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

特許第4663437号
(P4663437)

(45)発行日　平成23年4月6日(2011.4.6)　(24)登録日　平成23年1月14日(2011.1.14)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601C
G06F 21/24	(2006.01)	H04L	9/00	601E
G06F 21/06	(2006.01)	G06F	12/14	540B
H04N 7/16	(2011.01)	G06F	12/14	540P
		G06F	12/14	560E

請求項の数 17　(全 33 頁)　最終頁に続く

(21)出願番号　特願2005-210645 (P2005-210645)
(22)出願日　平成17年7月20日 (2005.7.20)
(65)公開番号　特開2006-60793 (P2006-60793A)
(43)公開日　平成18年3月2日 (2006.3.2)
審査請求日　平成20年7月7日 (2008.7.7)
(31)優先権主張番号　特願2004-213690 (P2004-213690)
(32)優先日　平成16年7月22日 (2004.7.22)
(33)優先権主張国　日本国(JP)

(73)特許権者　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(74)代理人　100105924
弁理士　森下　賢樹
(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】コンテンツ利用情報送信方法およびその方法を利用可能なコンテンツ利用情報提供装置およびコンテンツ利用情報享受装置

(57)【特許請求の範囲】

【請求項１】

暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報を送受信する方法であって、

前記コンテンツ利用情報の送信元装置が前記コンテンツ利用情報の送信先装置を認証するステップと、

前記送信先装置が承認された場合に、前記送信元装置と前記送信先装置の間で第１の対称鍵を共有するステップと、

前記送信元装置が、前記コンテンツ利用情報を暗号化して前記送信先装置へ送信するステップと、を含み、

前記第１の対称鍵を共有するステップは、

Elliptic Curve Diffie-Hellman暗号アルゴリズムにより、前記送信先装置の公開鍵を用いて、前記第１の対称鍵を前記送信先装置との間で共有するためのデータを生成するステップと、

前記データを相手の装置に送信するステップと、を含み、

前記コンテンツ利用情報を送信するステップは、

前記コンテンツ利用情報を送信するタイミングが到来したときに、前記送信元装置と前記送信先装置の間で第２の対称鍵を共有するステップと、

前記第１の対称鍵及び前記第２の対称鍵により前記コンテンツ利用情報を暗号化して前記送信先装置へ送信するステップと、を含む

ことを特徴とするコンテンツ利用情報送信方法。
【請求項２】
前記第１の対称鍵は、前記コンテンツ利用情報を送信するステップの終了後も、前記送信元装置及び前記送信先装置において保持されて、次にコンテンツ利用情報を送信するときに利用されることを特徴とする請求項１に記載のコンテンツ利用情報送信方法。
【請求項３】
前記第２の対称鍵は、前記コンテンツ利用情報を送受信するステップの終了後に、次のコンテンツ利用情報を送信するときには新たに発行され、前記送信元装置及び前記送信先装置の間で共有されることを特徴とする請求項１又は２に記載のコンテンツ利用情報送信方法。
【請求項４】
前記第１の対称鍵は、前記送信元装置及び前記送信先装置のうちいずれか一方が発行し、前記第２の対称鍵は、他方が発行することを特徴とする請求項１から３のいずれかに記載のコンテンツ利用情報送信方法。
【請求項５】
前記第２の対称鍵を共有するために使用する第３の対称鍵を前記送信元装置と前記送信先装置との間で共有するステップを更に含み、
前記第２の対称鍵を共有するステップは、前記第２の対称鍵を前記第３の対称鍵で暗号化して送受信することにより前記第２の対称鍵を共有することを特徴とする請求項１から４のいずれかに記載のコンテンツ利用情報送信方法。
【請求項６】
前記第３の対称鍵は、前記コンテンツ利用情報を送信するステップの終了後も、前記送信元装置及び前記送信先装置において保持されて、次に前記第２の対称鍵を共有するときに利用されることを特徴とする請求項５に記載のコンテンツ利用情報送信方法。
【請求項７】
前記送信元装置及び前記送信先装置の一方は、ストレージデバイスであることを特徴とする請求項１から６のいずれかに記載のコンテンツ利用情報送信方法。
【請求項８】
暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報享受装置に提供するコンテンツ利用情報提供装置であって、
前記コンテンツ利用情報享受装置から認証情報を取得して、その認証情報の正当性を検証する検証手段と、
前記検証手段が前記コンテンツ利用情報享受装置を承認したときに、前記コンテンツ利用情報享受装置との間で公開鍵暗号方式を用いて第１の対称鍵を共有する第１の対称鍵共有手段と、
前記コンテンツ利用情報を送信するタイミングが到来したときに、前記コンテンツ利用情報享受装置との間で第２の対称鍵を共有する第２の対称鍵共有手段と、
前記コンテンツ利用情報を前記第１の対称鍵及び前記第２の対称鍵により暗号化する暗号化手段と、
前記暗号化手段により暗号化された前記コンテンツ利用情報を前記コンテンツ利用情報享受装置へ送信するコンテンツ利用情報送信手段と、を備え、
前記第１の対称鍵共有手段は、
乱数を発生する乱数発生手段と、
Elliptic Curve Diffie-Hellman暗号アルゴリズムにより前記乱数と前記コンテンツ利用情報享受装置の公開鍵を用いて前記第１の対称鍵を生成するとともに、前記第１の対称鍵を前記コンテンツ利用情報享受装置との間で共有するためのデータを生成する第１の対称鍵生成手段と、
前記データを前記コンテンツ利用情報享受装置に送信する送信手段と、を含む
ことを特徴とするコンテンツ利用情報提供装置。
【請求項９】

前記コンテンツ利用情報提供装置は、
前記コンテンツ利用情報を生成するコンテンツ利用情報生成部と、
前記コンテンツデータを前記コンテンツ鍵によって暗号化し、前記暗号化コンテンツデータを出力するコンテンツデータ暗号部と、
を更に備えることを特徴とする請求項８に記載のコンテンツ利用情報提供装置。
【請求項１０】
前記コンテンツ利用情報提供装置は、
前記暗号化コンテンツデータを格納する第１の格納部と、
前記コンテンツ利用情報を格納する第２の格納部と、を更に備え、
前記第２の格納部は、耐タンパ構造によって構成されることを特徴とする請求項８又は９に記載のコンテンツ利用情報提供装置。
【請求項１１】
暗号化されたコンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報享受装置に提供するコンテンツ利用情報提供装置であって、
前記コンテンツ利用情報享受装置との間でデータの授受を制御するインタフェースと、
前記コンテンツ利用情報享受装置との通信においてテンポラルに生成する第１の対称鍵を生成する対称鍵生成部と、
前記コンテンツ利用情報享受装置に設定された第１の公開鍵によって、データを暗号化する第１の暗号部と、
前記対称鍵生成部により生成された第１対称鍵によってデータを復号する復号部と、
前記コンテンツ利用情報享受装置に設定された楕円曲線暗号の第２の公開鍵を用いて、Ｅｌｌｉｐｔｉｃ　ｃｕｒｖｅ　Ｄｉｆｆｉｅ　－　Ｈｅｌｌｍａｎ暗号アルゴリズムにしたがい、データを暗号化する第２の暗号部と、
前記第２の暗号部に供給する乱数を生成する乱数生成部と、
前記コンテンツ利用情報享受装置で生成された第２の対称鍵によってデータを暗号化する第３の暗号部と、
制御部とを備え、
前記第２の暗号部は、
前記乱数生成部において生成された乱数を取得し、前記取得した乱数と前記第２の公開鍵に基づいて、暗号化に用いるシェアード鍵と、このシェアード鍵を前記コンテンツ利用情報享受装置と共有するためのデータとを生成する機能と、前記生成したシェアード鍵によって前記コンテンツ利用情報を暗号化する機能を有し、
前記対称鍵生成部において前記第１の対称鍵が生成されて初めての前記第２の公開鍵による暗号化処理において、前記乱数生成部において生成された乱数を取得し、前記取得した乱数と前記第２の公開鍵に基づいて、暗号化に用いるシェアード鍵と、このシェアード鍵を前記コンテンツ利用情報享受装置と共有するためのデータとを生成し、前記シェアード鍵によってデータを暗号化し、
前記対称鍵生成部において前記第１の対称鍵が生成されて２回目以降の暗号化処理において、前回のシェアード鍵によって前記コンテンツ利用情報を暗号化し、
前記制御部は、
前記第１の対称鍵を生成するように前記対称鍵生成部を制御し、
前記第１の公開鍵によって暗号化された前記第１の対称鍵を前記第１の暗号部から受け取って、前記インタフェースを介して前記コンテンツ利用情報享受装置へ送信し、
前記インタフェースを介して受信した前記第１の対称鍵によって暗号化された前記第２の対称鍵および前記第２の公開鍵を、前記コンテンツ利用情報享受装置から受け取って前記復号部に与え、
前記復号部で復号した第２の公開鍵に基づいて生成されたシェアード鍵と第２の対称鍵とによって暗号化された暗号化コンテンツ利用情報を前記第２の暗号部または前記第３の暗号部から受け取って、前記インタフェースを介して前記コンテンツ利用情報享受装置へ送信する

ことを特徴とするコンテンツ利用情報提供装置。
【請求項１２】
前記コンテンツ利用情報を生成し、かつ、生成したコンテンツ利用情報に含まれる前記コンテンツ鍵でコンテンツデータを暗号化するコンテンツ暗号部をさらに備え、
前記制御部は、前記コンテンツ暗号部が生成した前記コンテンツ利用情報を取得し、前記第３の暗号部に与える、請求項１１に記載のコンテンツ利用情報提供装置。
【請求項１３】
本コンテンツ利用情報提供装置は、ストレージデバイスであることを特徴とする請求項８から１２のいずれかに記載のコンテンツ利用情報提供装置。
【請求項１４】
暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報提供装置から享受するコンテンツ利用情報享受装置であって、
前記コンテンツ利用情報提供装置に自身の認証情報を送信する認証情報送信手段と、
前記コンテンツ利用情報提供装置が前記認証情報を承認したときに、前記コンテンツ利用情報提供装置との間で公開鍵暗号方式を用いて第１の対称鍵を共有する第１の対称鍵共有手段と、
前記コンテンツ利用情報を受信するタイミングが到来したときに、前記コンテンツ利用情報提供装置との間で第２の対称鍵を共有する第２の対称鍵共有手段と、
前記第１の対称鍵及び前記第２の対称鍵により暗号化された前記コンテンツ利用情報を前記コンテンツ利用情報提供装置から受信するコンテンツ利用情報受信手段と、
前記暗号化された前記コンテンツ利用情報を復号する復号手段と、を備え、
前記第１の対称鍵共有手段は、
前記コンテンツ利用情報提供装置に自身の公開鍵を提供する公開鍵提供手段と、
前記第１の対称鍵を前記コンテンツ利用情報提供装置との間で共有するためのデータを取得する取得手段と、
Elliptic Curve Diffie-Hellman暗号アルゴリズムにより前記データと前記公開鍵と対をなす秘密鍵とを用いて前記第１の対称鍵を生成する第１の対称鍵生成手段と、を含む
ことを特徴とするコンテンツ利用情報享受装置。
【請求項１５】
前記コンテンツ利用情報享受装置は、
前記暗号化コンテンツデータを前記コンテンツ鍵により復号するコンテンツデータ復号部と、
前記コンテンツデータ復号部により復号されたコンテンツデータを再生する再生部と、
を更に備えることを特徴とする請求項１４に記載のコンテンツ利用情報享受装置。
【請求項１６】
前記コンテンツ利用情報享受装置は、
前記暗号化コンテンツデータを格納する第１の格納部と、
前記コンテンツ利用情報を格納する第２の格納部とを含み、
前記第２の格納部は、耐タンパ構造によって構成されることを特徴とする請求項１４又は１５に記載のコンテンツ利用情報享受装置。
【請求項１７】
本コンテンツ利用情報享受装置は、ストレージデバイスであることを特徴とする請求項１４から１６のいずれかに記載のコンテンツ利用情報享受装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データ入出力技術に関し、とくに、記憶装置とホスト装置との間で秘匿すべきデータを暗号化して入出力する技術に関する。
【背景技術】
【０００２】

ライセンスデータの秘匿性を高めたコンテンツデータ配信システムとして、例えば、特許文献１では、ライセンスデータを非暗号化の状態で扱う装置を、サーバ装置、メモリカード（ストレージデバイス）、デコーダ（利用装置）の３つの装置に分類し、装置間（サーバ装置とストレージデバイス、ストレージデバイスと利用装置）のライセンスデータの送受信は、ライセンスデータの送受信を行う２つの装置間に暗号化通信路を構築し、その暗号化通信路を介して行い、かつ、サーバ装置、ストレージデバイス、および利用装置は、暗号化されたライセンスデータを扱えるＴＲＭ（Tamper-Resistant-Module）とを備える。

【０００３】

暗号化通信路の構築では、最初にライセンスデータを享受する装置（ライセンス享受装置と呼ぶ）が公開鍵を含んだ証明書を、ライセンスデータを提供する装置（ライセンス提供装置と呼ぶ）に送信する。そして、ライセンス提供装置がこの証明書を検証して、検証の結果、ライセンス享受装置からの証明書が、正規の証明書であり、かつ、証明書破棄リストによって無効とされていない場合に、この証明書に含まれる公開鍵を利用して、装置間で鍵交換を行う。そして、ライセンス提供装置は、前記鍵交換においてライセンス享受装置から送られた鍵で暗号化したライセンスデータを、ライセンス享受装置に送信する。

【０００４】

ＴＲＭは、物理的に秘匿性が保護された回路モジュールであって、暗号化通信路を介する以外の他の装置との間でのライセンスデータのやり取りが制限されるよう構成されている。

【０００５】

なお、ライセンスデータ取得時には、メモリカードはサーバ装置と通信可能な端末装置に装着され、端末装置を介してサーバ装置からライセンスデータを受信する。また、コンテンツ利用時には、メモリカードはデコーダを内蔵した端末装置に装着され、端末装置を介してデコーダへライセンスデータを送信する。

【０００６】

以上のように、コンテンツ配信サービスにおいては、コンテンツデータの暗号化と、ライセンスデータの秘匿によって、コンテンツに係る著作権保護の徹底が図られている。そして、このようにコンテンツ著作権の保護の徹底を図ることにより、配信対象のコンテンツを安心してラインアップに加えることができ、その結果として、配信サービスを受けるユーザのニーズを、より広範に満たし得るようになる。

【特許文献１】特開２００４－１３３６５４号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

高精細テレビに対応した映像コンテンツが台頭しつつある。ここでは、高精細テレビ画質の映像コンテンツをＨＤコンテンツと呼び、従来のテレビ画質の映像コンテンツをＳＤコンテンツと呼ぶ。

【０００８】

ＨＤコンテンツは、単位時間当たりのデータ量がＳＤコンテンツに比べて多い。たとえば、デジタル放送で利用されるＭＰＥＧ２方式では、ＳＤコンテンツの単位時間当たりのデータ量に対してＨＤコンテンツの単位時間当たりのデータ量は、約３倍である。したがって、ＨＤコンテンツを記録するストレージデバイスに対しては、更なる高速アクセスが要求されている。

【０００９】

一方、このようなＨＤコンテンツに対して従来システムの著作権保護機能を利用することを検討する。従来システムでは、ライセンスデータの送受信に公開鍵暗号を用いている。この公開鍵暗号の演算時間は、共通鍵暗号の演算時間に比して時間を要するため、１つのライセンスの送信又は受信に要する時間は、この公開鍵暗号の演算時間を必要とする。

【００１０】

番組などの単位でライセンスデータを記録し、番組単位で再生を行う場合、ライセンスデータのアクセス頻度は低く、アクセス時間はそれほど問題にはならないが、特殊再生（スキップ再生、複数の番組を部分的に連続させるプログラム再生など）を提供する場合には、ライセンスデータのアクセス頻度が高まり、ライセンスデータにもより高速なアクセスが求められるようになる。

【００１１】

本発明はこうした状況に鑑みてなされたものであり、その目的は、記憶装置とホスト装置との間で秘匿すべきデータを暗号化して入出力するとき、そのアクセス時間の短縮を図ろうとするものである。

【課題を解決するための手段】

【００１２】

上記課題に鑑み、本発明はそれぞれ以下の特徴を有する。

【００１３】

本発明のある態様は、コンテンツ利用情報送信方法に関する。このコンテンツ利用情報送信方法は、暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報を送受信する方法であって、前記コンテンツ利用情報の送信元が前記コンテンツ利用情報の送信先を認証するステップと、前記送信先が承認された場合に、前記送信元と前記送信先の間で第１の対称鍵を共有するステップと、前記送信元が、前記コンテンツ利用情報を暗号化して前記送信先へ送信するステップと、を含み、前記第１の対称鍵を共有するステップは、Elliptic Curve Diffie-Hellman暗号アルゴリズムにより、前記送信先の公開鍵を用いて、前記第１の対称鍵を前記送信先との間で共有するためのデータを生成するステップと、前記データを相手の装置に送信するステップと、を含み、前記コンテンツ利用情報を送信するステップは、前記コンテンツ利用情報を送信するタイミングが到来したときに、前記送信元と前記送信先の間で第２の対称鍵を共有するステップと、前記第１の対称鍵及び前記第２の対称鍵により前記コンテンツ利用情報を暗号化して前記送信先へ送信するステップと、を含むことを特徴とする。

【００１４】

これにより、楕円曲線上の演算を利用した公開鍵暗号方式を用いて安全に対称鍵（シェアード鍵）を共有することができる。また、いったん共有した対称鍵を継続して保持し、ライセンスデータの暗号化及び復号に利用することにより、ライセンスデータを送受信する際の演算量を低減させることができ、処理を高速化することができるとともに、回路規模を低減することができる。また、コンテンツ利用情報のような秘匿すべきデータを送受信する際に、いったん暗号通信路を確立した後は、公開鍵暗号アルゴリズムを用いず、共通鍵暗号アルゴリズムのみを用いてデータを暗号化して送受信することができる。共通鍵暗号アルゴリズムは、公開鍵暗号アルゴリズムに比べて演算量が少なく、ハードウェア化も容易であるから、共通鍵暗号アルゴリズムのみを用いることで、処理効率及び処理速度を向上させることができる。また、コンテンツ利用情報を第１の対称鍵と第２の対称鍵で二重に暗号化して送受信するので、安全性を損なわずに効率よく暗号化データを送受信することができる。

【００１５】

前記第１の対称鍵は、前記コンテンツ利用情報を送信するステップの終了後も、前記送信元及び前記送信先において保持されて、次にコンテンツ利用情報を送信するときに利用されてもよい。前記コンテンツ利用情報を送信するタイミングが到来したときに、既に前記第１の対称鍵が前記送信元と前記送信先の間で共有されている場合には、前記認証するステップ及び前記第１の対称鍵を共有するステップを省略してもよい。これにより、コンテンツ利用情報を繰り返して送受信する場合に、安全性を損なうことなく、迅速に暗号化して送受信することができる。また、継続的にコンテンツ利用情報を送受信する際には、認証処理を省略することにより、安全性を損なわずに処理を高速化することができる。前記送信先を再度認証する必要が生じたときには、既に共有していた前記第１の対称鍵は破棄され、前記第１の対称鍵を共有するステップは、新たに発行された前記第１の対称鍵を

共有してもよい。例えば、装置間の接続が解除されたり、一方の電源がオフになったりして、いったん確立された暗号通信路を維持することができなくなったときに、第１の対称鍵を破棄し、暗号通信路を切断してもよい。これにより、暗号通信の安全性を確保することができる。

【００１６】

前記第２の対称鍵は、前記コンテンツ利用情報を送受信するステップの終了後に、次のコンテンツ利用情報を送信するときには新たに発行され、前記送信元及び前記送信先の間で共有されてもよい。コンテンツ利用情報を送信するたびに、新たに発行された第２の対称鍵でコンテンツ利用情報を暗号化するので、コンテンツ利用情報の漏洩を防止することができ、安全性を高めることができる。

【００１７】

前記第１の対称鍵は、前記送信元及び前記送信先のうちいずれか一方が発行し、前記第２の対称鍵は、他方が発行してもよい。これにより、いずれか一方が不正な装置であった場合でも、コンテンツ利用情報の漏洩を防止することができるので、安全性を高めることができる。

【００１８】

コンテンツ利用情報送信方法は、前記第２の対称鍵を共有するために使用する第３の対称鍵を前記送信元と前記送信先との間で共有するステップを更に含んでもよく、前記第２の対称鍵を共有するステップは、前記第２の対称鍵を前記第３の対称鍵で暗号化して送受信することにより前記第２の対称鍵を共有してもよい。第３の対称鍵は、公開鍵暗号方式を用いて共有されてもよい。前記第３の対称鍵は、前記コンテンツ利用情報を送信するステップの終了後も、前記送信元及び前記送信先において保持されて、次に前記第２の対称鍵を共有するときに利用されてもよい。これにより、いったん暗号通信路を確立した後は、公開鍵暗号アルゴリズムを用いず、共通鍵暗号アルゴリズムのみを用いてデータを暗号化して送受信することができるので、処理効率及び処理速度を向上させることができる。

【００１９】

前記送信先を再度認証する必要が生じたときには、既に共有していた前記第３の対称鍵は破棄され、前記第３の対称鍵を共有するステップは、新たに発行された前記第３の対称鍵を共有してもよい。これにより、暗号通信の安全性を確保することができる。

【００２０】

本発明の別の態様は、コンテンツ利用情報提供装置に関する。このコンテンツ利用情報提供装置は、暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報享受装置に提供するコンテンツ利用情報提供装置であって、前記コンテンツ利用情報享受装置から認証情報を取得して、その認証情報の正当性を検証する検証手段と、前記検証手段が前記コンテンツ利用情報享受装置を承認したときに、前記コンテンツ利用情報享受装置との間で公開鍵暗号方式を用いて第１の対称鍵を共有する第１の対称鍵共有手段と、前記コンテンツ利用情報を送信するタイミングが到来したときに、前記ライセンス利用情報享受装置との間で第２の対称鍵を共有する第２の対称鍵共有手段と、前記コンテンツ利用情報を前記第１の対称鍵及び前記第２の対称鍵により暗号化する暗号化手段と、前記暗号化手段により暗号化された前記コンテンツ利用情報享受装置へ送信するコンテンツ利用情報送信手段と、を備え、前記第１の対称鍵共有手段は、乱数を発生する乱数発生手段と、Elliptic Curve Diffie-Hellman暗号アルゴリズムにより前記乱数と前記コンテンツ利用情報享受装置の公開鍵を用いて前記第１の対称鍵を生成するとともに、前記第１の対称鍵を前記コンテンツ利用情報享受装置との間で共有するためのデータを生成する第１の対称鍵生成手段と、前記データを前記コンテンツ利用情報享受装置に送信する送信手段と、を含むことを特徴とする。

【００２１】

本発明の更に別の態様は、コンテンツ利用情報享受装置に関する。このコンテンツ利用情報享受装置は、暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報提供装置から享受するコンテンツ利用情報享受装置であ

って、前記コンテンツ利用情報提供装置に自身の認証情報を送信する認証情報送信手段と、前記コンテンツ利用情報提供装置が前記認証情報を承認したときに、前記コンテンツ利用情報提供装置との間で公開鍵暗号方式を用いて第１の対称鍵を共有する第１の対称鍵共有手段と、前記コンテンツ利用情報を受信するタイミングが到来したときに、前記コンテンツ利用情報提供装置との間で第２の対称鍵を共有する第２の対称鍵共有手段と、前記第１の対称鍵及び前記第２の対称鍵により暗号化された前記コンテンツ利用情報を前記コンテンツ利用情報提供装置から受信するコンテンツ利用情報受信手段と、前記暗号化された前記コンテンツ利用情報を復号する復号手段と、を備え、前記第１の対称鍵共有手段は、

前記コンテンツ利用情報提供装置に自身の公開鍵を提供する公開鍵提供手段と、前記第１の対称鍵を前記コンテンツ利用情報提供装置との間で共有するためのデータを取得する取得手段と、Elliptic Curve Diffie-Hellman暗号アルゴリズムにより前記データと前記公開鍵と対をなす秘密鍵とを用いて前記第１の対称鍵を生成する第１の対称鍵生成手段と、を含むことを特徴とする。

【００２２】

本発明の更に別の態様は、コンテンツ利用情報提供装置に関する。このコンテンツ利用情報提供装置は、暗号化されたコンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報享受装置に提供するコンテンツ利用情報提供装置であって、前記コンテンツ利用情報享受装置との間でデータの授受を制御するインタフェースと、前記コンテンツ利用情報享受装置との通信においてテンポラルに生成する第１の対称鍵を生成する対称鍵生成部と、前記コンテンツ利用情報享受装置に設定された第１の公開鍵によって、データを暗号化する第１の暗号部と、前記対称鍵生成部により生成された第１対称鍵によってデータを復号する復号部と、前記コンテンツ利用情報享受装置に設定された楕円曲線暗号の第２の公開鍵を用いて、Ｅｌｌｉｐｔｉｃ　ｃｕｒｖｅ　Ｄｉｆｆｉｅ　－　Ｈｅｌｌｍａｎ暗号アルゴリズムにしたがい、データを暗号化する第２の暗号部と、前記第２の暗号部に供給する乱数を生成する乱数生成部と、前記コンテンツ利用情報享受装置で生成された第２の対称鍵によってデータを暗号化する第３の暗号部と、制御部とを備え、前記第２の暗号部は、前記乱数生成部において生成された乱数を取得し、前記取得した乱数と前記第２の公開鍵に基づいて、暗号化に用いるシェアード鍵と、このシェアード鍵を前記コンテンツ利用情報享受装置と共有するためのデータとを生成する機能と、前記生成したシェアード鍵によって前記コンテンツ利用情報を暗号化する機能を有し、前記対称鍵生成部において前記第１の対称鍵が生成されて初めての前記第２の公開鍵による暗号化処理において、前記乱数生成部において生成された乱数を取得し、前記取得した乱数と前記第２の公開鍵に基づいて、暗号化に用いるシェアード鍵と、このシェアード鍵を前記コンテンツ利用情報享受装置と共有するためのデータとを生成し、前記シェアード鍵によってデータを暗号化し、前記対称鍵生成部において前記第１の対称鍵が生成されて２回目以降の暗号化処理において、前回のシェアード鍵によって前記コンテンツ利用情報を暗号化し、前記制御部は、前記第１の対称鍵を生成するように前記対称鍵生成部を制御し、前記第１の公開鍵によって暗号化された前記第１の対称鍵を前記第１の暗号部から受け取って、前記インタフェースを介して前記コンテンツ利用情報享受装置へ送信し、前記インタフェースを介して受信した前記第１の対称鍵によって暗号化された前記第２の対称鍵および前記第２の公開鍵を、前記コンテンツ利用情報享受装置から受け取って前記復号部に与え、前記復号部で復号した第２の公開鍵に基づいて生成されたシェアード鍵と第２の対称鍵とによって暗号化された暗号化コンテンツ利用情報を前記第２の暗号部または前記第３の暗号部から受け取って、前記インタフェースを介して前記コンテンツ利用情報享受装置へ送信することを特徴とする。

【００２３】

コンテンツ利用情報提供装置は、前記コンテンツ利用情報を生成し、かつ、生成したコンテンツ利用情報に含まれる前記コンテンツ鍵でコンテンツデータを暗号化するコンテンツ暗号部をさらに備えてもよく、前記制御部は、前記コンテンツ暗号部が生成した前記コンテンツ利用情報を取得し、前記第３の暗号部に与えてもよい。

【００２４】
コンテンツ利用情報提供装置は、前記コンテンツ利用情報を記憶する記憶部をさらに備えてもよく、前記制御部は、前記記憶部から、前記記憶部に格納されている前記コンテンツ利用情報を取得し、前記第３の暗号部に与えてもよい。
【００２５】
前記記憶部は、前記暗号化コンテンツデータを格納する第１の格納部と、前記コンテンツ利用情報を格納する第２の格納部とを含んでもよく、前記第２の格納部は、機密性の高い耐タンパ構造によって構成されてもよい。
【００２６】
本発明の更に別の態様は、コンテンツ利用情報享受装置に関する。このコンテンツ利用情報享受装置は、暗号化コンテンツデータを復号および再生するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報提供装置から享受するコンテンツ利用情報享受装置であって、前記コンテンツ利用情報提供装置との間でデータの授受を制御するインタフェースと、前記コンテンツ利用情報享受装置に設定された第１の公開鍵によって暗号化されたデータを復号するための第１の秘密鍵を保持する第１秘密鍵保持部と、前記コンテンツ利用情報享受装置に設定された楕円曲線暗号の第２の公開鍵を保持する第２公開鍵保持部と、前記第２の公開鍵によって暗号化されたデータを復号するための第２の秘密鍵を保持する第２秘密鍵保持部と、前記第１の公開鍵によって暗号化されたデータを前記第１の秘密鍵で復号する第１の復号部と、前記コンテンツ利用情報提供装置で生成された第１の対称鍵によって、データを暗号化する暗号部と、前記コンテンツ利用情報提供装置との通信を特定するための第２の対称鍵を生成する対称鍵生成部と、前記第２の対称鍵で暗号化されたデータを復号する第２の復号部と、前記第２の公開鍵によって暗号化されたデータを前記第２の秘密鍵によってＥｌｌｉｐｔｉｃ　ｃｕｒｖｅ　Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ暗号アルゴリズムにしたがってデータを復号する第３の復号部と、制御部とを備え、前記第３の復号部は、前記コンテンツ利用情報提供装置から取得したシェアード鍵を共有するためのデータと前記第２の秘密鍵に基づいて前記シェアード鍵を生成する機能と、前記シェアード鍵で暗号化されたデータを復号する機能とを有し、前記第１の復号部において前記第１の対称鍵が復号されて初めて受け取った前記第２の公開鍵で暗号化されたデータを復号する復号処理において、前記共有するためのデータと前記第２の秘密鍵に基づいて前記シェアード鍵を生成した後、そのシェアード鍵を用いて暗号化されたデータを復号し、前記第１の復号部において前記第１の対称鍵が復号されて２回目以降の復号処理において、前回の復号に使用したシェアード鍵を用いて暗号化されたデータを復号し、前記制御部は、前記第１の公開鍵によって暗号化された前記第１の対称鍵を前記インタフェースから受け取り、その受け取った前記暗号化された第１の対称鍵を前記第１の復号部に与え、前記第２の対称鍵を生成するように前記対称鍵生成部を制御し、前記暗号部において前記第１の対称鍵によって暗号化された前記第２の対称鍵と前記第２の公開鍵とを前記インタフェースを介して前記コンテンツ利用情報提供装置へ送信し、前記インタフェースを介して受信した前記第２の公開鍵および前記第２の対称鍵によって暗号化された暗号化コンテンツ利用情報を、前記第２の復号部に与えることを特徴とする。
【００２７】
コンテンツ利用情報享受装置は、前記第３の復号部で取り出された前記コンテンツ利用情報に含まれる前記コンテンツ鍵によって、前記暗号化コンテンツデータを復号してコンテンツデータを再生するコンテンツ再生部をさらに備えてもよい。
【００２８】
コンテンツ利用情報享受装置は、前記コンテンツ利用情報を記憶する記憶部をさらに備えてもよく、前記制御部は、前記第３の復号部で取り出された前記コンテンツ利用情報を、前記記憶部に格納してもよい。
【００２９】
本発明の特徴ないしその技術的意義は、以下に示す実施の形態の説明により更に明らかとなろう。ただし、以下の実施の形態は、あくまでも、本発明の一つの実施形態であって

、本発明ないし各構成要件の用語の意義等は、以下の実施の形態に記載されたものに制限されるものではない。

【発明の効果】

【００３０】

本発明によれば、ストレージデバイスとホスト装置との間で秘匿すべきデータを暗号化して入出力するときの処理効率を向上させることができる。

【発明を実施するための最良の形態】

【００３１】

（第１の実施の形態）

図１は、第１の実施の形態に係るデータ管理システム１０の全体構成を示す。データ管理システム１０は、ストレージデバイス２００へのデータの記録を制御する記録装置１００、ストレージデバイス２００に記録されたデータの再生を制御する再生装置３００、およびデータを記録保持するストレージデバイス２００を備える。本実施の形態のストレージデバイス２００は、データを保持する記憶媒体だけでなく、記録装置１００または再生装置３００などのホスト装置と記憶媒体との間でのデータの入出力を制御するコントローラなどの構成を備えるドライブ一体型のストレージデバイスである。本実施の形態では、ストレージデバイス２００として、ハードディスクドライブを例にとって説明する。

【００３２】

従来のハードディスクドライブは、一つのホスト装置に固定的に接続されて使用されるのが一般的であったが、本実施の形態のストレージデバイス２００は、記録装置１００および再生装置３００などのホスト装置に対して着脱自在に構成されている。すなわち、本実施の形態のストレージデバイス２００は、ＣＤやＤＶＤなどと同様にホスト装置から取り外して持ち運ぶことができ、記録装置１００、再生装置３００、記録および再生が可能な記録再生装置など、複数のホスト装置間で共用することが可能な記憶装置である。

【００３３】

このように、本実施の形態のストレージデバイス２００は、複数のホスト装置に接続されることを前提にしており、たとえば所有者以外の第三者のホスト装置に接続されて、内部に記録されたデータを読み出される可能性もある。このストレージデバイス２００に、音楽や映像などの著作権により保護されるべきコンテンツ、企業や個人の機密情報などの秘匿すべきデータを記録することを想定したとき、それらの秘匿データが外部に漏洩することを防ぐためには、ストレージデバイス２００自身にデータを適切に保護するための構成を設け、十分な耐タンパ機能を持たせることが好ましい。

【００３４】

このような観点から、本実施の形態のストレージデバイス２００は、ホスト装置との間で秘匿データを入出力するときに、その秘匿データを暗号化してやり取りするための構成を備える。また、秘匿データを格納するために、通常の記憶領域とは異なる機密データ記憶領域を設け、その機密データ記憶領域はストレージデバイス２００内に設けられた暗号エンジンを介さないとアクセスできないように構成する。この暗号エンジンは、正当な権限を有すると検証されたホスト装置のみと秘匿データの入出力をする。以下、このようなデータ保護機能を「セキュア機能」ともいう。上記の構成および機能により、ストレージデバイス２００に記録された秘匿データを適切に保護することができる。

【００３５】

ストレージデバイス２００のリムーバブルメディアとしての特徴を最大限に生かすため、通常のデータについては、セキュア機能に非対応のホスト装置でも入出力可能とするのが好ましい。そのため、本実施の形態のストレージデバイス２００は、従来のハードディスクとの互換性を保つべく、ＡＮＳＩ（American National Standards Institute）の標準規格であるＡＴＡ（AT Attachment）に対応しており、上述のセキュア機能は、ＡＴＡの拡張命令として実現される。

【００３６】

以下、秘匿データの入出力の例として、映像などのコンテンツデータを記録再生する場

合について説明する。コンテンツデータ自身を秘匿データとして扱ってもよいが、本実施の形態では、コンテンツデータを暗号化し、暗号化されたコンテンツデータ自身は、ストレージデバイス２００に通常のデータとして記録する。そして、暗号化されたコンテンツを復号するための鍵（コンテンツ鍵と呼ぶ）と、コンテンツの再生制御やライセンスの利用、移動、複製に関する制御に関する情報（利用規則と呼ぶ）を含むデータ（ライセンスデータと呼ぶ）を、秘匿データとして上述のセキュア機能を用いて入出力を行う。これにより、十分な耐タンパ性を維持しつつ、データの入出力を簡略化し、処理の高速化および消費電力の低減を図ることができる。ここで、ライセンスデータは、コンテンツ鍵や利用規則の他に、ライセンスデータを特定するためのライセンスＩＤなどを含む。

【００３７】

以下、記録装置１００、再生装置３００などのホスト装置がストレージデバイス２００に対して発行する命令のうち、セキュア機能のための拡張命令を「セキュアコマンド」とも呼び、その他の命令を「通常コマンド」とも呼ぶ。

【００３８】

図２は、実施の形態に係る記録装置１００の内部構成を示す。この構成は、ハードウエア的には、任意のコンピュータのＣＰＵ、メモリ、その他のＬＳＩなどで実現でき、ソフトウエア的にはメモリにロードされた記録制御機能のあるプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロックがハードウエアのみ、ソフトウエアのみ、またはそれらの組合せによっていろいろな形で実現できることは、当業者には理解されるところである。

【００３９】

記録装置１００は、主に、コントローラ１０１、ストレージインタフェース１０２、暗号エンジン１０３、暗号器１０４、コンテンツエンコーダ１０５、およびそれらを電気的に接続するデータバス１１０を備える。

【００４０】

コンテンツエンコーダ１０５は、オンラインまたはオフラインにより取得したコンテンツを所定の形式にコーディングする。ここでは、放送波などから取得した映像データをＭＰＥＧ形式にコーディングする。

【００４１】

暗号器１０４は、暗号化コンテンツを復号するためのコンテンツ鍵を含むライセンスデータＬＩＣを発行し、このコンテンツ鍵を用いて、コンテンツエンコーダ１０５にてコーディングされたコンテンツを暗号化する。暗号化されたコンテンツは、データバス１１０およびストレージインタフェース１０２を介してストレージデバイス２００に記録される。発行されたライセンスデータＬＩＣは、暗号エンジン１０３に通知され、暗号エンジン１０３を介してストレージデバイス２００に記録される。

【００４２】

暗号エンジン１０３は、ライセンスデータＬＩＣをストレージデバイス２００に入力するために、ストレージデバイス２００との間で暗号通信の制御を行う。ストレージインタフェース１０２は、ストレージデバイス２００とのデータの入出力を制御する。コントローラ１０１は、記録装置１００の構成要素を統括的に制御する。

【００４３】

図３は、実施の形態に係る再生装置３００の内部構成を示す。これらの機能ブロックも、ハードウエアのみ、ソフトウエアのみ、またはそれらの組合せによっていろいろな形で実現できる。

【００４４】

再生装置３００は、主に、コントローラ３０１、ストレージインタフェース３０２、暗号エンジン３０３、復号器３０４、コンテンツデコーダ３０５、およびそれらを電気的に接続するデータバス３１０を備える。

【００４５】

ストレージインタフェース３０２は、ストレージデバイス２００とのデータの入出力を

制御する。暗号エンジン３０３は、コンテンツ鍵を含むライセンスデータＬＩＣをストレージデバイス２００から受信するために、ストレージデバイス２００との間で暗号通信の制御を行う。

【００４６】

復号器３０４は、ストレージデバイス２００から読み出した暗号化されたコンテンツを、ストレージデバイス２００から入手したライセンスデータＬＩＣに含まれるコンテンツ鍵により復号する。

【００４７】

コンテンツデコーダ３０５は、復号器３０４により復号されたコンテンツをデコードして出力する。たとえば、ＭＰＥＧ形式のコンテンツであれば、コンテンツから映像信号と音声信号を復元し、映像信号を図示しない表示装置に出力し、音声信号を図示しないスピーカに出力する。コントローラ３０１は、再生装置３００の構成要素を統括的に制御する。

【００４８】

図４は、実施の形態に係るストレージデバイス２００の内部構成を示す。ストレージデバイス２００は、主に、コントローラ２０１、ストレージインタフェース２０２、暗号エンジン２０３、耐タンパ記憶部２０４、通常データ記憶部２０５、およびそれらを電気的に接続するデータバス２１０を備える。

【００４９】

ストレージインタフェース２０２は、記録装置１００および再生装置３００とのデータの入出力を制御する。暗号エンジン２０３は、コンテンツ鍵を含むライセンスデータＬＩＣなどの秘匿データを記録装置１００および再生装置３００との間で入出力するための暗号通信の制御を行う。通常データ記憶部２０５は、暗号化されたコンテンツや通常のデータなどを記録する通常記憶領域である。耐タンパ記憶部２０４は、コンテンツ鍵を含むライセンスデータＬＩＣなどの秘匿データを記録する機密データ記憶領域である。コントローラ２０１は、ストレージデバイス２００の構成要素を統括的に制御する。通常データ記憶部２０５は、外部から直接アクセス（データの入出力）が行われるが、耐タンパ記憶部２０４は、暗号エンジン２０３を介さないとアクセス（データの入出力）ができないように構成される。

【００５０】

ここで、本実施の形態で用いる鍵について説明する。本実施の形態では、鍵はすべて大文字の「Ｋ」から始まる文字列として表記する。

【００５１】

第２文字が小文字の「ｃ」あるいは「ｓ」である場合は対称鍵（共通鍵）を表す。「ｃ」の場合はチャレンジ鍵であり、暗号化データの送信元で生成されるテンポラルな対称鍵である。「ｓ」の場合はセッション鍵であり、暗号化データの送信先で生成されるテンポラルな対称鍵である。

【００５２】

第２文字が大文字の「Ｐ」である場合は、公開鍵暗号方式の公開鍵を示す。この鍵には対応する秘密鍵が必ず存在し、この秘密鍵は公開鍵の表記から第２文字の大文字の「Ｐ」を除く表記となる。

【００５３】

鍵を示す文字列が小文字の「ｄ」を含む場合は、装置のグループ毎に与えられた鍵であることを表す。また鍵を示す文字列が小文字「ｐ」を含む場合は、装置毎に与えられた鍵であることを表す。それぞれは、公開鍵と秘密鍵の対として与えられ、グループ毎に与えられた公開鍵は、電子署名付きの公開鍵証明書として与えられている。

【００５４】

鍵を示す文字列の最後に記載される文字、たとえば、公開鍵ＫＰｄ２の「２」は、その鍵が与えられる暗号エンジンを識別するための記号である。本実施の形態では、提供先が明確な場合には、「１」、「２」、「３」などの数字により表記し、当該暗号エンジン以

外から提供される鍵であって提供先が不明な場合あるいは特定しない場合には、「ｘ」、「ｙ」などの英文字によって表記する。本実施の形態では、記録装置１００の暗号エンジン１０３に対しては識別記号として「１」、ストレージデバイス２００の暗号エンジン２０３については識別記号として「２」、再生装置３００の暗号エンジン３０３については識別記号として「３」をそれぞれ使用する。

【００５５】

ここで、実施の形態で用いる暗号アルゴリズムについて説明する。本実施の形態では、公開鍵暗号方式および対称鍵（共通）暗号方式の２つの方式から、１つずつ暗号アルゴリズムを採用する。

【００５６】

公開鍵暗号方式は、暗号および復号を異なった鍵を用いて行う暗号方式である。暗号化する鍵を公開鍵、復号する鍵を秘密鍵と呼ぶ。公開鍵はその名が示すとおり、公開可能な鍵であり、秘密に管理する必要がない。これに対して、秘密鍵は秘密に管理される。

【００５７】

この方式では、ＲＳＡ、ＥＣ－ＤＨ（Elliptic Curve Diffie-Hellman）などの暗号アルゴリズムが知られている。本実施の形態では、ＥＣ－ＤＨアルゴリズムを採用する。ＥＣ－ＤＨは、有限体上の楕円曲線における乗算（この演算アルゴリズムを楕円曲線暗号と呼ぶ）によって、双方で共有した対称鍵（シェアード鍵と呼ぶ）でデータを暗号化する。暗号化データは、データを暗号化した結果と、シェアード鍵を共有するためのデータ（パラメータと呼ぶ）を連結した形式となる。

【００５８】

たとえば、公開鍵ＫＰｄｘ、秘密鍵Ｋｄｘにおける暗号データの送信について説明する。ＥＣ－ＤＨでは、両者の関係は、ＫＰｄｘ＝Ｋｄｘ＊Ｂとなる。ここで、楕円曲線上のベースポイントを「Ｂ」、楕円曲線上の乗算を「＊」で示している。なお、以下の説明において、「ｘ」は暗号データを受け取る側（受信側と呼ぶ）を示し、「ｙ」は暗号データ提供する側（送信側とよぶ）を示す。

【００５９】

受信側は公開鍵ＫＰｄｘを、送信側に伝達する。送信側は、公開鍵ＫＰｄｘを受け取ると、暗号データを作成するために、まず、乱数ｒｄｙを生成する。そして、公開鍵ＫＰｄｘと、乱数ｒｄｙとを楕円曲線上で掛け合わせシェアード鍵ＫＰｄｘ＊ｒｄｙを演算によって求める。同時に、受信側とシェアード鍵ＫＰｄｘ＊ｒｄｙを共有するために、パラメータＢ＊ｒｄｙを演算する。なお、ベースポイントＢは、楕円曲線の方程式とともに事前に共有している。

【００６０】

生成したシェアード鍵ＫＰｄｘ＊ｒｄｙで、対象となるデータ（Ｄａｔａと記す）を暗号化し、暗号データＥｓ（ＫＰｄｘ＊ｒｄｙ，Ｄａｔａ）を生成する。そして、パラメータＢ＊ｒｄｙと、この結果を連結したＢ＊ｒｄｙ／／Ｅｓ（ＫＰｄｘ＊ｒｄｙ，Ｄａｔａ）をＥｐ（ＫＰｄｘ，Ｄａｔａ）として受信側に送る。

【００６１】

ここで、記号「／／」は、データの連結を示し、Ｂ＊ｒｄｙ／／Ｅｓ（ＫＰｄｘ＊ｒｄｙ，Ｄａｔａ）は、パラメータＢ＊ｒｄｙと暗号データＥｓ（ＫＰｄｘ＊ｒｄｙ，Ｄａｔａ）を並べて結合したデータ列を示す。また、Ｅｓは共通鍵暗号方式による暗号化関数を示し、Ｅｓ（ＫＰｄｘ＊ｒｄｙ，Ｄａｔａ）は、対称鍵ＫＰｄｘ＊ｒｄｙで対象となるデータＤａｔａを暗号化したものであることを示す。また、Ｅｐは公開鍵暗号方式による暗号化関数を示し、公開鍵ＫＰｄｘで対象となるデータＤａｔａを暗号化したものであることを示す。

【００６２】

このように、ＥＣ－ＤＨでは、Ｅｐ（ＫＰｄｘ，Ｄａｔａ）＝Ｂ＊ｒｄｙ／／Ｅｓ（ＫＰｄｘ＊ｒｄｙ、Ｄａｔａ）となる。

【００６３】

受信側では、Ｅｐ（ＫＰｄｘ，Ｄａｔａ）を受け取ると、保持している秘密鍵ＫｄｘとパラメータＢ＊ｒｄｙとを楕円曲線上で掛け合わせシェアード鍵Ｋｄｘ＊Ｂ＊ｒｄｙ＝ＫＰｄｘ＊ｒｄｙを求める。求めたシェアード鍵ＫＰｄｘ＊ｒｄｙで、暗号データＥｓ（ＫＰｄｘ＊ｒｄｙ、Ｄａｔａ）を復号する。なお、公開鍵ＫＰｐｘと秘密鍵Ｋｐｘの組についても同様である。

【００６４】

共通鍵暗号方式は同一の鍵によって暗号および復号を行う暗号方式であり、暗号アルゴリズムとしてＤＥＳ（Data Encryption Standard）、ＡＥＳ（Advanced Encryption Standard）などが知られている。本実施の形態では、いずれの方式も採用可能であるが、前述する公開鍵暗号方式での利用と暗号強度のバランスを考慮し、ＡＥＳを採用する。

【００６５】

図５は、図２に示した記録装置１００の暗号エンジン１０３の内部構成を示す。暗号エンジン１０３は、証明書検証部１２０、乱数発生部１２１、第１暗号部１２２、復号部１２３、第２暗号部１２４、第３暗号部１２５、およびこれらの構成要素の少なくとも一部を電気的に接続するローカルバス１３０を備える。

【００６６】

証明書検証部１２０は、ストレージデバイス２００から取得した証明書Ｃ［ＫＰｄ２］を検証する。証明書Ｃ［ＫＰｄ２］は、公開鍵ＫＰｄ２を含む平文の情報（「証明書本体」と呼ぶ）と、証明書本体に対して付される電子署名からなる。この電子署名は、証明書本体に対してハッシュ関数による演算（この演算処理を「ハッシュ演算」と呼ぶ）を施した結果を、第三者機関である認証局（図示せず）のルート鍵Ｋａによって暗号化したデータである。ルート鍵Ｋａは、認証局によって厳重に管理されている非公開な鍵であり、認証局の秘密鍵となる。証明書検証部１２０は、このルート鍵Ｋａと対をなす検証鍵ＫＰａを保持している。この検証鍵ＫＰａは証明書の正当性を検証する公開鍵である。

【００６７】

証明書の検証は、証明書の正当性と証明書の有効性によって判断する。証明書の正当性の確認は、検証すべき証明書の証明書本体に対するハッシュ関数の演算結果と、検証鍵ＫＰａで電子署名を復号した結果を比較する処理であり、両者が一致したとき、正当であると判断する。証明書検証部１２０は、無効となった証明書のリストである証明書破棄リスト（Certificate Revocation List：ＣＲＬと呼ぶ）を保持し、証明書の有効性について、このＣＲＬに検証すべき証明書が記載されていない場合に有効であると判断する。このように、証明書の正当性と有効性を判断し正当な証明書を承認する処理を検証と呼ぶ。

【００６８】

証明書検証部１２０は、検証に成功すると、ストレージデバイス２００の公開鍵ＫＰｄ２を取り出して第１暗号部１２２に伝達し、検証結果を通知する。検証に失敗した場合には、検証エラー通知を出力する。

【００６９】

乱数発生部１２１は、乱数を発生する。乱数は、疑似乱数であってもよい。ここでは、ストレージデバイス２００との間で暗号通信を行うために一時的に使用されるチャレンジ鍵Ｋｃ１と乱数ｒｄ１、ｒｐ１を生成する。暗号通信を行う度に、乱数であるチャレンジ鍵Ｋｃ１を生成することで、チャレンジ鍵Ｋｃ１を見破られる可能性を最小限に抑える。生成されたチャレンジ鍵Ｋｃ１は、第１暗号部１２２および復号部１２３に伝達される。また、乱数ｒｄ１、ｒｐ１は、それぞれ第１暗号部１２２、第２暗号部１２４に伝達され、ＥＤ－ＤＨによる暗号化に使用される。

【００７０】

第１暗号部１２２は、ストレージデバイス２００にチャレンジ鍵Ｋｃ１を通知するために、証明書検証部１２０により取り出されたストレージデバイス２００の公開鍵ＫＰｄ２でチャレンジ鍵Ｋｃ１を暗号化して、暗号化チャレンジ鍵Ｅｐ（ＫＰｄ２，Ｋｃ１）＝Ｂ＊ｒｄ１／／Ｅｓ（ＫＰｄ２＊ｒｄ１，Ｋｃ１）を生成する。暗号化には、乱数発生部１２１が生成した乱数ｒｄ１を使用する。

【００７１】
復号部１２３は、チャレンジ鍵Ｋｃ１で暗号化されたデータを復号する。ストレージデバイス２００で発行されたセッション鍵Ｋｓ２およびストレージデバイス２００の保持する公開鍵ＫＰｐ２は、セッション情報Ｅｓ（Ｋｃ１，Ｋｓ２／／ＫＰｐ２）としてストレージデバイス２００から供給されるため、復号部１２３は、乱数発生部１２１が発生したチャレンジ鍵Ｋｃ１を取得して、セッション情報Ｅｓ（Ｋｃ１，Ｋｓ２／／ＫＰｐ２）を復号し、セッション鍵Ｋｓ２および公開鍵ＫＰｐ２を取り出す。取り出された公開鍵ＫＰｐ２とセッション鍵Ｋｓ２は、それぞれ第２暗号部１２４、第３暗号部１２５に伝達される。

【００７２】
第２暗号部１２４は、暗号器１０４がコンテンツを暗号化する際に発行したコンテンツ鍵を含むライセンスデータＬＩＣを取得し、そのライセンスデータＬＩＣをライセンスデータの提供先、すなわち、ストレージデバイス２００の公開鍵ＫＰｐ２で暗号化したＥｐ（ＫＰｐ２、ＬＩＣ）＝Ｂ＊ｒｐ１／／Ｅｓ（ＫＰｐ２＊ｒｐ１，ＬＩＣ）を生成する。暗号化には、乱数発生部１２１が生成した乱数ｒｐ１を取得し、使用する。そして、Ｅｐ（ＫＰｐ２、ＬＩＣ）は、第３暗号部１２５に伝達される。

【００７３】
第３暗号部１２５は、第２暗号部１２４によって生成されたＥｐ（ＫＰｐ２，ＬＩＣ）を、さらに、ストレージデバイス２００で発行されたセッション鍵Ｋｓ２により暗号化し、暗号化ライセンスデータＥｓ（Ｋｓ２，Ｅｐ（ＫＰｐ２，ＬＩＣ））を生成する。

【００７４】
図５では、暗号エンジン１０３の構成要素のうち、証明書検証部１２０、第１暗号部１２２、復号部１２３、および第３暗号部１２５がローカルバス１３０により電気的に接続されており、ローカルバス１３０を介して記録装置１００のデータバス１１０に接続されている。各構成要素を接続する形態にはいろいろな変更例が考えられるが、本実施の形態では、乱数発生部１２１が発生したチャレンジ鍵Ｋｃ１、乱数ｒｄ１およびｒｐ１、ストレージデバイス２００から受け取ったセッション鍵Ｋｓ２が、直接データバス１１０に流れないよう配慮している。これにより、暗号エンジン１０３内で使用される各鍵が、記録装置１００の他の構成要素などを介して外部に漏洩することを防ぎ、セキュリティ性を向上させることができる。

【００７５】
図６は、図３に示した再生装置３００の暗号エンジン３０３の内部構成を示す。暗号エンジン３０３は、証明書出力部３２０、乱数発生部３２１、第１復号部３２２、暗号部３２３、第２復号部３２４、第３復号部３２５、およびこれらの構成要素の少なくとも一部を電気的に接続するローカルバス３３０を備える。

【００７６】
証明書出力部３２０は、再生装置３００の証明書Ｃ［ＫＰｄ３］を出力する。証明書は、証明書出力部３２０が保持してもよいし、図示しない証明書保持部に保持しておき、それを読み出してもよい。証明書は、再生装置３００の公開鍵ＫＰｄ３を含む証明書本体と、証明書本体に対して付される電子署名からなる。電子署名は、ストレージデバイス２００の証明書と同様に、認証局のルート鍵Ｋａにより暗号化される。

【００７７】
乱数発生部３２１は、ストレージデバイス２００との間で暗号通信を行うために一時的に使用されるセッション鍵Ｋｓ３を発生する。生成されたセッション鍵Ｋｓ３は、暗号部３２３および第２復号部３２４に伝達される。

【００７８】
第１復号部３２２は、公開鍵ＫＰｄ３によって暗号化されたデータを秘密鍵Ｋｄ３で復号する。再生時には、ストレージデバイス２００で発行されたチャレンジ鍵Ｋｃ２は、再生装置３００の公開鍵ＫＰｄ３により暗号化したチャレンジ情報Ｅｐ（ＫＰｄ３，Ｋｃ２）としてストレージデバイス２００から供給されるため、第１復号部３２２は、自身の秘

密鍵Ｋｄ３により復号して、チャレンジ鍵Ｋｃ２を取り出す。取り出されたチャレンジ鍵Ｋｃ２は、暗号部３２３に伝達される。

【００７９】

暗号部３２３は、第１復号部３２２により取り出されたチャレンジ鍵Ｋｃ２で、データの暗号化を行う。乱数発生部３２１で発生したセッション鍵Ｋｓ３と自身の公開鍵ＫＰｐ３を連結して、これを暗号化し、セッション情報Ｅｓ（Ｋｃ２，Ｋｓ３／／ＫＰｐ３）を生成する。

【００８０】

第２復号部３２４は、セッション鍵Ｋｓ３で暗号化されたデータを復号する。ライセンスデータは、公開鍵ＫＰｐ３およびセッション鍵Ｋｓ３により２重に暗号化された暗号化ライセンスデータＥｓ（Ｋｓ３，Ｅｐ（ＫＰｐ３，ＬＩＣ））としてストレージデバイス２００から供給されるため、第２復号部３２４は、乱数発生部３２１が発生したセッション鍵Ｋｓ３により復号して、その結果を第３復号部３２５に伝達される。

【００８１】

第３復号部３２５は、公開鍵ＫＰｐ３で暗号化されたデータの復号を行う。公開鍵ＫＰｐ３と対をなす秘密鍵Ｋｐ３で、第２復号部３２４の結果を復号し、ライセンスデータＬＩＣを取り出す。取り出されたライセンスデータＬＩＣは、復号器３０４に伝達され、復号器３０４はこのライセンスデータＬＩＣに含まれるコンテンツ鍵を用いて暗号化コンテンツを復号する。

【００８２】

図６に示した暗号エンジン３０３においても、各構成要素を接続する形態にはいろいろな変更例が考えられるが、本実施の形態では、乱数発生部３２１が発生したセッション鍵Ｋｓ３、公開鍵と対をなしている秘密鍵Ｋｄ３およびＫｐ３、ストレージデバイス２００から受け取ったセッション鍵Ｋｓ２が、データバス３１０上を流れないように構成することで、暗号エンジン３０３内で使用される復号鍵が外部に漏洩することを防ぐ。

【００８３】

図７は、図４に示したストレージデバイス２００の暗号エンジン２０３の内部構成を示す。これらの機能ブロックも、ハードウエアのみ、ソフトウエアのみ、またはそれらの組合せによっていろいろな形で実現できる。暗号エンジン２０３は、制御部２２０、乱数発生部２２１、証明書出力部２２２、証明書検証部２２３、第１復号部２２４、第１暗号部２２５、第２復号部２２６、第３復号部２２７、第２暗号部２２８、第４復号部２２９、第３暗号部２３０、第４暗号部２３１およびこれらの構成要素の少なくとも一部を電気的に接続するローカルバス２４０を備える。

【００８４】

制御部２２０は、ストレージデバイス２００のコントローラ２０１の指示に従って暗号エンジン２０３の内部の構成の制御および外部の構成との間でデータの入出力を仲介する。

【００８５】

乱数発生部２２１は、記録装置１００または再生装置３００との間の暗号通信に一時的に使用される乱数ｒｄ２およびｒｐ２、セッション鍵Ｋｓ２、チャレンジ鍵Ｋｃ２を、乱数演算によって発生する。具体的には、ストレージデバイス２００がライセンスデータを提供する場合、乱数ｒｄ２、ｒｐ２とチャレンジ鍵Ｋｃ２を生成し、ストレージデバイス２００がライセンスデータの提供を受ける場合、セッション鍵Ｋｓ２を生成する。

【００８６】

証明書出力部２２２は、ストレージデバイス２００の証明書Ｃ［ＫＰｄ２］を出力する。証明書は、証明書出力部２２２が保持してもよいし、ストレージデバイス２００の所定の記憶領域、たとえば耐タンパ記憶部２０４に保持しておき、それを読み出してもよい。証明書は、ストレージデバイス２００の公開鍵ＫＰｄ２を含む証明書本体と、証明書本体に付された電子署名とを含む。電子署名は、認証局のルート鍵Ｋａにより暗号化される。

【００８７】

証明書検証部２２３は、外部から提供された証明書の検証を行う。具体的には、記録装置１００から取得した証明書Ｃ［ＫＰｄ１］および再生装置３００から取得した証明書Ｃ［ＫＰｄ３］を認証鍵ＫＰａにより検証する。検証の詳細な処理は、先に説明を行ったので、ここでは説明を省略する。

【００８８】

第１復号部２２４は、自身の公開鍵ＫＰｄ２で暗号化されたデータを復号する。具体的には、記録時には、記録装置１００で発行されたチャレンジ鍵Ｋｃ１が、ストレージデバイス２００の公開鍵ＫＰｄ２で暗号化されチャレンジ情報Ｅｐ（ＫＰｄ２，Ｋｃ１）＝Ｂ＊ｒｄ１／／Ｅｓ（ＫＰｄ２＊ｒｄ１，Ｋｃ１）として記録装置１００から供給されるため、これを自身の秘密鍵Ｋｄ２で復号し、チャレンジ鍵Ｋｃ１を取り出す。取り出したチャレンジ鍵Ｋｃ１は、第１暗号部２２５に与えられる。

【００８９】

第１暗号部２２５は、記録装置１００が発行したチャレンジ鍵Ｋｃ１でデータを暗号化する。具体的には、具体的には、乱数発生部２２１が発生したセッション鍵Ｋｓ２と自身の公開鍵ＫＰｐ２を連結して、チャレンジ鍵Ｋｃ１で暗号化し、セッション情報Ｅｓ（Ｋｃ１，Ｋｓ２／／ＫＰｐ２）を生成する。

【００９０】

第２復号部２２６は、乱数発生部２２１が発生したセッション鍵Ｋｓ２で暗号化されたデータを復号する。具体的には、ライセンスデータＬＩＣが、公開鍵ＫＰｐ２およびセッション鍵Ｋｓ２により２重に暗号化された暗号化ライセンスデータＥｓ（Ｋｓ２，Ｅｐ（ＫＰｐ２，ＬＩＣ））として記録装置１００から受け取るため、これをセッション鍵Ｋｓ２により復号して、結果を第３復号部２２７に与える。

【００９１】

第３復号部２２７は、自身の公開鍵ＫＰｐ２で暗号化されたデータを復号する。第２復号部２２６から与えられる公開鍵ＫＰｐ２で暗号化されたライセンスデータＥｐ（ＫＰｐ２，ＬＩＣ）＝Ｂ＊ｒｐ１／／Ｅｓ（ＫＰｐ２＊ｒｐ１，ＬＩＣ）を、公開鍵ＫＰｐ２と対をなす自身の秘密鍵Ｋｐ２で復号し、ライセンスデータＬＩＣを取り出す。

【００９２】

取り出されたライセンスデータＬＩＣは、ローカルバス２４０、制御部２２０を介して、データバス２１０に供給され、コントローラ２０１の指示に従って、耐タンパ記憶部２０４に記憶される。

【００９３】

第２暗号部２２８は、再生装置３００の公開鍵ＫＰｄ３でデータを暗号化する。具体的には、再生装置３００に対してライセンスデータを提供する場合に、再生装置３００から受け取った証明書Ｃ［ＫＰｄ３］から取り出された公開鍵ＫＰｄ３で、乱数発生部２２１が生成したチャレンジ鍵Ｋｃ２を暗号化し、チャレンジ情報Ｅｐ（ＫＰｄ３，Ｋｃ２）＝Ｂ＊ｒｄ２／／Ｅｓ（ＫＰｄ３＊ｒｄ２，Ｋｃ２）を生成する。暗号化には、乱数発生部２２１が生成した乱数ｒｄ２を使用する。生成した暗号化チャレンジ鍵Ｅｐ（ＫＰｄ３，Ｋｃ２）は、ローカルバス２４０を介して制御部２２０へ与えられる。

【００９４】

第４復号部２２９は、乱数発生部２２１が生成したチャレンジ鍵Ｋｃ２で暗号化されたデータを復号する。再生装置３００から受け取ったセッション情報Ｅｓ（Ｋｃ２，Ｋｓ３／／ＫＰｐ３）を、乱数発生部２２１が生成したチャレンジ鍵Ｋｃ２で復号し、セッション鍵Ｋｓ３および再生装置３００の公開鍵ＫＰｐ３を取り出す。取り出されたセッション鍵Ｋｓ３と公開鍵ＫＰｐ３は、それぞれ第４暗号部２３１、第３暗号部２３０に伝達される。

【００９５】

第３暗号部２３０は、再生装置３００の公開鍵ＫＰｐ３でデータを暗号化する。再生装置３００に対してライセンスデータを提供する場合、再生装置３００から受け取った公開鍵ＫＰｐ３で、ライセンスデータＬＩＣを暗号化し、Ｅｐ（ＫＰｐ３，ＬＩＣ）＝Ｂ＊ｒ

ｐ２／／Ｅｓ（ＫＰｐ３＊ｒｐ２，ＬＩＣ）する。ライセンスデータは、コントローラ２０１の指示に従って、耐タンパ記憶部２０４から読み出され、データバス２１０、制御部２２０およびローカルバス２４０を介して第３暗号部２３０に供給される。また、暗号化には、乱数発生部２２１が生成した乱数ｒｐ２を使用する。

【００９６】

第４暗号部２３１は、再生装置３００が発行したセッション鍵Ｋｓ３でデータを暗号化する。具体的には、セッション鍵Ｋｓ３で、第３暗号部２３０において再生装置３００の公開鍵ＫＰｐ３で暗号化されたライセンスデータをさらに暗号化し、暗号化ライセンスデータＥｓ（Ｋｓ３，Ｅｐ（ＫＰｐ３，ＬＩＣ））を生成する。

【００９７】

図８および図９は、記録装置１００がストレージデバイス２００にライセンスデータＬＩＣを記録するまでの手順を示す。

【００９８】

まず、記録装置１００のコントローラ１０１は、ストレージデバイス２００に対して証明書出力命令を発行する（Ｓ１０２）。ストレージデバイス２００のコントローラ２０１は、証明書出力命令を正常に受理する（Ｓ１０４）と、暗号エンジン２０３に証明書の出力を命じ、暗号エンジン２０３から証明書Ｃ［ＫＰｄ２］を読み出して記録装置１００へ出力する（Ｓ１０６）。

【００９９】

コントローラ１０１は、ストレージデバイス２００から証明書Ｃ［ＫＰｄ２］を取得すると、それを記録装置１００の暗号エンジン１０３に送る（Ｓ１０８）。暗号エンジン１０３がストレージデバイス２００の証明書Ｃ［ＫＰｄ２］を受信すると（Ｓ１１０）、証明書検証部１２０は、検証鍵ＫＰａで証明書を検証する（Ｓ１１２）。証明書が承認されなかった場合（Ｓ１１２のＮ）、証明書検証部１２０は検証エラー通知をコントローラ１０１に送信する（Ｓ１９０）。コントローラ１０１は、エラー通知を受信すると（Ｓ１９２）、処理を異常終了する。

【０１００】

証明書が承認された場合（Ｓ１１２のＹ）、暗号エンジン１０３は、乱数発生部１２１においてチャレンジ鍵Ｋｃ１を生成し、生成したチャレンジ鍵Ｋｃ１を第１暗号部１２２と復号部１２３に伝達する。復号部１２３は、このチャレンジ鍵Ｋｃ１を内部に保持する（Ｓ１１４）。さらに、乱数発生部１２１は、乱数ｒｄ１を生成し、生成した乱数ｒｄ１を第１暗号部１２２に伝達する。第１暗号部１２２では、乱数ｒｄ１を用いて、シェアード鍵ＫＰｄ２＊ｒｄ１とパラメータＢ＊ｒｄ１を演算する（Ｓ１１６）。このシェアード鍵ＫＰｄ２＊ｒｄ１で、チャレンジ鍵Ｋｃ１を暗号化して、チャレンジ情報Ｅｐ（ＫＰｄ２，Ｋｃ１）＝Ｂ＊ｒｄ１／／Ｅｓ（ＫＰｄ２＊ｒｄ１，Ｋｃ１）を生成し、コントローラ１０１に伝達する（Ｓ１１８）。

【０１０１】

コントローラ１０１は、チャレンジ情報Ｅｐ（ＫＰｄ２，Ｋｃ１）を受信すると（Ｓ１２０）、ストレージデバイス２００に対してチャレンジ情報処理命令を発行する（Ｓ１２４）。ストレージデバイス２００では、コントローラ２０１がチャレンジ情報処理命令を受理すると、チャレンジ情報Ｅｐ（ＫＰｄ２，Ｋｃ１）の入力を要求する（Ｓ１２６）。記録装置１００のコントローラ１０１は、この要求に応じてチャレンジ情報Ｅｐ（ＫＰｄ２，Ｋｃ１）をストレージデバイス２００へ出力する（Ｓ１２８）。

【０１０２】

ストレージデバイス２００は、チャレンジ情報Ｅｐ（ＫＰｄ２，Ｋｃ１）を受理すると（Ｓ１３０）、暗号エンジン２０３では、第１復号部２２４が、チャレンジ情報Ｅｐ（ＫＰｄ２，Ｋｃ１）をパラメータＢ＊ｒｄ１と暗号化チャレンジ鍵Ｅｓ（ＫＰｄ２＊ｒｄ１，Ｋｃ１）に分解する。パラメータＢ＊ｒｄ１と自身の秘密鍵Ｋｄ２から、シェアード鍵Ｋｄ２＊Ｂ＊ｒｄ１（＝ＫＰｄ２＊ｒｄ１）を演算し（Ｓ１３２）、これで暗号化チャレンジ鍵Ｅｓ（ＫＰｄ２＊ｒｄ１，Ｋｃ１）を復号し、チャレンジ鍵Ｋｃ１を取り出す（Ｓ

１３４）。そして、第１復号部２２４にて取り出されたチャレンジ鍵Ｋｃ１は、第１暗号部２２５に保持される（Ｓ１３６）。

【０１０３】

一方、コントローラ１０１は、ストレージデバイス２００においてチャレンジ情報処理命令の処理が終了すると、ストレージデバイス２００に対してセッション情報生成命令を発行する（Ｓ１３８）。ストレージデバイス２００では、コントローラ２０１がセッション情報生成命令を受理すると（Ｓ１４０）、暗号エンジン２０３では制御部２２０の指示に従って、乱数発生部２２１がセッション鍵Ｋｓ２を生成し、生成したセッション鍵Ｋｓ２を第２復号部２２６および第１暗号部２２５に与える。そして、第２復号部２２６は、このセッション鍵Ｋｓ２を保持する（Ｓ１４２）。第１暗号部２２５は、このセッション鍵Ｋｓ２と自身の公開鍵ＫＰｐ２とを連結し、ステップＳ１３６で保持したチャレンジ鍵Ｋｃ１で暗号化して、セッション情報Ｅｓ（Ｋｃ１，Ｋｓ２／／ＫＰｐ２）を生成する（Ｓ１４４）。

【０１０４】

一方、記録装置１００のコントローラ１０１は、ストレージデバイス２００においてセッション情報生成命令の処理が終了すると、セッション情報出力命令を発行する（Ｓ１４６）。ストレージデバイス２００では、セッション情報出力命令を受理すると（Ｓ１４８）、コントローラ２０１が、暗号エンジン２０３からセッション情報Ｅｓ（Ｋｃ１，Ｋｓ２／／ＫＰｐ２）を読み出し、記録装置１００のコントローラ１０１へ出力する（Ｓ１５０）。

【０１０５】

記録装置１００のコントローラ１０１は、ストレージデバイス２００からセッション情報Ｅｓ（Ｋｃ１，Ｋｓ２／／ＫＰｐ２）を受信すると、それを暗号エンジン１０３に送る（Ｓ１５２）。暗号エンジン１０３が、コントローラ１０１からセッション情報Ｅｓ（Ｋｃ１，Ｋｓ２／／ＫＰｐ２）を受信すると（Ｓ１５４）、復号部１２３は、ステップＳ１１４で保持したチャレンジ鍵Ｋｃ１でセッション情報Ｅｓ（Ｋｃ１，Ｋｓ２／／ＫＰｐ２）を復号し、セッション鍵Ｋｓ２とストレージデバイス２００の公開鍵ＫＰｐ２を取り出し（Ｓ１５６）、それぞれ第３暗号部１２５、第２暗号部１２４に伝達する。

【０１０６】

つづいて、暗号エンジン１０３は、このライセンスデータの記録が、ステップＳ１１４のチャレンジ鍵Ｋｃ１保持後、初回の記録処理か、繰り返し記録による２回目以降の記録処理かを判断する（Ｓ１５８）。初回の処理の場合（Ｓ１５８のＹ）、暗号エンジン１０３は、乱数発生部１２１において乱数ｒｐ１を生成し、生成した乱数ｒｐ１を第２暗号部１２４に伝達する。第２暗号部１２４では、乱数ｒｐ１を用いて、シェアード鍵ＫＰｐ２＊ｒｐ１とパラメータＢ＊ｒｐ１を演算し、内部に保持する（Ｓ１６０）。

【０１０７】

一方、２回目以降の処理の場合（Ｓ１５８のＮ）、ステップＳ１６０をスキップし、すなわち、シェアード鍵ＫＰｐ２＊ｒｐ１とパラメータＢ＊ｒｐ１を生成せず、次のステップＳ１６２へ進む。

【０１０８】

第２暗号部１２４は、保持しているシェアード鍵ＫＰｐ２＊ｒｐ１で、暗号器１０４が発行したライセンスデータＬＩＣを暗号化して、暗号化ライセンスデータＥｐ（ＫＰｐ２，ＬＩＣ）＝Ｂ＊ｒｐ１／／Ｅｓ（ＫＰｐ２＊ｒｐ１，ＬＩＣ）を生成し、第３暗号部１２５に伝達する。そして、第３暗号部１２５は、第２暗号部１２４により生成された暗号化ライセンスデータＥｐ（ＫＰｐ２，ＬＩＣ）を、さらに、ストレージデバイス２００が発行したセッション鍵Ｋｓ２で暗号化し、暗号化ライセンスデータＥｓ（Ｋｓ２，Ｅｐ（ＫＰｐ２，ＬＩＣ））を生成し、コントローラ１０１に送る（Ｓ１６２）。

【０１０９】

このように、初回の場合（１５８のＹ）、新しくシェアード鍵ＫＰｐ２＊ｒｐ１とパラメータＢ＊ｒｐ１を生成する楕円曲線上での乗算、すなわち、公開鍵暗号方式による暗号

演算を行い、演算結果であるシェアード鍵ＫＰｐ２＊ｒｐ１とパラメータＢ＊ｒｐ１を用いてステップＳ１６２を実施し、暗号化ライセンスデータＥｓ（Ｋｓ２，Ｅｐ（ＫＰｐ２，ＬＩＣ））を生成し、コントローラ１０１に送る。

【０１１０】

一方、２回目以降の処理の場合（Ｓ１５８のＮ）、新たにシェアード鍵ＫＰｐ２＊ｒｐ１とパラメータＢ＊ｒｐ１を生成せず、ステップＳ１６０へ進み、初回の処理で作成し、第２暗号部１２４の内部に保持されたシェアード鍵ＫＰｐ２＊ｒｐ１とパラメータＢ＊ｒｐ１を用いて、ステップＳ１６２を実施し、暗号化ライセンスデータＥｓ（Ｋｓ２，Ｅｐ（ＫＰｐ２，ＬＩＣ））を生成し、コントローラ１０１に送る。すなわち、シェアード鍵ＫＰｐ２＊ｒｐ１とパラメータＢ＊ｒｐ１の生成を行わないため、楕円曲線上での乗算を省略でき、データの暗号化処理のみを行う。この場合の処理時間は、共通鍵暗号方式の暗号演算と同様であり、高速演算が可能である。このように、２回目以降の処理は、楕円曲線上での乗算を行う初回の処理と比べて、高速に処理することができる。

【０１１１】

コントローラ１０１は、暗号化ライセンスデータＥｓ（Ｋｓ２，Ｅｐ（ＫＰｐ２，ＬＩＣ））を受信すると（Ｓ１６４）、ストレージデバイス２００に対してライセンスデータ書込命令を発行する（Ｓ１６６）。ライセンス書込命令は、耐タンパ記憶部２０４における記録位置を指定するアドレスと、暗号化ライセンスデータを復号する時に、シェアード鍵生成の演算の有無を示す制御情報を伴っている。ここでアドレスとは、論理アドレスを示し、耐タンパ記憶部２０４における記録位置を直接指定するものではないが、アドレスを指定して記録したデータは、同じアドレスを指定することで読み出せるようにコントローラ２０１によって管理されている。しかしながら、直接、耐タンパ記憶部２０４における位置を示す物理アドレスであってもよい。

【０１１２】

ストレージデバイス２００は、ライセンス書込命令を受理すると（Ｓ１６８）、暗号化ライセンスデータの入力を要求し、記録装置１００のコントローラ１０１は、この要求に応じて、暗号化ライセンスデータＥｓ（Ｋｓ２，Ｅｐ（ＫＰｐ２，ＬＩＣ））をストレージデバイス２００へ出力する（Ｓ１７０）。

【０１１３】

ストレージデバイス２００は、暗号化ライセンスデータＥｓ（Ｋｓ２，Ｅｐ（ＫＰｐ２，ＬＩＣ））を受理すると（Ｓ１７２）、暗号エンジン２０３の第２復号部２２６に伝達する。第２復号部２２６は、内部に保持しているセッション鍵Ｋｓ２で暗号化ライセンスデータＥｓ（Ｋｓ２，Ｅｐ（ＫＰｐ２，ＬＩＣ））を復号し、自身の公開鍵ＫＰｐ２で暗号化されたライセンスデータＥｐ（ＫＰｐ２，ＬＩＣ）を取り出す（Ｓ１７４）。そして、取り出した暗号化されたライセンスデータＥｐ（ＫＰｐ２，ＬＩＣ）を第３復号部２２７に伝達する。

【０１１４】

そして、制御部２２０は、シェアード鍵の生成の有無を示す制御情報を確認する（Ｓ１７６）。生成が必要な場合、すなわち、このライセンスデータの記録が、ステップＳ１３６の共通鍵Ｋｃ１保持後、初回の記録処理の場合（Ｓ１７６のＹ）、第３復号部２２７は、伝達されたＥｐ（ＫＰｐ２，ＬＩＣ）＝Ｂ＊ｒｐ１／／Ｅｓ（ＫＰｐ２＊ｒｐ１，ＬＩＣ）から、パラメータＢ＊ｒｐ１を取り出し、パラメータＢ＊ｒｐ１と自身の秘密鍵Ｋｐ２から、シェアード鍵Ｋｐ２＊Ｂ＊ｒｐ１＝ＫＰｐ２＊ｒｐ１を楕円曲線上で演算し、これを内部に保持する（Ｓ１７８）。

【０１１５】

一方、シェアード鍵の演算が不要な場合、すなわち、２回目以降の処理の場合（Ｓ１７６のＮ）、ステップＳ１７８をスキップし、シェアード鍵Ｋｐ２＊Ｂ＊ｒｐ１を生成せず、次のステップＳ１８０へ進む。

【０１１６】

第３復号部２２７は、内部に保持する鍵Ｋｐ２＊Ｂ＊ｒｐ１で、第２復号部２２６から

伝達された暗号化されたライセンスデータＥｐ（ＫＰｐ２，ＬＩＣ）を復号してライセンスデータＬＩＣを取り出し（Ｓ１８０）、ローカルバス２４０、制御部２２０を介してデータバス２１０に伝達する。

【０１１７】

このように、初回の場合（１７６のＹ）、新しくシェアード鍵Ｋｐ２＊Ｂ＊ｒｐ１とを生成する楕円曲線上での乗算、すなわち、公開鍵暗号方式による暗号演算を行い、演算結果であるシェアード鍵ＫＰｐ２＊ｒｐ１で、暗号化ライセンスデータＥｐ（ＫＰｐ２，ＬＩＣ）を復号し、ライセンスデータＬＩＣを取り出す。

【０１１８】

一方、２回目以降の処理の場合（Ｓ１７６のＮ）、新たにシェアード鍵ＫＰｐ２＊ｒｐ１を生成せずにステップＳ１８０へ進み、初回の処理で作成し、第３復号部２２７に保持されたシェアード鍵Ｋｐ２＊Ｂ＊ｒｐ１を用いて、暗号化ライセンスデータＥｐ（ＫＰｐ２，ＬＩＣ）を復号し、ライセンスデータＬＩＣを取り出す。

【０１１９】

コントローラ２０１は、データバス２１０に伝達されたライセンスデータを耐タンパ記憶部２０４の指定されたアドレスに記憶する格納処理を行う（Ｓ１８２）。

【０１２０】

一方、コントローラ１０１は、ストレージデバイス２００においてライセンスデータ書込命令の処理が終了後、続けてライセンスデータを記録するか否か判断する（Ｓ１８４）。

【０１２１】

続けてライセンスデータを記録する場合（Ｓ１８４のＹ）、ステップＳ１３８に移行して、セッション情報の生成命令の発行から手順を開始する。これは、複数のライセンスデータを記録する場合に、証明書の検証処理および、公開鍵暗号方式による暗号演算および復号演算を複数の記録処理で共有し、続けてライセンスデータを記録する場合に、２回目以降の記録にかかる処理時間を短縮するための手順である。１つのライセンスデータの記録後、直ちに次のライセンスデータの記録を行わなければならないわけではない。暗号エンジン１０３とストレージデバイス２００が、チャレンジ鍵Ｋｃ１とシェアード鍵ＫＰｐ２＊ｒｐ１とパラメータＢ＊ｒｐ１を共有している、具体的には、記録装置１００の暗号エンジン１０３の復号部１２３と、ストレージデバイス２００の暗号エンジン２０３の第１暗号部２２５が、同じチャレンジ鍵Ｋｃ１を保持し、かつ、記録装置１００の暗号エンジン１０３の第２暗号部１２４と、ストレージデバイス２００の暗号エンジン２０３の第３復号部２２７が、同じシェアード鍵ＫＰｐ２＊ｒｐ１とパラメータＢ＊ｒｐ１をともに保持している状態であればいかなるタイミングであっても良い。

【０１２２】

また、続けてライセンスデータを記録する場合であっても、ステップＳ１０２から手順を開始してもよいが、２回目以降であっても、初回として扱われるために記録時に時間を要することになる。

【０１２３】

一方、続けてライセンスデータを記録しない場合（Ｓ１８４のＮ）、処理は正常終了する。

【０１２４】

以上の手順により、暗号化されたコンテンツを復号し再生するために必要なライセンスデータがストレージデバイス２００に記録される。暗号化コンテンツは、通常データであり、通常コマンドによって直接ストレージデバイス２００の通常データ記憶部２０５に記憶される。この通常データの記憶処理については、その説明を省略する。

【０１２５】

なお、ストレージデバイス２００へのライセンスデータと暗号化コンテンツデータの記録順序は、いずれが先であってもかまわない。さらには、暗号化コンテンツデータの記録時における、空き時間にセキュアコマンドを分割して発行することで、ライセンスデータ

を記録するようにしてもよい。

【０１２６】

また、ストレージデバイス２００の暗号エンジン２０３の制御部２２０において、初回の処理か、２回目以降の処理かを判断する手段として、ライセンス書込命令に、シェアード鍵生成の演算の有無を指示するように示したが、本実施の形態のように、シェアード鍵の演算の有無に関わらず、暗号化ライセンスデータにパラメータが含まれる場合、初回の処理時にパラメータを保持しておき、保持したパラメータと受理した暗号化ライセンスデータに含まれるパラメータの一致・不一致をもって、２回目以降か否かを判断してもよい。さらには、２回目以降は、暗号化ライセンスデータにパラメータを含まない形式とし、パラメータの有無によって判断するようにしてもよい。また、本実施の形態における暗号エンジン１０３と同様に、処理手順を内部で管理して判断してもよい。なお、暗号エンジン１０３における判断も同様にすることができる。

【０１２７】

なお、図８および図９に示した記録装置１００がストレージデバイス２００にライセンスデータを記録するまでの手順は、正常に処理が推移した場合の例である。

【０１２８】

図１０および図１１は、再生装置３００がストレージデバイス２００からライセンスデータを読み出すまでの手順を示す。

【０１２９】

まず、再生装置３００のコントローラ３０１は、暗号エンジン３０３に対して証明書の送信要求を行う（Ｓ３０２）。暗号エンジン３０３は、この送信要求を受け取ると（Ｓ３０４）、証明書出力部３２０により、証明書Ｃ［ＫＰｄ３］をコントローラ３０１へ送る（Ｓ３０６）。コントローラ３０１は、暗号エンジン３０３から証明書Ｃ［ＫＰｄ３］を受信すると（Ｓ３０８）、ストレージデバイス２００に対して証明書検証命令を発行する（Ｓ３１０）。

【０１３０】

ストレージデバイス２００は、証明書検証命令を受理すると（Ｓ３１２）、証明書の入力を要求し、再生装置３００のコントローラ３０１は、この要求に応じて、暗号エンジン３０３から受け取った証明書Ｃ［ＫＰｄ３］をストレージデバイス２００へ出力する（Ｓ３１４）。

【０１３１】

ストレージデバイス２００は、証明書Ｃ［ＫＰｄ３］を受理すると（Ｓ３１６）、証明書Ｃ［ＫＰｄ３］を内部の暗号エンジン２０３に与える。暗号エンジン２０３内では制御部２２０の指示に従って、証明書検証部２２３が、証明書Ｃ［ＫＰｄ３］を検証鍵ＫＰａで検証する（Ｓ３１８）。証明書が承認されなかった場合（Ｓ３１８のＮ）、証明書検証部２２３は検証エラー通知を制御部２２０、コントローラ２０１、ストレージインタフェース２０２を介して、コントローラ３０１に送信する（Ｓ４００）。再生装置３００のコントローラ３０１は、エラー通知を受信すると（Ｓ４０２）、処理を異常終了する。

【０１３２】

一方、証明書Ｃ［ＫＰｄ３］が承認された場合（Ｓ３１８のＹ）、暗号エンジン２０３は、公開鍵ＫＰｄ３を第２暗号部２２８に保持する（Ｓ３２０）。

【０１３３】

一方、再生装置３００のコントローラ３０１は、ストレージデバイス２００で、暗号エンジン３０３の証明書Ｃ［ＫＰｄ３］が承認されると、ストレージデバイス２００に対してチャレンジ情報生成命令を発行する（Ｓ３２２）。そして、ストレージデバイス２００は、チャレンジ情報生成命令を受理する（Ｓ３２４）。そして、暗号エンジン２０３内では制御部２２０の指示に従って、乱数発生部２２１がチャレンジ鍵Ｋｃ２を生成し、生成したチャレンジ鍵Ｋｃ２を第２暗号部２２８および第４復号部２２９に伝達する。そして、第４復号部２２９は、このチャレンジ鍵Ｋｃ２を内部に保持する（Ｓ３２６）。さらに乱数発生部２２１は、乱数ｒｄ２を生成し、生成した乱数ｒｄ２を第２暗号部２２８に伝

達する。そして、第２暗号部２２８は、ステップＳ３２０にて保持した公開鍵ＫＰｄ３と乱数ｒｄ２とを演算し、シェアード鍵ＫＰｄ３＊ｒｄ２およびパラメータＢ＊ｒｄ２を算出する（Ｓ３２８）。そして、乱数発生部２２１から伝達されたチャレンジ鍵Ｋｃ２を、演算したシェアード鍵ＫＰｄ３＊ｒｄ２で暗号化し、チャレンジ情報Ｅｐ（ＫＰｄ３，Ｋｃ２）を生成する（Ｓ３３０）。

【０１３４】

一方、コントローラ１０１は、ストレージデバイス２００においてチャレンジ情報生成命令の処理が終了すると、チャレンジ情報出力命令を発行する（Ｓ３３２）。そして、ストレージデバイス２００は、チャレンジ情報出力命令を受理すると（Ｓ３３４）、コントローラ２０１によって、暗号エンジン２０３からチャレンジ情報Ｅｐ（ＫＰｄ３，Ｋｃ２）を取り出し、再生装置３００のコントローラ３０１へ出力する（Ｓ３３６）。

【０１３５】

再生装置３００のコントローラ３０１は、チャレンジ情報Ｅｐ（ＫＰｄ３，Ｋｃ２）を受信すると、それを暗号エンジン３０３に送る（Ｓ３３８）。そして、暗号エンジン３０３が、チャレンジ情報Ｅｐ（ＫＰｄ３，Ｋｃ２）を受信すると（Ｓ３４０）、暗号エンジン３０３では、第１復号部３２２は、チャレンジ情報Ｅｐ（ＫＰｄ３，Ｋｃ２）をパラメータＢ＊ｒｄ２と暗号化チャレンジ鍵Ｅｓ（ＫＰｄ３＊ｒｄ２，Ｋｃ２）に分解する。パラメータＢ＊ｒｄ２と自身の秘密鍵Ｋｄ３から、シェアード鍵Ｋｄ３＊Ｂ＊ｒｄ２（＝ＫＰｄ３＊ｒｄ２）を演算し（Ｓ３４２）、これで暗号化チャレンジ鍵Ｅｓ（ＫＰｄ３＊ｒｄ２，Ｋｃ２）を復号し、チャレンジ鍵Ｋｃ２を取り出す（Ｓ３４４）。そして、取り出されたチャレンジ鍵Ｋｃ２は、暗号部３２３に伝達され保持される（Ｓ３４６）。

【０１３６】

一方、再生装置３００のコントローラ３０１は、ストレージデバイス２００に対してライセンス読出命令を発行する（Ｓ３４８）。ライセンス読出命令は、耐タンパ記憶部２０４における読み出し位置を指定するアドレスを伴っている。ストレージデバイス２００は、ライセンス読出命令を受理すると（Ｓ３５０）、耐タンパ記憶部２０４の指定されたアドレスに記憶されているライセンスデータＬＩＣを読み出し、読み出されたライセンスデータＬＩＣは暗号エンジン２０３の第３暗号部２３０によって保持される（Ｓ３５２）。

【０１３７】

一方、再生装置３００のコントローラ３０１は、暗号エンジン３０３に対してセッション情報の送信要求を行う（Ｓ３５４）。暗号エンジン３０３は、この送信要求を受け取ると（Ｓ３５６）、暗号エンジン３０３では、乱数発生部３２１が、セッション鍵Ｋｓ３を生成して、暗号部３２３および第２復号部３２４に伝達する。第２復号部３２４では、このセッション鍵Ｋｓ３を内部に保持する（Ｓ３５８）。

【０１３８】

暗号部３２３は、乱数発生部３２１が生成したセッション鍵Ｋｓ３に自身の公開鍵ＫＰｐ３を連結したＫｓ３／／ＫＰｐ３を、ステップＳ３４６で保持したチャレンジ鍵Ｋｃ２で暗号化して、セッション情報Ｅｓ（Ｋｃ２，Ｋｓ３／／ＫＰｐ３）を生成し、コントローラ３０１へ送る（Ｓ３６０）。コントローラ３０１は、暗号エンジン３０３からセッション情報Ｅｓ（Ｋｃ２，Ｋｓ３／／ＫＰｐ３）を受信すると（Ｓ３６２）、ストレージデバイス２００に対してセッション情報処理命令を発行する（Ｓ３６４）。このセッション情報処理命令は、ライセンスデータを暗号化する時に、シェアード鍵生成の有無を示す制御情報を伴っている。

【０１３９】

ストレージデバイス２００は、セッション情報処理命令を受理すると（Ｓ３６６）、セッション情報の入力を要求し、再生装置３００のコントローラ３０１は、この要求に応じて、暗号エンジン３０３から受け取ったセッション情報Ｅｓ（Ｋｃ２，Ｋｓ３／／ＫＰｐ３）をストレージデバイス２００へ出力する（Ｓ３６７）。ストレージデバイス２００は、セッション情報Ｅｓ（Ｋｃ２，Ｋｓ３／／ＫＰｐ３）を受理すると（Ｓ３６８）、暗号エンジン２０３の第４復号部２２９に与える。第４復号部２２９は、与えられたセッショ

ン情報Ｅｓ（Ｋｃ２，Ｋｓ３／／ＫＰｐ３）を、ステップＳ３２６で保持したチャレンジ鍵Ｋｃ２で復号する。そして、再生装置３００が発行したセッション鍵Ｋｓ３と再生装置３００の公開鍵ＫＰｐ３を取り出し、それぞれ第４暗号部２３１、第３暗号部２３０に伝達する（Ｓ３７０）。

【０１４０】

そして、制御部２２０は、シェアード鍵生成の有無を示す制御情報を確認する（Ｓ３７２）。シェアード鍵生成が必要な場合、すなわち、ステップＳ３２６のチャレンジ鍵Ｋｃ２の生成後、初めての再生処理の場合（Ｓ３７２のＹ）、制御部２２０は、乱数発生部２２１に乱数ｒｐ２の生成を指示する。乱数発生部２２１は、乱数ｒｐ２を生成し、生成した乱数ｒｐ２を第３暗号部２３０に伝達する。第３暗号部２３０では、乱数ｒｐ２を用いて、シェアード鍵ＫＰｐ３＊ｒｐ２とパラメータＢ＊ｒｐ２を演算し、内部に保持する（Ｓ３７４）。

【０１４１】

一方、シェアード鍵生成が不要な場合、すなわち、ステップＳ３２６のチャレンジ鍵Ｋｃ２の生成後、２回目以降の再生処理の場合（Ｓ３７２のＮ）、ステップＳ３７４をスキップし、シェアード鍵ＫＰｐ３＊ｒｐ２とパラメータＢ＊ｒｐ２を生成せずに次のステップＳ３７６へ進む。

【０１４２】

第３暗号部２３０は、ステップＳ３５２で保持したライセンスデータＬＩＣを、保持しているシェアード鍵ＫＰｐ３＊ｒｐ２で暗号化し、この結果と保持しているパラメータＢ＊ｒｐ２を連結して、暗号化ライセンスデータＢ＊ｒｐ２／／Ｅｓ（ＫＰｐ３＊ｒｐ２，ＬＩＣ）＝Ｅｐ（ＫＰｐ３，ＬＩＣ）を生成し、第４暗号部２３１に伝達する。第４暗号部２３１は、暗号化ライセンスデータＥｐ（ＫＰｐ３，ＬＩＣ）を、第４復号部２２９から与えられたセッション鍵Ｋｓ３で暗号化し、暗号化ライセンスデータＥｓ（Ｋｓ３，（Ｅｐ（ＫＰｐ３，ＬＩＣ））を生成する（Ｓ３７６）。

【０１４３】

一方、再生装置３００のコントローラ３０１は、ストレージデバイス２００においてセッション情報処理命令の処理が終了、すなわち、暗号化ライセンスデータが生成されると、暗号化ライセンス出力命令を発行する（Ｓ３７８）。ストレージデバイス２００では、暗号化ライセンス出力命令を受理する（Ｓ３８０）と、コントローラ２０１が、暗号エンジン２０３から暗号化ライセンスデータＥｓ（Ｋｓ３，Ｅｐ（ＫＰｐ３，ＬＩＣ））を取り出し、再生装置３００のコントローラ３０１へ出力する（Ｓ３８２）。

【０１４４】

再生装置３００のコントローラ３０１は、ストレージデバイス２００から暗号化ライセンスデータＥｓ（Ｋｓ３，Ｅｐ（ＫＰｐ３，ＬＩＣ））を受信すると、それを暗号エンジン３０３に送る（Ｓ３８４）。暗号エンジン３０３が暗号化ライセンスデータを受信すると（Ｓ３８６）、第２復号部３２４は、ステップＳ３５８で保持したセッション鍵Ｋｓ３で暗号化ライセンスデータＥｓ（Ｋｓ３，Ｅｐ（ＫＰｐ３，ＬＩＣ））を復号し（Ｓ３８８）、復号結果Ｅｐ（ＫＰｐ３，ＬＩＣ）を第３復号部３２５に伝達する。

【０１４５】

そして、この再生処理がステップＳ３４６のチャレンジ鍵Ｋｃ２保持後、初回の処理か、２回目以降の処理か判断する（Ｓ３９０）。初回の再生処理の場合（Ｓ３９０のＹ）、第３復号部３２５は、伝達されたＥｐ（ＫＰｐ３，ＬＩＣ）＝Ｂ＊ｒｐ２／／Ｅｓ（ＫＰｐ３＊ｒｐ２，ＬＩＣ）から、パラメータＢ＊ｒｐ２を取り出し、パラメータＢ＊ｒｐ２と自身の秘密鍵Ｋｐ３から、シェアード鍵Ｋｐ３＊Ｂ＊ｒｐ２＝ＫＰｐ３＊ｒｐ２を楕円曲線上で演算し、演算結果を内部に保持する（Ｓ３９２）。

【０１４６】

一方、シェアード鍵の生成が必要でない場合、すなわち、２回目以降の再生処理の場合（Ｓ３９０のＮ）、ステップＳ３９２をスキップし、シェアード鍵Ｋｐ３＊Ｂ＊ｒｐ２を生成せずに次のステップＳ３９４へ進む。

【０１４７】
第３復号部３２５は、伝達されたＥｐ（ＫＰｐ３，ＬＩＣ）＝Ｂ＊ｒｐ２／／Ｅｓ（ＫＰｐ３＊ｒｐ２，ＬＩＣ）から、暗号化されたライセンスデータＥｓ（ＫＰｐ３＊ｒｐ２，ＬＩＣ）を取り出し、内部に保持するシェアード鍵Ｋｐ３＊Ｂ＊ｒｐ２で復号し、ライセンスデータＬＩＣを取り出す（Ｓ３９４）。そして、ライセンスデータは、復号器３０４に送られ（Ｓ３９６）、復号器３０４が暗号化コンテンツデータを復号する際に用いられる。以上の手順により、暗号化コンテンツを復号するためのライセンスデータが、ストレージデバイス２００から再生装置３００により読み出される。
【０１４８】
このように、再生処理が初回の場合（３９０のＹ）、新しくシェアード鍵Ｋｐ３＊Ｂ＊ｒｐ２を生成する楕円曲線上での乗算、すなわち、公開鍵暗号方式による暗号演算を行い、演算結果であるシェアード鍵ＫＰｐ３＊ｒｐ２で、暗号化ライセンスデータＥｐ（ＫＰｐ３，ＬＩＣ）を復号し、ライセンスデータＬＩＣを取り出す。
【０１４９】
一方、２回目以降の再生処理の場合（Ｓ３９０のＮ）、シェアード鍵ＫＰｐ３＊ｒｐ２とパラメータＢ＊ｒｐ２を生成せずに復号処理のステップＳ３９４へ進み、初回の処理で作成し、第３復号部３２５に保持されたシェアード鍵Ｋｐ３＊Ｂ＊ｒｐ２で、暗号化ライセンスデータＥｐ（ＫＰｐ３，ＬＩＣ）を復号し、ライセンスデータＬＩＣを取り出す。
【０１５０】
再生装置３００のコントローラ３０１は、ストレージデバイス２００においてライセンスデータの読み出し後、続けて、他のライセンスデータを読み出す場合（Ｓ３９８のＹ）、ステップＳ３４８に移行し、ライセンス読出命令の発行から手順を開始する。これは、複数のライセンスデータの読み出しにおいて、証明書の検証処理を共有とすることで処理を軽減することを目的とした手順である。ここで、続けてライセンスデータを読み出するとしたが、１つのライセンスデータを読み出し後、直ちに次の読み出しを行わなければならないわけではない。暗号エンジン１０３とストレージデバイス２００が、チャレンジ鍵Ｋｃ２とシェアード鍵ＫＰｐ３＊ｒｐ２とパラメータＢ＊ｒｐ２を共有している、具体的には、ストレージデバイス２００の暗号エンジン２０３の第４復号部２２９と再生装置３００の暗号エンジン３０３の暗号部３２３とが、同じチャレンジ鍵Ｋｃ２を共有し、かつ、ストレージデバイス２００の暗号エンジン２０３の第３暗号部２３０と、再生装置３００の暗号エンジン３０３の第２復号部３２４とが、同じシェアード鍵ＫＰｐ３＊ｒｐ２と同じパラメータＢ＊ｒｐ２をともに保持している状態であればいかなるタイミングであっても良い。
【０１５１】
また、続けてライセンスデータを読み出す場合であっても、ステップＳ３０２から手順を開始してもよいが、この場合、再生処理が２回目以降であっても、初回として扱われるため時間を要す。
【０１５２】
続けて他のライセンスデータを読み出さない場合（Ｓ３９８のＮ）には、コントローラ３０１は、正常に処理を終了する。
【０１５３】
上記実施の形態では、ストレージデバイス２００の暗号エンジン２０３の制御部２２０において、初回の処理か、２回目以降の処理かを判断する手段として、ライセンス書込命令に、シェアード鍵の演算の有無を指示するように示したが、本実施の形態のように、シェアード鍵の演算の有無に関わらず、セッション情報に公開鍵ＫＰｐ３が含まれる場合、初回の処理時に、公開鍵ＫＰｐ３を保持しておき、保持した公開鍵ＫＰｐ３と受理したセッション情報に含まれる公開鍵ＫＰｐ３との一致・不一致をもって、２回目以降の処理をか否か判断することもできる。さらに、２回目以降の処理では、セッション情報に公開鍵ＫＰｐ３を含まない形式とし、公開鍵ＫＰｐ３の有無によって判断するようにしてもよい。また、制御部２２０によって処理手順を内部で管理して判断してもよい。

【０１５４】
このようにして、ストレージデバイス２００に記録されたライセンスデータを、他のストレージデバイスに対して複製（ストレージデバイス２００に記録されたライセンスデータが利用可能）あるいは移動（ストレージデバイス２００に記録されたライセンスデータが削除あるいは無効化される）によって記録する処理を提供することができる。新たにライセンスデータを記録する他のストレージメディアが同様な機能を備えていれば、同様な手順にてストレージデバイス間でライセンスを転送し、ストレージデバイス２００から他のストレージデバイスにライセンスを記録することができることは明らかである。この場合、ストレージデバイス２００から他のストレージデバイスへのライセンスの転送は、上記ストレージデバイス２００から再生装置３００へのライセンスの利用と、また、他のストレージデバイスからストレージデバイス２００へのライセンスの転送は、上記記録装置１００からストレージデバイス２００へのライセンスの記録と同様に機能する。
【０１５５】
上記実施の形態では、簡単化のためシェアード鍵Ｋｐ２＊Ｂ＊ｒｐ１＝ＫＰｐ２＊ｒｐ１、Ｋｐ３＊Ｂ＊ｒｐ２＝ＫＰｐ３＊ｒｐ２によりデータを暗号化すると説明したが、データの暗号化については、Ｋｐ２＊Ｂ＊ｒｐ１またはＫｐ３＊Ｂ＊ｒｐ２から対称鍵アルゴリズムの鍵長のデータを導出してから、この導出関数の結果によりデータを暗号化するすることもできる。これにより、楕円曲線暗号により共有されるシェアード鍵Ｋｐ２＊Ｂ＊ｒｐ１、Ｋｐ３＊Ｂ＊ｒｐ２と、対称鍵暗号アルゴリズムで使用できる鍵の形式の違いを補償することができる。なお、このとき、楕円曲線上の２次元座標であるシェアード鍵Ｋｐ２＊Ｂ＊ｒｐ１、Ｋｐ３＊Ｂ＊ｒｐ２の２つの座標値、或いは一方の座標値から、データを暗号化する対称鍵暗号アルゴリズムの鍵長のデータを求める導出関数をベースポイントと共に事前にライセンスデータ送信元とライセンスデータ送信先で共有しておく必要がある。
【０１５６】
上記実施の形態によれば、公開鍵暗号アルゴリズムに、公開鍵暗号アルゴリズムに比べて演算量が少なく、またハードウェア化も容易な共通鍵暗号アルゴリズムを組み合わせることにより、ライセンスデータのような秘匿すべきデータに対するアクセス（記録あるいは読み出し）を繰り返して行う場合にも、安全性を損なうことなく高速に秘匿データにアクセスすることができるため、ストレージデバイスとホスト装置との間で秘匿すべきデータを暗号化して入出力するときの処理効率を向上させることができる。
【０１５７】
（第２の実施の形態）
図１２は、第２の実施の形態に係る記録再生装置４００の構成を示す。本実施の形態では、第１の実施の形態における記録装置１００および再生装置３００が一つの記録再生装置４００として実現されている。
【０１５８】
本実施の形態の記録再生装置４００は、コントローラ４０１、ストレージインタフェース４０２、記録部４０３、再生部４０４、およびこれらの構成要素の少なくとも一部を電気的に接続するデータバス４１０を備える。記録部４０３は図２に示した第１の実施の形態における記録装置１００の構成を、再生部４０４は図３に示した第１の実施の形態における再生装置３００の構成を各々備えている。なお、本図中、第１の実施の形態と同様の構成には同じ符号を付している。
【０１５９】
暗号エンジン１０３は、第１の実施の形態における記録装置１００の暗号エンジン１０３に対応し、暗号エンジン３０３は、第１の実施の形態における再生装置３００の暗号エンジン３０３に対応する。暗号エンジン１０３の内部構成は、図５に示した第１の実施の形態の暗号エンジン１０３と同様であり、暗号エンジン３０３の内部構成は、図６に示した第１の実施の形態の暗号エンジン３０３の内部構成と同様である。コントローラ４０１は、第１の実施の形態における記録装置１００のコントローラ１０１と再生装置３００の

コントローラ３０１の双方の機能を有する。ストレージインタフェース４０２は、ストレージデバイス２００とのデータの入出力を制御し、データバス４１０は、記録再生装置４００の構成を電気的に接続する。

【０１６０】

本実施の形態における記録再生装置４００の動作も、第１の実施の形態における動作と同様であり、第１の実施の形態で説明した動作において、記録装置１００および再生装置３００を記録再生装置４００に、コントローラ１０１および３０１をコントローラ４０１に、ストレージインタフェース１０２および３０２をストレージインタフェース４０２に、データバス１１０および３１０をデータバス４１０にそれぞれ置き換えたものと同様である。

【０１６１】

なお、本実施の形態では、記録部４０３、再生部４０４は、各々暗号エンジン１０３、暗号エンジン３０３を備えるが、これらの暗号エンジン内の同一機能ブロックを共有する構成としても良く、この場合、第１の実施の形態における図７で示すストレージデバイス２００における暗号エンジン２０３と同様の構成となる。

【０１６２】

（第３の実施の形態）

図１３は、第３の実施の形態に係るコンテンツ配信システムの構成を示す。本実施の形態では、第１の実施の形態における記録装置１００が、コンテンツを配信する配信サーバ５００とコンテンツの提供を受ける端末装置５２０として実現されている。なお、本図中、第１の実施の形態における記録装置１００と同一の構成には同じ符号を付している。

【０１６３】

配信サーバ５００は、暗号エンジン１０３、通信装置５０２、コンテンツデータベース５０３、ライセンスデータベース５０４、ユーザデータベース５０５、それらを制御するコントローラ５０１、およびそれらを電気的に接続するデータバス５１０を備える。端末装置５２０は、コントローラ１０１、ストレージインタフェース１０２、通信装置５２１、およびそれらを電気的に接続するデータバス５２２を備える。配信サーバ５００と端末装置５２０は、それぞれ通信装置５０２、５２１を介して、ネットワークの一例としてのインターネット２０により接続される。

【０１６４】

配信サーバ５００の暗号エンジン１０３は、第１の実施の形態の暗号エンジン１０３と同様の機能を有し、端末装置５２０のコントローラ１０１およびストレージインタフェース１０２は、それぞれ第１の実施の形態のコントローラ１０１およびストレージインタフェース１０２と同様の機能を有する。

【０１６５】

コンテンツデータベース５０３は、ユーザに提供するコンテンツを保持する。ライセンスデータベース５０４は、コンテンツを暗号化するのに用いられるコンテンツ鍵を含むライセンスデータを保持する。本実施の形態では、コンテンツは既にコンテンツ鍵により暗号化されてコンテンツデータベース５０３に格納されているが、コンテンツデータベース５０３に暗号化される前のコンテンツを格納しておき、配信サーバ５００に、第１の実施の形態の記録装置１００が備えるコンテンツエンコーダ１０５および暗号器１０４をさらに設け、コンテンツデータベース５０３からコンテンツを読み出してエンコードし、暗号化してもよい。ユーザデータベース５０５は、コンテンツの提供先であるユーザの情報を保持する。たとえば、ユーザの個人情報、ユーザの端末装置５２０のアドレス、コンテンツの購入履歴、課金情報などを保持してもよい。

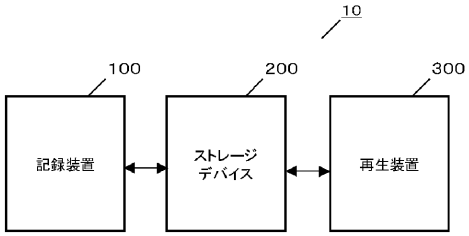
【０１６６】

コントローラ５０１は、ユーザの要求に応じて暗号化コンテンツをコンテンツデータベース５０３から読み出し、ユーザに提供する。そして、暗号エンジン１０３によりそのコンテンツを復号するためのライセンスデータがユーザに提供されると、このコンテンツ提供の対価を課金すべくユーザデータベース５０５を更新する。

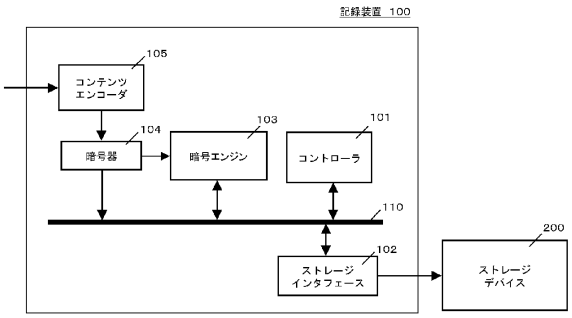
【０１６７】
本実施の形態において、データバス５１０、通信装置５０２、インターネット２０、通信装置５２１およびデータバス５２２を、構成を電気的に接続している第１の実施の形態におけるデータバス１１０とすれば、第１の実施の形態と同様の構成となる。
【０１６８】
本実施の形態の暗号入出力処理の手順は、第１の実施の形態と同様である。本実施の形態では、暗号エンジン１０３とコントローラ１０１との間の通信がインターネット２０を介して行われるのが、図８および図９で説明したように、暗号エンジン１０３とコントローラ１０１との間でも必ずデータを暗号化して送受信を行うので、高い耐タンパ性を実現することができる。
【０１６９】
コンテンツの再生については、第１の実施の形態における再生装置３００、または、第２の実施の形態における記録再生装置４００に、ストレージデバイス２００を装着することによって行うことができる。さらに、端末装置５２０に、第２の実施の形態における記録再生装置４００の再生部４０４を備える構成として、再生を行うようにしてもよい。
【０１７０】
以上、本発明に係る実施の形態について説明したが、この実施の形態は例示であり、本発明はこの実施の形態に限定されるものではなく、それらの各構成要素や各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。
【０１７１】
例えば、上記の実施の形態では、暗号エンジン内において暗号化を行う機能ブロックと復号を行う機能ブロックとを別個に設けたが、これらの構成要素において回路を共有してもよい。これにより、回路規模を抑え、小型化、低消費電力化に寄与することができる。
【０１７２】
本発明の実施の形態は、特許請求の範囲に示された技術的思想の範囲内において、適宜種々の変更が可能である。
【図面の簡単な説明】
【０１７３】
【図１】第１の実施の形態に係るデータ管理システムの全体構成を示す図である。
【図２】第１の実施の形態に係る記録装置の内部構成を示す図である。
【図３】第１の実施の形態に係る再生装置の内部構成を示す図である。
【図４】第１の実施の形態に係るストレージデバイスの内部構成を示す図である。
【図５】図２に示した暗号エンジンの内部構成を示す図である。
【図６】図３に示した暗号エンジンの内部構成を示す図である。
【図７】図４に示した暗号エンジンの内部構成を示す図である。
【図８】記録装置がストレージデバイスにライセンスデータを記録するまでの手順を示す図である。
【図９】記録装置がストレージデバイスにライセンスデータを記録までの手順を示す図である。
【図１０】再生装置がストレージデバイスからライセンスデータを読み出すまでの手順を示す図である。
【図１１】再生装置がストレージデバイスからライセンスデータを読み出すまでの手順を示す図である。
【図１２】第２の実施の形態に係る記録再生装置の内部構成を示す図である。
【図１３】第３の実施の形態に係る記録再生装置の内部構成を示す図である。
【符号の説明】
【０１７４】
１００　記録装置
２００　ストレージデバイス

３００　再生装置
４００　記録再生装置
５００　配信サーバ
５２０　端末装置

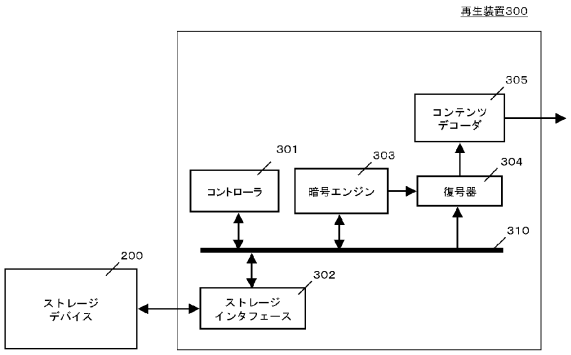
【図１】



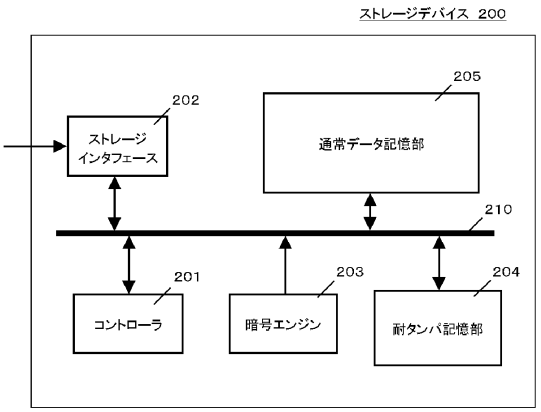
【図２】



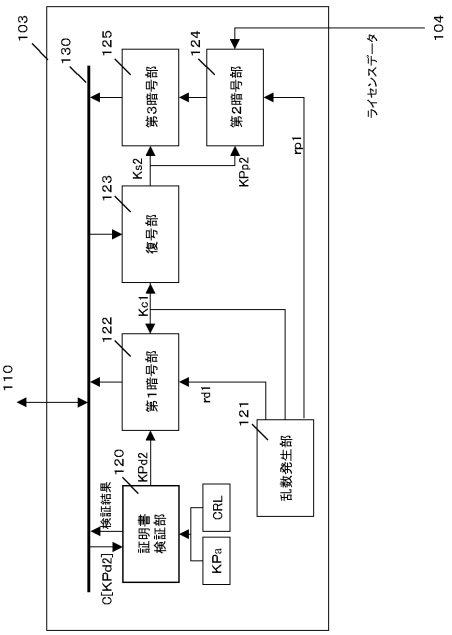
【図３】



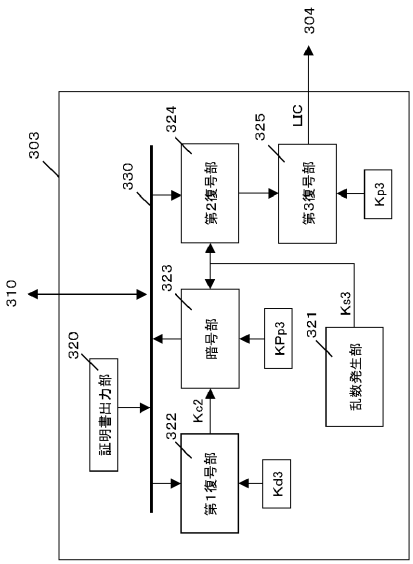
【図４】


ストレージデバイス 200
202
ストレージ
インタフェース
205
通常データ記憶部
210
201
コントローラ
203
暗号エンジン
204
耐タンパ記憶部

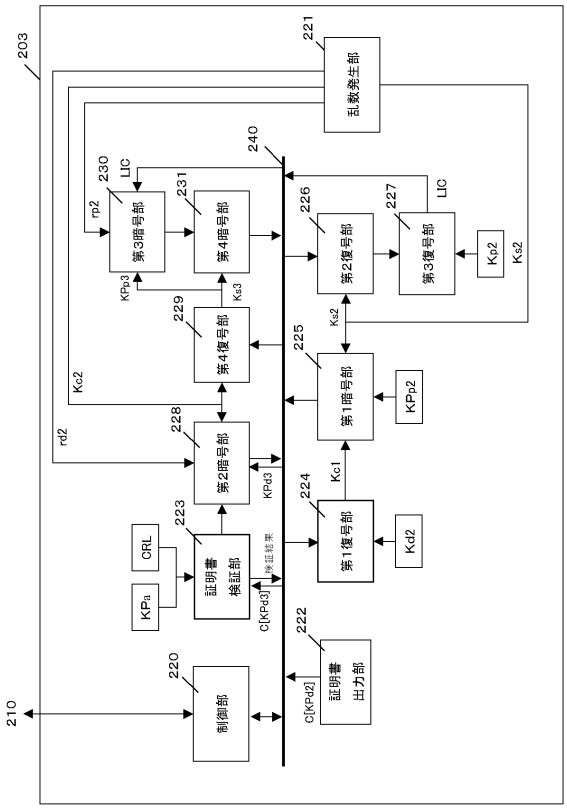
【図５】


103
104
ライセンスデータ
130
125
第3暗号部
124
第2暗号部
rp1
Ks2
KPp2
123
復号部
Kc1
122
第1暗号部
rd1
110
121
乱数発生部
120
KPd2
検証結果
証明書
検証部
CRL
KPa
C[KPd2]

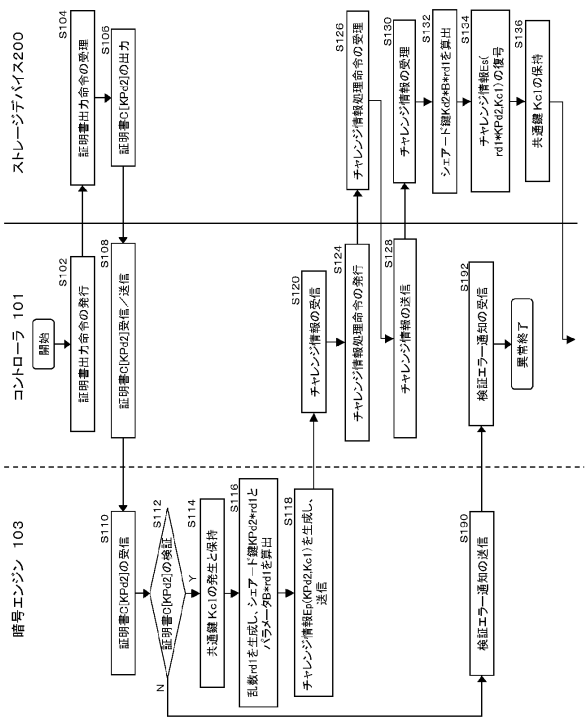
【図６】


304
303
330
324
第2復号部
325
LIC
第3復号部
Kp3
310
323
暗号部
KPp3
321
Ks3
乱数発生部
320
証明書出力部
322
Kc2
第1復号部
Kd3

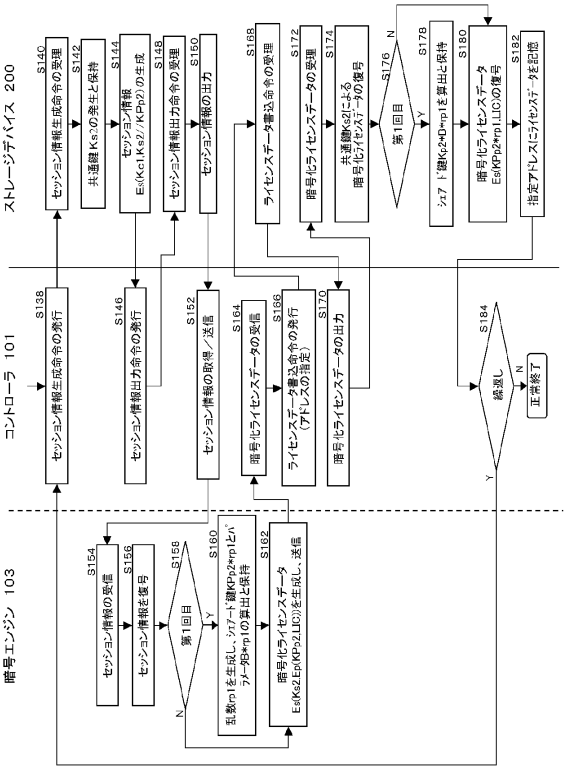
【図７】


203
221
乱数発生部
240
LIC
230
rp2
231
第3暗号部
第4暗号部
226
227
第2復号部
第3復号部
Kp2
Ks2
KPp3
Ks3
229
第4復号部
Kc2
225
第1暗号部
KPp2
rd2
228
第2暗号部
KPd3
224
Kc1
第1復号部
Kd2
CRL
223
証明書
検証部
検証結果
KPa
C[KPd3]
222
証明書
出力部
C[KPd2]
220
制御部
210

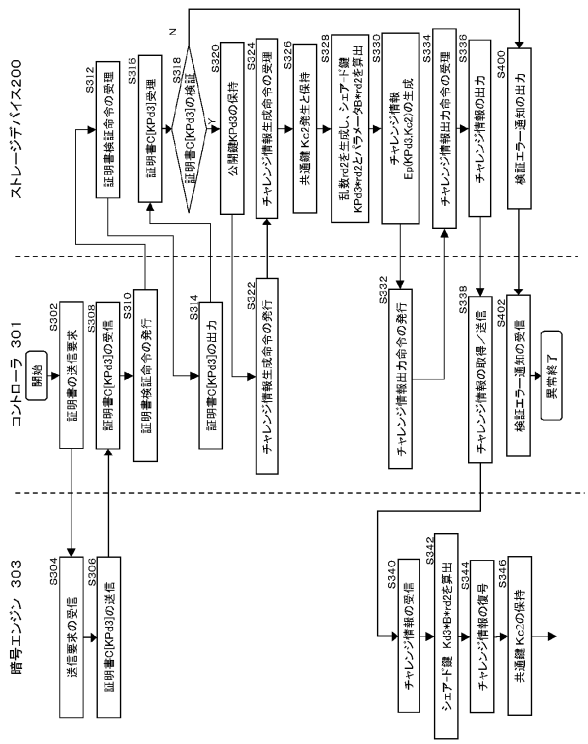
【図８】


ストレージデバイス200
コントローラ 101
暗号エンジン 103
開始
証明書出力命令の発行
証明書C(KPd2)の受信／送信
証明書出力命令の受理
証明書C(KPd2)の出力
証明書C(KPd2)の受信
証明書C(KPd2)の検証
共通鍵 Kc1の発生と保持
乱数rd1を生成し、シェアード鍵KPd2*rd1とパラメータBを算出
チャレンジ情報Ep(KPd2,Kc1)を生成し、送信
チャレンジ情報処理命令の発行
チャレンジ情報の受信
チャレンジ情報処理命令の受理
チャレンジ情報の送信
チャレンジ情報の受理
シェアード鍵(d2*B*rd1)を算出
チャレンジ情報Es(rd1*KPd2,Kc1)の復号
共通鍵 Kc1の保持
検証エラー通知の送信
検証エラー通知の受信
異常終了

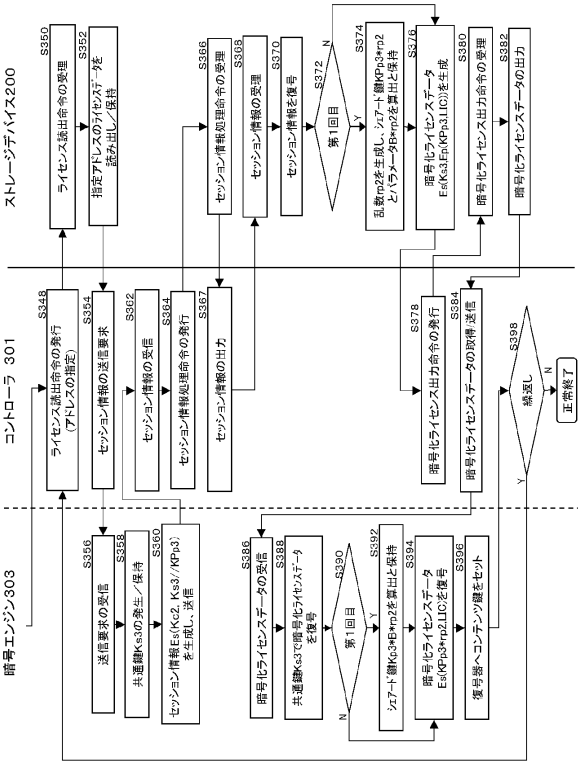
【図９】


ストレージデバイス 200
コントローラ 101
暗号エンジン 103
セッション情報生成命令の受理
セッション情報生成命令の発行
共通鍵 Ks3の発生と保持
セッション情報 Es(Kc1,Ks3／KPd2)の生成
セッション情報出力命令の受理
セッション情報出力命令の発行
セッション情報の出力
セッション情報の取得／送信
セッション情報の受信
セッション情報を復号
乱数rp1を生成し、シェアード鍵KPp2*rp1とパラメータB*rp1の算出と保持
暗号化ライセンスデータ Es(Ks2,Ep(KPp2,LIC))を生成し、送信
暗号化ライセンスデータの受理
ライセンス書込命令の発行（アドレスの指定）
ライセンスデータ書込命令の受理
暗号化ライセンスデータの出力
暗号化ライセンスデータの受理
共通鍵Ks2による暗号化ライセンスデータの復号
第1回目
シェアード鍵Kp2*Dmpまを算出と保持
暗号化ライセンスデータ Es(KPp2*rp1,LIC)の復号
指定アドレスにライセンスデータを記憶
終了L
正常終了

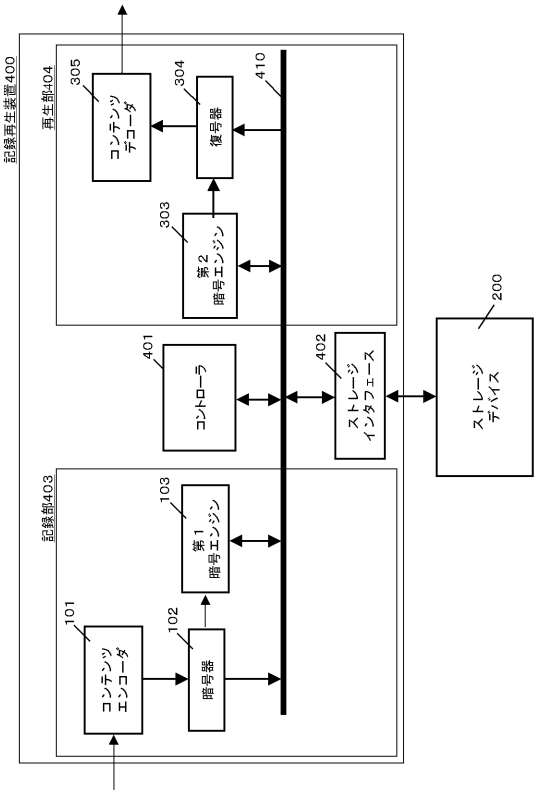
【図１０】


ストレージデバイス200
コントローラ 301
暗号エンジン 303
開始
証明書の送信要求
証明書C(KPd3)の受信
証明書検証命令の発行
証明書C(KPd3)の出力
証明書検証命令の受理
証明書C(KPd3)の受信
証明書C(KPd3)の検証
公開鍵KPd3の保持
チャレンジ情報生成命令の受理
共通鍵 Kc2の発生と保持
乱数rp2を生成し、シェアード鍵KPd3*rd2とパラメータBを算出
チャレンジ情報 Ep(KPd3,Kc2)の生成
チャレンジ情報出力命令の発行
チャレンジ情報出力命令の受理
チャレンジ情報の出力
検証エラー通知の出力
証明書C(KPd3)の送信
チャレンジ情報の受信
チャレンジ情報の取得／送信
検証エラー通知の受信
異常終了
チャレンジ情報の受信
シェアード鍵 Kd3=Kd2を算出
チャレンジ情報の復号
共通鍵 Kc2の保持

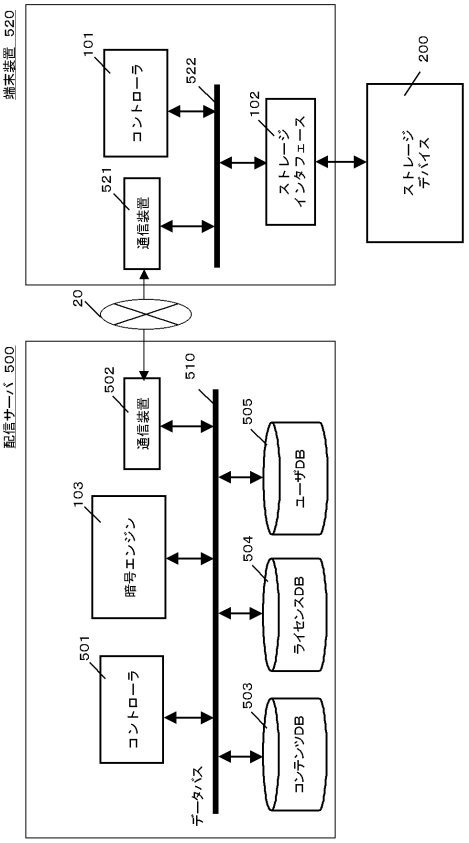
【図１１】


ストレージデバイス200
コントローラ 301
暗号エンジン303
ライセンス読出命令の受理
ライセンス読出命令の発行（アドレスの指定）
指定アドレスのライセンスデータを読み出し／保持
セッション情報の送信要求
セッション情報の受信
セッション情報処理命令の発行
セッション情報の出力
セッション情報処理命令の受理
セッション情報の受理
セッション情報を復号
第1回目
乱数rp2を生成し、シェアード鍵KPp3*rp2とパラメータB*rp2を算出と保持
暗号化ライセンスデータ Es(Ks3,Ep(KPp3,LIC))を生成
暗号化ライセンス出力命令の受理
暗号化ライセンスデータの出力
送信要求の受信
共通鍵Ks3の発生／保持
セッション情報 Es(Kc2, Ks3／KPp3)を生成し、送信
暗号化ライセンスデータの受信
共通鍵Ks3で暗号化ライセンスデータを復号
第1回目
シェアード鍵Kp3*B*rp2を算出と保持
暗号化ライセンスデータ Es(KPp3*rp2,LIC)を復号
復号器へコンテンツ鍵をセット
暗号化ライセンスデータの放棄 送信
終了L
正常終了

【図１２】


記録再生装置400
再生部404
コンテンツデコーダ
305
復号器
304
第２暗号エンジン
303
410
コントローラ
401
ストレージインタフェース
402
ストレージデバイス
200
記録部403
第１暗号エンジン
103
コンテンツエンコーダ
101
暗号器
102

【図１３】


端末装置 520
コントローラ
101
通信装置
521
522
ストレージインタフェース
102
ストレージデバイス
200
20
配信サーバ 500
通信装置
502
510
暗号エンジン
103
コントローラ
501
データバス
ユーザDB
505
ライセンスDB
504
コンテンツDB
503

フロントページの続き

(51)Int.Cl. FI
H04N 7/16 Z

(56)参考文献 特開２００６－３３７６４（ＪＰ，Ａ）
Tatsuya Hirai and Yoshihiro Hori, “An HDD-based Removable Medium and its AT-Attachment Interface Architecture for Copyright Protection”, IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, [online], ２００３年１１月, Volume 49, Issue 4, p.1161-1168, [検索日：平成２２年１１月２６日], インターネット, ＵＲＬ, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1261212
Tatsuya Hirai, Yoshihiro Hori, “Considerations about an HDD-based Removable Medium and its AT-Attachment Interface Architecture for Copyright Protection”, ieee international conference on consumer electronics 2003 digest of technical papers, ２００３年 ６月１７日, WAM 13.4, p.152-153
日置敏昭, “デジタルコンテンツ向け次世代データプラットホーム “ｉＶＤＲ”リムーバブル・ハードディスクの概要”, ＪＥＩＴＡ Ｒｅｖｉｅｗ, 日本, 社団法人電子情報技術産業協会, ２００４年 ６月 １日, Ｖｏｌ．５, Ｎｏ．６, ｐ．３０－３５
金井雄一, 堀吉宏, 牧野恵, 池上淳二, 日置敏昭, “ディジタルコンテンツ受け次世代プラットホーム“ｉＶＤＲ”の概要－基本技術規格編－”, ＳＡＮＹＯ ＴＥＣＨＮＩＣＡＬ ＲＥＶＩＥＷ, 日本, [online], ２００３年 ６月, Ｖｏｌ．３５, Ｎｏ．１, 通巻第７２号, ｐ．５５－５９, [検索日：平成２２年１１月２６日], インターネット, ＵＲＬ, http://sanyo.com/technical_review/jp/no72/pdf/7206.pdf
堀吉宏, “ｉＶＤＲハードディスクドライブの標準化動向”, 電子情報通信学会技術研究報告, 日本, 社団法人電子情報通信学会, ２００５年 １月 ６日, Ｖｏｌ．１０４, Ｎｏ．５４６, ｐ．２１－２６, [検索日：平成２２年１１月２６日], インターネット, ＵＲＬ, http://ci.nii.ac.jp/naid/110003205534
堀吉宏, 泰間健司, 池上淳二, 金井雄一, 日置敏昭, “ｉＶＤＲ向け著作権保護技術ＳＡＦＩＡ”, ＳＡＮＹＯ ＴＥＣＨＮＩＣＡＬ ＲＥＶＩＥＷ, 日本, [online], ２００６年 ３月, Ｖｏｌ．３７, Ｎｏ．２, 通巻第７７号, ｐ．２２－２７, [検索日：平成２２年１１月２６日], インターネット, ＵＲＬ, http://sanyo.com/technical_review/jp/no77/pdf/7703.pdf
澤辺孝夫, “リムーバブル記録メディア（可搬記録媒体）の最新動向－４ 応用技術”, 電気学会誌, 日本, 社団法人電気学会, ２００５年 ２月 １日, Ｖｏｌ．１２５, Ｎｏ．２, ｐ．８９－９３

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｇ０６Ｆ ２１／０６
Ｇ０６Ｆ ２１／２４
Ｈ０４Ｎ ７／１６
ＪＳＴＰｌｕｓ（ＪＤｒｅａｍＩＩ）
ＪＭＥＤＰｌｕｓ（ＪＤｒｅａｍＩＩ）
ＪＳＴ７５８０（ＪＤｒｅａｍＩＩ）