(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-242519
(P2005-242519A)
(43)公開日　平成17年9月8日(2005.9.8)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 17/60	G06F 17/60	142	5J104
H04L 9/08	G06F 17/60	302E	
	G06F 17/60	512	
	H04L 9/00	601B	
	H04L 9/00	601F	

審査請求 未請求　請求項の数 10　OL　（全 38 頁）

(21)出願番号　特願2004-49164(P2004-49164)
(22)出願日　平成16年2月25日(2004.2.25)

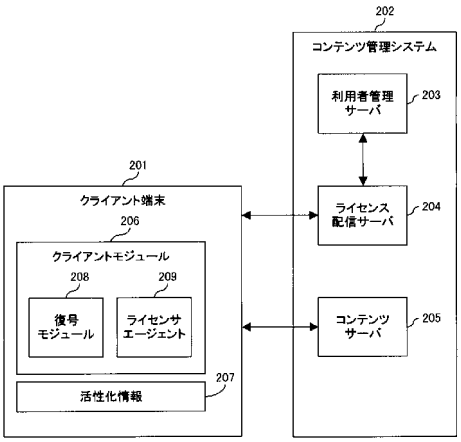
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　100067987
弁理士　久木元　彰
(72)発明者　徳谷　崇
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　畠山　卓久
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】デジタル著作権管理のための情報処理装置

(57)【要約】
【課題】　デジタルコンテンツのライセンス配信に用いる公開鍵証明書の管理・運用を簡単にし、デジタル著作権管理を改善する。
【解決手段】　ライセンス配信サーバ２０４は、公開鍵証明書と秘密鍵の情報を活性化情報２０７として、クライアントモジュール２０６とは別に、クライアント端末２０１に配信する。そして、公開鍵証明書が危殆化した場合、活性化情報２０７のみを再度配信する。また、ライセンス配信サーバ２０４は、要求されたコンテンツおよび要求者に対応する許諾条件を記述したアクセス制御リストが複数存在する場合、１つのアクセス制御リストを選択して個別ライセンスを生成し、クライアント端末２０１に配信する。
【選択図】図２

コンテンツ保護システムの構成図



【特許請求の範囲】
【請求項１】
暗号化されたデジタルコンテンツを復号するためのライセンスデータを公開鍵基盤を利用して取得するプログラムである端末モジュールを、利用者端末に配信する情報処理装置であって、
暗号鍵を格納する格納手段と、
前記公開鍵基盤に基づく暗号化通信に必要な公開鍵証明書および該公開鍵証明書の公開鍵に対する秘密鍵の情報を、前記暗号鍵を用いて暗号化して、暗号化情報を生成する生成手段と、
前記暗号化情報を復号する復号鍵を含み、前記利用者端末上で起動された後に該暗号化情報を復号して、前記公開鍵証明書および秘密鍵の情報を取得する端末モジュールと、該暗号化情報とを前記利用者端末に送信する送信手段と
を備えることを特徴とする情報処理装置。
【請求項２】
利用者端末からデジタルコンテンツに対するアクセス要求を受信し、該デジタルコンテンツにアクセスするためのライセンスデータを応答として該利用者端末に配信する情報処理装置であって、
デジタルコンテンツに対応付けて、アクセスが許可される利用者、許可されるアクセス形態、および許諾条件を記述した複数のアクセス制御リストを格納する格納手段と、
前記複数のアクセス制御リストの中から、前記アクセス要求に含まれるコンテンツ識別子に対応し、かつ、該アクセス要求を送信した要求者の利用者識別子に対応するアクセス制御リストを取得し、得られたアクセス制御リストが複数存在する場合、得られた複数のアクセス制御リストの中から１つのアクセス制御リストを選択し、選択したアクセス制御リストに基づく個別ライセンスデータを生成する生成手段と、
前記個別ライセンスデータを前記利用者端末に送信する送信手段と
を備えることを特徴とする情報処理装置。
【請求項３】
デジタルコンテンツに対するアクセス要求をライセンス配信装置に送信し、該デジタルコンテンツにアクセスするためのライセンスデータを応答として該ライセンス配信装置から受信する情報処理装置であって、
前記デジタルコンテンツに対して許可されるアクセス形態および許諾条件を記述した複数のアクセス制御リストと選択処理を指定する情報とを含み、前記ライセンス配信装置から受信した前記ライセンスデータを格納する格納手段と、
前記ライセンスデータにより指定された選択処理を実行して、前記複数のアクセス制御リストの中から１つのアクセス制御リストを選択する選択手段と
を備えることを特徴とする情報処理装置。
【請求項４】
暗号化されたデジタルコンテンツを復号するためのライセンスデータを公開鍵基盤を利用して取得するプログラムである端末モジュールを、利用者端末に配信するコンピュータのためのプログラムであって、
前記公開鍵基盤に基づく暗号化通信に必要な公開鍵証明書および該公開鍵証明書の公開鍵に対する秘密鍵の情報を、格納手段に格納された暗号鍵を用いて暗号化して、暗号化情報を生成し、
前記暗号化情報を復号する復号鍵を含み、前記利用者端末上で起動された後に該暗号化情報を復号して、前記公開鍵証明書および秘密鍵の情報を取得する端末モジュールと、該暗号化情報とを前記利用者端末に送信する
処理を前記コンピュータに実行させることを特徴とするプログラム。
【請求項５】
暗号化されたデジタルコンテンツを復号するためのライセンスデータを、ライセンス配信装置から公開鍵基盤を利用して取得するコンピュータのためのプログラムであって、

格納手段に格納された暗号化情報を前記プログラムに含まれる復号鍵を用いて復号して、前記公開鍵基盤に基づく暗号化通信に必要な公開鍵証明書および該公開鍵証明書の公開鍵に対する秘密鍵の情報を取得し、
前記公開鍵証明書および秘密鍵の情報を用いて暗号化通信を行うことで、前記ライセンス配信装置から前記ライセンスデータを取得する
処理を前記コンピュータに実行させることを特徴とするプログラム。
【請求項６】
利用者端末からデジタルコンテンツに対するアクセス要求を受信し、該デジタルコンテンツにアクセスするためのライセンスデータを応答として該利用者端末に配信するコンピュータのためのプログラムであって、
デジタルコンテンツに対応付けて、アクセスが許可される利用者、許可されるアクセス形態、および許諾条件を記述した、格納手段に格納された複数のアクセス制御リストの中から、前記アクセス要求に含まれるコンテンツ識別子に対応し、かつ、該アクセス要求を送信した要求者の利用者識別子に対応するアクセス制御リストを取得し、
得られたアクセス制御リストが複数存在する場合、得られた複数のアクセス制御リストの中から１つのアクセス制御リストを選択し、
選択したアクセス制御リストに基づく個別ライセンスデータを生成する
処理を前記コンピュータに実行させることを特徴とするプログラム。
【請求項７】
公開鍵証明書の識別名の一部分を表す相対識別名であって、前記選択したアクセス制御リストの許諾ドメインサブジェクトリストに記述された該相対識別名と、前記利用者端末が保有する公開鍵証明書の識別名を比較し、該利用者端末が保有する公開鍵証明書の識別名の一部分と該相対識別名が一致したとき、前記個別ライセンスデータを該利用者端末に配信する処理を、前記コンピュータにさらに実行させることを特徴とする請求項６記載のプログラム。
【請求項８】
デジタルコンテンツに対するアクセス要求をライセンス配信装置に送信し、該デジタルコンテンツにアクセスするためのライセンスデータを応答として該ライセンス配信装置から受信するコンピュータのためのプログラムであって、
前記デジタルコンテンツに対して許可されるアクセス形態および許諾条件を記述した複数のアクセス制御リストと選択処理を指定する情報とを含み、前記ライセンス配信装置から受信して格納手段に格納されたライセンスデータを参照し、
前記ライセンスデータにより指定された選択処理を実行して、前記複数のアクセス制御リストの中から１つのアクセス制御リストを選択する
処理を前記コンピュータに実行させることを特徴とするプログラム。
【請求項９】
暗号化されたデジタルコンテンツを復号するためのライセンスデータを公開鍵基盤を利用して取得するプログラムである端末モジュールを、利用者端末に配信する情報処理方法であって、
生成手段が、前記公開鍵基盤に基づく暗号化通信に必要な公開鍵証明書および該公開鍵証明書の公開鍵に対する秘密鍵の情報を、格納手段に格納された暗号鍵を用いて暗号化して、暗号化情報を生成し、
送信手段が、前記暗号化情報を復号する復号鍵を含み、前記利用者端末上で起動された後に該暗号化情報を復号して、前記公開鍵証明書および秘密鍵の情報を取得する端末モジュールと、該暗号化情報とを前記利用者端末に送信する
ことを特徴とする情報処理方法。
【請求項１０】
利用者端末からデジタルコンテンツに対するアクセス要求を受信し、該デジタルコンテンツにアクセスするためのライセンスデータを応答として該利用者端末に配信する情報処理方法であって、

生成手段が、デジタルコンテンツに対応付けて、アクセスが許可される利用者、許可されるアクセス形態、および許諾条件を記述した、格納手段に格納された複数のアクセス制御リストの中から、前記アクセス要求に含まれるコンテンツ識別子に対応し、かつ、該アクセス要求を送信した要求者の利用者識別子に対応するアクセス制御リストを取得し、

前記生成手段が、得られたアクセス制御リストが複数存在する場合、得られた複数のアクセス制御リストの中から１つのアクセス制御リストを選択し、

前記生成手段が、選択したアクセス制御リストに基づく個別ライセンスデータを生成する

ことを特徴とする情報処理方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、電子機密文書等のデジタルコンテンツの登録から配信までを管理し、配信されたコンテンツの閲覧、保存、編集、コピー等の操作を制御する技術に係り、デジタル著作権管理（Digital Rights Management , ＤＲＭ）技術を用いてデジタルコンテンツを安全に管理するための情報処理装置に関する。

【背景技術】

【０００２】

インターネット上におけるデジタルコンテンツの著作権保護の問題に対処する技術として、ＤＲＭ技術が知られている。ＤＲＭ技術とは、一般的には、デジタルコンテンツを保護し、コンテンツの配布および管理を行う技術である。ただし、本明細書で用いるＤＲＭ技術は、以下のようなものを指している。

・コンテンツを暗号化し、コンテンツに対する許諾条件とコンテンツの復号鍵をライセンスに格納しておく。

・利用者は、コンテンツを利用するときに、暗号化コンテンツをコンテンツサーバからダウンロードし、ライセンス配信サーバからライセンスをダウンロードした後、そのライセンスの許諾条件に従ってコンテンツを使用する。

【０００３】

ＤＲＭ技術を用いて電子文書を管理する上で、ライセンスの配信制御と、利用者ごとの個別ライセンスを生成する仕組みについては、先願の「機密コンテンツ管理方法」（特願２００３－０９５７２３）に記載されている。

【０００４】

また、本願の発明者が考案に関与したＤＲＭ技術の方式であるＵＤＡＣ（Universal Distribution with Access Control）を開示した技術論文（非特許文献１参照）には、ＵＤＡＣの音楽コンテンツの適用事例等が記載されている。

【非特許文献１】穴澤建明、武村浩司、常広隆司、長谷部高行、畠山卓久、“コンテンツ保護の柔軟化を実現した開放型超流通基盤”、［online］、情報処理学会研究会報告　ＥＩＰ１４－５、２００１年１１月、［平成１６年２月４日検索］、インターネット＜ＵＲＬ：http://www.keitaide-music.org/pdf/EIP14-5.pdf ＞

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかしながら、上述した従来のコンテンツ管理方法には以下のような問題がある。

（１）ＤＲＭによるコンテンツ管理システムでは、ライセンスを配信するときに、クライアントーサーバ間の通信に公開鍵基盤（Public Key Infrastructure , ＰＫＩ）に基づく公開鍵証明書を利用している。その公開鍵証明書の管理・運用にあたっては、認証局（Certificate Authority , ＣＡ）を導入する必要がある。高いセキュリティ強度の維持を要求するシステムは、厳格な認証局を利用し、顧客のセキュリティドメインごとにクライアントモジュールを耐攻撃モジュール（Tamper Resistant Module , ＴＲＭ）化する必要がある。しかし、現在では、セキュリティ強度が多少落ちても、簡易認証局を利用して手軽

かつ安価にＤＲＭを運用したいという要望の方が多い。
【０００６】
また、開発元は、クライアントモジュール内にあらかじめクラス公開鍵証明書とそれに対応する秘密鍵を埋め込んだ状態で、クライアントモジュールをＴＲＭ化し出荷している。この形態では、クラス公開鍵証明書が危殆化した場合、もう一度開発元がクライアントモジュールを作り直さなければならず、利用者は、クライアントモジュールをインストールし直さなければならない。
（２）各利用者に配信されるライセンスは、ライセンス配信サーバがアクセス制御リスト（Access Control List，ＡＣＬ）を参照して個別に生成する。ライセンスはグループや利用者単位で設定されており、具体的には、グループＡにはコンテンツの印刷を許諾し、グループＢには印刷を禁止する等の許諾条件が設定される。このような状況の中で、利用者が１つ以上のグループに所属している場合があり、その利用者に対してどの許諾条件のライセンスを配信すべきかを決めなければならない。
（３）クライアント端末にダウンロードされたライセンスを、ある限られた別のクライアント端末に渡す制御は実現されていない。
（４）図４６に示すように、保護対象となるコンテンツに対してクライアント端末１１でどのような操作が行われたかを示す操作ログ１３は、クライアント端末１１により管理され、適切なタイミングでログ管理サーバ１２に送信されて、ログデータ１４として管理される。しかし、クライアント側でログを管理すると、改ざん等を容易に行うことが可能である。また、改ざん防止等の処置をとろうとするとコストがかかってしまい、実施するのは難しい。
（５）ライセンス配信サーバは、１回のライセンス要求に対して１つのコンテンツに対する許諾条件しか配信することができない。そのため、複数のコンテンツを利用するとき、クライアント端末は、ライセンス配信サーバに複数回のライセンス要求を行わなければならない。
（６）クライアント端末によるライセンスの取得時に、ＤＲＭによるコンテンツ保護システムで認証された端末かどうかをライセンス配信サーバに知らせる仕組みがないので、認証されていないクライアント端末にまでライセンスが配信されてしまう。
（７）クライアント端末が、同一コンテンツに対して複数の許諾条件を格納しているライセンスを受信した場合、その中から１つの許諾条件を選択する方法がないため、受信したライセンスを利用することができない。
（８）ＤＲＭで保護されたコンテンツを編集する際に、コンテンツ内のデータの切り取りやコピー等の操作により、共有メモリ（クリップボード）からデータが盗まれてしまう。
【０００７】
本発明の第１の課題は、公開鍵証明書が危殆化した場合でもクライアントモジュールの再作成・再インストールを行う必要がなく、公開鍵証明書の管理・運用を簡便に行えるような情報処理装置を提供することである。
【０００８】
本発明の第２の課題は、改善されたＤＲＭによるコンテンツ管理を実現する情報処理装置を提供することである。
【課題を解決するための手段】
【０００９】
図１は、本発明の第１および第２の情報処理装置の原理図である。図１の情報処理装置は、格納手段１０１、生成手段１０２、および送信手段１０３を備える。第１および第２の情報処理装置は、例えば、後述する図２のライセンス配信サーバ２０４に対応し、格納手段１０１、生成手段１０２、および送信手段１０３は、例えば、後述する図４４のメモリ４４０２、ＣＰＵ（中央処理装置）４４０１、およびネットワーク接続装置４４０７にそれぞれ対応する。
【００１０】
第１の情報処理装置は、暗号化されたデジタルコンテンツを復号するためのライセンス

データを公開鍵基盤を利用して取得するプログラムである端末モジュール１１１を、利用者端末に配信する。格納手段１０１は、暗号鍵を格納し、生成手段１０２は、公開鍵基盤に基づく暗号化通信に必要な公開鍵証明書およびその公開鍵に対する秘密鍵の情報を、暗号鍵を用いて暗号化して、暗号化情報１１２を生成する。送信手段１０３は、暗号化情報１１２を復号する復号鍵を含み、利用者端末上で起動された後に暗号化情報を復号して、公開鍵証明書および秘密鍵の情報を取得する端末モジュール１１１と、暗号化情報１１２とを利用者端末に送信する。

【００１１】

生成手段１０２は、暗号鍵を格納手段１０１から取り出し、その暗号鍵を用いて公開鍵証明書および秘密鍵の情報を暗号化して暗号化情報１１２を生成する。送信手段１０３は、端末モジュール１１１と生成された暗号化情報１１２を利用者端末に送信する。利用者端末上で端末モジュール１１１が起動されると、端末モジュール１１１は復号鍵を用いて暗号化情報１１２を復号して、公開鍵証明書および秘密鍵の情報を取得し、その情報を用いてライセンス配信サーバと暗号化通信を行って、ライセンスデータ１１３を取得する。

【００１２】

このように、公開鍵証明書および秘密鍵の情報を端末モジュール１１１とは別に配信しておけば、利用者端末上で公開鍵証明書が危殆化した場合でも、新たな公開鍵証明書および秘密鍵の情報を含む暗号化情報を再度配信するだけで済む。したがって、端末モジュール１１１の再作成・再インストールを行う必要がなく、証明書更新のためのコストを低く抑えることができる。

【００１３】

端末モジュール１１１および暗号化情報１１２は、例えば、図２のクライアントモジュール２０６および活性化情報２０７にそれぞれ対応する。また、利用者端末は、例えば、図２のクライアント端末２０１に対応し、暗号鍵および復号鍵は、例えば、図４のＫｓおよびＫｍ３に対応し、公開鍵証明書および秘密鍵は、例えば、図４のＣｃｉおよびＫｃｉ（ｉ＝１，２，．．．，ｎ）に対応する。

【００１４】

第２の情報処理装置は、利用者端末からデジタルコンテンツに対するアクセス要求を受信し、デジタルコンテンツにアクセスするためのライセンスデータを応答として利用者端末に配信する。格納手段１０１は、デジタルコンテンツに対応付けて、アクセスが許可される利用者、許可されるアクセス形態、および許諾条件を記述した複数のアクセス制御リストを格納する。生成手段１０２は、それらのアクセス制御リストの中から、アクセス要求に含まれるコンテンツ識別子に対応し、かつ、アクセス要求を送信した要求者の利用者識別子に対応するアクセス制御リストを取得し、得られたアクセス制御リストが複数存在する場合、得られた複数のアクセス制御リストの中から１つのアクセス制御リストを選択し、選択したアクセス制御リストに基づく個別ライセンスデータを生成する。送信手段１０３は、その個別ライセンスデータを利用者端末に送信する。

【００１５】

生成手段１０２は、格納手段１０１に格納された複数のアクセス制御リストのうち、アクセス要求のコンテンツ識別子に対応するものを参照し、要求者の利用者識別子に対応するアクセス制御リストを抽出する。そして、得られたアクセス制御リストが複数存在する場合、その中から１つのアクセス制御リストを選択し、選択したアクセス制御リストに基づく個別ライセンスデータを生成する。送信手段１０３は、生成された個別ライセンスデータを、アクセス要求に対する応答として利用者端末に送信する。

【００１６】

このような情報処理装置によれば、要求者が複数のグループに所属しており、要求されたコンテンツに対して適用される許諾条件が複数存在する場合でも、その要求者に対して適用すべき許諾条件を自動的に決定し、ライセンスを配信することができる。

【００１７】

本発明の第３の情報処理装置は、格納手段および選択手段を備え、デジタルコンテンツ

に対するアクセス要求をライセンス配信装置に送信し、デジタルコンテンツにアクセスするためのライセンスデータを応答としてライセンス配信装置から受信する。格納手段は、デジタルコンテンツに対して許可されるアクセス形態および許諾条件を記述した複数のアクセス制御リストと選択処理を指定する情報とを含み、ライセンス配信装置から受信したライセンスデータを格納する。選択手段は、ライセンスデータにより指定された選択処理を実行して、それらのアクセス制御リストの中から１つのアクセス制御リストを選択する。

【００１８】

選択手段は、ライセンス配信装置から受信して格納手段に格納されたライセンスデータを参照して、指定された選択処理を実行し、ライセンスデータに含まれる複数のアクセス制御リストの中から１つのアクセス制御リストを選択する。

【００１９】

このような情報処理装置によれば、同一コンテンツに対して複数の許諾条件を格納しているライセンスを受信した場合でも、所定の選択処理により自動的に１つの許諾条件を選択して、受信したライセンスを利用することができる。

【００２０】

第３の情報処理装置は、例えば、図２のクライアント端末２０１に対応し、格納手段および選択手段は、例えば、図４４のメモリ４４０２およびＣＰＵ４４０１にそれぞれ対応する。また、ライセンス配信装置は、例えば、図２のライセンス配信サーバ２０４に対応し、選択処理を指定する情報は、例えば、後述する図３９のｓｃｒｉｐｔ＿ｉｄに対応する。

【発明の効果】

【００２１】

本発明によれば、ＰＫＩを利用したＤＲＭによるコンテンツ管理システムにおいて、厳格な認証局を利用する場合に比べて、簡便な方法で公開鍵証明書の管理・運用を行うことができる。これにより、ＰＫＩの構築およびＤＲＭによるコンテンツ管理システムの開発が容易になる。

【００２２】

また、ＤＲＭによるコンテンツ管理が以下の点で改善される。

（１）１つ以上のグループに所属している利用者に対して配信すべきライセンスを自動的に決定することができる。

（２）利用者端末が同一コンテンツに対して複数の許諾条件を格納しているライセンスを受信した場合でも、自動的に１つの許諾条件を選択してライセンスを利用することができる。

【発明を実施するための最良の形態】

【００２３】

以下、図面を参照しながら、本発明を実施するための最良の形態を詳細に説明する。

本実施形態のコンテンツ保護システムでは、ＤＲＭクライアントモジュールと活性化情報とを別々に生成し、別々に配布する。ＤＲＭクライアントモジュールは、ライセンス取得機能と暗号化コンテンツ復号機能を備えたプログラムである。活性化情報は、利用されるクラス公開鍵証明書と、その証明書の公開鍵に対する秘密鍵の情報を含んでおり、ＤＲＭクライアントモジュールを活性化してその機能を有効にするために用いられる。

【００２４】

利用者は、ＤＲＭクライアントモジュールが配布された後、活性化情報を取得し、そのＤＲＭクライアントモジュールが、活性化情報内にあるクラス公開鍵証明書と秘密鍵をＤＲＭクライアントモジュールに自動的にセットする。その後、ＤＲＭクライアントモジュールは、ライセンス配信サーバからライセンスを取得するようになる。

【００２５】

図２は、このようなコンテンツ保護システムの構成図である。図２のコンテンツ保護システムは、クライアント端末２０１およびコンテンツ管理システム２０２からなり、コン

テンツ管理システム２０２は、利用者管理サーバ２０３、ライセンス配信サーバ２０４、およびコンテンツサーバ２０５を含む。クライアント端末２０１、利用者管理サーバ２０３、ライセンス配信サーバ２０４、およびコンテンツサーバ２０５は、例えば、情報処理装置（コンピュータ）に対応し、通信ネットワークを介して相互に通信することができる。

【００２６】

クライアント端末２０１は、コンテンツを利用する利用者の端末であり、コンテンツサーバ２０５から暗号化コンテンツをダウンロードし、ライセンス配信サーバ２０４からライセンスをダウンロードし、そのライセンスの許諾条件に従って暗号化コンテンツを復号する。

【００２７】

コンテンツサーバ２０５は、暗号化コンテンツを格納するデータベースを備え、利用者管理サーバ２０３は、利用者ごとの認証方式等の管理情報を格納するデータベースを備える。ライセンス配信サーバ２０４は、ライセンスを格納するデータベースを備え、ＤＲＭクライアントモジュールであるクライアントモジュール２０６と活性化情報２０７とを別々に生成し、クライアント端末２０１に配信する。クライアントモジュール２０６は、復号モジュール２０８とライセンサエージェント２０９からなる。

【００２８】

クライアント端末２０１に配信されたライセンサエージェント２０９は、別に配信された活性化情報２０７を取得する。その後、ライセンサエージェント２０９は、ライセンス配信サーバ２０４からライセンスを取得し、復号モジュール２０８は、ライセンスを用いて暗号化コンテンツを復号する。

【００２９】

ここで、ライセンサエージェント２０９がどのような活性化情報でも受け付けてしまう場合、悪意のある利用者が偽のライセンス配信サーバを立ち上げて、適当な活性化情報を配信することにより、その利用者が作成した復号モジュールにライセンスが渡り、利用される可能性がある。

【００３０】

例えば、図３に示すように、正当なライセンス配信サーバ３０１がライセンサエージェント３０３および復号モジュール３０４をクライアント端末に配信した場合を想定してみる。悪意のない利用者がコンテンツを利用する場合、ライセンサエージェント３０３は、ライセンス配信サーバ３０１から活性化情報３１１を取得した後に、ライセンス３１３を取得する。

【００３１】

しかし、悪意のある利用者が偽の復号モジュール３０５をクライアント端末に用意し、偽のライセンス配信サーバ３０２を立ち上げて、偽の活性化情報３１２を配信すると、ライセンサエージェント３０３は、ライセンス配信サーバ３０１から取得したライセンス３１３を復号モジュール３０５に渡してしまう可能性がある。

【００３２】

そこで、本実施形態では、証明書発行・埋込みを安全かつ自動的に実現する「クライアント活性化機能」を次のように想定する。

（１）ライセンス配信サーバインストール時に次の処理を自動的に実施する。

・認証局秘密鍵と公開鍵証明書のセットを生成し、認証局モジュール内に維持する。

・ライセンス配信サーバに認証局公開鍵証明書を登録する。

（２）「クライアント活性化コマンド（関数）」で次の処理を自動的に実施する。

・クライアントモジュールの秘密鍵と公開鍵のセットを生成する。

・その公開鍵を認証局モジュールに入力し、公開鍵証明書を発行させる。

・指定されたクライアントモジュールに秘密鍵および公開鍵証明書と、認証局公開鍵証明書を埋め込む。

・クライアント名と証明書リストの対応表を管理のために保存する。

（３）「証明書失効コマンド（関数）」で次の処理を自動的に実施する。
・失効する証明書を指定する。
・認証局で従来のＣＲＬ（Certificate Revocation List ）（失効した証明書のリスト）に指定証明書を追加したＣＲＬを生成する。
・生成したＣＲＬをライセンス配信サーバに設定する。
（４）ユニバーサル公開鍵証明書（Universal Certificate ）をクライアント活性化機能に維持し、全世界のＤＲＭ間での相互運用も可能にしておく。

【００３３】

より具体的には、認証局運用とクライアントを活性化する機能をライセンス配信サーバ管理・運用システムに実装する。クライアントモジュールのＴＲＭ化は、証明書発行ごとではなく、クライアントモジュールの提供時とバージョンアップ時にのみ実施する。クライアントモジュール活性化キーの発行は、管理・運用システム上の活性化キー自動発行機能で自動的に実施する。

【００３４】

図４は、このようなクライアント活性化機能を実現する構成を示している。ここでは、ライセンス配信サーバ管理・運用システムがライセンス配信サーバ２０４内に設けられた場合を想定している。ライセンス配信サーバ２０４は、クライアント活性化モジュール４０２、認証局モジュール４０３、および記憶装置４０４を含み、クライアント端末２０１は、記憶装置４０５を含む。

【００３５】

図４で用いられる鍵および証明書の表記法は以下の通りである。
｛Ｘ｝Ｋ：情報Ｘが鍵Ｋで復号できるように暗号化されていることを示す。
Ｋｍ２：契約鍵。各顧客（コンテンツ登録者、コンテンツ利用者等）に秘密情報を安全に提供するために必要な鍵。公開鍵暗号方式でも対称鍵暗号方式でも可。顧客がライセンス配信サーバ２０４に設定する。
Ｃｒ１：認証局の公開鍵証明書。自己署名付き。
Ｋｃｉ（ｉ＝１，２，．．．，ｎ）：ＤＲＭクラス秘密鍵。
Ｃｃｉ（ｉ＝１，２，．．．，ｎ）：Ｋｃｉに対応するクラス公開鍵証明書。
Ｋｓ：クライアントモジュール活性化キー送信ごとに変更されるセッション鍵。対称鍵暗号方式の鍵。
Ｋｍ３：クライアントマスター鍵。製造者によりクライアントモジュールに埋め込まれる対称鍵暗号方式の秘密鍵。１つのクライアントモジュールは複数種類のＫｍ３を持つことができる。

【００３６】

契約鍵Ｋｍ２は、顧客とライセンス配信サーバ管理・運用システムとで共有される。Ｋｍ２は活性化キー生成ツール４０１により生成され、配布された後、一定期間ごとに更新される。クライアントマスター鍵Ｋｍ３は、顧客とクライアントモジュールとで共有される。クライアントモジュール活性化キー｛Ｋｓ｝Ｋｍ３｜｜｛Ｋｓ｝Ｋｍ２は、活性化キー生成ツール４０１により生成され、クライアントモジュール２０６の提供時とバージョンアップ時に発行される。クライアント活性化モジュール４０２は、契約鍵とクライアントモジュール活性化キーを用いて活性化情報２０７を生成する。

【００３７】

図５は、ライセンス配信サーバ２０４の運用者による活性化情報生成手順のフローチャートである。管理・運用システムは、まず、初期化処理を行って（ステップ５０１）、その結果を判定する（ステップ５０２）。初期化処理では、認証局のルート（ルート認証局）公開鍵証明書の取得等が行われる。

【００３８】

結果がＯＫであれば、図４の（ａ）に示すように、契約鍵取得処理を行って（ステップ５０３）、その結果を判定する（ステップ５０４）。これにより、契約鍵Ｋｍ２がクライアント活性化モジュール４０２に安全に設定される。

【００３９】
結果がＯＫであれば、次に、クライアントモジュール活性化キー取得処理を行って（ステップ５０５）、その結果を判定する（ステップ５０６）。この処理では、図４の（ｃ）に示すように、活性化キー生成ツール４０１に対してクライアントモジュール活性化キーの発行を依頼し、（ｄ）に示すように、活性化キー生成ツール４０１から発行されたクライアントモジュール活性化キー｛Ｋｓ｝Ｋｍ３｜｜｛Ｋｓ｝Ｋｍ２を受け取る。クライアントモジュール活性化キーは、電子メールの交換により取得してもよい。
【００４０】
結果がＯＫであれば、次に、活性化情報生成処理を行って（ステップ５０７）、その結果を判定する（ステップ５０８）。ステップ５０２、５０４、５０６、および５０８において結果がＮＧであれば、エラー処理を行う（ステップ５０９）。
【００４１】
図６は、図５のステップ５０７でクライアント活性化モジュール４０２により行われる活性化情報生成処理のフローチャートである。クライアント活性化モジュール４０２は、まず、クライアントモジュール活性化キー取得処理を行って（ステップ６０１）、その結果を判定する（ステップ６０２）。
【００４２】
結果がＯＫであれば、次に、契約鍵Ｋｍ２でクライアントモジュール活性化キーを復号してセッション鍵Ｋｓを取得し（ステップ６０３）、その結果を判定する（ステップ６０４）。
【００４３】
結果がＯＫであれば、次に、ＤＲＭクラス秘密鍵Ｋｃｉとクラス公開鍵証明書Ｃｃｉを取得し（ステップ６０５）、その結果を判定する（ステップ６０６）。このとき、認証局モジュール４０３は、図４の（ｅ）に示すように、クラス公開鍵証明書Ｃｃｉを発行する。
【００４４】
結果がＯＫであれば、次に図４の（ｆ）に示すように、ＤＲＭクラス秘密鍵Ｋｃｉとクラス公開鍵証明書Ｃｃｉを契約鍵Ｋｍ２で暗号化し（ステップ６０７）、その結果を判定する（ステップ６０８）。このとき、図４の（ｂ）に示すように認証局が生成した公開鍵証明書Ｃｒ１も、ＫｃｉおよびＣｃｉとともに暗号化される。
【００４５】
結果がＯＫであれば、次に図４の（ｇ）に示すように、暗号化された情報とクライアントモジュール活性化キーの一部である｛Ｋｓ｝Ｋｍ３とを結合して、活性化情報２０７を生成し（ステップ６０９）、その結果を判定する（ステップ６１０）。ステップ６０２、６０４、６０６、６０８、および６１０において結果がＮＧであれば、エラー処理を行う（ステップ６１１）。
【００４６】
生成された活性化情報２０７は、図４の（ｈ）に示すように、ＴＲＭ化されたクライアントモジュール２０６とともに、記憶装置４０４内の活性化クライアントモジュール４１１に埋め込まれ、（ｉ）に示すように、ドメイン内に配布される。こうして、活性化クライアントモジュール４１１は、一旦、配布先のクライアント端末２０１の記憶装置４０５内に格納される。
【００４７】
図７は、クライアント端末２０１内のクライアントモジュール２０６による活性化情報設定処理のフローチャートである。クライアントモジュール２０６は、図４の（ｊ）に示すように、クライアント端末２０１上で起動されると、まず、活性化情報２０７を取得し（ステップ７０１）、その結果を判定する（ステップ７０２）。
【００４８】
結果がＯＫであれば、次に図４の（ｋ）に示すように、クライアントマスター鍵Ｋｍ３で活性化情報を復号してＫｃｉおよびＣｃｉを取得し（ステップ７０３）、その結果を判

定する（ステップ７０４）。この処理では、まず、｛Ｋｓ｝Ｋｍ３をＫｍ３で復号してＫｓが取り出され、次に、残りの活性化情報をＫｓで復号してＫｃｉ、Ｃｃｉ、およびＣｒ１が取り出される。

【００４９】

ステップ７０２および７０４において結果がＮＧであれば、エラー処理を行う（ステップ７０５）。

その後、クライアントモジュール２０６は、取得したＤＲＭクラス秘密鍵と証明書を用いてライセンス配信サーバ２０４と通信し、ライセンスを取得する。

【００５０】

このような仕組みによれば、クライアント端末２０１のクラス公開鍵証明書が危殆化した場合でも、クライアントモジュール２０６の再作成・再インストールを行う必要がなく、活性化情報２０７を入れ替えるだけで済む。したがって、証明書更新のためのコストを低く抑えることができる。

【００５１】

なお、図４の構成では、ライセンス配信サーバ２０４内の認証局モジュール４０３を利用してＰＫＩを構築しているが、代わりに外部認証局４０６を利用することも可能である。また、ＤＲＭクラス秘密鍵Ｋｃｉとクラス公開鍵証明書Ｃｃｉに加えて、秘密鍵Ｋｃｕとユニバーサル公開鍵証明書Ｃｃｕのセットを活性化情報２０７に追加してもよい。

【００５２】

次に、本実施形態で用いられるライセンスの例を示しながら、コンテンツ保護システムの仕組みをより詳細に説明する。

図８および図９は、ライセンスのデータ構造（ＬｉｃｅｎｓｅＩｎｆｏ構造）を示しており、図１０は、図９のａｃｌ（アクセス制御リスト）フィールドのデータであるＡｃｌ構造を示している。図１１、１２、および１３は、図１０のａｃｌ＿ｅｎｔｒｙフィールドのデータであるＡＣＬＥｎｔｒｙ構造を示しており、図１４、１５、および１６は、図１１のａｃｐ（デコーダアクセス条件）フィールドのデータであるＡｃｐ構造を示しており、図１７、１８、および１９は、図１１のａｃｍ（メディアアクセス条件）フィールドのデータであるＡｃｍ構造を示している。

【００５３】

前述した、悪意のある利用者が作成した復号モジュールにライセンスが渡り、利用できてしまう問題に対しては、以下のような対策が講じられる。図９に示すように、ライセンス内にｒｐｋ＿ｈａｓｈ＿ｌｉｓｔというフィールドを設け、ライセンス発行時に証明書チェックに利用するルート公開鍵のハッシュ値のリストを格納する。また、復号モジュール２０８、ライセンサエージェント２０９、およびライセンス配信サーバ２０４にそれぞれルート公開鍵証明書を保持させておく。

【００５４】

図２０に示すように、クライアント端末２０１のライセンサエージェント２０９は、ライセンス配信サーバ２０４にライセンス取得要求を送信する。このとき、ライセンサエージェント２０９は、証明書のルート公開鍵のハッシュ値ｒｐｋ＿ｈａｓｈ＿ｖａｌｕｅをライセンス配信サーバ２０４に送信し、ライセンス配信サーバ２０４は、受信したハッシュ値を検証する。

【００５５】

ライセンス配信サーバ２０４は、受信したハッシュ値をライセンスのｒｐｋ＿ｈａｓｈ＿ｌｉｓｔに格納されたハッシュ値と比較し、そのリスト内に該当する値が存在すれば、ライセンスを配信する。しかし、リスト内に該当する値が存在しない場合は、ライセンスを配信しない。

【００５６】

同様に、クライアント端末２０１内においても、復号モジュール２０８とライセンサエージェント２０９の間でｒｐｋ＿ｈａｓｈ＿ｌｉｓｔを用いた処理を行う。復号モジュール２０８は、公開鍵のハッシュ値ｒｐｋ＿ｈａｓｈ＿ｖａｌｕｅをライセンサエージェン

ト２０９に転送し、ライセンサエージェント２０９は、そのハッシュ値を検証する。そして、ライセンスのリスト内に該当する値が存在すれば、ライセンスを復号モジュール２０８に転送し、リスト内に該当する値が存在しない場合は、ライセンスを転送しない。

【００５７】

このような検証処理を行うことで、悪意のある利用者が作成した復号モジュールにライセンスを渡さないようにすることができる。

次に、１つ以上のグループに所属している利用者に対して配信すべきライセンスを自動的に決定する処理について説明する。

【００５８】

ライセンス配信サーバ２０４は、コンテンツまたはコンテンツ集合に対応して、コンテンツへのアクセスが許可されるユーザまたはユーザグループと、それぞれについて許可するアクセス形態および許諾条件を記述したアクセス制御リスト（ＡＣＬ）を、データベースに登録しておく。クライアント端末２０１上でアクセス要求が発生するたびに、要求情報がクライアント端末２０１からライセンス配信サーバ２０４に送られ、ライセンス配信サーバ２０４が応答としてライセンスを配信する。

【００５９】

このとき、ライセンス配信サーバ２０４は、ユーザまたはユーザグループによるアクセスの可否を判定した上で、コンテンツに対応するＡＣＬから個別ライセンスを生成する。具体的には、要求者が属するグループのＡＣＬエントリと要求者に対するＡＣＬエントリから、要求者用の許諾条件を生成し、個別ライセンスを生成する。個別ライセンスの生成手順は、以下の通りである。

１．ＡＣＬエントリの取得

データベースに登録された各ＡＣＬエントリのＡＣＬＥｎｔｒｙ構造（図１１）には、ユーザＩＤおよびグループＩＤが含まれている。そこで、要求されたコンテンツ識別子（ｃｏｎｔｅｎｔ＿ｉｄ）に対応する複数のＡＣＬエントリのうち、所定のＡＰＩ（Application Program Interface）を実装したクラスのｃｈｅｃｋＰｒｉｎｃｉｐａｌメソッドにより得られたユーザＩＤおよびグループＩＤを有するＡＣＬエントリを取得する。ｃｈｅｃｋＰｒｉｎｃｉｐａｌメソッドは、利用者のユーザ認証情報を元に、利用者管理サーバ２０３から利用者のユーザ情報およびグループ情報を取得するメソッドである。

２．ＡＣＬエントリの有効性の判断

取得したＡＣＬエントリに対して、以下の（１）～（７）のいずれかの条件を満たした場合に、そのＡＣＬエントリを無効とする。取得したすべてのＡＣＬエントリ無効であった場合は、要求を拒否して終了する。ただし、条件（２）を満たした場合は、直ちに要求を拒否して終了する。

（１）Ａｃｍ構造に含まれる許諾保持期限（ｋｅｐｔ＿ｌｉｍｉｔ）、許諾開始日時（ｓｔａｒｔ＿ｔｉｍｅ）（図１９）が無効。

（２）Ａｃｍ構造に含まれる優先的拒否フラグ（ｄｅｎｙフラグ）（図１８のｂｉｔ７）がオン。

（３）Ａｃｍ構造に含まれる権利数（図１９）が０（ｒｉｇｈｔｓ＿ｃｏｕｎｔ＝＝０）

（４）Ａｃｍ構造に含まれるコンテンツ操作許諾可能数（図１７）が０（ｏｐｅｒａｔｉｏｎ＿ｃｏｕｎｔ＝＝０）

（５）Ｏｐｅｎ時の証明書のサブジェクトがＡｃｍ構造に含まれる許諾サブジェクトドメインリスト（ｓｕｂｊｅｃｔ＿ｌｉｓｔ）（図１９）に該当しない。

（６）Ｇｅｔ＿Ｌｉｃｅｎｓｅで要求された操作（ｏｐｅｒａｔｉｏｎ）がＡＣＬＥｎｔｒｙ構造のｏｐｅｒａｔｉｏｎ（図１１）に合っていない。Ｇｅｔ＿Ｌｉｃｅｎｓｅは、クライアント端末２０１からライセンス配信サーバ２０４に送信されるライセンス取得要求に対応する。

（７）ｃｈｅｃｋＰｒｉｎｃｉｐａｌメソッドにより得られた認証方式条件リスト（ａｕｔｈｅｎｔｉｃａｔｉｏｎ＿ｌｉｓｔ）のビットが０で、かつ、そのビットに対応するＡＣＬエントリのａｕｔｈｅｎｔｉｃａｔｉｏｎ＿ｌｉｓｔ（図１２）のビットが１になっ

ているような認証方式が、ｂｉｔ０からｂｉｔ７の中に存在する。
【００６０】
例えば、図２１の例では、ｂｉｔ１において、ｃｈｅｃｋＰｒｉｎｃｉｐａｌで得られた条件がＡＣＬエントリで設定されているａｕｔｈｅｎｔｉｃａｔｉｏｎ＿ｌｉｓｔを満たしていないため、このＡＣＬエントリは個別条件設定に使用できない。
３．ライセンス利用形態（オンライン／オフライン）の判別
（１）Ｇｅｔ＿Ｌｉｃｅｎｓｅのａｃｍの逐次ライセンス指定フラグ（ｄｙｎａｍｉｃ＿ｌｉｃｅｎｓｅフラグ）がオンの場合
上記２の処理までに残ったＡＣＬエントリの中からｄｙｎａｍｉｃ＿ｌｉｃｅｎｓｅフラグ（図１８のｂｉｔ４）がオンのもののみを残す。２の処理までに残ったすべてのＡＣＬエントリのｄｙｎａｍｉｃ＿ｌｉｃｅｎｓｅフラグがオフの場合、要求を拒否する。この場合のｒｅｊｅｃｔ　ｃｏｄｅは８１１１ｈであり、有効なＡＣＬエントリが存在しないことを表す。
【００６１】
逐次ライセンス（オンラインライセンス）は、発行後すぐに使用するタイプのライセンスであり、使用後はクライアント端末２０１により破棄される。これに対して、オフラインライセンスは、一旦、クライアント端末２０１内に保存され、その後ライセンス配信サーバ２０４に接続しなくても使用できるタイプのライセンスである。
（２）Ｇｅｔ＿Ｌｉｃｅｎｓｅのａｃｍのｄｙｎａｍｉｃ＿ｌｉｃｅｎｓｅフラグがオフ、またはａｃｍの指定がない場合
２の処理までに残ったＡＣＬエントリの中からｄｙｎａｍｉｃ＿ｌｉｃｅｎｓｅフラグがオフのもののみを残す。２の処理２までに残ったすべてのＡＣＬエントリのｄｙｎａｍｉｃ＿ｌｉｃｅｎｓｅフラグがオンの場合、要求を拒否する。この場合のｒｅｊｅｃｔ　ｃｏｄｅも８１１１ｈである。
４．ＡＣＬエントリの選択と個別ライセンスの配信
（１）Ｇｅｔ＿Ｌｉｃｅｎｓｅでａｃｍ、ａｃｐの指定がない場合
図２２の優先順位表に従ってＡＣＬエントリを選択する。ある優先順位の選択ルールにより複数のＡＣＬエントリが選択された場合は、次の優先順位の選択ルールに従ってＡＣＬエントリを選択する。
【００６２】
実際には、コンテンツの部分コピーを許可する部分コピーライセンスにおいて部分コピー禁止フラグがオンになることはないので、部分コピーライセンスの選択時に優先順位４の選択ルールを用いることはない。また、コンテンツの保存を許可する保存ライセンスにおいて保存禁止フラグがオンになることはないので、保存ライセンスの選択時に優先順位５の選択ルールを用いることはない。さらに、コンテンツの印刷を許可する印刷ライセンスにおいて印刷禁止フラグがオンになることはないので、印刷ライセンスの選択時に優先順位６の選択ルールを用いることはない。
【００６３】
以上の選択処理により複数のＡＣＬエントリが残る場合は、データベースに登録された順番でＡＣＬエントリを選択する。
（２）Ｇｅｔ＿Ｌｉｃｅｎｓｅでａｃｍ、ａｃｐの指定がある場合
残ったＡＣＬエントリの中から、Ｇｅｔ＿Ｌｉｃｅｎｓｅで指定されたａｃｍ、ａｃｐを満たすＡＣＬエントリを選択し、それを個別ライセンスに格納し、配信する。
（２－１）ａｃｍ、ａｃｐを満足するＡＣＬエントリが複数存在する場合
図２２の優先順位表に従ってＡＣＬエントリを選択する。それでも複数のＡＣＬエントリが残る場合は、データベースに登録された順番でＡＣＬエントリを選択する。
（２－２）ａｃｍ、ａｃｐを満足するＡＣＬエントリが存在しない場合
要求を拒否して終了する。ｒｅｊｅｃｔ　ｃｏｄｅは８１１１ｈである。
【００６４】
上述の手順に従って最終的に１つのＡＣＬエントリを選択した後、そのＡＣＬエントリ

を有するライセンスを配信する。このとき、ライセンスのｍｏｖｅ＿ｃｏｕｎｔは００ｈに設定し、ｒｉｇｈｔｓ＿ｃｏｕｎｔは０１ｈに設定して配信する。ただし、ｄｙｎａｍｉｃ＿ｌｉｃｅｎｓｅフラグがオンのＡＣＬエントリが選択された場合、逐次ライセンス（ｏｐｅｒａｔｉｏｎ＿ｃｏｕｎｔ　０１ｈ、ｍｏｖｅ＿ｃｏｕｎｔ　００ｈ、ｒｉｇｈｔｓ＿ｃｏｕｎｔ　０１ｈ）を配信する。

５．サーバ側のデータベースの減算処理

ライセンス配信サーバ２０４は、上記４の処理で選択したＡＣＬエントリのｒｉｇｈｔｓ＿ｃｏｕｎｔを１だけ減算する。

【００６５】

図２３は、このような個別ライセンス選択処理のフローチャートである。ライセンス配信サーバ２０４は、まず上記１の処理により、利用者管理サーバ２０３から要求者が所属するグループのグループＩＤリストを取得し（ステップ２３０１）、その結果を判定する（ステップ２３０２）。所属グループが２つ以上であれば、次に上記２および３の処理により、ＡＣＬエントリを選択し（ステップ２３０３）、その結果を判定する（ステップ２３０４）。

【００６６】

ここで、複数のＡＣＬエントリが残った場合は、上記４の処理により、ＡＣＬエントリを１つだけ選択し、ライセンスを配信する（ステップ２３０５）。そして、上記５の処理により、データベースの権利数を１だけ減算する（ステップ２３０６）。

【００６７】

ステップ２３０２において所属グループが１つの場合、および、ステップ２３０４においてＡＣＬエントリが１つだけ残った場合は、直ちにライセンスを配信し（ステップ２３０５）、ステップ２３０６の処理を行う。また、ステップ２３０２において所属グループが０の場合は、要求者に要求破棄を通知する（ステップ２３０８）。

【００６８】

図２４は、図２３のステップ２３０３におけるＡＣＬエントリ選択処理のフローチャートである。ライセンス配信サーバ２０４は、まず上記２の処理により、ＡＣＬエントリの有効性を判断し（ステップ２４０１）、その結果を判定する（ステップ２４０２）。

【００６９】

ＡＣＬエントリが有効であれば、次に上記３の処理により、そのＡＣＬエントリが要求条件を満たしているか否かを判別する（ステップ２４０３および２４０４）。要求条件を満たしているＡＣＬエントリが存在すれば、それを選択結果として図２３の処理に復帰する。要求条件を満たしているＡＣＬエントリが存在しなければ、要求者に要求破棄を通知する（ステップ２４０５）。

【００７０】

このような個別ライセンス選択処理によれば、１つ以上のグループに所属している利用者に対して配信すべきライセンスを自動的に決定することができる。

次に、ライセンスをクライアント端末にダウンロードする際のアクセス可否を判定する制御と、ダウンロードされたライセンスを別のクライアント端末に安全に渡す制御について説明する。この制御では、公開鍵証明書（Ｘ．５０９証明書）のサブジェクトのリストを用いて許諾・拒否ドメインを限定する。

【００７１】

公開鍵証明書のサブジェクトとは、証明書主体者を識別するための名前であり、通常は、Ｘ．５００名前システムで表記される。例えば、ＴＲＵＳＴ株式会社のネットワーク事業部に所属するｈａｎａという人は、以下のように表記される。

｛Ｃｏｕｎｔｒｙ＝ＪＰ，Ｏｒｇａｎｉｚａｔｉｏｎ＝ＴＲＵＳＴ　Ｃｏｒｐ．，ＯｒｇａｎｉｚａｔｉｏｎＵｎｉｔ＝Ｎｅｔｗｏｒｋ，ＣｏｍｍｏｎＮａｍｅ＝ｈａｎａ｝

このように１つのエントリを表記する形式は、Ｘ．５００ディレクトリシステムで定義

されており、ＤＮ（Distinguished Name：識別名）と呼ばれている。また、ＤＮの一部分はＲＤＮ（Relative Distinguished Name ：相対識別名）と呼ばれている。ＲＤＮは、Ｘ．５０１で規定された相対識別名であり、ＤＮは、Ｘ．５０１で規定された絶対識別名である。ｈａｎａのＲＤＮは、例えば、以下のようになる。

｛Ｃｏｕｎｔｒｙ＝ＪＰ，Ｏｒｇａｎｉｚａｔｉｏｎ＝ＴＲＵＳＴ　Ｃｏｒｐ．｝，
｛Ｏｒｇａｎｉｚａｔｉｏｎ＝ＴＲＵＳＴ　Ｃｏｒｐ．｝，
｛ＣｏｍｍｏｎＮａｍｅ＝ｈａｎａ｝

ここでは、ライセンスを配信、移動する範囲を、クライアント端末が保有する公開鍵証明書（メディアクラス公開鍵証明書）のＤＮで制御する。そのために、ライセンスの許諾条件の１つとして、許諾したいＤＮおよびＲＤＮのリストをＡＣＬエントリの許諾サブジェクトドメインリスト（ｓｕｂｊｅｃｔ＿ｌｉｓｔ）（図１９）に設定しておく。

【００７２】

そして、公開鍵証明書のＤＮに含まれるＲＤＮを上位から順番に取り出して、許諾サブジェクトドメインリストの各エントリ（ＲＤＮ）と比較する。公開鍵証明書のサブジェクトの上位ＲＤＮとリストのある１つのエントリとが一致すれば、アクセスを許諾する。これにより、許諾サブジェクトドメインリスト内のＲＤＮに一致するクライアント端末にしか、ライセンスを配信しないような制御が可能になる。

【００７３】

例えば、図２５に示すように、ＴＲＵＳＴ株式会社２５０１とＩＴ株式会社２５０２があり、ＴＲＵＳＴ株式会社２５０１には、ネットワーク事業部２５１１とソフトウェア事業部２５１２があるとする。このとき、ある保護情報をＴＲＵＳＴ株式会社２５０１のネットワーク事業部２５１１とＩＴ株式会社２５０２で共有したい場合、許諾サブジェクトドメインリストに以下のような情報を設定することで、それ以外の組織へライセンスを配信しないようにできる。ただし、ＲＤＮは、最上位ＲＤＮから順番に指定される。

｛Ｃｏｕｎｔｒｙ＝ＪＰ，Ｏｒｇａｎｉｚａｔｉｏｎ＝ＴＲＵＳＴ　Ｃｏｒｐ．，ＯｒｇａｎｉｚａｔｉｏｎＵｎｉｔ＝Ｎｅｔｗｏｒｋ｝，
｛Ｃｏｕｎｔｒｙ＝ＪＰ，Ｏｒｇａｎｉｚａｔｉｏｎ＝ＩＴ　Ｉｎｃ．｝

この許諾サブジェクトドメインリストに従って、ライセンス配信サーバ２０４は、ＴＲＵＳＴ株式会社２５０１のネットワーク事業部２５１１とＩＴ株式会社２５０２にライセンスを配信し、ＴＲＵＳＴ株式会社２５０１のソフトウェア事業部２５１２にはライセンスを配信しない。

【００７４】

許諾サブジェクトドメインリストは、許諾条件の１つとしてライセンスに格納されて配信されるので、ライセンスを受信したクライアント端末のライセンサエージェントは、そのリストを解釈し、リストに示された範囲内でライセンスをコピー、移動することができる。

【００７５】

したがって、図２６に示すように、ライセンスがＩＴ株式会社２５０２に配信された後、ＩＴ株式会社２５０２のライセンサエージェントは、上記許諾サブジェクトドメインリストに従って、ＴＲＵＳＴ株式会社２５０１のネットワーク事業部２５１１にライセンスをコピー、移動する。しかし、ＴＲＵＳＴ株式会社２５０１のソフトウェア事業部２５１２にライセンスをコピー、移動することはない。

【００７６】

次に、ＩＣ（Integrated Circuit）カードを使って、配信されたライセンスを別のクライアント端末に安全にコピー、移動する方法について説明する。この方法では、ライセンスにＤＮを入れてクライアント端末に配信し、クライアントモジュールがそのＤＮとＩＣ

カードのＤＮが一致するか否かを確認する。

【００７７】

この場合、図２７に示すように、クライアントモジュール２０６内に、ＩＣカード認証連携モジュール２７０１を設ける。ＩＣカード認証連携モジュール２７０１は、クライアントモジュール２０６に対して、ＩＣカード２７０２により利用者の認証を行うモジュールである。ＩＣカード２７０２にはＩＣカード利用者の証明書が格納されており、ＩＣカード２７０２はクライアント端末２０１のスロットに挿入されるものとする。クライアントモジュール２０６は、認証されたＩＣカード２７０２に対してのみ、ライセンスをコピー、移動する。

【００７８】

図２８は、ＩＣカード認証連携モジュール２７０１によるＩＣカード認証シーケンスを示している。このシーケンスでは、毎回乱数を生成し、それを署名し、署名検証を行うことで認証が行われる。

【００７９】

ＩＣカード認証連携モジュール２７０１は、ライセンス利用時にＩＣカード２７０２に対して状態を問い合わせて、クライアント端末２０１にＩＣカード２７０２が接続されているか否かを確認する。ＩＣカードが抜かれている場合、利用者に対してＩＣカードの挿入とＰＩＮ（Personal Identification Number）コードの入力を要求する。これを受けて、利用者は、クライアント端末２０１にＩＣカード２７０２を挿入し、ＰＩＮコードを入力する（手順２８０１）。

【００８０】

次に、ＩＣカード認証連携モジュール２７０１は、乱数を生成し、ＩＣカード２７０２の機能であるセキュアセッションを使用して乱数をＩＣカード２７０２に送信する（手順２８０２）。

【００８１】

ＩＣカード２７０２は、保有する証明書に対する暗号鍵を使って、受信した乱数にデジタル署名を施す（手順２８０３）。そして、そのデジタル署名と証明書をセキュアセッションでＩＣカード認証連携モジュール２７０１に送信する。

【００８２】

ＩＣカード認証連携モジュール２７０１は、ＩＣカード２７０２の証明書の有効性を検証し（手順２８０４）、証明書のＤＮが現在クライアント端末２０１にログインしているアカウントと同一であるか否か（証明書のＤＮと配信されたライセンスのＤＮが一致するか否か）をチェックし（手順２８０５）、ＩＣカード２７０２から受け取ったデジタル署名を、証明書を用いて検証する（手順２８０６）。

【００８３】

ＤＮチェックのためには、ＩＣカード２７０２の証明書のＤＮとクライアント端末２０１のアカウントをマップするデータが必要となるが、ＩＣカード認証連携モジュール２７０１はこのようなデータを保持しているものとする。

【００８４】

クライアント端末２０１にＩＣカード２７０２が接続されたままの状態の場合は、利用者にＰＩＮコードを入力させる必要はなく、手順２８０２以降のシーケンスに従ってＩＣカード２７０２の認証が行われる。

【００８５】

図２９は、このようなＩＣカード認証処理のフローチャートである。ＩＣカード認証連携モジュール２７０１は、まず、乱数を生成し（ステップ２９０１）、それをＩＣカード２７０２に送信する（ステップ２９０２）。次に、ＩＣカード２７０２からデジタル署名と証明書を受信し（ステップ２９０３）、証明書の有効性検証を行って（ステップ２９０４）、その結果を判定する（ステップ２９０５）。

【００８６】

結果がＯＫであれば、次に、証明書のＤＮチェックを行って（ステップ２９０６）、そ

の結果を判定する（ステップ２９０７）。結果がＯＫであれば、次に、デジタル署名の検証を行って（ステップ２９０８）、その結果を判定する（ステップ２９０９）。ステップ２９０５、２９０７、および２９０９において結果がＮＧであれば、エラー処理を行う（ステップ２９１０、２０１１、および２９１２）。

【００８７】

なお、この例ではＩＣカードを用いてライセンスをコピー、移動しているが、そのほかにもコンピュータ読み取り可能な任意の可搬記録媒体を利用することができる。

次に、クライアント端末上でログの改ざん等が行われるという問題に対処するために、ライセンス配信サーバがクライアント端末におけるコンテンツの表示、印刷、保存、部分コピー、転送、メール添付等の操作ごとにログをとる方法について説明する。

【００８８】

この方法では、ライセンス内にｏｐｅｒａｔｉｏｎというコンテンツの操作種別を表すフィールド（図１１）を設けておく。利用者は、現在どの操作がしたいかによって、ライセンス配信サーバに希望する操作種別のライセンスを要求する。そして、ライセンス配信サーバは、どの操作種別のライセンスをクライアント端末に配信したかを示すログデータを保存することにより、クライアント端末のコンテンツに対する操作を特定する。

【００８９】

このようなログ管理によれば、ログデータがサーバ側で作成・管理されるので、利用者による改ざん等が行われる可能性が非常に低くなる。

次に、クライアント端末が複数の暗号化コンテンツを利用するとき、それらのコンテンツに対するライセンスを一度に取得する方法について説明する。この方法では、ライセンス内に複数のコンテンツに対応する許諾条件・復号鍵を格納して、それらのコンテンツを制御する。また、１つのコンテンツに対する許諾条件を表すＡＣＬエントリのフィールドを複数個格納できるフィールド（図１０）をライセンス内に設けることにより、複数個の許諾条件を１回で配信できるようにする。

【００９０】

図３０は、ライセンス内のコンテンツ復号情報（ｄｅｃｏｄｅ＿ｉｎｆｏｒｍａｔｉｏｎ）のデータであるＤｅｃｏｄｅＩｎｆｏｒｍａｔｉｏｎ構造（図９）を示しており、図３１は、ＤｅｃｏｄｅＩｎｆｏｒｍａｔｉｏｎ構造内の暗号化コンテンツエレメント－復号鍵対応リスト（ｅｌｅｍｅｎｔ－ｋｅｙ－ｍａｐ）のデータであるＥｌｅｍｅｎｔＫｅｙＭａｐ型を示している。

【００９１】

暗号化コンテンツは、一般に、図３２のような形式で配信され、Ｎ個の異なるエレメント（コンテンツ）を格納することができる。図３３は、図３２のヘッダ（Ｃｏｎｔｅｎｔ Ｈｅａｄｅｒ）の形式を示しており、図３４は、図３３のコンテンツ情報（Ｃｏｎｔｅｎｔ Ｉｎｆｏｒｍａｔｉｏｎ）を示しており、図３５は、図３３の各エレメント情報（Ｅｌｅｍｅｎｔ Ｉｎｆｏｒｍａｔｉｏｎ）を示している。図３０のＤｅｃｏｄｅＩｎｆｏｒｍａｔｉｏｎ構造を用いることで、図３２の複数のエレメント（コンテンツ）に対応する復号鍵をライセンス内に格納することができる。

【００９２】

また、ＡＣＬエントリのデータであるＡＣＬＥｎｔｒｙ構造には、許諾コンテンツエレメント番号リスト（ｅｌｅｍｅｎｔ＿ｌｉｓｔ）（図１３）のフィールドがあり、そのＡＣＬエントリの許諾条件で利用できるエレメントのエレメント番号が格納されている。したがって、図１０のＡｃｌ構造を用いることで、複数のエレメントに対応する許諾条件をライセンス内に格納することができる。

【００９３】

次に、ライセンスのＡＣＬエントリの中に認証方式を記述するためのフィールドを設けて、過去において利用者を認証済みの認証方式と、そのフィールドに記述された認証方式とを比較することにより、アクセスを制御する方法について説明する。この方法では、比較すべき２つの認証方式の論理演算を行って、演算結果をアクセス条件として用いる。

【００９４】
ライセンス配信サーバ２０４は、利用者がどのような認証方式で認証されたかを利用者管理サーバ２０３に問い合わせて、認証方式条件を取得する。そして、取得した条件と、クライアント端末が要求したライセンスに格納されている認証方式条件リスト（ａｕｔｈｅｎｔｉｃａｔｉｏｎ＿ｌｉｓｔ）（図１２）を比較し、ライセンスの配信可否を決定する。ａｕｔｈｅｎｔｉｃａｔｉｏｎ＿ｌｉｓｔには、ライセンスの登録時に必要な認証方式が設定されている。
【００９５】
具体的には、ライセンス内のａｕｔｈｅｎｔｉｃａｔｉｏｎ＿ｌｉｓｔは、各ビットが各認証方式にマップされているビット列のデータであり、図３６に示すような８つのビットから構成されている。必要な認証方式に対応するビットはオン（論理１）に設定される。
【００９６】
ライセンス配信サーバ２０４は、利用者管理サーバ２０３から取得した認証方式の情報を図３６の形式のデータにマップするとき、利用者が各認証方式による認証を正常に終了していれば、対応するビットをオンにする。例えば、利用者が既にＩＤ／パスワード方式とサイン方式で認証されている場合、００００１００１という値が生成される。
【００９７】
生成されたデータのビットが０で、かつ、そのビットに対応するａｕｔｈｅｎｔｉｃａｔｉｏｎ＿ｌｉｓｔのビットが１になっているような認証方式が存在する場合に限り、ライセンス配信サーバ２０４はライセンスを配信しない。
【００９８】
この制御を命題論理で説明すると、ａｕｔｈｅｎｔｉｃａｔｉｏｎ＿ｌｉｓｔのビットをＡとし、マップされたデータのビットをＢとして、各ビットに対して図３７に示すような論理演算Ａ⇒Ｂを行った結果、１つでも０のビットが存在すれば、ライセンス配信を拒否する処理を行う。
【００９９】
図３８の例では、ｂｉｔ１において、利用者管理サーバ２０３から取得した条件がライセンス内のａｕｔｈｅｎｔｉｃａｔｉｏｎ＿ｌｉｓｔを満たしていないため、そのライセンスはクライアント端末２０１に配信されない。このような制御によれば、ＤＲＭによるコンテンツ保護システムで認証されていないクライアント端末へのライセンス配信を防止することができる。
【０１００】
次に、クライアント端末が、同一コンテンツに対して複数の許諾条件を格納しているライセンスを受信した場合、登録者の意図に従った方法でその中から１つの許諾条件を選択してライセンスを利用する方法について説明する。
【０１０１】
ライセンス内にはｌｉｃｅｎｓｅ＿ｓｃｒｉｐｔ＿ｓｐｅｃというフィールド（図８）があり、ＡＣＬＥｎｔｒｙ構造にはｒｉｇｈｔｓ＿ｓｃｒｉｐｔというフィールド（図１１）がある。これらのフィールドのデータには、図３９に示すＲｉｇｈｔｓＳｃｒｉｐｔＳｐｅｃ構造が含まれている。このＲｉｇｈｔｓＳｃｒｉｐｔＳｐｅｃ構造に記述された識別子（ｓｃｒｉｐｔ＿ｉｄ）には、許諾条件選択処理が対応付けられている。
【０１０２】
許諾条件選択処理の例としては、前述した図２２の優先順位表に基づくＡＣＬエントリ選択処理が挙げられる。そのほかにも、図４０に示すように、許諾条件の優先順位を入れ替えた優先順位表に対して、ｓｃｒｉｐｔ＿ｉｄを付与することができる。さらに、図４１に示すように、選択ルールを変更した優先順位表に対しても、ｓｃｒｉｐｔ＿ｉｄを付与することができる。このように、ＲｉｇｈｔｓＳｃｒｉｐｔＳｐｅｃ構造は、複数のＡＣＬエントリのうちの１つを選択する処理を指定している。
【０１０３】

また、この優先順位表に記述された選択ルールは、ライセンス配信システムを利用する人がだれでも見ることができるように、Ｗｅｂ等で公開してもよい。これにより、登録者はどのように許諾条件が選択されるかを把握することができる。

【０１０４】

図４２は、クライアントモジュール２０６が、受信したライセンスのＲｉｇｈｔｓＳｃｒｉｐｔＳｐｅｃ構造を利用してＡＣＬエントリを選択する処理のフローチャートである。クライアントモジュール２０６は、まず、ライセンス内にＡＣＬエントリが複数存在するか否かをチェックする（ステップ４２０１）。ＡＣＬエントリが１つしか存在しなければ、そのＡＣＬエントリが選択される。

【０１０５】

ＡＣＬエントリが複数存在すれば、各ＡＣＬエントリのｒｉｇｈｔｓ＿ｓｃｒｉｐｔのＲｉｇｈｔｓＳｃｒｉｐｔＳｐｅｃ構造をチェックし（ステップ４２０２）、それらが同じか否かを判定する（ステップ４２０３）。

【０１０６】

それらのＲｉｇｈｔｓＳｃｒｉｐｔＳｐｅｃ構造が同じであれば、そのｓｃｒｉｐｔ＿ｉｄに対応する許諾条件選択処理により１つのＡＣＬエントリを選択する（ステップ４２０４）。それらのＲｉｇｈｔｓＳｃｒｉｐｔＳｐｅｃ構造の中に異なるものが存在すれば、ｌｉｃｅｎｓｅ＿ｓｃｒｉｐｔ＿ｓｐｅｃのＲｉｇｈｔｓＳｃｒｉｐｔＳｐｅｃ構造のｓｃｒｉｐｔ＿ｉｄに対応する許諾条件選択処理により１つのＡＣＬエントリを選択する（ステップ４２０５）。

【０１０７】

次に、コンテンツ編集時にデータが盗まれる問題に対する対策について説明する。利用者がコンテンツを編集するときに、コンテンツの一部をコピーしてクリップボードに入れるとき、クライアントモジュール２０６がコピー部分のデータを暗号化してクリップボードに入れる。そして、許諾された者がペースト操作を行った場合にのみ、その部分を復号して貼り付ける処理を行う。これにより、保護文書に対する編集操作（コピー・ペースト）を許諾された者だけに限定する制御を強制的に実現する。

【０１０８】

本実施形態のライセンスでは、さらに以下のような制御を実現するための情報も含まれている。

（１）ユーザやグループへの優先的拒否制御を拒否期間や拒否ドメイン限定で実施する。

【０１０９】

ライセンス発行期間を許諾開始日時から許諾保持期限までとして発行期間を制御し、ライセンス発行期間内で、発行先のユーザおよびユーザが所属するグループにどのような許諾が与えられていても、ライセンスの発行を優先的に拒否する。

【０１１０】

図１９に示したように、ライセンス内に、ｋｅｐｔ＿ｐｅｒｉｏｄ、ｋｅｐｔ＿ｌｉｍｉｔ、およびｓｔａｒｔ＿ｔｉｍｅのフィールドを設ける。ｋｅｐｔ＿ｐｅｒｉｏｄには許諾保持期間が格納され、ｋｅｐｔ＿ｌｉｍｉｔには許諾保持期限が格納され、ｓｔａｒｔ＿ｔｉｍｅにはライセンスの配信を開始する日時（許諾開始日時）が格納される。ライセンス配信サーバ２０４は、これらの情報と図１８のｄｅｎｙフラグとを連動させることにより、所定期間、アクセス制御対象の利用者によるコンテンツ利用可否を制御する。

【０１１１】

ある利用者に対するＡＣＬエントリにおいて、ｓｔａｒｔ＿ｔｉｍｅおよびｋｅｐｔ＿ｌｉｍｉｔが設定され、ｄｅｎｙフラグがオンに設定されている場合、図４３に示すように、ｓｔａｒｔ＿ｔｉｍｅからｋｅｐｔ＿ｌｉｍｉｔまでの期間は利用者に対してライセンスが配信されない。

（２）オフラインライセンスを最初に利用するときに、利用者がパスワードを設定し、そのパスワードの入力可能期間をコンテンツ登録者が指定できるようにする。

【０１１２】

オフラインライセンスをパスワード認証を使って利用する場合、ライセンス内に、オフライン利用時に使用するパスワードの最低の長さを格納するｐａｓｓｗｏｒｄ＿ｍｉｎ＿ｌｅｎというフィールド（図１２）と、ライセンスがクライアント端末に到着してからパスワードをクライアント端末に入力するまでの時間を格納するｐｗ＿ｉｎｐｕｔ＿ｐｅｒｉｏｄというフィールド（図１３）を設ける。

【０１１３】

利用者は、ｐｗ＿ｉｎｐｕｔ＿ｐｅｒｉｏｄに設定された時間内に、ｐａｓｓｗｏｒｄ＿ｍｉｎ＿ｌｅｎに設定された長さ以上のパスワードを入力し、クライアントモジュール２０６は、そのパスワードを保存・設定する。以後、オフラインでライセンスを利用するときに、利用者は設定されたパスワードを使用する。

（３）ＤＲＭ技術と重畳表示／印刷の連携方式

現状のＤＲＭによる保護方法では、例えば、悪意のある利用者が保護文書を表示している間に、その表示画面をデジタルカメラで撮影し、撮影データを第三者に渡すことが考えられる。また、印刷権限があるライセンスを正当に取得し、印刷した保護文書をコピー機でコピーして、第三者に渡すことも考えられる。

【０１１４】

そこで、ライセンス内に、ライセンス発行日時、ライセンス発行主体や発行主体が所属するグループ等の属性情報等といった重畳情報を格納しておく。重畳情報が格納されたライセンスを取得したクライアントモジュール２０６は、コンテンツの表示または印刷時に、強制的に重畳情報を表示または印刷する。これにより、誰がいつコンテンツを表示または印刷したかという情報がコンテンツ自身に付加されるため、コンテンツの配布経路を特定しやくなる。

【０１１５】

ところで、図２のクライアント端末２０１、利用者管理サーバ２０３、ライセンス配信サーバ２０４、およびコンテンツサーバ２０５は、例えば、図４４に示すような情報処理装置（コンピュータ）を用いて構成される。図４４の情報処理装置は、ＣＰＵ（中央処理装置）４４０１、メモリ４４０２、入力装置４４０３、出力装置４４０４、外部記憶装置４４０５、媒体駆動装置４４０６、ネットワーク接続装置４４０７を備え、それらはバス４４０８により互いに接続されている。

【０１１６】

メモリ４４０２は、例えば、ＲＯＭ（read only memory）、ＲＡＭ（random access memory）等を含み、処理に用いられるプログラムおよびデータを格納する。ＣＰＵ４４０１は、メモリ４４０２を利用してプログラムを実行することにより、必要な処理を行う。

【０１１７】

図４の記憶装置４０４および４０５は、メモリ４４０２または外部記憶装置４４０５に対応する。図２のクライアントモジュール２０６、復号モジュール２０８、ライセンサエージェント２０９、図４の活性化キー生成ツール４０１、クライアント活性化モジュール４０２、認証局モジュール４０３、および図２７のＩＣカード認証連携モジュール２７０１は、メモリ４４０２に格納されたプログラムまたはその機能に対応する。

【０１１８】

入力装置４４０３は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、コンテンツ登録者、管理者、利用者等のオペレータからの指示や情報の入力に用いられる。出力装置４４０４は、例えば、ディスプレイ、プリンタ、スピーカ等であり、オペレータへの問い合わせや処理結果等の出力に用いられる。

【０１１９】

外部記憶装置４４０５は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置、テープ装置等である。情報処理装置は、この外部記憶装置４４０５に、上記プログラムおよびデータを格納しておき、必要に応じて、それらをメモリ４４０２にロードして使用する。また、外部記憶装置４４０５は、利用者管理サーバ２０３、ライセンス配信サーバ２０４、およびコンテンツサーバ２０５のデータベースとしても使用される。

【０１２０】
媒体駆動装置４４０６は、可搬記録媒体４４０９を駆動し、その記録内容にアクセスする。可搬記録媒体４４０９は、メモリカード、フレキシブルディスク、ＣＤ－ＲＯＭ（compact disk read only memory ）、光ディスク、光磁気ディスク等の任意のコンピュータ読み取り可能な記録媒体である。オペレータは、この可搬記録媒体４４０９に上記プログラムおよびデータを格納しておき、必要に応じて、それらをメモリ４４０２にロードして使用する。
【０１２１】
ネットワーク接続装置４４０７は、ＬＡＮ（local area network）やインターネット等の任意の通信ネットワークに接続され、通信に伴うデータ変換を行う。情報処理装置は、必要に応じて、上記プログラムおよびデータを外部の装置からネットワーク接続装置４４０７を介して受け取り、それらをメモリ４４０２にロードして使用する。
【０１２２】
図４５は、図４４の情報処理装置にプログラムおよびデータを供給することのできるコンピュータ読み取り可能な記録媒体を示している。可搬記録媒体４４０９やサーバ４５０１のデータベース４５１１に格納されたプログラムおよびデータは、情報処理装置４５０２のメモリ４４０２にロードされる。サーバ４５０１は、そのプログラムおよびデータを搬送する搬送信号を生成し、ネットワーク上の任意の伝送媒体を介して情報処理装置４５０２に送信する。ＣＰＵ４４０１は、そのデータを用いてそのプログラムを実行し、必要な処理を行う。
【０１２３】
（付記１）　暗号化されたデジタルコンテンツを復号するためのライセンスデータを公開鍵基盤を利用して取得するプログラムである端末モジュールを、利用者端末に配信する情報処理装置であって、
暗号鍵を格納する格納手段と、
前記公開鍵基盤に基づく暗号化通信に必要な公開鍵証明書および該公開鍵証明書の公開鍵に対する秘密鍵の情報を、前記暗号鍵を用いて暗号化して、暗号化情報を生成する生成手段と、
前記暗号化情報を復号する復号鍵を含み、前記利用者端末上で起動された後に該暗号化情報を復号して、前記公開鍵証明書および秘密鍵の情報を取得する端末モジュールと、該暗号化情報とを前記利用者端末に送信する送信手段と
を備えることを特徴とする情報処理装置。
【０１２４】
（付記２）　利用者端末からデジタルコンテンツに対するアクセス要求を受信し、該デジタルコンテンツにアクセスするためのライセンスデータを応答として該利用者端末に配信する情報処理装置であって、
デジタルコンテンツに対応付けて、アクセスが許可される利用者、許可されるアクセス形態、および許諾条件を記述した複数のアクセス制御リストを格納する格納手段と、
前記複数のアクセス制御リストの中から、前記アクセス要求に含まれるコンテンツ識別子に対応し、かつ、該アクセス要求を送信した要求者の利用者識別子に対応するアクセス制御リストを取得し、得られたアクセス制御リストが複数存在する場合、得られた複数のアクセス制御リストの中から１つのアクセス制御リストを選択し、選択したアクセス制御リストに基づく個別ライセンスデータを生成する生成手段と、
前記個別ライセンスデータを前記利用者端末に送信する送信手段と
を備えることを特徴とする情報処理装置。
【０１２５】
（付記３）　デジタルコンテンツに対するアクセス要求をライセンス配信装置に送信し、該デジタルコンテンツにアクセスするためのライセンスデータを応答として該ライセンス配信装置から受信する情報処理装置であって、
前記デジタルコンテンツに対して許可されるアクセス形態および許諾条件を記述した複

数のアクセス制御リストと選択処理を指定する情報とを含み、前記ライセンス配信装置から受信した前記ライセンスデータを格納する格納手段と、
前記ライセンスデータにより指定された選択処理を実行して、前記複数のアクセス制御リストの中から１つのアクセス制御リストを選択する選択手段と
を備えることを特徴とする情報処理装置。
【０１２６】
（付記４） 暗号化されたデジタルコンテンツを復号するためのライセンスデータを公開鍵基盤を利用して取得するプログラムである端末モジュールを、利用者端末に配信するコンピュータのためのプログラムであって、
前記公開鍵基盤に基づく暗号化通信に必要な公開鍵証明書および該公開鍵証明書の公開鍵に対する秘密鍵の情報を、格納手段に格納された暗号鍵を用いて暗号化して、暗号化情報を生成し、
前記暗号化情報を復号する復号鍵を含み、前記利用者端末上で起動された後に該暗号化情報を復号して、前記公開鍵証明書および秘密鍵の情報を取得する端末モジュールと、該暗号化情報とを前記利用者端末に送信する
処理を前記コンピュータに実行させることを特徴とするプログラム。
【０１２７】
（付記５） 暗号化されたデジタルコンテンツを復号するためのライセンスデータを、ライセンス配信装置から公開鍵基盤を利用して取得するコンピュータのためのプログラムであって、
格納手段に格納された暗号化情報を前記プログラムに含まれる復号鍵を用いて復号して、前記公開鍵基盤に基づく暗号化通信に必要な公開鍵証明書および該公開鍵証明書の公開鍵に対する秘密鍵の情報を取得し、
前記公開鍵証明書および秘密鍵の情報を用いて暗号化通信を行うことで、前記ライセンス配信装置から前記ライセンスデータを取得する
処理を前記コンピュータに実行させることを特徴とするプログラム。
【０１２８】
（付記６） 利用者端末からデジタルコンテンツに対するアクセス要求を受信し、該デジタルコンテンツにアクセスするためのライセンスデータを応答として該利用者端末に配信するコンピュータのためのプログラムであって、
デジタルコンテンツに対応付けて、アクセスが許可される利用者、許可されるアクセス形態、および許諾条件を記述した、格納手段に格納された複数のアクセス制御リストの中から、前記アクセス要求に含まれるコンテンツ識別子に対応し、かつ、該アクセス要求を送信した要求者の利用者識別子に対応するアクセス制御リストを取得し、
得られたアクセス制御リストが複数存在する場合、得られた複数のアクセス制御リストの中から１つのアクセス制御リストを選択し、
選択したアクセス制御リストに基づく個別ライセンスデータを生成する
処理を前記コンピュータに実行させることを特徴とするプログラム。
【０１２９】
（付記７） 公開鍵証明書の識別名の一部分を表す相対識別名であって、前記選択したアクセス制御リストの許諾ドメインサブジェクトリストに記述された該相対識別名と、前記利用者端末が保有する公開鍵証明書の識別名を比較し、該利用者端末が保有する公開鍵証明書の識別名の一部分と該相対識別名が一致したとき、前記個別ライセンスデータを該利用者端末に配信する処理を、前記コンピュータにさらに実行させることを特徴とする付記６記載のプログラム。
【０１３０】
（付記８） 前記プログラムは、前記個別ライセンスデータに公開鍵証明書の識別名を記述して前記利用者端末に配信する処理を前記コンピュータにさらに実行させ、該利用者端末は、該個別ライセンスデータに記述された識別名と可搬記録媒体に格納された公開鍵証明書の識別名が一致したとき、該可搬記録媒体に該個別ライセンスデータを格納するこ

とを特徴とする付記６記載のプログラム。

【０１３１】

（付記９） 前記個別ライセンスデータを前記利用者端末に配信したとき、該個別ライセンスデータにより該利用者端末に対して許可されるコンテンツ操作種別を示すログデータを保存する処理を、前記コンピュータにさらに実行させることを特徴とする付記６記載のプログラム。

【０１３２】

（付記１０） 前記個別ライセンスデータは、複数のデジタルコンテンツのそれぞれにアクセスするための複数の許諾条件および複数の復号鍵を含むことを特徴とする付記６記載のプログラム。

【０１３３】

（付記１１） 前記個別ライセンスデータに記述された利用者の認証方式と、前記要求者を既に認証済みの認証方式とを比較し、該個別ライセンスデータに記述された認証方式が該認証済みの認証方式に該当しない場合に該個別ライセンスデータを前記利用者端末に配信しない処理を、前記コンピュータにさらに実行させることを特徴とする付記６記載のプログラム。

【０１３４】

（付記１２） デジタルコンテンツに対するアクセス要求をライセンス配信装置に送信し、該デジタルコンテンツにアクセスするためのライセンスデータを応答として該ライセンス配信装置から受信するコンピュータのためのプログラムであって、

前記デジタルコンテンツに対して許可されるアクセス形態および許諾条件を記述した複数のアクセス制御リストと選択処理を指定する情報とを含み、前記ライセンス配信装置から受信して格納手段に格納されたライセンスデータを参照し、

前記ライセンスデータにより指定された選択処理を実行して、前記複数のアクセス制御リストの中から１つのアクセス制御リストを選択する

処理を前記コンピュータに実行させることを特徴とするプログラム。

【０１３５】

（付記１３） 利用者が前記ライセンスデータを用いて前記デジタルコンテンツにアクセスし、該デジタルコンテンツの一部をコピーしてクリップボードに入れるとき、コピー部分のデータを暗号化してクリップボードに入れ、許諾された者がペースト操作を行った場合に該コピー部分のデータを復号して貼り付ける処理を、前記コンピュータにさらに実行させることを特徴とする付記１２記載のプログラム。

【０１３６】

（付記１４） 暗号化されたデジタルコンテンツを復号するためのライセンスデータを公開鍵基盤を利用して取得するプログラムである端末モジュールを、利用者端末に配信するコンピュータのためのプログラムを記録した記録媒体であって、

前記プログラムは、

前記公開鍵基盤に基づく暗号化通信に必要な公開鍵証明書および該公開鍵証明書の公開鍵に対する秘密鍵の情報を、格納手段に格納された暗号鍵を用いて暗号化して、暗号化情報を生成し、

前記暗号化情報を復号する復号鍵を含み、前記利用者端末上で起動された後に該暗号化情報を復号して、前記公開鍵証明書および秘密鍵の情報を取得する端末モジュールと、該暗号化情報とを前記利用者端末に送信する

処理を前記コンピュータに実行させることを特徴とするコンピュータ読み取り可能な記録媒体。

【０１３７】

（付記１５） 暗号化されたデジタルコンテンツを復号するためのライセンスデータを、ライセンス配信装置から公開鍵基盤を利用して取得するコンピュータのためのプログラムを記録した記録媒体であって、

前記プログラムは、

格納手段に格納された暗号化情報を前記プログラムに含まれる復号鍵を用いて復号して、前記公開鍵基盤に基づく暗号化通信に必要な公開鍵証明書および該公開鍵証明書の公開鍵に対する秘密鍵の情報を取得し、
前記公開鍵証明書および秘密鍵の情報を用いて暗号化通信を行うことで、前記ライセンス配信装置から前記ライセンスデータを取得する
処理を前記コンピュータに実行させることを特徴とするコンピュータ読み取り可能な記録媒体。

【０１３８】

（付記１６） 利用者端末からデジタルコンテンツに対するアクセス要求を受信し、該デジタルコンテンツにアクセスするためのライセンスデータを応答として該利用者端末に配信するコンピュータのためのプログラムを記録した記録媒体であって、
前記プログラムは、
デジタルコンテンツに対応付けて、アクセスが許可される利用者、許可されるアクセス形態、および許諾条件を記述した、格納手段に格納された複数のアクセス制御リストの中から、前記アクセス要求に含まれるコンテンツ識別子に対応し、かつ、該アクセス要求を送信した要求者の利用者識別子に対応するアクセス制御リストを取得し、
得られたアクセス制御リストが複数存在する場合、得られた複数のアクセス制御リストの中から１つのアクセス制御リストを選択し、
選択したアクセス制御リストに基づく個別ライセンスデータを生成する
処理を前記コンピュータに実行させることを特徴とするコンピュータ読み取り可能な記録媒体。

【０１３９】

（付記１７） デジタルコンテンツに対するアクセス要求をライセンス配信装置に送信し、該デジタルコンテンツにアクセスするためのライセンスデータを応答として該ライセンス配信装置から受信するコンピュータのためのプログラムを記録した記録媒体であって、
前記プログラムは、
前記デジタルコンテンツに対して許可されるアクセス形態および許諾条件を記述した複数のアクセス制御リストと選択処理を指定する情報とを含み、前記ライセンス配信装置から受信して格納手段に格納されたライセンスデータを参照し、
前記ライセンスデータにより指定された選択処理を実行して、前記複数のアクセス制御リストの中から１つのアクセス制御リストを選択する
処理を前記コンピュータに実行させることを特徴とするコンピュータ読み取り可能な記録媒体。

【０１４０】

（付記１８） 暗号化されたデジタルコンテンツを復号するためのライセンスデータを公開鍵基盤を利用して取得するプログラムである端末モジュールを、利用者端末に配信する情報処理方法であって、
生成手段が、前記公開鍵基盤に基づく暗号化通信に必要な公開鍵証明書および該公開鍵証明書の公開鍵に対する秘密鍵の情報を、格納手段に格納された暗号鍵を用いて暗号化して、暗号化情報を生成し、
送信手段が、前記暗号化情報を復号する復号鍵を含み、前記利用者端末上で起動された後に該暗号化情報を復号して、前記公開鍵証明書および秘密鍵の情報を取得する端末モジュールと、該暗号化情報とを前記利用者端末に送信する
ことを特徴とする情報処理方法。

【０１４１】

（付記１９） 利用者端末からデジタルコンテンツに対するアクセス要求を受信し、該デジタルコンテンツにアクセスするためのライセンスデータを応答として該利用者端末に配信する情報処理方法であって、
生成手段が、デジタルコンテンツに対応付けて、アクセスが許可される利用者、許可さ

れるアクセス形態、および許諾条件を記述した、格納手段に格納された複数のアクセス制御リストの中から、前記アクセス要求に含まれるコンテンツ識別子に対応し、かつ、該アクセス要求を送信した要求者の利用者識別子に対応するアクセス制御リストを取得し、

前記生成手段が、得られたアクセス制御リストが複数存在する場合、得られた複数のアクセス制御リストの中から１つのアクセス制御リストを選択し、

前記生成手段が、選択したアクセス制御リストに基づく個別ライセンスデータを生成する

ことを特徴とする情報処理方法。

【図面の簡単な説明】

【０１４２】

【図１】本発明の情報処理装置の原理図である。

【図２】コンテンツ保護システムの構成図である。

【図３】ライセンスの不正利用を示す図である。

【図４】クライアント活性化機能を示す図である。

【図５】活性化情報生成手順のフローチャートである。

【図６】活性化情報生成処理のフローチャートである。

【図７】活性化情報設定処理のフローチャートである。

【図８】ライセンスのデータ構造を示す図（その１）である。

【図９】ライセンスのデータ構造を示す図（その２）である。

【図１０】Ａｃｌ構造を示す図である。

【図１１】ＡＣＬＥｎｔｒｙ構造を示す図（その１）である。

【図１２】ＡＣＬＥｎｔｒｙ構造を示す図（その２）である。

【図１３】ＡＣＬＥｎｔｒｙ構造を示す図（その３）である。

【図１４】Ａｃｐ構造を示す図（その１）である。

【図１５】Ａｃｐ構造を示す図（その２）である。

【図１６】Ａｃｐ構造を示す図（その３）である。

【図１７】Ａｃｍ構造を示す図（その１）である。

【図１８】Ａｃｍ構造を示す図（その２）である。

【図１９】Ａｃｍ構造を示す図（その３）である。

【図２０】ルート公開鍵のハッシュ値を用いた検証処理を示す図である。

【図２１】認証方式の第１の比較結果を示す図である。

【図２２】第１の優先順位表を示す図である。

【図２３】個別ライセンス選択処理のフローチャートである。

【図２４】ＡＣＬエントリ選択処理のフローチャートである。

【図２５】許諾サブジェクトドメインリストによる制御を示す図である。

【図２６】オフライン制御を示す図である。

【図２７】オフライン制御を示す図である。

【図２８】ＩＣカード認証シーケンスを示す図である。

【図２９】ＩＣカード認証処理のフローチャートである。

【図３０】ＤｅｃｏｄｅＩｎｆｏｒｍａｔｉｏｎ構造を示す図である。

【図３１】ＥｎｔｒｙｋｅｙＭａｐ型を示す図である。

【図３２】暗号化コンテンツの形式を示す図である。

【図３３】Ｃｏｎｔｅｎｔ　Ｈｅａｄｅｒの形式を示す図である。

【図３４】Ｃｏｎｔｅｎｔ　Ｉｎｆｏｒｍａｔｉｏｎを示す図である。

【図３５】Ｅｌｅｍｅｎｔ　Ｉｎｆｏｒｍａｔｉｏｎを示す図である。

【図３６】認識方式条件リストを示す図である。

【図３７】論理演算を示す図である。

【図３８】認証方式の第２の比較結果を示す図である。

【図３９】ＲｉｇｈｔｓＳｃｒｉｐｔＳｐｅｃ構造を示す図である。

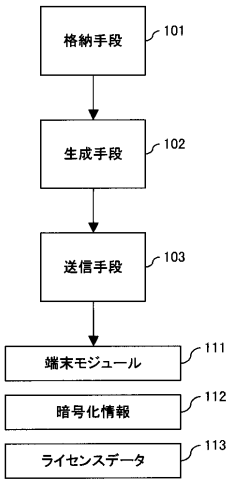
【図４０】第２の優先順位表を示す図である。

【図４１】第３の優先順位表を示す図である。
【図４２】クライアントモジュールによるＡＣＬエントリ選択処理のフローチャートである。
【図４３】ライセンスを配信しない期間を示す図である。
【図４４】情報処理装置の構成図である。
【図４５】記録媒体を示す図である。
【図４６】従来のログ管理を示す図である。
【符号の説明】
【０１４３】
１１、２０１　クライアント端末
１２　ログ管理サーバ
１３　操作ログ
１４　ログデータ
１０１　格納手段
１０２　生成手段
１０３　送信手段
１１１　端末モジュール
１１２　暗号化情報
１１３　ライセンスデータ
２０２　コンテンツ管理システム
２０３　利用者管理サーバ
２０４、３０１、３０２　ライセンス配信サーバ
２０５　コンテンツサーバ
２０６　クライアントモジュール
２０７、３１１、３１２　活性化情報
２０８、３０４、３０５　復号モジュール
２０９、３０３　ライセンサエージェント
３１３　ライセンス
４０１　活性化キー生成ツール
４０２　クライアント活性化モジュール
４０３　認証局モジュール
４０４、４０５　記憶装置
４０６　外部認証局
４１１　活性化クライアントモジュール
２５０１　ＴＲＵＳＴ株式会社
２５０２　ＩＴ株式会社
２５１１　ネットワーク事業部
２５１２　ソフトウェア事業部
２７０１　ＩＣカード認証連携モジュール
２７０２　ＩＣカード
４４０１　ＣＰＵ
４４０２　メモリ
４４０３　入力装置
４４０４　出力装置
４４０５　外部記憶装置
４４０６　媒体駆動装置
４４０７　ネットワーク接続装置
４４０８　バス
４４０９　可搬記録媒体
４５０１　サーバ

４５０２　情報処理装置
４５１１　データベース

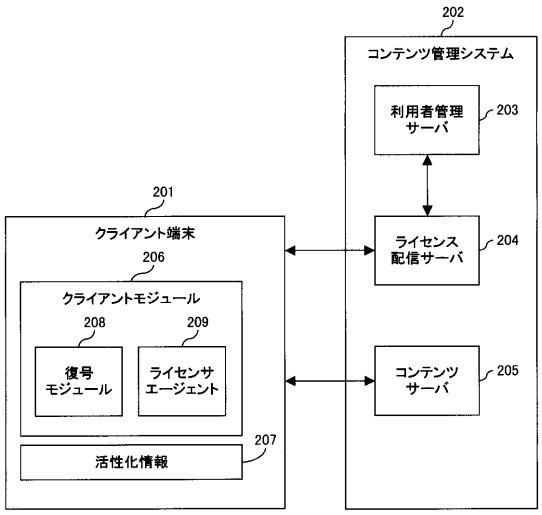
【図１】

本発明の情報処理装置の原理図



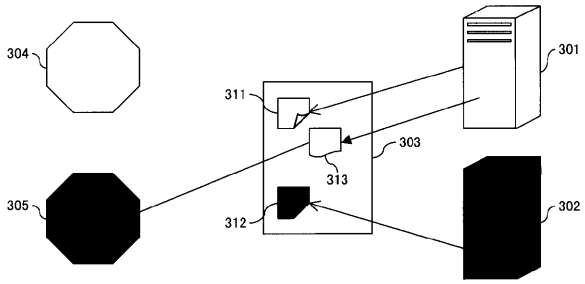
【図２】

コンテンツ保護システムの構成図



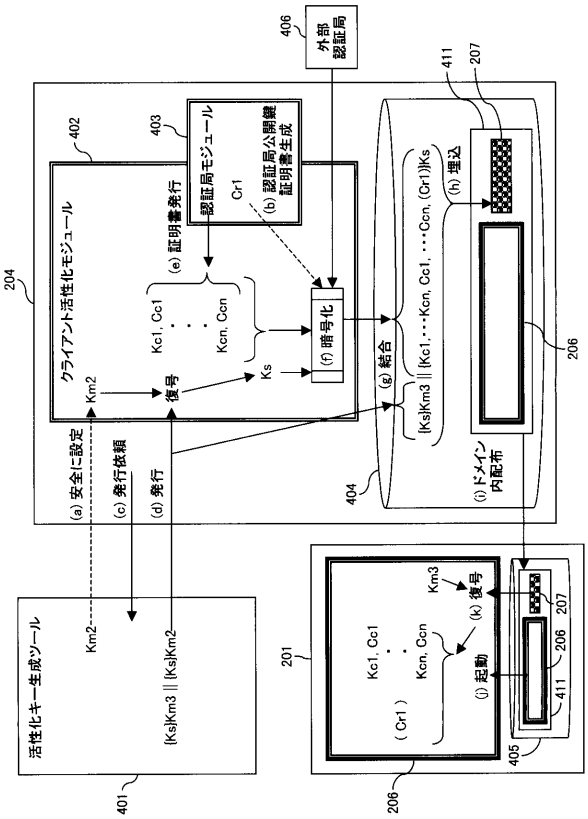
【図３】

ライセンスの不正利用を示す図



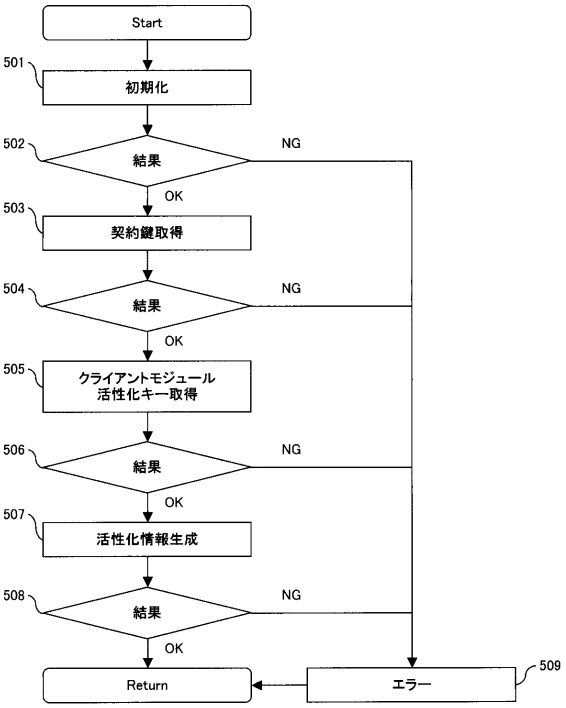
【図４】

クライアント活性化機能を示す図



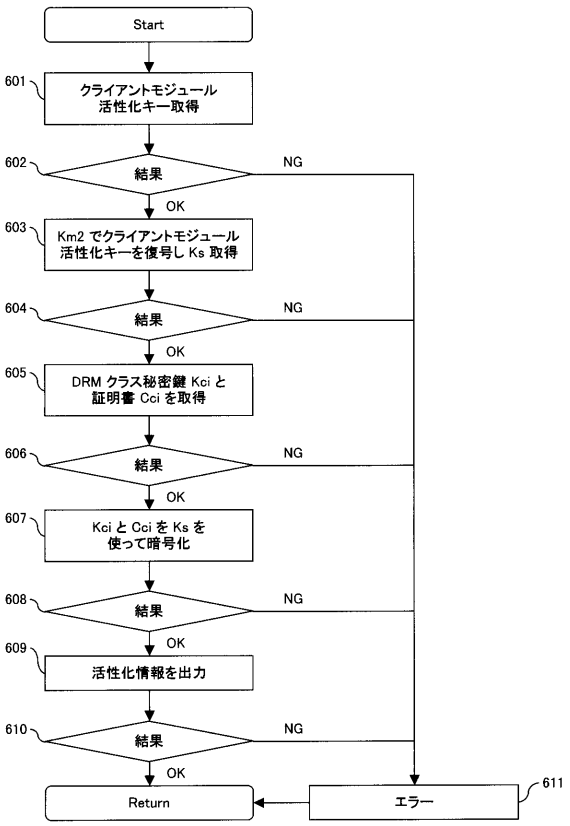
【図５】

活性化情報生成手順のフローチャート



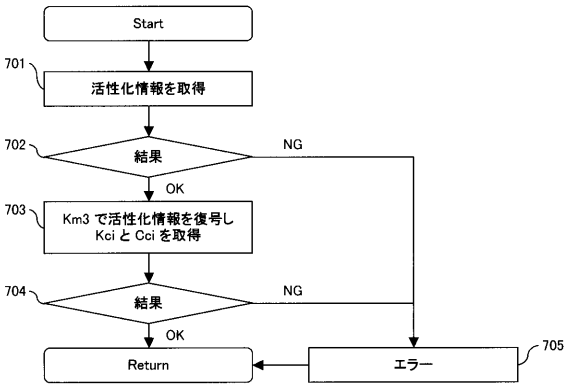
【図６】

活性化情報生成処理のフローチャート



【図７】

活性化情報設定処理のフローチャート



【図８】

ライセンスのデータ構造を示す図（その1）

LicenseInfo構造	content_id ‖transaction_id ‖ decode_information ‖acl
Size	可変長
Data	SEQUENCE型構造化データ
protocol_version	ライセンス送信プロトコルバージョン
Size	2バイト固定
Data	BIT STRING型。bit 0がLSBとする。 各ビットが次の各プロトコルバージョンに相当し，ビットがOn(1)であれば，ライセンスが当該プロトコルバージョンを実装したメディアDRMで解釈できることを示す。 bit0：Version 1 bit1：Version 2 少なくともRES_OPENで確定したバージョンのビットがOn(1)でなければならない。
content_id【license_id】	コンテンツID【ライセンスID】
Size	可変長
Data	コンテンツID【ライセンスID】。 OCTET STRING型。
transaction_id	トランザクションID
Size	12バイト固定
Data	発行時のトランザクションID OCTET STRING型
license_script_spec	本ライセンス形式とその解釈の仕様を示す情報
Size	可変長
Data	LicenseInfo記述の形式とその解釈の方針を決定する情報を格納する。本オプションが省略された場合，UDAC汎用権利記述仕様が選択されたものと解釈し，decode_informationとaclの2つのフィールドを設定必須とする。 同じLicenseInfo内にrights_script_specの値の異なるACLEntryが存在し，rights_script_spec間で複数ACLEntryからの個別ライセンス生成ポリシーが異なる場合，個別ライセンス生成は本フィールドのポリシーを優先して実施するものとする。その際，本フィールドが省略されていた場合のポリシーは，実装するシステムに依存するものとする。

【図９】

ライセンスのデータ構造を示す図（その2）

acm	ACm
Size	可変長
Data	Acm
decode_information	デコーダDRM向けコンテンツ復号情報
Size	可変長
Data	DecodeInformationタグ付きSEQUENCE型。 Kcまたは暗号化したデコーダDRM向けライセンスまたはそれらのリスト。
acl	ACL（アクセス制御リスト）
Size	可変長
Data	Acl構造
rpk_hash_list	利用許諾ルート公開鍵ハッシュリスト
Size	可変長
Data	先頭にha_idがAlgorithmIdentifier型で入る。 続いてSEQUENCE OF BIT STRING型で利用許諾ルート公開鍵のハッシュ値リストが入る。 ライセンス発行時に，証明書のチェックに利用するルート公開鍵のハッシュ値がここで指定されるリストに存在しない場合，ライセンスを発行してはならない。

【図１０】

Acl構造を示す図

Acl構造	ACL（アクセス制御リスト）
Size	可変長
Data	SEQUENCE OF型構造化データ
acl_entry	ACL（アクセス制御リスト）エントリ
Size	可変長
Data	ACLEntry構造
・ ・<繰り返し> ・	・ ・ ・
acl_entry	ACL（アクセス制御リスト）エントリ
Size	可変長
Data	ACLEntry構造

【図１１】

ACLEntry構造を示す図（その1）

ACLEntry構造	principal || acm || acp
Size	可変長
Data	SEQUENCE型。
rights_script	本ライセンス形式に対応するアプリケーション種別
Size	可変長
Data	権限記述の形式と解釈の方針を決定する情報を格納する。
operation	コンテンツ(保護オブジェクト)利用操作の種類
Size	1バイト固定
Data	00h: play。表示・再生 01h: print。印刷 02h: save。保存 03h: parts_copy。部分コピー。表示・再生・編集中のコンテンツの部分コピー 省略値は00h(表示・再生)
principal_type	許諾対象タイプ
Size	1バイト固定
Data	'A': Authenticated one。認証済利用者。 'E': Everyone。すべての利用者。 'G': グループID 'U': ユーザID 'A'はGET_LICENSE時の要求ACL内に設定して使用する。
principal	許諾対象ユーザまたはグループのID
Size	可変長
Data	配信サーバまたはメディアDRMから発行されるライセンスの場合には，利用者管理プラグインで取得したユーザIDを設定しなければならない。 principal_typeが'E'の場合，本フィールドの内容は無視されなければならない。
acm	メディアアクセス条件
Size	可変長
Data	Acm構造
acp	デコーダアクセス条件
Size	可変長
Data	Acp構造

【図１２】

ACLEntry構造を示す図（その2）

authentication_list	認証方式条件リスト
Size	可変長
Data	各ビットが各ユーザ認証方式にマッピングされ，ビットがon(1)になっている認証方式すべてでユーザ認証が正常終了している場合にかぎり，本ライセンスを発行する。一つでも異常終了していれば，ライセンス発行を拒否しなければならない。 各ビットに対応する認証方式は次のとおり。 0:ID／パスワード方式 1:ICカードによるPKI認証方式 2:指紋認証方式 3:サイン認証方式 4:静脈認証方式 5:顔認証方式 6:網膜認証方式 7:声紋認証方式 本フィールド省略値は「全ビットがoff」とする。
password_min_len	パスワード最小長さ(バイト長)
Size	1バイト
Data	符号無し整数で入力パスワードの最小長さを示す。 ライセンス許諾対象ユーザが入力し，メディアDRM内でライセンスにリンクするパスワードの最低の長さをバイト長で示す。本フィールドが存在し，有効な値が設定されているライセンスを受信したメディアDRMは，ローカルな利用者からの一回のパスワード登録と2回目以降の入力パスワード照合を実行しなければならない。本フィールドで指定された値以上の長さのパスワードが入力されるまで，本ライセンスを許諾してはならない。 本フィールドの値が0の場合，パスワード入力なしでも操作を許諾することを意味する。 本フィールドは，authentication_listのビット0(ID／パスワード方式)がOnの場合のみ有効。

【図１３】

ACLEntry構造を示す図（その3）

pw_input_ period	パスワード入力可能期間(秒)
Size	4バイト固定
Data	符号無し整数表現として解釈する。単位は秒(seconds)。本フィールドが省略された場合には「無限」として解釈する。 ライセンスを取得してから，パスワードの入力が許諾されるまでの時間を示す。
dn	許諾対象ユーザまたはグループのDN (Distinguished Name)
Size	可変長
Data	Dnタグ付きRDNSequence構造。構造は[RFC 3280]に定義された通りとする。 本フィールドは配信サーバがメディアDRMに渡す際に追加する。 メディアDRMで本フィールドを持つライセンスを利用するにあたっては，次の処理をメディアDRM内で実施する。 1) ローカルシステムに挿入されたICカードの証明書を取り込む。 2) ルート公開鍵で証明書の正当性をチェックする。 3) 証明書を用い，ICカードを認証する。 以上の確認が正常に終了すれば，ライセンス利用を許可する。 本フィールドは，authentication_listのビット1(ICカードによるPKI認証方式)がOnの場合のみ有効。
element_list	許諾コンテンツエレメント番号リスト
Size	可変長
Data	ElementList構造。 本ACLEntryの条件での利用操作が許諾されるコンテンツエレメントのエレメント番号をリストで示す。

【図１４】

Acp構造を示す図（その1）

Acp構造	flags || operation_length || not_after
Size	可変長
Data	再生許諾されたライセンスを用いて,暗号化コンテンツを復号し,表示・再生する際の限定条件リスト。複数ある条件のすべてを満たす場合にのみ，表示・再生の権限が有効となるものとする。
flags	アクセス条件指定フラグの集合
Size	1バイト固定
Data	内容はビット列で，各ビットは以下に示す意味を持ち，bit値が0ならOff，1ならOnとする。 bit 0: 操作可能サイズ制限フラグ bit 1: 操作期限指定フラグ bit 2: 印刷禁止フラグ bit 3: 保存禁止フラグ bit 4: 部分コピー禁止フラグ bit 5:キャプチャー禁止フラグ キャプチャー容認(Off)のとき，プロセス間交換情報のキャプチャー対策が実施されていないアプリケーションでもコンテンツ操作が可能。

【図１５】

Acp構造を示す図(その2)

ext_flags	拡張アクセス条件指定フラグの集合
Size	可変長
Data	ExtFlagsタグ付きのOCTET STRING型。 内容はビット列で，各ビットは以下に示す意味を持ち，bit値が0ならOff，1ならOnとする。(bit 0がLSB) bit 0: 重畳再生強制フラグ (On:強制／Off:重畳なし) 強制(On)のとき再生コンテンツにユーザIDと再生日時を重畳しなければならない。配信サーバまたはメディアDRMはLicenseInfo内のacl_entry.principalフィールドとtime_stampフィールドに計測したライセンス発行時刻を代入して，ライセンスを発行することとする。 bit 1: 重畳印刷強制フラグ (On:強制／Off:重畳なし) 強制(On)のとき印刷コンテンツにユーザIDと印刷日時を重畳しなければならない。配信サーバまたはメディアDRMはLicenseInfo内のacl_entry.principalフィールドとtime_stampフィールドに適切な値を代入して，ライセンスを発行することとする。 bit 2: 内部コード出力禁止フラグ (On:禁止／Off:許可) 禁止(On)のとき，HTML，XML，スクリプト，中間言語など，コンテンツの内部表現ソースコードを表示，印刷などすることで出力してはならないことを示す。 bit 3: 画面キャプチャー禁止フラグ (On:禁止／Off:許可) 禁止(On)のとき，画面印刷機能の実行を禁止する。 bit 4: 平文保存禁止フラグ (On:禁止／Off:許可) 禁止(On)のとき，コンテンツを平文で保存してはならないことを示す。本フラグがOffでかつflagsの保存禁止フラグもOffのときにのみ，コンテンツを平文で保存することが許可される。 bit 5: メール添付禁止フラグ (On:禁止／Off:許可) 禁止(On)のとき，コンテンツをメールに添付できないことを示す。本フラグがOffのとき，コンテンツをメールに添付することが許可される。 bit 6: 転送禁止フラグ (On:禁止／Off:許可) 禁止(On)のとき，メールなどで送信したコンテンツを転送できないことを示す。本フラグがOffのときにのみ，転送することが許可される。 bit 7: Reserved(予約)。すべてOff (0)とする。 各Operationライセンスのext_flagsデフォルト値は次のとおりとする。 playライセンス：0001 1000b (18h) printライセンス：0001 1000b (18h) saveライセンス：0001 1000b (18h) copyライセンス：0001 1000b (18h)

【図１６】

Acp構造を示す図(その3)

operation_length	操作長さ。一回の操作許諾でアプリケーションで操作可能な暗号化コンテンツの総サイズ
Size	8バイト固定
Data	OperationLengthタグ付きのOCTET STRING型。 一回の操作許諾で操作可能な総バイト数を格納する。 符号無し整数で表す暗号化コンテンツ先頭からのバイト数。 操作可能サイズ制限フラグがOnで本フィールドがない場合は，操作を中止する。また操作可能サイズ制限フラグがOffで本フィールドがある場合は，本フィールドの値は無効とす値がFFFFFFFFFFFFFFFFhの場合は無制限に操作できることを示す。 not_afterとともに指定された場合は，先に操作中止条件に達したほうが実効力を持つこととなる。

【図１７】

Acm構造を示す図(その1)

Acm構造	operation_count || move_count || safe_level || kept_period・・・
Size	可変長
Data	ライセンスを配信・移動したり,デコーダDRMに再生許諾する際の限定条件リスト。
operation_count	コンテンツ操作許諾可能数
Size	1バイト固定
Data	再生・表示・実行・印刷などの操作許諾を配信サーバまたはメディアDRMからデコーダDRMに発行可能な回数。

【図１８】

Acm構造を示す図(その2)

control_flags	制御フラグ群
Size	1バイト固定
Data	各ビットは次に示す意味を持ち，bit値が0ならOff，1ならOnとする。(bit 0がLSB) bit 0: self_export。自出力フラグ (On:出力／Off:非出力) 非出力の場合，Exportしても Export元DRMのライセンス内のrights countの値は変化しない。 出力の場合，Exportすると，Export元DRMのライセンス内のrights countの値はExportした数だけ減算する。 bit 1: export_ac。アクセス条件出力フラグ(On:出力／Off:非出力) 出力(On)と非出力(Off)それぞれの意味はexport_countの説明で規定される。 出力(On)の場合，他方式DRMへのライセンス転送を仲介するデコーダDRMには，acmオプションを付加したPlayInformation（表11.15で定義）を送信しなければならない。 bit 2: copy_kept_limit。許諾保持期限コピーフラグ On:配信サーバまたはVMDRMからメディアDRMに許諾保持期限をコピーしたライセンスを発行する。 Off: 配信サーバまたはVMDRMではメディアDRMに発行する個別ライセンス内の許諾保持期限を省略する。 bit 3: copy_start_time。許諾開始日時コピーフラグ On:配信サーバまたはVMDRMからメディアDRMに許諾開始期限をコピーしたライセンスを発行する。 Off: 配信サーバまたはメディアDRMでは，許諾開始日時になるまで，他のメディアDRMにライセンスを発行してはならない。 bit 4: dynamic_license。逐次ライセンス指定フラグ On: 逐次ライセンス(dynamic license)限定。配信サーバまたはメディアDRM内のライセンスで本フラグがOnの場合，オフラインライセンスが要求されれば，許諾を拒否しなければならない。 Off: オフライン(offline)ライセンス限定。配信サーバまたはメディアDRM内のライセンスで本フラグがOffの場合，オフラインライセンスのみが発行可能。 逐次ライセンス発行時にはACLを解釈し，個別ライセンスを生成・発行する。逐次ライセンスとして発行された個別ライセンスのrights_countには01hを設定しなければならない。またその際，move countには00hを設定しなければならない。 bit 5: decoder_cert。デコーダ証明書必須フラグ On: デコーダ証明書の利用が必須。ライセンス送信側はライセンス内のKcとACpをデコーダDRM証明書の公開鍵で暗号化して，受信側に発行する。このため，ライセンス配信を要求するクライアントはOpen時に配信サーバまたはメディアDRMにデコーダDRMの公開鍵証明書を送信しなければならない。このデコーダDRMの公開鍵による暗号部分は，デコーダDRM Off: デコーダ証明書の利用は必須ではない。クライアントは，配信サーバまたはメディアDRMにデコーダDRMの公開鍵証明書を送信する必要はない。 bit 6: Reserved(予約)。Off (0)とする。 bit 7: deny。優先的拒否フラグ(On:拒否／Off:許諾) 拒否(On)の場合,ライセンス発行先のユーザおよびユーザが所属するグループにどのような許諾が与えられていても,本フィールドを含むACLEntryで指定されたOperationを優先的に拒否する。Onならkept_limitとstart_time以外のフィールドは無効とする。 本フラグはGET_LICENSEのフィールド内では必ずOffとする。 省略時はすべてOff (0)とする。

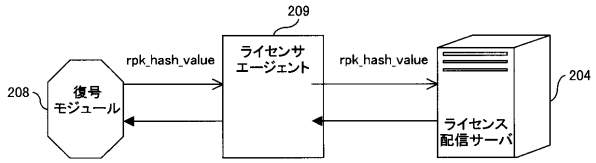
【図１９】

Acm構造を示す図(その3)

rights_count	権利数。コピー可能回数－1に相当する。配信サーバまたは配信先メディアDRMから他メディアDRMへ配信または移動可能なライセンス数
Size	1バイト固定
Data	00h～FEh：符号なし整数表現。配信サーバ，VMDRM，メディアDRMから他のVMDRMまたはメディアDRMに配信または移動可能なライセンス数を示す。配信・移動元DRM内では，ライセンスの配信・移動の実行ごとに本フィールドの値を配信または移動した数だけ減算する。00hになれば，他メディアDRMへの配信・移動はできないし，配信・移動元DRMでのライセンスも無効となる。 FFh：他メディアDRMに無限回コピーが可能なことを示す。ライセンスの配信・移動後も値は変わらない。
kept_period	許諾保持期間。配信先DRMにライセンスが記録されてからのライセンスをDRM内に維持可能な期間。
Size	4バイト固定
Data	符号無し整数表現として解釈する。単位は秒(seconds)。本フィールドが省略された場合には「無限」として解釈する。
kept_limit	許諾保持期限。
Size	可変長
Data	DateAndTime構造。 配信サーバのデータベース内ライセンスに本フィールド指定がある場合，指定期限の後はライセンス配信を停止しなければならない。 無効な値が設定されている場合はライセンスを無効とする。 kept_periodとともに指定された場合は，タイムアウトが早い側が実効力を持つこととなる。 省略値は「無限」。
start_time	許諾開始日時。
Size	可変長
Data	DateAndTime構造。 配信サーバやVMDRMのデータベース内ライセンスに本フィールド指定がある場合，指定時刻を過ぎるまではライセンス配信をしてはならない。メディアDRM内ライセンスに本フィールド指定がある場合，指定時刻まではライセンスを無効とし，デコーダDRMへのライセンス許諾もメディアDRMへのライセンス移動・コピーも停止しなければならない。 省略値は「即時許諾」。
subject_list	許諾サブジェクトドメインリスト。
Size	可変長
Data	SubjectList構造型。 本リストは，ライセンスを許諾するDRMの証明書サブジェクト名上位RDNのリストを示す。すなわち，本リストで指定された上位RDNを持つサブジェクト名(DN)の証明書を持つDRMのみに本ライセンスの発行が許諾される。

【図２０】

ルート公開鍵のハッシュ値を
用いた検証処理を示す図



【図２１】

認証方式の第１の比較結果を示す図

Bit	意味	(1)～(6)を満たさない ACL Entryの 認証方式条件リスト	checkPrincipalで 得られた 認証方式条件リスト	結果
0	ID/パスワード	1	1	1
1	ICカードによるPKI認証	1	0	0
2	:指紋認証	0	1	1
3	サイン(筆跡)認証	0	0	1
4	静脈認証	0	0	1
5	顔認証	0	0	1
6	網膜認証	0	0	1
7	声紋認証	0	0	1

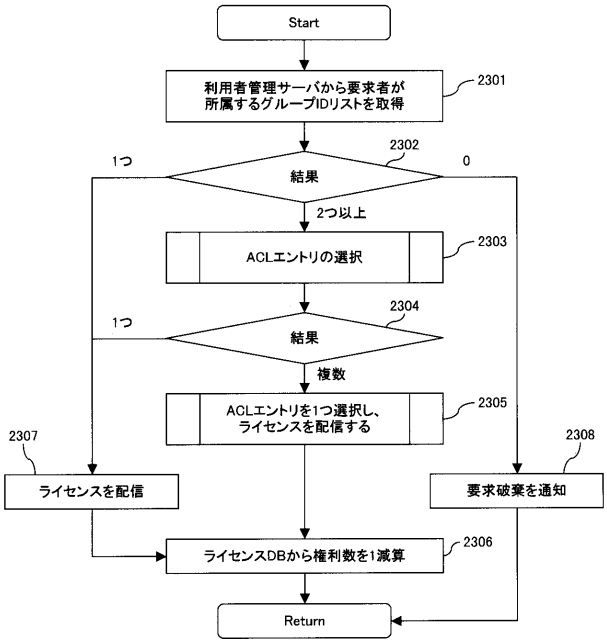
【図２２】

第１の優先順位表を示す図

順番	許諾条件		選択ルール
1	acm	kept_limit	最も短いACL Entryを選択する。
2	acm	operation_count	最小値のACL Entryを選択する。
3	acm	kept_period	最も短いACL Entryを選択する。
4	acp	flags 部分コピー禁止	OnのACL Entryを選択する*。
5	acp	flags 保存禁止	OnのACL Entryを選択する*。
6	acp	flags 印刷禁止	OnのACL Entryを選択する*。
7	acm	rights_count	最小値のACL Entryを選択する。

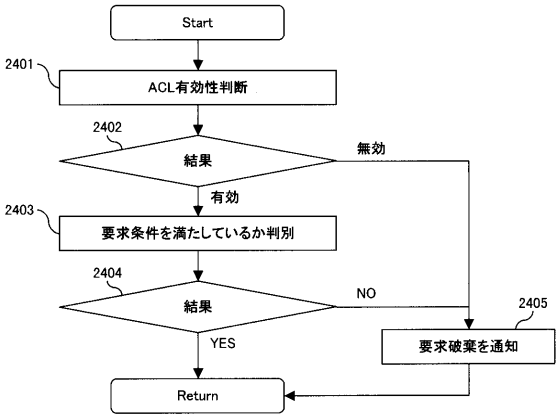
【図２３】

個別ライセンス選択処理のフローチャート



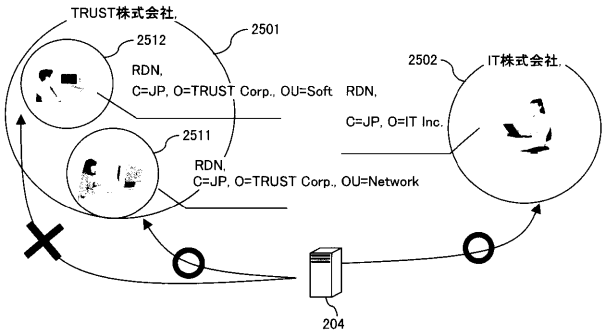
【図２４】

ACLエントリ選択処理のフローチャート



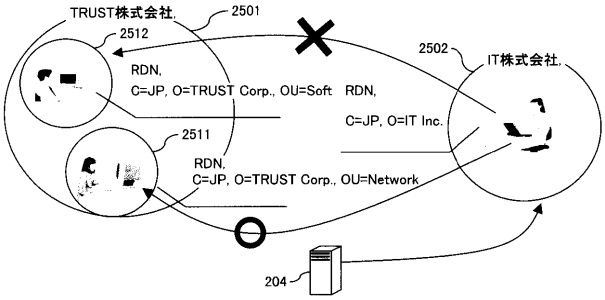
【図２５】

許諾サブジェクトドメインリストによる制御を示す図



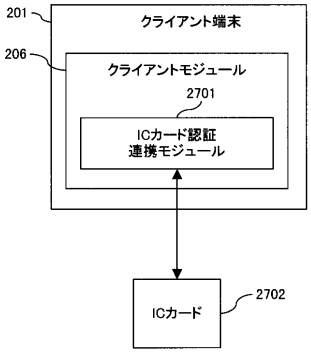
【図２６】

オフライン制御を示す図



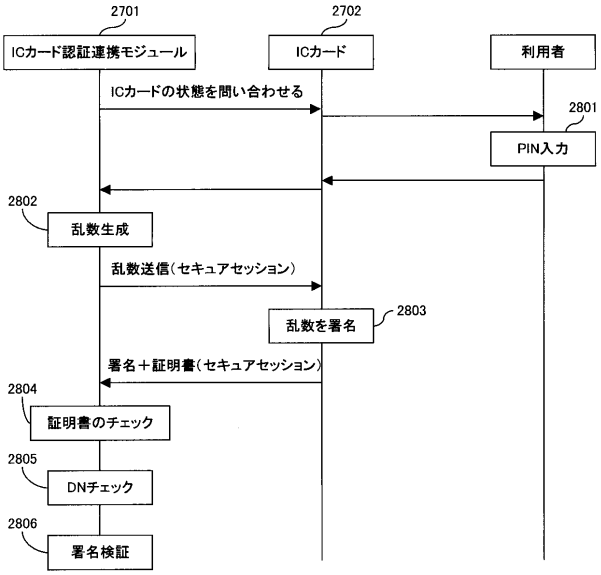
【図２７】

ICカード認証連携モジュールを示す図



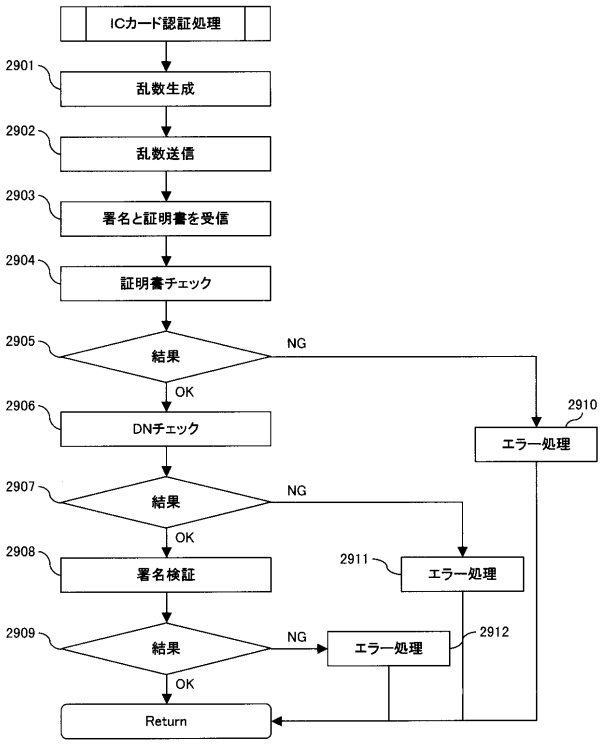
【図２８】

ICカード認証シーケンスを示す図



【図２９】

ICカード認証処理のフローチャート



【図３０】

DecodeInformation構造を示す図

DecodeInformation構造	Kc，暗号化したデコーダDRM向けLicenseInfoおよびそれらの配列の選択
Size	可変長
Data	SEQUENCE型。
symmetric_key	Kc。コンテンツ復号鍵。
Size	可変長
Data	SymmetricKey型。
encrypted_play_info	デコーダDRM証明書の公開鍵で暗号化したLicenseInfo
Size	可変長
Data	EncryptedCode型。 LicenseInfo型のデータがデコーダDRM証明書の公開鍵で暗号化されて格納される。
decode_info_sequence	Kcなどコンテンツ復号情報の順位付きリスト。
Size	可変長
Data	SEQUENCE OF DecodeInformation型。ただし，このフィールド内にdecode_info_sequenceフィールドを含んではならない。
element-key-map	暗号化コンテンツのエレメント－復号鍵対応リスト
Size	可変長
Data	ElemetKeyMap型。 各Kcに対応する暗号化コンテンツエレメントの番号。対応するDecodeInformationにより復号を許諾された暗号化コンテンツエレメント番号を一覧にした内容。decode_info_sequence内の各Kcが，本フィールド内で同じ順位のエレメント番号に対応する。 本フィールドが存在する場合，この番号リストに存在しないエレメントは対象のDecodeInformationを用いて復号してはならない。 decode_info_sequenceフィールドが選択されたDecodeInformation内にのみ存在する。

【図３１】

ElementKeyMap型を示す図

ElementKeyMap型	暗号化コンテンツエレメント・復号鍵対応一覧
Size	可変長
Data	各暗号化コンテンツエレメントの番号に対応するコンテンツ復号鍵または許諾情報を示す。すなわち，暗号化コンテンツエレメント番号とそのエレメントを復号するために必要な情報を格納する。 本フィールドが存在する場合，そのエレメント番号リストに存在しないエレメントは，そのフィールドが存在するライセンスを用いて復号してはならない。
element-number	暗号化コンテンツエレメント番号
Size	4バイト
Data	次のフィールドで指定されるコンテンツ復号鍵または許諾情報に対応する暗号化コンテンツエレメントの番号。すなわち，対応するDecodeInformationにより復号可能な暗号化コンテンツエレメント番号。(暗号化コンテンツのElement Numberに対応する番号)
decode_info	コンテンツを復号する鍵などの復号情報
Size	可変長
Data	前のフィールドで指定された暗号化コンテンツエレメントに対応するDecodeInformationの値を示す。 ただし，このフィールド内にdecode_infoフィールドを含んではならない。
	・ 以上2つのフィールドをセットとして繰り返し ・

【図３２】

暗号化コンテンツの形式を示す図

Content Header	Element1	Element2	・・・	ElementN

【図３３】

Content Headerの形式を示す図

Content Information
Element 1 Information
:
Element N Information
Element 1 Attribute
:
Element N Attribute

【図３４】

Content Informationを示す図

Data	Summary
Size of Content Information	Content Data Informationサイズ
Size of Content ID	Content ID サイズ
Content ID	コンテンツID
Size of Content Data	コンテンツデータサイズ(byte)
Number of Elements	構成要素(Element)の総数

【図３５】

Element Informationを示す図

Data	Summary
Element Number	エレメント識別番号 各エレメントに付与されるユニークな番号。
Start Offset of Element	データの先頭を基準としたElementの開始オフセット(byte)
Size of Element	エレメントサイズ
Element Type	エレメントタイプ
Cryptosystem	コンテンツの暗号方式
Key Length	コンテンツ鍵の鍵長(bit)
Size of Block	サイズをバイト数で示す。
Size of Original Data	データ本来のサイズ(byte) ブロックヘッダやパディングを含まない純粋なデータサイズ
Start Offset of Attribute	データの先頭を基準としたElement Attributeの開始オフセット
Size of Attribute	Element Attributeのサイズ
Character Code Set	File Nameの文字コードセット
Size of File Name	後続するファイル名のサイズ
File Name	エレメントに付けられたファイル名

【図３６】

認識方法条件リストを示す図

ビット	方式
Bit 0	ID／パスワード方式
Bit 1	ICカードによるPKI認証方式
Bit 2	指紋認証方式
Bit 3	サイン方式
Bit 4	静脈認証方式
Bit 5	顔認証方式
Bit 6	網膜認証方式
Bit 7	声紋認証方式

【図３７】

論理演算を示す図

A	B	A ⇒ B
0	0	1
0	1	1
1	0	0
1	1	1

【図３８】

認証方式の第2の比較結果を示す図

Bit	意味	利用者管理サーバから取得した認証方式条件をauthentication_listの形式にマップした情報	authentication_list	結果
0	ID/パスワード	1	1	1
1	ICカードによるPKI認証	0	1	0
2	:指紋認証	1	0	1
3	サイン(筆跡)認証	0	0	1
4	静脈認証	0	0	1
5	顔認証	0	0	1
6	網膜認証	0	0	1
7	声紋認証	0	0	1

【図３９】

RightsScriptSpec構造を示す図

RightsScriptSpec構造	権限記述仕様指定情報
Size	可変長
Data	SEQUENCE型。
	OBJECT IDENTIFIER型。
script_id	権限記述方式のOBJECT IDENTIFIER
Size	可変長
Data	OBJECT IDENTIFIER型。 権利記述言語とその解釈ポリシーを示すID。 省略値の解釈は実装システムに依存する。

【図４０】

第2の優先順位表を示す図

順番	許諾条件		選択ルール
1	acm	operation_count	最小値のACL Entryを選択する。
2	acp	flags 部分コピー禁止	OnのACL Entryを選択する*。
3	acp	flags 保存禁止	OnのACL Entryを選択する*。
4	acm	kept_limit	最も短いACL Entryを選択する。
5	acm	kept_period	最も短いACL Entryを選択する。
6	acp	flags 印刷禁止	OnのACL Entryを選択する*。
7	acm	rights_count	最小値のACL Entryを選択する。

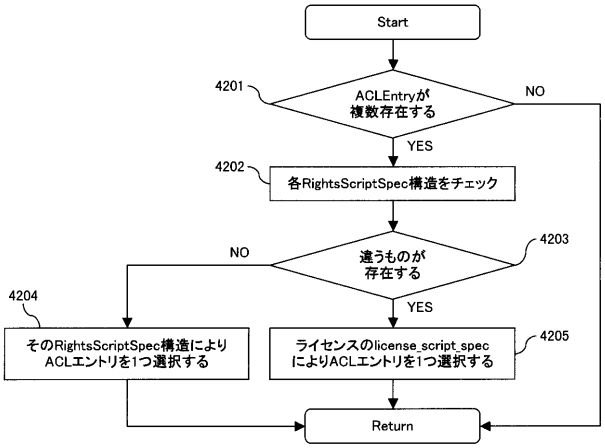
【図４１】

第3の優先順位表を示す図

順番	許諾条件		選択ルール
1	acm	operation_count	最大値のACL Entryを選択する。
2	acp	flags 部分コピー禁止	OffのACL Entryを選択する*。
3	acp	flags 保存禁止	OnのACL Entryを選択する*。
4	acm	kept_limit	最も長いACL Entryを選択する。
5	acm	kept_period	最も短いACL Entryを選択する。
6	acp	flags 印刷禁止	OnのACL Entryを選択する*。
7	acm	rights_count	最小値のACL Entryを選択する。

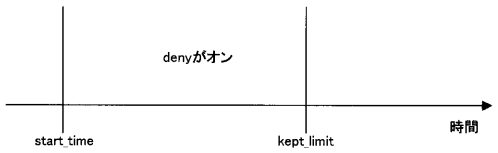
【図４２】

クライアントモジュールによる
ACLエントリ選択処理のフローチャート



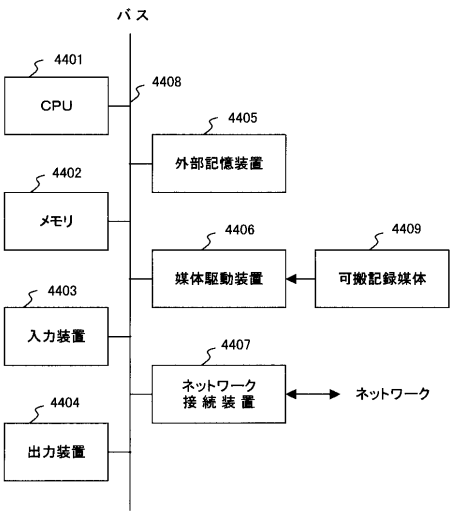
【図４３】

ライセンスを配信しない期間を示す図



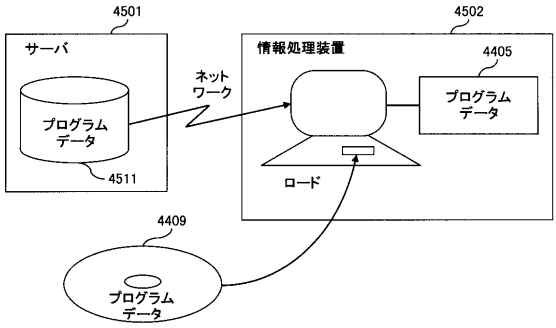
【図４４】

情報処理装置の構成図



【図４５】

記録媒体を示す図



【図４６】

従来のログ管理を示す図

フロントページの続き

(72)発明者　田中　啓士郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　由良　正和
愛知県名古屋市東区葵一丁目１６番３８号　株式会社富士通プライムソフトテクノロジ内
(72)発明者　長岡　輝良
愛知県名古屋市東区葵一丁目１６番３８号　株式会社富士通プライムソフトテクノロジ内

Ｆターム(参考) 5J104 AA16　EA17　EA18　PA14