(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5990569号
(P5990569)
(45)発行日　平成28年9月14日(2016.9.14)　(24)登録日　平成28年8月19日(2016.8.19)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| G06F 21/10 | (2013.01) | G06F | 21/10 | |
| G06F 21/60 | (2013.01) | G06F | 21/60 | 320 |
| G06F 21/44 | (2013.01) | G06F | 21/44 | |

請求項の数 17　(全 27 頁)

| | |
|---|---|
| (21)出願番号 | 特願2014-503592 (P2014-503592) |
| (86)(22)出願日 | 平成24年4月3日 (2012.4.3) |
| (65)公表番号 | 特表2014-510355 (P2014-510355A) |
| (43)公表日 | 平成26年4月24日 (2014.4.24) |
| (86)国際出願番号 | PCT/KR2012/002490 |
| (87)国際公開番号 | WO2012/138098 |
| (87)国際公開日 | 平成24年10月11日 (2012.10.11) |
| 審査請求日 | 平成27年4月3日 (2015.4.3) |
| (31)優先権主張番号 | 10-2011-0030474 |
| (32)優先日 | 平成23年4月4日 (2011.4.4) |
| (33)優先権主張国 | 韓国 (KR) |
| (31)優先権主張番号 | 10-2012-0002122 |
| (32)優先日 | 平成24年1月6日 (2012.1.6) |
| (33)優先権主張国 | 韓国 (KR) |

(73)特許権者　503447036
サムスン　エレクトロニクス　カンパニー　リミテッド
大韓民国・４４３－７４２・キョンギ－ド・スウォン－シ・ヨントン－ク・サムスン－ロ・１２９
(74)代理人　100110364
弁理士　実広　信哉
(72)発明者　ボ－ギョン・カン
大韓民国・キョンギ－ド・４４３－７１４・スウォン－シ・ヨントン－グ・メタン・３－ドン・（番地なし）・イムワン・アパート・＃１－６０７

審査官　平井　誠

最終頁に続く

(54)【発明の名称】コンテンツを保護するための方法、ホスト装置、格納装置、及び機械読み取り可能な格納媒体

(57)【特許請求の範囲】
【請求項１】
格納装置のコンテンツを保護する方法であって、
ホスト装置によって、前記格納装置から前記格納装置の制御部に関する第１の情報を獲得するステップと、
前記ホスト装置によって、前記格納装置から前記格納装置のメモリに関する第２の情報を獲得するステップと、
前記ホスト装置によって、前記第１の情報、前記第２の情報及びアプリケーションに割り当てられた値に基づいて算出された第３の情報を獲得するステップと、
前記ホスト装置によって、前記第３の情報に基づいて前記格納装置に格納されている暗号化されたコンテンツへのアクセスを許容するステップと、を含み、
前記ホスト装置は、前記格納装置から前記暗号化されたコンテンツを受信するように構成されることを特徴とする方法。
【請求項２】
前記暗号化されたコンテンツを暗号化するために使用されたコンテンツ暗号化キーを用いて前記暗号化されたコンテンツを復号するステップを
をさらに有することを特徴とする請求項１に記載の方法。
【請求項３】
前記暗号化されたコンテンツへのアクセスは、前記暗号化されたコンテンツの再生、移動、コピー、読み取り、格納、及び削除のうちの一つであることを特徴とする請求項１に

記載の方法。
【請求項４】
前記コンテンツの暗号化キーはランダムな値であることを特徴とする請求項２に記載の方法。
【請求項５】
前記暗号化されたコンテンツへのアクセスは、前記格納装置のメモリが認証され、前記第３の情報が有効である場合に許容されることを特徴とする請求項１に記載の方法。
【請求項６】
ランダムな値であるコンテンツ暗号化キーを生成するステップと、
前記コンテンツ暗号化キーを用いてコンテンツを暗号化するステップと、
前記暗号化されたコンテンツと前記第３の情報を前記格納装置に格納するステップと、をさらに含むことを特徴とする請求項１に記載の方法。
【請求項７】
請求項１～６のいずれか１項による格納装置のコンテンツ保護方法を実行するためのプログラムを記録する機械読み取り可能な格納媒体。
【請求項８】
格納装置のコンテンツを保護するためのホスト装置であって、
前記格納装置から前記格納装置の制御部に対する第１の情報を獲得し、
前記格納装置から前記格納装置のメモリに対する第２の情報を獲得し、
前記第１の情報、前記第２の情報及びアプリケーションに割り当てられた値に基づいて算出された第３の情報を獲得し、
前記第３の情報に基づいて前記格納装置に格納された暗号化されたコンテンツへのアクセスを許容するように構成された制御部を含み、
前記ホスト装置は、前記格納装置から前記暗号化されたコンテンツを受信するように構成されることを特徴とするホスト装置。
【請求項９】
前記ホスト装置の制御部は、前記暗号化されたコンテンツを暗号化するために使用されたコンテンツ暗号化キーを用いて前記暗号化されたコンテンツを復号するように構成されることを特徴とする請求項８に記載のホスト装置。
【請求項１０】
前記第１の情報及び前記第２の情報のうちの少なくとも一つは暗号化された値であることを特徴とする請求項８に記載のホスト装置。
【請求項１１】
前記第３の情報は、前記第１の情報、前記第２の情報、アプリケーションに割り当てられた値及び前記暗号化されたコンテンツを暗号化するために使用されたコンテンツ暗号化キーに基づいて算出されることを特徴とする請求項８に記載のホスト装置。
【請求項１２】
前記暗号化されたコンテンツへのアクセスは、前記暗号化されたコンテンツの再生、移動、コピー、読み取り、格納及び削除のうちの一つであることを特徴とする請求項８に記載のホスト装置。
【請求項１３】
前記暗号化されたコンテンツへのアクセスは、前記格納装置のメモリが認証され、前記第３の情報が有効である場合に許容されることを特徴とする請求項８に記載のホスト装置。
【請求項１４】
コンテンツを保護するための格納装置であって、
第１の情報を含み、前記第１の情報をホスト装置に提供するように構成された制御部と、
第２の情報を含み、前記第２の情報を前記ホスト装置に提供し、暗号化されたコンテンツを格納するように構成されたメモリと、を含み、

前記格納装置は、前記暗号化されたコンテンツ及び第３の情報を前記ホスト装置に提供するように構成され、

前記第３の情報は、前記第１の情報、前記第２の情報及びアプリケーションに割り当てられた値に基づいて算出されることを特徴とする格納装置。

【請求項１５】

前記暗号化されたコンテンツを暗号化するために使用されたコンテンツ暗号化キーはランダムな値であることを特徴とする請求項１４に記載の格納装置。

【請求項１６】

前記第３の情報は、前記第１の情報、前記第２の情報、アプリケーションに割り当てられた値及び前記暗号化されたコンテンツを暗号化するために使用されたコンテンツ暗号化キーに基づいて算出されることを特徴とする請求項１４に記載の格納装置。

【請求項１７】

前記コンテンツ暗号化キーはランダムな値であることを特徴とする請求項１６に記載の格納装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はコンテンツを保護するための方法及び装置に関するもので、特に複数のモジュールを具備する格納装置内に格納されたコンテンツを保護するための方法及び装置に関する。

【背景技術】

【０００２】

コンテンツ保護のためにデジタル著作権管理(Digital Rights Management：ＤＲＭ)、コピー防止(copy protection)などの技術が要求されるように、このようなコンテンツを格納するＳＳＤ(Solid State Disk)、フラッシュメモリカードのような非揮発性メモリ(Non-Volatile Memory：ＮＶＭ)装置などを含む格納装置を認証するための技術が要求されている。すなわち、コンテンツの暗号化技術はもちろん、格納装置のハードウェア(H/W)側面の適合性を検証する技術が要求されている。

【０００３】

ＤＲＭ技術、ＳＤ(Secure Digital)カードのためのＣＰＲＭ(Content Protection for Recordable Media)技術、及びブルーレイ(Blue-ray)ディスクのためのＡＡＣＳ(Advanced Access Content System)技術では、公開キー基盤(Public Key Infrastructure：ＰＫＩ)又は他の暗号技術(cryptographic technology)を使用する装置認証方法が提供されるが、これらは、格納装置自体のコピーに対する解決策を提供することではない。

【０００４】

ＤＲＭ技術、ＣＰＲＭ及びＡＡＣＳ規格は、固有なメディア識別子(Media ID)とこれに対応する暗号技術(例えば、ＰＫＩ認証)を用いて格納されているコンテンツとこれに結合(binding)されるか、あるいは結合された機器を認証する方法を提供する。また、固有の識別子にコンテンツ自体またはコンテンツを暗号化するのに使われる暗号化キーなどを対応させることによって、格納装置の貯蔵領域にアクセスすること、すなわちデータの違法コピーのための不適切な作動(読み取り、書き込みなど)を行うことを防止する技術を提供する。

【０００５】

従来技術は格納装置の構造に関係なく固有なメディア識別子が対応するので、格納装置を構成している多様なチップ(制御部、及びＰＲＡＭ(Programmable Random Access Memory)、ＤＲＡＭ(Dynamic Random Access Memory)、フラッシュ、ＨＤＤ(Hard Disk Drive)のようなメモリなど)のうち一部が不適切に使用(又は代替)される場合、違法認証が発生するという問題点を有する。

【発明の概要】

【発明が解決しようとする課題】

【０００６】
したがって、本発明は上記した従来技術に鑑みてなされたものであって、その目的は、格納装置の任意のモジュールの不適切な作動により発生するセキュリティ攻撃(security attack)に対して防御する方法及び装置を提供することにある。
【課題を解決するための手段】
【０００７】
上記のような目的を達成するために、本発明の一態様によれば、格納装置のコンテンツを保護する方法が提供される。第１のモジュールに関する第１の認証情報が獲得される。この第１のモジュールは、格納装置内に含まれる複数のモジュールのうちいずれか一つである。第１のモジュールは、第１の固有個体情報(Unique Individual Information：ＵＩＩ)及び第１の認証情報に基づいて認証される。第２のモジュールに関する第２の認証情報が獲得される。この第２のモジュールは、格納装置に含まれている複数のモジュールのうち他の一つである。第２のモジュールは、その第２のＵＩＩ及び第２の認証情報に基づいて認証される。格納装置に格納されているコンテンツへのアクセスは、少なくとも第１及び第２のモジュールが成功的に認証される場合に許容される。
【０００８】
本発明の別の態様によれば、機械読み取り可能な格納媒体は、格納装置のコンテンツを保護する方法を実行するためのプログラムが記録される。その方法は、格納装置内に具備された複数のモジュールのうち第１のモジュールに関する第１の認証情報を獲得するステップと、第１のモジュールの第１の固有個体情報(ＵＩＩ)及び第１の認証情報に基づいて第１のモジュールを認証するステップと、格納装置に具備された複数のモジュールのうち第２のモジュールに関する第２の認証情報を獲得するステップと、第２のモジュールの第２のＵＩＩ及び第２の認証情報に基づいて第２のモジュールを認証するステップと、少なくとも第１及び第２のモジュールが成功的に認証される場合、格納装置に格納されているコンテンツにアクセスを許容するステップとを有する。
【０００９】
本発明のもう一つの態様によれば、格納装置のコンテンツを保護するためのホスト装置が提供される。ホスト装置は、第１のモジュールに関する第１の認証情報を獲得し、第１のモジュールに関する第１の固有個体情報(ＵＩＩ)及び第１の認証情報に基づいて第１のモジュールを認証する第１のモジュール認証部を含む。第１のモジュールは、格納装置に含まれた複数のモジュールのうちいずれか一つである。また、ホスト装置は、第２のモジュールに関する第２の認証情報を獲得し、第２のモジュールに関する第２のＵＩＩ及び第２の認証情報に基づいて第２のモジュールを認証する第２のモジュール認証部を含む。第２のモジュールは、格納装置に含まれた複数のモジュールのうち他の一つである。さらに、ホスト装置は、予め設定された認証ポリシーを格納するメモリと、認証ポリシーに従って第１及び第２のモジュール認証部を制御し、少なくとも第１及び第２のモジュールが成功的に認証された場合に格納装置に格納されているコンテンツのアクセスを許容する認証コーディネータとを含む。
【００１０】
本発明のもう一つの態様によれば、格納装置は、コンテンツを保護するために提供される。格納装置は、第１の固有個体情報(ＵＩＩ)及び第１の認証情報を有する第１のモジュールを含む。第１のモジュールは、ホスト装置の要請によって第１のＵＩＩ及び第１の認証情報を提供する。また、格納装置は、第２のＵＩＩ及び第２の認証情報を有する第２のモジュールを含む。第２のモジュールは、ホスト装置の要請によって第２のＵＩＩ及び第１の認証情報を提供し、暗号化されたコンテンツを格納する。暗号化されたコンテンツは、第１及び第２のＵＩＩ、第１及び第２の認証情報に関連したコンテンツ暗号化キーを用いて暗号化される。
【発明の効果】
【００１１】
本発明は、相互に異なる機能を有する多様なモジュール(デバイス-メモリ、制御部など

)が格納装置(ＳＤ(Secure Digital)カード、ＨＤＤ(Hard Disk Drive)、ＵＳＢ(Universal Serial Bus)など)に使用される場合、ＵＩＩ及び認証情報は各モジュールに発行される。ホスト装置は、各モジュールに対して独立認証を遂行して認証結果を最終的に判断することによって、格納装置を安全に認証できる効果がある。特に、いろいろなＵＩＩを統合して使用することによって、一つのモジュールの不適切な機能により発生する攻撃を防止することができる効果がある。

【００１２】

本発明の上記及び他の態様、特徴、及び利点は、添付の図面と共に述べる以下の詳細な説明から、一層明らかになるはずである。

【図面の簡単な説明】

【００１３】

【図１】本発明の一実施形態による安全(又はセキュリティ)格納装置の初期構成を示すブロック構成図である。

【図２】本発明の一実施形態による認証情報を格納する方法を示す図である。

【図３】本発明の一実施形態による認証情報を格納する方法を示す図である。

【図４】本発明の一実施形態による格納装置の認証方法を示す図である。

【図５】本発明の一実施形態により、図４に示す認証方法に関連したホスト装置を示す図である。

【図６】本発明の一実施形態による格納装置の認証方法を示すフローチャートである。

【図７】本発明の一実施形態により、暗号化されたコンテンツの格納/記録方法を示す図である。

【図８】本発明の一実施形態により、暗号化/復号化装置の主要構成を示す図である。

【図９】本発明の一実施形態により、暗号化されたコンテンツの格納/記録方法を示す図である。

【図１０】本発明の一実施形態により、暗号化されたコンテンツの格納/記録方法を示すフローチャートである。

【図１１】本発明の一実施形態により、図１０に関連したホスト装置の主要構成を示す図である。

【図１２】本発明の一実施形態により、暗号化されたコンテンツの再生方法を示すフローチャートである。

【図１３】本発明の一実施形態により、暗号化されたコンテンツの再生方法を示す図である。

【図１４】本発明の一実施形態により、図１２に関連したホスト装置の主要構成を示す図である。

【図１５】本発明の一実施形態により、追加認証情報生成装置を示すブロック構成図である。

【図１６】本発明の一実施形態により、暗号化されたコンテンツの格納/記録方法を示す図である。

【図１７】本発明の一実施形態により、追加認証情報生成装置を示すブロック構成図である。

【図１８】本発明の一実施形態により、暗号化されたコンテンツの格納/記録方法を示すフローチャートである。

【図１９】本発明の一実施形態により、図１８に関連したホスト装置の主要構成を示す図である。

【図２０】本発明の一実施形態により、暗号化されたコンテンツの再生方法を示すフローチャートである。

【図２１】本発明の一実施形態により、図２０の再生方法を示す図である。

【図２２】本発明の一実施形態により、図２０の再生方法に関連したホスト装置の主要構成を示すブロック構成図である。

【図２３】本発明の一実施形態により、暗号化キー抽出装置を示すブロック構成図である

。
【発明を実施するための形態】
【００１４】
以下、本発明の望ましい実施形態を添付の図面を参照して詳細に説明する。
【００１５】
図面において、同一の構成要素に対してはできるだけ同一の参照符号及び参照番号を付して説明する。下記の説明で、本発明に関連した公知の機能又は構成に関する具体的な説明が本発明の要旨を不明にすると判断された場合に、その詳細な説明を省略する。
【００１６】
図１は、本発明の一実施形態による安全(又はセキュリティ)格納装置の初期構成を示すブロック構成図である。
【００１７】
安全格納装置(secure storage)１００は、制御部１１０及び非揮発性メモリ(Non-Volatile Memory：ＮＶＭ)１２０を含む。この格納装置１００は、固有なメディア識別子(Media Identifier(ＩＤ)を有する。本発明において、格納装置１００は、格納メディア(又は媒体)の具体的な一例として提示されるが、同一の意味で使用され得る。
【００１８】
制御部１１０は、格納装置１００のモジュールＡ(又は第１のモジュール)に該当し、第１の固有個体情報(Unique Individual Information：ＵＩＩ)を有する。非揮発性メモリ１２０は、格納装置１００のモジュールＢ(又は第２のモジュール)に該当し、第２のＵＩＩを有する。ＵＩＩは、ハードウェア(H/W)又はモジュールを識別するための固有識別子(ＩＤ)に該当する。制御部１１０は、ＣＰＵ(Central Processing Unit)、揮発性メモリで構成され、ホストインターフェース(Ｉ/Ｆ)を介してホスト装置と通信する(例えば、データ処理命令を受信)。非揮発性メモリ１２０は、ＮＶＭインターフェースを介して制御部１１０と通信し、第２のホストインターフェース、又は制御部１１０及びホストインターフェースを介してホスト装置２００と通信することができる。
【００１９】
ホスト装置２００は、例えば個人用コンピュータ(ＰＣ)、移動電話、カメラのように、格納装置１００、及びデジタルＴＶ(ＤＴＶ)のように格納装置１００のためのインターフェース(Ｉ/Ｆ)を使用する装置である。ホスト装置２００は、制御部、ディスプレイ部、入力装置、メモリ、有線/無線通信部などを含む端末であり得る。また、ホスト装置２００は、格納装置１００に格納されているコンテンツを再生するプレーヤー(player)、あるいは格納装置１００に新たなコンテンツを格納する記録(recording)装置であり得る。より詳細には、ホスト装置２００と格納装置１００との間の通信は、例えばＳＤ(Secure Digital)/ＭＭＣ(Multi Media Card)システムのようなメモリカードシステム関連のプロトコル、及びＡＴＡ(Advanced Technology Attachment)/Ｓ-ＡＴＡ(Serial-ATA)などのハードディスクのような格納装置に関連したプロトコルのように、そのアプリケーションに従って変化する。
【００２０】
格納装置１００は、暗号化(encryption)/復号化(decryption)のためのソフトウェア又はハードウェアのようなセキュリティエンジンをさらに含むことができる。制御部１１０は、ホスト装置２００のファイルシステムへのアクセスを適切に制御することで、非揮発性メモリ１２０のメモリセルにデータを格納するＦＴＬ(Flash Translation Layer)を含むことができる。格納装置１００は、内蔵装置としてスマートフォン、タブレットＰＣなどに搭載され、外部装置に装着又は付着することができる。
【００２１】
以後、格納装置１００の各モジュール１１０とＮＶＭ１２０は、各々認証情報をさらに格納する。
【００２２】
図２は、本発明の一実施形態による認証情報を格納する方法を示す。格納方法は、モジ

ュールＡ　１１０ａのモジュールＡメーカー(manufacturer)１０でなく、格納装置１００ａの製造社(fabricator)３０が格納装置１００ａに提供される一実施形態に基づいて説明される。各々ＵＩＩが割り当てられるモジュールＡ　１１０ａとモジュールＢ　１２０ａとの間のモジュールＡ　１１０ａの認証情報が格納される。

【００２３】

モジュールＡメーカー１０は、第１～第ｎのモジュールを製造し、各モジュールにＵＩＩを割り当て及び格納する。その後、モジュールＡメーカー１０は、ステップＳ１１０で、第１～第ｎのモジュールＡに割り当て及び格納された第(Ａ-１)～第(Ａ-ｎ)のＵＩＩをモジュール認証センター２０に報告する。

【００２４】

モジュール認証センター２０は、第(Ａ-１)～第(Ａ-ｎ)のＵＩＩをデータベースに登録し、第(Ａ-１)～第(Ａ-ｎ)のＵＩＩに対応する第(Ａ-１)～第(Ａ-ｎ)の認証情報を生成する。

【００２５】

モジュール認証センター２０は、ステップＳ１２０で、第(Ａ-１)～第(Ａ-ｎ)のＵＩＩを含むＵＩＩリストを発行(生成)し、ＵＩＩリストをモジュールＡメーカー１０に伝送する。モジュール認証センター２０は、第(Ａ-１)～第(Ａ-ｎ)認証情報をＵＩＩリストとともに伝送することができる。ＵＩＩリストは、対応する認証情報の獲得に使われることができる。

【００２６】

モジュールＡメーカー１０は、ステップＳ１３０で、ＵＩＩリストを格納装置の製造社３０に伝送する。

【００２７】

格納装置製造社３０は、ステップＳ１４０で、モジュール認証センター２０にＵＩＩリストを提出し、このＵＩＩリストに応答して、ステップＳ１５０で、ＵＩＩリストに対応する認証情報リスト、すなわち第(Ａ-１)～第(Ａ-ｎ)の認証情報を受信及び確保する。

【００２８】

格納装置製造社３０は、ステップＳ１６０で、格納装置１００ａまたはモジュールＡ　１１０ａからＵＩＩを要請し、ステップＳ１７０で、格納装置１００ａ又はモジュールＡ　１１０ａから該当ＵＩＩ(ＵＩＩａ)を受信する。

【００２９】

格納装置製造社３０は、ステップＳ１８０で、モジュールＡ　１１０ａのＵＩＩに対応する認証情報を選択又は決定し、決定された認証情報をモジュールＡ　１１０ａに挿入及び格納する。例えば、格納装置製造社３０は、認証情報リストで受信したＵＩＩ(例えば、第(Ａ-１)のＵＩＩ)に対応する第(Ａ-１)の認証情報を検索し、検索したモジュールＡ　１１０ａ(例えば、第１のモジュールＡ)に格納することができる。

【００３０】

本発明の実施形態において、モジュールＡメーカー１０、格納装置製造社３０、又はモジュール認証センター２０は、制御部、ディスプレイ部、入力装置、メモリ、有線/無線通信部などを含むコンピュータであり得る。コンピュータ間の通信は、有線又は無線で遂行できる。

【００３１】

図３は、本発明の実施形態による認証情報を格納する方法を示す。格納方法は、ＵＩＩが割り当てられたモジュールＡ　１１０ｂを有する格納装置１００ｂに含まれるモジュールＢ　１２０ｂの認証情報をモジュールＢメーカー１０ａが格納する一実施形態に基づく。図３は、容易な理解のために、モジュールＢ　１２０ｂが格納装置１００ｂに具備されるが、格納方法は、格納装置１００ｂにモジュールＢ　１２０ｂが提供される前に遂行される。しかしながら、格納方法は、モジュールＢ　１２０ｂが格納装置１００ｂに提供されている状態でオンライン通信を通じて実行可能である。

【００３２】

Ｂモジュール認証センター２０ａは、ステップＳ２１０で、モジュールＢメーカー１０ａにＵＩＩリスト及び認証情報リストを伝送し、あるいはモジュールＢメーカー１０ａにＵＩＩ及び関連した認証情報を生成できるツール(tool)(Ｓ/Ｗ又はＨ/Ｗ)を提供する。

【００３３】

モジュールＢメーカー１０ａは、ステップＳ２２０で、生産されたモジュールＢ　１２０ｂにＵＩＩｂ及び関連した認証情報を挿入及び格納する。例えば、モジュールＢメーカー１０ａは、生産したモジュールＢ(例えば、第２のモジュールＢ)に第(Ｂ-２)のＵＩＩ及び第(Ｂ-２)の認証情報を割り当て及び格納することができる。

【００３４】

本発明の実施形態において、ＵＩＩは、ランダム値又は暗号化された誤り訂正可能な情報であり得る。対称キー、非対称キーのような多様な暗号化方式がＵＩＩと関連した認証情報に適用され得る。例えば、よく知られているＰＫＩ(Public Key Infrastructure)が適用された認証書は、認証情報として使用することができる。認証情報として使われるＰＫＩを使用する認証書“証明書(Certificate)(認証情報)”は、次のように表示される。

【００３５】

証明書(認証情報)＝署名(認証センターの秘密キー、ＵＩＩ、データ)

【００３６】

特に、認証書“証明書(認証情報）”は、認証センターの電子署名値“署名(Signature)”を含み、この電子署名値は、ＵＩＩ及び/又はデータを認証センターの秘密キー“Private Key of Authorization Center”で署名した値を示す。データは、証明書の有効期間、証明書の使用対象のように、他の証明書関連情報を意味する。

【００３７】

図４は、本発明の一実施形態による格納装置の認証方法を示す。図５は、本発明の一実施形態により、認証方法と関連したホスト装置の主要構成を示す。

【００３８】

ホスト装置２００は、Ａモジュール認証部２１０、Ｂモジュール認証部２２０、Ｃモジュール認証部２３０、認証コーディネータ２４０、及び認証に対するポリシーを格納するメモリ２５０を含み、これらは、ホスト装置２００の認証部２０５を形成する。Ａモジュール認証部２１０、Ｂモジュール認証部２２０、及びＣモジュール認証部２３０は、各々第１～第３のモジュール認証部として称される。

【００３９】

Ａモジュール認証部２１０は、ステップＳ３１０で、格納装置１００ｃに集積された複数のモジュールのうちモジュールＡ　１１０ｃに関する第１の認証情報を要請する。Ａモジュール認証部２１０は、ステップＳ３２０で、モジュールＡ　１１０ｃに関する第１の認証情報を受信及び獲得する。Ａモジュール認証部２１０は、モジュールＡ　１１０ｃの第１のＵＩＩ(ＵＩＩａ)、及び第１の認証情報に基づいてモジュールＡ　１１０ｃを認証する。この手順は、認証プロトコルと称される。各モジュール認証部２１０，２２０，２３０は、該当モジュール１１０ｃ，１２０ｃ，１３０ｃのＵＩＩを既に知っており、これらは、格納装置１００ｃから受信することができる。特定モジュールの認証情報は、格納装置１００ｃの制御部(本例ではモジュールＡ　１１０ｃ)を通じて、あるいは特定モジュールから直接に受信することができる。例えば、各モジュール認証部２１０，２２０，２３０は、該当認証情報を構成する電子署名値に既知のモジュールメーカーの公開キーを適用して該当モジュールのＵＩＩを復号化する。各モジュール認証部２１０，２２０，２３０は、既に知られているモジュールのＵＩＩと復号化されたＵＩＩを比較し、それによってモジュールに対する認証を遂行する。

【００４０】

Ｂモジュール認証部２２０は、ステップＳ３３０で、複数のモジュールのうちモジュールＢ　１２０ｃに対する第２の認証情報を要請する。Ｂモジュール認証部２２０は、ステップ３４０で、モジュールＢ　１２０ｃに関する第２の認証情報を受信及び獲得する。Ｂモジュール認証部２２０は、モジュールＢ　１２０ｃの第２のＵＩＩ(ＵＩＩｂ)、及び第

２の認証情報に基づいてモジュールＢ　１２０ｃを認証する。
【００４１】
Ｃモジュール認証部２３０は、ステップＳ３５０で、複数のモジュールのうちモジュールＣ　１３０ｃに対する第３の認証情報を要請する。Ｃモジュール認証部２３０は、ステップ３６０で、モジュールＣ　１３０ｃに関する第３の認証情報を受信及び獲得する。Ｃモジュール認証部２３０は、モジュールＣ　１３０ｃの第３のＵＩＩ(ＵＩＩｃ)、及び第３の認証情報に基づいてモジュールＣ　１３０ｃを認証する。
【００４２】
各モジュール認証部２１０，２２０，２３０は、該当認証情報に適用された暗号化方式による認証方法で該当モジュールを認証する。モジュールＣ　１３０ｃは、第３のＵＩＩ以外に別の認証情報を有しないので、第３の認証情報は、第３のＵＩＩであり、この第３のＵＩＩは認証に必要な情報を有することができる。
【００４３】
各認証情報は、該当モジュールに格納されていることを説明したが、他のモジュールに格納され得る。例えば、第１及び第２の認証情報は、第３のモジュール１３０ｃに格納することができる。
【００４４】
本実施形態では、各モジュールに対する認証ステップが順次に遂行されるが、これら認証ステップは、並列的に、または同時に遂行できる。
【００４５】
メモリ２５０は、予め設定された認証ポリシーを格納する。認証ポリシーは、格納装置１００ｃに含まれたモジュール１１０ｃ，１２０ｃ，１３０ｃの中からどのモジュールに対して、どの順序及び方法で認証を遂行するかに対する規則を定義する。
【００４６】
認証コーディネータ２４０は、認証ポリシーによって格納装置１００ｃに対する認証を遂行するようにモジュール認証部２１０，２２０，２３０を制御する。認証コーディネータ２４０は、格納装置１００ｃに含まれている複数のモジュール１１０ｃ，１２０ｃ，１３０ｃに対する優先順位リストに基づいて、第１及び第２順位のモジュール１１０ｃ，１２０ｃに対する認証プロトコルを順次に遂行し、第１及び第２順位のモジュール１１０ｃ，１２０ｃが両方とも成功的に認証される場合、格納装置１００ｃに格納されたコンテンツへのアクセスを許容する。
【００４７】
認証ポリシーに関する他の実施形態において、認証コーディネータ２４０は、格納装置１００ｃに含まれた３個のモジュール１１０ｃ，１２０ｃ，１３０ｃのうち、特定モジュール、例えばモジュールＢ　１２０ｃに対する認証が失敗した場合、格納装置１００ｃに対する認証が最終的に失敗し、あるいは特定機能に限定されて認証が成功したとみなされることができる。特定機能は、例えば読み取り機能であり、このような場合に、ホスト装置２００は、格納装置１００ｃに対して、読み取り動作のみを許容し、書き込み動作は許容しない。
【００４８】
図６は、本発明の一実施形態による格納装置の認証方法を示すフローチャートである。認証方法と関連した装置構成は、図４及び図５を参照する。
【００４９】
ホスト装置２００は、ステップＳ４１０で、格納装置１００ｃに対する認証要請を受信する。例えば、この認証要請の受信ステップは、ユーザーによるコンテンツビュー、コンテンツ再生などのコンテンツ関連命令をホスト装置２００に具備された入力装置(例えば、キーボード、キーパッド、キーボタン、マウス、タッチスクリーンなど)を通じて受信するステップに対応することができる。
【００５０】
認証コーディネータ２４０は、ステップＳ４１５で、格納装置１００ｃの認証のための

アルゴリズムを開始する。すなわち、認証コーディネータ２４０は、メモリ２５０に格納された認証ポリシーを読み取り、認証ポリシーに対応するアルゴリズムにより動作する。

【００５１】

認証コーディネータ２４０は、ステップＳ４２０で、後述する手順に従ってＡモジュール認証部２１０及びＢモジュール認証部２２０を順次に制御する。

【００５２】

Ａモジュール認証部２１０は、ステップＳ４２５で、認証ポリシーに定義された認証プロトコルを遂行することによってモジュールＡ　１１０ｃを認証する。Ａモジュール認証部２１０は、格納装置１００ｃに集積された複数のモジュールのうちモジュールＡ　１１０ｃに対する第１の認証情報を要請し、モジュールＡ　１１０ｃに関する第１の認証情報を受信及び獲得する。Ａモジュール認証部２１０は、モジュールＡ　１１０ｃの第１のＵＩＩ及び第１の認証情報に基づいて、モジュールＡ　１１０ｃを認証する。

【００５３】

ステップＳ４３０で、認証が成功したか否かを判定する。モジュールＡ　１１０ｃに対する認証が失敗する場合(ステップＳ４３０で“いいえ”)、認証コーディネータ２４０は、ステップＳ４３５，Ｓ４４０で、認証ポリシーによって他のモジュールの認証プロトコルを実行するか否かを判定する。

【００５４】

他のモジュールの認証を遂行しないと判定される場合(ステップＳ４４０で“いいえ”)、認証コーディネータ２４０は、ステップＳ４４５で、格納装置１００ｃを不適切なものと認証する。特に、認証コーディネータ２４０は、格納装置１００ｃの認証が失敗したと決定するかみなし、格納装置１００ｃに格納されたコンテンツの全部又は一部へのアクセスを遮断し、あるいは格納装置１００ｃに対するすべての機能又は特定機能(読み取り、書き込みなど)の遂行を遮断する。

【００５５】

モジュールＡ　１１０ｃに対する認証が成功し(ステップＳ４３０で“はい”)、あるいは他のモジュールに対する認証を遂行すると決定される場合(ステップＳ４４０で“はい”)、Ｂモジュール認証部２２０は、認証ポリシーに定義される認証プロトコルに従ってモジュールＢ　１２０ｃを認証する。Ｂモジュール認証部２２０は、格納装置１１０ｃに集積された複数のモジュールのうちモジュールＢ　１２０ｃに対する第２の認証情報を要請し、モジュールＢ　１２０ｃに関する第２の認証情報を受信及び獲得する。Ｂモジュール認証部２２０は、モジュールＢ　１２０ｃの第２のＵＩＩ及び第２の認証情報に基づいてモジュールＢ　１２０ｃを認証する。

【００５６】

ステップＳ４５５において、認証が成功したか否かを判定する。モジュールＢ　１２０ｃに対する認証が失敗した場合(ステップＳ４５５で“いいえ”)、認証コーディネータ２４０は、ステップＳ４４５で、格納装置１００ｃに対する認証が失敗したと決定又はみなす。

【００５７】

モジュールＢ　１２０ｃに対する認証が成功した場合(ステップＳ４５５で“はい”)、認証コーディネータ２４０は、ステップＳ４６０で、格納装置１００ｃが適法であると認証する。すなわち、認証コーディネータ２４０は、格納装置１００ｃに対する認証が成功したと決定又はみなし、格納装置１００ｃに格納されているコンテンツへのアクセスを許容し、あるいは格納装置１００ｃに対するすべての機能又は特定機能(読み取り、書き込みなど)の遂行を許容する。

【００５８】

図７は、本発明の一実施形態により、暗号化されたコンテンツの格納/記録方法を示す。記録は、格納の一例である。図７において、ホスト装置２００ａは、コンテンツサービスサーバ４０から注文型(on-demand)方式でコンテンツサービスを要請し、コンテンツサービスサーバ４０から提供されるコンテンツを格納装置１００ｄに格納する。コンテンツ

サービスサーバ４０は、制御部、ディスプレイ部、入力装置、メモリ、有線/無線通信部などを具備したコンピュータであり得る。ホスト装置２００ａは、図５に示したホスト装置２００の構成と同様である。

【００５９】

ホスト装置２００ａは、入力装置を通じるユーザーから入力されるコンテンツサービス要請に応じてコンテンツサービスサーバ４０からコンテンツサービスを要請する。

【００６０】

コンテンツサービスサーバ４０は、ステップＳ５１０で、ホスト装置２００ａに格納装置１００ｄの認証を要請する。また、ホスト装置２００ａは、コンテンツサービスサーバ４０からの認証要請を受信せずに格納装置１００ｄの認証を自動で遂行することができる。

【００６１】

モジュールＡ，Ｂ，Ｃ　１１０ｄ，１２０ｄ，１３０ｄのすべてが認証される場合、ホスト装置２００ａは、ステップＳ５１５，Ｓ５２５，Ｓ５３５で、Ａ，Ｂ，Ｃモジュール認証部２１０，２２０，２３０を用いて格納装置１００ｄに集積されたモジュールＡ，Ｂ，Ｃ　１１０ｄ，１２０ｄ，１３０ｄに対する第１～第３の認証情報を要請し、ステップＳ５２０，Ｓ５３０，Ｓ５４０で、第１～第３の認証情報を受信及び獲得する。Ａ，Ｂ，Ｃモジュール認証部は、第１～第３のＵＩＩ(ＵＩＩａ、ＵＩＩｂ、ＵＩＩｃ)と第１～第３の認証情報に基づいてモジュールＡ，Ｂ，Ｃ　１１０ｄ，１２０ｄ，１３０ｄを認証する。

【００６２】

ホスト装置２００ａは、ステップＳ５４５で、格納装置１００ｄの認証結果と、認証関連情報をコンテンツサービスサーバ４０に伝送する。格納装置１００ｄの認証結果は、明確に示されず、例えば、格納装置１００ｄに対する認証が成功した場合、認証関連情報はコンテンツサービスサーバ４０に伝送される。格納装置１００ｄの認証が失敗した場合には、認証関連情報の提供なしにこれを通知できる。認証関連情報は、第１～第３の認証情報、第１～第３のＵＩＩ、及び格納装置１００ｄのメディア識別子を含む。

【００６３】

コンテンツサービスサーバ４０は、認証関連情報を用いて格納装置１００ｄを認証することもできる。

【００６４】

コンテンツサービスサーバ４０は、認証関連情報を用いてコンテンツを暗号化するための暗号化/復号化装置を含む。コンテンツサービスサーバ４０は、ステップＳ５５０で、暗号化コンテンツ及びキー情報をホスト２００ａに伝送する。ホスト２００ａは、暗号化コンテンツ及びキー情報を格納装置１００ｄに格納又は記録する。

【００６５】

図８は、本発明の一実施形態により、暗号化/復号化装置の主要構成を示す。図８は、コンテンツ暗号化キーの生成に関連した構成要素のみを示す。例えば、暗号化/復号化装置３００は、コンテンツ暗号化キーを用いてコンテンツを暗号化するためのコンテンツ暗号化ブロック、キー情報を用いて暗号化されたコンテンツを復号化するコンテンツブロックをさらに含むことができる。ブロック又は関数は、該当機能を遂行する機能ブロック又はモジュールを称される。

【００６６】

暗号化/復号化装置３００は、モジュールＡ，Ｂ，Ｃ　１１０ｄ，１２０ｄ，１３０ｄの第１～第３のＵＩＩ及び第１～第３の認証情報に関連又は結合される(あるいはこれらに基づいて生成される)コンテンツ暗号化キーを生成する。コンテンツ暗号化キーは、格納装置１００ｄのメディア識別子(ＩＤ)にも関連することができる。

【００６７】

すなわち、暗号化/復号化装置３００は、コンテンツが格納される格納装置１００ｄのメディア識別子と各モジュール１１０ｄ，１２０ｄ，１３０ｄのＵＩＩ及び認証情報を統

合してコンテンツ暗号化キーを生成する。
【００６８】
抽出関数３１０は、モジュールＡ，Ｂ，Ｃ　１１０ｄ，１２０ｄ，１３０ｄの第１～第３のＵＩＩと第１～第３の認証情報、格納装置１００ｄのメディア識別子を受信し、入力情報の全部又は一部と関連した情報(すなわち、抽出情報)を出力する。抽出関数３１０は、下記のように、一方向暗号化関数であり得る。
【００６９】
抽出関数Ｆ＝ハッシュ(モジュールＡのＵＩＩ‖認証情報、ハッシュ(モジュールＢのＵＩＩ、認証情報)、…)
【００７０】
ハッシュ()は、通常のハッシュ関数を表し、上記したように、他のハッシュ関数は、ハッシュ関数内に含まれることができる。結合演算子、‖は、その右側オペランド(operand)(すなわち、認証情報)をその左側オペランドの終端に連結させる。抽出関数３１０から出力される抽出情報は、各モジュール１１０ｄ，１２０ｄ，１３０ｄのＵＩＩ及び認証情報を使用するハッシュ関数の出力値に該当する。
【００７１】
コンテンツ暗号化キー生成関数３２０は、抽出関数３１０から出力される抽出情報とキー情報を受信し、これらと関連したコンテンツ暗号化キーを生成及び出力する。
【００７２】
コンテンツ暗号化キー生成関数３２０は、よく知られている暗号アルゴリズムで実現され、キー情報のような情報は、下記のように、任意に(すなわち、ランダム値として)生成することができる。ＡＥＳは、対称キー暗号システムであり、ＡＥＳ-ハッシュは、対称キー暗号システムを使用する一方向ハッシュ関数を表す。
【００７３】
コンテンツ暗号化キー生成関数Ｇ＝ＡＥＳ-ハッシュ(抽出情報、キー情報)
【００７４】
暗号化/復号化装置３００は、抽出関数３１０とコンテンツ暗号化キー生成関数３２０を通じてコンテンツ暗号化キーを生成し、コンテンツ暗号化キーでコンテンツを暗号化する。
【００７５】
図７のステップＳ５５０に示すように、コンテンツサービスサーバ４０は、暗号化されたコンテンツ及びキー情報をホスト装置２００ａに伝送する。
【００７６】
図９は、本発明の一実施形態により、暗号化されたコンテンツの格納/記録方法を示す。図９は、ホスト装置２００ｂが直接にコンテンツを暗号化する一例を示す。ホスト装置２００ｂは、図５に示したホスト装置２００の構成と同様であり、ホスト装置２００ｂは、図８に示す暗号化/復号化装置３００をさらに含む。
【００７７】
ホスト装置２００ｂは、キー情報を直接に生成し、コンテンツ暗号化を遂行する。特に、コンテンツサービスサーバ４０により放送されるコンテンツがホスト装置２００ｂにより格納装置１００ｅに格納される場合、ホスト装置２００ｂは、コンテンツ暗号化キーを生成することができる。
【００７８】
ホスト装置２００ｂは、ステップＳ６１０，Ｓ６２０で、Ａ及びＢモジュール認証部を用いて、格納装置１００ｅに集積された制御部１１０ｅ及び非揮発性メモリ１２０ｅ(各々モジュールＡ及びＢに該当)に対する認証プロトコルを順次に遂行する。
【００７９】
具体的には、ホスト装置２００ｂは、第１及び第２の認証情報を要請して受信及び獲得し、Ａ及びＢモジュール認証部を用いて第１及び第２のＵＩＩと第１及び第２の認証情報に基づいて制御部１１０ｅ及び非揮発性メモリ１２０ｅを認証する。

【００８０】
ホスト装置２００ｂに含まれている暗号化/復号化装置は、抽出関数を用いて制御部１１０ｅ及び非揮発性メモリ１２０ｅの第１及び第２のＵＩＩと第１及び第２の認証情報と関連または結合される抽出情報を生成し、キー情報を生成する。また、暗号化/復号化装置は、抽出情報及びキー情報と結合または関連したコンテンツ暗号化キーを生成及び出力する。
【００８１】
ホスト装置２００ｂは、ステップＳ６３０，Ｓ６４０で、生成されたコンテンツ暗号化キーを用いてコンテンツを暗号化し、暗号化されたコンテンツコンテンツとキー情報を格納装置の非揮発性メモリに格納又は記録する。
【００８２】
図１０は、本発明の一実施形態により、暗号化されたコンテンツコンテンツの格納/記録方法を示すフローチャートである。図１１は、本発明の一実施形態により、図１０に関連したホスト装置の主要構成を示す。格納動作は、図９に示す格納装置１００ｅに対して遂行される。
【００８３】
ホスト装置２００ｃは、ステップＳ７１０で、特定コンテンツの格納/記録要請を受信する。例えば、このような格納/記録要請の受信ステップは、ユーザーによるコンテンツ記録又は格納命令をホスト装置２００ｃに具備されている入力装置を通じて受信するステップに該当する。
【００８４】
ホスト装置２００ｃに含まれている認証部２０５ｃは、図５に示した認証部２０５の構成と同様であり、図８に示した抽出関数３１０をさらに含む。認証部２０５ｃは、複数のモジュール認証部を用いて格納装置１００ｅに集積された複数のモジュール１１０ｅ，１２０ｅに対するＵＩＩ(ＵＩＩａ，ＵＩＩｂ)、及び認証情報を要請して受信及び獲得する。認証部２０５ｃは、ステップＳ７２０で、制御部１１０ｅ及び非揮発性メモリ１２０ｅに対する第１及び第２のＵＩＩと第１及び第２の認証情報に基づいて格納装置１００ｅを認証する。
【００８５】
認証部２００ｃは、ステップＳ７３０で、抽出関数を用いて制御部１１０ｅ及び非揮発性メモリ１２０ｅに対するＵＩＩ及び認証情報と関連した抽出情報を生成する。
【００８６】
認証部２００ｃは、ステップＳ７４０で、抽出情報を暗号化装置３００ｃに伝達する。
【００８７】
暗号化装置３００ｃは、図８に示した暗号化/復号化装置の構成と同様であるが、抽出関数３１０は含まれない。暗号化装置３００ｃは、ステップＳ７５０で、キー情報を生成し、コンテンツ暗号化キー生成関数を用いて抽出情報及びキー情報と関連したコンテンツ暗号化キーを生成する。
【００８８】
暗号化装置３００ｃは、ステップＳ７６０で、コンテンツ暗号化キーでコンテンツを暗号化する。
【００８９】
暗号化装置３００ｃは、ステップＳ７７０で、暗号化されたコンテンツ及びキー情報を格納装置１００ｅに格納する。
【００９０】
図１２は、本発明の一実施形態により、暗号化されたコンテンツの再生方法を示すフローチャートである。図１３は、本発明の一実施形態により、暗号化されたコンテンツを再生する方法を示す。図１４は、本発明の一実施形態により、図１２に関連したホスト装置の主要構成を示す。
【００９１】

ホスト装置２００ｄは、ステップＳ８１０で、特定コンテンツに対する再生要請を受信する。例えば、このような再生要請の受信ステップは、ユーザーによるコンテンツ再生命令をホスト装置２００ｄに提供された入力装置を通じて受信するステップに該当する。

【００９２】

ホスト装置２００ｄに含まれた認証部２０５ｄは、図５に示した認証部２０５の構成と同様であり、図８に示した抽出関数３１０をさらに含む。認証部２０５ｄは、ステップＳ８２０で、複数のモジュール認証部を用いて格納装置１００ｆに集積された制御部１１０ｆ及び非揮発性メモリ１２０ｆに対する認証プロトコルを順次に遂行する。具体的には、ホスト装置２００ｄは、第１及び第２のＵＩＩ(ＵＩＩａ、ＵＩＩｂ)と第１及び第２の認証情報を要請して受信及び獲得する。認証部２０５ｄは、制御部１１０ｆ及び非揮発性メモリ１２０ｆに対する第１及び第２のＵＩＩと第１及び第２の認証情報に基づいて格納装置１００ｆを認証する。

【００９３】

格納装置１００ｆに対する認証が成功した後に、ホスト装置２００ｄは、格納装置１００ｆから暗号化されたコンテンツ及びキー情報を受信する。

【００９４】

認証部２０５ｄは、ステップＳ８３０で、抽出関数を用いて、制御部１１０ｆ及び非揮発性メモリ１２０ｆに対するＵＩＩ及び認証情報と関連した抽出情報を生成する。

【００９５】

認証部２０５ｄは、ステップＳ８４０で、抽出情報を復号化装置３００ｄに伝達する。

【００９６】

復号化装置３００ｄは、ステップＳ８５０で、キー情報を受信し、コンテンツ暗号化キー生成関数を用いて抽出情報及びキー情報に関連したコンテンツ暗号化キーを生成する。

【００９７】

復号化装置３００ｄは、ステップＳ８６０で、コンテンツ暗号化キーを用いて暗号化されたコンテンツを復号化する。

【００９８】

復号化装置３００ｄは、復号化されたコンテンツをコンテンツ再生装置４００に伝達する。

【００９９】

コンテンツ再生装置４００は、ステップＳ８７０で、復号化されたコンテンツを再生する。

【０１００】

本発明の一実施形態において、コンテンツへのアクセスは、コンテンツの再生、移動、コピー、読み取り、格納、削除などの動作を意味する。

【０１０１】

上記の実施形態において、格納装置内の制御部、すなわちモジュールＡ(又は第１のモジュール)に対する第１のＵＩＩと、格納装置内の非揮発性メモリ、すなわちモジュールＢ(又は第２のモジュール)に対する第２のＵＩＩは、固有識別子である。上記した認証方法では、このようなＵＩＩを用いて認証が遂行される。ＵＩＩは、任意に選択される固有識別子であるか、あるいは特定演算により計算される値であり得る。例えば、第２のモジュールに対するＵＩＩは、下記のように計算できる。

【０１０２】

ＥＭＩＤ＝ハッシュ(第２のモジュールの識別子情報、第２のモジュールのプレフィックス情報)

【０１０３】

ＥＭＩＤ(Enhanced Media ID)は、第２のモジュールのＵＩＩを意味し、第２のモジュールの識別子情報は、例えばモジュールメーカーが第２のモジュールに割り当てられた識別子を意味し、プレフィックス情報(prefixed information)は、コンテンツ又はアプリケーション付加情報であって、第２のモジュールに格納されるコンテンツの種類(例え

ば、動画像、静止画像のようなマルチメディアデータ、 銀行口座のような金融(financing)情報 、連絡先番号のような個人情報など)又はコンテンツにアクセスするアプリケーション(又は提供サービス)の種類(例えば、マルチメディアアプリケーション、金融関連アプリケーション、個人情報関連アプリケーションなど)に従って割り当てられた値を表す。プレフィックス情報、ホスト装置のみに格納され、あるいはホスト装置及び格納装置両方ともに格納することができる。

【０１０４】

より詳しくは、本発明は一つのモジュールに対してコンテンツの種類またはアプリケーションの種類によって複数のＵＩＩを割り当てることができ、本発明による認証方法は、該当コンテンツの種類又はアプリケーションの種類に対応するＵＩＩに基づいて遂行できる。

【０１０５】

例えば、図４及び図５を参照すると、Ｂモジュール認証部２２０は、モジュールＢ　１２０ｃに対する第２の認証情報を要請する場合、格納装置１００ｃがアクセスを希望するコンテンツが、マルチメディアデータであるか、あるいはコンテンツにアクセスする実行中であるアプリケーションがマルチメディアアプリケーションである場合に、マルチメディアデータに割り当てられた第２の認証情報を要請できる。Ｂモジュール認証部２２０は、モジュールＢ　１２０ｃのマルチメディアデータに関連した第２のＵＩＩ及び第２の認証情報に基づいてモジュールＢ　１２０ｃを認証できる。モジュールＢ　１２０ｃは、複数のコンテンツ種類又は複数のアプリケーション種類に対応する複数の第２のＵＩＩと、複数の第２のＵＩＩに対応する複数の第２の認証情報を格納することができる。

【０１０６】

モジュールの識別子情報とプレフィックス情報に基づいて生成されるＥＭＩＤは、本発明の実施形態に多様に適用でき、例えば、コンテンツ暗号化キーを生成、又は追加認証情報を生成するために使用され得る。

【０１０７】

図７及び図８を参考すると、抽出関数３１０は、モジュールＢ　１２０ｄの第２のＵＩＩと予め知られているＢモジュール１２０ｄのプレフィックス情報に基づいてモジュールＢ　１２０ｄのＥＭＩＤを生成し、ＥＭＩＤ及びモジュールＡ　１１０ｄの第１のＵＩＩに基づいて抽出情報を出力する。この抽出情報は、下記のように表示することができる。

【０１０８】

例１)抽出情報＝メディアＩＤ　ＸＯＲ　ＥＭＩＤ

例２)抽出情報＝メディアＩＤ‖ＥＭＩＤ

【０１０９】

上記した実施形態において、メディアＩＤは、モジュールＡ　１１０ｄの第１のＵＩＩに該当する。

【０１１０】

コンテンツ暗号化キー生成関数３２０は、抽出関数３１０から出力された抽出情報とランダム値であるキー情報を受信し、これら抽出情報とキー情報に関連したコンテンツ暗号化キーを生成及び出力できる。

【０１１１】

上記した実施形態では、モジュールに対する認証が成功した場合に格納装置が適法なことに決定するが、ＥＭＩＤを用いる追加的な認証情報がさらに提供され得る。このような追加認証情報の認証まで成功した場合に格納装置が適法なことに決定することができる。追加認証情報は、図６に示した各モジュールの認証の代わりにモジュールを認証するために使われることができる。具体的には、追加認証情報が有効なことに決定されると、格納装置は、適法なことに決定することができる。

【０１１２】

追加認証情報生成装置は、図８に示した暗号化/復号化装置３００の構成と同様であり、コンテンツサービスサーバ又はホスト装置に提供することができる。追加認証情報は、

図８に示した暗号化/復号化装置３００又は図１１に示した暗号化装置３００ｃを用いて生成することができる。以下、追加認証情報生成装置は、図７に示したコンテンツサービスサーバ４０に提供される場合を例示する。

【０１１３】

図１５は、本発明の一実施形態による追加認証情報生成装置６００を示すブロック構成図である。

【０１１４】

図７及び図１５を参照すると、抽出関数６１０は、モジュールＢ　１２０ｄの第２のＵＩＩと既知のモジュールＢ　１２０ｄのプレフィックス情報に基づいてモジュールＢ　１２０ｄのＥＭＩＤを生成する。

【０１１５】

ＥＭＩＤ＝ハッシュ(第２のＵＩＩ、モジュールＢのプレフィックス情報)

【０１１６】

抽出関数６１０は、ＥＭＩＤ及びモジュールＡ　１１０ｄの第１のＵＩＩに基づいて計算された抽出情報を出力する。この抽出情報は、下記のように示すことができる。

【０１１７】

例１)抽出情報＝第１のＵＩＩ　ＸＯＲ　ＥＭＩＤ

例２)抽出情報＝第１のＵＩＩ‖ＥＭＩＤ

【０１１８】

認証情報生成器６２０は、抽出関数６１０から出力される抽出情報とランダム値であるキー情報を受信し、この抽出情報及びキー情報に関連した追加認証情報を生成及び出力する。

【０１１９】

追加認証情報生成装置６００は、追加認証情報及びキー情報をホスト装置２００ａに伝送し、ホスト装置２００ａは、追加認証情報及びキー情報を格納装置１００ｄに格納する。

【０１２０】

図１３及び図１４を参照すると、認証部２０５ｄ及び復号化装置３００ｄは、コンテンツ復号化に加えて追加認証情報を処理するために使用することができる。

【０１２１】

認証部２０５ｄは、複数のモジュール認証部を用いて、格納装置１００ｆに集積される制御部１１０ｆ及び非揮発性メモリ１２０ｆに対する認証プロトコルを順次に遂行する。その後、認証部２０５ｄは、抽出関数を用いて非揮発性メモリ１２０ｆのＥＭＩＤ及び制御部１１０ｆのＵＩＩと関連した抽出情報を生成する。

【０１２２】

復号化装置３００ｄは、コンテンツ暗号化キー生成関数を用いて抽出情報及びキー情報と関連した追加認証情報を生成する。復号化装置３００ｄは、格納装置１００ｆから受信した追加認証情報(又はその構成情報)と生成された追加認証情報(又はその構成情報)を比較して格納装置１００ｆに対する認証が成功したか否かを判定できる。

【０１２３】

上記の実施形態では、暗号化キーは、予め設定された式により生成され、コンテンツは、この暗号化キーを用いて暗号化又は復号化されるが、本発明の他の実施形態によると、暗号化キーは、ランダム値を有することができる。

【０１２４】

図１６は、本発明の一実施形態により、暗号化されたコンテンツの格納/記録方法を示す。図１６は、ホスト装置２００ｄが直接にコンテンツを暗号化する一例を示す。ホスト装置２００ｄは、図５に示したホスト装置２００の構成と同様であり、ホスト装置２００ｄは、図１７に示す追加認証情報生成装置７００をさらに含む。

【０１２５】

ホスト装置２００ｄは、ランダム値である暗号化キーを生成し、コンテンツ暗号化を実

行する。特に、コンテンツサービスサーバによりブロードキャスティングされるコンテンツがホスト装置２００ｄから格納装置１００ｇに格納される場合、ホスト装置２００ｄは、コンテンツ暗号化キーを生成できる。

【０１２６】

ホスト装置２００ｄは、ステップＳ９１０及びＳ９２０で、Ａ及びＢモジュール認証部により、格納装置１００ｇに集積された制御部１１０ｇ及び非揮発性メモリ１２０ｇ(モジュールＡ及びＢに該当)に対する認証プロトコルを順次に遂行する。

【０１２７】

すなわち、ホスト装置２００ｄは、第１及び第２の認証情報を要請して受信及び獲得し、Ａ及びＢモジュール認証部を用いて第１及び第２のＵＩＩ(ＵＩＩａ、ＵＩＩｂ)と第１及び第２の認証情報に基づいて制御部１１０ｇ及び非揮発性メモリ１２０ｇを認証する。

【０１２８】

図１７は、本発明の一実施形態により、追加認証情報生成装置７００を示すブロック構成図である。追加認証情報生成装置７００は、ランダムな値である暗号化キーを受信することを除き、図１５に示した追加認証情報生成装置６００の構成と同様である。

【０１２９】

抽出関数７１０は、下記のように、非揮発性メモリ１２０ｇの第２のＵＩＩと既知の非揮発性メモリ１２０ｇのプレフィックス情報に基づいて非揮発性メモリ１２０ｇのＥＭＩＤを生成する。

【０１３０】

ＥＭＩＤ＝ハッシュ(第２のＵＩＩ、非揮発性メモリのプレフィックス情報)

【０１３１】

抽出関数７１０は、ＥＭＩＤ及び制御部１１０ｇの第１のＵＩＩに基づいて計算された抽出情報を出力する。この抽出情報は、下記のように表示することができる。

【０１３２】

例１)抽出情報＝第１のＵＩＩ ＸＯＲ ＥＭＩＤ

例２)抽出情報＝第１のＵＩＩ‖ＥＭＩＤ

【０１３３】

認証情報生成器７２０は、抽出関数７１０から出力される抽出情報、ランダム値である暗号化キーを受信する。認証情報生成器７２０は、抽出情報と暗号化キーに関連した追加認証情報を生成及び出力する。

【０１３４】

図１６を参照すると、ホスト装置２００ｄは、ステップＳ９３０、Ｓ９４０で、ランダム暗号化キーでコンテンツを暗号化し、暗号化されたコンテンツと追加認証情報を格納装置１００ｇの非揮発性メモリ１２０ｇに格納又は記録する。

【０１３５】

図１８は、本発明の一実施形態により、暗号化されたコンテンツの格納/記録方法を示すフローチャートである。図１９は、本発明の一実施形態により、図１８に関連したホスト装置の主要構成を示す。図１６に示した格納装置１００ｇに格納が遂行される。

【０１３６】

ホスト装置２００ｆは、ステップＳ１０１０で、特定コンテンツに対する格納/記録要請を受信する。例えば、この格納/記録要請の受信ステップは、ユーザーによるコンテンツ記録又は格納命令をホスト装置２００ｆに含まれた入力装置を通じて受信するステップに対応できる。

【０１３７】

ホスト装置２００ｆに含まれた認証部２０５ｆは、図５に示した認証部２０５と類似した構成を有する。認証部２０５ｆは、複数のモジュール認証部を用いて、格納装置１００ｇ内に集積された複数のモジュール１１０ｇ，１２０ｇに対するＵＩＩ(ＵＩＩａ、ＵＩＩｂ)及び認証情報を要請して受信及び獲得する。認証部２０５ｆは、ステップＳ１０２０において、制御部１１０ｇ及び非揮発性メモリ１２０ｇに関する第１及び第２のＵＩＩ

と第１及び第２の認証情報に基づいて格納装置１００ｇを認証する。

【０１３８】

追加認証情報生成装置７００は、ステップ１０３０で、ランダムなコンテンツ暗号化キーを生成する。この追加認証情報生成装置７００は、ステップＳ１０４０で、ＥＭＩＤに基づいた抽出情報とランダム値であるコンテンツ暗号化キーに関連した追加認証情報を生成及び出力する。

【０１３９】

暗号化装置３００ｆは、ステップＳ１０５０で、ランダム暗号化キーでコンテンツを暗号化する。

【０１４０】

暗号化装置３００ｆは、ステップ１０６０で、暗号化されたコンテンツ及び追加認証情報を格納装置１００ｇに格納する。

【０１４１】

図２０は、本発明の一実施形態による暗号化されたコンテンツの再生方法を示すフローチャートである。図２１は、本発明の一実施形態により、図２０の再生方法を示す。図２２は、本発明の一実施形態により、図２０の再生方法に関連したホスト装置の主要構成を示すブロック構成図である。図２３は、本発明の一実施形態により、暗号化キー抽出装置を示すブロック構成図である。

【０１４２】

ホスト装置２００ｇは、ステップ１１１０で、特定コンテンツに対する再生要請を受信する。例えば、このような再生要請受信ステップは、ユーザーによるコンテンツ再生命令をホスト装置２００ｇに含まれている入力装置を通じて受信するステップに対応する。

【０１４３】

ホスト装置２００ｇに含まれている認証部２０５ｇは、図２３に示すように暗号化キー抽出装置８００をさらに含むことを除き、図５に示した認証部２０５の構成と同様である。

【０１４４】

認証部２０５ｇは、ステップＳ１１２０で、複数のモジュール認証部を用いて格納装置１００ｈに集積された制御部１１０ｈ及び非揮発性メモリ１２０ｈに対する認証プロトコルを順次に遂行する。すなわち、ホスト装置２００ｇは、第１及び第２のＵＩＩ(ＵＩＩａ、ＵＩＩｂ)と第１及び第２の認証情報を要請して受信及び獲得する。認証部２０５ｇは、制御部１１０ｈ及び非揮発性メモリ１２０ｈに対する第１及び第２のＵＩＩと第１及び第２の認証情報に基づいて格納装置１００ｈを認証する。

【０１４５】

図２３を参照すれば、暗号化キー抽出装置８００の抽出関数８１０は、下記のように、非揮発性メモリ１２０ｈの第２のＵＩＩと既知の非揮発性メモリ１２０ｈのプレフィックス情報に基づいて非揮発性メモリ１２０ｈのＥＭＩＤを生成する。

【０１４６】

ＥＭＩＤ＝ハッシュ(第２のＵＩＩ、非揮発性メモリのプレフィックス情報)

【０１４７】

抽出関数８１０は、ステップＳ１１３０で、ＥＭＩＤ及び制御部１１０ｈの第１のＵＩＩに基づいて計算された抽出情報を出力する。この抽出情報は、下記のように表示することができる。

【０１４８】

例１)抽出情報＝第１のＵＩＩ ＸＯＲ ＥＭＩＤ

例２)抽出情報＝第１のＵＩＩ‖ＥＭＩＤ

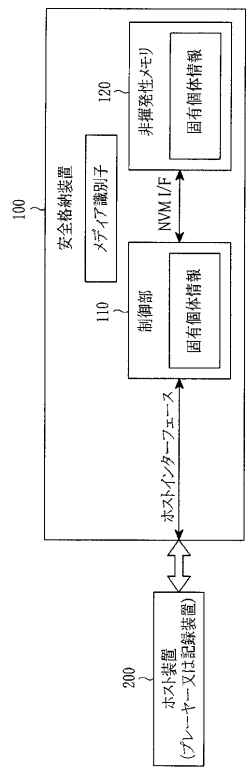
【０１４９】

暗号化キー抽出器８２０は、ステップＳ１１４０で、抽出関数８１０から出力される抽出情報と追加認証情報を受信し、ランダムな値であるコンテンツ暗号化キーを抽出及び出力する。

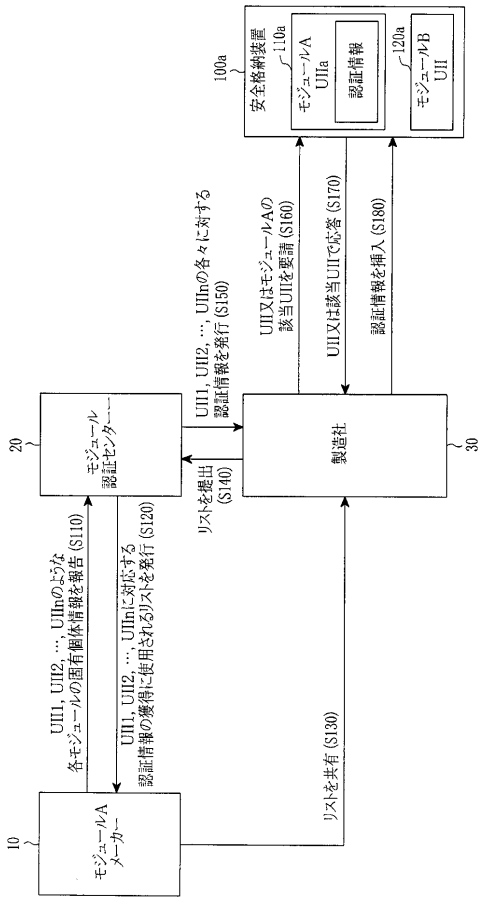
【０１５０】
図２２を参照すると、復号化装置３００ｇは、キー情報を受信し、コンテンツ暗号化キー生成関数を用いて抽出情報及びキー情報と関連したコンテンツ暗号化キーを生成する。
【０１５１】
復号化装置３００ｇは、ステップＳ１１５０で、コンテンツ暗号化キーを用いて暗号化されたコンテンツを復号化する。
【０１５２】
復号化装置３００ｇは、復号化されたコンテンツをコンテンツ再生装置４００ａに伝達する。
【０１５３】
コンテンツ再生装置４００ａは、ステップＳ１１６０でコンテンツを再生する。
【０１５４】
本発明の実施形態は、ハードウェア、ソフトウェア、又はハードウェアとソフトウェアの組み合わせで実現されることができる。このような任意のソフトウェアは、例えば、削除可能または再記録可能であるか否かに関係なく、ＲＯＭ(Read-Only Memory)のような揮発性又は非揮発性格納装置と、ＲＡＭ(Random Access Memory)、メモリチップ、デバイス、又は集積回路のようなメモリと、ＣＤ(Compact Disc)、ＤＶＤ(Digital Versatile Disk)、磁気ディスク、又は磁気テープのような光学又は磁気記録可能であり、かつ機械(例えば、コンピュータ)読み取り可能な格納存媒体に格納することができる。ホスト装置内に含まれるメモリは、本発明の実施形態を実現するための指示を含むプログラム又はプログラムを格納するのに適合した機械読み取り可能な格納媒体の一例であり得る。したがって、本発明の実施形態は、任意の請求項に記載された装置又は方法を実現するためのコードを含むプログラム及びこのようなプログラムを格納する機械読み取り可能な格納媒体を含む。このプログラムは、有線又は無線接続を通じて伝送される通信信号のような任意の媒体を通じて電子的に伝送され、本発明は、これと均等なことを適切に含むことができる。
【０１５５】
ホスト装置は、有線又は無線方式で接続されるプログラム提供装置からプログラムを受信して格納することができる。プログラム提供装置は、ホスト装置が予め設定されたコンテンツ保護方法を遂行するようにする指示を含むプログラム、コンテンツ保護方法に必要な情報などを格納するためのメモリと、ホスト装置との有線又は無線通信を遂行するための通信部と、ホスト装置の要請又は自動的に該当プログラムをホスト装置に伝送する制御部とを含むことができる。
【０１５６】
以上、本発明の詳細な説明においては具体的な実施形態に関して説明したが、特許請求の範囲の記載及びこれと均等なものに基づいて定められる本発明の範囲及び精神を逸脱することなく、形式や細部の様々な変更が可能であることは、当該技術分野における通常の知識を持つ者には明らかである。
【符号の説明】
【０１５７】
１０　モジュールＡメーカー
２０　モジュール認証センター
３０　製造社
４０　コンテンツサービスサーバ
１００　安全格納装置
１１０　制御部
１２０　非揮発性メモリ
２００　ホスト装置
２０５　認証部
２１０　Ａモジュール認証部

２２０　Ｂモジュール認証部
２３０　Ｃモジュール認証部
２４０　認証コーディネータ
２５０　認証に対するポリシー
３００　暗号化/復号化装置
３１０　抽出関数
３２０　コンテンツ暗号化キー生成関数
４００　コンテンツ再生装置
６００　追加認証情報生成装置

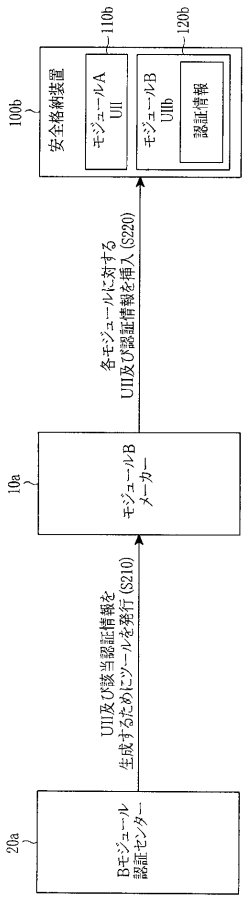
【図１】



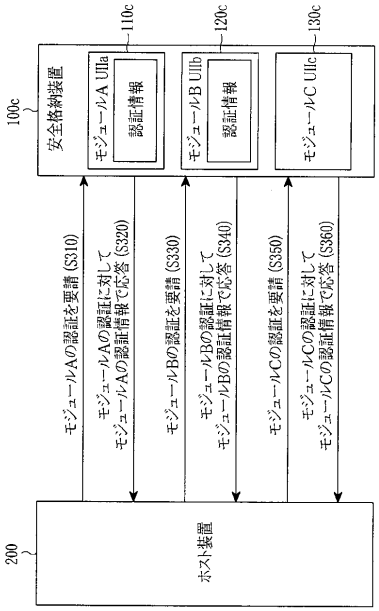

【図２】



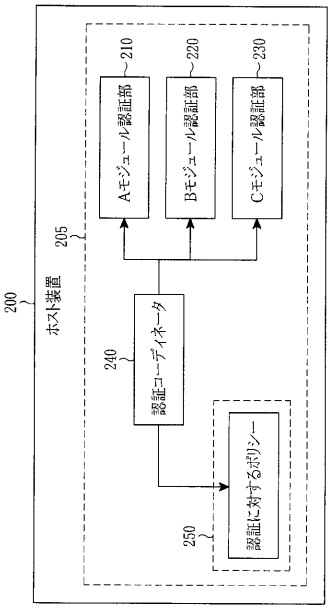
【図３】


100b
安全格納装置
110b
モジュールA UII
120b
モジュールB UIIb
認証情報
各モジュールに対する UII及び認証情報を挿入 (S220)
10a
モジュールB メーカー
UII及び該当認証情報を 生成するためにツールを発行 (S210)
20a
Bモジュール 認証センター

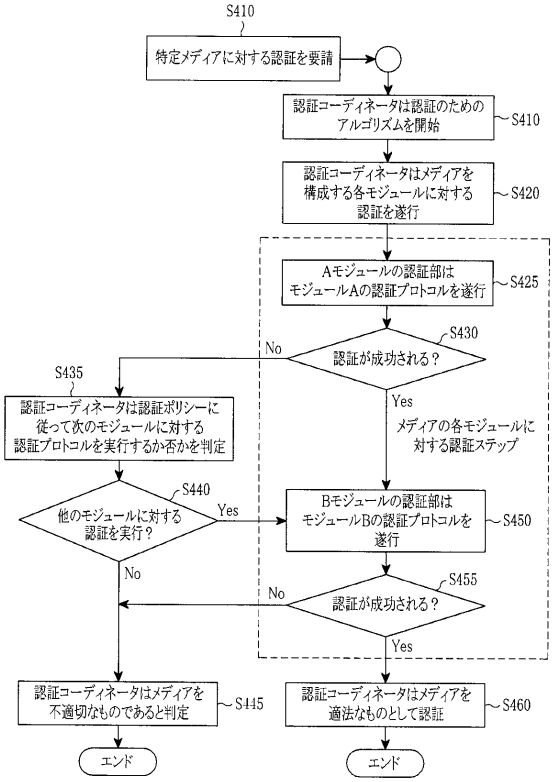
【図４】


100c
安全格納装置
110c
モジュールA UIIa
認証情報
120c
モジュールB UIIb
認証情報
130c
モジュールC UIIc
モジュールAの認証を要請 (S310)
モジュールAの認証に対して モジュールAの認証情報で応答 (S320)
モジュールBの認証を要請 (S330)
モジュールBの認証に対して モジュールBの認証情報で応答 (S340)
モジュールCの認証を要請 (S350)
モジュールCの認証に対して モジュールCの認証情報で応答 (S360)
200
ホスト装置

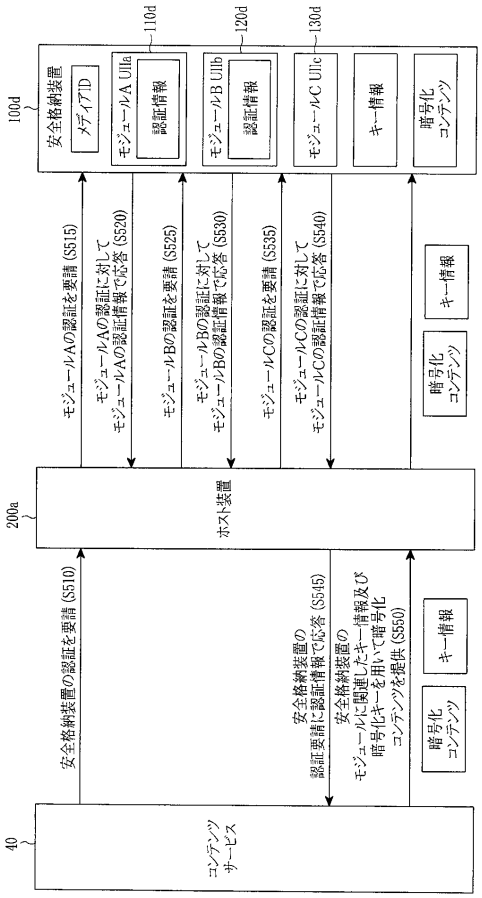
【図５】


200
ホスト装置
205
210
Aモジュール認証部
220
Bモジュール認証部
230
Cモジュール認証部
240
認証コーディネータ
250
認証に対するポリシー

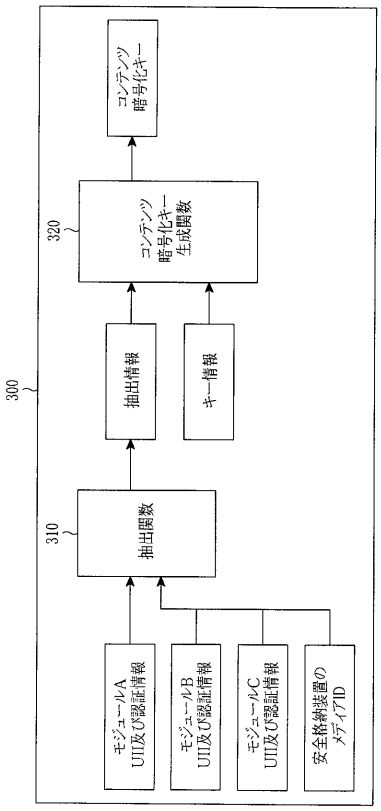
【図６】


S410
特定メディアに対する認証を要請
認証コーディネータは認証のための アルゴリズムを開始
S410
認証コーディネータはメディアを 構成する各モジュールに対する 認証を遂行
S420
Aモジュールの認証部は モジュールAの認証プロトコルを遂行
S425
S430
認証が成功される？
No
Yes
S435
認証コーディネータは認証ポリシーに 従って次のモジュールに対する 認証プロトコルを実行するか否かを判定
メディアの各モジュールに 対する認証ステップ
S440
他のモジュールに対する 認証を実行？
Yes
Bモジュールの認証部は モジュールBの認証プロトコルを 遂行
S450
No
S455
No
認証が成功される？
Yes
認証コーディネータはメディアを 不適切なものであると判定
S445
認証コーディネータはメディアを 適法なものとして認証
S460
エンド
エンド

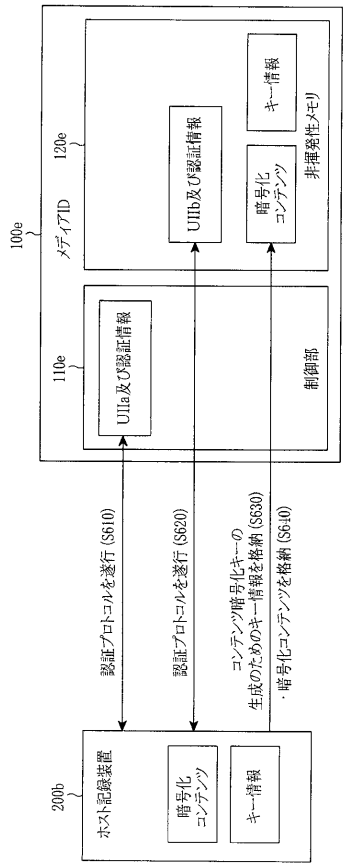
【図７】


100d
安全格納装置
メディアID
110d
モジュールA UIIa
認証情報
120d
モジュールB UIIb
認証情報
130d
モジュールC UIIc
キー情報
暗号化コンテンツ
モジュールAの認証を要請 (S515)
モジュールAの認証に対して
モジュールAの認証情報で応答 (S520)
モジュールBの認証を要請 (S525)
モジュールBの認証に対して
モジュールBの認証情報で応答 (S530)
モジュールCの認証を要請 (S535)
モジュールCの認証に対して
モジュールCの認証情報で応答 (S540)
200a
ホスト装置
暗号化コンテンツ
キー情報
安全格納装置の認証を要請 (S510)
安全格納装置の
認証要請に認証情報で応答 (S545)
安全格納装置の
モジュールに関連したキー情報及び
暗号化キーを用いて暗号化
コンテンツを提供 (S550)
暗号化コンテンツ
キー情報
40
コンテンツサービス

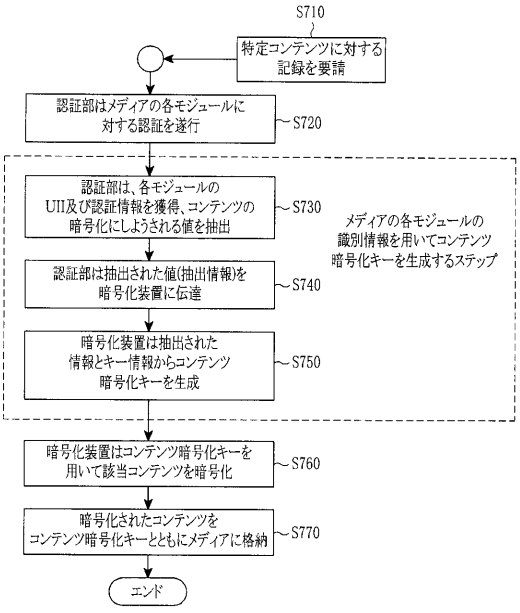
【図８】


コンテンツ暗号化キー
320
コンテンツ暗号化キー生成関数
抽出情報
キー情報
300
310
抽出関数
モジュールA UII及び認証情報
モジュールB UII及び認証情報
モジュールC UII及び認証情報
安全格納装置のメディアID

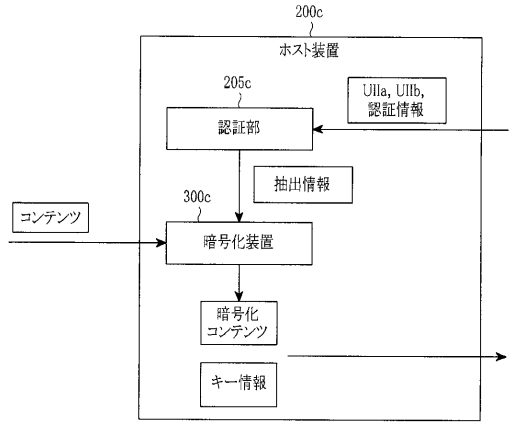
【図９】


100e
メディアID
120e
UIIb及び認証情報
暗号化コンテンツ
キー情報
非揮発性メモリ
110e
UIIa及び認証情報
制御部
認証プロトコルを遂行 (S610)
認証プロトコルを遂行 (S620)
コンテンツ暗号化キーの
生成のためのキー情報を格納 (S630)
・暗号化コンテンツを格納 (S640)
200b
ホスト記録装置
暗号化コンテンツ
キー情報

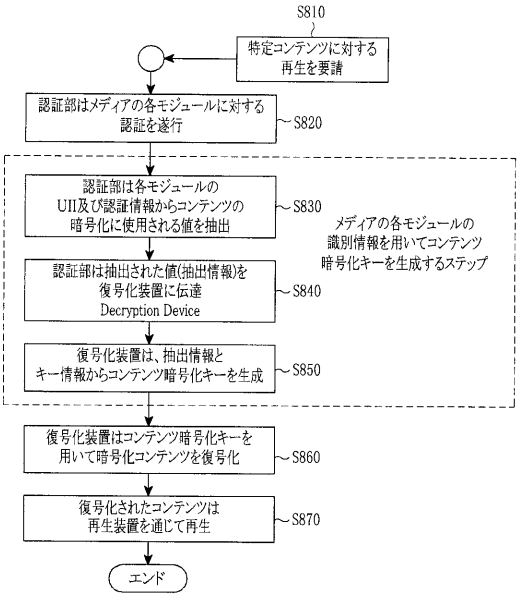
【図１０】


S710
特定コンテンツに対する
記録を要請
認証部はメディアの各モジュールに
対する認証を遂行
S720
認証部は、各モジュールの
UII及び認証情報を獲得、コンテンツの
暗号化にしようされる値を抽出
S730
認証部は抽出された値(抽出情報)を
暗号化装置に伝達
S740
暗号化装置は抽出された
情報とキー情報からコンテンツ
暗号化キーを生成
S750
メディアの各モジュールの
識別情報を用いてコンテンツ
暗号化キーを生成するステップ
暗号化装置はコンテンツ暗号化キーを
用いて該当コンテンツを暗号化
S760
暗号化されたコンテンツを
コンテンツ暗号化キーとともにメディアに格納
S770
エンド

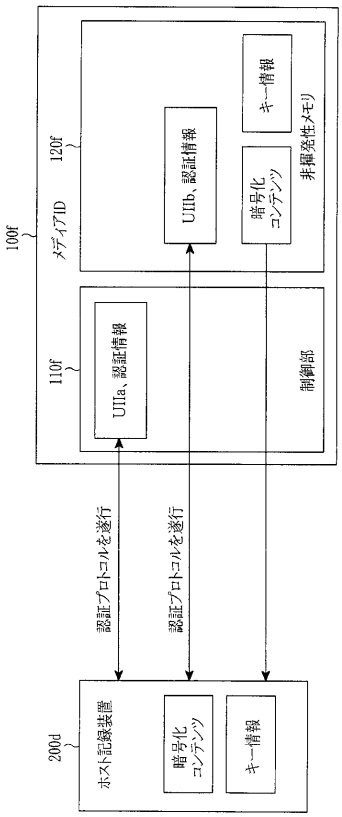
【図１１】



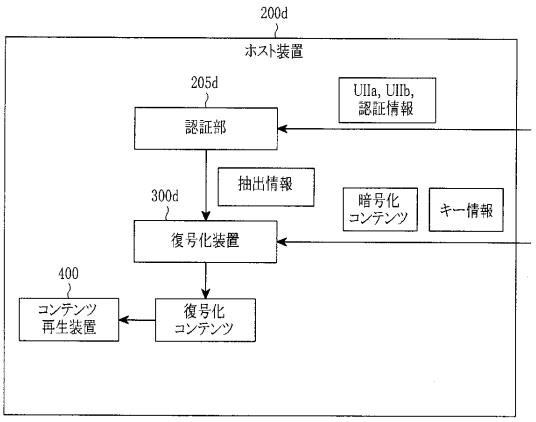

【図１２】



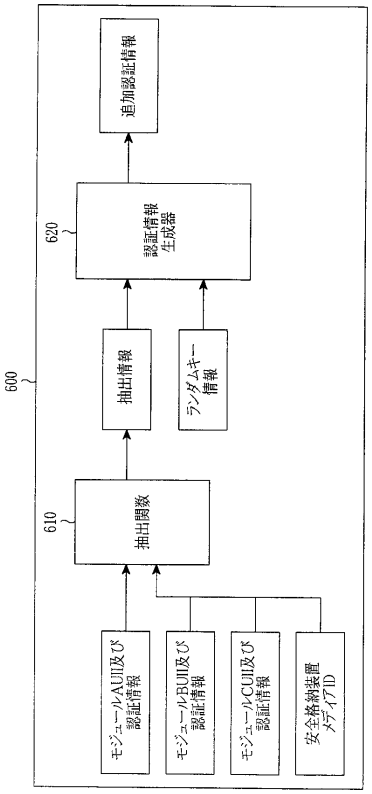

【図１３】



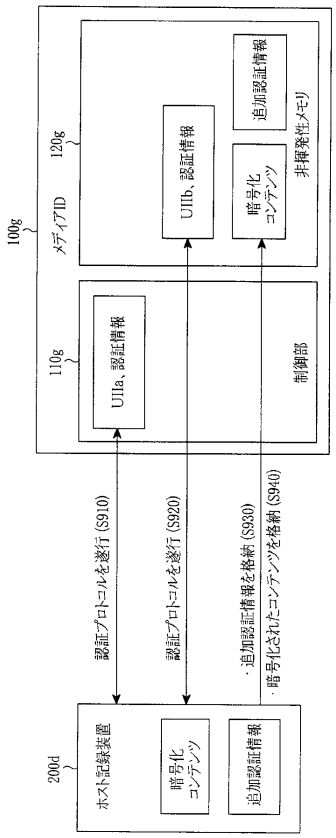

【図１４】



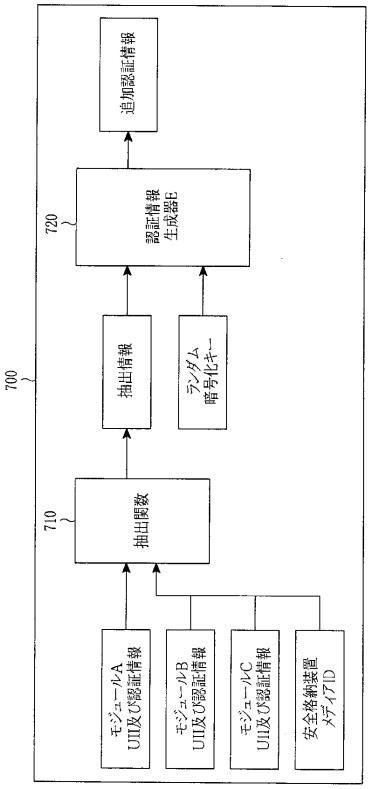
【図１５】



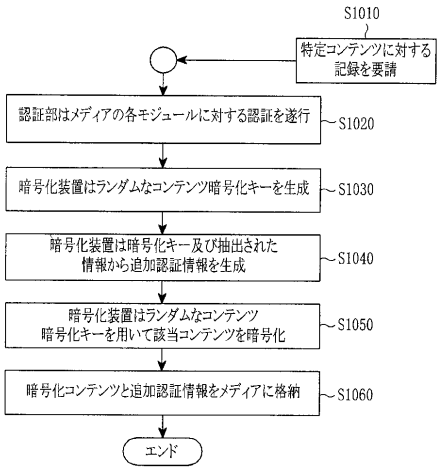

【図１６】



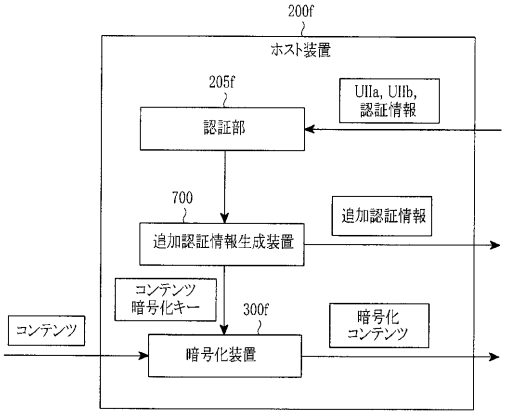

【図１７】



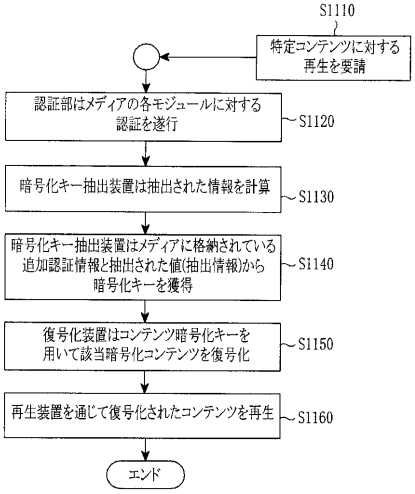

【図１８】



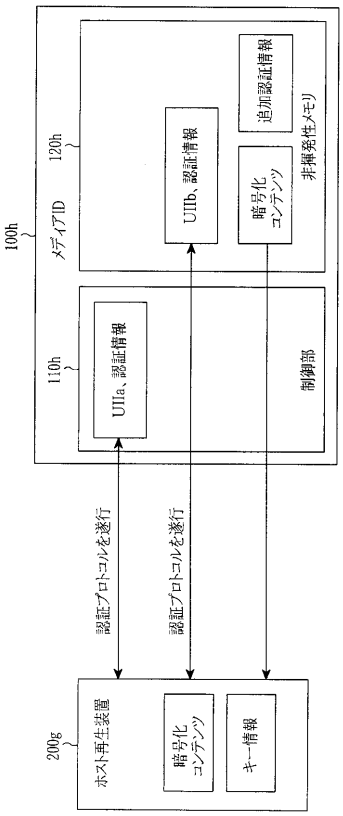
【図１９】



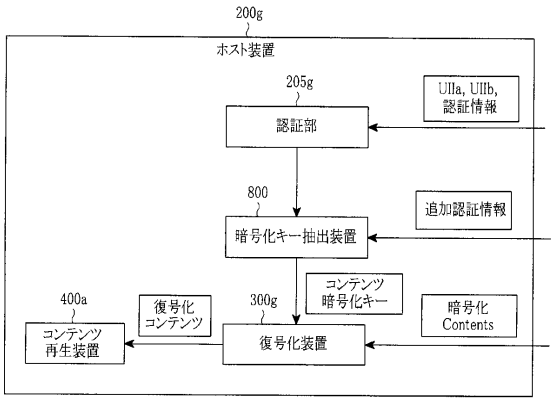

【図２０】



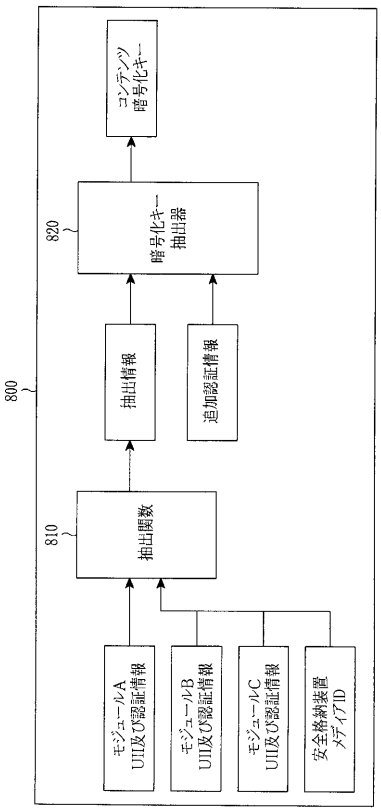

【図２１】




【図２２】



【図２３】


800
810
抽出関数
820
暗号化キー
抽出器
抽出情報
追加認証情報
コンテンツ
暗号化キー
モジュールA
UII及び認証情報
モジュールB
UII及び認証情報
モジュールC
UII及び認証情報
安全格納装置
メディアID

フロントページの続き

(56)参考文献 特開２０１２－１４１８２１（ＪＰ，Ａ）
国際公開第２０１０／０３５４４９（WO，Ａ１）
特開２００２－２２９８５９（ＪＰ，Ａ）
特開２００５－０１８４４５（ＪＰ，Ａ）
特開２０１０－２６８４１７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１