）を暗号化したすげ替えデータのデータ格納構成を示している。

【０２９７】
図２７（ａ）に示す正当データ格納構成では、
メモリカードの汎用領域に、以下のデータが格納される。
（ａ１）コンテンツ（Ｃ１）に対する正当なタイトルキー（Ｋｔ１）で暗号化された暗号化コンテンツ（Ｃ１（Ｋｔ１））
（ａ２）コンテンツ（Ｃ１）に対する正当な利用制御情報（ＵＲ１）
（ａ３）コンテンツ（Ｃ１）に対する正当な暗号化コンテンツ署名ファイル（ＥＣＳファイル：ＥＣＳ１（Ｃ１，Ｋｔ１））
【０２９８】
なお、ＥＣＳファイルには、ＥＣＳ発行装置署名（ＥＣＳＳｉｇ）が格納されており、このＥＣＳ発行装置署名（ＥＣＳＳｉｇ）は、先に、図１３を参照して説明したように、コンテンツ（Ｃ１）のハッシュリスト集合と、タイトルキー（Ｋｔ１）のハッシュ値を含むデータに基づいて生成された電子署名を含む。この署名データの生成元データを明示するため、ＥＣＳファイルは、ＥＣＳ１（Ｃ１，Ｋｔ１）として記載している。
【０２９９】
また、図２７（ａ）に示す正当データ格納構成では、
メモリカードの保護領域のブロックＮに、タイトルキー（Ｋｔ１）の変換データ、すなわち、以下のデータが記録される。
Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ
ただし、
ＵＲ１：コンテンツ１に対応する利用制御情報
ＥＣＳ１Ｓｉｇ：コンテンツ１に対応するＥＣＳファイルの構成データであるＥＣＳ発行装置署名（Ｓｉｇｎａｔｕｒｅ　ｂｙ　ＥＣＳ　Ｉｓｓｕｅｒ）
また、演算子としての記号、
（＋）：排他的論理和演算
｜｜：データの連結を意味し、ａ｜｜ｂはデータａとデータｂの連結データを意味する。
ｈａｓｈ：ハッシュ値を意味し、（ａ｜｜ｂ）ｈａｓｈは、データａとデータｂの連結データのハッシュ値を意味する。
【０３００】
例えば、悪意のあるコンテンツ提供サーバやユーザ装置は、このコンテンツ（Ｃ１）の利用制御情報（ＵＲ１）の書き換えを行う。
この不正処理の結果、メモリカードには、図２７（ｂ）に示す「すげ替えデータ」が格納される。
【０３０１】
図２７（ｂ）に示す「すげ替えデータ」格納構成では、
メモリカードの汎用領域に、以下のデータが格納される。
（ｂ１）コンテンツ（Ｃ１）に対する不正生成したタイトルキー（Ｋｔ２）で暗号化された不正暗号化コンテンツ（Ｃ１（Ｋｔ２））
（ｂ２）コンテンツ（Ｃ１）に対応させて不正に生成した利用制御情報（ＵＲ２）
（ｂ３）コンテンツ（Ｃ１）に対応させて不正に生成した暗号化コンテンツ署名ファイル（ＥＣＳ２［＝ＥＣＳ２（Ｃ１，Ｋｔ２）］
【０３０２】
なお、不正なＥＣＳファイル：ＥＣＳ２に格納されるＥＣＳ発行装置署名（ＥＣＳＳｉｇ）は、コンテンツ（Ｃ１）のハッシュリスト集合と、不正生成したタイトルキー（Ｋｔ２）のハッシュ値を含むデータに基づいて、漏えいしたＥＣＳ発行装置の署名鍵（秘密鍵）によって生成した電子署名を含む。この署名データの生成元データを明示するため、ＥＣＳファイルは、ＥＣＳ２（Ｃ１，Ｋｔ２）として記載している。
【０３０３】
また、図２７（ｂ）に示す「すげ替えデータ」格納構成では、

メモリカードの保護領域のブロックＮに、タイトルキー（Ｋｔ１）の変換データ、すなわち、以下のデータが記録される。

Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ

【０３０４】

この図２７（ｂ）に示す「すげ替えデータ」の記録処理シーケンスについて図２８に示すフローチャートを参照して説明する。

なお、この図２８に示す処理は、既に、図２７（ａ）に示すコンテンツ（Ｃ１）に対応する正当なデータセットを格納したメモリカードを利用して実行され、メモリカードの保護領域のブロックＮに対するアクセス権としてデータ記録処理の権利を有する装置、例えばコンテンツ提供サーバやユーザ装置によって実行される処理である。

【０３０５】

まず、ステップＳ２４１において、コンテンツＣ１対応の利用制御情報ＵＲ１を汎用領域から読み出して、例えば利用期限情報などの書き換え等の改ざんを行い不正な利用制御情報（ＵＲ２）を生成する。

【０３０６】

次に、ステップＳ２４２において、メモリカードの汎用領域に記録されたコンテンツ（Ｃ１）の利用制御情報（ＵＲ１）から、「ブロック識別子」及び「タイトルキー識別子」を取得し、これらの取得情報に基づいて、保護領域の所定ブロック、すなわちタイトルキー格納ブロックから、正当なコンテンツ（Ｃ１）に対応する以下のタイトルキー変換データを読み出す。

Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ

なお、ＥＣＳ１Ｓｉｇ＝Ｓｉｇｎ（ＥＣＳ署名鍵，Ｍ）

Ｍ＝コンテンツＣ１のコンテンツハッシュリスト集合｜｜Ｋｔ１ハッシュ値

である。

【０３０７】

次に、ステップＳ２４３において、汎用領域から読み出した正当なコンテンツ（Ｃ１）に対応する利用制御情報（ＵＲ１）とＥＣＳファイル（ＥＣＳ１（Ｃ１，Ｋｔ１））の連結データのハッシュ値を算出し、算出結果と、保護領域から読み出した上記のタイトルキー変換データとの排他的論理和演算（ＸＯＲ）を実行してコンテンツ（Ｃ１）に対応する正当なタイトルキー（Ｋｔ１）を取得する。

すなわち、

Ｋｔ１＝（汎用領域からの読み出しデータ）（＋）（保護領域からの読み出しデータ）

＝（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ（＋）Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ

上記式に従ってタイトルキー（Ｋｔ１）を取得する。

なお、（＋）は排他的論理和演算（ＸＯＲ）を意味する。

【０３０８】

さらに、コンテンツＣ２の暗号化と復号に適用するタイトルキーＫｔ２を以下の式に従って算出する。

Ｋｔ２＝（Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ（＋）（ＵＲ２｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ

【０３０９】

次に、ステップＳ２４４において、ステップＳ２４３で生成したタイトルキーＫｔ１を適用してコンテンツＣ１（Ｋｔ１）を復号し、さらに、ステップＳ２４３で生成した新たなタイトルキーＫｔ２を適用してコンテンツＣ１暗号化して暗号化コンテンツＣ１（Ｋｔ２）を生成する。

【０３１０】

次に、ステップＳ２４５において、暗号化コンテンツＣ１（Ｋｔ２）をメモリカードの汎用領域に記録する。

【０３１１】

次に、ステップＳ２４６において、コンテンツＣ１から生成したコンテンツハッシュリスト集合及びＫｔ２ハッシュ値に対する暗号化コンテンツ署名ＥＣＳ２Ｓｉｇを生成する。以下の署名データである。

ＥＣＳ２Ｓｉｇ＝Ｓｉｇｎ（ＥＣＳ署名鍵，Ｍ）

ただし、

Ｍ＝コンテンツＣ１のコンテンツハッシュリスト集合｜｜Ｋｔ２ハッシュ値

である。

なお、署名生成には漏えいした暗号化コンテンツ署名発行装置の署名鍵（秘密鍵）を適用する。

【０３１２】

次に、ステップＳ２４７において、ステップＳ２４６で不正に生成したＥＣＳ署名（ＥＣＳ２Ｓｉｇ（Ｃ１，Ｋｔ２））を含むＥＣＳファイルを生成してメモリカードの汎用領域に記録する。

最後に、ステップＳ２４８において、ステップＳ２４１で生成した利用制御情報ＵＲ２を汎用領域に記録する。

この図２８に示す一連の処理によって図２７（ｂ）に示す「すげ替えデータ」の記録処理が終了する。

このようなすげ替え処理によって、コンテンツＣ１に対して不正に生成した利用制御情報（ＵＲ２）が対応づけられる。なお、コンテンツＣ１は新たなタイトルキーＫｔ２によって暗号化されて記録される。

【０３１３】

次に、図２７（ｂ）に示す「すげ替えデータ」を利用してコンテンツＣ１を再生するユーザ装置の処理について、図２９に示すフローチャートを参照して説明する。

まず、ステップＳ２６１において、ユーザ装置は、メモリカードの汎用領域から再生予定の暗号化コンテンツＣ１（Ｋｔ２）と、このコンテンツに対して生成されたＥＣＳファイル（ＥＣＳ２（Ｃ１，Ｋｔ２））を読み出す。

【０３１４】

次にステップＳ２６２において、メモリカードの汎用領域からコンテンツＣ１に対応付けて不正に生成した新たな利用制御情報（ＵＲ２）からタイトルキーの格納ブロックを示すブロック識別子、タイトルキー識別子を読み取る。

このブロック識別子、タイトルキー識別子は、改ざん前の正当な利用制御情報（ＵＲ１）のままに設定されている。

すなわち、このブロック識別子、タイトルキー識別子は、コンテンツＣ１に対する正当なタイトルキーＫｔ１の格納されたブロックと、そのブロックに格納されたタイトルキーに対応する識別子である。

したがって、読み取りデータは、コンテンツＣ１に対するタイトルキー変換データ、すなわち、

Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ

となる。

【０３１５】

次に、ステップＳ２６３において、汎用領域から読み出した不正に生成した利用制御情報（ＵＲ２）と不正に生成したＥＣＳファイル（ＥＣＳ２（Ｃ１，Ｋｔ２））の連結データのハッシュ値を算出し、算出結果と、保護領域から読み出した上記のタイトルキー変換データとの排他的論理和演算（ＸＯＲ）を実行してコンテンツＣ１に対応する復号用のタイトルキーＫｔ３の取得を試みる。

ここでは、Ｋｔ３＝Ｋｔ２となるタイトルキーＫｔ３が得られればタイトルキーの取得に成功したことになる。

【０３１６】

ステップＳ２６３では、以下の式に従ってタイトルキー算出処理を試みる。

Ｋｔ３＝（保護領域からの読み出しデータ）（＋）（汎用領域からの読み出しデータ）

＝Ｋｔ１（＋）（ＵＲ１｜｜ＥＣＳ１Ｓｉｇ）ｈａｓｈ（＋）（ＵＲ２｜｜ＥＣＳ２Ｓｉｇ）ｈａｓｈ
上記タイトルキー算出式に従ってタイトルキー（Ｋｔ３）を生成する。
なお、（＋）は排他的論理和演算（ＸＯＲ）を意味する。

【０３１７】
しかし、上記タイトルキー算出式において、
Ｋｔ２は得られない。
上記算出式によってえられる値：Ｋｔ３は、Ｋｔ１ともＫｔ２とも異なる値、すなわち、
Ｋｔ３≠Ｋｔ２
Ｋｔ３≠Ｋｔ１
となる。

【０３１８】
この結果、ユーザ装置は、コンテンツＣ１の再暗号化に適用したタイトルキーＫｔ２を取得することはできず、コンテンツＣ１の復号、再生は失敗する。ステップＳ２６４の処理である。

【０３１９】
また、ステップＳ２６５において、ユーザ装置は、予め規定された再生シーケンスに従って、汎用領域から読み出したＥＣＳファイルに含まれるＥＣＳ発行装置署名（ＥＣＳＳｉｇ）の検証処理を実行する。
以下の式に従って署名検証処理を行う。
Ｖｅｒｉｆｙ（ＥＣＳ発行装置公開鍵，ＥＣＳ２Ｓｉｇ，Ｍ）
ただし、
Ｖｅｒｉｆｙ（ｋ，Ｓ，Ｍ）は、データＭに対する電子署名Ｓを検証鍵ｋを用いて検証する処理を示す。
Ｍ＝コンテンツＣ１のコンテンツハッシュリスト集合｜｜Ｋｔ３ハッシュである。
Ｋｔ３は、ステップＳ２６３で算出した値を利用することになる。

【０３２０】
ＥＣＳファイルに格納したＥＣＳ２Ｓｉｇは、図２８に示すフローのステップＳ２４６において生成した不正な署名であり、以下のデータである。
ＥＣＳ２Ｓｉｇ＝Ｓｉｇｎ（ＥＣＳ署名鍵，Ｍ）
ただし、
Ｍ＝コンテンツＣ１のコンテンツハッシュリスト集合｜｜Ｋｔ２ハッシュ値
である。

【０３２１】
このように、
署名検証に適用するデータＭは、Ｋｔ３ハッシュ値を含むデータであるのに対して、
ＥＣＳファイルに格納された署名データＥＣＳ２Ｓｉｇは、Ｋｔ２ハッシュを含むＭに対して生成されている。
従って、このステップＳ２６５における署名検証は失敗する。図２９のステップＳ２６６に記載の通りである。

【０３２２】
このように、ユーザ装置は、図２７（ｂ）に示す「すげ替えデータ」を適用してコンテンツＣ１の復号、再生を行おうとしても、
コンテンツＣ１の復号に失敗、
ＥＣＳファイルの署名検証に失敗、
これらの結果となり、結果としてコンテンツＣ１を利用することはできない。

【０３２３】
このように、メモリカードの保護領域に記録するタイトルキーを、
利用制御情報（ＵＲ）とＥＣＳ発行装置署名（ＥＣＳＳｉｇ）との連結データのハッシ

ュ値との排他的論理和（ＸＯＲ）演算結果として格納することで、ＥＣＳ発行装置署名（ＥＣＳＳｉｇ）に適用するＥＣＳ発行装置の署名鍵（秘密鍵）の漏えいが発生した場合にもコンテンツの不正利用を防止することが可能となる。

【０３２４】

例えば、コンテンツ提供サーバやユーザ装置が、漏えいしたＥＣＳ発行装置の署名鍵（秘密鍵）を適用した不正処理、具体的には、暗号化コンテンツの暗号鍵のすげ替え処理や、利用制御情報の改ざんなどによるコンテンツ不正利用を防止可能となる。

【０３２５】

［１１．暗号化コンテンツ署名（ＥＣＳ）ファイルに記録したブロック識別子の適用処理について］

次に、暗号化コンテンツ署名（ＥＣＳ）ファイルに記録したブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）の適用処理について説明する。

【０３２６】

先に、図９を参照して説明したように、暗号化コンテンツ署名（ＥＣＳ）ファイルには、ブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が記録される。

ブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）は、図１３を参照して説明したように、コンテンツ提供装置（Ｃｏｎｔｅｎｔ　Ｓｅｒｖｅｒ）１０３から、暗号化コンテンツ署名（ＥＣＳ）発行装置１０２に通知されるデータであり、コンテンツ提供装置１０３がユーザ装置１０４に対して提供したコンテンツに対応する暗号鍵であるタイトルキーを格納したメディアの保護領域のブロックの識別子である。これは、コンテンツ提供装置１０３が利用可能なメディアの保護領域におけるブロックの識別子である。

先に、図３、図６等を参照して説明したように、コンテンツ提供装置の利用可能なメディアの保護領域のブロックは予め設定されており、これらのアクセス許容ブロック情報が記録される。

【０３２７】

また、このブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）に対応する情報は、図９を参照して説明したようにＥＣＳ発行装置証明書にも記録される。

先に、図９を参照して説明したように、

（ａ）ブロック識別子開始番号（Ｓｔａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）

（ｂ）ブロック識別子範囲（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ　Ｃｏｕｎｔｅｒ）

である。

【０３２８】

（ａ）ブロック識別子開始番号（Ｓｔａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）は、ＥＣＳ発行装置１０２が、コンテンツ提供装置１０３に対して許容可能なメディアの保護領域のアクセス許容ブロックの開始番号である。

（ｂ）ブロック識別子範囲（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ　Ｃｏｕｎｔｅｒ）は、ＥＣＳ発行装置１０２が、コンテンツ提供装置１０３に対して許容可能なメディアの保護領域のアクセス許容ブロックの開始番号からの範囲を示す情報である。

【０３２９】

さらに、先に図２３を参照して説明したように、ブロック識別子は、コンテンツ対応の利用制御情報（ＵＲ）にも記録される。利用制御情報（ＵＲ）に記録されるブロック識別子は、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を示すブロック識別子である。

【０３３０】

図３０に、

暗号化コンテンツ署名（ＥＣＳ）ファイル、

利用制御情報（ＵＲ）、

これらに記録されたブロック識別子と保護領域のタイトルキー格納ブロック（図に示す例ではブロックｋ）との対応関係を示す。

【０３３１】

図３０に示すように、メモリカードの汎用領域にはコンテンツに対応する、
暗号化コンテンツ署名（ＥＣＳ）ファイル、
利用制御情報（ＵＲ）、
これらのデータが格納される。
また、保護領域のブロックｋには、
コンテンツに対応するタイトルキーの変換データ、すなわち、
Ｋｔ（＋）ＵＲ｜｜（ＥＣＳＳｉｇ）ｈａｓｈ
が格納される。

【０３３２】

ユーザ装置に対して、コンテンツを提供するコンテンツ提供装置は、自己の有するホスト証明書（図４参照）に記録された保護領域アクセス権情報としてのブロック識別子と、ＥＣＳ発行装置証明書中のブロック識別子としての書き込み許容ブロック領域情報とを比較する。

この比較結果に応じて、コンテンツ提供の可否を判定する。

【０３３３】

また、コンテンツ再生を行うユーザ装置は、利用制御情報中のブロック識別子とＥＣＳファイル中のブロック識別子とを比較する。

この比較結果に応じて、コンテンツ再生の可否を判定する。

【０３３４】

まず、コンテンツ提供サーバにおけるブロック識別子を利用したコンテンツ提供の可否判定シーケンスについて図３１に示すフローチャートを参照して説明する。

【０３３５】

なお、図３１に示すフローチャートのステップＳ４０１の前処理として、コンテンツ提供装置は、暗号化コンテンツ署名ファイル（ＥＣＳファイル）発行装置から受信した暗号化コンテンツ署名ファイル（ＥＣＳファイル）に設定されたＥＣＳ発行装置署名を適用した署名検証を実行する。

この署名検証が成立し、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の正当性が確認され場合は、さらに、暗号化コンテンツ署名ファイル（ＥＣＳファイル）に格納されたＥＣＳ発行装置証明書の署名検証を実行する。これらの２つの署名検証が成立したことを条件としてステップＳ４０１以下の処理を行う。

【０３３６】

上記２つの署名検証の少なくともいずれかが成立しなかった場合は、暗号化コンテンツ署名ファイル（ＥＣＳファイル）またはＥＣＳ発行装置証明書の正当性が確認されないので、ステップＳ４０１以下の処理は実行されない。この場合はコンテンツ提供処理も実行しないことになる。

なお、暗号化コンテンツ署名ファイル（ＥＣＳファイル）に格納されるコンテンツハッシュリスト集合の元データであるコンテンツハッシュは、暗号化コンテンツのハッシュまたは暗号化前のコンテンツのハッシュ、いずれの設定としてもよい。

【０３３７】

暗号化コンテンツ署名ファイル（ＥＣＳファイル）と、ＥＣＳ発行装置証明書の２つの署名検証が成立し、暗号化コンテンツ署名ファイル（ＥＣＳファイル）とＥＣＳ発行装置証明書の正当性が確認された場合、コンテンツ提供装置は、ステップＳ４０１の処理を実行する。

コンテンツ提供装置は、まず、ステップＳ４０１において、ＥＣＳファイル内のＥＣＳ発行装置証明書を読み出して、ＥＣＳ発行装置証明書に記録されたブロック識別子情報を読み出す。

【０３３８】

このステップＳ４０１の処理の詳細について、図３２に示すフローを参照して説明する。

ステップＳ４２１において、ＥＣＳ発行装置証明書内のブロック識別子開始番号（Ｓｔ

ａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ　）を読みだす。
　ブロック識別子開始番号（Ｓｔａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）は、ＥＣＳ発行装置１０２が、コンテンツ提供装置１０３に対して許容したメディアの保護領域のアクセス許容ブロックの開始番号である。
【０３３９】
　次に、ステップＳ４２２において、ＥＣＳ発行装置証明書内のブロック識別子開始番号（Ｓｔａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が０ｘＦＦＦＦＦＦＦＦであるか否かを判定する。
　なお、ブロック識別子開始番号（Ｓｔａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が０ｘＦＦＦＦＦＦＦＦである場合は全ブロックに対するアクセス許容が設定された状態に対応する。
【０３４０】
　ステップＳ４２２において、ブロック識別子開始番号（Ｓｔａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が０ｘＦＦＦＦＦＦＦＦであると判定した場合は、ステップＳ４２３に進み、メディアの保護領域に設定された全ブロックをアクセス許容ブロックとみなす。
【０３４１】
　一方、ステップＳ４２２において、ブロック識別子開始番号（Ｓｔａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が０ｘＦＦＦＦＦＦＦＦでないと判定した場合は、ステップＳ４２４に進む。
　ステップＳ４２４では、ＥＣＳ発行装置証明書内のブロック識別子範囲情報（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ　Ｃｏｕｎｔｅｒ）を読みだす。
　ブロック識別子範囲（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ　Ｃｏｕｎｔｅｒ）は、ＥＣＳ発行装置１０２が、コンテンツ提供装置１０３に対して許容可能なメディアの保護領域のアクセス許容ブロックの開始番号からの範囲を示す情報である。
【０３４２】
　次のステップＳ４２５～Ｓ４２８の処理は、ブロック識別子を示す変数Ｉを０から順次、１，２，３・・とインクリメントして実行する繰り返しルーチンである。
　まずステップＳ４２５において
　変数：Ｉ＝１とする。
【０３４３】
　次に、ステップＳ４２６において、ブロック識別子開始番号（Ｓｔａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）＋Ｉをブロック識別子リスト（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ　Ｌｉｓｔ）に追加する。
【０３４４】
　次に、ステップＳ４２７において、
　Ｉ＝Ｉ＋１
　とする。
【０３４５】
　次に、ステップＳ４２８において、Ｉがブロック識別子範囲情報（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ　Ｃｏｕｎｔｅｒ）と等しいか否かを判定する。
　等しければ、処理を終了する。等しくなければ、ステップＳ４２６に戻り、処理を繰り返す。
　この処理に従って、図３１に示すフローのステップＳ４０１の処理が行われる。
【０３４６】
　ステップＳ４０１では、ＥＣＳ発行装置証明書内のブロック識別子開始番号（Ｓｔａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）と、ブロック識別子範囲情報（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ　Ｃｏｕｎｔｅｒ）を適用して、ＥＣＳ発行装置証明書において規定されたアクセス許容範囲を算出しこれをアクセス許容ブロック識別子リストとして設定する。
【０３４７】

次に、ステップＳ４０２において、ステップＳ４０１で生成したアクセス許容ブロック識別子リストに、暗号化コンテンツ署名（ＥＣＳ）ファイルの記録データとして記載されたブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が含まれるか否かを判定する。

【０３４８】

含まれていなければ、ステップＳ４０５に進み、ユーザ装置に対するコンテンツ提供処理は実行しない。

一方、含まれている場合は、ステップＳ４０３に進む。

【０３４９】

ステップＳ４０３では、暗号化コンテンツ署名（ＥＣＳ）ファイルの記録データとして記載されたブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が、利用制御情報（ＵＲ）に記録されたブロック識別子と一致するか否かを判定する。

一致しなければ、ステップＳ４０５に進み、ユーザ装置に対するコンテンツ提供処理は実行しない。

一方、一致した場合は、ステップＳ４０４に進み、ユーザ装置に対するコンテンツ提供を実行する。

【０３５０】

このように、コンテンツ提供装置は、

（ａ）暗号化コンテンツ署名（ＥＣＳ）ファイルに記録されたブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が、ＥＣＳ発行装置証明書に記録されたアクセス許容ブロックの範囲内であること、

（ｂ）暗号化コンテンツ署名（ＥＣＳ）ファイルに記録されたブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が、利用制御情報（ＵＲ）に記録されたブロック識別子に一致すること、

これら（ａ）、（ｂ）の条件を満足するか否かを判定し、満足する場合にのみ、ユーザ装置に対するコンテンツ提供を実行する。

【０３５１】

次に、図３３に示すフローチャートを参照して、コンテンツ再生処理を実行するユーザ装置におけるブロック識別子の適用処理について説明する。

【０３５２】

なお、ユーザ装置は、図３３に示すステップＳ４５１以前に、コンテンツ提供装置から受信した暗号化コンテンツ署名ファイル（ＥＣＳファイル）に設定されたＥＣＳ発行装置署名を適用した署名検証を実行する。

この署名検証が成立し、暗号化コンテンツ署名ファイル（ＥＣＳファイル）の正当性が確認され場合は、さらに、暗号化コンテンツ署名ファイル（ＥＣＳファイル）に格納されたＥＣＳ発行装置証明書の署名検証を実行する。これらの２つの署名検証が成立したことを条件としてステップＳ４５１以下の処理を行う。

【０３５３】

上記２つの署名検証の少なくともいずれかが成立しなかった場合は、暗号化コンテンツ署名ファイル（ＥＣＳファイル）またはＥＣＳ発行装置証明書の正当性が確認されないので、ステップＳ４５１以下の処理は実行されない。この場合はコンテンツ再生処理も実行しないことになる。

【０３５４】

暗号化コンテンツ署名ファイル（ＥＣＳファイル）と、ＥＣＳ発行装置証明書の２つの署名検証が成立し、暗号化コンテンツ署名ファイル（ＥＣＳファイル）とＥＣＳ発行装置証明書の正当性が確認された場合、ユーザ装置は、ステップＳ４５１の処理を実行する。

【０３５５】

ステップＳ４５１は、先にコンテンツ提供装置の処理として説明した図３１に示すフローのステップＳ４０１の処理と同様の処理である。すなわち、図３２に示すフローを参照して詳細を説明したように、ＥＣＳ発行装置証明書内のブロック識別子開始番号（Ｓｔａｒｔ　ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）と、ブロック識別子範囲情報（ＰＡＤ　Ｂｌ

ｏｃｋ　Ｎｕｍｂｅｒ　Ｃｏｕｎｔｅｒ）を適用して、ＥＣＳ発行装置証明書において規定されたアクセス許容範囲を算出しこれをアクセス許容ブロック識別子リストとして設定する。

【０３５６】

次に、ステップＳ４５２において、ステップＳ４５１で生成したアクセス許容ブロック識別子リストに、暗号化コンテンツ署名（ＥＣＳ）ファイルの記録データとして記載されたブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が含まれるか否かを判定する。

【０３５７】

含まれていなければ、ステップＳ４５５に進み、コンテンツ再生処理は実行しない。

一方、含まれている場合は、ステップＳ４５３に進む。

【０３５８】

ステップＳ４５３では、暗号化コンテンツ署名（ＥＣＳ）ファイルの記録データとして記載されたブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が、利用制御情報（ＵＲ）に記録されたブロック識別子と一致するか否かを判定する。

一致しなければ、ステップＳ４５５に進み、コンテンツ再生処理は実行しない。

一方、一致した場合は、ステップＳ４５４に進み、コンテンツ再生を実行する。

【０３５９】

なお、コンテンツ再生処理の開始前に、さらに、暗号化コンテンツの復号に適用するタイトルキーの取得や生成処理、さらに、暗号化コンテンツ署名ファイルに含まれるコンテンツハッシュリストを適用したハッシュ値照合処理を実行する。ハッシュ値照合において照合が成立し、コンテンツの改ざんのないことが確認された場合にコンテンツの再生が許容されることになる。

【０３６０】

このように、コンテンツ再生を実行するユーザ装置は、

（ａ）暗号化コンテンツ署名（ＥＣＳ）ファイルに記録されたブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が、ＥＣＳ発行装置証明書に記録されたアクセス許容ブロックの範囲内であること、

（ｂ）暗号化コンテンツ署名（ＥＣＳ）ファイルに記録されたブロック識別子（ＰＡＤ　Ｂｌｏｃｋ　Ｎｕｍｂｅｒ）が、利用制御情報（ＵＲ）に記録されたブロック識別子に一致すること、

これら（ａ）、（ｂ）の条件を満足するか否かを判定し、満足する場合にのみ、コンテンツ再生を実行する。

【０３６１】

［１２．各装置のハードウェア構成例について］

最後に、図３４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。

図３４は、図７、図８に示すユーザ装置１０４、コンテンツ提供装置１０３、暗号化コンテンツ署名発行装置１０２、ライセンス発行装置１０１のいずれにも適用可能な情報処理装置のハードウェア構成例を示している。

【０３６２】

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、上述した各フローチャートに従った処理を実行する。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。

【０３６３】

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。

【０３６４】

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。

【０３６５】

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。

【０３６６】

図３５は、情報記憶装置である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。

【０３６７】

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。

【０３６８】

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。

【０３６９】

なお、上述した実施例では、コンテンツ提供装置が提供するコンテンツは暗号化コンテンツである例を代表例として説明したが、本開示の構成は、提供コンテンツが暗号化コンテンツである場合に限らず、暗号化されていない平文コンテンツである場合にも適用可能である。なお、コンテンツが平文コンテンツである場合、上述の実施例で説明したタイトルキーは既知のデータ列、例えばオール０の値からなるキーデータであるものとして、上述した暗号化コンテンツの提供処理と同様の処理を行うことができる。

【０３７０】

［１３．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。

【０３７１】

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） 暗号化コンテンツおよび暗号化コンテンツの復号に適用する暗号鍵を格納する記憶部を有し、
前記記憶部は、前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵を格納し、
前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名であり、
前記記憶部から前記暗号化コンテンツを読み出して復号処理を実行する再生装置に、前記変換暗号鍵に対する電子署名の適用演算による暗号鍵取得を行わせることを可能とした情報記憶装置。
【０３７２】
（２）前記変換暗号鍵は、前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算結果である前記（１）に記載の情報記憶装置。
（３）前記記憶部は、アクセス制限の設定された保護領域を有し、前記変換暗号鍵を、前記保護領域に格納した構成である前記（１）または（２）に記載の情報記憶装置。
（４）前記情報記憶装置は、前記保護領域に対するアクセス要求装置から受領した証明書に基づいて、前記保護領域に対するアクセス可否を判定するデータ処理部を有する前記（３）に記載の情報記憶装置。
【０３７３】
（５）前記記憶部は、アクセス制限の設定された保護領域と、アクセス制限のない汎用領域を有し、前記変換暗号鍵を、前記保護領域に格納し、前記暗号化コンテンツと、前記暗号化コンテンツ署名ファイルを、前記汎用領域に格納した構成である前記（１）～（４）いずれかに記載の情報記憶装置。
（６）前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵、さらに、前記暗号化コンテンツ署名ファイルの構成データを含むデータに対する電子署名である前記（１）～（５）いずれかに記載の情報記憶装置。
（７）前記電子署名は、前記暗号化コンテンツ署名ファイルの構成データである前記暗号化コンテンツ署名ファイルの発行日時情報を含むデータに対する電子署名である前記（６）に記載の情報記憶装置。
【０３７４】
（８） メディアに記録された暗号化コンテンツの復号および再生処理を実行するデータ処理部を有し、
前記データ処理部は、
前記暗号化コンテンツの復号処理に際して、前記メディアに記録された前記暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を読み出し、該変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を実行し、
前記変換暗号鍵は、
前記暗号鍵を前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、
前記データ処理部は、
前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する情報処理装置。
【０３７５】
（９）前記電子署名は、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名である前記（８）に記載の情報処理装置。
（１０）前記変換暗号鍵は、前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演

算結果であり、前記データ処理部は、前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名と、前記メディアに記録された利用制御情報を取得し、取得したデータを適用した演算処理を実行して暗号鍵の取得処理を実行する前記（８）または（９）に記載の情報処理装置。

（１１）前記データ処理部は、前記メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名に対する署名検証処理を実行し、該署名検証処理に成功し、前記暗号化コンテンツ署名ファイルの正当性を確認したことを条件として、前記暗号鍵の取得処理を行う前記（８）～（１０）いずれかに記載の情報処理装置。

【０３７６】

（１２）　メディアに記録する暗号化コンテンツと、該暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を出力するデータ処理部を有し、

前記データ処理部は、

前記暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名であり、前記暗号化コンテンツの構成データおよび前記暗号鍵を含むデータに対する電子署名と、前記暗号鍵の演算処理により、前記変換暗号鍵を生成する情報処理装置。

（１３）前記データ処理部は、前記暗号化コンテンツに対応して設定される利用制御情報と、前記電子署名との連結データに対するハッシュ値と、前記暗号鍵との排他的論理和演算を実行して前記変換暗号鍵を生成する前記（１２）に記載の情報処理装置。

【０３７７】

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。

【０３７８】

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。

【０３７９】

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】

【０３８０】

以上、説明したように、本開示の一実施例の構成によれば、コンテンツの不正利用を効果的に防止する装置、方法が実現される。

具体的には、暗号化コンテンツの復号処理に際して、メディアに記録された暗号化コンテンツの復号に適用する暗号鍵の変換データである変換暗号鍵を読み出し、変換暗号鍵に対する演算処理を実行して暗号鍵の取得処理を実行する。変換暗号鍵は、暗号鍵と、暗号化コンテンツに対応して設定された暗号化コンテンツ署名ファイルの構成データである電子署名との演算によって生成された変換暗号鍵であり、再生装置は、メディアに記録された暗号化コンテンツ署名ファイルの構成データである電子署名を取得し、取得した電子署名を適用した演算処理を実行して暗号鍵の取得処理を実行する。電子署名は、暗号化コンテンツの構成データおよび暗号鍵を含むデータに対する電子署名として設定される。

この暗号化コンテンツ署名ファイルの署名データを変換暗号鍵の構成データとすること

で、鍵の掛け替え処理などによるコンテンツ不正利用を防止することが可能となる。

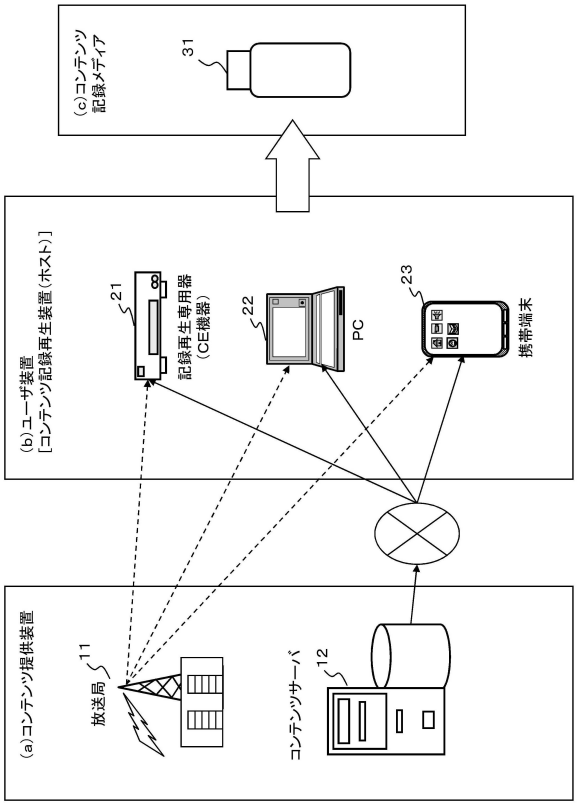
【符号の説明】

【０３８１】

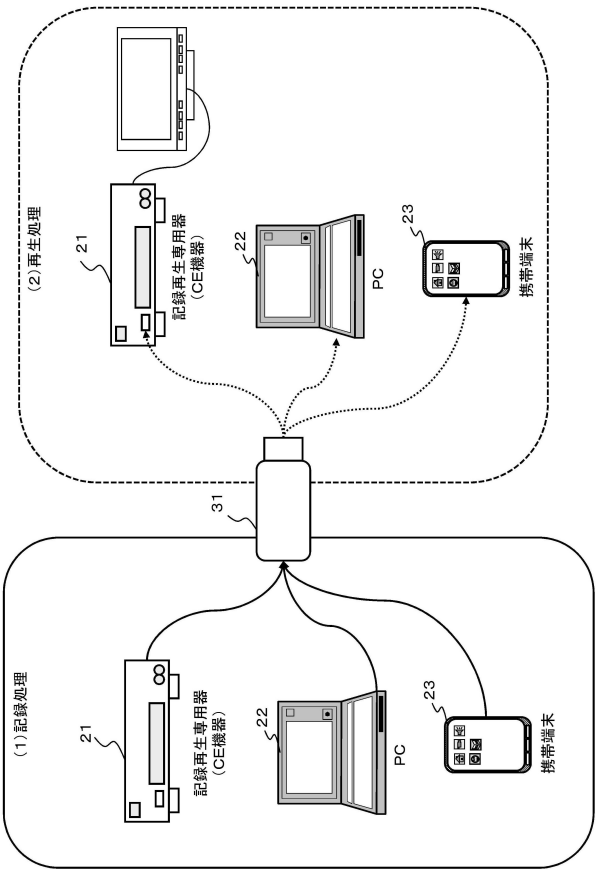
１１　放送局
１２　コンテンツサーバ
２１　記録再生専用器
２２　ＰＣ
２３　携帯端末
３１　メモリカード
５１　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
５２　汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）
６１　サーバＡ
６２　サーバＢ
６３　ホスト
６４　サーバＣ
６５　サーバＤ
７０　メモリカード
８０　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
８１　ブロック＃０
８２　ブロック＃１
９０　汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）
１０１　ライセンス発行装置
１０２　暗号化コンテンツ署名（ＥＣＳ）発行装置
１０３　コンテンツ提供装置
１０４　ユーザ装置
１８１　コンテンツ
１８２　タイトルキー
１８３　コンテンツハッシュリスト集合
２０１　コンテンツ提供装置（サーバ）
２０２　ユーザ装置（ホスト）
２１０　メモリカード
２１１　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
２１２　汎用領域（Ｇｅｎｅｒａｌ　Ｐｕｒｐｏｓｅ　Ａｒｅａ）
２２１　ブロック＃０
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）

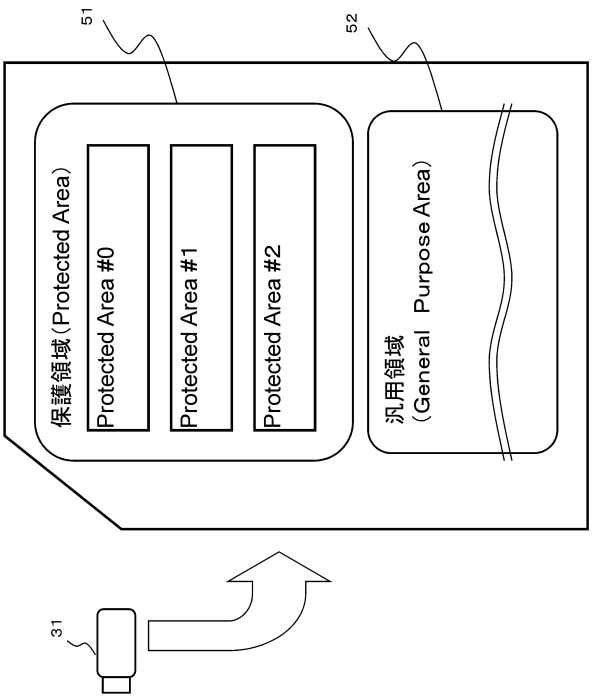
【図１】



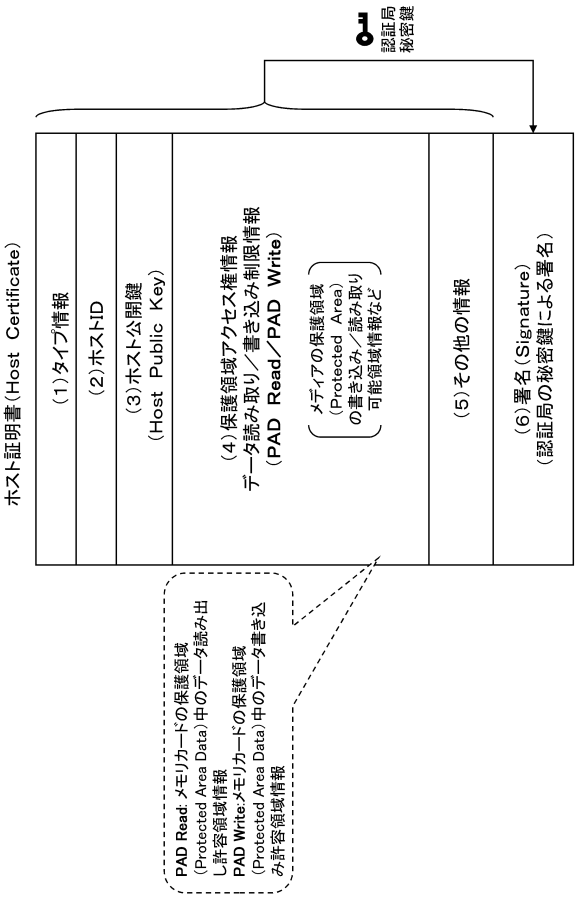
【図２】



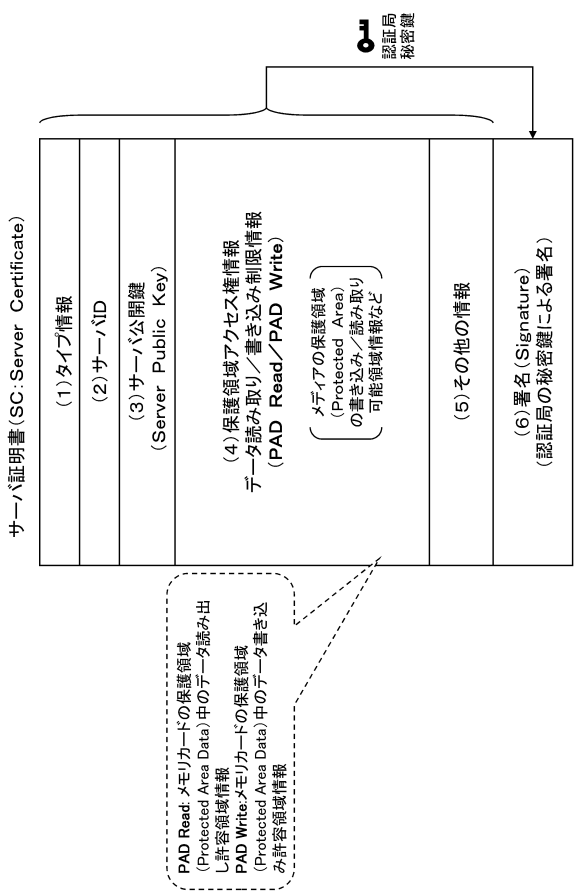
【図３】


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

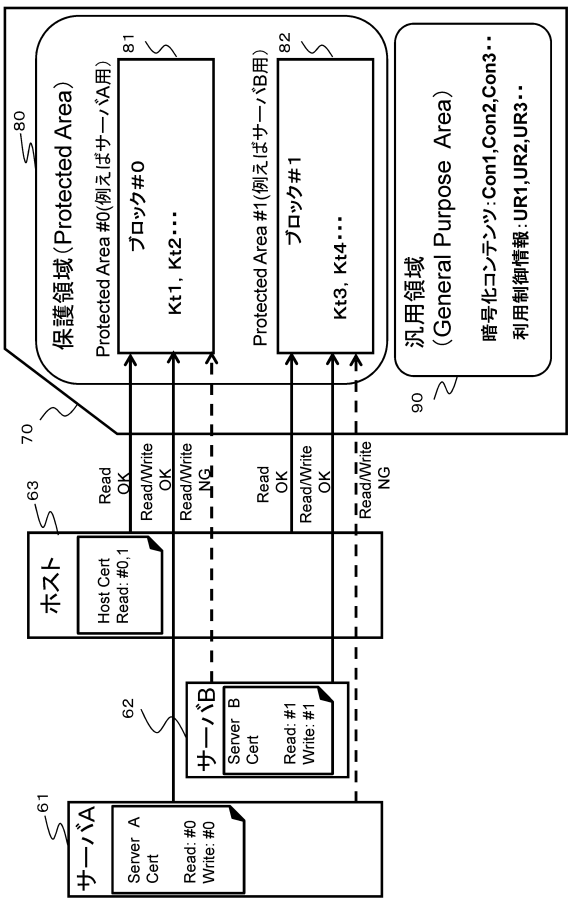
【図４】


認証局
秘密鍵
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)
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

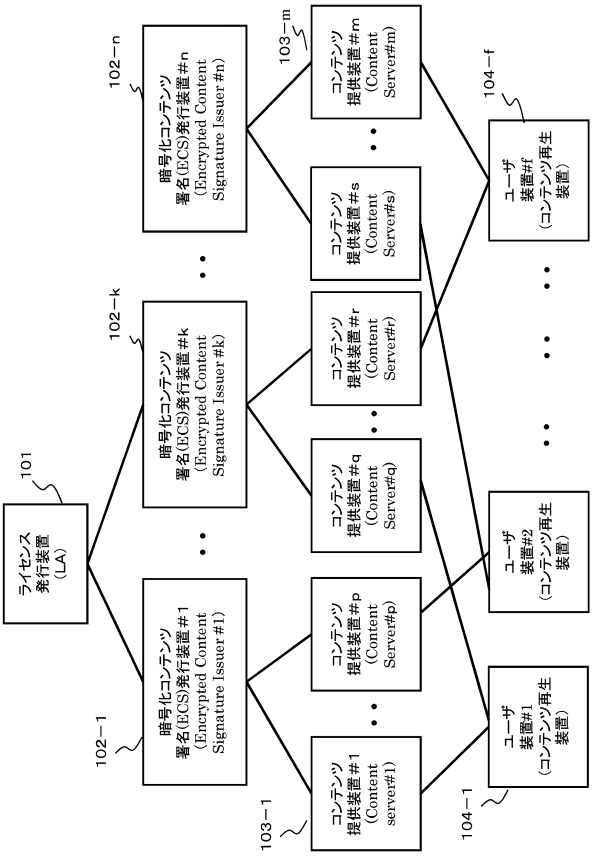
【図５】


認証局
秘密鍵
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)
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

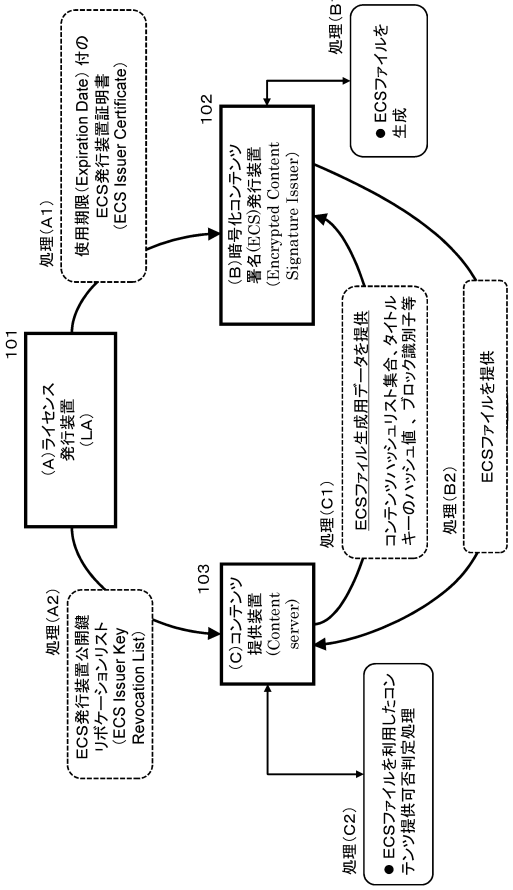
【図６】


80
保護領域(Protected Area)
Protected Area #0(例えばサーバA用)
81
ブロック#0
Kt1, Kt2・・・
Protected Area #1(例えばサーバB用)
82
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・・
90
70
63
ホスト
Host Cert
Read: #0,1
62
サーバB
Server B
Cert
Read: #1
Write: #1
61
サーバA
Server A
Cert
Read: #0
Write: #0
Read
OK
Read/Write
OK
Read/Write
NG
Read
OK
Read/Write
OK
Read/Write
NG

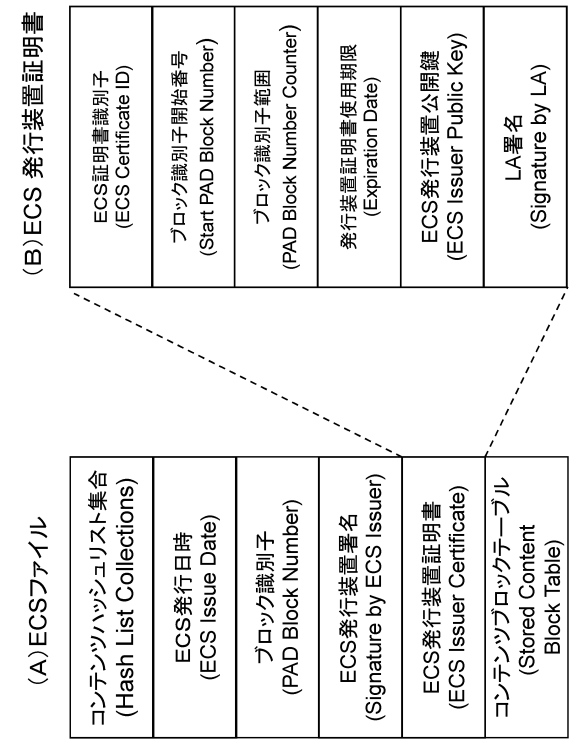
【図７】


ライセンス
発行装置
(LA)
101
暗号化コンテンツ
署名(ECS)発行装置#1
(Encrypted Content
Signature Issuer #1)
102−1
暗号化コンテンツ
署名(ECS)発行装置#k
(Encrypted Content
Signature Issuer #k)
102−k
暗号化コンテンツ
署名(ECS)発行装置#n
(Encrypted Content
Signature Issuer #n)
102−n
コンテンツ
提供装置#1
(Content
server#1)
103−1
コンテンツ
提供装置#p
(Content
Server#p)
コンテンツ
提供装置#q
(Content
Server#q)
コンテンツ
提供装置#r
(Content
Server#r)
コンテンツ
提供装置#s
(Content
Server#s)
コンテンツ
提供装置#m
(Content
Server#m)
103−m
ユーザ
装置#1
(コンテンツ再生
装置)
104−1
ユーザ
装置#2
(コンテンツ再生
装置)
ユーザ
装置#f
(コンテンツ再生
装置)
104−f

【図８】


(A)ライセンス
発行装置
(LA)
101
処理(A1)
使用期限(Expiration Date)付の
ECS発行装置証明書
(ECS Issuer Certificate)
処理(A2)
ECS発行装置公開鍵
リボケーションリスト
(ECS Issuer Key
Revocation List)
(B)暗号化コンテンツ
署名(ECS)発行装置
(Encrypted Content
Signature Issuer)
102
処理(B1)
● ECSファイルを
生成
(C)コンテンツ
提供装置
(Content
server)
103
処理(C1)
ECSファイル生成用データを提供
コンテンツハッシュリスト集合、タイトル
キーのハッシュ値、ブロック識別子等
処理(B2)
ECSファイルを提供
処理(C2)
● ECSファイルを利用したコン
テンツ提供可否判定処理

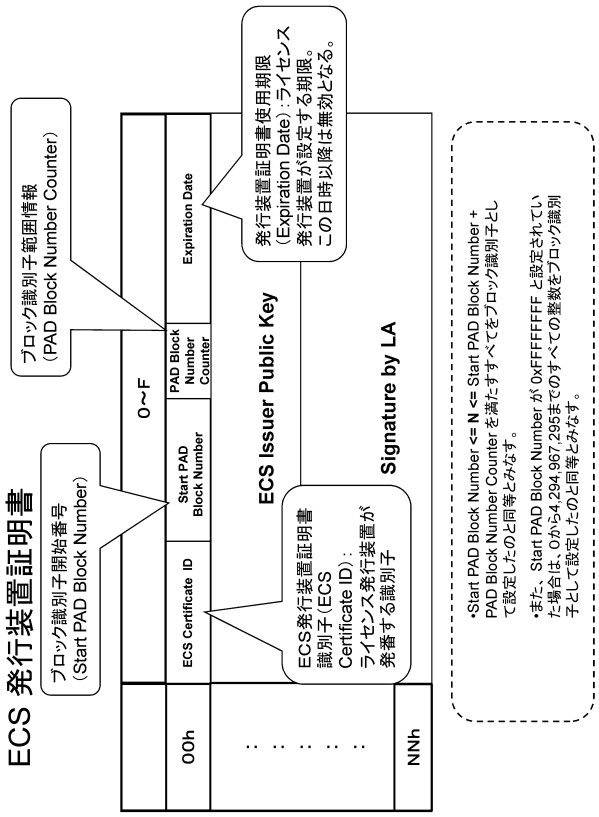
【図９】


(A)ECSファイル
コンテンツハッシュリスト集合
(Hash List Collections)
ECS発行日時
(ECS Issue Date)
ブロック識別子
(PAD Block Number)
ECS発行装置署名
(Signature by ECS Issuer)
ECS発行装置証明書
(ECS Issuer Certificate)
コンテンツブロックテーブル
(Stored Content
Block Table)
(B)ECS 発行装置証明書
ECS証明書識別子
(ECS Certificate ID)
ブロック識別子開始番号
(Start PAD Block Number)
ブロック識別子範囲
(PAD Block Number Counter)
発行装置証明書使用期限
(Expiration Date)
ECS発行装置公開鍵
(ECS Issuer Public Key)
LA署名
(Signature by LA)

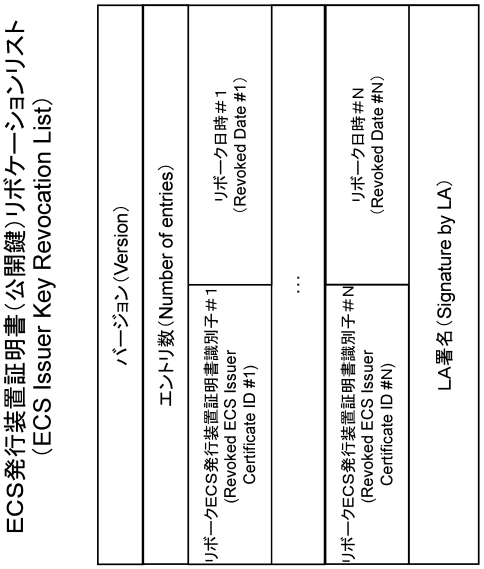
【図１０】

ECSファイル
00h
10h
NNh
Version
ECS
Type
Offset to ECS
Signature
Offset to Stored
Content Block
Table
Number Of Hash List
Collection
0~F
Hash List Collections
ECS Issue Date
PAD Block Number
ECS Signature
ECS Issuer Certificate
Stored Content Block Table
ECS発行日時：
ECS Signature
を生成した日時
ブロック識別子：
コンテンツの暗号化に使用
したタイトル鍵が記録された
保護領域のブロック番号

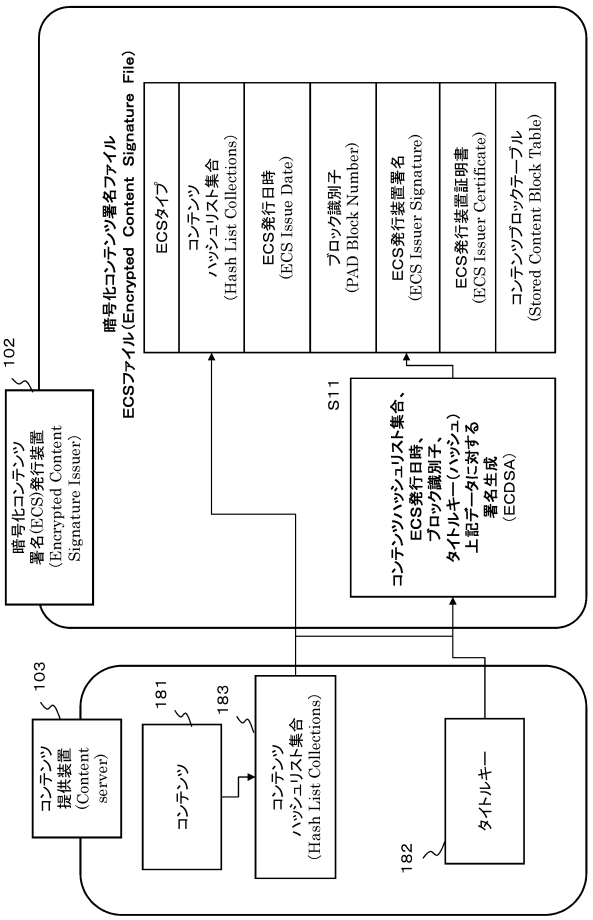
【図１１】



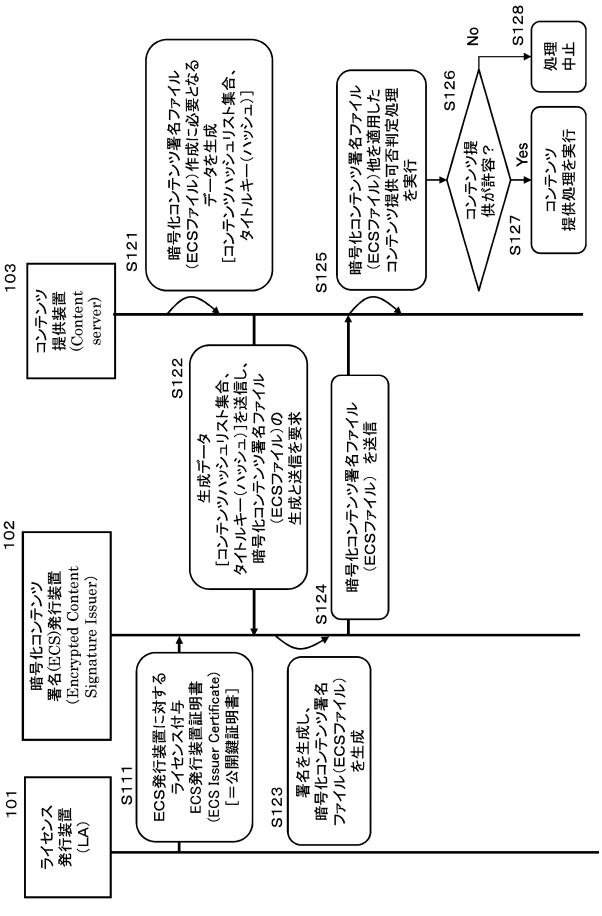
【図１２】



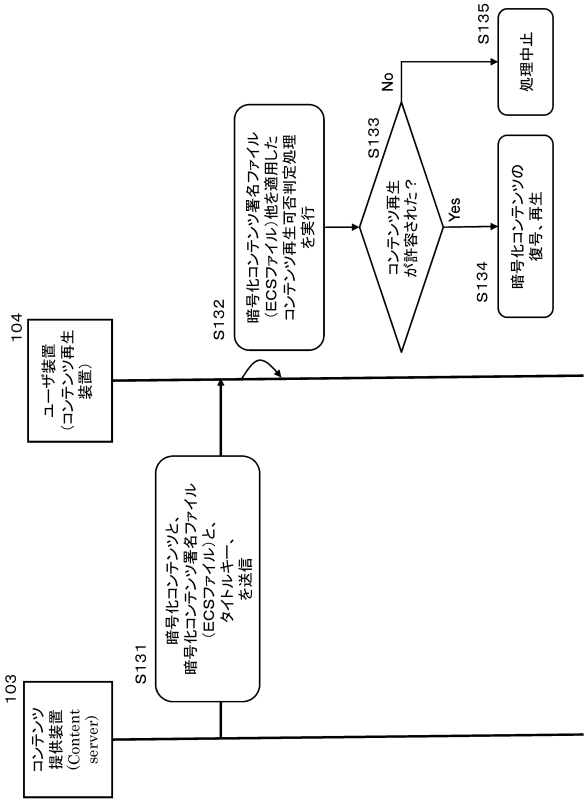
【図１３】



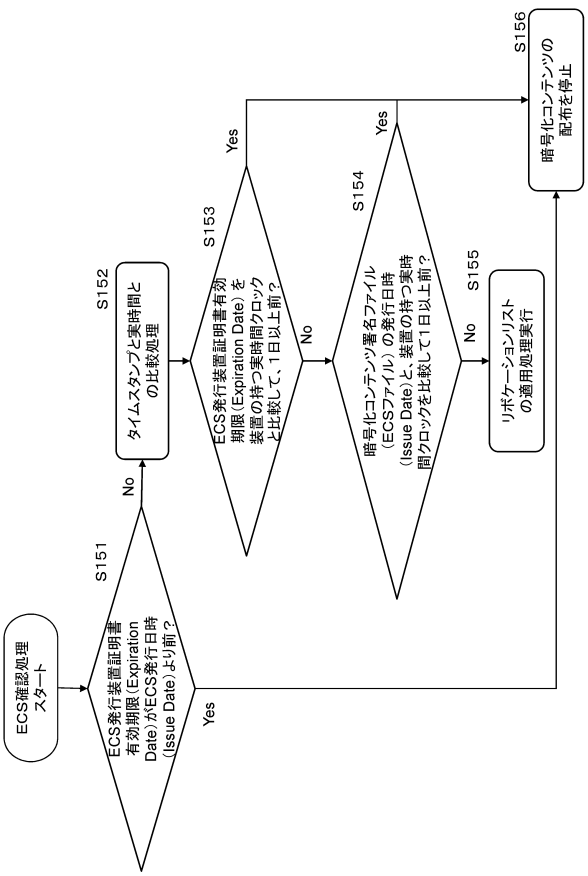
【図１４】



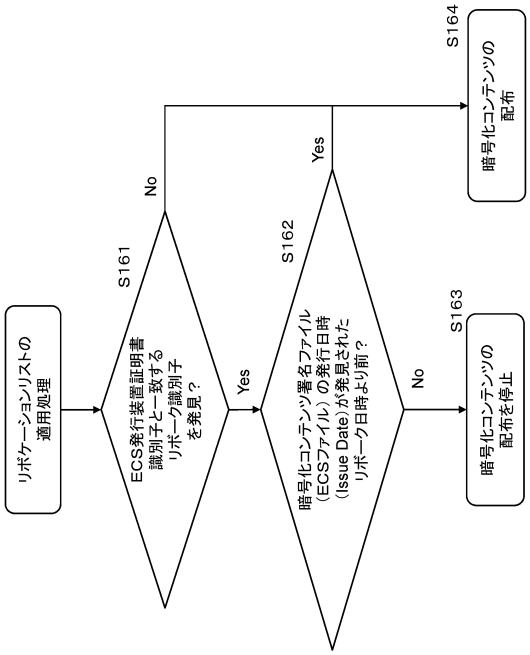
【図１５】



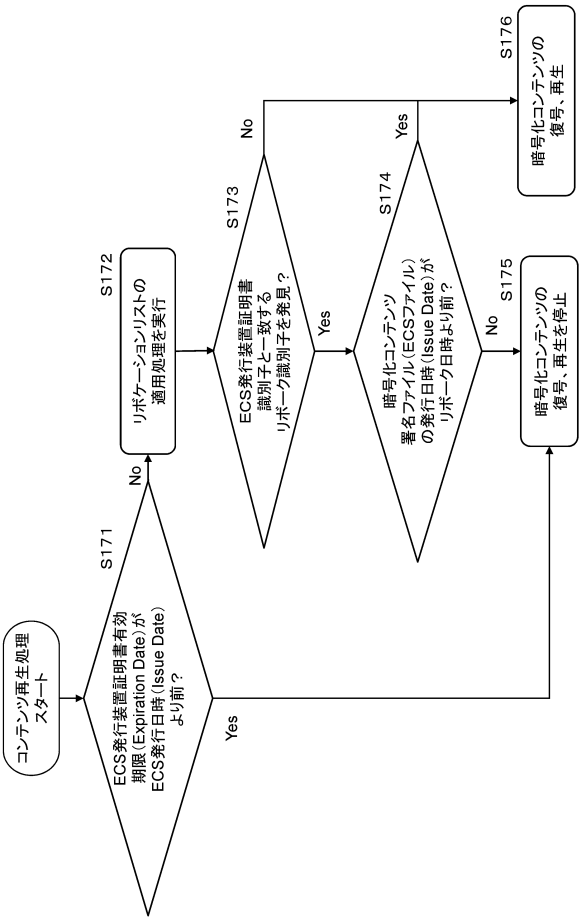
【図１６】



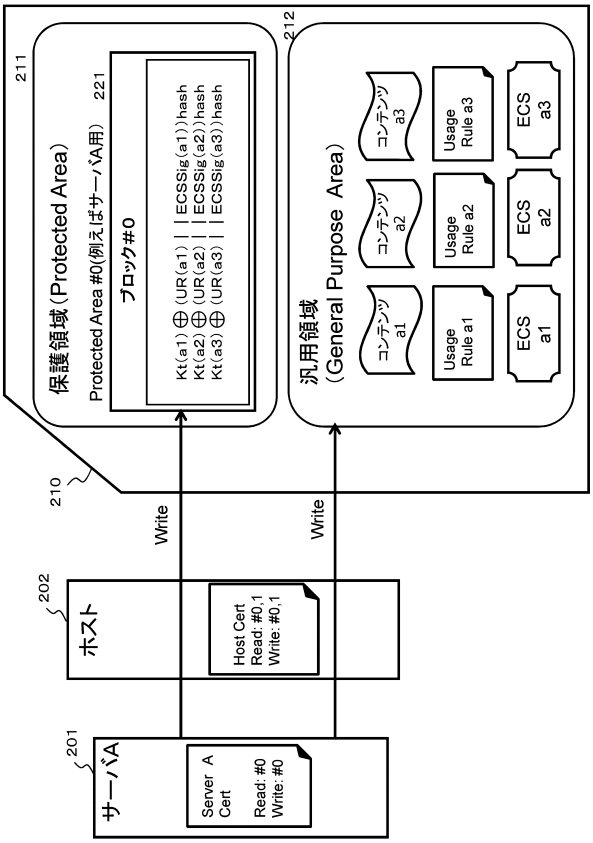
【図１７】



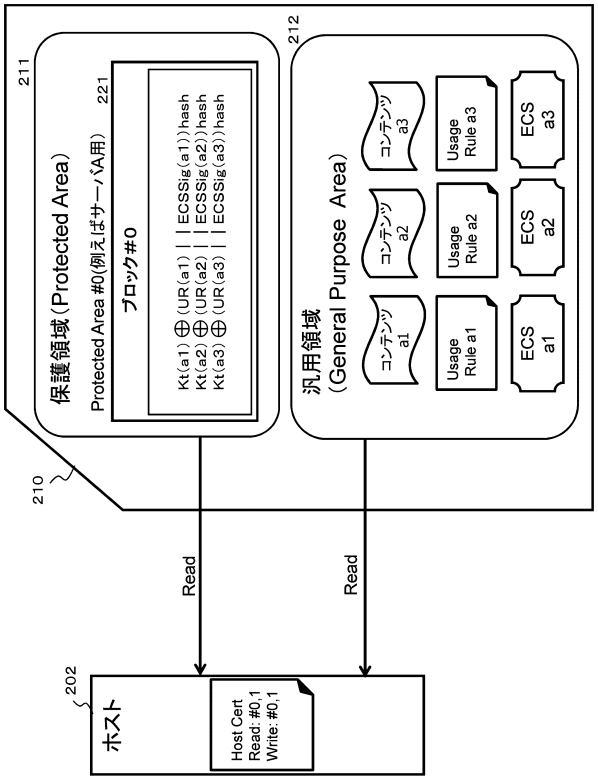
【図１８】



【図１９】



【図２０】



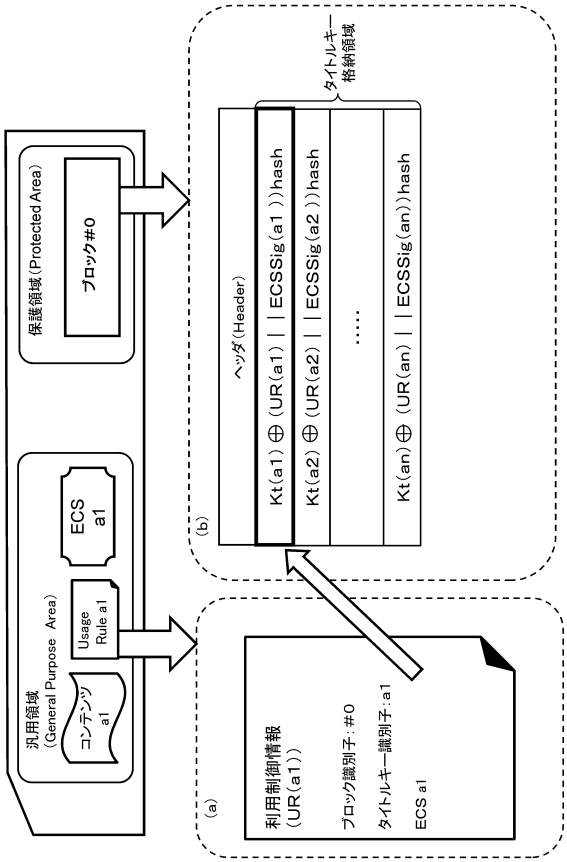
【図２１】

	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)||ECSSig(a1))hash Kt(a2)⊕UR(a2)||ECSSig(a2))hash Kt(a3)⊕UR(a3)||ECSSig(a3))hash	― ― ―	Con(a1), UR(a1), ECS(a1) Con(a2), UR(a2), ECS(a2) Con(a3), UR(a3), ECS(a3)
サーバB	― ― ―	Kt(b1)⊕(UR(b1)||ECSSig(b1))hash Kt(b2)⊕(UR(b2)||ECSSig(b2))hash	Con(b1), UR(b1), ECS(b1) Con(b2), UR(b2), ECS(b2)

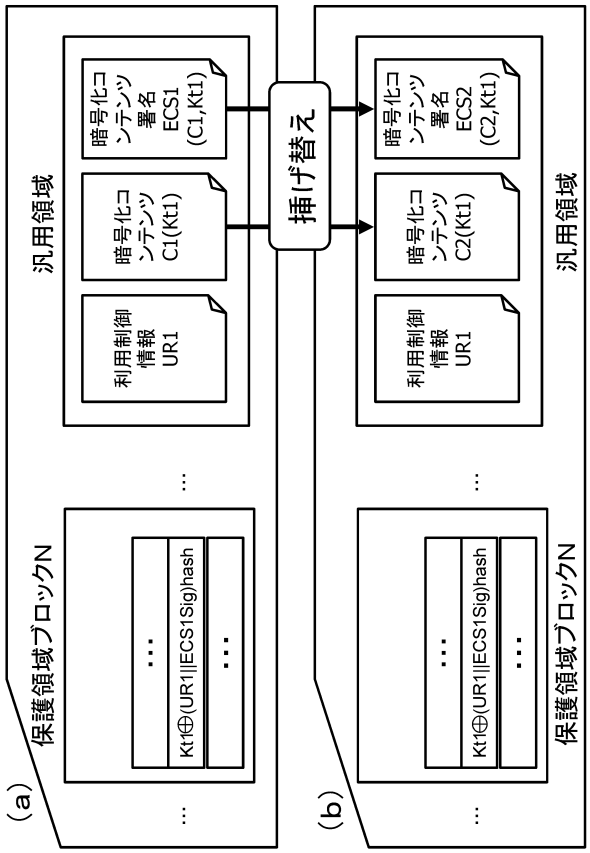
【図２２】

	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)||ECSSig(a1))hash Kt(a2)⊕(UR(a2)||ECSSig(a2))hash Kt(a3)⊕(UR(a3)||ECSSig(a3))hash	― ― ―	Con(a1), UR(a1), ECS(a1) Con(a2), UR(a2), ECS(a2) Con(a3), UR(a3), ECS(a3)
サーバB	Kt(b1)⊕(UR(b1)||ECSSig(b1))hash Kt(b2)⊕(UR(b2)||ECSSig(b2))hash	― ― ―	Con(b1), UR(b1), ECS(b1) Con(b2), UR(b2), ECS(b2)
サーバC	― ― ―	Kt(c1)⊕(UR(c1)||ECSSig(c1))hash	Con(c1), UR(c1), ECS(c1)
サーバD	― ― ―	Kt(d1)⊕(UR(d1)||ECSSig(d1))hash Kt(d2)⊕(UR(d2)||ECSSig(d2))hash	Con(d1), UR(d1), ECS(d1) Con(d2), UR(d2), ECS(d2)

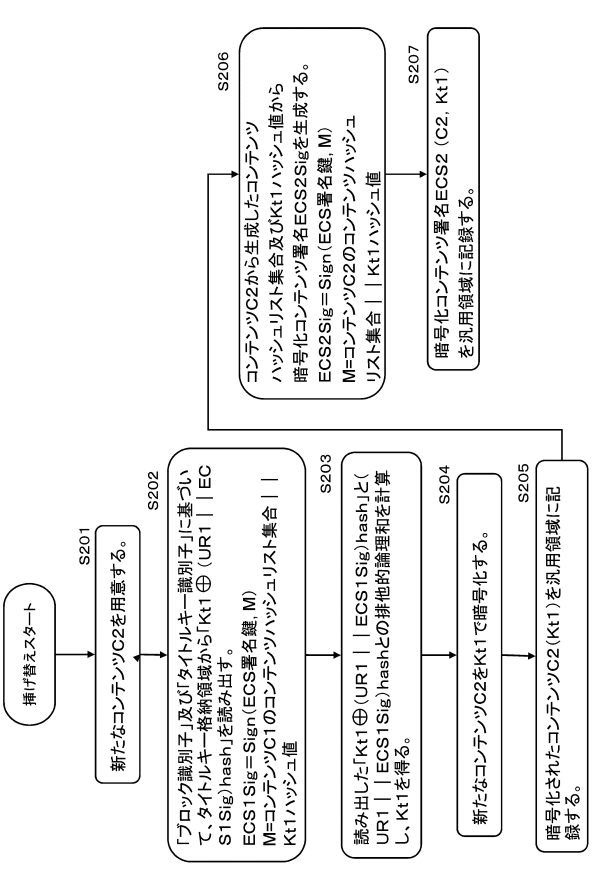
【図２３】



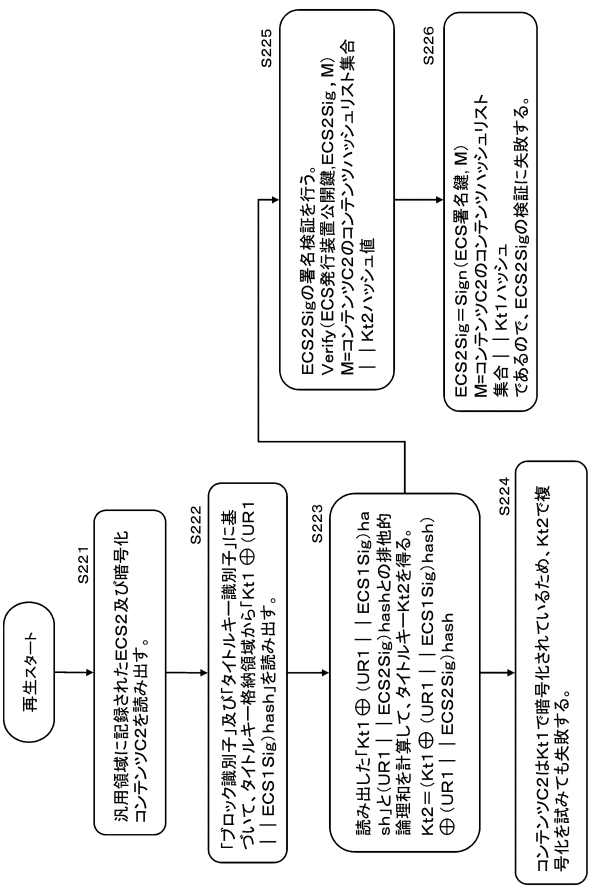
【図２４】



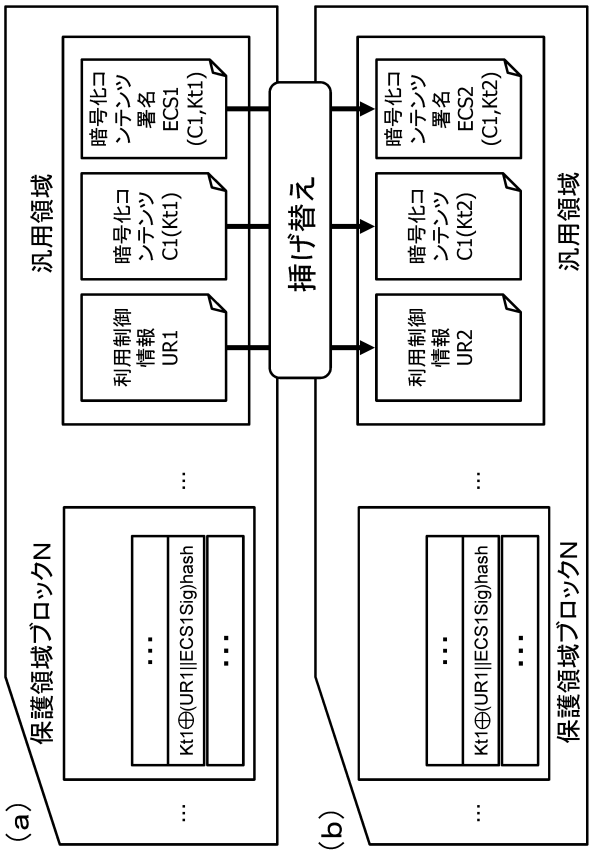
【図２５】



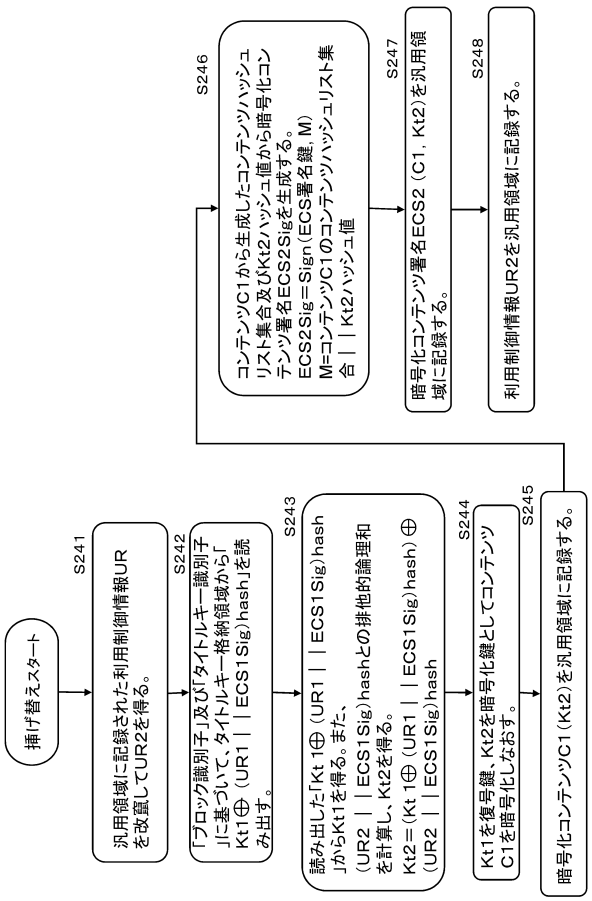
【図２６】



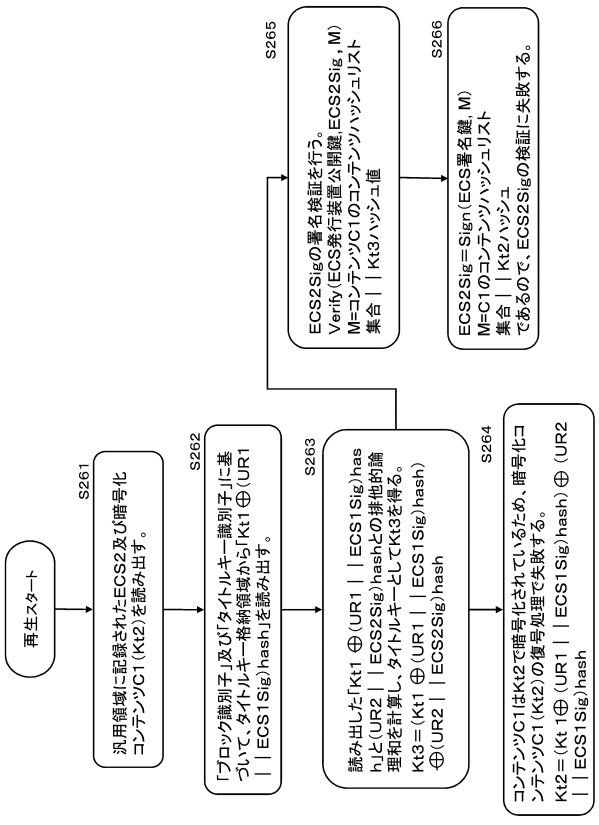
【図２７】



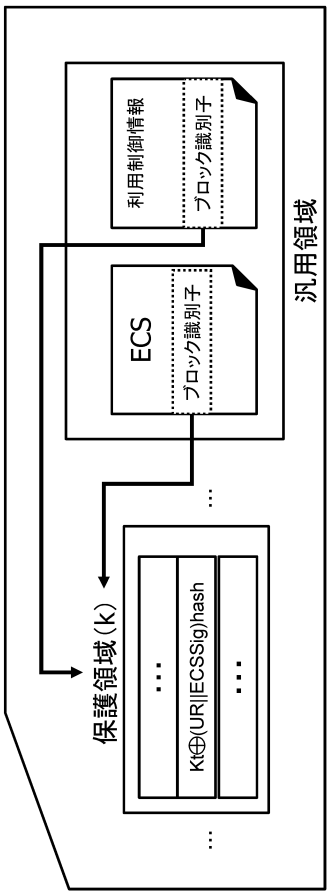
【図２８】



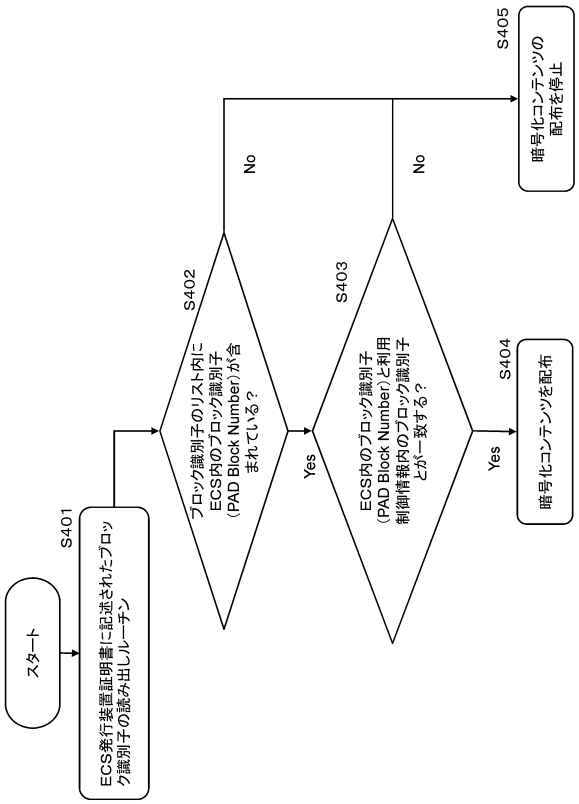
【図２９】



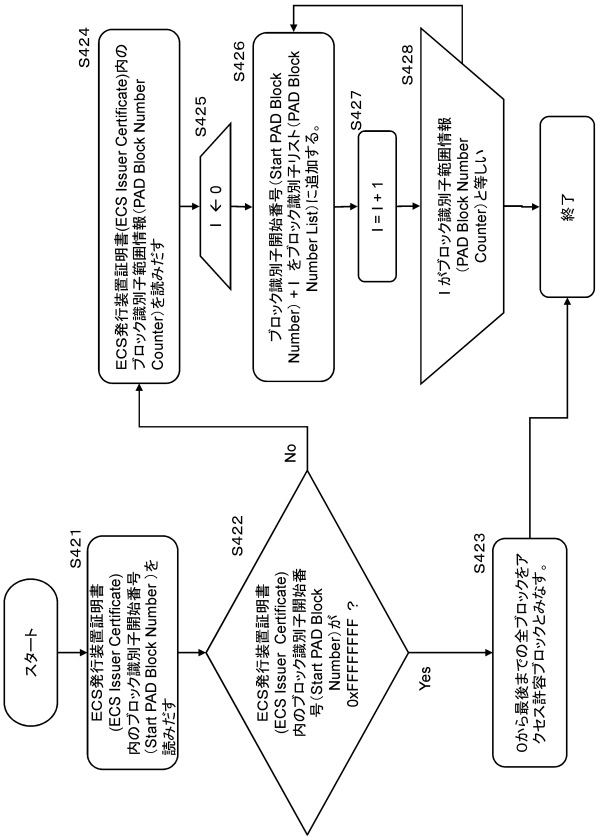
【図３０】



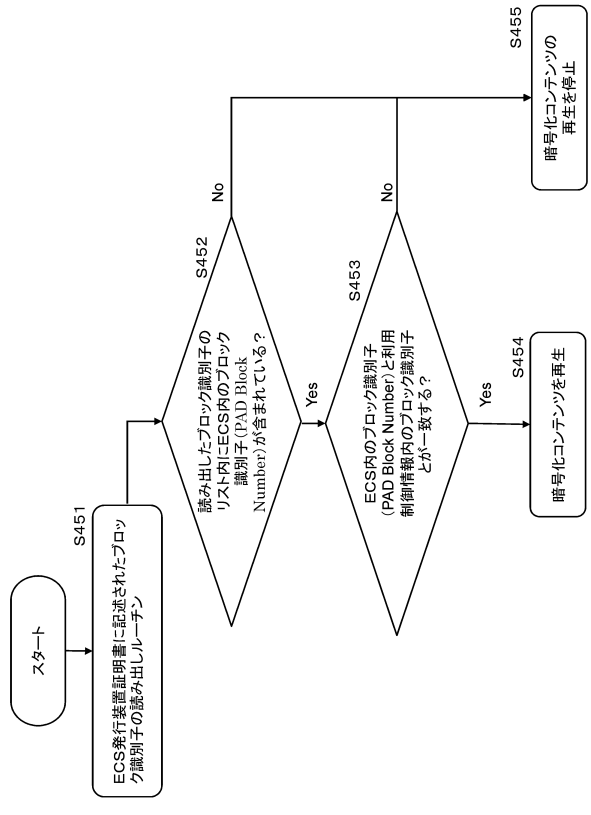
【図３１】



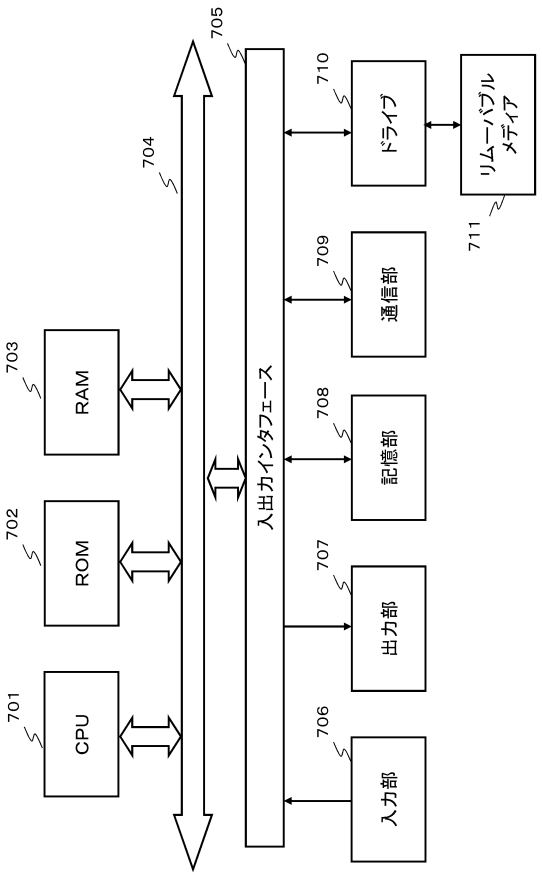
【図３２】



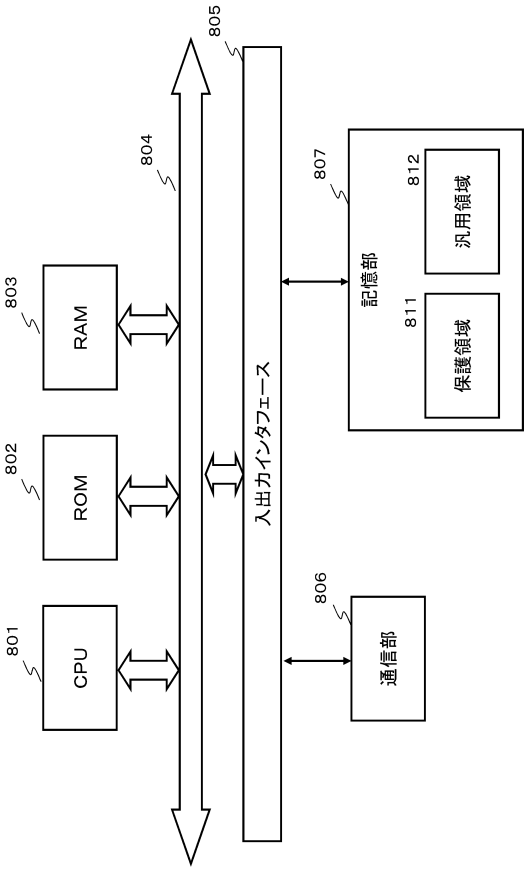
【図３３】



【図３４】



【図３５】


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

フロントページの続き

合議体
審判長　高木　進
審判官　石井　茂和
審判官　須田　勝巳

(56)参考文献　国際公開第２０１３／０３１１２４（WO，Ａ１）
国際公開第２００６／０５７２４８（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L9/00