(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5644467号
(P5644467)
(45)発行日　平成26年12月24日(2014.12.24)　(24)登録日　平成26年11月14日(2014.11.14)

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

請求項の数 20　(全 39 頁)

(21)出願番号　特願2010-282607 (P2010-282607)
(22)出願日　平成22年12月20日 (2010.12.20)
(65)公開番号　特開2012-133426 (P2012-133426A)
(43)公開日　平成24年7月12日 (2012.7.12)
審査請求日　平成25年11月6日 (2013.11.6)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100086531
弁理士　澤田　俊夫
(74)代理人　100095496
弁理士　佐々木　榮二
(74)代理人　110000763
特許業務法人大同特許事務所

最終頁に続く

(54)【発明の名称】情報処理装置、および情報処理方法、並びにプログラム

(57)【特許請求の範囲】
【請求項１】
置換鍵を適用した暗号化領域を含む第１暗号化コンテンツをホスト装置に提供するサーバと、
前記サーバから前記第１暗号化コンテンツと、置換鍵を適用した暗号化領域を示す置換鍵適用領域情報を受信するホスト装置と、
前記サーバから前記置換鍵と、サーバからのコンテンツ配信処理単位で異なる設定とされた個別鍵を受信し、前記第１暗号化コンテンツの置換鍵適用領域を、個別鍵による暗号化領域に変更する鍵掛け替え処理を実行して鍵掛け替え処理後の第２暗号化コンテンツをデータ記録領域に格納するデータ記憶装置と、
を有するコンテンツ提供システム。
【請求項２】
前記データ記憶装置は、
前記置換鍵を外部からのアクセスを許容しない保護領域に格納し、データ記憶装置内部において前記鍵掛け替え処理を実行する請求項１に記載のコンテンツ提供システム。
【請求項３】
前記ホスト装置は、
前記置換鍵適用領域情報を参照して、サーバから受信した前記第１暗号化コンテンツから置換鍵を適用した暗号化領域データを抽出して前記データ記憶装置に提供し、
前記データ記憶装置は、前記ホスト装置から受領した置換鍵適用暗号化領域データを個

別鍵による暗号化領域に変更する鍵掛け替え処理を実行する請求項１に記載のコンテンツ提供システム。

【請求項４】

前記サーバは、

前記第１暗号化コンテンツを、前記置換鍵を適用した暗号化領域である置換鍵適用領域と、コンテンツ対応のタイトル鍵を適用した暗号化領域であるタイトル鍵適用領域の混在した暗号化コンテンツを前記ホスト装置に提供し、

前記データ記憶装置は、

前記サーバから前記置換鍵と、前記個別鍵と、前記タイトル鍵を受信し、前記置換鍵を外部からのアクセスを許容しない第１保護領域に格納し、前記個別鍵と、前記タイトル鍵は、認証の成立した外部装置からのアクセスを許容する第２保護領域に格納する請求項１に記載のコンテンツ提供システム。

【請求項５】

外部から入力する置換鍵による暗号化データを、コンテンツ配信処理単位で異なる設定とされた個別鍵による暗号化データに変更する鍵掛け替え処理を実行するデータ処理部と、

前記置換鍵を格納した記憶領域であり、外部からのアクセスを禁止した第１保護領域と、

前記個別鍵を格納した記憶領域であり、認証の成立した外部装置からのアクセスを許容した第２保護領域を有するデータ記憶装置。

【請求項６】

前記データ記憶装置は、

サーバとの相互認証実行し、該相互認証の成立を条件として、サーバから前記置換鍵と個別鍵を受信し、前記置換鍵を第１保護領域に格納し、前記個別鍵を第２保護領域に格納する請求項５に記載のデータ記憶装置。

【請求項７】

前記データ記憶装置は、

ホスト装置との通信を実行して、該ホスト装置から受信した置換鍵適用暗号化領域データを個別鍵による暗号化領域に変更する鍵掛け替え処理を実行する請求項５に記載のデータ記憶装置。

【請求項８】

前記データ記憶装置は、

コンテンツ再生を実行する再生装置であるホスト装置から、前記第２保護領域に対するアクセス権限を記録したホスト証明書を受信し、

前記ホスト証明書の記載に基づいて、前記第２保護領域に対するホスト装置のアクセス権限が認められた場合に前記第２保護領域に格納された個別鍵を前記ホスト装置に提供する請求項５に記載のデータ記憶装置。

【請求項９】

置換鍵を適用した暗号化領域を含む第１暗号化コンテンツと、前記置換鍵を適用した暗号化領域を示す置換鍵適用領域情報を取得し、前記置換鍵適用領域情報を参照して、前記第１暗号化コンテンツから置換鍵を適用した暗号化領域データを抽出してデータ記憶装置に提供し、データ記憶装置における鍵掛け替え処理によって生成された個別鍵暗号化領域データを受信し、該受信データを元の置換鍵適用領域に設定した第２暗号化コンテンツを生成して、前記データ記憶装置に格納するデータ処理部を有する情報処理装置。

【請求項１０】

前記情報処理装置は、

前記第１暗号化コンテンツと、前記置換鍵適用領域情報をサーバから受信する通信部を有し、

前記データ処理部は、前記サーバとの相互認証処理を実行し、相互認証の成立を条件として、前記サーバから前記第１暗号化コンテンツと、前記置換鍵適用領域情報を受信する

請求項９に記載の情報処理装置。
【請求項１１】
置換鍵を適用した暗号化領域を含む第１暗号化コンテンツと、
前記置換鍵と、前記置換鍵の暗号化領域に対する鍵掛け替え後の暗号鍵であり、コンテンツ配信処理単位で異なる設定とした個別鍵と、
前記置換鍵を適用した暗号化領域を示す置換鍵適用領域情報と、
を取得または生成してクライアントに送信する処理を実行するデータ処理部を有するサーバ装置。
【請求項１２】
前記データ処理部は、
前記クライアントを構成するデータ記憶装置との相互認証処理を実行し、該相互認証処理の成立を条件として、前記置換鍵と前記個別鍵を暗号化して前記データ記憶装置に送信する請求項１１に記載のサーバ装置。
【請求項１３】
前記データ処理部は、
前記個別鍵を、前記クライアントと対応付けた管理情報を生成して記憶部に格納する処理を行う請求項１１に記載のサーバ装置。
【請求項１４】
コンテンツ配信処理単位で異なる設定とした個別鍵による暗号化領域を含む暗号化コンテンツの再生処理を実行する再生装置であり、
データ記憶装置との相互認証処理を実行し、該相互認証処理の成立を条件として前記データ記憶装置から個別鍵を読み出し、
さらに、前記データ記憶装置から、前記個別鍵による暗号化領域を示す暗号化領域情報を取得し、該暗号化領域情報を参照して鍵選択を実行して暗号化コンテンツの復号処理を実行するデータ処理部を有する再生装置。
【請求項１５】
データ記憶装置において実行する情報処理方法であり、
データ処理部が、外部から置換鍵による暗号化データを入力するステップと、
前記データ処理部が、外部からのアクセスを禁止した第１保護領域から置換鍵を取得し、前記暗号化データの復号処理を実行して復号データを生成するステップと、
前記データ処理部が、認証の成立した外部装置からのアクセスを許容した第２保護領域から、コンテンツ配信処理単位で異なる設定とされた個別鍵を取得し、取得した個別鍵を適用して前記復号データの暗号化を実行して鍵掛け替え処理を行うステップとを実行する情報処理方法。
【請求項１６】
情報処理装置において実行する情報処理方法であり、
データ処理部が、置換鍵を適用した暗号化領域を含む第１暗号化コンテンツと、前記置換鍵を適用した暗号化領域を示す置換鍵適用領域情報を取得し、前記置換鍵適用領域情報を参照して、前記第１暗号化コンテンツから置換鍵を適用した暗号化領域データを抽出してデータ記憶装置に提供し、データ記憶装置における鍵掛け替え処理によって生成された個別鍵暗号化領域データを受信し、該受信データを元の置換鍵適用領域に設定した第２暗号化コンテンツを生成して、前記データ記憶装置に格納する情報処理方法。
【請求項１７】
コンテンツ配信を実行するサーバ装置における情報処理方法であり、
データ処理部が、
置換鍵を適用した暗号化領域を含む第１暗号化コンテンツと、
前記置換鍵と、前記置換鍵の暗号化領域に対する鍵掛け替え後の暗号鍵であり、コンテンツ配信処理単位で異なる設定とした個別鍵と、
前記置換鍵を適用した暗号化領域を示す置換鍵適用領域情報と、
を取得または生成してクライアントに送信する処理を実行する情報処理方法。

【請求項１８】
データ記憶装置においてデータ処理を実行させるプログラムであり、
データ処理部に、外部から置換鍵による暗号化データを入力させるステップと、
前記データ処理部に、外部からのアクセスを禁止した第１保護領域から置換鍵を取得し、前記暗号化データの復号処理を実行して復号データを生成させるステップと、
前記データ処理部に、認証の成立した外部装置からのアクセスを許容した第２保護領域から、コンテンツ配信処理単位で異なる設定とされた個別鍵を取得し、取得した個別鍵を適用して前記復号データの暗号化を実行して鍵掛け替え処理を行わせるステップとを実行させるプログラム。
【請求項１９】
情報処理装置において情報処理を実行させるプログラムであり、
データ処理部において、置換鍵を適用した暗号化領域を含む第１暗号化コンテンツと、前記置換鍵を適用した暗号化領域を示す置換鍵適用領域情報を取得し、前記置換鍵適用領域情報を参照して、前記第１暗号化コンテンツから置換鍵を適用した暗号化領域データを抽出してデータ記憶装置に提供し、データ記憶装置における鍵掛け替え処理によって生成された個別鍵暗号化領域データを受信し、該受信データを元の置換鍵適用領域に設定した第２暗号化コンテンツを生成して、前記データ記憶装置に格納する処理を実行させるプログラム。
【請求項２０】
コンテンツ配信を実行するサーバ装置において情報処理を実行させるプログラムであり、
データ処理部に、
置換鍵を適用した暗号化領域を含む第１暗号化コンテンツと、
前記置換鍵と、前記置換鍵の暗号化領域に対する鍵掛け替え後の暗号鍵であり、コンテンツ配信処理単位で異なる設定とした個別鍵と、
前記置換鍵を適用した暗号化領域を示す置換鍵適用領域情報と、
を取得または生成してクライアントに送信する処理を実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、および情報処理方法、並びにプログラムに関する。特に、コンテンツの不正利用の防止構成を実現する情報処理装置、および情報処理方法、並びにプログラムに関する。
【背景技術】
【０００２】
昨今、情報記録媒体として、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）や、Ｂｌｕ－ｒａｙ　Ｄｉｓｃ（登録商標）、あるいはフラッシュメモリなど、様々なメディアが利用されている。特に、昨今は、大容量のフラッシュメモリを搭載したＵＳＢメモリなどのメモリカードの利用が盛んになっている。ユーザは、このような様々な情報記録媒体（メディア）に音楽や映画などのコンテンツを記録して再生装置（プレーヤ）に装着してコンテンツの再生を行うことができる。
【０００３】
また、近年、ネットワークを介したコンテンツの流通が盛んになり、ユーザによるコンテンツ購入処理の形態は、コンテンツを予め記録したディスクの購入処理から、ネットワーク接続したサーバからダウンロードする処理に次第にシフトしている。
【０００４】
具体的なコンテンツ購入形態としては、ＲＯＭディスク等のメディアの購入を行う処理の他、例えば、以下のようなコンテンツ購入形態がある。
（ａ）ネットワーク接続可能な端末やＰＣ等のユーザ装置を利用してコンテンツ提供サーバに接続して、コンテンツをダウンロードして購入するＥＳＴ（Ｅｌｅｃｔｒｉｃ　Ｓ

ｅｌｌ　Ｔｈｒｏｕｇｈ）。
（ｂ）コンビニや、駅等の公共スペースに設置された共用端末を利用して、ユーザのメディア（メモリカード等）にコンテンツを記録するＭｏＤ（Ｍａｎｕｆａｃｔｕｒｉｎｇ　ｏｎ　Ｄｅｍａｎｄ）。
【０００５】
このように、ユーザは、コンテンツ記録用のメモリカードなどのメディアを有していれば、様々なコンテンツ提供プロバイダ等のコンテンツソースから自由に様々なコンテンツを選択購入し、自分のメディアに記録することができる。
なお、ＥＳＴ、ＭｏＤ等の処理については、例えば特許文献１（特開２００８－９８７６５号公報）に記載されている。
【０００６】
しかし、音楽データ、画像データ等の多くのコンテンツは、その作成者あるいは販売者に著作権、頒布権等が保有されている。従って、ユーザにコンテンツを提供する場合には、一定の利用制限、すなわち正規な利用権を持つユーザのみにコンテンツの利用を許諾し、許可のないコピー等の無秩序な利用が行われないような制御を行うのが一般的となっている。
【０００７】
具体的には、ユーザが映画等のコンテンツをサーバからダウンロードしてユーザのメモリカード等の記録メディアに記録する場合、例えば以下のような処理が行われる。
サーバはコンテンツを暗号化コンテンツとしてクライアント（ユーザ装置）に提供する。
さらに、正規なコンテンツ購入処理を行ったユーザにのみ、暗号化コンテンツを復号するための鍵を提供する。
このようなコンテンツ提供処理を行うことで、コンテンツの利用制御を実現しようとしている。
【０００８】
しかし、上述の処理を行っても、例えば、正規なコンテンツ購入処理を行ったユーザが、サーバから取得したコンテンツ復号用の鍵を、他人に提供してしまうことを防止することは難しい。具体的には、サーバから取得した鍵をネット上で公開するなどして、不特定多数のユーザが利用可能な状態に設定されることも想定される。このような行為が行われると、この流出鍵を用いて誰でも暗号化コンテンツの復号、再生、利用を行うことが可能となり、コンテンツの不正利用が蔓延するといった事態が発生する。
【先行技術文献】
【特許文献】
【０００９】
【特許文献１】特開２００８－９８７６５号公報
【発明の概要】
【発明が解決しようとする課題】
【００１０】
本発明は、例えば上記問題点に鑑みてなされたものであり、暗号化コンテンツの復号に利用される鍵の流出によるコンテンツ不正利用を効果的に防止する構成を実現する情報処理装置、および情報処理方法、並びにプログラムを提供することを目的とする。
【課題を解決するための手段】
【００１１】
本発明の第１の側面は、
置換鍵を適用した暗号化領域を含む第１暗号化コンテンツをホスト装置に提供するサーバと、
前記サーバから前記第１暗号化コンテンツと、置換鍵を適用した暗号化領域を示す置換鍵適用領域情報を受信するホスト装置と、
前記サーバから前記置換鍵と、サーバからのコンテンツ配信処理単位で異なる設定とさ

れた個別鍵を受信し、前記第１暗号化コンテンツの置換鍵適用領域を、個別鍵による暗号化領域に変更する鍵掛け替え処理を実行して鍵掛け替え処理後の第２暗号化コンテンツをデータ記録領域に格納するデータ記憶装置と、
を有するコンテンツ提供システムにある。
【００１２】
さらに、本発明のコンテンツ提供システムの一実施態様において、前記データ記憶装置は、前記置換鍵を外部からのアクセスを許容しない保護領域に格納し、データ記憶装置内部において前記鍵掛け替え処理を実行する。
【００１３】
さらに、本発明のコンテンツ提供システムの一実施態様において、前記ホスト装置は、前記置換鍵適用領域情報を参照して、サーバから受信した前記第１暗号化コンテンツから置換鍵を適用した暗号化領域データを抽出して前記データ記憶装置に提供し、前記データ記憶装置は、前記ホスト装置から受領した置換鍵適用暗号化領域データを個別鍵による暗号化領域に変更する鍵掛け替え処理を実行する。
【００１４】
さらに、本発明のコンテンツ提供システムの一実施態様において、前記サーバは、前記第１暗号化コンテンツを、前記置換鍵を適用した暗号化領域である置換鍵適用領域と、コンテンツ対応のタイトル鍵を適用した暗号化領域であるタイトル鍵適用領域の混在した暗号化コンテンツを前記ホスト装置に提供し、前記データ記憶装置は、前記サーバから前記置換鍵と、前記個別鍵と、前記タイトル鍵を受信し、前記置換鍵を外部からのアクセスを許容しない第１保護領域に格納し、前記個別鍵と、前記タイトル鍵は、認証の成立した外部装置からのアクセスを許容する第２保護領域に格納する。
【００１５】
さらに、本発明の第２の側面は、
外部から入力する置換鍵による暗号化データを、コンテンツ配信処理単位で異なる設定とされた個別鍵による暗号化データに変更する鍵掛け替え処理を実行するデータ処理部と、
前記置換鍵を格納した記憶領域であり、外部からのアクセスを禁止した第１保護領域と、
前記個別鍵を格納した記憶領域であり、認証の成立した外部装置からのアクセスを許容した第２保護領域を有するデータ記憶装置にある。
【００１６】
さらに、本発明のデータ記憶装置の一実施態様において、前記データ記憶装置は、サーバとの相互認証実行し、該相互認証の成立を条件として、サーバから前記置換鍵と個別鍵を受信し、前記置換鍵を第１保護領域に格納し、前記個別鍵を第２保護領域に格納する。
【００１７】
さらに、本発明のデータ記憶装置の一実施態様において、前記データ記憶装置は、ホスト装置との通信を実行して、該ホスト装置から受信した置換鍵適用暗号化領域データを個別鍵による暗号化領域に変更する鍵掛け替え処理を実行する。
【００１８】
さらに、本発明のデータ記憶装置の一実施態様において、前記データ記憶装置は、コンテンツ再生を実行する再生装置であるホスト装置から、前記第２保護領域に対するアクセス権限を記録したホスト証明書を受信し、前記ホスト証明書の記載に基づいて、前記第２保護領域に対するホスト装置のアクセス権限が認められた場合に前記第２保護領域に格納された個別鍵を前記ホスト装置に提供する。
【００１９】
さらに、本発明の第３の側面は、
置換鍵を適用した暗号化領域を含む第１暗号化コンテンツと、前記置換鍵を適用した暗号化領域を示す置換鍵適用領域情報を取得し、前記置換鍵適用領域情報を参照して、前記第１暗号化コンテンツから置換鍵を適用した暗号化領域データを抽出してデータ記憶装置

に提供し、データ記憶装置における鍵掛け替え処理によって生成された個別鍵暗号化領域データを受信し、該受信データを元の置換鍵適用領域に設定した第２暗号化コンテンツを生成して、前記データ記憶装置に格納するデータ処理部を有する情報処理装置にある。

【００２０】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記第１暗号化コンテンツと、前記置換鍵適用領域情報をサーバから受信する通信部を有し、前記データ処理部は、前記サーバとの相互認証処理を実行し、相互認証の成立を条件として、前記サーバから前記第１暗号化コンテンツと、前記置換鍵適用領域情報を受信する。

【００２１】

さらに、本発明の第４の側面は、

置換鍵を適用した暗号化領域を含む第１暗号化コンテンツと、

前記置換鍵と、前記置換鍵の暗号化領域に対する鍵掛け替え後の暗号鍵であり、コンテンツ配信処理単位で異なる設定とした個別鍵と、

前記置換鍵を適用した暗号化領域を示す置換鍵適用領域情報と、

を取得または生成してクライアントに送信する処理を実行するデータ処理部を有するサーバ装置にある。

【００２２】

さらに、本発明のサーバ装置の一実施態様において、前記データ処理部は、前記クライアントを構成するデータ記憶装置との相互認証処理を実行し、該相互認証処理の成立を条件として、前記置換鍵と前記個別鍵を暗号化して前記データ記憶装置に送信する。

【００２３】

さらに、本発明のサーバ装置の一実施態様において、前記データ処理部は、前記個別鍵を、前記クライアントと対応付けた管理情報を生成して記憶部に格納する処理を行う。

【００２４】

さらに、本発明の第５の側面は、

コンテンツ配信処理単位で異なる設定とした個別鍵による暗号化領域を含む暗号化コンテンツの再生処理を実行する再生装置であり、

データ記憶装置との相互認証処理を実行し、該相互認証処理の成立を条件として前記データ記憶装置から個別鍵を読み出し、

さらに、前記データ記憶装置から、前記個別鍵による暗号化領域を示す暗号化領域情報を取得し、該暗号化領域情報を参照して鍵選択を実行して暗号化コンテンツの復号処理を実行するデータ処理部を有する再生装置にある。

【００２５】

さらに、本発明の第６の側面は、

データ記憶装置において実行する情報処理方法であり、

データ処理部が、外部から置換鍵による暗号化データを入力するステップと、

前記データ処理部が、外部からのアクセスを禁止した第１保護領域から置換鍵を取得し、前記暗号化データの復号処理を実行して復号データを生成するステップと、

前記データ処理部が、認証の成立した外部装置からのアクセスを許容した第２保護領域から、コンテンツ配信処理単位で異なる設定とされた個別鍵を取得し、取得した個別鍵を適用して前記復号データの暗号化を実行して鍵掛け替え処理を行うステップとを実行する情報処理方法にある。

【００２６】

さらに、本発明の第７の側面は、

情報処理装置において実行する情報処理方法であり、

データ処理部が、置換鍵を適用した暗号化領域を含む第１暗号化コンテンツと、前記置換鍵を適用した暗号化領域を示す置換鍵適用領域情報を取得し、前記置換鍵適用領域情報を参照して、前記第１暗号化コンテンツから置換鍵を適用した暗号化領域データを抽出してデータ記憶装置に提供し、データ記憶装置における鍵掛け替え処理によって生成された

個別鍵暗号化領域データを受信し、該受信データを元の置換鍵適用領域に設定した第２暗号化コンテンツを生成して、前記データ記憶装置に格納する情報処理方法にある。

【００２７】

さらに、本発明の第８の側面は、

コンテンツ配信を実行するサーバ装置における情報処理方法であり、

データ処理部が、

置換鍵を適用した暗号化領域を含む第１暗号化コンテンツと、

前記置換鍵と、前記置換鍵の暗号化領域に対する鍵掛け替え後の暗号鍵であり、コンテンツ配信処理単位で異なる設定とした個別鍵と、

前記置換鍵を適用した暗号化領域を示す置換鍵適用領域情報と、

を取得または生成してクライアントに送信する処理を実行する情報処理方法にある。

【００２８】

さらに、本発明の第９の側面は、

データ記憶装置においてデータ処理を実行させるプログラムであり、

データ処理部に、外部から置換鍵による暗号化データを入力させるステップと、

前記データ処理部に、外部からのアクセスを禁止した第１保護領域から置換鍵を取得し、前記暗号化データの復号処理を実行して復号データを生成させるステップと、

前記データ処理部に、認証の成立した外部装置からのアクセスを許容した第２保護領域から、コンテンツ配信処理単位で異なる設定とされた個別鍵を取得し、取得した個別鍵を適用して前記復号データの暗号化を実行して鍵掛け替え処理を行わせるステップとを実行させるプログラムにある。

【００２９】

さらに、本発明の第１０の側面は、

情報処理装置において情報処理を実行させるプログラムであり、

データ処理部において、置換鍵を適用した暗号化領域を含む第１暗号化コンテンツと、前記置換鍵を適用した暗号化領域を示す置換鍵適用領域情報を取得し、前記置換鍵適用領域情報を参照して、前記第１暗号化コンテンツから置換鍵を適用した暗号化領域データを抽出してデータ記憶装置に提供し、データ記憶装置における鍵掛け替え処理によって生成された個別鍵暗号化領域データを受信し、該受信データを元の置換鍵適用領域に設定した第２暗号化コンテンツを生成して、前記データ記憶装置に格納する処理を実行させるプログラムにある。

【００３０】

さらに、本発明の第１１の側面は、

コンテンツ配信を実行するサーバ装置において情報処理を実行させるプログラムであり、

データ処理部に、

置換鍵を適用した暗号化領域を含む第１暗号化コンテンツと、

前記置換鍵と、前記置換鍵の暗号化領域に対する鍵掛け替え後の暗号鍵であり、コンテンツ配信処理単位で異なる設定とした個別鍵と、

前記置換鍵を適用した暗号化領域を示す置換鍵適用領域情報と、

を取得または生成してクライアントに送信する処理を実行させるプログラムにある。

【００３１】

なお、本発明のプログラムは、例えば、様々なプログラム・コードを実行可能な情報処理装置やコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体によって提供可能なプログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、情報処理装置やコンピュータ・システム上でプログラムに応じた処理が実現される。

【００３２】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムと

は、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【発明の効果】

【００３３】

本発明の一実施例の構成によれば、コンテンツの暗号鍵の漏洩に基づくコンテンツの不正利用を防止する構成が実現される。例えばサーバから受領するコンテンツに含まれる置換鍵で暗号化された置換鍵適用領域を復号して、コンテンツ配信単位に異なる個別鍵を適用して暗号化する鍵の掛け替え処理を実行して、鍵掛け替え後の暗号化コンテンツをデータ記憶装置に格納する。鍵掛け替え処理はデータ記憶装置内部で実行し、置換鍵は外部からのアクセスが禁止された保護領域に格納する。個別鍵は、再生装置等、認証の成立した装置のみアクセスが許容される第２の保護領域に格納する。鍵掛け替え後の暗号化コンテンツはクライアント毎に異なる暗号化コンテンツとなり、コンテンツや個別鍵の漏えい元のクライアントの特定が可能となる。

【図面の簡単な説明】

【００３４】

【図１】コンテンツ提供処理および利用処理の概要について説明する図である。

【図２】メモリカードに記録されたコンテンツの利用形態について説明する図である。

【図３】従来の一般的なユーザに対する提供コンテンツとデータの基本構成例について説明する図である。

【図４】メモリカードの記憶領域の具体的構成例について説明する図である。

【図５】サーバ証明書のデータ構成例について説明する図である。

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

【図７】本発明の一実施例に従ったサーバの提供コンテンツの構成例について説明する図である。

【図８】本発明の一実施例に従ったサーバからのコンテンツ提供シーケンスについて説明する図である。

【図９】本発明の一実施例に従った記録メディアであるメモリカードにおける鍵データの格納例について説明する図である。

【図１０】本発明の一実施例に従った記録メディアであるメモリカードにおける鍵データや、コンテンツ等のデータ格納例について説明する図である。

【図１１】本発明の一実施例に従ったコンテンツ格納処理における鍵掛け替え処理シーケンスについて説明する図である。

【図１２】サーバからクライアントに対する提供データの構成例について説明する図である。

【図１３】サーバにおける管理情報に記録されるデータ例について説明する図である。

【図１４】サーバにおけるコンテンツのクライアントに対する提供処理シーケンスについて説明するフローチャートを示す図である。

【図１５】再生装置におけるコンテンツ再生シーケンスについて説明するシーケンス図である。

【図１６】サーバおよびクライアントとしての情報処理装置のハードウェア構成例について説明する図である。

【図１７】メモリカードのハードウェア構成例について説明する図である。

【発明を実施するための形態】

【００３５】

以下、図面を参照しながら本発明の情報処理装置、および情報処理方法、並びにプログラムの詳細について説明する。なお、説明は以下の項目に従って行う。

１．コンテンツ提供処理および利用処理の概要について

２．ユーザに対する提供コンテンツとデータの従来の基本構成例について

３．コンテンツ記録メディアとしてのメモリカードの構成例について

４．本発明に従ったクライアント（ユーザ）へのコンテンツ提供処理例について
５．本発明に従ったクライアントにおけるコンテンツ再生処理について
６．各装置のハードウェア構成例について

【００３６】

［１．コンテンツ提供処理および利用処理の概要について］

【００３７】

以下、図面を参照しながら本発明の情報処理装置、および情報処理方法、並びにプログラムの詳細について説明する。

【００３８】

まず、図１以下を参照して、コンテンツ提供処理および利用処理の概要について説明する。

図１には、左から、
（ａ）コンテンツ提供元
（ｂ）コンテンツ記録装置（ホスト）
（ｃ）コンテンツ記録メディア
これらを示している。

【００３９】

（ｃ）コンテンツ記録メディアはユーザがコンテンツを記録して、コンテンツの再生処理に利用するメディアである。図１には、例えばフラッシュメモリ等からなる記録部を持つメモリカード３１ａ、３１ｂを示している。

【００４０】

ユーザは、例えば音楽や映画などの様々なコンテンツをメモリカード３１に記録して利用する。これらのコンテンツは例えば著作権管理コンテンツ等、利用制御対象となるコンテンツである。所定の利用条件下での利用のみが許容され、基本的に無秩序なコピー処理やコピーデータの無制限な配布等は禁止される。なお、メモリカード３１にコンテンツを記録する場合、その記録コンテンツの許容コピー回数などのコピー制限情報や、他機器への出力制限情報などを規定した利用制御情報（Ｕｓａｇｅ　Ｒｕｌｅ）も併せて記録される場合が多い。

【００４１】

図１に示す（ａ）コンテンツ提供元は、利用制限のなされた音楽や映画等のコンテンツの提供元である。図１には、コンテンツサーバ１１と、予めコンテンツの記録されたＲＯＭディスク等のコンテンツ記録ディスク１２を示している。

コンテンツサーバ１１は、音楽や映画等のコンテンツを提供するサーバである。コンテンツ記録ディスク１２は予め音楽や映画等のコンテンツを記録したＲＯＭディスク等のディスクである。

【００４２】

ユーザは、図１に示す（ｃ）コンテンツ記録メディアである例えばメモリカード３１を（ｂ）コンテンツ記録装置（ホスト）に装着し、（ｂ）コンテンツ記録装置（ホスト）を介してコンテンツサーバ１１に接続して、コンテンツを受信（ダウンロード）してメモリカード３１に記録することができる。

【００４３】

なお、コンテンツサーバ１１は、このダウンロード処理に際して、所定のシーケンスに従った処理を行い、暗号化コンテンツの他、暗号化コンテンツの復号に適用する鍵情報等コンテンツ再生に必要な情報をクライアントに提供する。さらに、コンテンツに対する利用制御情報、コンテンツＩＤ他のコンテンツ管理情報を記録したトークン等のコンテンツ関連情報を提供する場合もある。

【００４４】

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

【００４５】
例えば、ユーザは、メモリカード３１を装着した（ｂ）コンテンツ記録装置（ホスト）に、予めコンテンツの記録されたＲＯＭディスク等のコンテンツ記録ディスク１２を装着してコンテンツ記録ディスク１２の記録コンテンツをメモリカード３１にコピーを行う。ただし、このコピー処理が無秩序に実行されると、コピーコンテンツが無制限に増加することになる。このような事態を防止するため、例えばＡＡＣＳ（Ａｄｖａｎｃｅｄ Ａｃｃｅｓｓ Ｃｏｎｔｅｎｔ Ｓｙｓｔｅｍ）規格に従った暗号化コンテンツを記録したメディアからのコンテンツコピー処理に際しては、コンテンツサーバ１１に接続して所定のシーケンスに従った処理が必須とされている。このコピー処理は、マネージドコピー（ＭＣ：Ｍａｎａｇｅｄ Ｃｏｐｙ）と呼ばれる。なお、ＡＡＣＳはコンテンツの著作権保護のための様々な規格を規定している。
【００４６】
マネージドコピー（ＭＣ：Ｍａｎａｇｅｄ Ｃｏｐｙ）に従ったコンテンツコピーを行う場合、図１（ｂ）に示すコンテンツ記録装置（ホスト）としての記録再生装置２２や、ＰＣ２３はコンテンツサーバ１１に接続し、コンテンツサーバ１１から、コピーコンテンツに対応する利用制御情報やトークン、さらにさらに暗号化コンテンツの復号に適用する鍵情報等のコンテンツ管理情報を受信し、コピー先メディアに記録する。
【００４７】
ユーザは、このように、
サーバからのコンテンツのダウンロード処理、あるいは、
コンテンツが記録されたディスクからのコンテンツコピー処理、
これらのいずれかの形態で、ユーザの所有する図１（ｃ）に示すメモリカード３１等のコンテンツ記録メディアにコンテンツを記録して利用することができる。
【００４８】
なお、ユーザのメディアにコンテンツを記録する装置としては、図１（ｂ）コンテンツ記録装置（ホスト）に示すように、
不特定多数のユーザが利用可能な公共スペース、例えば駅やコンビニ等に設置された共用端末２１、
ユーザ機器としての記録再生器［ＣＥ（Ｃｏｎｓｕｍｅｒ Ｅｌｅｃｔｒｏｎｉｃｓ）機器］２２、ＰＣ２３、
これらの様々な機器がある。
これらはすべて（ｃ）コンテンツ記録メディアであるメモリカード３１を装着可能な装置である。
また、これらの（ｂ）コンテンツ記録装置（ホスト）は、コンテンツサーバ１１からのダウンロード処理を実行する構成である場合は、ネットワークを介したデータ送受信処理を実行する通信部を備えていることが必要であり、コンテンツ記録ディスク１２を利用する構成である場合は、ディスク再生可能な装置であることが必要である。
【００４９】
図１に示すように、ユーザは、
（ａ）コンテンツ提供元であるコンテンツサーバ１１からのダウンロードコンテンツ、あるいはＲＯＭディスク等のコンテンツ記録ディスク１２に記録されたコンテンツを（ｂ）コンテンツ記録装置（ホスト）を介して、（ｃ）コンテンツ記録メディアとしてのメモリカード３１に記録する。
【００５０】
このメモリカード３１に記録されたコンテンツの利用形態について図２を参照して説明する。
ユーザは、コンテンツを記録したメモリカード３１を、例えば、図１（ｂ）を参照して説明した（ｂ）コンテンツ記録装置（ホスト）としてのユーザ機器である記録再生器（ＣＥ機器）２２やＰＣ２３等に装着してメモリカード３１に記録されたコンテンツを読み取り、再生する。

【００５１】
なお、多くの場合、これらのコンテンツは暗号化コンテンツとして記録されており、記録再生器（ＣＥ機器）２２やＰＣ２３等の再生装置は、所定のシーケンスに従った復号処理を実行した後、コンテンツ再生を行う。
なお、メモリカード３１に記録されたコンテンツを再生する機器は、図１（ｂ）を参照して説明した（ｂ）コンテンツ記録装置（ホスト）に限られず、その他の再生装置（プレーヤ）であってもよい。ただし、例えば予め規定されたシーケンスに従った暗号化コンテンツの復号処理等を実行可能な機器、すなわち予め規定された再生処理シーケンスを実行するプログラムを格納した機器であることが必要となる。なお、コンテンツ再生シーケンスの詳細については、後段で説明する。
【００５２】
［２．ユーザに対する提供コンテンツとデータの従来の基本構成例について］
次に、図３を参照して、従来の一般的なユーザに対する提供コンテンツとデータの基本構成例について説明する。
【００５３】
図３に示す構成は、例えばＢｌｕ－ｒａｙ（登録商標）ディスク等に記録されるＡＡＣＳ（Ａｄｖａｎｃｅｄ　Ａｃｃｅｓｓ　Ｃｏｎｔｅｎｔ　Ｓｙｓｔｅｍ）規格に従った暗号化コンテンツの基本的な構成例である。なお、前述したようにＡＡＣＳはコンテンツの著作権保護のための様々な規格を規定している。ＡＡＣＳ規格の代表的な暗号化構成として、コンテンツをユニット単位に区分してユニット毎に異なる暗号化鍵を適用する構成がある。このような暗号化構成を採用することで、ユニット単位のコンテンツの利用制御が可能となり、厳格で多様なコンテンツ利用制御が実現される。
【００５４】
図３には、以下の各データを示している。
（ａ）暗号化コンテンツ
（ｂ）暗号化コンテンツを構成する各ユニットの暗号化フォーマット
（ｃ）ユーザに対する提供データ（従来）
【００５５】
図３（ａ）暗号化コンテンツは、例えば映画等のコンテンツであり、例えばＢＤ（Ｂｌｕ－ｒａｙ（登録商標）ディスク）等に記録されるコンテンツの構成に対応する。
図３（ａ）に示すようにコンテンツはユニット（Ｕｎｉｔ）単位に区分されている。
１ユニットは、６１４４バイト単位のデータから構成される。
【００５６】
図３（ｂ）には、ユニット単位の暗号化フォーマットを示している。
（ｂ１）にはユニット１（Ｕｎｉｔ１）、（ｂｎ）にはユニットｎ（Ｕｎｉｔｎ）に対する暗号化フォーマットを示している。
ユニット１～ユニットｎは、それぞれ共通の構成、すなわち、
１６バイトのシード（ＳＥＥＤ）、
６１２８バイトのブロック（Ｂｌｏｃｋ）データ、
を有している。
【００５７】
シードは暗号鍵生成用データとして用いられ、ブロックはシードを適用して生成した暗号鍵によって暗号化されるデータ領域である。
具体的には、各ユニットｘ（ｘ＝１～ｎ）において、コンテンツ対応の暗号鍵であるタイトル鍵（Ｋｔ）と、各ユニットのシード（ＳＥＥＤｘ）を利用してブロックに対する暗号鍵であるブロック鍵（Ｋｂｘ）が生成され、生成したブロック鍵（Ｋｂｘ）でブロック（Ｂｌｏｃｋ＿ｘ）が暗号化される。
すなわち図に示す例ではｎ個のユニット１～ｎの各ユニットのブロック１～ｎは、それぞれ異なるシード１～ｎを用いて生成された異なるブロック鍵（Ｋｂ１～Ｋｂｎ）によって暗号化されることになる。

図３（ｃ１）暗号化コンテンツに示すような構成を持つ暗号化コンテンツである。

【００５８】

なお、ブロック鍵（Ｋｂｘ）は、例えば、以下の演算処理によって生成される。

Ｋｂｘ＝（ＡＥＳ＿Ｅ（Ｋｔ，ＳＥＥＤｘ））（ＸＯＲ）（ＳＥＥＤｘ）

上記式において、

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

（ＸＯＲ）は、排他論理和演算、

を示している。

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

【００５９】

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

【００６０】

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

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

（ｃ１）暗号化コンテンツ

（ｃ２）タイトル鍵（Ｋｔ）

【００６１】

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

（ｃ２）タイトル鍵（Ｋｔ）は、コンテンツ対応のタイトル鍵（Ｋｔ）である。

【００６２】

これらの

（ｃ１）暗号化コンテンツ

（ｃ２）タイトル鍵（Ｋｔ）

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

【００６３】

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

Ｋｂｘ＝（ＡＥＳ＿Ｅ（Ｋｔ，ＳＥＥＤｘ））（ＸＯＲ）（ＳＥＥＤｘ）

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

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

【００６４】

しかし、このように、ユーザに対して、

（ｃ１）暗号化コンテンツ

（ｃ２）タイトル鍵（Ｋｔ）

を提供した場合、

その後、ユーザがタイトル鍵（Ｋｔ）を漏洩してしまうと、例えば不正なコピーコンテ

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

【００６５】
［３．コンテンツ記録メディアとしてのメモリカードの構成例について］
次に、コンテンツの記録先として利用されるフラッシュメモリ等によって構成されるメモリカードの構成例について説明する。

【００６６】
メモリカード１００の記憶領域の具体的構成例を図４に示す。
メモリカード１００の記憶領域は、図４に示すように、
（ａ）保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１、
（ｂ）非保護領域（Ｕｓｅｒ　Ａｒｅａ）１０２、
これら２つの領域によって構成される。

【００６７】
（ｂ）非保護領域（Ｕｓｅｒ　Ａｒｅａ）１０２はユーザの利用する記録再生装置によって、自由にアクセス可能な領域であり、コンテンツや一般のコンテンツ管理データ等が記録される。ユーザによって自由にデータの書き込みや読み取りを行うことか可能な領域である。

【００６８】
一方、（ａ）保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１は、自由なアクセスが許容されない領域である。
例えば、ユーザの利用する記録再生装置、再生装置、あるいはネットワークを介して接続されるサーバ等によってデータの書き込みあるいは読み取りを行おうとする場合、メモリカード１００に予め格納されたプログラムに従って、各装置に応じて読み取り（Ｒｅａｄ）または書き込み（Ｗｒｉｔｅ）の可否が決定される。

【００６９】
メモリカード１００は、予め格納されたプログラムを実行するためのデータ処理部や認証処理を実行する認証処理部を備えており、メモリカード１００は、まず、メモリカード１００に対してデータの書き込みまたは読み取りを実行しようとする装置との認証処理を行う。

【００７０】
この認証処理の段階で、相手装置、すなわちアクセス要求装置から公開鍵証明書等の装置証明書（たとえばサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ））を受信し、その証明書に記載された情報を用いて、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１の各区分保護領域のアクセスが許容されるか否かを判定する。この判定処理は、図４に示す保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１内の区分保護領域（図に示す領域＃０，＃１，＃２・・・）単位で判定処理が行われ、許可された区分保護領域で許可された処理のみが実行される。

【００７１】
メモリカードに対するデータ書き込みを実行する装置であるサーバのサーバ証明書のデータ例を図５に示す。図５は、認証局がサーバに提供するサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）のデータ構成例を示す図である。
サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）は、認証局がコンテンツ提供処理を認めたサーバに対して発行するサーバの証明書であり、サーバ公開鍵等を格納した証明書である。サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）は、認証局秘密鍵によって署名が設定され、改ざんの防止されたデータとして構成される。

【００７２】
サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）には、図５に示すように、以下のデータが含まれる。
（１）タイプ情報
（２）サーバＩＤ
（３）サーバ公開鍵（Ｓｅｒｖｅｒ　Ｐｕｂｌｉｃ　Ｋｅｙ）
（４）メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）
（５）その他の情報
（６）署名（Ｓｉｇｎａｕｒｅ）
【００７３】
以下、上記（１）～（６）の各データについて説明する。
（１）タイプ情報
タイプ情報は、証明書のタイプやコンテンツサーバのタイプを示す情報であり、例えば本証明書がサーバ証明書であることを示すデータや、サーバの種類、例えば音楽コンテンツの提供サーバであるとか、映画コンテンツの提供サーバであるといったサーバの種類などを示す情報が記録される。
【００７４】
（２）サーバＩＤ
サーバＩＤはサーバ識別情報としてのサーバＩＤを記録する領域である。
（３）サーバ公開鍵（Ｓｅｒｖｅｒ　Ｐｕｂｌｉｃ　Ｋｅｙ）
サーバ公開鍵（Ｓｅｒｖｅｒ　Ｐｕｂｌｉｃ　Ｋｅｙ）はサーバの公開鍵である。サーバに提供されるサーバ秘密鍵とともに公開鍵暗号方式に従った鍵ペアを構成する。
【００７５】
（４）メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）
メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）は、コンテンツを記録するメディア、例えば図４に示すメモリカード１００の記憶領域中に設定される保護領域（ＰＤＡ：Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１内のデータ読み取り（Ｒｅａｄ）や、書き込み（Ｗｒｉｔｅ）が許容された区分保護領域についての情報が記録される。
【００７６】
メモリカードは、例えばサーバから認証処理の段階で受領する図５に示すサーバ証明書のこの記録フィールドを参照して、例えば、図４に示す保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１内の区分領域（図に示す領域＃０，＃１，＃２・・・）単位で書き込み、読み取りの許可判定処理を行い、許可された区分領域で許可された処理のみの実行を許容する。
【００７７】
図５に示すように、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）には、上述したデータの他、［（５）その他の情報］が記録され、さらに、（１）～（５）の各データに対して認証局の秘密鍵によって生成された（６）署名（Ｓｉｇｎａｔｕｒｅ）が記録される。この署名により改ざんの防止構成が実現される。
サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）を利用する場合は、署名検証を実行して、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）の正当性を確認した上で利用が行われる。なお、署名検証は、認証局の公開鍵を利用して実行される。
【００７８】
メモリカードの保護領域に対するアクセス要求を行うサーバ以外の装置、例えば記録装置、再生装置等もホスト公開鍵を格納し、図５（４）に示すメディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）を記録したホスト証明書を保持し、このホスト証明書をメモリカードに提示する。

【００７９】
メモリカードはアクセス要求を行う装置から提示された証明書の署名検証を行い、証明書の正当性を確認した上で、証明書内の読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）の記録を参照して図４に示す保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１内の区分保護領域（図に示す領域＃０，＃１，＃２・・・）単位で書き込み、読み取りの許可判定処理を行い、許可された区分保護領域で許可された処理のみの実行を許容する。
【００８０】
上述したように、メディアに対する読み取り／書き込み制限情報（ＰＡＤ　Ｒｅａｄ／ＰＡＤＷｒｉｔｅ）は、例えば、アクセスしようとする装置、例えばコンテンツサーバ、あるいは記録再生装置（ホスト）単位で設定される。これらの情報は各装置対応のサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）や、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）に記録される。
【００８１】
メモリカード１００は、メモリカード１００に予め格納された規定のプログラムに従って、サーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ）や、ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔ）の記録データを検証して、アクセス許可のなされた領域についてのみアクセスを許容する処理を行う。
【００８２】
図６を参照して、メモリカードに対するアクセス要求装置がサーバである場合と、記録再生装置等のホスト機器である場合のアクセス制限の設定例について説明する。
【００８３】
図６には、左から、メモリカードに対するアクセス要求装置であるサーバ１２０、ホスト機器１４０、メモリカード１００を示している。
サーバ１２０は、例えばコンテンツの提供処理や、コンテンツ復号に適用する暗号鍵の書き込み処理を実行するサーバである。
ホスト機器１４０は、メモリカード１００に格納されたコンテンツの再生処理を行う装置であり、コンテンツの復号処理のために、メモリカードに記録された暗号鍵を取得する必要がある機器である。
【００８４】
メモリカード１００は、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１と、非保護領域（Ｕｓｅｒ　Ａｒｅａ）１０２を有し、暗号化コンテンツ等は非保護領域（Ｕｓｅｒ　Ａｒｅａ）１０２に記録される。
暗号化コンテンツの復号に適用する暗号鍵は保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１に記録される。なお、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１に記録される暗号鍵には例えばコンテンツ記録処理ごとに異なる個別鍵（Ｋｉｎｄ）が含まれる。個別鍵（Ｋｉｎｄ）の利用処理については後段で詳細に説明する。
【００８５】
先に図４を参照して説明したように、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１は、複数の領域に区分されている。
図６に示す例では、
保護領域＃０（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃０）１１０、
保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）１１１、
保護領域＃２（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃２）１１２、
これらの３つの保護領域を持つ例を示している。
【００８６】
メモリカード１００はアクセス要求装置との認証処理の段階で、相手装置、すなわちアクセス要求装置から公開鍵証明書等の装置証明書（たとえばサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔ））を受信し、その証明書に記載された情報を用いて、保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１の各保護領域のアクセスが許容されるか否かを判定する。こ

の判定処理の結果、許可された保護領域で許可された処理のみが実行される。

【００８７】

例えば、サーバのサーバ証明書（Ｓｅｒｖｅｒ　Ｃｅｒｔｉｆｉｃａｔｅ）に記録される書き込み許容領域情報（ＰＡＤ　Ｗｒｉｔｅ）は、保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）１１１に対する書き込み（Ｗｒｉｔｅ）許可が設定された証明書として構成される。すなわち、図に示すように、

読み取り（Ｒｅａｄ）許容領域：＃１

書き込み（Ｗｒｉｔｅ）許容領域：＃１

このような設定で構成される。

なお、図に示す例では、書き込み（Ｗｒｉｔｅ）の許容された保護領域に対しては、読み取り（Ｒｅａｄ）についても許容された設定として示している。

【００８８】

また、例えば保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）１１１に記録された暗号鍵を読み取ってコンテンツ再生を実行する再生装置であるホスト機器１４０の保持するホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）は、保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）１１１に対する読み取り（Ｒｅａｄ）許可のみが設定された証明書、すなわち、図に示すように、

読み取り（Ｒｅａｄ）許容領域：＃０，１

書き込み（Ｗｒｉｔｅ）許容領域：＃０

このような設定で構成される。

【００８９】

ホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）には、保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）１１１に対する書き込み（Ｗｒｉｔｅ）許可は設定されない。

ただし、コンテンツ削除時に、削除コンテンツに対応する暗号鍵の削除が可能な設定とするため、削除処理については許可する設定としてもよい。

【００９０】

保護領域＃２（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃２）１１２は、サーバ、ホストともアクセスの許容されない領域、すなわち外部アクセス禁止領域として設定される。

すなわち、保護領域＃２（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃２）１１２は、メモリカード１００内部でのデータ処理を実行する場合にのみ、メモリカード１００内のデータ処理部がアクセス（データ書き込みと読み取り）する領域として設定される。

【００９１】

このように、メモリカードのデータ処理部は、アクセス要求装置からの保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）１０１に対するデータ書き込みとデータ読み取りについて、装置証明書に基づいて許可するか否かを判定する。

【００９２】

［４．本発明に従ったクライアント（ユーザ）へのコンテンツ提供処理について］

図７以下を参照して本発明の一実施例に従ったユーザに対する提供コンテンツの構成と、コンテンツ提供シーケンスについて説明する。

【００９３】

図７は、サーバ１２０がユーザ装置としてのクライアントに提供するコンテンツのデータ構成例を説明する図である。

図７には、

（Ａ）暗号化前のコンテンツ

（Ｂ）サーバからの提供コンテンツ

これらのコンテンツを示している。

クライアントに提供されるコンテンツは［（Ｂ）サーバからの提供コンテンツ］である。

【００９４】

サーバ１２０は、例えば、平文コンテンツである［（Ａ）暗号化前のコンテンツ］に対

する所定の暗号化処理を実行して、［（Ｂ）サーバからの提供コンテンツ］を生成する。
［（Ｂ）サーバからの提供コンテンツ］は、
タイトル鍵Ｋｔを適用した暗号化領域
置換鍵Ｋａを適用した暗号化領域
これらの２つの暗号化領域が混在した構成となっている。

【００９５】

サーバ１２０は、平文コンテンツである［（Ａ）暗号化前のコンテンツ］に対して、所定領域単位でタイトル鍵Ｋｔを適用した暗号化処理と、置換鍵Ｋａを適用した暗号化処理を実行して、［（Ｂ）サーバからの提供コンテンツ］を生成する。
なお、タイトル鍵を適用した暗号化処理は、例えば、先に図３を参照して説明したと同様の暗号化処理として実行される。置換鍵Ｋａを適用した暗号化処理は、タイトル鍵の代わりに置換鍵Ｋａを適用して、同様の図３を参照して説明した暗号化処理として実行される。

【００９６】

サーバは、クライアントに対して、この図７（Ｂ）に示すタイトル鍵Ｋｔを適用した暗号化領域と、置換鍵Ｋａを適用した暗号化領域との２つの異なる鍵を適用した暗号化領域が混在した暗号化コンテンツを提供する。

【００９７】

なお、クライアント側では、この［（Ｂ）サーバからの提供コンテンツ］に示す暗号化コンテンツをそのままメモリカードに記録することはしない。
メモリカード内のデータ処理部が、この［（Ｂ）サーバからの提供コンテンツ］に含まれる置換鍵Ｋａを適用した暗号化領域を復号して、別途説明する個別鍵Ｋｉｎｄによる暗号化データに置き換える処理を実行してメモリカードに記録する。この処理については後段で説明する。

【００９８】

なお、図７の［（Ｂ）サーバからの提供コンテンツ］に示すタイトル鍵Ｋｔを適用した暗号化領域と、置換鍵Ｋａを適用した暗号化領域との区分は自由な設定が可能である。一例として、置換鍵Ｋａによって暗号化される領域をコンテンツの重要なシーン（ハイライトシーン）を含む設定とすることが好ましい。
また、例えばＭＰＥＧデータとして設定されるコンテンツの場合には、置換鍵Ｋａによって暗号化される領域をＭＰＥＧデータにおける重要データとなるＩピクチャ、またはＩピクチャの一部を含むような設定とすることが好ましい。

【００９９】

次に、図８参照して、サーバ１２０からクライアントに対するコンテンツ提供シーケンスについて説明する。
図８には、左から、
（１）コンテンツ提供処理を実行するサーバ１２０、
（２）サーバ１２０の提供コンテンツを受信しメモリカード１００に記録するホスト機器１４０、
（３）ホスト機器１４０に装着され、暗号化コンテンツや鍵データの記録を行うメモリカード１００、
これらを示している。
なお、ホスト１４０、メモリカード１００とも、認証処理、暗号処理を含むデータ処理を実行可能なプロセッサ等を含むデータ処理部や通信部を有する。

【０１００】

サーバ１２０は、図７（Ｂ）に示す暗号化コンテンツ、すなわち、
タイトル鍵Ｋｔを適用した暗号化領域、
置換鍵Ｋａを適用した暗号化領域、
これらの２つの暗号化領域が混在したコンテンツをデータベースに格納し、さらに、タイトル鍵Ｋｔと、置換鍵Ｋａもデータベース内に保持しているものとする。

【０１０１】
図８に示すシーケンス図に従って、サーバ１２０からクライアントに対するコンテンツ提供シーケンスについて説明する。
まず、ステップＳ１１において、サーバ１２０と、ホスト機器１４０に装着されたメモリカード１００間において、相互認証処理と共有秘密鍵としてのセッション鍵の共有処理を実行する。
【０１０２】
例えば公開鍵暗号方式に従って、双方の公開鍵証明書の交換処理等を含む相互認証処理を行う。サーバ１２０は認証局の発行した公開鍵を格納したサーバ証明書（Ｓｅｒｖｅｒ Ｃｅｒｔｉｆｉｃａｔｅ）と秘密鍵を保持している。メモリカード１００も予め認証局から公開鍵証明書と秘密鍵のペアを受信し自己の記憶部に格納している。
【０１０３】
なお、メモリカードは相互認証処理や、先に図４等を参照して説明した保護領域（Ｐｒｏｔｅｃｔｅｄ Ａｒｅａ）に対するアクセス可否判定を行うプログラムを格納し、これらのプログラムを実行するデータ処理部を有する。
【０１０４】
コンテンツサーバ１２０とメモリカード１００間の相互認証が成立し、双方の正当性が確認されると、サーバ１２０はメモリカード１００に対して様々なデータを提供する。相互認証が成立しない場合は、サーバ１２０からのデータ提供処理は行われない。
【０１０５】
相互認証の成立後、サーバ１２０は、ステップＳ１２において個別鍵Ｋｉｎｄを生成する。
個別鍵Ｋｉｎｄは、コンテンツの配信処理単位で生成するコンテンツ配信単位の個別鍵であり、各クライアントに対応した個別鍵である。複数のクライアントに同じコンテンツを配信する場合にも、個別鍵Ｋｉｎｄは異なる鍵として設定される。
ステップＳ１２においてサーバの実行する個別鍵Ｋｉｎｄの生成は、例えば乱数生成装置などを利用して行われ、逐次、新たなデータ構成を持つ個別鍵を生成する。
【０１０６】
ステップＳ１３において、サーバ１２０は、生成した、
個別鍵Ｋｉｎｄと、
図７（Ｂ）を参照して説明した暗号化コンテンツの暗号鍵として適用した２つの鍵、すなわち、
タイトル鍵：Ｋｔ
置換鍵：Ｋａ、
これら３つの鍵をメモリカード１００に送信する。
【０１０７】
なお、送信時には、これらの鍵データをセッション鍵：Ｋｓで暗号化して送信する。すなわち、
Ｅｎｃ（Ｋｓ，Ｋｔ||Ｋｉｎｄ）、Ｅｎｃ（Ｋｓ，Ｋａ）
これらのデータを送信する。
なお、Ｅｎｃ（ａ，ｂ）はデータｂを鍵ａで暗号化したデータであることを示す。
（ａ||ｂ）は、データａ，ｂとの連結データであることを意味する。
【０１０８】
ステップＳ１４において、メモリカード１００は、サーバ１２０から受信したデータ、
Ｅｎｃ（Ｋｓ，Ｋｔ||Ｋｉｎｄ）、Ｅｎｃ（Ｋｓ，Ｋａ）
これらのデータをセッシヨン鍵：Ｋｓを適用して復号する。
さらに、復号して得られた３つの鍵データをメモリカード１００の保護領域に格納する。
タイトル鍵：Ｋｔと、個別鍵：Ｋｉｎｄについては、ホスト機器１４０のアクセスの許容された保護領域、本実施例では保護領域＃１（Ｐｒｏｔｅｃｔｅｄ ａｒｅａ＃１）に

記録する。
置換鍵：Ｋａのみは、ホスト機器を含む外部機器からのアクセスが許容されない保護領域、本実施例では保護領域＃２（Ｐｒｏｔｅｃｔｅｄ　ａｒｅａ＃２）に記録する。
【０１０９】
メモリカード１００における鍵データの格納例を図９に示す。
図９に示すように、
メモリカード１００内の保護領域１０１に設定されたホスト機器１４０からのアクセス許容領域である保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　ａｒｅａ＃１）１１１に、タイトル鍵：Ｋｔと、個別鍵：Ｋｉｎｄを記録する。
また、メモリカード１００内の保護領域１０１に設定されたホスト機器１４０を含む外部機器からのアクセスが許容されない保護領域＃２（Ｐｒｏｔｅｃｔｅｄ　ａｒｅａ＃２）１１２に、置換鍵：Ｋａを記録する。
【０１１０】
図８に戻り、コンテンツ提供シーケンスの続きを説明する。
ステップＳ１５において、サーバ１２０は、ホスト機器１４０に対して、図７（Ｂ）に示すタイトル鍵と置換鍵Ｋａの暗号化領域が混在した暗号化コンテンツ中の、置換鍵Ｋａの適用領域情報を提供する。
具体的には、例えば、図７（Ｂ）に示すコンテンツにおけるＫａ適用領域各々についての、
（１）コンテンツ先頭からのオフセット情報、
（２）各Ｋａ適用領域のサイズ、
これら（１），（２）の情報からなるリストを置換鍵適用領域情報としてホスト機器１４０に提供する。
【０１１１】
さらに、ステップＳ２１において、サーバ１２０は、ホスト機器１４０に対して、図７（Ｂ）に示すタイトル鍵と置換鍵Ｋａの暗号化領域が混在した暗号化コンテンツを提供する。
【０１１２】
ステップＳ２２において、ホスト機器１４０は、置換鍵適用領域情報（リスト）を参照して、受信暗号化コンテンツ、すなわち、図７（Ｂ）に示すタイトル鍵と置換鍵Ｋａの暗号化領域が混在した暗号化コンテンツから、置換鍵適用領域データ（置換鍵：Ｋａによる暗号化コンテンツ）のみを選択してメモリカード１００に送信する。
【０１１３】
なお、このステップＳ２２の処理を開始する前提として、ホスト機器１４０とメモリカード１００間で相互認証処理を実行し、双方の機器の正当性を確認する。すなわち、相互認証の成立が前提となる。相互認証が不成立の場合は、ステップＳ２２以下の処理は実行しない。
【０１１４】
ステップＳ２３において、メモリカード１００は、ホスト機器１４０から受信した置換鍵適用領域データ（置換鍵：Ｋａによる暗号化コンテンツ）を、
保護領域＃２（Ｐｒｏｔｅｃｔｅｄ　ａｒｅａ＃２）１１２に記録した置換鍵：Ｋａを適用して復号し、さらに、
保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　ａｒｅａ＃１）１１１に記録した個別鍵：Ｋｉｎｄを適用して暗号化する処理を実行する。
すなわち、鍵の架け換え処理を実行する。
【０１１５】
ステップＳ２４において、メモリカード１００は、個別鍵：Ｋｉｎｄで暗号化したデータをホスト機器１４０に提供する。
ステップＳ２５において、ホスト機器１４０は、メモリカード１００から受信した個別鍵：Ｋｉｎｄによる暗号化データを、元のコンテンツ位置、すなわち、置換鍵：Ｋａによ

る暗号化データの設定された位置に配置する。
すなわち、タイトル鍵：Ｋｔによる暗号化領域と、個別鍵：Ｋｉｎｄによる暗号化領域からなる暗号化コンテンツを生成して、メモリカード１００の非保護領域に記録する。さらに、置換鍵適用領域情報（リスト）もメモリカード１００の非保護領域に記録する。
なお、ステップＳ２１～Ｓ２５の処理は、サーバ１２０からのコンテンツダウンロードが終了するまで、繰り返し実行される。

【０１１６】

これらの処理結果として、メモリカード１００に記録されるデータ例を図１０に示す。図１０に示すように、メモリカード１００には、以下のデータが記録される。
（ａ）タイトル鍵：Ｋｔと、個別鍵：Ｋｉｎｄ
これらの鍵データは、メモリカード１００内の保護領域１０１に設定されたホスト機器１４０からのアクセス許容領域である保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　ａｒｅａ＃１）１１１に記録される。
（ｂ）置換鍵：Ｋａ
この鍵データは、メモリカード１００内の保護領域１０１に設定されたホスト機器１４０を含む外部機器からのアクセスが許容されない保護領域＃２（Ｐｒｏｔｅｃｔｅｄ　ａｒｅａ＃２）１１２に記録される。
（ｃ）暗号化コンテンツ（タイトル鍵：Ｋｔと個別鍵：Ｋｉｎｄによる暗号化データの混在コンテンツ）は外部機器からアクセス可能な非保護領域に記録される。
（ｄ）置換鍵：Ｋａによる暗号化領域（＝個別鍵：Ｋｉｎｄによる暗号化領域）の領域情報であるリスト（領域識別用のオフセットとデータサイズからなるリスト）は外部機器からアクセス可能な非保護領域に記録される。
図１０に示すように、これらの各データがメモリカード１００の各領域に記録される。

【０１１７】

図８のシーケンス図を参照して説明したコンテンツの記録処理に際して、ホスト機器１４０とメモリカード１００間において実行する処理シーケンスについて、図１１を参照して説明する。

【０１１８】

図１１は、鍵掛け替え処理の詳細シーケンスを説明する図である。すなわちサーバ１２０から受信するタイトル鍵Ｋｔと置換鍵Ｋａの２つの鍵によって暗号化されたコンテンツに対して、置換鍵Ｋａ適用領域のみを個別鍵Ｋｉｎｄの暗号化データに置き換える処理である。

【０１１９】

なお、鍵データ（タイトル鍵：Ｋｔ、置換鍵：Ｋａ、個別鍵：Ｋｉｎｄ）はサーバ１２０からメモリカード１００に提供されてメモリカードの保護領域に格納済みであるとする。
また、タイトル鍵：Ｋｔと置換鍵：Ｋａの２つの鍵を適用して領域単位で暗号化された暗号化コンテンツと、置換鍵適用領域を示す置換鍵適用領域情報（オフセットとデータサイズのリスト）は、サーバ１２０からホスト機器１４０が受信済みであるとする。

【０１２０】

まず、ステップＳ５１において、ホスト機器１４０は、サーバ１２０から受信した置換鍵適用領域情報（オフセットとデータサイズのリスト）を利用して、サーバ１２０から受信した暗号化コンテンツ内の置換鍵Ｋａによる暗号化データを選択取得し、この選択データをメモリカード１００に提供する。

【０１２１】

メモリカード１００は、ステップＳ５２において、ホスト機器１４０から受信した置換鍵Ｋａによる暗号化データの復号処理を実行する。
すなわち、メモリカード１００のデータ処理部が、全ての外部装置からのアクセスを禁止した保護領域＃２（Ｐｒｏｔｅｃｔｅｄ　ａｒｅａ＃２）に記録した置換鍵：Ｋａを取得して、置換鍵：Ｋａを適用して復号する。

【０１２２】
次に、ステップＳ５３において、メモリカード１００のデータ処理部は、復号データに対して、個別鍵：Ｋｉｎｄを適用した暗号化処理を実行する。
すなわち、メモリカード１００のデータ処理部が、保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　ａｒｅａ＃１）に記録した個別鍵：Ｋｉｎｄを取得して、個別鍵：Ｋｉｎｄ適用した暗号化処理を実行する。
なお、保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　ａｒｅａ＃１）は、一部の外部装置、例えばメモリカードとの相互認証が成立した再生装置（ホスト機器）等によってアクセスが許容される領域として設定される。
【０１２３】
メモリカード１００において個別鍵：Ｋｉｎｄを適用した暗号化処理によって、鍵の架け換えの実行されたデータは、ホスト機器１４０に送信される。
ステップＳ５４において、ホスト機器１４０は、メモリカード１００から受信した個別鍵：Ｋｉｎｄによる暗号化データを、元のコンテンツ位置、すなわち、置換鍵：Ｋａによる暗号化データの設定された位置に配置する。
【０１２４】
その後、ホスト機器１４０は、タイトル鍵：Ｋｔによる暗号化領域と、個別鍵：Ｋｉｎｄによる暗号化領域からなる暗号化コンテンツと、置換鍵適用領域情報（リスト）［＝個別鍵適用領域情報］を、メモリカード１００の非保護領域に記録する。
この結果として、メモリカード１００には、図１０を参照して説明した各データが各領域に記録されることになる。
【０１２５】
サーバ１２０が各クライアントに提供するデータの設定例について図１２を参照して説明する。
図１２に示すように、サーバ１２０は、各クライアント１８１，１８２に対して
（Ａ）共通データ、
（Ｂ）個別データ、
をそれぞれ提供する。
なお、図には２つのクライアント１，１８１、クライアント２，１８２まのみを示しているが、この他にも多数のクライアントが存在し、共通データは、全てのクライアントに対する共通データとして設定されるデータであり、個別データは、各クライアント毎に異なるデータである。
【０１２６】
（Ａ）共通データには、
（ａ１）暗号化コンテンツ（タイトル鍵：Ｋｔと個別鍵：Ｋｉｎｄによる暗号化データの混在コンテンツ）、
（ａ２）タイトル鍵：Ｋｔ、
（ａ３）置換鍵：Ｋａ、
（ａ４）置換鍵：Ｋａによる暗号化領域情報（例えば領域識別用のオフセットとデータサイズからなるリスト）
これらのデータが含まれる。
【０１２７】
一方、各クライアント毎に異なる（Ｂ）個別データとして、
（ｂ１）個別鍵：Ｋｉｎｄ
が提供される。
【０１２８】
複数のクライアント１，２・・に対して、同じタイトル鍵：Ｋｔと置換鍵：Ｋａを適用した同じコンテンツを提供した場合にも、各クライアント１，２・・の各記録メディアには、タイトル鍵：Ｋｔと、各クライアント毎に異なる個別鍵：Ｋｉｎｄで暗号化された異なる暗号化コンテンツが記録される。

【０１２９】
従って、例えばタイトル鍵が漏洩し、不特定多数のユーザによって利用可能な状況となっても、個別鍵は、クライアント単位（配信コンテンツ単位）で異なるデータであり、これらの個別データが不特定多数が利用可能な状況にならない限り、コンテンツの不正利用が広がることはない。
【０１３０】
また、個別鍵はサーバによって、配信先情報とともに管理されるので、万が一、不正に広まった個別鍵や暗号化シードが発見された場合は、その個別鍵の配送先を特定することが可能となる。
【０１３１】
図１３にサーバの記憶手段に保持される管理情報のデータ構成例を示す。
図１３に示すように、管理情報には、
配信コンテンツに対応する固有ＩＤ、
配信コンテンツ情報、
個別鍵（Ｋｉｎｄ）情報
配信先情報、
配信ユーザ情報、
配信日時情報、
例えばこれらの情報が含まれる。
【０１３２】
なお、配信先情報としては、ホスト機器１４０と、メモリカード（記録メディア）１００を個別に登録する設定としてもよい。あるいはいずれかのみを登録する設定としてもよい。
個別鍵（Ｋｉｎｄ）情報は、全てのエントリに対して異なるデータが記録される。なお、配信先のユーザが同じ場合には、同じ個別鍵を利用する構成としてもよい。この場合、個別鍵は配信処理単位ではなく配信先ユーザ単位で異なる鍵として設定されることになる。
この場合でも、不正なデータ流出があった場合には個別鍵の照合によって流出元としてのユーザの特定は可能となる。
なお、図１３に示す管理情報の例は一例であり、これらの情報の全てが必須ではなく、また、これらの情報以外の情報を管理情報として保持してもよい。
【０１３３】
このように、本発明の構成では、コンテンツ配信処理を行うサーバが、
各クライアントに対する共通データとして、
タイトル鍵：Ｋｔと、置換鍵：Ｋａによる暗号化領域を持つ暗号化コンテンツを提供するとともに、コンテンツ配信単位で異なる個別鍵（Ｋｉｎｄ）を生成してデータ記憶装置としてのメモリカードに提供する。
メモリカード側で、暗号化コンテンツ中の置換鍵：Ｋａによる暗号化領域を、個別鍵：Ｋｉｎｄによる暗号化データに置き換えた後、メモリカード内に格納する。
【０１３４】
この設定とすることで、メモリカードに格納された暗号化コンテンツの復号処理には、必ず、
タイトル鍵：Ｋｔと、
個別鍵：Ｋｉｎｄ、
この２種類の鍵が必要となる。
【０１３５】
すなわち、タイトル鍵：Ｋｔが漏えいしてもコンテンツの完全な復号は不可能となる。
万が一、タイトル鍵：Ｋｔと、個別鍵：Ｋｉｎｄの双方が漏えいした場合は、図１３に示す管理データに基づいて、漏えい元のクライアントを特定することが可能となる。
【０１３６】

次に、サーバ１２０の実行するコンテンツおよび鍵提供処理シーケンスについて、図１４に示すフローチャートを参照して説明する。

ステップＳ２０１において、２種類の鍵（タイトル鍵と置換鍵）の暗号化領域を持つ暗号化コンテンツを生成または取得する。先に図７（Ｂ）を参照して説明した暗号化コンテンツである。

【０１３７】

次に、ステップＳ２０２において、コンテンツ配信処理対象のクライアント固有の個別鍵：Ｋｉｎｄを生成する。

【０１３８】

次に、ステップＳ２０３において、個別鍵：Ｋｉｎｄと、タイトル鍵：Ｋｔと置換鍵：Ｋａを記録メディア（メモリカード）に送信する。なお、これらのデータの送信処理の前提として、サーバと記録メディア（メモリカード）間の相互認証が成立し、セッション鍵：Ｋｓを共有していることが前提となる。

送信鍵データは、セッション鍵：Ｋｓを適用した暗号化データとして送信される。

【０１３９】

次に、ステップＳ２０４において、２種類の鍵（タイトル鍵と置換鍵）の暗号化領域を持つ暗号化コンテンツを記録装置（ホスト機器）に送信する。

次に、ステップＳ２０５において、個別鍵と、コンテンツを提供したクライアント（記録装置／記録メディア）情報を対応付けた管理データを生成してサーバ１２０内のデータベースに登録する。

【０１４０】

［５．本発明に従ったクライアントにおけるコンテンツ再生処理について］

次に、メモリカードに格納された暗号化コンテンツ、すなわちタイトル鍵：Ｋｔと、個別鍵：Ｋｉｎｄによる暗号化データの混在データとして設定された暗号化コンテンツの再生シーケンスについて図１５に示すシーケンス図を参照して説明する。

図１５には、左から、

（１）コンテンツ再生処理を実行するホスト機器１４０に装着され、暗号化コンテンツや鍵データを格納したメモリカード１００、

（２）コンテンツ再生処理を実行するホスト機器１４０、

これらを示している。

【０１４１】

記録メディアとしてのメモリカード１００は、図４、図６等を参照して説明したメモリカード１００に対応し、機器に応じたアクセス制限のなされる保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）と、アクセス制限のない非保護領域（Ｕｓｅｒ　Ａｒｅａ）を有する。

【０１４２】

なお、コンテンツ再生処理を実行する再生装置は、例えば先の図８のシーケンス図の説明において、コンテンツ記録処理を実行したホスト機器１４０と同一の装置であってもよいし、異なる装置も例えば再生処理専用の装置であってもよい。ただし、コンテンツを記録した記録装置であるメモリカード１００のデータの読み出しが可能な装置であることが必要である。

なお、図１５に示すシーケンス図においては、コンテンツ再生を実行する装置は、記録機器と同じホスト機器１４０であると想定して説明する。

【０１４３】

図１５に示すシーケンス図の各ステップの処理について説明する。

ステップＳ３０１において、

コンテンツを記録したメモリカード１００と、コンテンツ再生を実行するホスト機器１４０との間で相互認証処理とセッション鍵：Ｋｓの共有処理を実行する。

この処理は、先に図８のステップＳ１１の処理として説明したサーバ１２０とメモリカード１００間における相互認証および鍵共有処理と同様の処理である。

【０１４４】

例えば公開鍵暗号方式に従って、双方の公開鍵証明書の交換処理等を含む相互認証処理を行う。ホスト機器１４０は認証局の発行した先に図５を参照して説明したサーバ証明書と同様のデータ構成を持つ公開鍵を格納したホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）と秘密鍵を保持している。メモリカード１００も予め認証局から公開鍵証明書と秘密鍵のペアを受信し自己の記憶部に格納している。

【０１４５】

なお、メモリカードは相互認証処理や、先に図４等を参照して説明した保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）に対するアクセス可否判定を行うプログラムを格納し、これらのプログラムを実行するデータ処理部を有する。

【０１４６】

メモリカード１００とホスト機器１４０間の相互認証が成立し、双方の正当性が確認されると、ステップＳ３０２に進む。相互認証が成立しない場合は、ステップｓ３０２以下の処理は実行されない。

【０１４７】

ステップＳ３０２において、ホスト機器１４０は、メモリカード１００に対して、保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）に格納されたタイトル鍵：Ｋｔと、個別鍵：Ｋｉｎｄの読み取り要求を出力する。

なお、ここでメモリカード１００の保護領域＃１は、図６を参照して説明したように、ホスト機器１４０によるアクセスが許容された領域であるとする。

【０１４８】

メモリカード１００は、ステップＳ３０３において、ホスト機器１０４の保護領域＃１に対するアクセス権の確認処理を実行する。先に、図６を参照して説明したように、コンテンツ再生を実行する再生装置であるホスト機器１４０の保持するホスト証明書（Ｈｏｓｔ　Ｃｅｒｔｉｆｉｃａｔｅ）は、保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）１１１に対する読み取り（Ｒｅａｄ）許可のみが設定された証明書、すなわち、図６に示すように、

読み取り（Ｒｅａｄ）許容領域：＃０，１

書き込み（Ｗｒｉｔｅ）許容領域：＃０

このような設定で構成されている。

メモリカード１００は、相互認証処理の際に取得したホスト証明書に基づいて、ホスト機器１４０が保護領域＃１に対するアクセス権を有する装置であることを確認する。

なお、アクセス権が確認されない場合は、ステップＳ３０４以下の処理は実行されない。

【０１４９】

ステップＳ３０３において、ホスト機器１４０が保護領域＃１に対するアクセス権を有する装置であることが確認された場合は、ステップＳ３０４に進む。

【０１５０】

ステップＳ３０４において、メモリカード１００は、メモリカード１００の保護領域＃１（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ＃１）に格納されたタイトル鍵：Ｋｔと、個別鍵：Ｋｉｎｄをセッション鍵：Ｋｓで暗号化してホスト機器１４０に出力する。

【０１５１】

ステップＳ３０５において、ホスト機器１４０は、メモリカードから受信した暗号化鍵データを受信し、セッション鍵：Ｋｓによる復号処理を実行して、タイトル鍵：Ｋｔと、個別鍵：Ｋｉｎｄを取得する。

【０１５２】

ステップＳ３０６において、メモリカード１００は、メモリカードの非保護領域に格納された置換鍵適用領域情報としてのリスト、すなわち、サーバから受信したタイトル鍵：Ｋｔと置換鍵：Ｋａによって暗号化されたコンテンツ中の置換鍵適用領域を示すリストをホスト機器１４０に提供する。

【０１５３】

なお、メモリカード１００の非保護領域に格納された暗号化コンテンツの置換鍵適用領域は、個別鍵適用領域に置き換えられている。

また、リストは、例えばコンテンツ中の置換鍵適用領域（＝個別鍵適用領域）各々についてのコンテンツ先頭からのオフセットを示す値と領域サイズの各情報によって構成される。

【０１５４】

次にステップＳ３０７において、ホスト機器１４０は、メモリカード１００の非保護領域から暗号化コンテンツを読み出す。この暗号化コンテンツは、タイトル鍵：Ｋｔと、個別鍵：Ｋｉｎｄによる暗号化領域が混在した暗号化コンテンツである。

【０１５５】

ホスト機器１４０は、ステップＳ３０８において、メモリカード１００から読み出した暗号化コンテンツを、先のステップＳＺ３０５の処理において取得したタイトル鍵：Ｋｔと、個別鍵：Ｋｉｎｄを適用して復号処理を実行し再生する。

なお、タイトル鍵：Ｋｔと、個別鍵：Ｋｉｎｄのどちらを適用した復号処理を行うかを判定は、ステップＳ３０６においてメモリカード１００から読み出した置換鍵適用領域情報（＝個別鍵適用領域情報）としてのリストを参照して行う。

【０１５６】

［６．各装置のハードウェア構成例について］

最後に、図１６以下を参照して、上述した処理を実行する各装置のハードウェア構成例について説明する。

まず、図１６を参照して、コンテンツ提供処理を実行するサーバ、およびメモリカードを装着してデータの記録や再生処理を行うクライアントとしての情報記録装置や情報再生装置のハードウェア構成例について説明する。

【０１５７】

ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）７０１は、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）７０２、または記憶部７０８に記憶されているプログラムに従って各種の処理を実行するデータ処理部として機能する。例えば、上述の各実施例において説明したサーバクライアント間の通信処理や受信データのメモリカード(図中のリムーバブルメディア７１１)に対する記録処理、メモリカード(図中のリムーバブルメディア７１１)からのデータ再生処理等を実行する。ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）７０３には、ＣＰＵ７０１が実行するプログラムやデータなどが適宜記憶される。これらのＣＰＵ７０１、ＲＯＭ７０２、およびＲＡＭ７０３は、バス７０４により相互に接続されている。

【０１５８】

ＣＰＵ７０１はバス７０４を介して入出力インタフェース７０５に接続され、入出力インタフェース７０５には、各種スイッチ、キーボード、マウス、マイクロホンなどよりなる入力部７０６、ディスプレイ、スピーカなどよりなる出力部７０７が接続されている。ＣＰＵ７０１は、入力部７０６から入力される指令に対応して各種の処理を実行し、処理結果を例えば出力部７０７に出力する。

【０１５９】

入出力インタフェース７０５に接続されている記憶部７０８は、例えばハードディスク等からなり、ＣＰＵ７０１が実行するプログラムや各種のデータを記憶する。通信部７０９は、インターネットやローカルエリアネットワークなどのネットワークを介して外部の装置と通信する。

【０１６０】

入出力インタフェース７０５に接続されているドライブ７１０は、磁気ディスク、光ディスク、光磁気ディスク、或いは半導体メモリなどのリムーバブルメディア７１１を駆動し、記録されているコンテンツや鍵情報、プログラム等の各種データを取得する。例えば、取得されたプログラムに従ったデータ処理、あるいはコンテンツや鍵データを用いて、ＣＰＵによって実行するデータ処理、記録再生プログラムに従って鍵生成、コンテンツの

暗号化、記録処理、復号、再生処理などが行われる。

【０１６１】

図１７は、メモリカードのハードウェア構成例を示している。

ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）８０１は、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）８０２、または記憶部８０７に記憶されているプログラムに従って各種の処理を実行するデータ処理部として機能する。例えば、上述の各実施例において説明したサーバや記録装置や再生装置等のホスト機器との通信処理やデータの記憶部８０７に対する書き込み、読み取り等の処理、記憶部８０７の保護領域８１１の区分領域単位のアクセス可否判定処理、鍵掛け替え処理等を実行する。ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）８０３には、ＣＰＵ８０１が実行するプログラムやデータなどが適宜記憶される。これらのＣＰＵ８０１、ＲＯＭ８０２、およびＲＡＭ８０３は、バス８０４により相互に接続されている。

【０１６２】

ＣＰＵ８０１はバス８０４を介して入出力インタフェース８０５に接続され、入出力インタフェース８０５には、通信部８０６、記憶部８０７が接続されている。

【０１６３】

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

【０１６４】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

【０１６５】

また、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。例えば、プログラムは記録媒体に予め記録しておくことができる。記録媒体からコンピュータにインストールする他、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、インターネットといったネットワークを介してプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０１６６】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【産業上の利用可能性】

【０１６７】

以上、説明したように、本発明の一実施例の構成によれば、コンテンツの暗号鍵の漏洩に基づくコンテンツの不正利用を防止する構成が実現される。例えばサーバから受領するコンテンツに含まれる置換鍵で暗号化された置換鍵適用領域を復号して、コンテンツ配信単位に異なる個別鍵を適用して暗号化する鍵の掛け替え処理を実行して、鍵掛け替え後の暗号化コンテンツをデータ記憶装置に格納する。鍵掛け替え処理はデータ記憶装置内部で実行し、置換鍵は外部からのアクセスが禁止された保護領域に格納する。個別鍵は、再生装置等、認証の成立した装置のみアクセスが許容される第２の保護領域に格納する。鍵掛け替え後の暗号化コンテンツはクライアント毎に異なる暗号化コンテンツとなり、コンテ

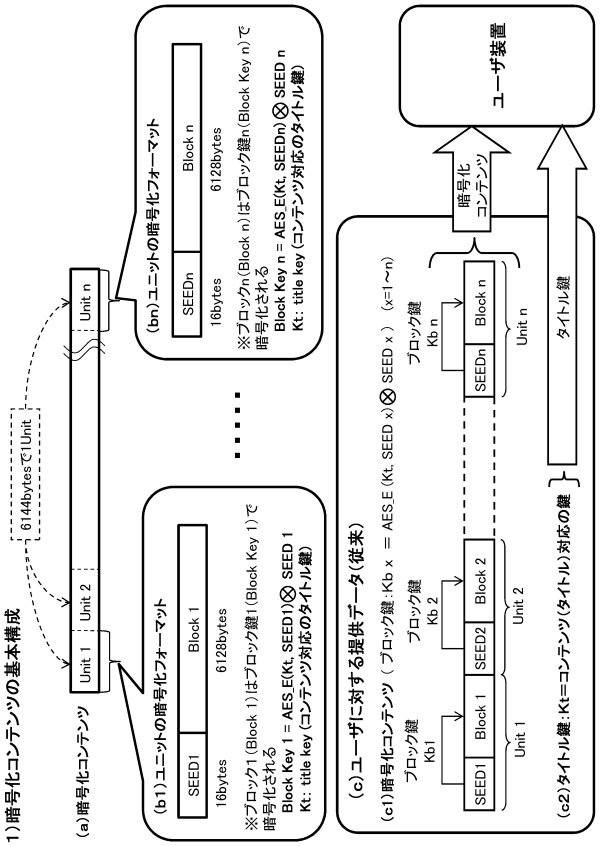
ンツや個別鍵の漏えい元のクライアントの特定が可能となる。

【符号の説明】

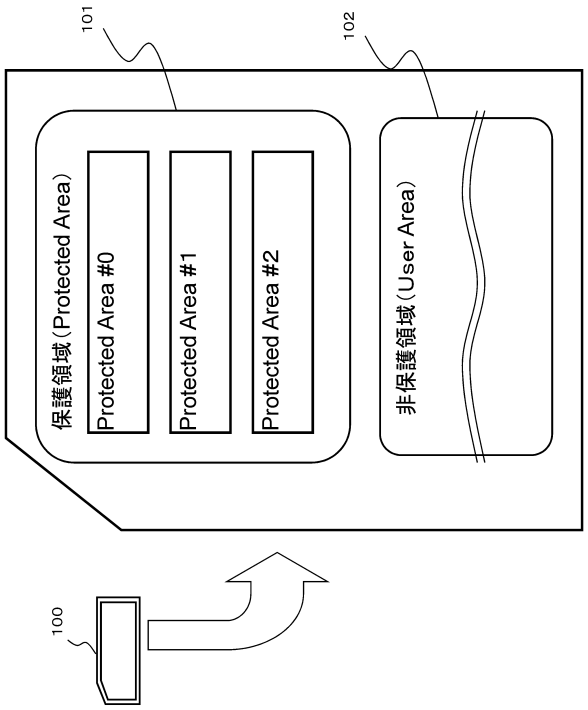
【０１６８】

１１　コンテンツサーバ
１２　コンテンツ記録ディスク
２１　共用端末
２２　記録再生器（ＣＥ機器）
２３　ＰＣ
３１　メモリカード
１００　メモリカード
１０１　保護領域
１０２　非保護領域
１１０～１１２　区分保護領域
１２０　サーバ
１４０　ホスト装置
１８１，１８２　クライアント
７０１　ＣＰＵ
７０２　ＲＯＭ
７０３　ＲＡＭ
７０４　バス
７０５　入出力インタフェース
７０６　入力部
７０７　出力部
７０８　記憶部
７０９　通信部
７１０　ドライブ
７１１　リムーバブルメディア
８０１　ＣＰＵ
８０２　ＲＯＭ
８０３　ＲＡＭ
８０４　バス
８０５　入出力インタフェース
８０６　通信部
８０７　記憶部
８１１　保護領域（Ｐｒｏｔｅｃｔｅｄ　Ａｒｅａ）
８１２　非保護領域（Ｕｓｅｒ　Ａｒｅａ）

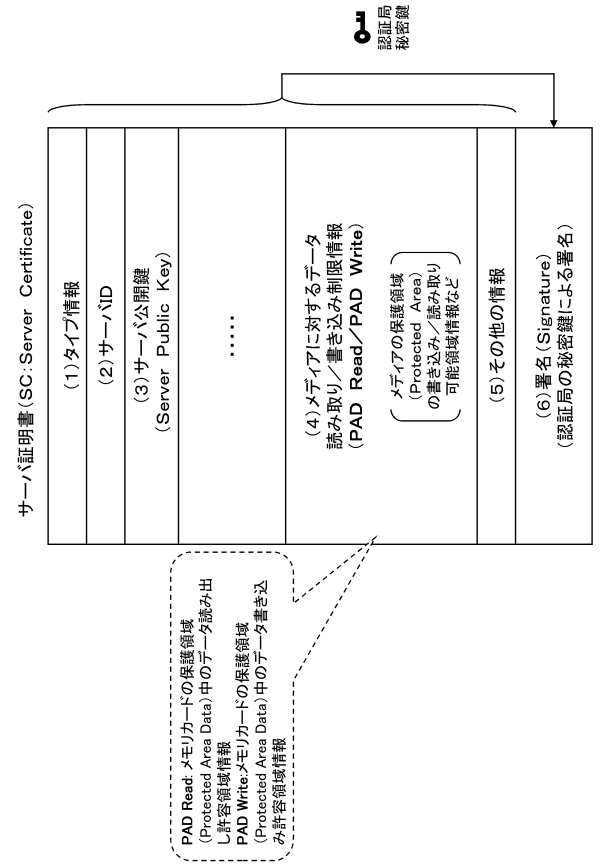
【図３】


(1)暗号化コンテンツの基本構成
6144bytesでUnit
(a)暗号化コンテンツ
Unit 1
Unit 2
Unit n
(b1)ユニットの暗号化フォーマット
SEED1
Block 1
16bytes
6128bytes
※ブロック1(Block 1)はブロック鍵1(Block Key 1)で暗号化される
Block Key 1 = AES_E(Kt, SEED1)⊗ SEED 1
Kt: title key (コンテンツ対応のタイトル鍵)
(bn)ユニットの暗号化フォーマット
SEEDn
Block n
16bytes
6128bytes
※ブロックn(Block n)はブロック鍵n(Block Key n)で暗号化される
Block Key n = AES_E(Kt, SEEDn)⊗ SEED n
Kt: title key (コンテンツ対応のタイトル鍵)
(c)ユーザに対する提供データ(従来)
(c1)暗号化コンテンツ (ブロック鍵:Kb x = AES_E (Kt, SEED x)⊗ SEED x) (x=1~n)
ブロック鍵 Kb1
ブロック鍵 Kb 2
ブロック鍵 Kb n
SEED1
Block 1
SEED2
Block 2
SEEDn
Block n
Unit 1
Unit 2
Unit n
暗号化コンテンツ
ユーザ装置
(c2)タイトル鍵:Kt=コンテンツ(タイトル)対応の鍵
タイトル鍵

【図４】


101
102
保護領域(Protected Area)
Protected Area #0
Protected Area #1
Protected Area #2
非保護領域(User Area)
100

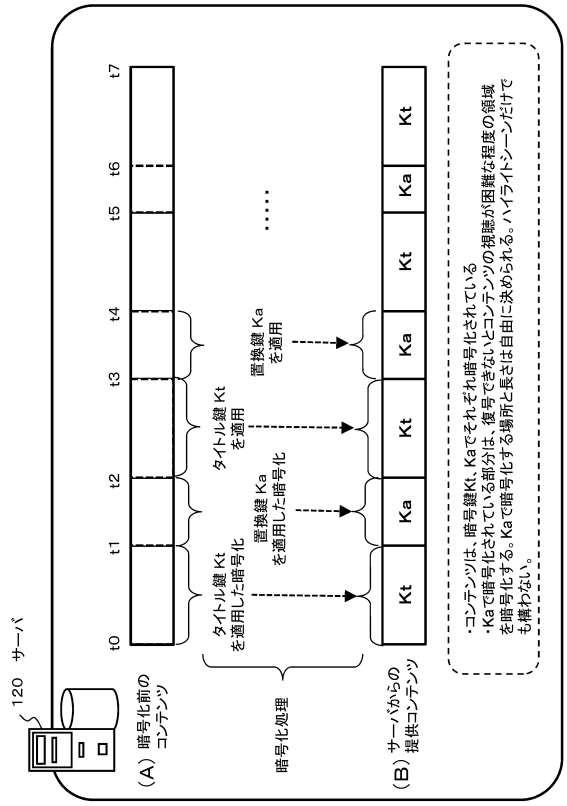
【図５】


認証局秘密鍵
サーバ証明書(SC:Server Certificate)
(1)タイプ情報
(2)サーバID
(3)サーバ公開鍵
(Server Public Key)
.....
(4)メディアに対するデータ読み取り/書き込み制限情報
(PAD Read/PAD Write)
メディアの保護領域(Protected Area)の書き込み/読み取り可能領域情報など
(5)その他の情報
(6)署名(Signature)
(認証局の秘密鍵による署名)
PAD Read:メモリカードの保護領域(Protected Area Data)中のデータ読み出し許容領域情報
PAD Write:メモリカードの保護領域(Protected Area Data)中のデータ書き込み許容領域情報

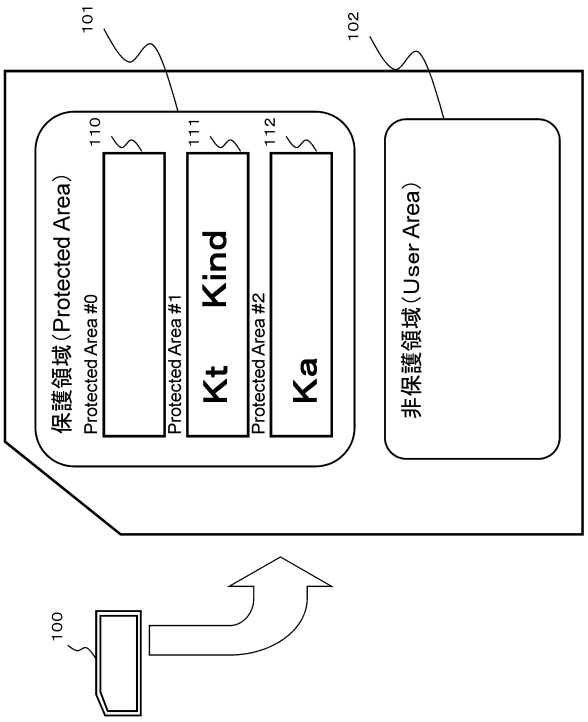
【図６】

101
保護領域(Protected Area)
Protected Area #0
Protected Area #1
Protected Area #2
110
111
112
非保護領域(User Area)
102
100
ホスト機器
140
Host Cert
Read: #0,1
Write: #0
サーバ
120
Server Cert
Read: #1
Write: #1
Read/Write OK
Read/Write NG
Read/Write OK
Read OK
Write NG
Read/Write NG
Read/Write NG

【図７】



【図９】

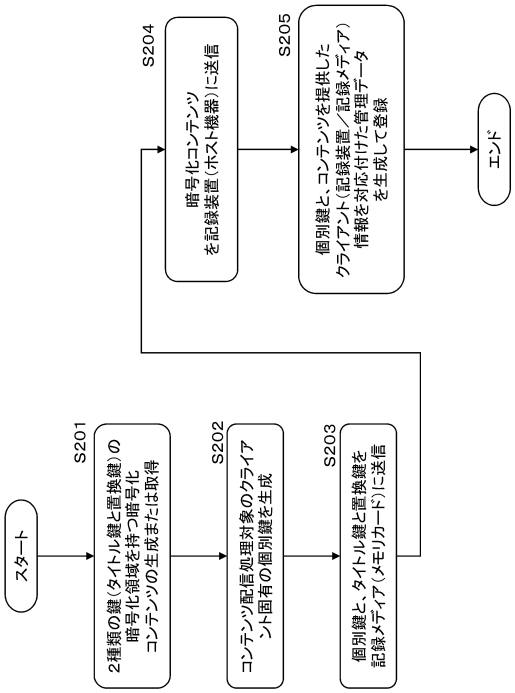


【図１３】

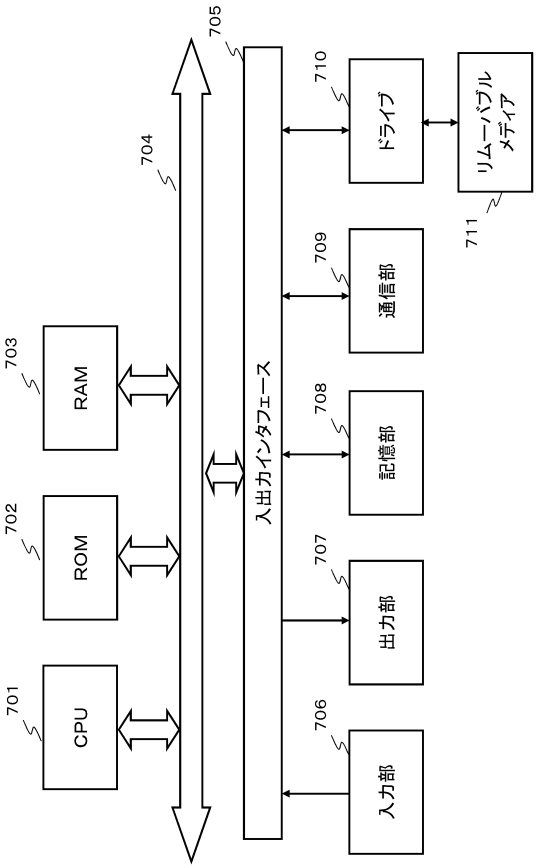
記録装置（ホスト機器）と記録メディア（メモリカード）を個別に登録してもよい

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

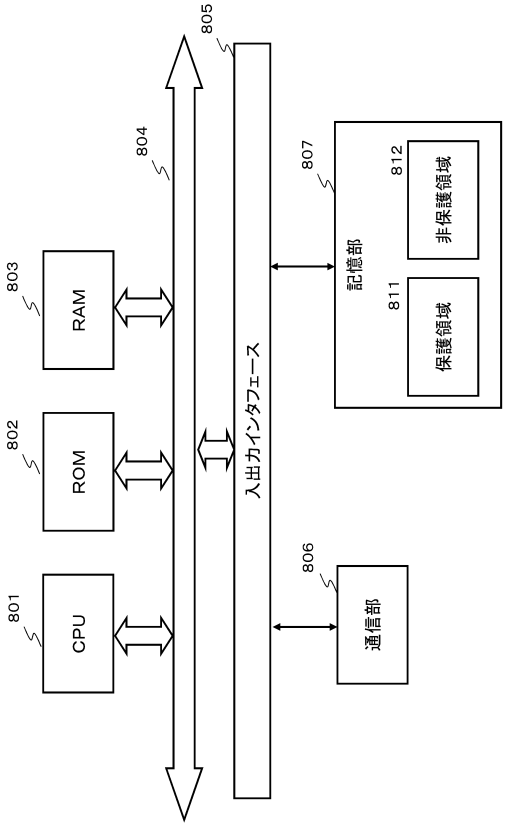
【図１４】



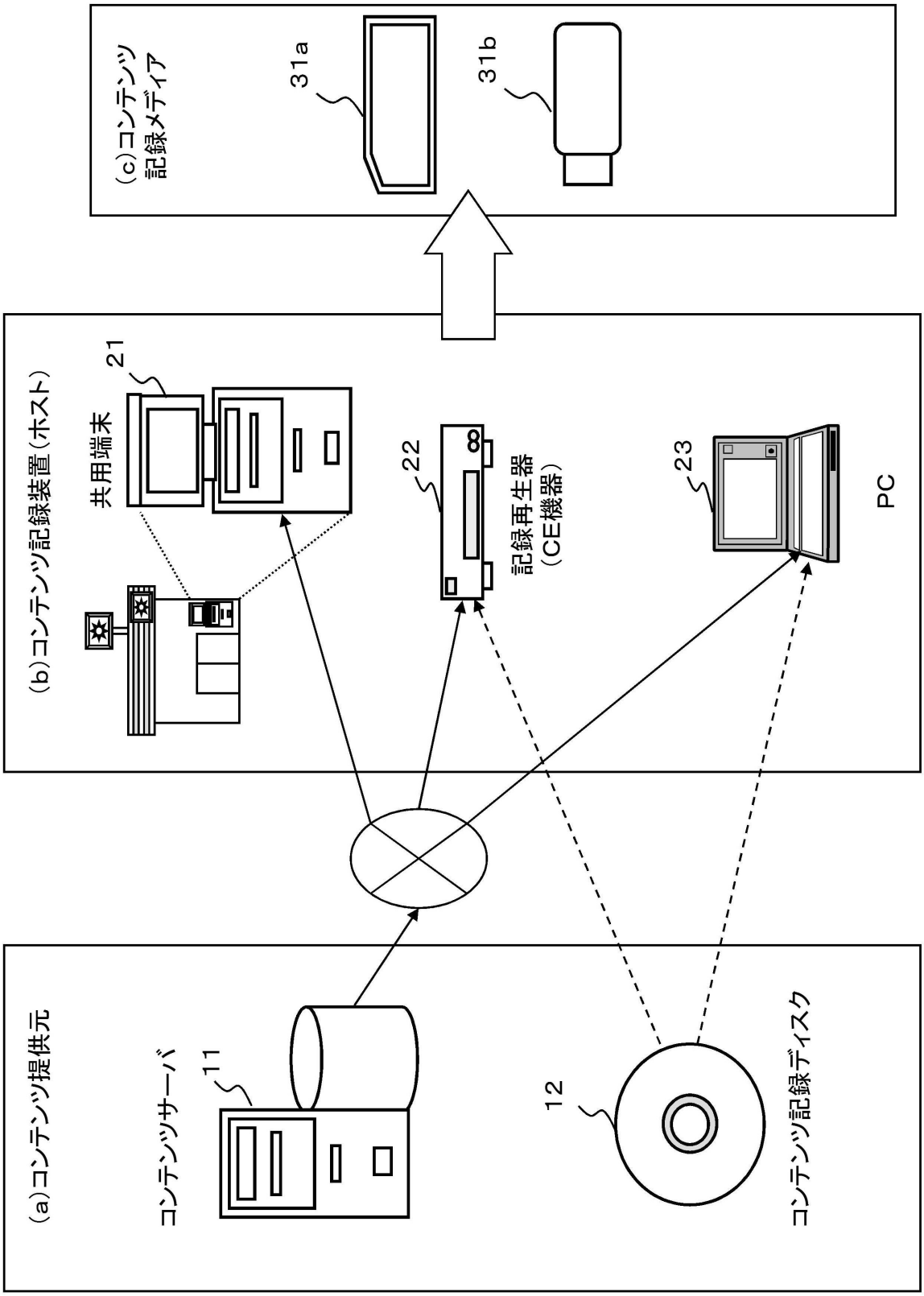
【図１６】


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

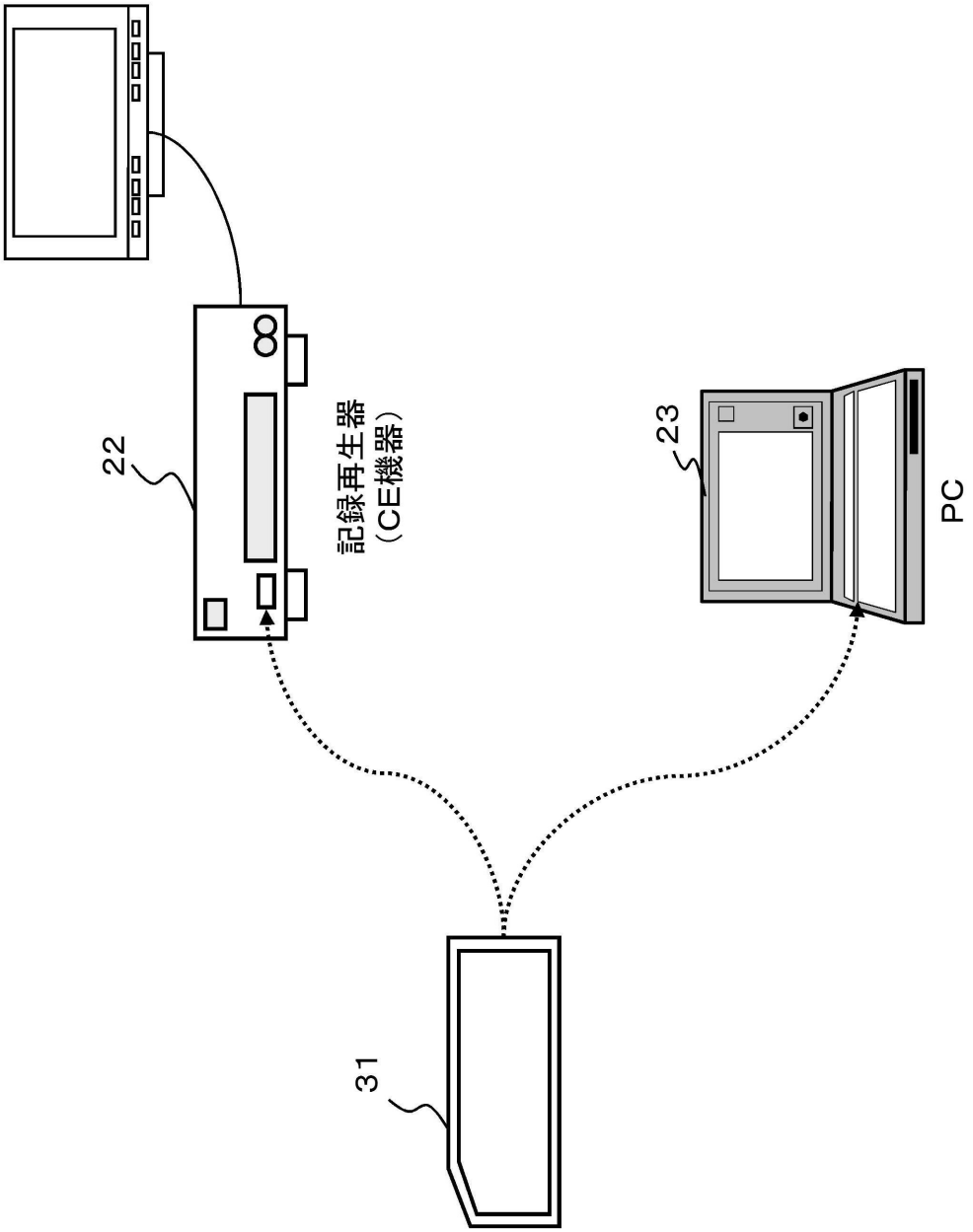
【図１７】


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

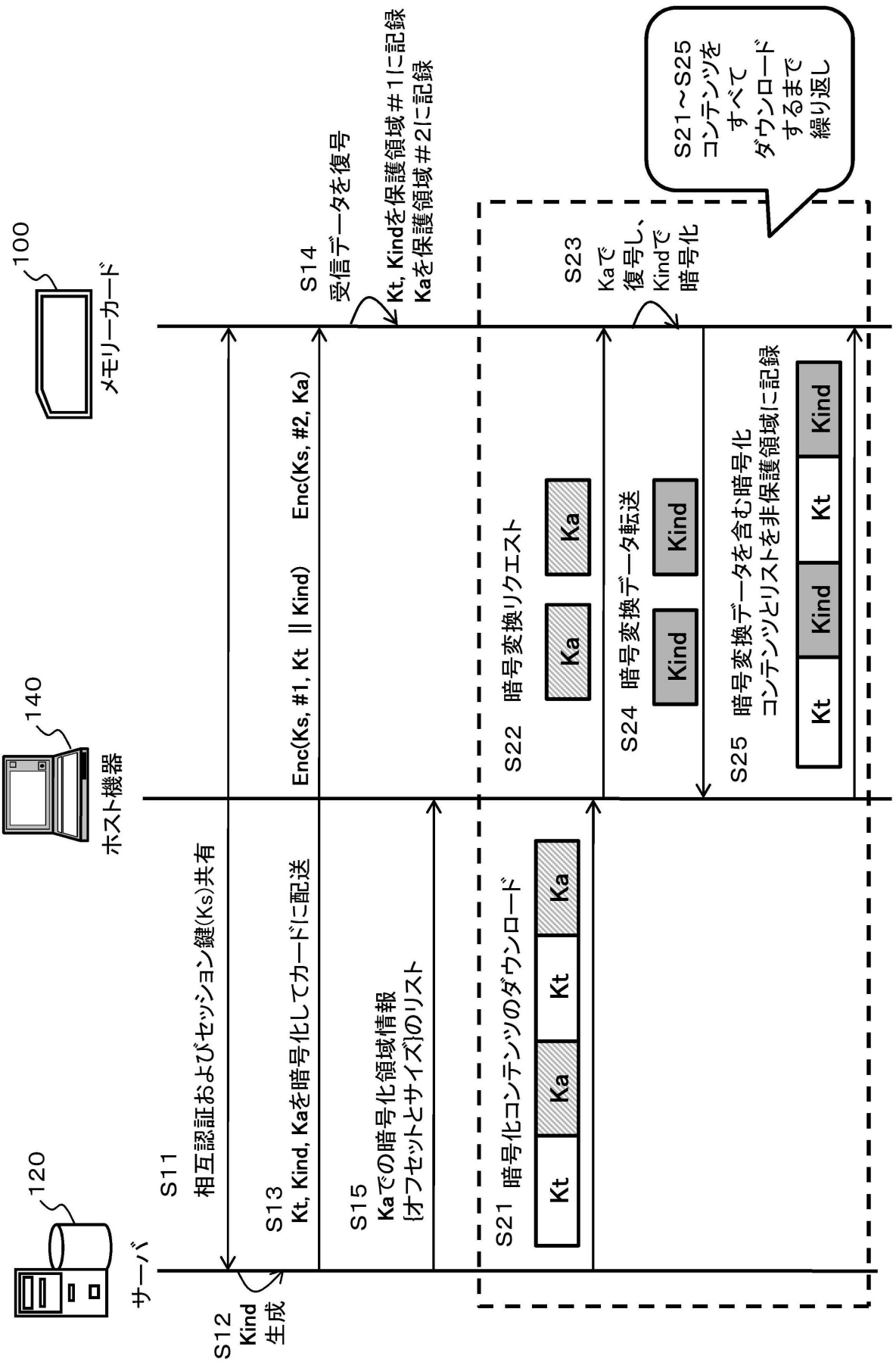
【図１】


(a)コンテンツ提供元
コンテンツサーバ
11
12
コンテンツ記録ディスク
(b)コンテンツ記録装置(ホスト)
共用端末
21
22
記録再生器
(CE機器)
23
PC
(c)コンテンツ
記録メディア
31a
31b

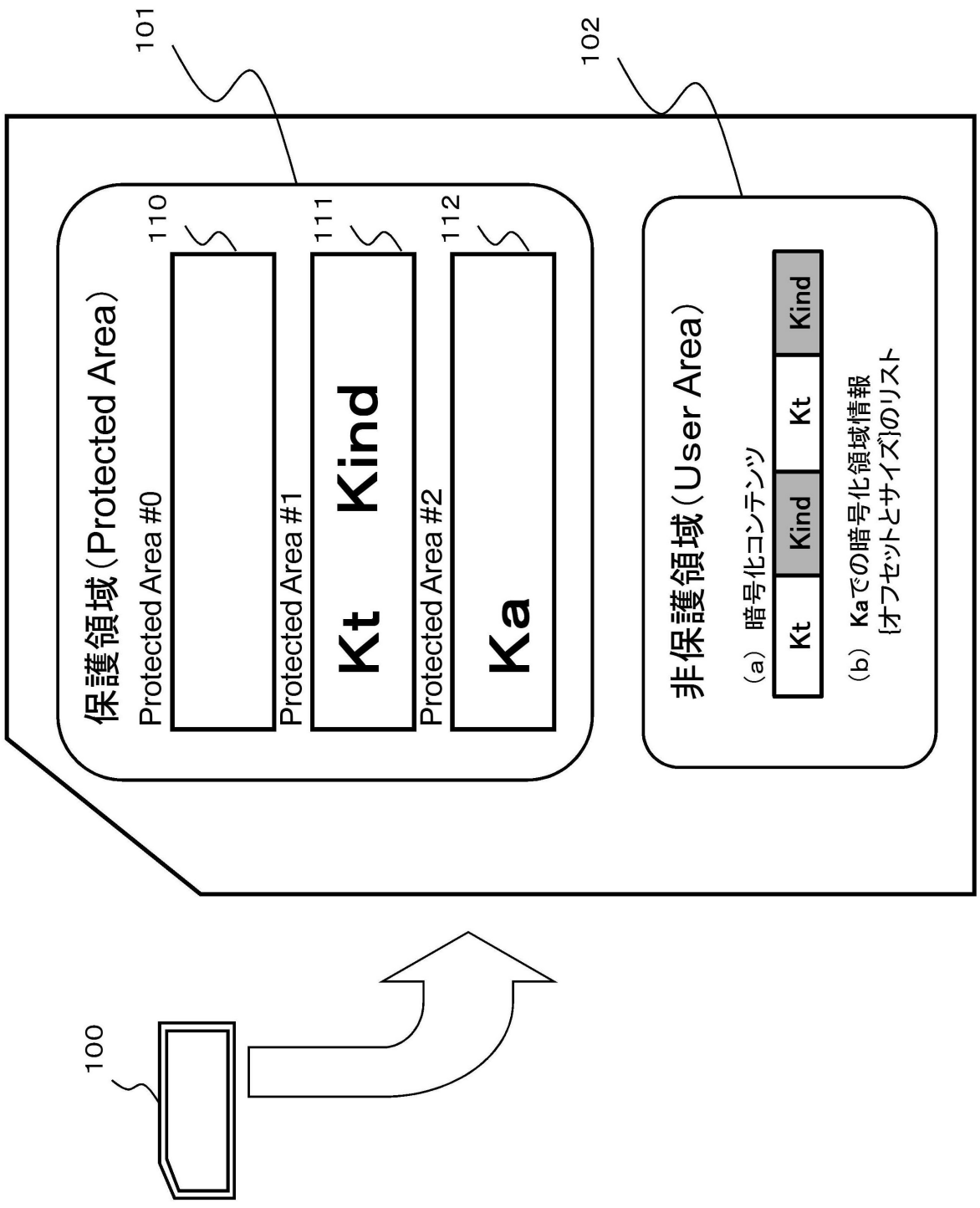
【図２】



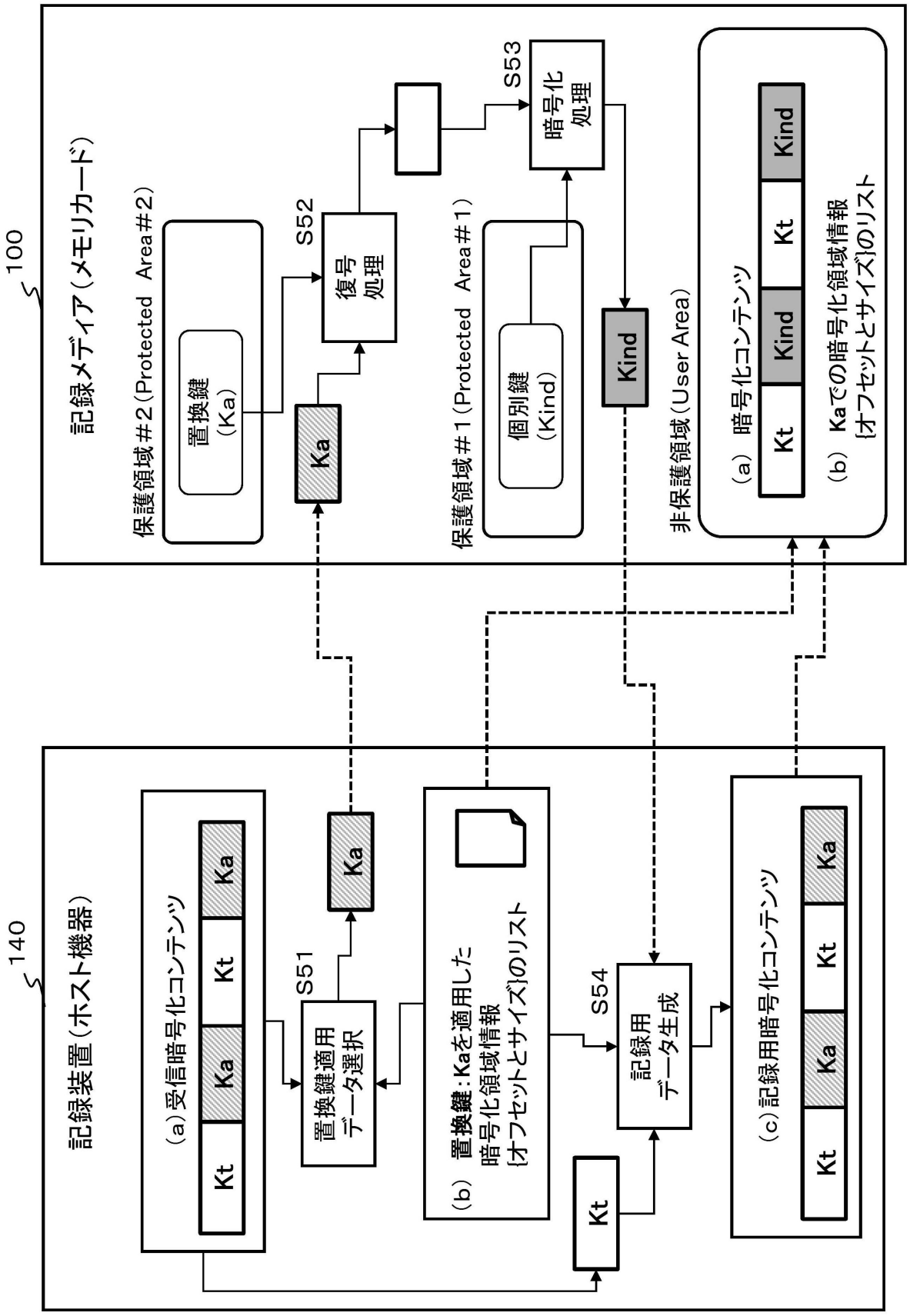
【図８】


100
メモリーカード
140
ホスト機器
120
サーバ
S11
相互認証およびセッション鍵(Ks)共有
S12
Kind
生成
S13
Kt, Kind, Kaを暗号化してカードに配送
Enc(Ks, #1, Kt || Kind)
Enc(Ks, #2, Ka)
S14
受信データを復号
Kt, Kindを保護領域#1に記録
Kaを保護領域#2に記録
S15
Kaでの暗号化領域情報
{オフセットとサイズ}のリスト
S21 暗号化コンテンツのダウンロード
Kt
Ka
Kt
Ka
S22 暗号変換リクエスト
Ka
Ka
S23
Kaで
復号し、
Kindで
暗号化
S24 暗号変換データ転送
Kind
Kind
S25 暗号変換データを含む暗号化
コンテンツとリストを非保護領域に記録
Kt
Kind
Kt
Kind
S21～S25
コンテンツを
すべて
ダウンロード
するまで
繰り返し

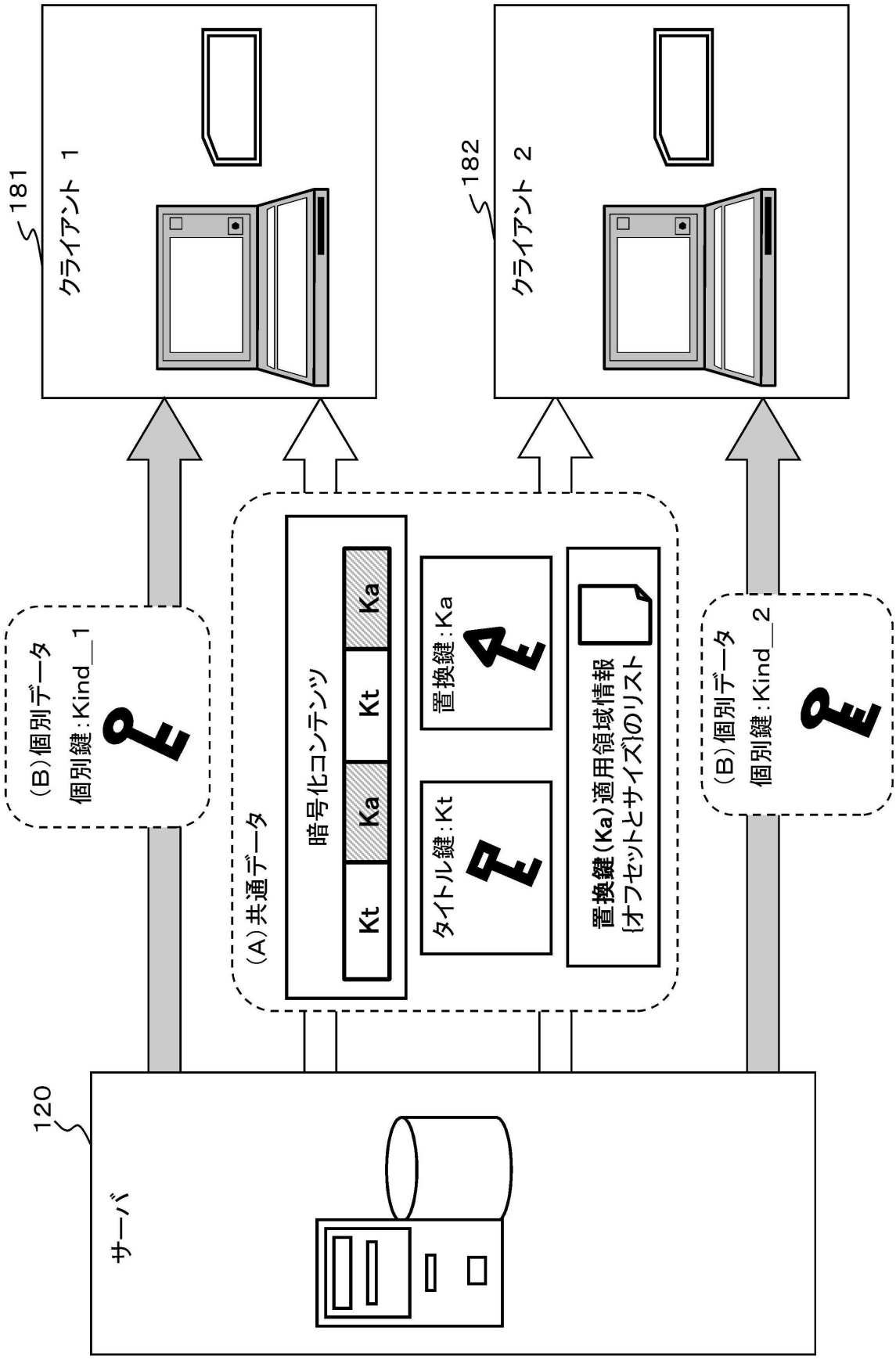
【図１０】


101
102
保護領域（Protected Area）
Protected Area #0
Protected Area #1
Protected Area #2
110
111
112
Kt
Kind
Ka
非保護領域（User Area）
（a）暗号化コンテンツ
Kt
Kind
Kt
Kind
（b）Kaでの暗号化領域情報
{オフセットとサイズ}のリスト
100

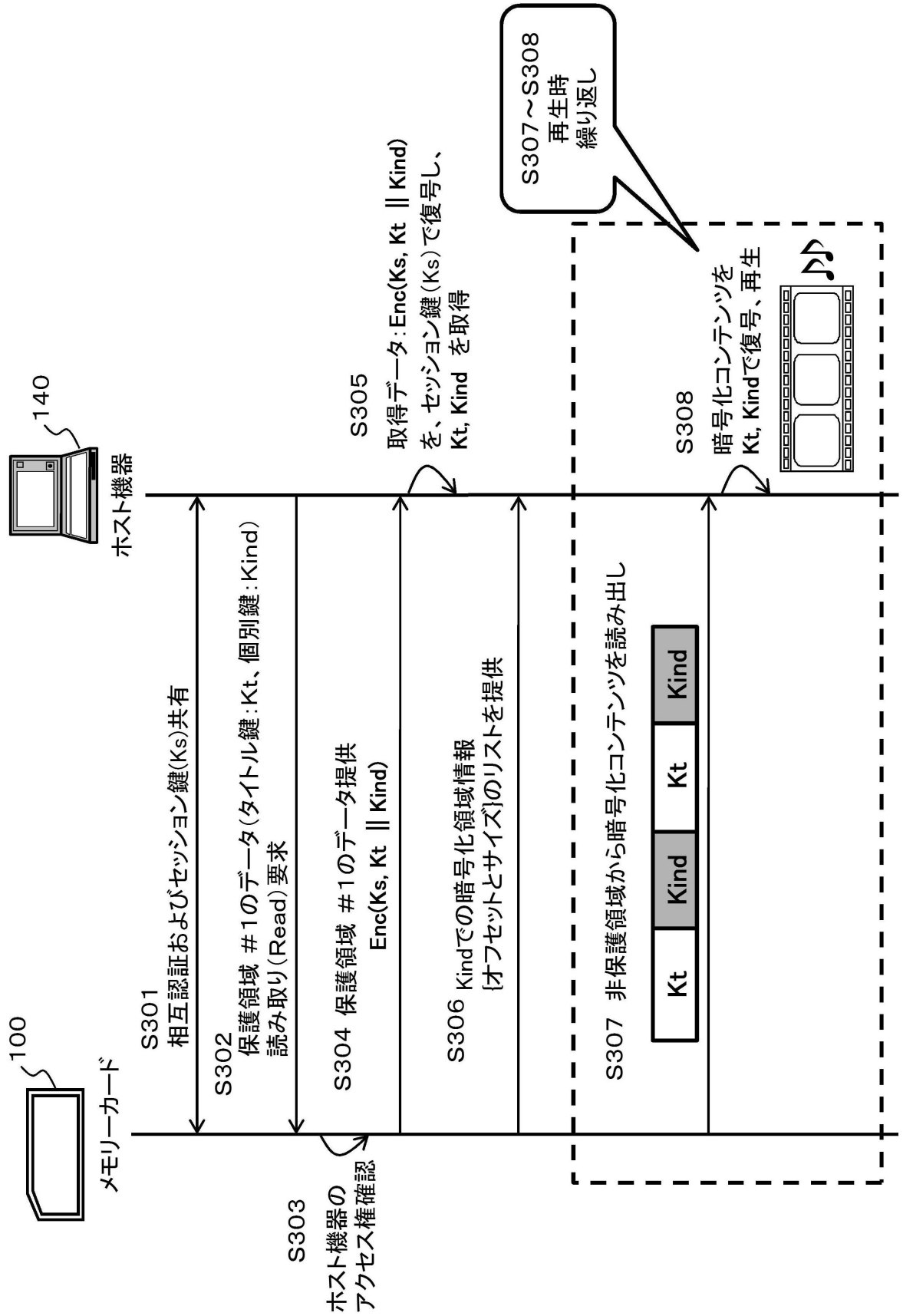
【図１１】


100
記録メディア（メモリカード）
保護領域＃2（Protected Area＃2）
置換鍵
（Ka）
Ka
S52
復号
処理
保護領域＃1（Protected Area＃1）
個別鍵
（Kind）
S53
暗号化
処理
Kind
非保護領域（User Area）
（a）暗号化コンテンツ
Kt
Kind
Kt
Kind
（b）Kaでの暗号化領域情報
{オフセットとサイズ}のリスト
140
記録装置（ホスト機器）
（a）受信暗号化コンテンツ
Kt
Ka
Kt
Ka
S51
置換鍵適用
データ選択
Ka
（b）置換鍵：Kaを適用した
暗号化領域情報
{オフセットとサイズ}のリスト
S54
記録用
データ生成
Kt
（c）記録用暗号化コンテンツ
Kt
Ka
Kt
Ka

【図１２】


クライアント 1
181
クライアント 2
182
(B)個別データ
個別鍵:Kind_1
(A)共通データ
暗号化コンテンツ
Kt
Ka
Kt
Ka
タイトル鍵:Kt
置換鍵:Ka
置換鍵(Ka)適用領域情報
{オフセットとサイズ}のリスト
(B)個別データ
個別鍵:Kind_2
サーバ
120

【図１５】


100
メモリーカード
140
ホスト機器
S301
相互認証およびセッション鍵(Ks)共有
S302
保護領域 #1のデータ(タイトル鍵:Kt、個別鍵:Kind)
読み取り(Read)要求
S303
ホスト機器の
アクセス権確認
S304 保護領域 #1のデータ提供
Enc(Ks, Kt || Kind)
S305
取得データ:Enc(Ks, Kt || Kind)
を、セッション鍵(Ks)で復号し、
Kt, Kind を取得
S306 Kindでの暗号化領域情報
{オフセットとサイズ}のリストを提供
S307 非保護領域から暗号化コンテンツを読み出し
Kt
Kind
Kt
Kind
S308
暗号化コンテンツを
Kt, Kindで復号、再生
S307～S308
再生時
繰り返し

フロントページの続き

(72)発明者　久野　浩
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　林　隆道
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　海老原　宗毅
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　上田　健二朗
東京都港区港南１丁目７番１号　ソニー株式会社内

審査官　岸野　徹

(56)参考文献　国際公開第２００９／０４５６６５（WO，Ａ１）
特開２００３－１５８５１４（ＪＰ，Ａ）
特開２００５－１６５７３８（ＪＰ，Ａ）
特開２０００－０９８８８５（ＪＰ，Ａ）
特開２０１０－２３９４３６（ＪＰ，Ａ）
特開２００６－１７３８５３（ＪＰ，Ａ）
特開２００２－２４７０２１（ＪＰ，Ａ）
特開２０１０－１１９０３４（ＪＰ，Ａ）
特表２００１－５０７１７７（ＪＰ，Ａ）

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