(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4323745号
(P4323745)
(45)発行日　平成21年9月2日(2009.9.2)　(24)登録日　平成21年6月12日(2009.6.12)

(51)Int.Cl.　F I
G06F 21/24 (2006.01)　G06F 12/14 550A
G06F 12/14 520P

請求項の数 19　(全 48 頁)

(21)出願番号　特願2002-6564(P2002-6564)
(22)出願日　平成14年1月15日(2002.1.15)
(65)公開番号　特開2003-208356(P2003-208356A)
(43)公開日　平成15年7月25日(2003.7.25)
審査請求日　平成16年12月8日(2004.12.8)

前置審査

(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
(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100064746
弁理士　深見　久郎
(74)代理人　100085132
弁理士　森田　俊雄
(74)代理人　100096781
弁理士　堀井　豊
(74)代理人　100109162
弁理士　酒井　將行

最終頁に続く

(54)【発明の名称】記憶装置

(57)【特許請求の範囲】
【請求項１】
一定の手順に従ってライセンスの入出力を行ない、かつ、前記ライセンスを記憶する記憶装置であって、
外部とデータの入出力を行なうインタフェースと、
前記ライセンスを格納するデータ記憶部と、
前記ライセンスの入出力に関する履歴情報を格納する複数のログ記憶部と、
前記ライセンスの入出力を制御する制御部とを備え、
前記複数のログ記憶部の各々は、履歴情報として、ライセンスを識別する識別情報を格納する識別情報領域と、ライセンスの入出力処理の進行状態を記録する状態情報領域と、ライセンスの入出力状態を記録する入出力特定情報領域とを含み、
前記制御部は、前記ライセンスの入出力の処理が開始されたことに伴い入出力の対象となったライセンスを識別する第１の識別情報を前記インタフェースを介して受取り、その受取った前記第１の識別情報を含む履歴情報を格納するログ記憶部が前記複数のログ記憶部に存在するかどうかを判断し、
前記制御部は、受取った前記第１の識別情報を含む履歴情報を格納するログ記憶部が前記複数のログ記憶部に存在する場合、前記複数のログ記憶部から前記第１の識別情報を含む履歴情報を格納するログ記憶部を選択し、その選択したログ記憶部に対して前記ライセンスの入出力の処理に従って履歴情報を格納し、
前記制御部は、受取った前記第１の識別情報を含む履歴情報が格納されたログ記憶部が

前記複数のログ記憶部に存在しない場合、前記複数のログ記憶部の中から、前記状態情報領域に入出力の対象となっていない他のライセンスの入力が完了したことを示す状態情報を含む履歴情報を検索し、検索結果に基づいて、前記入出力の対象となっていない他のライセンスの履歴情報を格納しているログ記憶部の１つを選択する、記憶装置。

【請求項２】

前記制御部は、前記検索結果に基づいて、前記複数のログ記憶部の中に、前記入出力の対象となっていない他のライセンスの入力が完了したことを示す状態情報を含む履歴情報が格納されたログ記憶部が存在しないと判断した場合に、前記複数のログ記憶部の中から、前記状態情報領域に入出力の対象となっていない他のライセンスが出力待ち状態であることを示す状態情報を含む履歴情報を検索し、検索結果に基づいて、前記入出力の対象となっていない他のライセンスの履歴情報を格納しているログ記憶部の１つを選択する、請求項１に記載の記憶装置。

【請求項３】

前記複数のログ記憶部のそれぞれに対応し、かつ、利用した順序を示す利用番号を記憶する複数のログ管理情報記憶部と、

前記利用番号の最新値を記憶する管理情報記憶部とをさらに備え、

前記制御部は、

前記ログ記憶部を選択した場合、前記管理情報記憶部に記憶された前記利用番号の最新値を更新し、前記選択したログ記憶部に対応したログ管理情報記憶部に格納されている利用番号を前記更新した利用番号の最新値により書換え、

前記複数のログ記憶部に格納された前記履歴情報に基づいてログ記憶部を選択できない場合、前記複数のログ管理情報記憶部にそれぞれ記憶された複数の利用番号と前記管理情報記憶部に記憶された前記利用番号の最新値との比較に基づいて、最も利用番号の差のある古い履歴情報が格納されているログ記憶部を前記複数のログ記憶部から選択する、請求項１または請求項２に記載の記憶装置。

【請求項４】

前記ライセンスの入力手順において、

前記制御部は、入力対象となるライセンスの識別情報を前記ライセンスの提供元から前記インタフェースを介して取得し、前記選択したログ記憶部の履歴情報として、前記取得した第１の識別情報を前記識別情報領域に格納し、前記状態情報領域に前記ライセンスの入力待ち状態であることを示す状態情報を格納する、請求項１～３のいずれか一項に記載の記憶装置。

【請求項５】

前記ライセンスの入出力を安全に行なうために前記ライセンスの提供元と暗号通信路を構築するための一時鍵であるセッション鍵を生成するセッション鍵生成部をさらに備え、

前記複数のログ記憶部の各々は、履歴情報として、さらに、セッション鍵を格納するセッション鍵領域をさらに含み、

前記ライセンスの入力手順において、

前記制御部は、前記選択したログ記憶部の履歴情報として、前記セッション鍵生成部において生成されたセッション鍵を前記セッション鍵領域に格納する、請求項４に記載の記憶装置。

【請求項６】

前記インタフェースを介して入力される、前記セッション鍵により暗号化された、入力対象となるライセンスおよび前記ライセンスを識別する第２の識別情報を含むライセンス情報を復号化する復号化処理部をさらに備え、

前記ライセンスの入力手順において、

前記制御部は、前記選択されたログ記憶部に格納された履歴情報に含まれる第１の識別情報と、前記復号化処理部で復号化されたライセンス情報に含まれる第２の識別情報とが一致するとき入力対象となるライセンスを前記データ記憶部に記憶し、不一致であるとき前記インタフェースを介してエラー通知を外部に出力する、請求項５に記載の記憶装置。

【請求項７】
前記制御部は、前記入力されたライセンスを前記データ記憶部に記憶したとき、前記選択したログ記憶部の履歴情報として、前記状態情報領域に前記ライセンスの入力が完了したことを示す状態情報を格納する、請求項６に記載の記憶装置。
【請求項８】
前記ライセンスの再入力手順において、
前記制御部は、入力対象となるライセンスの前記第２の識別情報と履歴情報の出力要求との入力に応じて、前記第２の識別情報と一致する識別情報を含む履歴情報を格納するログ記憶部を検索し、前記第２の識別情報と一致する識別情報を含む履歴情報を格納するログ記憶部を検出した場合、その検出したログ記憶部に格納されている履歴情報を前記インタフェースを介して外部に出力する、請求項６に記載の記憶装置。
【請求項９】
前記ライセンスの再入力手順において、
前記制御部は、前記第２の識別情報と一致する識別情報を含む履歴情報を格納するログ記憶部が存在する場合、さらに前記第２の識別情報と一致する識別情報に対応するライセンスが前記データ記憶部に記憶されているか否かを検索し、検索結果に応じて前記検出したログ記憶部の前記入出力特定情報領域に情報を格納して、前記検出したログ記憶部に格納されている履歴情報を前記インタフェースを介して外部に出力する、請求項８に記載の記憶装置。
【請求項１０】
前記データ記憶部に記憶された複数のライセンスの外部への出力を、前記ライセンスごとに許可あるいは禁止する有効情報を格納する有効情報記憶部をさらに備え、
前記ライセンスの再入力手順において、
前記制御部は、
前記第２の識別情報と一致する識別情報に対応するライセンスを前記データ記憶部から検出できなかったとき、前記検出したログ記憶部の前記入出力特定情報領域に、前記ライセンスが存在しないことを示す情報を格納して、前記検出したログ記憶部に格納されている履歴情報を外部に出力し、
前記第２の識別情報と一致する識別情報に対応するライセンスを前記データ記憶部から検出し、かつ、その検出したライセンスに対応する有効情報が禁止であるとき、前記検出したログ記憶部の前記入出力特定情報領域に、前記ライセンスを他の記憶装置へ移動したことを示す情報を格納して、前記検出したログ記憶部に格納されている履歴情報を外部に出力し、
前記第２の識別情報と一致する識別情報に対応するライセンスを前記データ記憶部から検出し、かつ、その検出したライセンスに対応する有効情報が許可であるとき、前記検出したログ記憶部の前記入出力特定情報領域に、前記ライセンスが存在することを示す情報を格納して、前記検出したログ記憶部に格納されている履歴情報を外部に出力する、請求項９に記載の記憶装置。
【請求項１１】
前記検出した履歴情報に含まれる前記セッション鍵領域に格納されたセッション鍵を前記提供元において生成されたセッション鍵によって暗号化して、暗号化データを生成する暗号化処理部と、
前記暗号化データと、前記検出したログ記憶部に格納されている前記識別情報領域、前記状態情報領域、前記入出力特定情報領域のデータとを合わせた履歴データを生成する履歴データ生成部と、
前記履歴データに対する署名値を演算する署名値演算部とをさらに備え、
前記暗号化処理部は、前記提供元において生成されたセッション鍵によって前記署名値をさらに暗号化し、
暗号化された署名値と前記履歴データとを合わせた署名付き履歴データを生成する署名付き履歴データ生成部をさらに備え、

前記制御部は、前記署名付き履歴データを前記履歴情報として前記提供元に出力する、請求項８から請求項１０のいずれか１項に記載の記憶装置。

【請求項１２】

前記ライセンスを他の記憶装置に提供するための出力手順において、

前記制御部は、出力対象となるライセンスの第１の識別情報を前記インタフェースを介して取得し、前記選択したログ記憶部の履歴情報として、前記取得した第１の識別情報を前記識別情報領域に格納し、前記状態情報領域に前記ライセンスの出力待ち状態であることを示す状態情報を格納する、請求項１～３のいずれか一項に記載の記憶装置。

【請求項１３】

前記制御部は、前記データ記憶部に格納されている前記ライセンスを前記インタフェースを介して外部に出力したとき、前記選択したログ記憶部の履歴情報として、前記状態情報領域に、前記ライセンスの出力が完了したことを示す態情報を格納する、請求項１２に記載の記憶装置。

【請求項１４】

前記データ記憶部に記憶された複数のライセンスの外部への出力を、前記ライセンスごとに許可あるいは禁止する有効情報を格納する有効情報記憶部をさらに備え、

前記制御部は、前記データ記憶部に格納されている前記ライセンスを前記インタフェースを介して外部に出力したとき、当該ライセンスに対応する有効情報について、許可を禁止する有効情報に変更し、当該ライセンスの外部への出力を禁止する、請求項１２または請求項１３に記載の記憶装置。

【請求項１５】

前記他の記憶装置に提供した前記ライセンスの再出力手順において、

前記制御部は、出力対象となるライセンスの第２の識別情報と再出力要求との入力に応じて、前記第２の識別情報と一致する識別情報を含む履歴情報を格納するログ記憶部を検索し、前記第２の識別情報と一致する識別情報を含む履歴情報を格納するログ記憶部を検出した場合、前記ライセンスの再出力手順の継続をするか否かを判断し、不一致であるとき、前記インタフェースを介してエラー通知を外部に出力する、請求項１２から請求項１４のいずれか１項に記載の記憶装置。

【請求項１６】

前記他の記憶装置に提供した前記ライセンスの再出力手順において、

前記制御部は、前記第２の識別情報と一致する識別情報を含む履歴情報を格納するログ記憶部を検出した場合、検出したログ記憶部の状態情報領域に前記ライセンスの出力待ち状態であることを示す状態情報が格納されているか否かを判断し、

前記ライセンスの出力待ち状態であることを示す状態情報が格納されている場合には、前記ライセンスの再出力手順の継続を許可する、請求項１５に記載の記憶装置。

【請求項１７】

前記他の記憶装置に提供した前記ライセンスの再出力手順において、

前記制御部は、前記他の記憶装置から前記ライセンスに関するもう１つの履歴情報を前記インタフェースを介して取得し、再出力するライセンスを識別する識別情報を前記インタフェースを介して取得して、前記もう１つの履歴情報に含まれる識別情報との比較に基づいて当該ライセンスの再出力手順を継続するか否かを判断する、請求項１６に記載の記憶装置。

【請求項１８】

前記他の記憶装置に提供した前記ライセンスの再出力手順において、

前記制御部は、前記第２の識別情報と一致する識別情報を含む履歴情報を格納するログ記憶部を検出した場合、検出したログ記憶部の状態情報領域に前記ライセンスの出力が完了した状態であることを示す状態情報が格納されているか否かを判断し、

前記ライセンスの出力が完了した状態であることを示す状態情報が格納されている場合には、前記ライセンスの再出力手順の継続を許可する、請求項１５に記載の記憶装置。

【請求項１９】

前記他の記憶装置に提供した前記ライセンスの再出力手順において、

前記制御部は、前記他の記憶装置から前記ライセンスに関するもう１つの履歴情報を前記インタフェースを介して取得し、再出力する機密情報を識別する識別情報を前記インタフェースを介して取得して、前記もう１つの履歴情報に含まれる識別情報との比較に基づいて当該ライセンスの再出力手順を継続するか否かを判断し、継続すると判断し、かつ、当該ライセンスに対応する有効情報が外部への出力を禁止している場合、当該ライセンスに対応する有効情報について、禁止を許可に変更し、当該ライセンスの外部への出力を許可する、請求項１８に記載の記憶装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生するためのライセンスを記憶する記憶装置に関し、特に、マルチアクセスが可能な記憶装置においてコピーされた情報に対する著作権保護を可能とする記憶装置に関するものである。

【０００２】

【従来の技術】

近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】

このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】

したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】

しかし、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００７】

この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【０００８】

そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンスを送信する。ライセンスは、暗号化コンテ

ンツデータを復号するための復号鍵（「コンテンツ鍵」と言う。以下同じ。）、ライセンスを識別するためのライセンスＩＤ、およびライセンスの利用を制限するための制御情報等を含んでいる。配信サーバからメモリカードに対してライセンスを送信する際には、配信サーバおよびメモリカードは、それぞれがセッション鍵を生成し、配信サーバとメモリカードとの間で鍵の交換を行なうことによって、暗号通信路を構築する。

【０００９】

最終的に、配信サーバはメモリカードに対して構築した暗号通信路を介してライセンスを送信する。その際、メモリカードは、受信した暗号化コンテンツデータとライセンスとを内部のメモリに記憶する。

【００１０】

メモリカードに記憶した暗号化コンテンツデータを再生する場合は、メモリカードを携帯電話機に装着する。携帯電話機は、通常の通話機能の他にメモリカードから暗号化コンテンツデータとコンテンツ鍵を読み出して暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。ライセンス鍵の読み出しに際しては、メモリカードと専用回路との間に暗号通信路を構築し、暗号通信路を介してメモリカードから専用回路に送信される。

【００１１】

また、メモリカードは、他のメモリカードとの間でライセンスの移動または複製を行なう機能を備えている。この場合、配信サーバからライセンスの送信と同様に、送信元のメモリカードと送信先のメモリカードの双方の機能によって暗号通信路を構築した上で、ライセンスが送信元のメモリカードから送信先のメモリカードに対して送信される。ライセンスを移動するか複製するかは、ライセンスに含まれる制御情報に従って決定される。

【００１２】

さらに、送受信中の不慮の中断によってライセンスが消失した場合に、その処理を再開でき、かつ、ライセンスの重複送信を防ぐためにライセンスの入出力に関する直近の履歴情報を記録し、必要に応じて出力する機能をメモリカードは備えている。送信元である配信サーバあるいはメモリカードは、送信先のメモリカードから履歴情報を取得して、この履歴情報に従ってライセンスの送受信の再開を判断する。履歴情報は、ライセンスＩＤと送受信を示すステータス情報を含んでいる。

【００１３】

このように、携帯電話機のユーザは、携帯電話網を用いて暗号化コンテンツデータとライセンスとを配信サーバから受信し、メモリカードに記憶したうえで、メモリカードに記憶された暗号化コンテンツデータを再生したり、他のメモリカードに移したりできる。また、著作権者の権利を保護することができる。

【００１４】

【発明が解決しようとする課題】

しかし、従来のメモリカードにおいては、直近の履歴情報を保持するのみで、中断後、他のライセンスに対する送受信を行った場合に先の中断に対する履歴情報が消えてしまう。このような場合、複数の履歴情報を格納することにより、ユーザの利便性を改善することが可能である。

【００１５】

また、記憶素子に対するアクセスの高速化に伴い、複数のライセンスの送受信を並行して行なう要求が発生することが、今後、予想される。その場合、少なくとも並行して行われる処理に関する履歴情報を格納できるようにする必要性が生ずる。

【００１６】

このように、複数の履歴情報を格納できるようにする場合に、ライセンスの受信後に、該ライセンスを他のメモリカードに対して移動したとすると、同一のライセンスＩＤに対して異なったステータスを持つ履歴情報が格納されるという問題が生じる。

【００１７】

そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、ラ

イセンスに対して著作権を保護し、かつ、ライセンスの送受信を再開可能とするための履歴情報を重複することなく複数格納できる記憶装置を提供することである。

【００１８】

【課題を解決するための手段】

この発明によれば、記憶装置は、一定の手順に従って機密データの入出力を行ない、かつ、機密データを記憶する記憶装置であって、外部とデータの入出力を行なうインタフェースと、機密データを格納するデータ記憶部と、機密データの入出力に関する履歴情報を格納する複数のログ記憶部と、機密データの入出力を制御する制御部とを備え、複数のログ記憶部に記憶される複数の履歴情報の各々は機密データを識別する識別情報を含み、制御部は、機密データの入出力の処理が開始されたことに伴い入出力の対象となった機密データを識別する識別情報をインタフェースを介して受取り、その受取った識別情報を含む履歴情報が格納されたログ記憶部を複数のログ記憶部から選択し、その選択したログ記憶部に対して機密データの入出力に対する手順の進行に従って履歴情報を格納する。

【００１９】

好ましくは、記憶装置は、複数のログ記憶部にそれぞれ記憶される履歴情報の各々は機密データの入出力の進行状態を記録する状態情報をさらに含み、制御部は、受取った識別情報を含む履歴情報が格納されたログ記憶部が複数のログ記憶部に存在しない場合、複数のログ記憶部から、状態情報によって他の機密データの入力が完了している履歴情報を格納しているログ記憶部の１つを選択する。

【００２０】

好ましくは、制御部は、状態情報によって他の機密データの入力が完了している履歴情報を格納しているログ記憶部が存在しない場合、複数のログ記憶部から、状態情報によって他の機密データの出力待ち状態にある履歴情報を格納しているログ記憶部の１つを選択する。

【００２１】

好ましくは、記憶装置は、複数のログ記憶部のそれぞれに対応し、かつ、利用した順序を示す利用番号を記憶する複数のログ管理情報記憶部と、利用番号の最新値を記憶する管理情報記憶部とをさらに備え、制御部は、ログ記憶部を選択した場合、管理情報記憶部に記憶された利用番号の最新値を更新し、選択したログ記憶部に対応したログ管理情報記憶部に格納されている利用番号を更新した利用番号の最新値により書換え、複数のログ記憶部に格納された履歴情報に基づいてログ記憶部を選択できない場合、複数のログ管理情報記憶部にそれぞれ記憶された複数の利用番号と管理情報記憶部に記憶された利用番号の最新値とに基づいて、最も古い履歴情報が格納されているログ記憶部を複数のログ記憶部から選択する。

【００２２】

好ましくは、記憶装置は、複数のログ記憶部の各々を利用した順序を管理するための管理情報を格納する管理情報記憶部をさらに備え、複数の履歴情報の各々は、機密データの入出力を特定する入出力特定情報と、機密データの入出力の進行状態を記録する状態情報とをさらに含み、制御部は、機密データの入出力手順において識別情報を含む履歴情報が重複して複数のログ記憶部に格納されないように、かつ、必要な履歴情報を保護するようにする所定の手順に従って、複数のログ記憶部から一つのログ記憶部を選択し、当該入出力手順に対応する履歴情報を選択したログ記憶部に格納する。

【００２３】

好ましくは、所定の手順は、入出力をしようとする機密データの識別情報と同じ識別情報を持つ履歴情報を格納したログ記憶部、機密データの消失が発生することのない状態を示す状態情報を持つ履歴情報を格納したログ記憶部、管理情報によって最も古いと判断される履歴情報を格納するログ記憶部の順序である。

【００２４】

好ましくは、機密データの入力手順において、制御部は、入力対象となる機密データの識別情報を機密データの提供元からインタフェースを介して取得し、所定の順序に従って選

択したログ記憶部に、取得した識別情報と当該入力手順を特定する入出力特定情報を格納し、選択したログ記憶部に格納される状態情報を入力待ちに変更する。

【００２５】

好ましくは、記憶装置は、機密データの入出力を安全に行なうために機密データの提供元と暗号通信路を構築するための一時鍵であるセッション鍵を生成するセッション鍵生成部をさらに備え、機密データの入力手順において、制御部は、セッション鍵生成部において生成されたセッション鍵を入出力特定情報として選択したログ記憶部に格納する。

【００２６】

好ましくは、機密データは、当該機密データを識別する識別情報を含み、制御部は、選択されたログ記憶部に格納された履歴情報に含まれる第１の識別情報と、入力された機密データに含まれる第２の識別情報が一致するとき入力された機密データをデータ記憶部に記憶し、第１の識別情報と第２の識別情報が不一致であるときインタフェースを介してエラー通知を外部に出力する。

【００２７】

好ましくは、制御部は、入力された機密情データをデータ記憶部に記憶したとき、選択したログ記憶部に格納される状態情報を入力済みに変更する。

【００２８】

好ましくは、インタフェースを介して入力される外部からの第１の識別情報と履歴情報の出力要求とに応じて、第１の識別情報と一致する識別情報を含む履歴情報を格納するログ記憶部を検索し、第１の識別情報と一致する識別情報を含む履歴情報を格納するログ記憶部を検出した場合、その検出したログ記憶部に格納されている履歴情報をインタフェースを介して外部に出力する。

【００２９】

好ましくは、履歴情報の入出力状態情報は、機密データの入出力の進行状態を記録する第１の状態情報と、機密データのデータ記憶部への記憶状態を示す第２の状態情報とから成り、制御部は、第１の識別情報と一致する識別情報を含む履歴情報を格納するログ記憶部が存在する場合、さらに第１の識別情報と一致する識別情報を含む機密データがデータ記憶部に記憶されているか否かを検索し、検索結果に応じて検出したログ記憶部に格納されている履歴情報の第２の状態情報を変更して検出したログ記憶部に格納されている履歴情報を、インタフェースを介して外部に出力する。

【００３０】

好ましくは、制御部は、第１の識別情報と同じ識別情報を含む機密データを検出できなかったとき第２の状態情報を機密データが存在しないことを示す記憶無に変更して検出した履歴情報を送信し、第１の識別情報と同じ識別情報を含む機密データを検出し、かつ、その検出した機密データが無効であるとき第２の状態情報を機密データを他の記憶装置へ移動したことを示す移動済に変更して検出した履歴情報を送信し、第１の識別情報と同じ識別情報を含む機密データを検出し、かつ、その検出した機密データが有効であるとき第２の状態情報を機密データが存在することを示す記憶有に変更して送信する。

【００３１】

好ましくは、記憶装置は、セッション鍵によってデータを暗号化する暗号処理部と、データに対する署名値を演算する署名値演算部とをさらに備え、暗号処理部は、提供元において生成されたセッション鍵によって検出した履歴情報に含まれる入出力特定情報を暗号化して第１の暗号化データを生成し、セッション鍵によって履歴情報署名値を暗号化して第２の暗号化データを生成し、署名値演算部は、入出力特定情報と第１の識別情報と第１の暗号化データとに対する署名値を演算して履歴情報署名値を生成し、制御部は、第１の識別情報、第１の暗号化データおよび第２の暗号化データを履歴情報として提供元へ送信する。

【００３２】

好ましくは、機密データを他の記憶装置に提供するための出力手順において、制御部は、出力する機密データを識別する識別情報と機密データの出力を特定する入出力特定情報と

をインタフェースを介して取得し、所定の順序に従って選択したログ記憶部に、取得した識別情報と当該出力手順を特定する入出力特定情報を格納し、選択したログ記憶部に格納される状態情報を出力待ちに変更する。

【００３３】

好ましくは、制御部は、データ記憶部に格納されている機密データをインタフェースを介して外部に出力したとき、選択したログ記憶部に格納される状態情報を出力済みに変更する。

【００３４】

好ましくは、記憶装置は、データ記憶部に記憶された複数の機密データの外部への出力を、機密データごとに禁止する失効情報を格納する失効情報記憶部をさらに備え、制御部は、データ記憶部に格納されている機密データをインタフェースを介して外部に出力したとき、当該機密データに対応する失効情報を変更し、当該機密データの外部への出力を禁止する。

【００３５】

好ましくは、機密データは、当該機密データを識別する識別情報を含み、制御部は、選択されたログ記憶部に格納された履歴情報に含まれる第１の識別情報とデータ記憶部に格納されている機密データに含まれる第２の識別情報とが一致するとき、データ記憶部に格納されている履歴情報をインタフェースを介して外部に出力し、第１の識別情報と第２の識別情報とが不一致であるとき、インタフェースを介してエラー通知を外部に出力する。

【００３６】

好ましくは、他の記憶装置に提供した機密データの再出力手順において、制御部は、再出力する機密情報を識別する識別情報をインタフェースを介して取得し、その取得した識別情報を含む履歴情報を格納するログ記憶部を複数のログ記憶部の中から検索し、当該履歴情報を格納するログ記憶部が存在し、かつ、当該ログ記憶部に格納された当該履歴情報の状態情報が出力状態である場合に、当該機密データの再出力手順の継続を許可する。

【００３７】

好ましくは、他の記憶装置に提供した機密データの再出力手順において、制御部は、他の記憶装置から機密データに関するもう１つの履歴情報をインタフェースを介して取得し、再出力する機密データを識別する識別情報をインタフェースを介して取得し、もう１つの履歴情報に基づいて当該機密データの再出力手順を継続するか否かを判断する。

【００３８】

好ましくは、他の記憶装置に提供した機密データの再出力手順において、制御部は、再出力する機密情報を識別する識別情報をインタフェースを介して取得し、その取得した識別情報を含む履歴情報を格納するログ記憶部を複数のログ記憶部の中から検索し、当該履歴情報を格納するログ記憶部が存在し、かつ、当該ログ記憶部に格納された当該履歴情報の状態情報が出力状態である場合に、当該機密データの再出力手順の継続を許可する。

【００３９】

好ましくは、他の記憶装置に提供した機密データの再出力手順において、制御部は、他の記憶装置から機密データに関するもう１つの履歴情報をインタフェースを介して取得し、再出力する機密情報を識別する識別情報をインタフェースを介して取得し、もう１つの履歴情報に基づいて当該機密データの再出力手順を継続するか否かを判断し、継続すると判断し、かつ、当該機密データに対応する失効情報が外部への出力を禁止している場合、当該機密データに対応する失効情報を変更し、当該機密データの外部への出力を許可する。

【００４０】

【発明の実施の形態】

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００４１】

図１は、本発明による記憶装置が暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明す

るための概略図である。

【００４２】

なお、以下では携帯電話網を介して音楽データをユーザの携帯電話機に装着されたメモリカード４０に配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【００４３】

図１を参照して、ダウンロードサーバ１０は、メモリカード４０を装着した端末装置（携帯電話機等）２０のユーザからの配信要求（配信リクエスト）を受信する。音楽データを管理するダウンロードサーバ１０は、データ配信を求めてアクセスして来た端末装置２０に装着されたメモリカード４０が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行なう。そして、ダウンロードサーバ１０は、正当なメモリカードに対して著作権を保護するために所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスを端末装置２０へ配信する。

【００４４】

図１においては、たとえば端末装置２０には、着脱可能なメモリカード４０が装着される構成となっている。メモリカード４０は、端末装置２０により受信された暗号化コンテンツデータおよびライセンスをバスＢＳを介して受取り、記録する。

【００４５】

さらに、たとえば、ユーザは、端末装置２０に接続したヘッドホーン（図示せず）等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【００４６】

なお、メモリカード４０がダウンロードサーバ１０から暗号化コンテンツデータおよびライセンスを受信する場合、端末装置２０は単に暗号化コンテンツデータおよびライセンスをバスＢＳを介してメモリカード４０へ転送する機能のみを果たすため、ダウンロードサーバ１０および端末装置２０をまとめてコンテンツ提供装置３０とする。

【００４７】

端末装置２０に装着されたメモリカード４０は、ダウンロードサーバ１０から受信した暗号化コンテンツデータおよびライセンスを他のメモリカードへ送信することも可能である。

【００４８】

図２は、メモリカード４０からメモリカード４１へ暗号化コンテンツデータおよびライセンスを送信する場合の概念図を示したものである。実際には、メモリカード４０は端末装置２０に装着されてバスＢＳを介して端末装置２０との間でデータをやり取りし、メモリカード４１は端末装置２１に装着されてバスＢＳを介して端末装置２１との間でデータをやり取りする。そして、メモリカード４０からメモリカード４１へ暗号化コンテンツデータおよびライセンスを送信する場合、メモリカード４０はバスＢＳを介して暗号化コンテンツデータおよびライセンスを端末装置２０へ送信し、端末装置２０は無線回線を介して暗号化コンテンツデータおよびライセンスを端末装置２１へ送信する。そして、端末装置２１は、端末装置２０から受信した暗号化コンテンツデータおよびライセンスをバスＢＳを介してメモリカード４１へ送信する。

【００４９】

しかし、メモリカード４０とメモリカード４１との間での暗号化コンテンツデータおよびライセンスの送信においては、端末装置２０，２１は、暗号化コンテンツデータおよびライセンスをそれぞれメモリカード４０，４１に単に転送する機能のみを果たすため図２においては、端末装置２０，２１を１つの端末装置として示した。

【００５０】

したがって、メモリカード４０からメモリカード４１へ暗号化コンテンツデータおよびライセンス送信する場合、メモリカード４０は、バスＢＳを介して暗号化コンテンツデータおよびライセンスを端末装置２０，２１へ送信し、端末装置２０，２１は、メモリカード４０から受信した暗号化コンテンツデータおよびライセンスをバスＢＳを介してメモリカード４１へ送信する。

【００５１】

また、同一の端末装置に２つのメモリカード４０，４１を装着できる場合においても同様に図２によって説明可能である。

【００５２】

図１に示したような構成においては、暗号化して配信されるコンテンツデータを端末装置で再生可能とするためにシステム上必要とされるのは、第１には、通信におけるライセンスを配信するための方式であり、さらに第２には、コンテンツデータを暗号化する方式そのものであり、さらに、第３には、このようなコンテンツデータの無断コピーを防止するための著作権保護を実現する構成である。

【００５３】

本発明の実施の形態においては、特に、配信、複製／移動および再生の各処理の発生時において、これらのライセンスの出力先に対する認証およびチェック機能を充実させ、非認証の記憶装置（メモリカード）および端末装置（コンテンツ再生回路を備える携帯電話機など）に対するコンテンツデータの出力を防止することによってライセンス鍵の流出を防ぎ、著作権の保護を強化する構成を説明する。

【００５４】

なお、以下の説明においては、ダウンロードサーバ１０から、端末装置に暗号化コンテンツデータまたはそのライセンスを伝送する処理を「配信」と称することとする。

【００５５】

図３は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００５６】

まず、ダウンロードサーバ１０より配信されるデータについて説明する。Ｄｃは、音楽データ等のコンテンツデータである。コンテンツデータＤｃは、コンテンツ鍵Ｋｃで復号可能な暗号化が施される。コンテンツ鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）がこの形式でダウンロードサーバ１０から端末装置２０のユーザに配布される。

【００５７】

なお、以下においては、Ｅ（Ｘ，Ｙ）という表記は、データＹを暗号鍵Ｘにより暗号化したことを示すものとする。

【００５８】

さらに、ダウンロードサーバ１０からは、暗号化コンテンツデータとともに、コンテンツデータに関する平文情報としての付加情報Ｄｉが配布される。なお、付加情報Ｄｉは、コンテンツデータＤｃを識別するためのデータＩＤ（ＤＩＤ）を含む。

【００５９】

また、ライセンスとしては、コンテンツ鍵Ｋｃ、ライセンスＩＤ（ＬＩＤ）、データＩＤ（ＤＩＤ）、制御情報ＡＣ等が存在する。

【００６０】

データＩＤは、コンテンツデータＤｃおよびコンテンツ鍵Ｋｃを識別するためのコードであり、ライセンスＩＤは、ダウンロードサーバ１０からのライセンスの配信を管理し、個々のライセンスを識別するためのコードである。制御情報ＡＣは、記憶装置（メモリカード）からのライセンスまたはコンテンツ鍵を外部に出力するに当っての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報などがある。

【００６１】

以後、ライセンスＩＤと、データＩＤと、コンテンツ鍵Ｋｃと、制御情報ＡＣとを併せて、ライセンスＬＩＣと総称することとする。

【００６２】

また、以降では、簡単化のため制御情報ＡＣは再生回数の制限を行なう制御情報である再生回数（０：再生不可、１～２５４：再生可能回数、２５５：制限無し）と、ライセンスの移動および複製を制限する移動・複製フラグ（０：移動複製禁止、１：移動のみ可、２：移動複製可）との２項目とする。

【００６３】

図４は、図１に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【００６４】

端末装置２０，２１内のコンテンツ再生回路、およびメモリカード４０，４１には固有の公開暗号鍵ＫＰｃｘｙが設けられる。ここで、公開暗号鍵ＫＰｃｘｙは、機器のクラス（種類などの一定の単位）ごとに付与され、ｘは、コンテンツ再生回路と記憶装置を識別する識別子である。機器がコンテンツ再生回路等の再生装置である場合ｘ＝ｐであり、機器がメモリカード等の記憶装置である場合ｘ＝ｍとする。また、ｙは、機器のクラスを識別する識別子である。公開暗号鍵ＫＰｃｘｙは、秘密復号鍵Ｋｃｘｙによって復号可能である。これら公開暗号鍵ＫＰｃｘｙおよび秘密復号鍵Ｋｃｘｙは、コンテンツ再生回路およびメモリカード等の種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵が共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【００６５】

また、メモリカードおよびコンテンツ再生回路のクラス証明書としてＣｘｙが設けられる。これらのクラス証明書は、コンテンツ再生回路、およびメモリカードのクラスごとに異なる情報を有する。

【００６６】

コンテンツ再生回路およびメモリカードのクラス証明書Ｃｘｙは、認証データＫＰｃｘｙ／／ｌｃｘｙ／／Ｅ（Ｋａ，Ｈ（ＫＰｃｘｙ／／ｌｃｘｙ））の形式で出荷時にコンテンツ再生回路およびメモリカードに記録される。なお、ｌｃｘｙは、クラスごとにまとめられた機器およびクラス公開暗号鍵ＫＰｃｘｙに関する情報データである。また、Ｈ（Ｘ）は、Ｘのハッシュ値を意味し、Ｘ／／ＹはＸとＹとの連結を意味する。Ｅ（Ｋａ，Ｈ（ＫＰｃｘｙ／／ｌｃｘｙ））は、ＫＰｃｘｙ／／ｌｃｘｙの署名データである。

【００６７】

ＫＰａはデータ配信システム全体で共通の公開認証鍵であり、クラス公開暗号鍵ＫＰｃｘｙとクラス情報ｌｃｘｙとを認証局においてマスタ鍵Ｋａで暗号化された署名データを復号する。マスタ鍵Ｋａは、認証局においてクラス証明書の署名データを作成するために使用される秘密暗号鍵である。

【００６８】

また、メモリカード４０，41内のデータ処理を管理するための鍵として、メモリカード４０，４１という記憶装置ごとに設定される公開暗号鍵ＫＰｏｍｚと、公開暗号鍵ＫＰｏｍｚで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Ｋｏｍｚが存在する。これらのメモリカードごとに設定される公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵ＫＰｏｍｚを個別公開暗号鍵、秘密復号鍵Ｋｏｍｚを個別秘密復号鍵と称する。ｚは記憶装置を識別する個々の識別子である。

【００６９】

ライセンスの配信、移動、複製および再生が行なわれるごとにダウンロードサーバ１０、端末装置２０，２１、およびメモリカード４０，４１において生成される共通鍵Ｋｓ１ｗ，Ｋｓ２ｗが用いられる。

【００７０】

ここで、共通鍵Ｋｓ１ｗ，Ｋｓ２ｗは、ダウンロードサーバ、コンテンツ再生回路もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１ｗ，Ｋｓ２ｗを「セッション鍵」とも呼ぶこととする。

【００７１】

これらのセッション鍵Ｋｓ１ｗ，Ｋｓ２ｗは、各処理ごとに固有の値を有することにより、ダウンロードサーバ、コンテンツ再生回路、および記憶装置（メモリカード）によって管理される。具体的には、セッション鍵Ｋｓ１ｗは、データの送信元で各処理ごとに発生される。セッション鍵Ｋｓ２ｗは、データの受信側で各処理ごとに発生される。各処理において、これらのセッション鍵を授受し、他の機器で生成されたセッション鍵を受けて、このセッション鍵による暗号化を実行した上でライセンス鍵等の送信を行なうことによって、処理におけるセキュリティ強度を向上させることができる。

【００７２】

図５は、図１に示したダウンロードサーバ１０の構成を示す概略ブロック図である。

【００７３】

ダウンロードサーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータやデータＩＤ等の配信情報を保持するための情報データベース３０４と、携帯電話機等の端末装置の各ユーザごとにコンテンツデータへのアクセスの開始に従った課金情報を保持するための課金データベース３０２と、情報データベース３０４に保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、ライセンスの配信ごとに生成され、かつ、ライセンスを特定するライセンスＩＤ等の配信に関するログを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリアとデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００７４】

データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５によって制御され、配信処理時にセッション鍵Ｋｓ１ｗを発生するためのセッション鍵発生部３１６と、メモリカードから送られてきた認証のための認証データＣｘｙ＝ＫＰｃｘｙ／／ｌｃｘｙ／／Ｅ（Ｋａ，Ｈ（ＫＰｃｘｙ／／ｌｃｘｙ））を復号するための公開復号鍵である認証鍵ＫＰａを保持する認証鍵保持部３１３と、メモリカードから送られてきた認証のための認証データＣｘｙを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの認証鍵ＫＰａによって復号処理を行なう復号処理部３１２と、セッション鍵発生部３１６より生成されたセッション鍵Ｋｓ１ｗを復号処理部３１２によって得られたクラス公開暗号鍵ＫＰｃｘｙを用いて暗号化して、バスＢＳ１に出力するための暗号処理部３１８と、セッション鍵Ｋｓ１ｗによって暗号化された上で送信されたデータをバスＢＳ１より受けて、セッション鍵Ｋｓ１ｗにより復号処理を行なう復号処理部３２０とを含む。

【００７５】

データ処理部３１０は、さらに、配信制御部３１５から与えられるコンテンツ鍵Ｋｃおよび制御情報ＡＣを、復号処理部３２０によって得られたメモリカードの個別公開暗号鍵ＫＰｏｍｚによって暗号化するための暗号処理部３２６と、暗号処理部３２６の出力を、復号処理部３２０から与えられるセッション鍵Ｋｓ２ｗによってさらに暗号化してバスＢＳ１に出力するための暗号処理部３２８とを含む。

【００７６】

ダウンロードサーバ１０の配信処理における動作については、後ほどフローチャートを使用して詳細に説明する。

【００７７】

図６は、図１に示したコンテンツ再生回路を備える端末装置２０の構成を説明するための

概略ブロック図である。

【００７８】

端末装置２０は、無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは端末装置２０からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、端末装置２０の各部のデータ授受を行なうためのバスＢＳ２と、バスＢＳ２を介して端末装置２０の動作を制御するためのコントローラ１１０６と、外部からの指示を端末装置２０に与えるための操作パネル１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるための表示パネル１１１０とを含む。

【００７９】

端末装置２０は、さらに、ダウンロードサーバ１０からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード４０と、メモリカード４０とバスＢＳ２との間のデータの授受を制御するためのメモリカードインタフェース１２００とコンテンツ再生回路１５５０とを含む。

【００８０】

コンテンツ再生回路１５５０は、認証データＣｐ３＝ＫＰｃｐ３Ｚ／／ｌｃｐ３／／Ｅ（Ｋａ，Ｈ（ＫＰｃｐ３／／ｌｃｐ３））を保持する認証データ保持部１５００を含む。ここで、端末装置２０のクラスｙは、ｙ＝３であるとする。

【００８１】

端末装置２０は、さらに、クラス固有の復号鍵であるＫｃｐ３を保持するＫｃｐ保持部１５０２と、バスＢＳ２から受けたデータを復号鍵Ｋｃｐ３によって復号し、メモリカード４０によって発生されたセッション鍵Ｋｓ１ｗを得る復号処理部１５０４とを含む。

【００８２】

端末装置２０は、さらに、メモリカード４０に記憶されたコンテンツデータの再生を行なう再生処理においてメモリカード４０との間でバスＢＳ２上においてやり取りされるデータを暗号化するためのセッション鍵Ｋｓ２ｗを乱数等により発生するセッション鍵発生部１５０８と、暗号化コンテンツデータの再生処理においてメモリカード４０からコンテンツ鍵Ｋｃおよび再生制御情報を受取る際に、セッション鍵発生部１５０８により発生されたセッション鍵Ｋｓ２ｗを復号処理部１５０４によって得られたメモリカード４０のセッション鍵Ｋｓ１ｗによって暗号化し、バスＢＳ２に出力する暗号処理部１５０６とを含む。

【００８３】

端末装置２０は、さらに、バスＢＳ２上のデータをセッション鍵Ｋｓ２ｗによって復号して、コンテンツ鍵Ｋｃを出力する復号処理部１５１０と、バスＢＳ２より暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を受けて、復号処理部１５１０からのコンテンツ鍵Ｋｃによって暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を復号してコンテンツデータＤｃを音楽再生部１５１８へ出力する復号処理部１５１６とを含む。

【００８４】

端末装置２０は、さらに、復号処理部１５１６からの出力を受けてコンテンツデータＤｃを再生するための音楽再生部１５１８と、音楽再生部１５１８の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１５１９と、ＤＡ変換器１５１９の出力をヘッドホーンなどの外部出力装置（図示省略）へ出力するための端子１５３０とを含む。

【００８５】

端末装置２０の各構成部分の各処理における動作については、後ほどフローチャートを使用して詳細に説明する。

【００８６】

図７は、図１に示すメモリカード４０の構成を説明するための概略ブロック図である。

【００８７】

既に説明したように、メモリカード４０のクラス公開暗号鍵およびクラス秘密復号鍵としてＫＰｃｍｙおよびＫｃｍｙがそれぞれ設けられ、メモリカードのクラス証明書Ｃｍｙ＝

ＫＰｃｍｙ／／ｌｃｍｙ／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍｙ／／ｌｃｍｙ））が設けられるが、メモリカード４０においては、クラス識別子ｙ＝１で表わされるものとする。また、メモリカードを識別する個別識別子ｚはｚ＝２で表されるものとする。

【００８８】

したがって、メモリカード４０は、認証データＣｍ１＝ＫＰｃｍ１／／ｌｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／ｌｃｍ１））を保持する認証データ保持部１４００と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Ｋｏｍ２を保持するＫｏｍ保持部１４０２と、クラス秘密復号鍵Ｋｃｍ１を保持するＫｃｍ保持部１４２１と、個別秘密復号鍵Ｋｏｍ２によって復号可能な公開暗号鍵ＫＰｏｍ２を保持するＫＰｏｍ保持部１４１６とを含む。

【００８９】

このように、メモリカードという記憶装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【００９０】

メモリカード４０は、さらに、メモリカードインタフェース１２００との間でデータを端子１４２６を介して授受するインタフェース１４２４と、インタフェース１４２４との間で信号をやり取りするバスＢＳ３と、バスＢＳ３にインタフェース１４２４から与えられるデータを、Ｋｃｍ保持部１４２１からのクラス秘密復号鍵Ｋｃｍ１により復号して、ダウンロードサーバ１０が配信処理において生成したセッション鍵Ｋｓ1ｗを接点Ｐａに出力する復号処理部１４２２と、ＫＰａ保持部１４１４から認証鍵ＫＰａを受けて、バスＢＳ３に与えられるデータから認証鍵ＫＰａによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ１４２０に、得られたクラス公開暗号鍵を暗号処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４６によって選択的に与えられるデータを暗号化してバスＢＳ３に出力する暗号処理部１４０６とを含む。

【００９１】

メモリカード４０は、さらに、配信、複製／移動および再生の各処理においてセッション鍵Ｋｓ２ｗを発生するセッション鍵発生部１４１８と、セッション鍵発生部１４１８が出力したセッション鍵Ｋｓ２ｗを復号処理部１４０８によって得られるクラス公開暗号鍵ＫＰｃｐｚもしくはＫＰｃｍｚによって暗号化してバスＢＳ３に送出する暗号処理部１４１０と、バスＢＳ３よりセッション鍵Ｋｓ２ｗによって暗号化されたデータを受けてセッション鍵発生部１４１８より得たセッション鍵Ｋｓ２ｗによって復号する復号処理部１４１２と、暗号化コンテンツデータの再生処理においてメモリ１４１５から読出されたコンテンツ鍵Ｋｃを、復号処理部１４１２で復号された他のメモリカードの個別公開暗号鍵ＫＰｏｍｚ（ｚ≠２）で暗号化する暗号処理部１４１７とを含む。

【００９２】

メモリカード４０は、さらに、バスＢＳ３上のデータを個別公開暗号鍵ＫＰｏｍ２と対をなすメモリカード４０の個別秘密復号鍵Ｋｏｍ２によって復号するための復号処理部１４０４と、ダウンロードサーバ１０や他のメモリカードとの間の通信における履歴を格納するログと、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）と、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を再生するためのライセンス（Ｋｃ，ＡＣ，ライセンスＩＤ，データＩＤ）と、付加情報Ｄｉと、暗号化コンテンツデータの再生リストと、ライセンスを管理するためのライセンス管理ファイルとをバスＢＳ３より受けて格納するためのメモリ１４１５とを含む。

【００９３】

また、メモリ１４１５は、ログ領域１４１５Ａと、ライセンス領域１４１５Ｂと、データ領域１４１５Ｃとから成る。ログ領域１４１５Ａは、ログを記録するための領域である。ログ領域１４１５Ａの詳細については後述する。

【００９４】

ライセンス領域１４１５Ｂは、ライセンスを記録するための領域である。ライセンス領域１４１５Ｂは、ライセンス（コンテンツ鍵Ｋｃ、制御情報ＡＣ、ライセンスＩＤ、データＩＤ）と有効フラグとを記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスと有効フラグとを格納する。ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリを格納位置によって指定する構成になっている。

【００９５】

本発明の実施の形態においては、送信元の記憶装置（メモリカード）から受信先の記憶装置へのライセンスの移動／複製において、送信元の記憶装置に保持されたライセンスの有効・無効を示す有効フラグの運用を行なう。この有効フラグが有効であるとき、ライセンスをメモリカードから外部へ出すことが可能であることを意味し、有効フラグが無効であるとき、ライセンスをメモリカードから外部へ出すことができないことを意味する。

【００９６】

データ領域１４１５Ｃは、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）の付加情報Ｄｉ、ライセンスを管理するために必要な情報を暗号化コンテンツデータごとに記録するライセンス管理ファイル、メモリカードに記録された暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）やライセンスにアクセスするための基本的な情報を記録する再生リスト、およびライセンス領域１４１５Ｂのエントリを管理するためのエントリ情報を記録するための領域である。そして、データ領域１４１５Ｃは、外部から直接アクセスが可能である。ライセンス管理ファイルおよび再生リストの詳細については後述する。

【００９７】

メモリカード４０は、さらに、バスＢＳ３を介して外部との間でデータ授受を行ない、バスＢＳ３との間で制御情報ＡＣを受けて、メモリカード４０の動作を制御するためのコントローラ１４２０を含む。

【００９８】

なお、データ領域１４１５Ｃを除く全ての構成は、耐タンパモジュール領域に構成される。

【００９９】

図８は、メモリカード４０に含まれるメモリ１４１５のログ領域１４１５Ａを詳細に説明するための図である。図８を参照して、ログ領域１４１５Ａは、履歴情報を格納するＭ個のログエントリ１６０１～１６０Ｍ（Ｍは自然数）と、Ｍ＋１個の管理情報記憶部１７００～１７０Ｍとを含む。ログエントリ１６０１～１６０Ｍは、メモリカード４０がダウンローダサーバ１０または他のメモリカードとの間でライセンスを送受信する際の各通信に対する履歴情報を１つ格納するための記憶部である。管理情報記憶部１７０１～１７０Ｍは、それぞれログエントリ１６０１～１６０Ｍに１対１に対応しており、ログエントリを利用した順序を示す記録順序番号を格納する記憶部である。管理情報記憶部１７００は、最も直近に更新された履歴情報を格納しているログエントリに対して付与した記録順序番号（「最終記録順序番号」と言う。以下同じ。）を格納しておく記憶部である。記録順序番号は、Ｎビットの自然数であって、ログエントリが利用されたログエントリに対して順に１ずつ増加した値を付与していく管理番号である。記録順序番号は、２のＮ乗の剰余系において演算される。

【０１００】

たとえば、ログエントリ１６０２が更新されるとき、記録順序番号「１０１」が付与されるとログエントリ１６０２に対応する管理情報記憶部１７０２と直近の記録順序番号を格納する管理情報記憶部１７００に記録順序番号「１０１」が格納される。次いで、ログエントリ１６０４の履歴情報が更新されると、管理情報記憶部１７００を参照して記録順序番号「１０１」を得た後、記録順序番号「１０１」に１加えた記録順序番号「１０２」をログエントリ１６０４の履歴情報に対して付与し、ログエントリ１６０４に対応する管理情報記憶部１７０４と管理情報記憶部１７００に記録順序番号「１０２」を格納する。最

終的には、管理情報記憶部１７００に格納される直近の記録順序番号と各ログエントリの履歴情報の更新に対して付与され、各ログエントリのそれぞれに対応した管理情報記憶部１７０１～１７０Ｍに格納されている記録順序番号を比較することで最も古い履歴情報を格納したログエントリを特定することができる。

【０１０１】

ログエントリ１６０１～１６０Ｍの各々は、ライセンスＩＤ領域１と、Ｋｓ２ｗ領域２と、ステータス領域３と、ＫＰｃｍｙ領域４とから成る。ライセンスＩＤ領域１は、送受信の対象となったライセンスのライセンスＩＤを格納する。Ｋｓ２ｗ領域２は、ライセンスを送受信する通信において受信先のメモリカードで発生したセッション鍵Ｋｓ２ｗを格納する。ステータス領域３は、ＳＴ１領域３１とＳＴ２領域３２とから成り、ＳＴ１領域３１には「受信待」、「受信済」、「送信待」、および「送信済」のいずれかが格納され、ＳＴ２領域３２には、「データ無」、「データ有」、および「移動済」のいずれかが格納される。すなわち、ＳＴ１領域３１は、ライセンスを送受信する通信の最終的な通信状態を表し、ＳＴ２領域３２は、実際にライセンスが送信または受信されたか否かを表す。

【０１０２】

ＫＰｃｍｙ領域４は、メモリカード間でのライセンスの複製／移動処理においてクラス公開暗号鍵ＫＰｃｍｙを格納する。

【０１０３】

ログエントリ１６０１～１６０Ｍは、有限個の履歴情報であり、履歴情報の個数であるＭと管理情報記憶部１７０１～１７０Ｍの各々に格納される記録順序番号のビット数との間には$2^{M}-1 \gg N$が成り立つようにＭおよびＮが決定される。すなわち、Ｍ個の履歴情報の各々を識別可能であり、かつ、桁数が最小になるようにＭおよびＮが決定される。

【０１０４】

以下、図１に示すデータ配信システムにおける各処理の動作について説明する。

【０１０５】

［配信］

まず、図１に示すデータ配信システムにおいて、ダウンロードサーバ１０から端末装置２０のメモリカード４０へ暗号化コンテンツデータを復号するためのライセンスを配信する動作について説明する。

【０１０６】

図９および図１０は、図１に示すデータ配信システムにおけるライセンスのダウンロード時に発生する端末装置２０に装着されたメモリカード４０へのライセンスの配信処理を説明するための第１および第２のフローチャートである。

【０１０７】

図９における処理以前に、端末装置２０のユーザは、ダウンロードサーバ１０に対して電話網を介して接続し、ダウンロードを希望するコンテンツに対するデータＩＤを取得し、ダウンロードサーバ１０に対して配信要求を行なっていること、さらに、メモリカード４０に対するエントリ管理情報を取得してライセンス領域１４１５Ｂ内の空きエントリを確認していることを前提としている。

【０１０８】

図９を参照して、端末装置２０のユーザから操作パネル１１０８を介してライセンスの受信処理が指示される。

【０１０９】

ライセンスの受信処理が指示されると、コントローラ１１０６は、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード４０へ認証データの出力要求を出力する（ステップＳ１００）。メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して認証データの出力要求を受信する（ステップＳ１０２）。そして、コントローラ１４２０は、バスＢＳ３を介して認証データ保持部１４００から認証データＣｍ１を読出し、認証データＣｍ１をバスＢＳ３、インタフェース１４２４および端子１４２６を介して出力する（ステップＳ１０４）。

【０１１０】
端末装置２０のコントローラ１１０６は、メモリカード４０からの認証データＣｍ１およびライセンス購入条件のデータＡＣをダウンロードサーバ１０に対して送信し、ダウンロードサーバ１０は、端末装置２０から認証データＣｍ１、およびライセンス購入条件のデータＡＣを受信する（ステップＳ１０６）。そして、復号処理部３１２は、メモリカード４０から出力された認証データＣｍ１＝ＫＰｃｍ１／／ｌｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／ｌｃｍ１））の署名データＥ（Ｋａ，Ｈ（ＫＰｃｍ１／／ｌｃｍ１）を認証鍵ＫＰａで復号し、その復号したデータであるハッシュ値Ｈ（ＫＰｃｍ１／／ｌｃｍ１）を配信制御部３１５へ出力する。配信制御部３１５は、認証データＣｍ１のＫＰｃｍ１／／ｌｃｍ１に対するハッシュ値を演算し、その演算したハッシュ値が復号処理部３１２から受けたハッシュ値Ｈ（ＫＰｃｍ１／／ｌｃｍ１）に一致するか否かを確認する。すなわち、ダウンロードサーバ１０は、復号処理部３１２が認証データＣｍ１の署名データＥ（Ｋａ，Ｈ（ＫＰｃｍ１／／ｌｃｍ１）を認証鍵ＫＰａで復号できること、および配信制御部３１５が送信元であるメモリカード４０から受信したハッシュ値と自ら演算したハッシュ値とが一致することを確認することにより認証データＣｍ１を検証する（ステップＳ１０８）。

【０１１１】
配信制御部３１５は、復号処理部３１２における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう。正当な認証データであると判断した場合、配信制御部３１５は、クラス公開暗号鍵ＫＰｃｍ１を受理する。そして、次の処理（ステップＳ１１０）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｃｍ１を受理しないで配信処理を終了する（ステップＳ１６６）。

【０１１２】
認証の結果、正当な認証データを持つメモリカードを装着した端末装置からのアクセスであることが確認されると、ダウンロードサーバ１０において、配信制御部３１５は、メモリカード４０からのクラス公開暗号鍵ＫＰｃｍ１を受理し（ステップＳ１１０）、配信要求のあったライセンスを識別するためのライセンスＩＤを生成する（ステップＳ１１２）。

【０１１３】
その後、セッション鍵発生部３１６は、配信のためのセッション鍵Ｋｓ１ａを生成する（ステップＳ１１４）。セッション鍵Ｋｓ１ａは、復号処理部３１２によって得られたメモリカード４０に対応するクラス公開暗号鍵ＫＰｃｍ１によって、暗号処理部３１８によって暗号化される（ステップＳ１１６）。

【０１１４】
配信制御部３１５は、ライセンスＩＤおよび暗号化されたセッション鍵Ｋｓ１ａを、ライセンスＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）として、バスＢＳ１および通信装置３５０を介して端末装置２０へ送信する（ステップＳ１１８）。

【０１１５】
端末装置２０が、ライセンスＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を受信すると、コントローラ１１０６は、ライセンスＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）をメモリカード４０に入力し、メモリカード４０においては、端子１４２６およびインタフェース１４２４を介して、コントローラ１４２０は、ライセンスＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を受理する（ステップＳ１２０）。そして、コントローラ１４２０は、バスＢＳ３を介して暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ａ）を復号処理部１４２２へ与え、復号処理部１４２２は、Ｋｃｍ保持部１４２１に保持されるメモリカード４０に固有なクラス秘密復号鍵Ｋｃｍ１によって復号処理することにより、セッション鍵Ｋｓ１ａを復号し、セッション鍵Ｋｓ１ａを受理する（ステップＳ１２２）。

【０１１６】
そうすると、ダウンロードサーバ１０の配信制御部３１５は、セッション鍵の出力要求を

バスＢＳ１および通信装置３５０を介して端末装置２０へ送信し、端末装置２０のコントローラ１１０６は、セッション鍵の出力要求を受信してメモリカードインタフェース１２００を介してメモリカード４０へ送信する。メモリカード４０のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介してセッション鍵の出力要求を受理し、セッション鍵を発生するようにセッション鍵発生部１４１８を制御する。そして、セッション鍵発生部１４１８は、セッション鍵Ｋｓ２ａを生成し（ステップＳ１２６）、コントローラ１４２０は、ダウンロードサーバ１０からライセンスを受信する通信を記録するための履歴情報を記憶するログエントリ１６０ｉ（１≦ｉ≦Ｍ）を所定の順序に従ってログ領域１４１５Ａの複数のログエントリ１６０１～１６０Ｍから採用する（ステップＳ１２８）。

【０１１７】

ここで、図１１を参照して、ダウンロードサーバ１０からライセンスを受信する通信を記録するためのログエントリを採用する方法について説明する。動作が開始されると、コントローラ１４２０は、ダウンロードサーバ１０から受信しようとしているライセンスＩＤ（ＬＩＤ）と同じライセンスＩＤを含む履歴情報がログエントリ１６０１～１６０Ｍの中に存在するか否かを検索する（ステップＳ１２８１）。そして、ダウンロードサーバ１０から受信しようとしているライセンスＩＤ（ＬＩＤ）と同じライセンスＩＤを含む履歴情報を格納するログエントリが検出された場合は、ステップＳ１２８５へ移行する。一方、ステップＳ１２８１において、ダウンロードサーバ１０から受信しようとしているライセンスＩＤ（ＬＩＤ）と同じライセンスＩＤを含む履歴情報を格納するログエントリが検出されないとき、ステータス領域３のＳＴ１領域３１に「受信済」が記録された履歴情報を格納するログエントリを検索し（ステップＳ１２８２）、ステータス領域３のＳＴ１領域３１に「受信済」が記録された履歴情報を格納するログエントリが検出されたときステップＳ１２８５へ移行する。そして、ステップＳ１２８２において、ステータス領域３のＳＴ１領域３１に「受信済」が記録された履歴情報を格納するログエントリが検出されないとき、ステータ領域３のＳＴ１領域３１に「送信待」が記録された履歴情報を格納するログエントリを検索し（ステップＳ１２８３）、ステータ領域３のＳＴ１領域３１に「送信待」が記録された履歴情報を格納するログエントリを検出したときステップＳ１２８５へ移行する。そして、ステータ領域３のＳＴ１領域３１に「送信待」が記録された履歴情報を格納するログエントリが検出されないとき、管理情報記憶部１７００を参照して格納されている直近に記録した履歴情報の記録順序番号と、Ｍ個の管理情報記憶部１７０１～１７０Ｍのそれぞれに格納されている記録順序番号との差が最も大きい記録順序番号が記録されている管理情報記憶部を特定し、その特定した管理情報記憶部に対応するログエントリを検出する、すなわち、最も古い履歴情報が記録されているログエントリを検出する（ステップＳ１２８４）。

【０１１８】

その後、コントローラ１４２０は、ステップＳ１２８１～Ｓ１２８４のいずれかによって検出されたログエントリ１６０ｉ（１≦ｉ≦Ｍ）を採用し（ステップＳ１２８５）、管理情報記憶部１７００に格納される直近に記録した履歴情報の記録順序番号を１だけ増加させる（ステップＳ１２８６）。そして、コントローラ１４２０は、採用したログエントリ１６０ｉに対応した管理情報記憶部１７０ｉに格納されている記録順序番号を管理情報記憶部１７００に格納される直近に記録した履歴情報の記録順序番号に変更し（ステップＳ１２８７）、ログエントリを選択する動作が終了する。

【０１１９】

上述したように、図１１に示す選択方法では、ログエントリ１６０１～１６０Ｍに格納される履歴情報に通信対象となったライセンスのライセンスＩＤを含むログエントリ、格納される履歴情報のＳＴ１領域３１が「受信済」であるログエントリ、格納される履歴情報のＳＴ１領域３１が「送信待」であるログエントリ、更新が最も古い履歴情報を格納するログエントリの順にログエントリ１６０１～１６０Ｍが選択される。

【０１２０】

第１の条件である履歴情報に通信対象となったライセンスのライセンスＩＤを含むログエントリは１つのライセンスに対して重複した履歴情報を記録させないための選択基準である。第２の条件である格納される履歴情報のＳＴ１領域３１が「受信済」であるログエントリ、および、第３の条件である格納される履歴情報のＳＴ１領域３１が「送信待」であるログエントリは、ライセンスの再送信処理を行なわなくても良い状態で更新されても問題がないものを選択する基準である。すなわち、「受信済」は、送信先のメモリカードにおいてライセンスがメモリ１４１５のライセンス領域１４１５Ｂに記憶済みであることを示し、「送信待」は、送信元のメモリードにおいてライセンスの出力が行われていない状態（ライセンスがメモリ１４１５のライセンス領域１４１５Ｂに記憶されている状態）であることを示している。第４の条件である更新が最も古い履歴情報を格納するログエントリは、最も再送信する確率が低いと推測されるものを選択する基準である。

【０１２１】

再び、図９を参照して、ステップＳ１２８の後、コントローラ１４２０は、受信したライセンスＩＤおよび生成されたセッション鍵Ｋｓ２ａをそれぞれステップＳ１２８において採用したログエントリ１６０ｉのライセンスＩＤ領域１およびＫｓ２ｗ領域２に格納し、ステータス領域３のＳＴ１領域３１を「受信待」に変更する（ステップＳ１３０）。

【０１２２】

暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４２２より与えられるセッション鍵Ｋｓ１ａによって、切換スイッチ１４４６の接点を順次切換えることによって与えられるセッション鍵Ｋｓ２ａ、および個別公開暗号鍵ＫＰｏｍ２を１つのデータ列として暗号化して、暗号化データＥ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をバスＢＳ３に出力する（ステップＳ１３２）。コントローラ１４２０は、バスＢＳ３に出力された暗号化データＥ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）にライセンスＩＤ（ＬＩＤ）を加えたデータＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２０に出力し（ステップＳ１３４）、端末装置２０は、データＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をダウンロードサーバ１０に送信する。

【０１２３】

ダウンロードサーバ１０は、データＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）を受信し（ステップＳ１３６）、復号処理部３２０は、暗号化データＥ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をセッション鍵Ｋｓ１ａによって復号し、メモリカード４０で生成されたセッション鍵Ｋｓ２ａ、およびメモリカード４０の個別公開暗号鍵ＫＰｏｍ２を受理する（ステップＳ１３８）。

【０１２４】

配信制御部３１５は、制御情報ＡＣを生成し（ステップＳ１４０）、データＩＤおよびコンテンツ鍵Ｋｃを情報データベース３０４から取得する（ステップＳ１４２）。

【０１２５】

配信制御部３１５は、生成したライセンスＬＩＣ、すなわち、ライセンスＩＤ、データＩＤ、コンテンツ鍵Ｋｃ、および制御情報ＡＣを暗号処理部３２６に与える。暗号処理部３２６は、復号処理部３２０によって得られたメモリカード４０の個別公開暗号鍵ＫＰｏｍ２によってライセンスＬＩＣを暗号化して暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を生成する（ステップＳ１４４）。そして、暗号処理部３２８は、暗号処理部３２６からの暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を復号処理部３２０からのセッション鍵Ｋｓ２ａによって暗号化し、暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を生成する（ステップＳ１４６）。

【０１２６】

図１０を参照して、配信制御部３１５は、バスＢＳ１および通信装置３５０を介して暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を端末装置２０へ送信する（ステップＳ１４８）。

【０１２７】

端末装置２０は、送信された暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を受信し、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード４０に入力する。そして、メモリカード４０は、暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を受理し（ステップＳ１５０）、復号処理部１４１２は、端子１４２６およびインタフェース１４２４を介して、バスＢＳ３に与えられた暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））をセッション鍵Ｋｓ２ａによって復号して暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を受理する（ステップＳ１５２）。そして、暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）は、復号処理部１４０４へ入力され、復号処理部１４０４は、Ｋｏｍ保持部１４０２に保持される個別秘密復号鍵Ｋｏｍ２によって暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を復号してライセンスＬＩＣを受理する（ステップＳ１５４）。

【０１２８】

そうすると、端末装置２０からライセンスの格納位置が出力され（ステップＳ１５６）、メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してライセンスの格納位置を受理する（ステップＳ１５８）。その後、コントローラ１４２０は、受理したライセンスＬＩＣに含まれるライセンスＩＤがステップＳ１３０においてログエントリ１６０ｉに格納されたライセンスＩＤに一致するか否かを判定し（ステップＳ１６０）、不一致であるときコントローラ１４２０は、エラー通知をバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２０へ出力する（ステップＳ１６２）。そして、端末装置２０は、メモリカードインタフェース１２００を介してエラー通知を受信してダウンロードサーバ１０へ送信し、ダウンロードサーバ１０は、エラー通知を受理する（ステップＳ１６４）。そして、書込拒否によって配信処理が終了する（ステップＳ１６６）。

【０１２９】

一方、ステップＳ１６０において２つのライセンスＩＤが一致したとき、コントローラ１４２０は、ライセンスＬＩＣをライセンス領域１４１５Ｂのライセンス格納位置によって指定されたエントリに記憶し（ステップＳ１６８）、ライセンスを受信する通信を記録するログエントリ１６０ｉのＳＴ１領域３１を「受信済」に変更し（ステップＳ１７０）、配信処理が正常に終了する（ステップＳ１７２）。

【０１３０】

なお、上記においては説明しなかったが、ライセンスをライセンス領域１４１５Ｂに記憶したとき、ライセンスを記憶したエントリに対応する有効フラグが有効に変更される。

【０１３１】

また、ライセンスの配信処理が終了した後、端末装置２０のコントローラ１１０６は、暗号化コンテンツデータの配信要求をダウンロードサーバ１０へ送信し、ダウンロードサーバ１０は、暗号化コンテンツデータの配信要求を受信する。そして、ダウンロードサーバ１０の配信制御部３１５は、情報データベース３０４より、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）および付加情報Ｄｉを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して端末装置２０へ送信する。

【０１３２】

端末装置２０は、データＥ（Ｋｃ，Ｄｃ）／／Ｄｉを受信して、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）および付加情報Ｄｉを受理する。そうすると、コントローラ１１０６は、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）および付加情報Ｄｉを１つのコンテンツファイルとしてバスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード４０に入力する。また、コントローラ１１０６は、メモリカード４０に格納されたライセンスのエントリ番号と、平文のライセンスＩＤと、データＩＤとを含み、かつ、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）と付加情報Ｄｉとに対するライセンス管理ファイルを生成し、その生成したライセンス管理ファイルをバスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード４０に入力する。さらに、コントローラ１１０６は、メモリカード４０のメモリ１４１５に記録されている再生リストに、受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や付加情

報Ｄｉから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し、全体の処理が終了する。

【０１３３】

このようにして、端末装置２０に装着されたライセンスを記憶するメモリカード４０が正規の認証データを保持する機器であること、同時に、公開暗号鍵ＫＰｃｍ１が有効であることを確認した上でコンテンツデータを配信することができ、不正なメモリカードへのコンテンツデータの配信を禁止することができる。

【０１３４】

さらに、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０１３５】

図１２は、メモリカード４０のメモリ１４１５におけるライセンス領域１４１５Ｂとデータ領域１４１５Ｃとを示したものである。データ領域１４１５Ｃには、再生リストファイル１６０と、エントリ管理情報１６５と、コンテンツファイル１６１１～１６１ｎと、ライセンス管理ファイル１６２１～１６２ｎとが記憶されている。コンテンツファイル１６１１～１６１ｎは、受信した暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）と付加情報Ｄｉとを１つのファイルとして記憶する。また、ライセンス管理ファイル１６２１～１６２ｎは、それぞれ、コンテンツファイル１６１１～１６１ｎに対応して記憶されている。

【０１３６】

メモリカード４０は、ダウンロードサーバ１０から暗号化コンテンツデータおよびライセンスを受信したとき、他のメモリカードから暗号化コンテンツデータおよびライセンスを「複製／移動処理」によって受信したとき、暗号化コンテンツデータおよびライセンスをメモリ１４１５に記憶する。

【０１３７】

メモリカード４０に送信された暗号化コンテンツデータのライセンスは、メモリ１４１５のライセンス領域１４１５Ｂのエントリ番号によって指定された領域に記録され、メモリ１４１５のデータ領域１４１５Ｃに記憶された再生リストファイル１６０のライセンス管理ファイルを読出せば、エントリ番号を取得でき、その取得したエントリ番号によって対応するライセンスをライセンス領域１４１５Ｂから読出すことができる。

【０１３８】

また、ライセンス管理ファイル１６２２は、点線で示されているが、実際には記憶されていないことを示す。コンテンツファイル１６１２は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、端末装置２０が他の端末装置から暗号化コンテンツデータだけを受信した場合に相当する。

【０１３９】

また、コンテンツファイル１６１３は、点線で示されているが、これは、たとえば、端末装置２０がダウンロードサーバ１０から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータだけを他の端末装置へ送信した場合に相当し、ライセンスはメモリ１４１５に存在するが暗号化コンテンツデータが存在しないことを意味する。

【０１４０】

［再送信］

上述した暗号化コンテンツデータのライセンスを配信する配信処理が書込拒否によって終了した場合（これは、図１０のステップＳ１４８～Ｓ１６２，Ｓ１６８，Ｓ１７０の間に通信が切断されることにより配信処理が終了する場合を含む。以下同じ。）、メモリカード４０へ対象となったライセンスを再送信できることが望ましい。ここで、図１０に示すステップＳ１４８～Ｓ１６２，Ｓ１６８，Ｓ１７０の間における動作がライセンスの再送信の対象となるのは、ダウンロードサーバ１０がライセンスＬＩＣを暗号化した暗号化デ

ータＥ（Ｋｓ２ｄ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を出力（図１０のステップＳ１４８参照）した後、その暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））が実際にメモリカード４０へ正確に送信されたか否かは、ステップＳ１６４においてメモリカード４０からエラー通知が出力されるまで解からないからである。

【０１４１】

図１３および図１４は、ライセンスを配信する配信処理が不慮の中断によって終了し、ライセンスが消失した場合に、その配信の対象となったライセンスをメモリカード４０へ再送信する場合の動作を説明するための第１および第２のフローチャートである。

【０１４２】

図１３を参照して、ライセンスの再送信の動作が開始されると、ダウンロードサーバ１０の配信制御部３１５は、ライセンスの再送信における通信を特定するためのセッション鍵Ｋｓ１ｂを発生するようにセッション鍵発生部３１６を制御し、セッション鍵発生部３１６は、セッション鍵Ｋｓ１ｂを発生する（ステップＳ２００）。そして、暗号処理部３１８は、セッション鍵Ｋｓ１ｂをメモリカード４０の公開暗号鍵ＫＰｃｍ１によって暗号化して暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）を生成する（ステップＳ２０２）。そうすると、配信制御部３１５は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）に配信の対象となったライセンスを識別するライセンスＩＤ（ＬＩＤ）を加えたデータＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）をバスＢＳ１および通信装置３５０を介して端末装置２０へ送信する（ステップＳ２０４）。端末装置２０は、データＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）を受信し、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード４０へ送信する。そして、メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してデータＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）を受理する（ステップＳ２０６）。

【０１４３】

コントローラ１４２０は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）を復号処理部１４２２に与え、復号処理部１４２２は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）をＫｃｍ保持部１４２１からの秘密復号鍵Ｋｃｍ１によって復号してセッション鍵Ｋｓ１ｂを受理する（ステップＳ２０８）。

【０１４４】

そうすると、ダウンロードサーバ１０の配信制御部３１５は、ログの出力要求をバスＢＳ１および通信装置３５０を介して端末装置２０へ出力し（ステップＳ２１０）、端末装置２０は、ログの出力要求を受信してバスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード４０へ出力する。メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してログの出力要求を受理する（ステップＳ２１２）。そして、コントローラ１４２０は、ステップＳ２０６において受理したライセンスＩＤと同じライセンスＩＤを含む履歴情報を格納するログエントリを検索し（ステップＳ２１４）、そのログエントリを検出できないときエラー通知を生成してバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２０へ出力する（ステップＳ２１６）。

【０１４５】

端末装置２０は、メモリカード４０からのエラー通知をダウンロードサーバ１０へ出力し、ダウンロードサーバ１０は、エラー通知を受理し（ステップＳ２１８）、再書込拒否により一連の動作は終了する（ステップＳ２５２）。

【０１４６】

一方、ステップＳ２１４において、ログエントリが検出されたとき、図９および図１０における中断であるためログエントリ１６０ｉが検出されることとなる。コントローラ１４２０は、ステップＳ２０６において受理したライセンスＩＤによってライセンス領域１４１５Ｂのエントリを検索し、そのライセンスＩＤと同じライセンスＩＤを含むライセンスが記憶されたエントリを検索する（ステップＳ２２０）。

【０１４７】

ステップＳ２２０において、ライセンスを記憶したエントリが検出されたとき、コントローラ１４２０は、検出したライセンスの有効性をエントリに対応した有効フラグ（図１２参照）によって判定し（ステップＳ２２２）、検出したライセンスが有効であるとき、ステップＳ２１４において検出したログエントリ１６０ｉのＳＴ２領域３２を「データ有」に変更する（ステップＳ２２４）。一方、ステップＳ２２２においてライセンスが無効であると判定されたとき、コントローラ１４２０は、ログエントリ１６０ｉのＳＴ２領域３２を「移動済」に変更する（ステップＳ２２６）。これは、ライセンスに含まれる有効フラグが無効になっている場合は、実際にはライセンス領域１４１５Ｂにライセンスは存在するが、そのライセンスは他のメモリカード等に移動されたので、ライセンスの複製を禁止する意味でメモリカード４０のライセンス領域１４１５Ｂからさらにライセンスを出力できなくしたことを意味する。つまり、ライセンスが無効であることは、そのライセンスが移動処理によって他のメモリカード等へ移動されたことを意味する。

【０１４８】

ステップＳ２２０において、ライセンスが検出されなかったとき、コントローラ１４２０は、メモリカード４０には配信の対象となったライセンスが存在しないことを意味するので、ログエントリ１６０ｉのＳＴ２領域３２を「データ無」に変更する（ステップＳ２２８）。

【０１４９】

ステップＳ２２４，Ｓ２２６，Ｓ２２８のいずれかの後、コントローラ１４２０は、ログエントリ１６０ｉに格納されている履歴情報を取得し（ステップＳ２３０）、その履歴情報のＫｓ２ｗ領域２に含まれるセッション鍵Ｋｓ２ｃを取り出して切換スイッチ１４４６の接点Ｐｆへ出力する。暗号処理部１４０６は、切換スイッチ１４４６の接点Ｐｆを介してセッション鍵Ｋｓ２ｃを受け、切換スイッチ１４４２の接点Ｐａを介してセッション鍵Ｋｓ１ｂを受ける。そして、暗号処理部１４０６は、セッション鍵Ｋｓ２ｃをセッション鍵Ｋｓ１ｂによって暗号化し、暗号化データＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）をバスＢＳ３へ出力する（ステップＳ２３２）。

【０１５０】

そうすると、コントローラ１４２０は、バスＢＳ３上の暗号化データＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）に、ステップＳ２３０において取得した履歴情報に格納されたライセンスＩＤ、およびステータス情報（ＳＴ１，ＳＴ２）を加えたログデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２を生成し、その生成したログデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２のハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）を生成する（ステップＳ２３４）。そして、コントローラ１４２０は、ハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）をバスＢＳ３を介して切換スイッチ１４４６の接点Ｐｆへ出力し、暗号処理部１４０６は、切換スイッチ１４４６の接点Ｐｆを介してハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）を受け、そのハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）をセッション鍵Ｋｓ１ｂによって暗号化して署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））をバスＢＳ３へ出力する（ステップＳ２３６）。

【０１５１】

その後、コントローラ１４２０は、署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））に、ログデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２を加えた署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を生成してバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２０へ出力する（ステップＳ２３８）。

【０１５２】

端末装置２０は、メモリカード４０から受けた署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，

Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））をダウンロードサーバ１０へ送信し、ダウンロードサーバ１０は、署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を受理する（ステップＳ２４０）。

【０１５３】

そうすると、配信制御部３１５は、署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を復号処理部３２０に与え、復号処理部３２０は、署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））をセッション鍵Ｋｓ１ｂによって復号し、その復号したハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）を配信制御部３１５へ出力する。そして、配信制御部３１５は、メモリカード４０から受信した署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））のうち、ログデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２に対するハッシュ値を演算し、その演算したハッシュ値が復号処理部３２０から受けたハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）に一致するかを確認する。そして、配信制御部３１５は、復号処理部３２０が署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を復号できたこと、およびメモリカード４０において演算されたハッシュ値とダウンロードサーバ１０において演算されたハッシュ値とが一致することを確認することにより署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を検証する（ステップＳ２４２）。署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））が非承認であるとき、再書込拒否によって一連の動作は終了する（ステップＳ２５２）。ステップＳ２４２において署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））が承認されたとき、配信制御部３１５は、ライセンスＩＤによって配信記録データベース（ログＤＢ）３０８を検索し、メモリカード４０への配信の対象となったライセンスが存在するか否かを検索する（ステップＳ２４４）。そして、ライセンスが存在しないとき、ステップＳ２５２へ移行して再書込拒否によって一連の動作が終了する。

【０１５４】

ステップＳ２４４においてライセンスが存在していた場合、メモリカード４０から受理した履歴情報のＳＴ１領域３１およびＳＴ２領域３２のデータに基づいてメモリカード４０が実際にライセンスを受理しているか否かを判定し（ステップＳ２４６）、メモリカード４０がライセンスを実際に受信済であるときステップＳ２５２へ移行して再書込拒否によって一連の動作が終了する。

【０１５５】

ステップＳ２４６において、メモリカード４０が実際にライセンスを受信していないと判定されたとき図１４のステップＳ２４８へ移行する。

【０１５６】

図１４を参照して、復号処理部３２０は、暗号化データＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）をセッション鍵Ｋｓ１ｂによって復号してメモリカード４０において生成されたセッション鍵Ｋｓ２ｃを受理する（ステップＳ２４８）。そして、配信制御部３１５は、ライセンスのメモリカード４０への配信処理においてメモリカード４０から受理したセッション鍵Ｋｓ２ａ（図９のステップＳ１３８参照）がステップＳ２４８において受理したセッション鍵Ｋｓ２ｃに一致するか否かを判定する（ステップＳ２５０）。そして、セッション鍵Ｋｓ２ａがセッション鍵Ｋｓ２ｃに不一致であるときステップＳ２５２へ移行し、再書込拒否によって一連の動作は終了する。

【０１５７】

ライセンスをメモリカード４０へ配信する配信処理においてメモリカード４０のログ領域１４１５Ａの履歴情報には、セッション鍵Ｋｓ２ａが格納され（図９のステップＳ１３０参照）、セッション鍵Ｋｓ２ａが格納された履歴情報がステップＳ２３０（図１３参照）においてログ領域１４１５Ａから取得され、ダウンロードサーバ１０へ送信されるが、ステップＳ１３０以降の各ステップにおいては、ライセンスのメモリカード４０への再送信の処理においてメモリカード４０からダウンロードサーバ１０へ送信された履歴情報に含まれるセッション鍵であることを明確にするために“Ｋｓ２ｃ”と表記している。したがって、通常、セッション鍵Ｋｓ２ａはセッション鍵Ｋｓ２ｃに一致する。

【０１５８】

そこで、ステップＳ２５０においてセッション鍵Ｋｓ２ａがセッション鍵Ｋｓ２ｃに一致すると判定されたとき、配信制御部３１５は、セッション鍵要求をバスＢＳ１および通信装置３５０を介して端末装置２０へ送信する（ステップＳ２５４）。

【０１５９】

端末装置２０は、セッション鍵要求を受信してバスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード４０へ送信し、メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してセッション鍵要求を受理する。そうすると、コントローラ１４２０は、セッション鍵発生部１４１８を制御し、セッション鍵発生部１４１８は、セッション鍵Ｋｓ２ｂを生成する（ステップＳ２５６）。そして、コントローラ１４２０は、図１１に示すフローチャートに従ってダウンロードサーバ１０がメモリカード４０へライセンスを再送信する通信を記録するための履歴情報を格納するログエントリをログ領域１４１５Ａのログエントリ１６０１～１６０Ｍから採用する（ステップＳ２５８）。なお、この場合は、ログエントリ１６０ｉが必ず採用される。

【０１６０】

コントローラ１４２０は、ステップＳ２０６において受理したライセンスＩＤとセッション鍵発生部１４１８によって生成されたセッション鍵Ｋｓ２ｂとを採用したログエントリ１６０ｉに格納し、ログエントリ１６０ｉのＳＴ１領域３１のＳＴ１を「受信待」に変更する（ステップＳ２６０）。その後、暗号処理部１４０６は、切換スイッチ１４４６の接点Ｐｅを介してＫＰｏｍ保持部１４１６からの個別公開暗号鍵ＫＰｏｍ２を受理し、切換スイッチ１４４６の接点Ｐｄを介してセッション鍵Ｋｓ２ｂを受理し、セッション鍵Ｋｓ２ｂと個別公開暗号鍵ＫＰｏｍ２とをセッション鍵Ｋｓ１ｂによって暗号化し、暗号化データＥ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ２）を生成してバスＢＳ３へ出力する（ステップＳ２６２）。そして、コントローラ１４２０は、暗号化データＥ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ２）にライセンスＩＤを加えたデータＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ２）をバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２０へ出力し（ステップＳ２６４）、端末装置２０は、データＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ２）をダウンロードサーバ１０へ送信し、ダウンロードサーバ１０は、データＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ２）を受理する（ステップＳ２６６）。

【０１６１】

ダウンロードサーバ１０においては、復号処理部３２０は、暗号化データＥ（Ｋｓ１ｂ，Ｋｓ２ｂ／／ＫＰｏｍ２）をセッション鍵Ｋｓ１ｂによって復号してセッション鍵Ｋｓ２ｂと個別公開暗号鍵ＫＰｏｍ２とを受理する（ステップＳ２６８）。そうすると、配信制御部３１５は、制御情報ＡＣを生成し（ステップＳ２７０）、データＩＤおよびコンテンツ鍵Ｋｃを情報データベース３０４から取得する（ステップＳ２７２）。

【０１６２】

配信制御部３１５は、生成したライセンスＬＩＣ、すなわち、ライセンスＩＤ、データＩＤ、コンテンツ鍵Ｋｃ、および制御情報ＡＣを暗号処理部３２６に与える。暗号処理部３２６は、復号処理部３２０によって得られたメモリカード４０の個別公開暗号鍵ＫＰｏｍ２によってライセンスＬＩＣを暗号化して暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を生成

する（ステップＳ２７４）。そして、暗号処理部３２８は、暗号処理部３２６からの暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を、復号処理部３２０からのセッション鍵Ｋｓ２ｂによって暗号化し、暗号化データＥ（Ｋｓ２ｂ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を生成する（ステップＳ２７６）。

【０１６３】

配信制御部３１５は、バスＢＳ１および通信装置３５０を介して暗号化データＥ（Ｋｓ２ｂ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を端末装置２０へ送信する（ステップＳ２７８）。

【０１６４】

端末装置２０は、送信された暗号化データＥ（Ｋｓ２ｂ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を受信し、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード４０に入力する。そして、メモリカード４０は、暗号化データＥ（Ｋｓ２ｂ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を受理し（ステップＳ２８０）、復号処理部１４１２は、端子１４２６およびインタフェース１４２４を介して、バスＢＳ３に与えられた暗号化データＥ（Ｋｓ２ｂ，Ｅ（ＫＰｏｍ２，ＬＩＣ））をセッション鍵Ｋｓ２ｂによって復号して暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を受理する（ステップＳ２８２）。そして、暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）は、復号処理部１４０４へ入力され、復号処理部１４０４は、Ｋｏｍ保持部１４０２に保持される個別秘密復号鍵Ｋｏｍ２によって暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を復号してライセンスＬＩＣを受理する（ステップＳ２８４）。

【０１６５】

そうすると、端末装置２０からライセンスの格納位置が出力され（ステップＳ２８６）、メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してライセンスの格納位置を受理する（ステップＳ２８８）。その後、コントローラ１４２０は、受理したライセンスＬＩＣに含まれるライセンスＩＤがステップＳ２６０においてログエントリ１６０ｉに格納されたライセンスＩＤに一致するか否かが判定され（ステップＳ２９０）、不一致であるときコントローラ１４２０は、エラー通知をバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２０へ出力する（ステップＳ２９２）。そして、端末装置２０は、メモリカードインタフェース１２００を介してエラー通知を受信してダウンロードサーバ１０へ送信し、ダウンロードサーバ１０は、エラー通知を受理する（ステップＳ２９４）。そして、書込拒否によって配信処理が終了する（ステップＳ２９６）。

【０１６６】

一方、ステップＳ２９０において２つのライセンスＩＤが一致したとき、コントローラ１４２０は、ライセンスＬＩＣをライセンス領域１４１５Ｂのライセンス格納位置によって指定されたエントリに記憶し（ステップＳ２９８）、ライセンスを再受信する通信を記録するログエントリ１６０ｉのＳＴ１領域３１を「受信済」に変更し（ステップＳ３００）、ライセンスの再送信の処理が正常に終了する（ステップＳ３０２）。

【０１６７】

暗号化コンテンツデータのライセンスをメモリカード４０へ再送信する処理が再書込拒否によって終了した場合（これは、図１４のステップＳ２７８～Ｓ２９２，Ｓ２９８，Ｓ３００の間に通信が切断されることにより再送信の処理が終了する場合を含む。以下同じ。）、図１３および図１４に示すフローチャートに従ってライセンスがメモリカード４０へ再送信される。

【０１６８】

また、図１４のステップＳ２７８～Ｓ２９２，Ｓ２９８，Ｓ３００の間の動作がライセンスの再送信の対象となる理由は上述した理由と同じである。

【０１６９】

［移動／複製］

上述したように、図１に示すデータ配信システムにおいて、端末装置２０に装着されたメモリカード４０は、ダウンロードサーバ１０から暗号化コンテンツデータおよびライセンスを受信して記録することができる。そして、端末装置２０のユーザは、自己のメモリカ

ード４０に記録された暗号化コンテンツデータを端末装置２１に装着されたメモリカード４１へ自由に複製することができる。しかし、端末装置２１のユーザは、暗号化コンテンツデータを自己のメモリカード４１に複製しても、その複製した暗号化コンテンツデータを復号するためのライセンスを取得しなければ複製した暗号化コンテンツデータを再生することができない。

【０１７０】

そこで、メモリカード４０からメモリカード４１へのライセンスの複製／移動について説明する。この場合、図２に示す系を用いて２つのメモリカード４０，４１間でライセンスの移動／複製が行なわれる。また、メモリカード４１は、メモリカード４０と同一の構成から成り、メモリカード４１のクラス識別子ｙをメモリカード４０と同一のｙ＝１とし、メモリカード個々を区別する識別子ｚは、ｚ＝５とする。

【０１７１】

図１５および図１６は、図２におけるメモリカード４０に記録されたライセンスをメモリカード４１に移動／複製するためのフローチャートである。なお、図１５における処理以前に、端末装置２０，２１のコントローラ１１０６は、ユーザがライセンスの移動／複製を行なうコンテンツの指定およびライセンスの移動／複製リクエストを行なうための入力手段（図示せず）に接続され、ユーザによってなされたライセンスの移動／複製を行なうコンテンツの指定、およびライセンスの移動／複製リクエストを受取る。そして、コントローラ１１０６は、送信元であるメモリカード４０内の再生リストを参照してライセンスの移動／複製を行なうライセンス管理ファイルを取得していることを前提としている。また、送信元のメモリカード４０および受信先のメモリカード４１内に格納されている、それぞれのエントリ管理情報を取得していることを前提としている。さらに、送信元のメモリカード４０に格納されたエントリ管理情報によって、受信先のメモリカード４１のライセンス領域１４１５Ｂ内に空きのエントリを確認していることを前提としている。

【０１７２】

図１５を参照して、移動／複製リクエストがユーザから指示されると、コントローラ１１０６は、認証データの出力要求をバスＢＳを介してメモリカード４１へ送信する（ステップＳ４００）。そして、メモリカード４１のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して認証データの出力要求を受信する（ステップＳ４０２）。

【０１７３】

メモリカード４１のコントローラ１４２０は、認証データの出力要求を受信すると、認証データ保持部１４００から認証データＣｍ１をバスＢＳ３を介して読出し、その読出した認証データＣｍ１をバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２１のコントローラ１１０６へ出力する（ステップＳ４０４）。そして、コントローラ１１０６は、バスＢＳを介して認証データＣｍ１を受理し（ステップＳ４０５）、バスＢＳを介してメモリカード４０へメモリカード４１の認証データＣｍ１を送信する（ステップＳ４０６）。

【０１７４】

そうすると、メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して認証データＣｍ１を受信し（ステップＳ４０８）、その受信した認証データＣｍ１をバスＢＳ３を介して復号処理部１４０８へ与える。そして、復号処理部１４０８は、ＫＰａ保持部１４１４からの認証鍵ＫＰａによって認証データＣｍ１の復号処理を実行し、その復号結果をコントローラ１４２０へ出力する。コントローラ１４２０は、認証データＣｍ１のデータＫＰｃｍ１／／ｌｃｍ１に対するハッシュ値を演算し、その演算したハッシュ値が復号処理部１４０８から受けたハッシュ値Ｈ（ＫＰｃｍ１／／ｌｃｍ１）に一致するか否かを確認する。すなわち、メモリカード４０は、復号処理部１４０８が認証データＣｍ１の暗号化データＥ（Ｋａ，Ｈ（ＫＰｃｍ１／／ｌｃｍ１）を認証鍵ＫＰａで復号できること、およびコントローラ１４２０が送信元であるメモリカード４１から受信したハッシュ値と自ら演算したハッシュ値とが一致することを

確認することにより認証データＣｍ１を検証する（ステップＳ４１０）。
【０１７５】
正当な認証データであると判断された場合、コントローラ１４２０は、認証データＣｍ１から取得したクラス公開暗号鍵ＫＰｃｍ１を承認し、受理する（ステップＳ４１２）。正当な認証データでない場合には、非承認とし、コントローラ１４２０は、エラー通知をバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２０のコントローラ１１０６へ出力し（ステップＳ４８８）、端末装置２０のコントローラ１１０６はエラー通知を受理し（ステップＳ４９０）、書込拒否によって一連の動作が終了する（ステップＳ４９２）。
【０１７６】
認証の結果、正当な認証データを持つメモリカードへのライセンスの移動／複製であることが確認されると、送信元のメモリカード４０において、コントローラ１４２０は、セッション鍵発生部１４１８を制御し、セッション鍵発生部１４１８は、移動のためのセッション鍵Ｋｓ１ｄを生成する（ステップＳ４１４）。セッション鍵Ｋｓ１ｄは、復号処理部１４０８によって得られたメモリカード４１に対応するクラス公開暗号鍵ＫＰｃｍ１によって、暗号処理部１４１０によって暗号化される（ステップＳ４１６）。そして、メモリカード４０のコントローラ１４２０は、バスＢＳ３を介して暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｄ）を取得し、バスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２０のコントローラ１１０６に出力する（ステップＳ４１８）。
【０１７７】
コントローラ１１０６は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｄ）を送信元から受理し（ステップＳ４２０）、送信元のメモリカード４０のライセンス管理情報からライセンスＩＤを取得する。そして、コントローラ１１０６は、取得したライセンスＩＤと、ステップＳ４２０において受理した暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｄ）とを１つのデータにしてデータＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｄ）をバスＢＳを介して送信先のメモリカード４１へ入力する（ステップＳ４２２）。そうすると、メモリカード４１のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ３を介してデータＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｄ）を受理する（ステップＳ４２４）。そして、コントローラ１４２０は、バスＢＳ３を介して暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｄ）を復号処理部１４２２へ与え、復号処理部１４２２は、Ｋｃｍ保持部１４２１に保持されるメモリカード４１に固有なクラス秘密復号鍵Ｋｃｍ１によって復号処理することにより、セッション鍵Ｋｓ１ｄを復号し、セッション鍵Ｋｓ１ｄを受理する（ステップＳ４２６）。
【０１７８】
そうすると、コントローラ１１０６は、セッション鍵の出力要求をバスＢＳを介してメモリカード４１へ送信し（ステップＳ４２８）、メモリカード４１のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介してセッション鍵の出力要求を受理し、セッション鍵を発生するようにセッション鍵発生部１４１８を制御する。そして、セッション鍵発生部１４１８は、セッション鍵Ｋｓ２ｄを生成し（ステップＳ４３０）、コントローラ１４２０は、メモリカード４０からライセンスを受信する通信の履歴情報を記録するためのログエントリを図１１に示した所定の順序に従ってログ領域１４１５Ａの複数のログエントリ１６０１～１６０Ｍから採用する（ステップＳ４３２）。ここでは、ログエントリ１６０ｊ（１≦ｊ≦Ｍ）が採用されるものとする。
【０１７９】
その後、コントローラ１４２０は、受信したライセンスＩＤおよび生成されたセッション鍵Ｋｓ２ｄをログエントリ１６０ｊのそれぞれライセンスＩＤ領域１およびＫｓ２ｗ領域２に格納し、ステータス領域３のＳＴ１領域３１を「受信待」に変更する（ステップＳ４３４）。
【０１８０】
暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４２２よ

り与えられるセッション鍵Ｋｓ１ｄによって、切換スイッチ１４４６の接点を順次切換えることによって与えられるセッション鍵Ｋｓ２ｄ、および個別公開暗号鍵ＫＰｏｍ５を１つのデータ列として暗号化して、暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ／／ＫＰｏｍ５）をバスＢＳ３に出力する（ステップＳ４３６）。コントローラ１４２０は、バスＢＳ３に出力された暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ／／ＫＰｏｍ５）にライセンスＩＤ（ＬＩＤ）を加えたデータＬＩＤ／／Ｅ（Ｋｓ１ｄ，Ｋｓ２ｄ／／ＫＰｏｍ５）をバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２１のコントローラ１１０６に出力し（ステップＳ４３８）、コントローラ１１０６は、データＬＩＤ／／Ｅ（Ｋｓ１ｄ，Ｋｓ２ｄ／／ＫＰｏｍ５）を受理し（ステップＳ４４０）、その受理したデータＬＩＤ／／Ｅ（Ｋｓ１ｄ，Ｋｓ２ｄ／／ＫＰｏｍ５）をバスＢＳを介してメモリカード４０に送信する（ステップＳ４４２）。

【０１８１】

メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してデータＬＩＤ／／Ｅ（Ｋｓ１ｄ，Ｋｓ２ｄ／／ＫＰｏｍ５）を受理し（ステップＳ４４４）、復号処理部１４１２は、暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ／／ＫＰｏｍ５）をセッション鍵Ｋｓ１ｄによって復号し、メモリカード４１で生成されたセッション鍵Ｋｓ２ｄ、およびメモリカード４１の個別公開暗号鍵ＫＰｏｍ５を受理する（ステップＳ４４６）。そして、コントローラ１４２０は、図１１に示す所定の順序に従ってライセンスをメモリカード４１へ複製／移動する通信の履歴情報を記録するログエントリをログ領域１４１５Ａの複数のログエントリ１６０１～１６０Ｍから採用する（ステップＳ４４８）。ここでは、ログエントリ１６０ｋ（１≦ｋ≦Ｍ）が採用されるものとする。そして、コントローラ１４２０は、ライセンスＩＤとセッション鍵Ｋｓ２ｄとクラス公開暗号鍵ＫＰｃｍ１とをその採用したログエントリ１６０ｋのライセンスＩＤ領域１、Ｋｓ２ｗ領域２およびＫＰｃｍｙ領域４にそれぞれ格納し、ログエントリ１６０ｋのＳＴ１領域３１を「送信待」に変更する（ステップＳ４５０）。

【０１８２】

そうすると、端末装置２０のコントローラ１１０６からライセンスの格納位置が出力され（ステップＳ４５２）、メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してライセンスの格納位置を受理する（ステップＳ４５４）。その後、コントローラ１４２０は、受理したライセンスの格納位置によって指定されたライセンス領域１４１５ＢのエントリからライセンスＬＩＣを取得し（ステップＳ４５６）、取得したライセンスＬＩＣに含まれるライセンスＩＤがステップＳ４５０においてログエントリ１６０ｋのライセンスＩＤ領域１に記録されたライセンスＩＤに一致するか否かを判定し（ステップＳ４５８）、不一致であるときコントローラ１４２０は、エラー通知をバスＢＳ３、インタフェース１４２４および端子１４２６を介してコントローラ１１０６へ出力し（ステップＳ４８８）、コントローラ１１０６はエラー通知を受理し（ステップＳ４９０）、書込拒否によって一連の動作が終了する（ステップＳ４９２）。

【０１８３】

ステップＳ４５８において２つのライセンスＩＤが一致すると判定されたとき図１６のステップＳ４６０へ移行する。

【０１８４】

図１６を参照して、メモリカード４０のコントローラ１４２０は、ステップ４５６において取得したライセンスＬＩＣに含まれる制御情報ＡＣに基づいてライセンスをメモリカード４１へ複製／移動することが禁止されていないか否かを確認する（ステップＳ４６０）。そして、複製／移動が禁止されているときステップＳ４８８，Ｓ４９０を経て書込拒否によって一連の動作が終了する（ステップＳ４９２）。複製／移動が許可されているとき、暗号処理部１４１７は、ライセンスＬＩＣをメモリカード４１の個別公開暗号鍵ＫＰｏｍ５によって暗号化し（ステップＳ４６２）、暗号処理部１４０６は、切換スイッチ１４４６の接点Ｐｃを介して暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）を受理し、切換スイッチ

１４４２の接点Ｐｂを介して受理したセッション鍵Ｋｓ２ｄによって暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）をさらに暗号化する（ステップＳ４６４）。

【０１８５】

そうすると、コントローラ１４２０は、制御情報ＡＣに基づいてライセンスの複製が許可されているのか、ライセンスの移動が許可されているのかを判定し（ステップＳ４６６）、ライセンスの移動が許可されていると判定したとき、移動の対象となったライセンスが格納されているエントリに対応した有効フラグを無効にし（ステップＳ４６８）、ログエントリ１６０ｋのＳＴ１領域３１を送信済に変更する（ステップＳ４７０）。

【０１８６】

ステップＳ４６６において、ライセンスの複製が許可されていると判定されたとき、またはステップＳ４７０の後、メモリカード４０コントローラ１４２０は、暗号化データＥ（Ｋｓ２ｄ，Ｅ（ＫＰｏｍ５，ＬＩＣ））をバスＳ３、インタフェース１４２４および端子１４２６を介してコントローラ１１０６へ出力する（ステップＳ４７２）。

【０１８７】

コントローラ１１０６は、送信された暗号化データＥ（Ｋｓ２ｄ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を受信し、バスＢＳを介してメモリカード４１に入力する。そして、メモリカード４１は、暗号化データＥ（Ｋｓ２ｄ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を受理し（ステップＳ４７４）、復号処理部１４１２は、端子１４２６およびインタフェース１４２４を介して、バスＢＳ３に与えられた暗号化データＥ（Ｋｓ２ｄ，Ｅ（ＫＰｏｍ５，ＬＩＣ））をセッション鍵Ｋｓ２ｄによって復号して暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）を受理する（ステップＳ４７６）。そして、暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）は、復号処理部１４０４へ入力され、復号処理部１４０４は、Ｋｏｍ保持部１４０２に保持されるメモリカード４１の個別秘密復号鍵Ｋｏｍ５によって暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）を復号してライセンスＬＩＣを受理する（ステップＳ４７８）。

【０１８８】

そうすると、コントローラ１１０６からライセンスの格納位置が出力され（ステップＳ４８０）、メモリカード４１のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してライセンスの格納位置を受理する（ステップＳ４８２）。その後、メモリカード４１のコントローラ１４２０は、受理したライセンスＬＩＣに含まれるライセンスＩＤがステップＳ４３４においてログエントリ１６０ｊに格納されたライセンスＩＤに一致するか否かを判定し（ステップＳ４８４）、不一致であるときコントローラ１４２０は、エラー通知をバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２１のコントローラ１１０６へ出力する（ステップＳ４８６）。そして、端末装置２１のコントローラ１１０６は、エラー通知を受信して端末装置２０へ送信し、端末装置２０は、エラー通知を受理する（ステップＳ４９０）。そして、書込拒否によって一連の動作が終了する（ステップＳ４９２）。

【０１８９】

一方、ステップＳ４８４において２つのライセンスＩＤが一致したとき、コントローラ１４２０は、ライセンスＬＩＣをライセンス領域１４１５Ｂのライセンス格納位置によって指定されたライセンス領域１４１５Ｂのエントリに記録し（ステップＳ４９４）、ライセンスを受信する通信を記録するログエントリ１６０ｊのＳＴ１領域３１を「受信済」に変更し（ステップＳ４９６）、複製／移動処理が正常に終了する（ステップＳ４９８）。

【０１９０】

なお、暗号化コンテンツデータのメモリカード４０からメモリカード４１への移動／複製は、ライセンスの移動／複製が終了した後、メモリカード４０のデータ領域１４１５Ｃから暗号化コンテンツデータを読出してメモリカード４１へ送信することによって行なえば良い。

【０１９１】

また、受信側のメモリカード４１に対しては、移動／複製したライセンスに対するライセンス管理ファイルが既に記録されている場合には、ライセンス管理ファイルに対して格納

位置などの書込みを行なうことで対象のライセンス管理ファイルを更新する。また、対象となるライセンス管理ファイルがメモリカード４１に記録されていない場合には、新たにライセンス管理ファイルを生成し、その生成したライセンス管理ファイルを受信側のメモリカード４１に記録する。

【０１９２】

このようにして、端末装置２１に装着されたメモリカード４１が正規の機器であること、同時に、クラス公開暗号鍵ＫＰｃｍ１が有効であることを確認した上で、正規なメモリカードへの移動要求に対してのみライセンスを移動することができ、不正なメモリカードへの移動を禁止することができる。

【０１９３】

また、メモリカードで生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、ライセンスの移動／複製の動作におけるセキュリティを向上させることができる。

【０１９４】

［複製／移動における再送信］

上述した暗号化コンテンツデータのライセンスを複製／移動処理が不慮の中断によって終了した場合（これは、図１５のステップＳ４５２から図１６のステップＳ４８６，Ｓ４９４，Ｓ４９６の間に通信が切断されることにより複製／移動処理が終了する場合を含む。以下同じ。）、メモリカード４１へ対象となったライセンスを再送信できることが望ましい。

【０１９５】

なお、図１５のステップＳ４５２から図１６のステップＳ４８６，Ｓ４９４，Ｓ４９６の間の動作が再送信の対象となる理由は上述した理由と同じである。

【０１９６】

図１７～図１９は、ライセンスの複製／移動処理が中断によって終了した場合に、その送信の対象となったライセンスをメモリカード４１へ再送信する場合の動作を説明するための第１、第２および第３のフローチャートである。

【０１９７】

図１７を参照して、ライセンスの複製／移動処理における再送信の動作が開始されると、端末装置２０のコントローラ１１０６は、データＬＩＤ／／リカバリー要求をメモリカード４０へ送信する（ステップＳ５００）。そして、メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してデータＬＩＤ／／リカバリー要求を受理し、その受理したライセンスＩＤ（ＬＩＤ）と同じライセンスＩＤを含むログエントリがあるか否かを検索し（ステップＳ５０２）、同じライセンスＩＤを含む履歴情報がないときコントローラ１４２０はバスＢＳ３、インタフェース１４２４および端子１４２６を介してエラー通知をコントローラ１１０６へ出力し（ステップＳ６３０）、コントローラ１１０６はエラー通知を受信し（ステップＳ６３４）、書込拒否によって一連の動作が終了する（ステップＳ６３６）。

【０１９８】

ステップＳ５０２において、同じライセンスＩＤを含む履歴情報が検出されると、コントローラ１４２０は、その履歴情報を読出し、その読出した履歴情報に含まれるＳＴ１領域３１に基づいてライセンスがメモリカード４１へ送信されていないか否かを判定し（ステップＳ５０４）、ライセンスがメモリカード４１へ送信されている場合はステップＳ６３０へ移行し、上述したように書込拒否によって一連の動作が終了する（ステップＳ６３６）。

【０１９９】

ステップＳ５０４において、ライセンスがメモリカード４１へ送信されていないと判定されたとき、コントローラ１４２０は、ライセンスのメモリカード４１への再送信における通信を特定するためのセッション鍵Ｋｓ１ｅを発生するようにセッション鍵発生部１４１

８を制御し、セッション鍵発生部１４１８は、セッション鍵Ｋｓ１ｅを発生する（ステップＳ５０６）。そして、暗号処理部１４１０は、セッション鍵Ｋｓ１ｅをメモリカード４１のクラス公開暗号鍵ＫＰｃｍ１によって暗号化して暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｅ）を生成する（ステップＳ５０８）。そうすると、配信制御部３１５は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｅ）に送信の対象となったライセンスを識別するライセンスＩＤ（ＬＩＤ）を加えたデータＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｅ）をバスＢＳ３、インタフェースおよび端子１４２６を介してコントローラ１１０６へ送信する（ステップＳ５１０）。コントローラ１１０６は、データＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｅ）を受信し（ステップＳ５１２）、データＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｅ）をバスＢＳを介してメモリカード４１へ送信する（ステップＳ５１４）。そして、メモリカード４１のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してデータＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｅ）を受理する（ステップＳ５１６）。

【０２００】

コントローラ１４２０は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｅ）を復号処理部１４２２に与え、復号処理部１４２２は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｅ）をＫｃｍ保持部１４２１からのクラス秘密復号鍵Ｋｃｍ１によって復号してセッション鍵Ｋｓ１ｅを受理する（ステップＳ５１８）。

【０２０１】

そうすると、端末装置２０のコントローラ１１０６は、ログの出力要求を端末装置２１へ出力し、端末装置２１のコントローラ１１０６は、バスＢＳを介してメモリカード４１へログの出力要求へ出力し（ステップＳ５２０）、メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してログの出力要求を受理する（ステップＳ５２２）。そして、コントローラ１４２０は、ステップＳ５１６において受理したライセンスＩＤと同じライセンスＩＤをライセンスＩＤ領域１に記録しているログエントリを検索し（ステップＳ５２４）、そのログエントリを検出できないときエラー通知を生成してバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２１のコントローラ１１０６へ出力する（ステップＳ６３２）。その後、上述したように書込拒否により一連の動作が終了する（ステップＳ６３４，Ｓ６３６）。

【０２０２】

一方、ステップＳ５２４において、同一のライセンスＩＤを格納しているログエントリが検出されたとき、処理が継続される。すなわち、コントローラ１４２０は、ステップＳ５１６において受理したライセンスＩＤによってライセンス領域１４１５Ｂのエントリを検索し、そのライセンスＩＤと同じライセンスＩＤを含むライセンスを検索する（ステップＳ５２６）。そして、コントローラ１４２０は、図１５および図１６に示された移動・複製処理が中断した場合にはログエントリ１６０ｊが検出される。

【０２０３】

ステップＳ５２６において、ライセンスが検出されたとき、コントローラ１４２０は、検出したライセンスが記録されるエントリに対応する有効フラグ（図１２参照）によってライセンスの有効性を判定し（ステップＳ５２８）、検出したライセンスが有効であるとき、ステップＳ５２４においてログエントリ１６０ｊのＳＴ２領域３２を「データ有」に変更する（ステップＳ５３０）。一方、ステップＳ５２８においてライセンスが無効であると判定されたとき、コントローラ１４２０は、ログエントリ１６０ｊのＳＴ２領域３２を「移動済」に変更する（ステップＳ５３２）。この「移動済」の意味は、上述したとおりである。

【０２０４】

ステップＳ５２６において、ライセンスが検出されなかったとき、コントローラ１４２０は、メモリカード４１には送信の対象となったライセンスが存在しないことを意味するので、ログエントリ１６０ｊのＳＴ２領域３２を「データ無」に変更する（ステップＳ５３４）。

【０２０５】

ステップＳ５３０，Ｓ５３２，Ｓ５３４のいずれかの後、コントローラ１４２０は、ログエントリ１６０ｊ内の履歴情報（ログ）ＬＩＤ／／Ｋｓ２ｆ／／ＳＴ１／／ＳＴ２を取得し（ステップＳ５３６）、セッション鍵Ｋｓ２ｆを取り出して切換スイッチ１４４６の接点Ｐｆへ出力する。暗号処理部１４０６は、切換スイッチ１４４６の接点Ｐｆを介してセッション鍵Ｋｓ２ｆを受け、切換スイッチ１４４２の接点Ｐａを介してセッション鍵Ｋｓ１ｅを受ける。そして、暗号処理部１４０６は、セッション鍵Ｋｓ２ｆをセッション鍵Ｋｓ１ｅによって暗号化し、暗号化データＥ（Ｋｓ１ｅ，Ｋｓ２ｆ）をバスＢＳ３へ出力する（ステップＳ５３８）。

【０２０６】

そうすると、コントローラ１４２０は、バスＢＳ３上の暗号化データＥ（Ｋｓ１ｅ，Ｋｓ２ｆ）に、ステップＳ５３６において取得した履歴情報に格納されたライセンスＩＤ、およびステータス情報（ＳＴ１，ＳＴ２）を加えたログデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２を生成し、その生成したログデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２のハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２）を演算する（ステップＳ５４０）。そして、コントローラ１４２０は、ハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２）をバスＢＳ３を介して切換スイッチ１４４６の接点Ｐｆへ出力し、暗号処理部１４０６は、切換スイッチ１４４６の接点Ｐｆを介してハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２）を受け、その受けたハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２）をセッション鍵Ｋｓ１ｅによって暗号化して署名データＥ（Ｋｓ１ｅ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２））をバスＢＳ３へ出力する（ステップＳ５４２）。

【０２０７】

その後、コントローラ１４２０は、署名データＥ（Ｋｓ１ｅ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２））に、ログデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２を加えた署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｅ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２））を生成してバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２１のコントローラ１１０６へ出力する（ステップＳ５４４）。

【０２０８】

コントローラ１１０６は、メモリカード４１から受けた署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｅ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２））を受理し（ステップＳ５４６）、その受理した署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｅ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２））をメモリカード４０へ出力する（ステップＳ５４８）。

【０２０９】

図１８を参照して、メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｅ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２））を受理する（ステップＳ５５０）。

【０２１０】

そうすると、コントローラ１４２０は、署名データＥ（Ｋｓ１ｅ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２））を復号処理部１４１２に与え、復号処理部１４１２は、署名データＥ（Ｋｓ１ｅ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２））をセッション鍵Ｋｓ１ｅによって復号し、その復号したハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２）をコントローラ１４２０へ出力する。また、コントローラ１４２０は、ログデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２に対するハッシュ値を演算し、その演算したハッシュ値がメ

モリカード４１において演算されたハッシュ値H（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２）に一致するか否かを確認する。そして、コントローラ１４２０は、復号処理部１４１２において署名データＥ（Ｋｓ１ｅ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２））が復号されたこと、および２つのハッシュ値が一致することを確認することによりメモリカード４１から受信した署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｅ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２））を検証する（ステップＳ５５２）。

【０２１１】

署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｅ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２））が非承認であるとき、上述したように書込拒否によって一連の動作は終了する（ステップＳ６３６）。一方、ステップＳ５５２において署名付きログデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｅ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｆ）／／ＳＴ１／／ＳＴ２））が承認されたとき、コントローラ１４２０は、ライセンスＩＤによってライセンス領域１４１５Ｂのエントリを検索し、メモリカード４１への送信の対象となったライセンスが存在するか否かを検索する（ステップＳ５５４）。そして、ライセンスが存在しないとき、ステップＳ６３０へ移行して書込拒否によって一連の動作が終了する（ステップＳ６３６）。

【０２１２】

ステップＳ５５４においてライセンスが存在していた場合、コントローラ１４２０は、そのライセンスのエントリに対応した有効フラグによってライセンスの有効性を判定し（ステップＳ５５６）、ライセンスが有効であるときステップＳ５６２へ移行する。一方、ステップＳ５５６においてライセンスが無効であると判定されたとき、コントローラ１４２０は、メモリカード４１から受理した履歴情報のＳＴ１領域３１およびＳＴ２領域３２のデータに基づいてメモリカード４１が実際にライセンスを受信しているか否かを判定し（ステップＳ５５８）、メモリカード４１がライセンスを実際に受信済であるときステップＳ６３０へ移行して書込拒否によって一連の動作が終了する（ステップＳ６３６）。

【０２１３】

ステップＳ５５８において、メモリカード４１が実際にライセンスを受信していないと判定されたとき、コントローラ１４２０は、検索したライセンスを有効にし（ステップＳ５６０）、リカバリー通知をバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２０のコントローラ１１０６へ出力する（ステップＳ５６２）。そして、コントローラ１１０６は、端末装置２１へリカバリー通知を出力し、端末装置２１のコントローラ１１０６はリカバリー通知を受理する（ステップＳ５６４）。

【０２１４】

そうすると、コントローラ１１０６は、セッション鍵要求をバスＢＳを介してメモリカード４１へ送信し（ステップＳ５６６）、メモリカード４１のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してセッション鍵要求を受理する。そうすると、コントローラ１４２０は、セッション鍵発生部１４１８を制御し、セッション鍵発生部１４１８は、セッション鍵Ｋｓ２ｅを生成する（ステップＳ５６８）。そして、コントローラ１４２０は、図１１に示すフローチャートに従ってメモリカード４０がメモリカード４１へライセンスを再送信する通信を記録するための履歴情報をログ領域１４１５Ａのログエントリ１６０１～１６０Ｍから採用する（ステップＳ５７０）。ここでは、必ず、ログエントリ１６０ｊが採用される。

【０２１５】

コントローラ１４２０は、ステップＳ５１６において受理したライセンスＩＤとセッション鍵発生部１４１８によって生成されたセッション鍵Ｋｓ２ｅとを採用したログエントリ１６０ｊに格納し、ログエントリ１６０ｊのＳＴ１領域３１を「受信待」に変更する（ステップＳ５７２）。その後、暗号処理部１４０６は、切換スイッチ１４４６の接点Ｐｅを介してＫＰｏｍ保持部１４１６からの個別公開暗号鍵ＫＰｏｍ５を受理し、切換スイッチ

１４４６の接点Ｐｄを介してセッション鍵Ｋｓ２ｅを受理し、セッション鍵Ｋｓ２ｅと個別公開暗号鍵ＫＰｏｍ５とをセッション鍵Ｋｓ１ｅによって暗号化して暗号化データＥ（Ｋｓ１ｅ，Ｋｓ２ｅ／／ＫＰｏｍ５）を生成してバスＢＳ３へ出力する（ステップＳ５７４）。そして、コントローラ１４２０は、暗号化データＥ（Ｋｓ１ｅ，Ｋｓ２ｅ／／ＫＰｏｍ５）にライセンスＩＤを加えたデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｅ／／ＫＰｏｍ５）をバスＢＳ３、インタフェース１４２４および端子１４２６を介してコントローラ１１０６へ出力し（ステップＳ５７６）、コントローラ１１０６は、データＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｅ／／ＫＰｏｍ５）を受理する（ステップＳ５７８）。そして、コントローラ１１０６は、データＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｅ／／ＫＰｏｍ５）をメモリカード４０へ出力し（ステップＳ５８０）、メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してデータＬＩＤ／／Ｅ（Ｋｓ１ｅ，Ｋｓ２ｅ／／ＫＰｏｍ５）を受理する（ステップＳ５８２）。

【０２１６】

メモリカード４０においては、復号処理部１４１２は、暗号化データＥ（Ｋｓ１ｅ，Ｋｓ２ｅ／／ＫＰｏｍ５）をセッション鍵Ｋｓ１ｅによって復号してセッション鍵Ｋｓ２ｅと個別公開暗号鍵ＫＰｏｍ５とを受理する（ステップＳ５８４）。

【０２１７】

図１９を参照して、ステップＳ５８４の後、コントローラ１４２０は、図１１に示す所定の順序に従ってライセンスをメモリカード４１へ再送信する通信を記録するためのログエントリを複数のログエントリ１６０１～１６０Ｍの中から採用する（ステップＳ５８６）。この場合、必ずログエントリ１６０ｋが選択される。そして、コントローラ１４２０は、ステップＳ５８２において受信したライセンスＩＤとセッション鍵発生部１４１８によって発生されたセッション鍵Ｋｓ２ｅとクラス公開暗号鍵ＫＰｃｍ１とを採用したログエントリ１６０ｋのライセンスＩＤ領域１、Ｋｓ２ｗ領域２およびＫＰｃｍｙ領域４にそれぞれ記録し、ログエントリ１６０ｋのＳＴ１領域３１を「送信待」に変更する（ステップＳ５８８）。

【０２１８】

そうすると、コントローラ１１０６からライセンスの格納位置がメモリカード４０へ出力され（ステップＳ５９０）、メモリカード４０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してライセンスの格納位置を受理する（ステップＳ５９２）。その後、コントローラ１４２０は、受理したライセンスの格納位置によって指定されたエントリからライセンスＬＩＣを取得し（ステップＳ５９４）、取得したライセンスＬＩＣに含まれるライセンスＩＤがステップＳ５８８においてログエントリ１６０ｊに格納されたライセンスＩＤに一致するか否かを判定し（ステップＳ５９６）、不一致であるときコントローラ１４２０は、エラー通知をバスＢＳ３、インタフェース１４２４および端子１４２６を介してコントローラ１１０６へ出力し（ステップＳ６３０）、コントローラ１１０６はエラー通知を受理し（ステップＳ６３４）、書込拒否によって一連の動作が終了する（ステップＳ６３６）。

【０２１９】

ステップＳ５９６において２つのライセンスＩＤが一致すると判定されたとき、コントローラ１４２０は、ステップ５９４において取得したライセンスＬＩＣに含まれる制御情報ＡＣに基づいてライセンスをメモリカード４１へ複製／移動することが禁止されていないか否かを確認する（ステップＳ５９８）。そして、複製／移動が禁止されているときステップＳ６３０，Ｓ６３４を経て書込拒否によって一連の動作が終了する（ステップＳ６３６）。複製／移動が許可されているとき、暗号処理部１４１７は、ライセンスＬＩＣをメモリカード４１の個別公開暗号鍵ＫＰｏｍ５によって暗号化し（ステップＳ６００）、暗号処理部１４０６は、切換スイッチ１４４６の接点Ｐｃを介して暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）を受理し、切換スイッチ１４４２の接点Ｐｂを介して受理したセッション鍵Ｋｓ２ｅによって暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）をさらに暗号化する（ステップＳ６０２）。

【０２２０】
そうすると、コントローラ１４２０は、制御情報ＡＣに基づいてライセンスの複製が許可されているのか、ライセンスの移動が許可されているのかを判定し（ステップＳ６０４）、ライセンスの移動が許可されていると判定したとき、移動の対象となったライセンスが記録されているエントリに対応した有効フラグを無効にし（ステップＳ６０６）、ログエントリ１６０ｋのＳＴ１領域３１を送信済に変更する（ステップＳ６０８）。
【０２２１】
ステップＳ６０４において、ライセンスの複製が許可されていると判定されたとき、またはステップＳ６０８の後、コントローラ１４２０は、暗号化データＥ（Ｋｓ２ｅ，Ｅ（ＫＰｏｍ５，ＬＩＣ））をバスＳ３、インタフェース１４２４および端子１４２６を介してコントローラ１１０６へ出力する（ステップＳ６１０）。
【０２２２】
コントローラ１１０６は、送信された暗号化データＥ（Ｋｓ２ｅ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を受信し、バスＢＳを介してメモリカード４１に入力する。そして、メモリカード４０は、暗号化データＥ（Ｋｓ２ｅ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を受理し（ステップＳ６１２）、復号処理部１４１２は、端子１４２６およびインタフェース１４２４を介して、バスＢＳ３に与えられた暗号化データＥ（Ｋｓ２ｅ，Ｅ（ＫＰｏｍ５，ＬＩＣ））をセッション鍵Ｋｓ２ｅによって復号して暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）を受理する（ステップＳ６１４）。そして、暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）は、復号処理部１４０４へ入力され、復号処理部１４０４は、Ｋｏｍ保持部１４０２に保持される個別秘密復号鍵Ｋｏｍ５によって暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）を復号してライセンスＬＩＣを受理する（ステップＳ６１６）。
【０２２３】
そうすると、コントローラ１１０６からライセンスの格納位置がメモリカード４１へ出力され（ステップＳ６１８）、メモリカード４１のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介してライセンスの格納位置を受理する（ステップＳ６２０）。その後、コントローラ１４２０は、受理したライセンスＬＩＣに含まれるライセンスＩＤがステップＳ５７２においてログエントリ１６０ｊのライセンスＩＤ領域１に格納されたライセンスＩＤに一致するか否かを判定し（ステップＳ６２２）、不一致であるときコントローラ１４２０は、エラー通知をバスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２１のコントローラ１１０６へ出力し（ステップＳ６３２）、コントローラ１１０６は、エラー通知を受理する（ステップＳ６３４）。そして、書込拒否により一連の動作が終了する（ステップＳ６３６）。
【０２２４】
一方、ステップＳ６２２において２つのライセンスＩＤが一致したとき、メモリカード４１のコントローラ１４２０は、ライセンスＬＩＣをライセンス領域１４１５Ｂのライセンス格納位置によって指定された位置に記録し（ステップＳ６２４）、ログエントリ１６０ｊのＳＴ１領域３１を「受信済」に変更し（ステップＳ６２６）、複製／移動の再送処理が正常に終了する（ステップＳ６２８）。
【０２２５】
なお、暗号化コンテンツデータのメモリカード４０からメモリカード４１への移動／複製は、ライセンスの移動／複製が終了した後、メモリカード４０のデータ領域１４１５Ｃから暗号化コンテンツデータを読出してメモリカード４１へ送信することによって行なえば良い。
【０２２６】
暗号化コンテンツデータのライセンスをメモリカード４１へ再送信するセッションが書込拒否によって終了した場合（これは、図１９のステップＳ６１０～Ｓ６２６の間に通信が切断されることにより再送信の処理が終了する場合を含む。以下同じ。）、図１７～図１９に示すフローチャートに従ってライセンスがメモリカード４１へ再送信される。
【０２２７】

なお、図１９のステップＳ６１０～Ｓ６２６の間の動作がライセンスの再送信の対象となる理由は上述した理由と同じである。

【０２２８】

［再生］

上述したように、端末装置２０に装着されたメモリカード４０は、ダウンロードサーバ１０から、直接、暗号化コンテンツデータおよびライセンスを受信できる。また、メモリカード４１は、メモリカード４０から暗号化コンテンツデータおよびライセンスを、「移動」という概念によって受信できる。

【０２２９】

そこで、次に、これらの各種の方法によってメモリカードが受信した暗号化コンテンツデータの再生について説明する。

【０２３０】

図２０は、メモリカード４０が受信した暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）の端末装置２０のコンテンツ再生回路１５５０における再生動作を説明するためのフローチャートである。メモリカード４１を端末装置２０に装着しても再生は可能であり、この場合も図２０に従って再生が行なわれる。なお、図２０における処理以前に、端末装置２０のユーザは、メモリカード４０のデータ領域１４１５Ｃに記録されている再生リストに従って、再生するコンテンツ（楽曲）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【０２３１】

図２０を参照して、再生動作の開始とともに、端末装置２０のユーザから操作パネル１１０８を介して再生リクエストが端末装置２０にインプットされる。そうすると、コントローラ１１０６は、バスＢＳ２を介して認証データの出力要求をコンテンツ再生回路１５５０に行ない、コンテンツ再生回路１５５０は、認証データＣｐ３を出力し、コントローラ１１０６は、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード４０へ認証データＣｐ３を入力する（ステップＳ７００）。

【０２３２】

そうすると、メモリカード４０は、認証データＣｐ３＝ＫＰｃｐ３／／ｌｃｐ３／／Ｅ（Ｋａ，Ｈ（ＫＰｃｐ３／／ｌｃｐ３））を受理し、復号処理部１４０８は、受理した認証データＣｐ３のうち、署名データＥ（Ｋａ，Ｈ（ＫＰｃｐ３／／ｌｃｐ３））をＫＰａ保持部１４１４に保持された認証鍵ＫＰａによって復号し、その復号したハッシュ値Ｈ（ＫＰｃｐ３／／ｌｃｐ３）をコントローラ１４２０へ出力する。コントローラ１４２０は、認証データＣｐ３のうちデータＫＰｃｐ３／／ｌｃｐ３に対するハッシュ値を演算し、その演算したハッシュ値がコンテンツ再生回路１５５０において演算されたハッシュ値Ｈ（ＫＰｃｐ３／／ｌｃｐ３）に一致するか否かを確認する。そして、コントローラ１４２０は、コンテンツ再生回路１５５０から受理した認証データＣｐ３のうち、署名データＥ（Ｋａ，Ｈ（ＫＰｃｐ３／／ｌｃｐ３））が復号処理部１４０８において復号されたこと、および２つのハッシュ値が一致することを確認することによりコンテンツ再生回路１５５０から受理した認証データＣｐ３を検証する（ステップＳ７０４）。認証データＣｐ３が非承認である場合、コントローラ１４２０は、バスＢＳ３、インタフェース１４２４および端子１４２６を介して端末装置２０のコントローラ１１０６へエラー通知を出力し（ステップＳ７５２）、コントローラ１１０６は、エラー通知を受理する（ステップＳ７５４）。そして、再生拒否によって一連の動作が終了する（ステップＳ７５６）。

【０２３３】

認証データＣｐ３が承認された場合、コントローラ１４２０は、公開暗号鍵ＫＰｃｐ３を受理し（ステップＳ７０６）、セッション鍵を発生するようにセッション鍵発生部１４１８を制御する。そうすると、セッション鍵発生部１４１８は、再生処理用のセッション鍵Ｋｓ１ｇを発生する（ステップＳ７０８）。そして、暗号処理部１４１０は、セッション鍵発生部１４１８からのセッション鍵Ｋｓ１ｇを、復号処理部１４０８で復号されたクラス公開暗号鍵ＫＰｃｐ３によって暗号化した暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｇ）を

バスＢＳ３へ出力する（ステップＳ７１０）。そうすると、コントローラ１４２０は、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｇ）を出力する（ステップＳ７１２）。端末装置２０のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｇ）を受理する（ステップＳ７１４）。そして、コントローラ１１０６は、暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｇ）をバスＢＳ２を介してコンテンツ再生回路１５５０の復号処理部１５０４へ与え、復号処理部１５０４は、Ｋｃｐ保持部１５０２から出力された、公開暗号鍵ＫＰｃｐ３と対になっているクラス秘密復号鍵Ｋｃｐ３によって暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｇ）を復号し、セッション鍵Ｋｓ２ｇを暗号処理部１５０６へ出力する（ステップＳ７１６）。そうすると、セッション鍵発生部１５０８は、再生処理用のセッション鍵Ｋｓ２ｇを発生させ、その発生させたセッション鍵Ｋｓ２ｇを暗号処理部１５０６へ出力する（ステップＳ７１８）。暗号処理部１５０６は、セッション鍵発生部１５０８からのセッション鍵Ｋｓ２ｇを復号処理部１５０４からのセッション鍵Ｋｓ１ｇによって暗号化して暗号化データＥ（Ｋｓ１ｇ，Ｋｓ２ｇ）を生成し（ステップＳ７２０）、コントローラ１１０６は、バスＢＳ３およびメモリカードインタフェース１２００を介して暗号化データＥ（Ｋｓ１ｇ，Ｋｓ２ｇ）をメモリカード４０へ出力する（ステップＳ７２２）。

【０２３４】

そうすると、メモリカード４０の復号処理部１４１２は、端子１４２６、インタフェース１４２４、およびバスＢＳ３を介して暗号化データＥ（Ｋｓ１ｇ，Ｋｓ２ｇ）を入力する（ステップＳ７２４）。復号処理部１４１２は、セッション鍵発生部１４１８において発生されたセッション鍵Ｋｓ１ｇによって暗号化データＥ（Ｋｓ１ｇ，Ｋｓ２ｇ）を復号して、端末装置２０で発生されたセッション鍵Ｋｓ２ｇを受理する（ステップＳ７２６）。

【０２３５】

端末装置２０のコントローラ１１０６は、メモリカード４０から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されている格納位置を取得し、メモリカードインタフェース１２００を介してメモリカード４０へ取得した格納位置を出力する（ステップＳ７２８）。

【０２３６】

メモリカード４０のコントローラ１４２０は、格納位置を受理し（ステップＳ７３０）、その受理した格納位置によって指定されたエントリに格納されたライセンスおよびエントリに対応した有効フラグを取得する。そして、コントローラ１４２０は、ライセンスの有効性を有効フラグにより確認する（ステップＳ７３２）。ステップＳ７３２において、ライセンスが「無効」の場合、指定されたエントリにライセンスが存在しないので、ステップＳ７５２，７５４を介して再生動作が再生拒否により終了する（ステップＳ７５６）。ステップＳ７３２において、ライセンスが「有効」の場合、指定された格納位置のエントリにライセンスが存在するのでライセンスを取得する（ステップＳ７３４）。

【０２３７】

そして、コントローラ１４２０は、制御情報ＡＣを確認する（ステップＳ７３６）。

【０２３８】

ステップＳ７３６においては、制御情報ＡＣを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、制御情報ＡＣの再生回数に制限がある場合には制御情報ＡＣの再生回数を変更した（ステップＳ７３８）後に次のステップに進む（ステップＳ７４０）。

【０２３９】

一方、制限情報ＡＣの再生回数によって再生が制限されていない場合においては、ステップＳ７３８はスキップされ、制御情報ＡＣの再生回数は変更されることなく処理が次のステップ（ステップＳ７４０）に進行される。

【０２４０】

ステップＳ７３６において、当該再生動作において再生が可能であると判断された場合に

は、メモリ１４１５のライセンス領域１４１５Ｂに記録された再生リクエスト曲のコンテンツ鍵ＫｃがバスＢＳ３上に出力される（ステップＳ７４０）。

【０２４１】

得られたコンテンツ鍵Ｋｃは、切換スイッチ１４４６の接点Ｐｆを介して暗号処理部１４０６に送られる。暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッション鍵Ｋｓ２ｇによって切換スイッチ１４４６を介して受けたコンテンツ鍵Ｋｃを暗号化し（ステップＳ７４２）、暗号化データＥ（Ｋｓ２ｇ，Ｋｃ）をバスＢＳ３に出力する（ステップＳ７４４）。

【０２４２】

バスＢＳ３に出力された暗号化データＥ（Ｋｓ２ｇ，Ｋｃ）は、インタフェース１４２４、端子１４２６、およびメモリカードインタフェース１２００を介して端末装置２０のコントローラ１１０６に送出される。

【０２４３】

端末装置２０においては、コントローラ１１０６は、メモリカードインタフェース１２００を介してバスＢＳ２に伝達される暗号化データＥ（Ｋｓ２ｇ，Ｋｃ）を受理し（ステップＳ７４６）、その受理した暗号化データＥ（Ｋｓ２ｇ，Ｋｃ）を復号処理部１５１０へ出力し、復号処理部１５１０は、暗号化データＥ（Ｋｓ２ｇ，Ｋｃ）をセッション鍵Ｋｓ２ｇによって復号し、コンテンツ鍵Ｋｃを受理する（ステップＳ７４８）。そして、復号処理部１５１０は、コンテンツ鍵Ｋｃを復号処理部１５１６に出力する。

【０２４４】

コントローラ１１０６は、メモリカードインタフェース１２００を介してメモリカード４０に暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を要求する。そうすると、メモリカード４０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を取得し、バスＢＳ３、インタフェース１４２４、および端子１４２６を介してメモリカードインタフェース１２００へ暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を出力する。

【０２４５】

端末装置２０のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を取得し、バスＢＳ２を介して暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）をコンテンツ再生回路１５５０へ与える。

【０２４６】

そして、コンテンツ再生回路１５５０の復号処理部１５１６は、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を復号処理部１５１０から出力されたコンテンツ鍵Ｋｃによって復号してコンテンツデータＤｃを取得する。

【０２４７】

そして、復号されたコンテンツデータＤｃは音楽再生部１５１８へ出力され、音楽再生部１５１８は、コンテンツデータを再生し、ＤＡ変換器１５１９はディジタル信号をアナログ信号に変換して端子１５３０へ出力する。そして、音楽データは端子１５３０から外部出力装置を介してヘッドホーンへ出力されて再生される。これによって再生動作が正常に終了する（ステップＳ７５０）。

【０２４８】

上記においては、暗号化コンテンツデータを復号するためのライセンスを例にして、ライセンスの復元処理について説明したが、本発明においては、復元の対象となるものは暗号化コンテンツデータを復号するためのライセンスに限らず、個人情報、およびクレジットカードの情報等の同時に２個以上存在してはいけない機密性が要求されるデータが復元の対象となる。このようなデータについても、上述した各処理を行なうことができる。

【０２４９】

この場合、機密性が要求されるデータをライセンス内のコンテンツ鍵Ｋｃと入れ替えることにより容易に実現できる。

【０２５０】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおいて暗号化コンテンツデータのライセンスを取得したメモリカード間におけるライセンスの移動を説明するための概念図である。

【図３】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図５】　図１に示すダウンロードサーバの構成を示す概略ブロック図である。

【図６】　図１に示す端末装置の構成を示す概略ブロック図である。

【図７】　図１に示すメモリカードの構成を示すブロック図である。

【図８】　図７に示すログ領域の構成を示すブロック図である。

【図９】　図１に示すデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図１０】　図１に示すデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図１１】　図９に示すステップＳ１２８の詳細な動作を説明するためのフローチャートである。

【図１２】　メモリカードにおける再生リストとライセンス領域との構成を示すブロック図である。

【図１３】　図１に示すデータ配信システムにおける再配信の動作を説明するための第１のフローチャートである。

【図１４】　図１に示すデータ配信システムにおける再配信の動作を説明するための第２のフローチャートである。

【図１５】　メモリカード間における複製／移動の動作を説明するための第１のフローチャートである。

【図１６】　メモリカード間における複製／移動の動作を説明するための第２のフローチャートである。

【図１７】　メモリカード間における複製／移動の再動作を説明するための第１のフローチャートである。

【図１８】　メモリカード間における複製／移動の再動作を説明するための第２のフローチャートである。

【図１９】　メモリカード間における複製／移動の再動作を説明するための第３のフローチャートである。

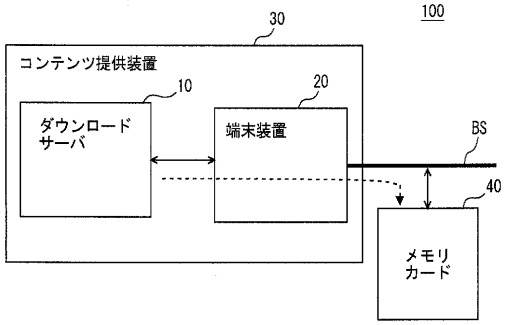
【図２０】　端末装置における暗号化コンテンツデータの再生動作を説明するためのフローチャートである。

【符号の説明】

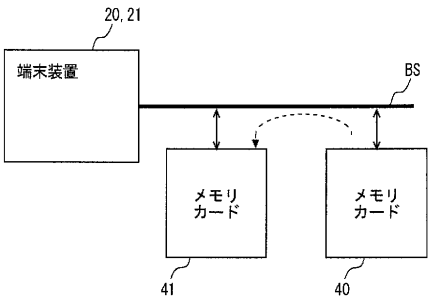
１　ライセンスＩＤ領域、２　Ｋｓ２ｗ領域、３　ステータス領域、４　ＫＰｃｍｙ領域、５　記録順序番号、１０　ダウンロードサーバ、２０，２１　端末装置、３０　コンテンツ提供装置、３１　ＳＴ１領域、３２　ＳＴ２領域、４０，４１　メモリカード、１００　データ配信システム、１６０　再生リストファイル、１６５　エントリ管理情報、３０２　課金データベース、３０４　情報データベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４１２，１４２２，１５０４，１５１０，１５１６　復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６，１４１８，１５０８　セッション鍵発生部、３１８，３２６，３２８，１４０６，１４１０，１４１７，１５０６　暗号処理部、３５

０　通信装置、１１０６，１４２０　コントローラ、１４２６，１５３０　端子、１１０８　操作パネル、１１１０　表示パネル、１２００　メモリカードインタフェース、１４００，１５００　認証データ保持部、１４０２　Ｋｏｍ保持部、１４１４　ＫＰａ保持部、１４１５　メモリ、１４１５Ａ　ログ領域、１４１５Ｂ　ライセンス領域、１４１５Ｃ　データ領域、１４１６　ＫＰｍｃ保持部、１４２１　Ｋｃｍ保持部、１４２４　インタフェース、１４４２，１４４６　切換スイッチ、１５０２　Ｋｃｐ保持部、１５１８　音楽再生部、１５１９　ＤＡ変換器、１５５０　コンテンツ再生回路、１６０１～１６０Ｍ　エントリ、１６１１～１６１ｎ　コンテンツファイル、１６２１～１６２ｎ　ライセンス管理ファイル、１７００～１７０Ｍ　管理情報記憶部。

【図１】



【図２】



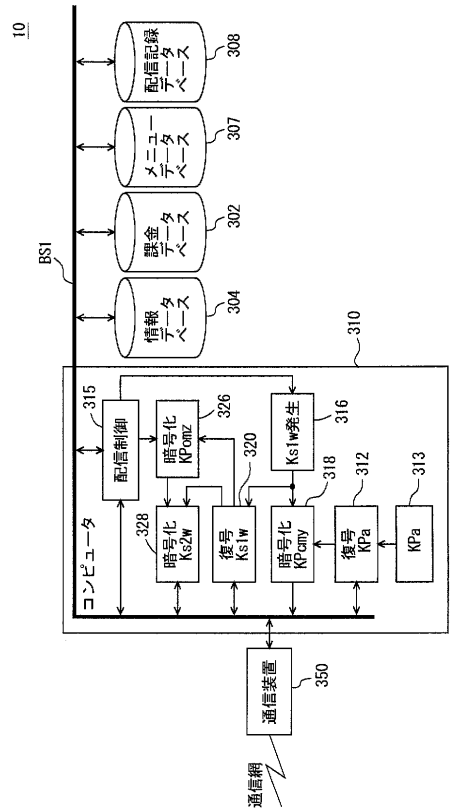
【図３】

名称	記号	属性	特性
データ	Dc	データ固有	例：音楽データ、朗読データ、教材データ、画像データ コンテンツ鍵にて暗号化した暗号化データ E(Kc, Dc)として記録管理される
データ情報	Di	データ固有	Dcに付随する平文データ。DIDを含む
データID	DID	データ固有	データおよびコンテンツ鍵を特定するための管理コード
コンテンツ鍵	Kc	データ固有	暗号データを暗号／復号する共通鍵
制御情報	AC	ライセンス固有	再生やライセンスの取り扱いに対する制限事項
ライセンスID	LID	ライセンス固有	ライセンスを特定するための管理コード
ライセンス	LIC	ライセンス固有	Kc//AC//DID//LIDの総称

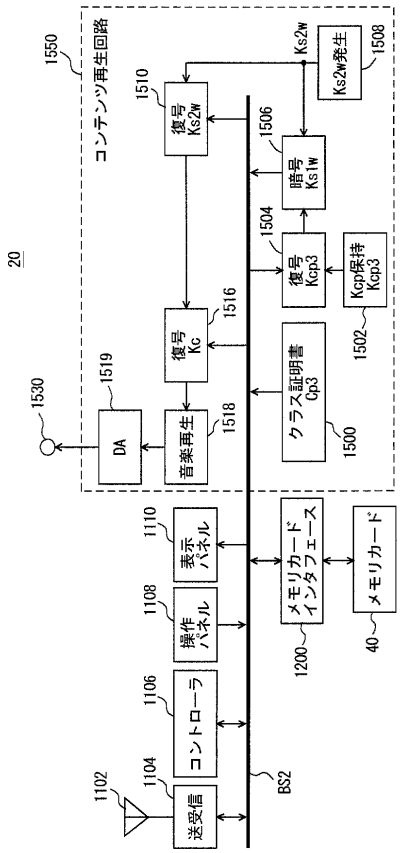
【図４】

名称	記号	特性
マスタ鍵	Ka	クラス証明書作成のために使用する秘密暗号鍵。 認証局にて運用される
認証鍵	KPa	認証局にて証明書を検証する公開復号鍵。 ライセンス提供側にて運用される
クラス公開暗号鍵	KPcxy	機器のクラス（種類などの一定の単位ごと）に付与される暗号鍵。 xは機器を識別する識別子。再生装置ではsp、記憶装置ではsmとする。 yはクラスを識別するための識別子
クラス秘密復号鍵	Kcxy	クラス公開暗号鍵KPcxyにて暗号化されたデータを復号する非対称な復号鍵
クラス情報	Icxy	クラスごとの機器およびクラス公開暗号鍵に関する情報データ
クラス証明書	Cxy	KPcxy // Icxy // E（Ka, H（KPcxy // Icxy）） 認証鍵によってその正当性を確認できる
個別公開暗号鍵	KPomz	記憶装置ごとに固有な値を持つ個別公開暗号鍵 zは記憶装置を識別するための識別子
個別秘密復号鍵	Komz	個別公開暗号鍵KPomzにて暗号化されたデータを復号する非対称な復号鍵
セッション鍵	Ks1w	ライセンスの授受ごとにライセンスの送信元で生成される一時鍵 共通鍵、wはセッション鍵の発生を識別するための識別子
セッション鍵	Ks2w	ライセンスの授受ごとにライセンスの送信先で生成される一時鍵 共通鍵、wはセッション鍵の発生を識別するための識別子

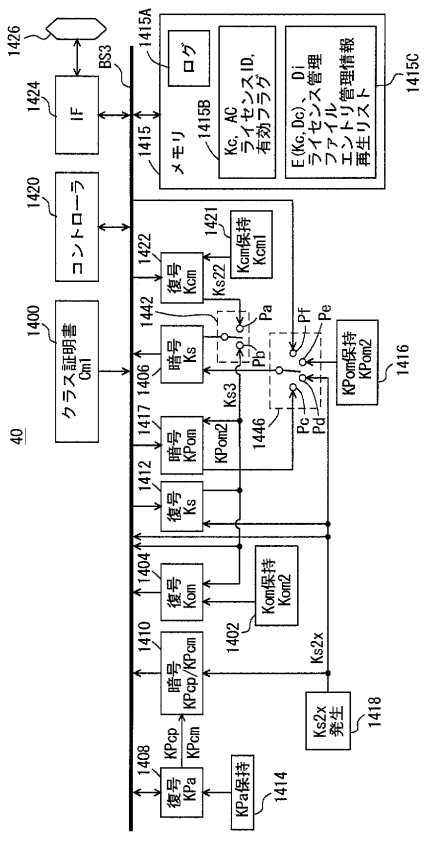
【図５】



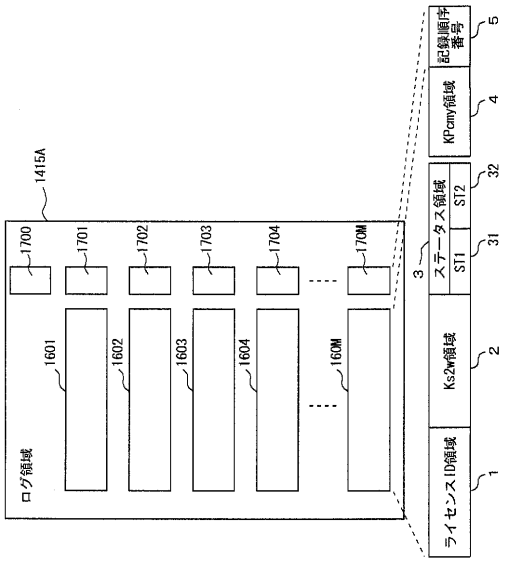
【図６】



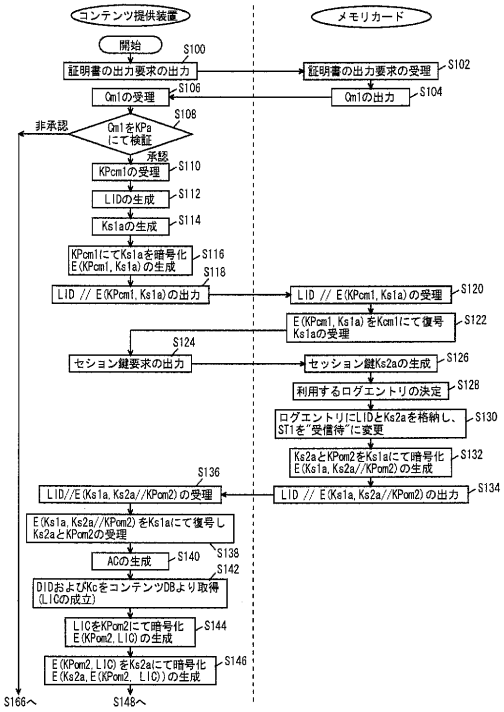
【図７】



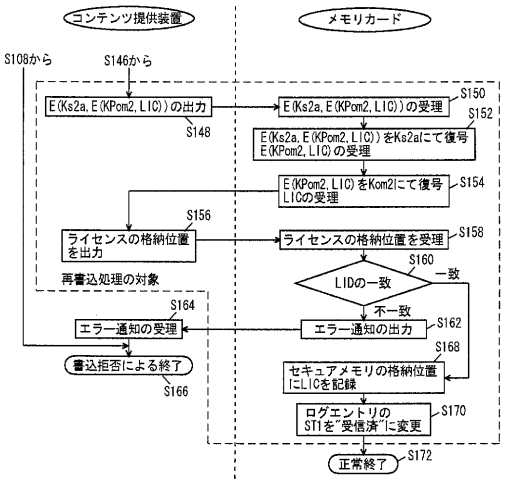
【図８】


1415A
1700
1701
1702
1703
1704
170M
1601
1602
1603
1604
160M
ログ領域
ライセンスID領域
Ks2a領域
ステータス領域
ST1
ST2
KPcmv領域
記録順序番号
1
2
3
4
5
31
32

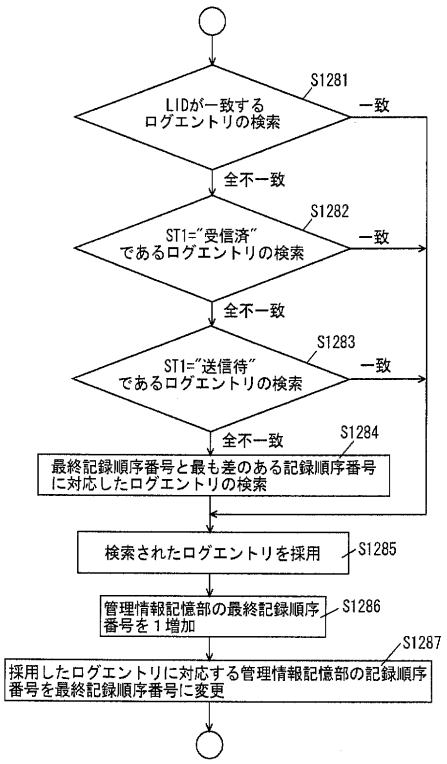
【図９】


コンテンツ提供装置
メモリカード
開始
S100
証明書の出力要求の出力
S102
証明書の出力要求の受理
S104
Cm1の出力
S106
Cm1の受理
S108
Cm1をKPaにて検証
非承認
承認
S110
KPcm1の受理
S112
LIDの生成
S114
Ks1aの生成
S116
KPcm1にてKs1aを暗号化 E(KPcm1, Ks1a)の生成
S118
LID // E(KPcm1, Ks1a)の出力
S120
LID // E(KPcm1, Ks1a)の受理
S122
E(KPcm1, Ks1a)をKcm1にて復号 Ks1aの受理
S124
セション鍵要求の出力
S126
セッション鍵Ks2aの生成
S128
利用するログエントリの決定
S130
ログエントリにLIDとKs2aを格納し、ST1を"受信待"に変更
S132
Ks2aとKPcm2をKs1aにて暗号化 E(Ks1a, Ks2a//KPcm2)の生成
S134
LID // E(Ks1a, Ks2a//KPcm2)の出力
S136
LID//E(Ks1a, Ks2a//KPcm2)の受理
E(Ks1a, Ks2a//KPcm2)をKs1aにて復号しKs2aとKPcm2の受理
S138
ACの生成
S140
DIDおよびKcをコンテンツDBより取得(LICの成立)
S142
LICをKPcm2にて暗号化 E(KPcm2, LIC)の生成
S144
E(KPcm2, LIC)をKs2aにて暗号化 E(Ks2a, E(KPcm2, LIC))の生成
S146
S166へ
S148へ

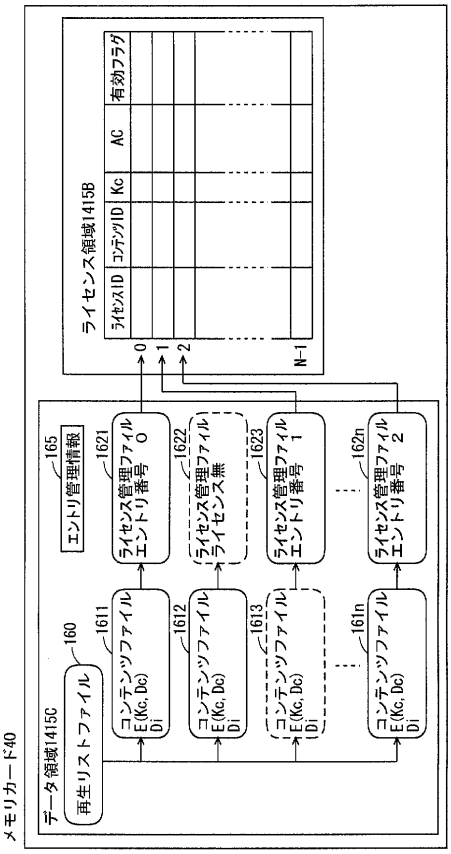
【図１０】


コンテンツ提供装置
メモリカード
S108から
S146から
E(Ks2a, E(KPcm2, LIC))の出力
S148
E(Ks2a, E(KPcm2, LIC))の受理
S150
E(Ks2a, E(KPcm2, LIC))をKs2aにて復号 E(KPcm2, LIC)の受理
S152
E(KPcm2, LIC)をKcm2にて復号 LICの受理
S154
ライセンスの格納位置を出力
S156
ライセンスの格納位置を受理
S158
LIDの一致
S160
一致
不一致
再書込処理の対象
エラー通知の受理
S164
エラー通知の出力
S162
書込拒否による終了
S166
セキュアメモリの格納位置にLICを記録
S168
ログエントリのST1を"受信済"に変更
S170
正常終了
S172

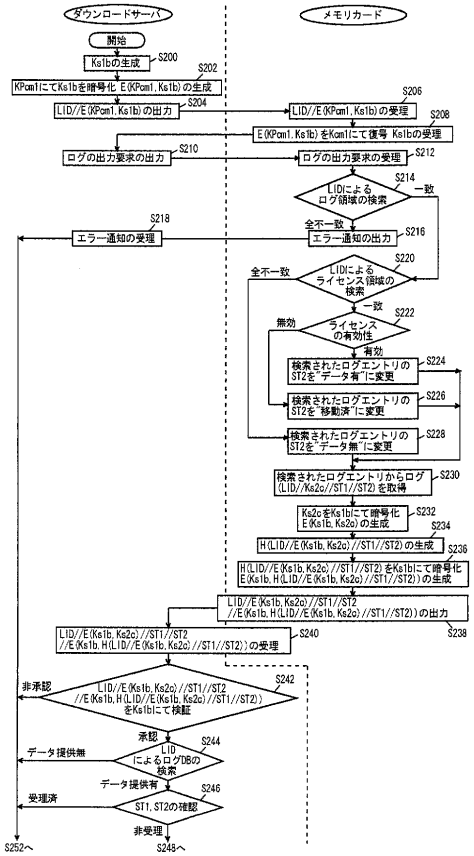
【図１１】


S1281
LIDが一致するログエントリの検索
一致
全不一致
S1282
ST1="受信済"であるログエントリの検索
一致
全不一致
S1283
ST1="送信待"であるログエントリの検索
一致
全不一致
S1284
最終記録順序番号と最も差のある記録順序番号に対応したログエントリの検索
検索されたログエントリを採用
S1285
管理情報記憶部の最終記録順序番号を１増加
S1286
S1287
採用したログエントリに対応する管理情報記憶部の記録順序番号を最終記録順序番号に変更

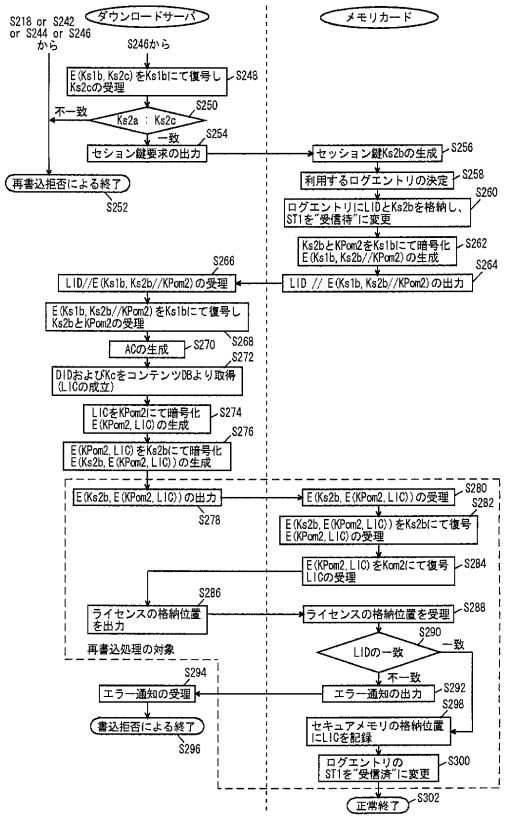
【図１２】



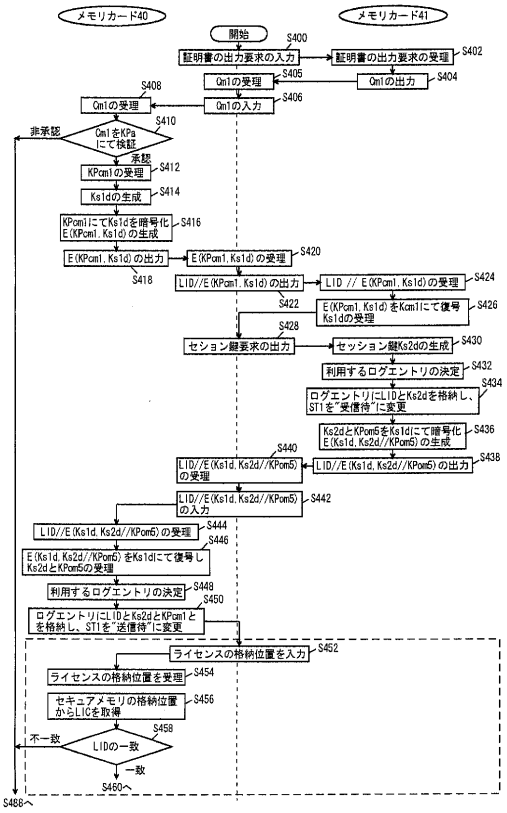
【図１３】



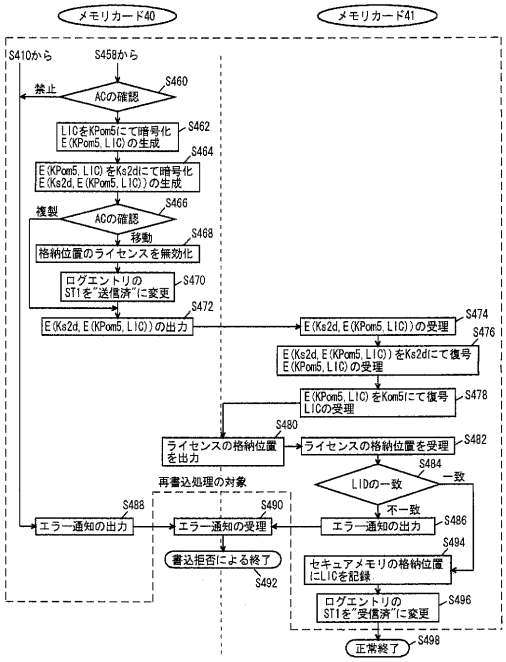
【図１４】



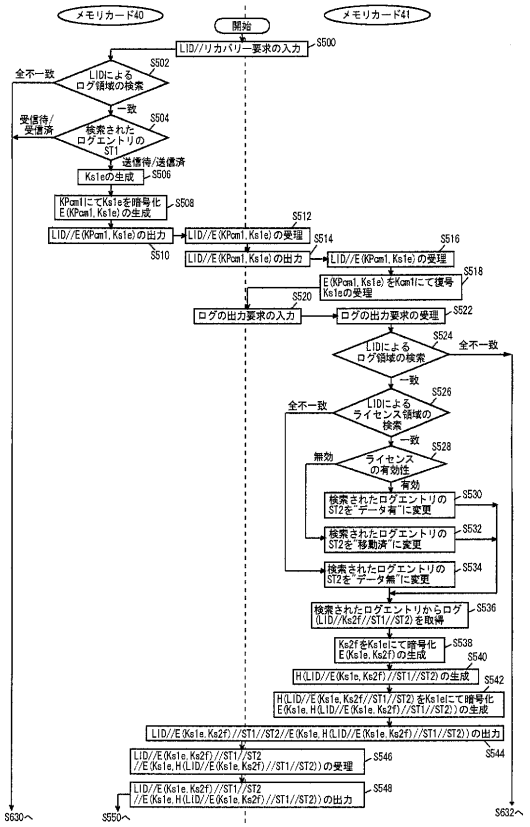
【図１５】



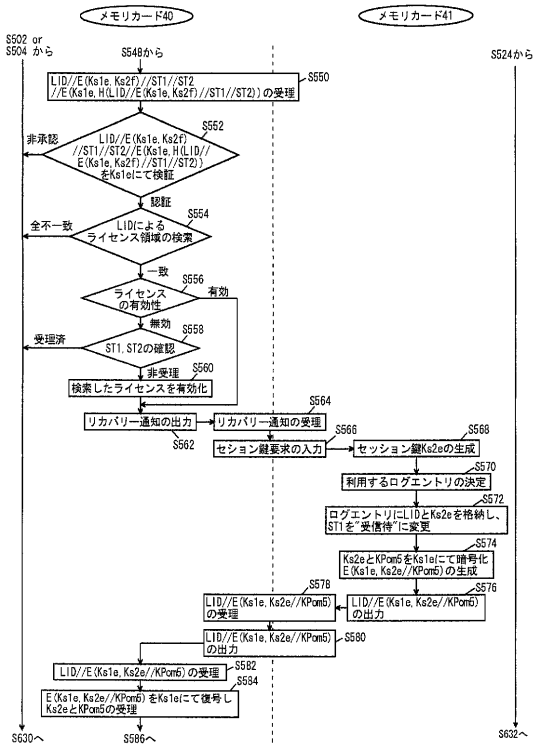
【図１６】



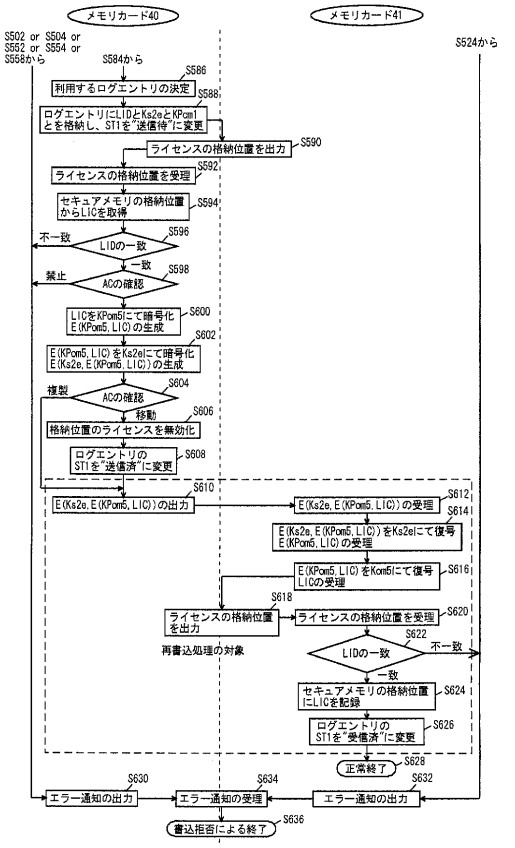
【図１７】



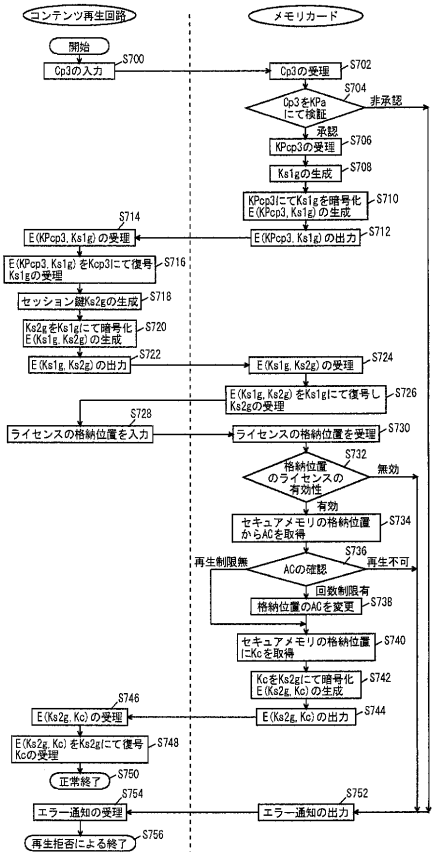
【図１８】



【図１９】



【図２０】


コンテンツ再生回路
メモリカード
開始
S700
Cp3の入力
S702
Cp3の受理
S704
Cp3をKPaにて検証
非承認
承認
S706
KPcp3の受理
S708
Ks1gの生成
S710
KPcp3にてKs1gを暗号化 E(KPcp3, Ks1g)の生成
S712
E(KPcp3, Ks1g)の出力
S714
E(KPcp3, Ks1g)の受理
S716
E(KPcp3, Ks1g)をKcp3にて復号 Ks1gの受理
S718
セッション鍵Ks2gの生成
S720
Ks2gをKs1gにて暗号化 E(Ks1g, Ks2g)の生成
S722
E(Ks1g, Ks2g)の出力
S724
E(Ks1g, Ks2g)の受理
S726
E(Ks1g, Ks2g)をKs1gにて復号し Ks2gの受理
S728
ライセンスの格納位置を入力
S730
ライセンスの格納位置を受理
S732
格納位置のライセンスの有効性
無効
有効
S734
セキュアメモリの格納位置からACを取得
S736
再生制限無
ACの確認
再生不可
回数制限有
S738
格納位置のACを変更
S740
セキュアメモリの格納位置にKcを取得
S742
KcをKs2gにて暗号化 E(Ks2g, Kc)の生成
S744
E(Ks2g, Kc)の出力
S746
E(Ks2g, Kc)の受理
S748
E(Ks2g, Kc)をKs2gにて復号 Kcの受理
正常終了
S750
S752
エラー通知の出力
S754
エラー通知の受理
再生拒否による終了
S756

フロントページの続き

(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
(72)発明者　平井　達哉
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所　横浜ラボラトリ内

審査官　赤穂　州一郎

(56)参考文献　国際公開第０１／０４１３５６（WO，Ａ１）
特開平０３－２３１３３７（ＪＰ，Ａ）
特開平１０－２８３２２９（ＪＰ，Ａ）
特開平１１－０３９４５０（ＪＰ，Ａ）
特開２００１－０３６５２３（ＪＰ，Ａ）
国際公開第００／００８９０９（WO，Ａ１）
米国特許第０６０７８３３８（ＵＳ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/24