

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2009-508412

(P2009-508412A)

(43) 公表日 平成21年2月26日(2009.2.26)

(51) Int.Cl.	F I	テーマコード (参考)
H04L 9/08 (2006.01)	H04L 9/00 601B	5B017
H04N 7/173 (2006.01)	H04N 7/173 630	5B285
G06Q 30/00 (2006.01)	H04L 9/00 601E	5C164
G06Q 50/00 (2006.01)	G06F 17/60 302E	5J104
G06Q 10/00 (2006.01)	G06F 17/60 142	

審査請求 未請求 予備審査請求 未請求 (全 80 頁) 最終頁に続く

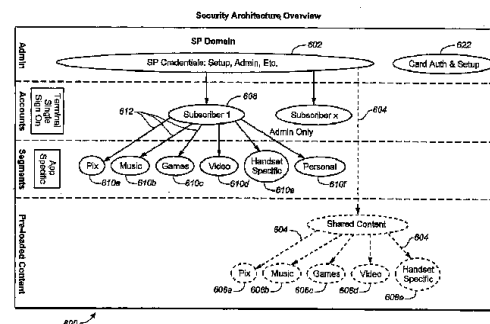
(21) 出願番号	特願2008-530239 (P2008-530239)	(71) 出願人	507208288 サンディスク コーポレーション アメリカ合衆国 95035 カリフォル ニア州, ミルピタス, マッカーシー ブ ールバード 601
(86) (22) 出願日	平成18年9月7日 (2006.9.7)	(74) 代理人	100083895 弁理士 伊藤 茂
(85) 翻訳文提出日	平成20年5月12日 (2008.5.12)	(74) 代理人	100150876 弁理士 松山 裕一郎
(86) 国際出願番号	PCT/US2006/035155	(72) 発明者	カワミ, バーマン アメリカ合衆国 95138 カリフォル ニア州, サンノゼ, キラーニ サークル 5899
(87) 国際公開番号	W02007/030760		
(87) 国際公開日	平成19年3月15日 (2007.3.15)		
(31) 優先権主張番号	60/715,524		
(32) 優先日	平成17年9月8日 (2005.9.8)		
(33) 優先権主張国	米国 (US)		
(31) 優先権主張番号	11/322,812		
(32) 優先日	平成17年12月30日 (2005.12.30)		
(33) 優先権主張国	米国 (US)		
(31) 優先権主張番号	11/322,766		
(32) 優先日	平成17年12月30日 (2005.12.30)		
(33) 優先権主張国	米国 (US)		

最終頁に続く

(54) 【発明の名称】 メディアコンテンツのセキュアストレージと配信のためのモバイルメモリシステム

(57) 【要約】

メモリデバイスは、メディアコンテンツが安全に記憶され、コンテンツ所有者又は配信に関与するサービスプロバイダによって想定される方法で配信できるようにする制御構造を含んでいる。当該メモリデバイスを使用してメディアコンテンツを配信するための多種多様な手段が利用できるようになり、デバイスは、要約されたプレビューメディアコンテンツ、暗号化されたノーカットのメディアコンテンツ、プリペイドコンテンツ、当該コンテンツへのアクセスを管理する権利及び／又は規則、の内の1つ又はそれ以上を含んでいる場合などが考えられる。メモリデバイスは、サービスプロバイダ（コンテンツ所有者でもよい）が、メディアコンテンツ配信のための安全な環境を作り出せるようにする或る型式の制御構造を有しており、そこでは、エンドユーザーと端末は、サービスプロバイダに登録し、サービスプロバイダにより制御された方法でコンテンツへアクセスすることができるようになる。ロードされる各種構成要素（例えば、要約されたプレビューメディアコンテンツ、暗号化されたノーカットのメディアコンテンツ、プリペイドコンテ



【特許請求の範囲】**【請求項 1】**

セキュアメモリ領域及び少なくとももう 1 つのメモリ領域を有している不揮発性書換可能メモリデバイスにより、メディアタイトルを配信する方法であって、前記デバイスは、前記セキュア領域に記憶されている 1 つ又は複数のコンテンツ暗号化鍵と、

前記デバイスのメモリ領域に記憶され、前記コンテンツ暗号化鍵（複数鍵）により暗号化されているメディアタイトル、前記メディアタイトルの選択された部分、及び／又は当該タイトルの制約無しにアクセスできる低品質バージョンを含んでいるコンテンツと、を備えており、前記方法は、

権利及び／又は規則に関する情報を受け取る段階と、

前記デバイスの前記セキュアメモリ領域に、認証情報が前記デバイスにより受け取られると前記デバイスに記憶されている選択された暗号化されているメディアタイトルを復号するためのコンテンツ暗号化鍵（複数鍵）へのアクセスを許可する、前記権利及び／又は規則を記憶する段階と、

少なくとも幾つかの前記メディアタイトルの前記選択された部分又は当該タイトルの低品質バージョンを、レンダリングするためにホストに供給する段階と、から成る方法。

【請求項 2】

前記認証情報を受け取る段階と、前記デバイスに記憶されている選択された暗号化されているメディアタイトルを、コンテンツ暗号化鍵を使用して復号する段階と、を更に含んでいる、請求項 1 に記載の方法。

【請求項 3】

当該認証情報が受け取られる前に、前記認証情報をセッション鍵で暗号化する段階を更に備えている、請求項 1 に記載の方法。

【請求項 4】

前記ホストが、前記暗号化されているメディアタイトルをレンダリングするために前記デバイスを操作する方法であって、前記方法は、

前記ホストをサーバに接続する段階と、

購入認証を前記ホストから前記サーバに送る段階と、

前記ホスト側で、前記サーバから前記認証情報及び前記権利及び／又は規則に関する情報を受け取る段階と、

前記認証情報及び前記権利及び／又は規則に関する情報を前記デバイスに供給する段階と、を更に含んでいる、請求項 1 に記載の方法。

【請求項 5】

前記デバイスに記憶されている前記選択された暗号化されているメディアタイトルを復号する段階と、

前記復号されたメディアタイトルをユーザー向けにレンダリングするために前記ホストに送る段階と、を更に含んでいる、請求項 4 に記載の方法。

【請求項 6】

前記復号された、選択された暗号化されているメディアタイトルをセッション鍵で暗号化する段階を更に含んでいる、請求項 5 に記載の方法。

【請求項 7】

前記ユーザーに当該メディアタイトルを購入するように促す段階を更に含んでいる、請求項 1 に記載の方法。

【請求項 8】

前記メディアタイトルはファイルに編成され、各ファイルは対応するコンテンツ暗号化鍵により暗号化され、前記デバイスは、前記ファイルの内の少なくとも幾つかのそれぞれについて、当該ファイルの前記対応するコンテンツ暗号化鍵を使用するための許可及び／又は制約を含むアクセス制御記録を更に備えており、前記ファイルの内の 1 つの第 1 アクセス制御記録は、前記認証情報が提示されたとき、前記対応するコンテンツ暗号化鍵にアクセスする前記許可の委譲を別のアクセス制御記録に許可するものであって、前記方法は

10

20

30

40

50

、

前記認証情報を前記第1アクセス制御記録に提示する段階と、

前記第1アクセス制御記録に、その対応するコンテンツ暗号化鍵にアクセスする許可を、前記第1アクセス制御記録とは異なる第2アクセス制御記録に委譲させる段階と、を更に含んでいる、請求項1に記載の方法。

【請求項9】

複数のアクセス制御記録のそれぞれに、その対応するコンテンツ暗号化鍵にアクセスする許可を、前記第1及び前記複数のアクセス制御記録とは異なる第2アクセス制御記録に委譲させる段階を更に含んでいる、請求項8に記載の方法。

【請求項10】

不揮発性書換可能メモリデバイスによりメディアタイトルを配信するための方法であって、前記デバイスは、

対応するコンテンツ暗号化鍵によりそれぞれに暗号化されるメディアファイルと、前記ファイルの内の少なくとも幾つかのそれぞれのための制御構造を備え、前記構造は、当該ファイルの前記対応するコンテンツ暗号化鍵を使用するための許可及び／又は制約を含み、前記ファイルの内の1つの第1制御構造は、認証情報が提示されたときに、前記対応するコンテンツ暗号化鍵にアクセスするための許可の委譲を別の制御構造に許可するものであって、前記方法は、

前記認証情報を前記第1制御構造に提示する段階と、

前記第1制御構造に、その対応するコンテンツ暗号化鍵にアクセスする許可を、前記第1制御構造とは異なる第2制御構造に委譲させる段階と、を含んでいる方法。

【請求項11】

前記第1及び第2制御構造は、アクセス制御記録を備えている、請求項10に記載の方法。

【請求項12】

セキュアメモリ領域と少なくとももう1つのメモリ領域とを有する不揮発性書換可能メモリデバイスによりメディアタイトルを配信するための方法であって、前記デバイスは、

前記デバイスに記憶されている暗号化されたコンテンツが関与し、前記セキュアメモリ領域に記憶されている、1つ又は複数のコンテンツ暗号化鍵及び権利及び／又は規則と、

前記デバイスのメモリ領域に記憶され、前記1つ又は複数のコンテンツ暗号化キーにより暗号化されているメディアタイトルを含み、前記権利及び／又は規則は、前記メディアタイトルの内の少なくとも幾つかの選択された部分又は当該タイトルの低品質バージョンだけが制約無しにアクセスできることを、又は当該タイトルが制限回数だけ再生され得ることを指定するコンテンツと、

を備え、

前記方法は、

前記コンテンツ暗号化鍵（複数鍵）へのアクセスを提供するための権利及び／又は規則に関する情報を受け取る段階と、

前記デバイスに記憶された、選択され暗号化されているメディアタイトルへのアクセスを許可するために、認証情報に応じて前記コンテンツ暗号化鍵（複数鍵）へのアクセスを提供する前記権利及び／又は規則を変更する段階と、から成る方法。

【請求項13】

ホストが、前記暗号化されているメディアタイトルをレンダリングするために前記デバイスを操作する方法であって、前記方法は、

前記ホストをサービスプロバイダに接続する段階と、

前記ホストからの購入認証を前記サービスプロバイダに送る段階と、

前記認証情報と、前記サービスプロバイダから、前記デバイス内の前記権利及び／又は規則を変更して前記コンテンツ暗号化鍵（複数鍵）へのアクセスを提供できるようにする情報を受け取る段階と、を更に含んでいる、請求項12に記載の方法。

【請求項14】

前記受け取った情報に応じて前記１つ又は複数のコンテンツ暗号化鍵（複数鍵）の内の少なくとも１つへのアクセスを提供するために、前記デバイスに記憶されている前記権利及び／又は規則を変更する段階を更に含んでいる、請求項１３に記載の方法。

【請求項１５】

前記デバイスに記憶されている選択された暗号化されているメディアタイトルを復号する段階と、

前記復号されたメディアタイトルをユーザー向けにレンダリングするために前記ホストに送る段階と、を更に含んでいる、請求項１４に記載の方法。

【請求項１６】

前記復号された、選択された暗号化されているメディアタイトルをセッション鍵で暗号化する段階を更に含んでいる、請求項１５に記載の方法。

10

【請求項１７】

ユーザー向けに、前記メディアタイトルの内の少なくとも幾つかの前記選択された部分又は当該タイトルの低品質バージョンを再生するか、又は当該タイトルを制限回数だけ再生する段階と、

前記ユーザーに当該メディアタイトルを購入するように促す段階と、を更に含んでいる、請求項１２に記載の方法。

【請求項１８】

前記デバイスに記憶されている前記選択された暗号化されているメディアタイトルを、前記１つ又は複数のコンテンツ暗号化鍵により復号する段階と、

20

前記復号されたメディアタイトルをユーザー向けにレンダリングする段階と、を更に含んでいる、請求項１２に記載の方法。

【請求項１９】

当該情報が受け取られる前に、前記認証情報をセッション鍵で暗号化する段階を更に含んでいる、請求項１２に記載の方法。

【請求項２０】

不揮発性書換可能メモリデバイスによりメディアタイトルを配信するための方法であって、前記デバイスは前記デバイスの中に記憶されているシステムエージェントを備え、

前記方法は、

前記デバイスが正規であると証明できるようにする情報を提供する段階と、

30

前記デバイスに記憶されている暗号化されているコンテンツへのアクセスに関与する権利及び／又は規則を制御するために、第１サービスプロバイダが、前記デバイス内に第１の対応する制御構造を作成できるように前記エージェントを使用する段階と、を備えている方法。

【請求項２１】

前記第１サービスプロバイダとは異なる少なくとも追加のサービスプロバイダが、前記デバイス内に前記第１制御構造とは異なる追加の対応する制御構造を作成できるように前記エージェントを使用する段階を更に含んでいる、請求項２０に記載の方法。

【請求項２２】

前記制御構造のそれぞれは、前記デバイスに記憶されている暗号化されているコンテンツにアクセスするための権利及び／又は規則を指定する方法であって、前記方法は、前記サービスプロバイダのそれぞれが、その対応する制御構造により指定された前記権利及び／又は規則に対する排他的制御を有することができるようにする段階を更に含んでいる、請求項２１に記載の方法。

40

【請求項２３】

前記サービスプロバイダは、互いに独立的に前記デバイスと対話し、或るサービスプロバイダの前記対応する制御構造により指定されている前記権利及び／又は規則は、別のサービスプロバイダによってアクセス、請求項２２に記載の方法。

【請求項２４】

前記デバイスで、前記第１サービスプロバイダと関係付けられているメディアコンテン

50

ツを受け取る段階と、前記デバイスで、前記メディアコンテンツを記憶する段階と、を更に含んでいる、請求項 20 に記載の方法。

【請求項 25】

ホストで動作している 1 つ又は複数のアプリケーションが、前記暗号化されているメディアタイトルをレンダリングするために前記デバイスと通信する方法であって、前記方法は、

前記アプリケーション（複数のアプリケーション）の事前に決められている証明書の提示に応じて、前記暗号化されているメディアタイトルを復号して、前記復号されたメディアタイトルを前記 1 つ又は複数のアプリケーションに（複数のアプリケーション）再生用に供給する段階を更に含んでいる、請求項 20 に記載の方法。

10

【請求項 26】

前記デバイスが、証明書を記憶し、提示された前記証明書が前記記憶されている証明書と比較して受け入れ可能なときだけ、前記暗号化されているメディアタイトルを復号して、それらが再生できるようにする、請求項 25 に記載の方法。

【請求項 27】

ホストが前記デバイスを操作し、前記方法は、前記デバイスと前記第 1 サービスプロバイダに接続されるホストの間にセキュアチャネルを確立する段階を更に含み、前記エージェントは、前記第 1 サービスプロバイダが、前記セキュアチャネルを通して前記第 1 制御構造を作成できるようにする、請求項 20 に記載の方法。

【請求項 28】

20

ホストが前記デバイスを操作する方法であって、前記方法は、

前記デバイスを正規であると認証し、前記デバイスが前記ホストを正規であると認証する段階と、

前記デバイスと前記ホストの間にセキュア接続を確立する段階と、を更に含んでいる、請求項 20 に記載の方法。

【請求項 29】

前記デバイスは、前記デバイスに記憶されているメディアコンテンツを暗号化するために使用されるコンテンツ暗号化鍵を記憶し、前記第一制御構造は、前記デバイスに記憶されている前記コンテンツ暗号化鍵の 1 つ又はそれ以上へアクセスするための権利及び／又は規則を指定し、前記権利及び／又は規則は、前記暗号化されているメディアコンテンツを復号するための前記コンテンツ暗号化鍵（複数鍵）へのアクセスを許可し、前記方法は、前記暗号化されているコンテンツを復号するための前記権利及び／又は規則に従って前記コンテンツ暗号化鍵の内の 1 つ又はそれ以上へのアクセスを許容する段階を更に含んでいる、請求項 20 に記載の方法。

30

【請求項 30】

前記第 1 制御構造は、前記暗号化されているメディアコンテンツを復号するための前記コンテンツ暗号化鍵の内の 1 つ又はそれ以上へのアクセスがサブスクリプションに基づくものになるように、前記権利及び／又は規則を指定する、請求項 20 に記載の方法。

【請求項 31】

不意揮発性書換可能メモリデバイスによりメディアタイトルを配信する方法であって、

40

前記デバイスは、暗号化されているメディアコンテンツと、前記メディアコンテンツを暗号化するために使用されるコンテンツ暗号化鍵と、及び事前に決められている証明書が前記デバイスに提示されたときに前記コンテンツ暗号化鍵の内の 1 つ又はそれ以上にアクセスするための権利及び／又は規則を指定している制御構造と、を備えている方法であって、前記方法は、

前記デバイスに提示された証明書が前記事前に決められている証明書であるか否かを判定する段階と、

前記事前に決められている証明書が提示されたときに、前記暗号化されているコンテンツを復号するための前記権利及び／又は規則に従って前記コンテンツ暗号化鍵の内の 1 つ又はそれ以上にアクセスを許容する段階と、から成る方法。

50

【請求項 3 2】

複数のホストによってレンダリングされ得るメディアタイトルを記憶する不揮発性書換可能メモリデバイスによりメディアタイトルを配信するための方法であって、

前記デバイスは、

暗号化されているメディアタイトルを記憶するための第 1 メモリ領域と、前記暗号化されているメディアコンテンツへのアクセスを制御する制御情報を記憶するための第 2 安全メモリ領域であって、前記制御情報は、それぞれが前記第 1 メモリ領域に記憶されている暗号化されているメディアタイトルのセットと関係付けられており且つそれぞれが対応する証明書を有している 1 つ又はそれ以上のアカウントに関する情報を含んでいる第 2 安全メモリ領域と、を備えており、

前記方法は、

暗号化されているメディアコンテンツにアクセスするための要求と証明書をホストから受け取る段階と、

前記ホストによって提示された証明書を、前記ホストによって要求されている、暗号化されているメディアタイトルが関係付けられている特定のアカウントの証明書と照合する段階と、

前記要求されている、暗号化されているメディアタイトルが見えるように及びアクセスできるようにするべきか否かを判定する段階と、

前記ホストにより提示された証明書が、前記ホストによって要求されている、暗号化されているメディアタイトルが関係付けられている前記特定のアカウントの証明書と一致したときに、前記要求されている、暗号化されているメディアタイトルを復号して、前記復号されたメディアタイトルを前記ホストにレンダリング用に供給する段階と、から成る方法。

【請求項 3 3】

複数のホストによりレンダリングされ得るメディアタイトルを記憶する不揮発性書換可能メモリデバイスによりメディアタイトルを配信するための方法であって、

前記デバイスは、

アクセスがサービスプロバイダによって制御される暗号化されているメディアタイトルを記憶するための第 1 メモリ領域と、前記第 1 メモリ領域に記憶されている前記暗号化されているメディアタイトルへのアクセスを制御する制御情報を記憶するための第 2 安全メモリ領域であって、前記制御情報は、前記サービスプロバイダにより制御されている前記暗号化されているメディアタイトルを識別するための識別情報を含んでいる前記第 2 安全メモリ領域を備えており、

前記方法は、

前記サービスプロバイダと関係付けられている前記暗号化されているメディアタイトルをホストが利用可能か否かを判定するために、当該ホストによって提示された証明書を、前記装置内の前記識別情報と照合する段階と、

前記ホストにより提示された証明書が照合され合格したとき、前記サービスプロバイダと関係付けられている、暗号化されているメディアタイトルを復号して、前記復号されたメディアタイトルを前記ホストにレンダリング用に供給する段階と、から成る方法。

【請求項 3 4】

ホストにより提示された前記証明書は、当該証明書の照合に合格するために、前記サービスプロバイダの前記識別情報を含んでいる、請求項 3 3 に記載の方法。

【請求項 3 5】

前記暗号化されているメディアタイトルは、アカウント識別情報を有する特定のアカウントと関係付けられている、暗号化されたメディアタイトルのセットを含み、前記照合は、ホストにより提示された証明書を前記アカウントの前記識別情報に反していないか否かを調べ、前記ホストにより要求されているメディアタイトルを当該ホストが利用可能か否かを判定し、

暗号化されているメディアタイトルが前記セット内に在ると判定され、及び前記ホスト

10

20

30

40

50

により提示された証明書が前記アカウントの前記識別情報を含んでいるとき、前記ホストにより要求されている、暗号化されているメディアタイトルを復号して、前記復号されたメディアタイトルを前記ホストにレンダリング用に供給する段階を含んでいる、請求項 3 に記載の方法。

【請求項 3 6】

前記アカウントは、エンドユーザーの家族と関係付けられ、前記アカウントの前記識別情報は、前記エンドユーザーの前記家族の識別情報を含み、前記照合は、ホストにより提示された証明書が、前記エンドユーザーの家族の誰かの識別情報を含んでいるか否かの照合を含む、請求項 3 5 に記載の方法。

【請求項 3 7】

前記アカウントは、個別のエンドユーザーと関係付けられ、前記アカウントの前記識別情報は、前記個別のエンドユーザーの識別情報を含み、前記照合は、ホストにより提示された証明書が、前記個別のエンドユーザーの識別情報を含んでいるか否かの照合を含む、請求項 3 5 に記載の方法。

【請求項 3 8】

不揮発性書換可能メモリデバイスにメディアコンテンツをロードするための方法であって、

権利オブジェクトとコンテンツ暗号化鍵を取得する段階と、

前記オブジェクトを、複数の不揮発性書換可能メモリデバイスのそれぞれのメモリ領域にロードする段階と、

引き続き、第 1 メディアコンテンツを、前記複数の不揮発性書換可能メモリデバイスのそれぞれのメモリ領域にロードする段階であって、前記メディアコンテンツは、前記コンテンツ暗号化鍵の内の 1 つ又はそれ以上により暗号化され、前記権利オブジェクトは、前記コンテンツ暗号化鍵へのアクセスを制御する、前記第 1 メディアコンテンツをロードする段階と、から成る方法。

【請求項 3 9】

複数の不揮発性書換可能メモリデバイスのそれぞれのメモリにセキュア領域を作成する段階を更に含み、前記権利オブジェクトは前記セキュア領域にロードされる、請求項 3 8 に記載の方法。

【請求項 4 0】

前記第 1 メディアコンテンツは、前記コンテンツのマスターコピーを生成することによりロードされる、請求項 3 8 に記載の方法。

【請求項 4 1】

前記第 1 メディアコンテンツの前記マスターコピーは、前記コンテンツ暗号化鍵により暗号化されたコンテンツを備えている、請求項 4 0 に記載の方法。

【請求項 4 2】

前記権利オブジェクトをロードする段階は、セキュアファシリティでなされる、請求項 4 0 に記載の方法。

【請求項 4 3】

前記入手する段階は、コンテンツ暗号化鍵を生成する段階と、前記コンテンツ暗号化鍵を権利発行者に送る段階と、前記権利オブジェクトを前記権利発行者から受け取る段階を含んでいる、請求項 3 8 に記載の方法。

【請求項 4 4】

前記デバイスのそれぞれの固有の識別コードを有し、前記デバイスは、それぞれが正の整数である N 個のデバイスを含んでいるセットに分割され、前記セットのそれぞれの、セット識別コードと、当該セットの前記デバイス内の暗号化されているコンテンツへのアクセスを制御するための対応する権利オブジェクトとを有し、各セット識別コードは、前記セットの前記デバイスの前記識別コードから導き出すことができる方法であって、

前記デバイスのそれぞれの前記セット識別コードを、その固有の識別コードから導き出す段階と、

10

20

30

40

50

前記導き出されたセット識別コードに対応する前記権利オブジェクトを、当該デバイスにロードする段階と、を含んでいる、請求項 38 に記載の方法。

【請求項 45】

各デバイスの前記識別コードはそのシリアル番号であり、前記セット識別コードを導き出すことは、前記シリアル番号を事前に決められた数で割る段階を含んでいる、請求項 44 に記載の方法。

【請求項 46】

制約の無いプレビューを許可するために、前記第 1 メディアコンテンツの暗号化されていない部分を前記デバイスにロードする段階を更に含んでいる、請求項 45 に記載の方法。

【請求項 47】

前記権利オブジェクトは、前記暗号化されている第 1 メディアコンテンツの制限されたプレビューを許可する、請求項 46 に記載の方法。

【請求項 48】

前記権利オブジェクトは、前記暗号化されているメディアコンテンツが、制限回数分再生されることを許可している、請求項 47 に記載の方法。

【請求項 49】

複数の不揮発性書換可能メモリデバイスに記憶されている、暗号化されているメディアコンテンツの配信を制御するための方法にあって、前記デバイスは、固有の識別コードを有しており、前記デバイスは、それぞれが N 個のデバイスを含んでいるセットに分割され、前記セットのそれぞれは、セット識別コードと、当該セットの前記デバイス内の暗号化されているコンテンツへのアクセスを制御するための対応する権利オブジェクトとを有し、

前記デバイスの少なくとも 1 つの前記セット識別コードを、その固有の識別コードから導き出す段階と、

前記導き出された識別コードから、前記少なくとも 1 つのデバイス内の暗号化されているコンテンツへのアクセスを制御するための前記権利オブジェクトを識別する段階と、

前記識別された権利オブジェクトをローディング用に前記少なくとも 1 つのデバイスに提供する段階と、から成る方法。

【請求項 50】

各デバイスの前記識別コードはそのシリアル番号であり、前記セット識別コードを導き出すことは、前記シリアル番号を事前に決められた数で割る段階を含んでいる、請求項 49 に記載の方法。

【請求項 51】

不揮発性書換可能メモリカードを使用してメディアコンテンツを配信するための方法にあって、前記カードはメモリ領域を有し、前記カードは、前記カードの前記メモリ領域に記憶されている第 1 メディアコンテンツを備え、前記コンテンツは、少なくとも幾つかのメディアタイトルの選択された暗号化されていない部分又は当該メディアタイトルの低品質の暗号化されていないバージョンだけを含み、前記方法は、

少なくとも幾つかのメディアタイトルの前記選択された暗号化されていない部分又は当該メディアタイトルの低品質の暗号化されていないバージョンをユーザーにレンダリングする段階と、

前記少なくとも幾つかのメディアタイトルのノーカットの又は高品質のバージョン（複数バージョン）にアクセスする権利の購入に関してユーザーに問い合わせを送る段階と、から成る方法。

【請求項 52】

前記メディアタイトルは、前記少なくとも幾つかのメディアタイトルの暗号化されているノーカットの又は高品質のバージョン（複数バージョン）にアクセスする権利の購入に関するコンテンツ情報を含み、前記方法は、前記メディアタイトルから前記情報を取得する段階を更に含み、前記送る段階は、前記問い合わせの一環として前記情報を前記ユーザ

10

20

30

40

50

ーに送る、請求項 5 1 に記載の方法。

【請求項 5 3】

前記少なくとも幾つかのメディアタイトルの前記暗号化されているノーカットの又は高品質のバージョン（複数のバージョン）を受け取る段階と、購入の証明が提供された後、前記少なくとも幾つかのメディアタイトルの前記暗号化されているバージョン（複数のバージョン）に関する前記権利及び／又は規則を実行する段階を更に含んでいる、請求項 5 2 に記載の方法。

【請求項 5 4】

不揮発性書換可能メモリカードを使用してメディアコンテンツを配信するための方法であって、前記カードはメモリ領域とセキュアメモリ領域を有し、前記カードは、前記カードの前記メモリ領域に記憶されている第 1 メディアコンテンツを備え、前記コンテンツは、少なくとも幾つかのメディアタイトルの選択された暗号化されていない部分又は当該メディアタイトルの低品質の暗号化されていないバージョンだけを含み、前記方法は、

前記少なくとも幾つかのメディアタイトルの暗号化されているバージョン（複数バージョン）であって、前記 1 つ又は複数のコンテンツ暗号化鍵（複数鍵）により暗号化されたバージョンが関与する 1 つ又は複数のコンテンツ暗号化鍵（複数鍵）と権利及び／又は規則を受け取る段階と、

前記権利及び／又は規則を前記セキュアメモリ領域に記憶する段階と、から成る方法。

【請求項 5 5】

前記少なくとも幾つかのメディアタイトルの前記暗号化されているバージョン（複数バージョン）を受け取る段階と、前記少なくとも幾つかのメディアタイトルの前記暗号化されているバージョン（複数バージョン）に関する前記権利及び／又は規則を実行する段階を更に含んでいる、請求項 5 4 に記載の方法。

【請求項 5 6】

不揮発性書換可能メモリカードを使用してメディアコンテンツを配信するための方法であって、前記カードはメモリ領域を有し、前記カードは、前記カードの前記メモリ領域に記憶されている第 1 メディアコンテンツを備え、前記コンテンツは、少なくとも幾つかのメディアタイトルの選択された暗号化されていない部分又は当該メディアタイトルの低品質の暗号化されていないバージョンだけを含み、前記方法は、

1 つ又は複数のコンテンツ暗号化鍵（複数鍵）により暗号化されている少なくとも幾つかのメディアタイトルを受け取る段階と、

前記暗号化されている少なくとも幾つかのメディアタイトルを前記メモリ領域に記憶する段階と、から成る方法。

【請求項 5 7】

前記暗号化されている少なくとも幾つかのメディアタイトルが関与する前記 1 つ又は複数のコンテンツ暗号化鍵（複数鍵）と権利及び／又は規則を受け取る段階と、前記権利及び／又は規則を前記セキュアメモリ領域に記憶する段階と、前記暗号化されている少なくとも幾つかのメディアタイトルに関する前記権利及び／又は規則を実行する段階を更に含んでいる、請求項 5 6 に記載の方法。

【請求項 5 8】

前記権利及び／又は規則は、前記少なくとも幾つかの暗号化されているメディアタイトルの購入の証明後に、前記 1 つ又は複数のコンテンツ暗号化鍵（複数鍵）へのアクセスを許可し、前記方法は、前記 1 つ又は複数のコンテンツ暗号化鍵（複数鍵）へのアクセスを提供する段階と、前記少なくとも幾つかの暗号化されているメディアタイトルを、当該タイトルの購入の証明が提供された後に、当該鍵（複数鍵）を使用して、復号する段階を更に含んでいる、請求項 5 7 に記載の方法。

【請求項 5 9】

不揮発性書換可能メモリカードを使用してメディアコンテンツを配信するための方法であって、前記カードはメモリ領域を有し、前記カードは、前記カードの前記メモリ領域に記憶されているメディアコンテンツを備え、前記コンテンツは、1 つ又は複数のコンテン

10

20

30

40

50

ッ暗号化鍵（複数鍵）を使用して暗号化されている少なくとも幾つかのメディアタイトルを含み、前記方法は、

前記カードに記憶されている前記メディアコンテンツが関与する前記１つ又は複数のコンテンツ暗号化鍵（複数鍵）と権利及び／又は規則を受け取る段階と、

前記権利及び／又は規則を前記カードのセキュアメモリ領域に記憶する段階と、から成る方法。

【請求項 60】

前記暗号化されている少なくとも幾つかのメディアタイトルを、前記権利及び／又は規則に従って復号するために、前記１つ又は複数のコンテンツ暗号化鍵（複数鍵）を使用する段階を更に含んでいる、請求項 59 に記載の方法。

10

【請求項 61】

不揮発性書換可能メモリカードを使用してメディアコンテンツを配信するための方法であって、前記カードはメモリ領域を有し、前記カードは、前記カードの前記メモリ領域に記憶されているメディアコンテンツを備え、前記コンテンツは、少なくとも幾つかのメディアタイトルを含み、前記方法は、

前記少なくとも幾つかのメディアタイトルに時間制限内にアクセスすることを許容する段階と、

前記少なくとも幾つかのメディアタイへのアクセスを追跡する段階と、

前記追跡されたアクセスに基づいてアクセスプロファイルをコンパイルする段階と、から成る方法。

20

【請求項 62】

前記少なくとも幾つかのメディアタイトルは、１つ又は複数のコンテンツ暗号化鍵（複数鍵）を使用して暗号化され、前記カードは、前記アクセスプロファイルがダウンロードされると、少なくとも幾つかのメディアタイトルへの時間制限アクセスに対して延長を提供する権利及び／又は規則を記憶している、請求項 61 に記載の方法。

【請求項 63】

前記少なくとも幾つかのメディアタイトルは、１つ又は複数のコンテンツ暗号化鍵（複数鍵）を使用して暗号化され、前記時間制限又はその延長中に、前記１つ又は複数のコンテンツ暗号化鍵（複数鍵）へのアクセスを許可することによって、時間制限アクセスが許容されるか延長される、請求項 62 に記載の方法。

30

【請求項 64】

不揮発性書換可能メモリカードを使用してメディアコンテンツを配信するための方法であって、前記カードはメモリ領域を有し、前記カードは、前記カードに記憶されるメディアコンテンツが関与する１つ又は複数のコンテンツ暗号化鍵（複数鍵）と権利及び／又は規則を備え、前記方法は、

前記メディアコンテンツを受け取る段階であって、当該コンテンツは、１つ又は複数のコンテンツ暗号化鍵（複数鍵）を使用して暗号化されている少なくとも幾つかのメディアタイトルを含んでいる、メディアコンテンツを受け取る段階と、

前記メディアコンテンツを前記カードの前記メモリ領域に記憶する段階と、から成る方法。

40

【請求項 65】

複数のダウンロードが前記権利及び／又は規則により許可されるとき、前記メディアコンテンツを複数回受け取る段階を更に含んでいる、請求項 64 に記載の方法。

【請求項 66】

不揮発性書換可能メモリデバイス内の権利オブジェクトをバックアップ及び復元するための方法であって、前記権利オブジェクトは、第１の証明書が前記デバイスに提示されたときには、読取専用機能についてアクセス可能になり、前記第１の証明書とは異なる第２の証明書が前記デバイスに提示されたときには、変更又は消去又はバックアップ／復元させるためにアクセス可能になるような方法で、前記デバイスに記憶され、

前記第２の証明書を前記デバイスに提示する段階と、

50

前記権利オブジェクトをバックアップする段階と、

前記第 2 の証明書が前記デバイスに提示されない限り、前記権利オブジェクトにアクセスして変更又は消去又はバックアップ／復元できないように、前記権利オブジェクトを前記デバイスに復元する段階と、から成る方法。

【請求項 67】

前記デバイスは、前記第 2 の証明書が提示されたとき、前記権利オブジェクトを変更又は消去するために前記権利オブジェクトへアクセスすることを許可する、請求項 66 に記載の方法。

【請求項 68】

前記バックアップする段階は、

前記権利オブジェクトを復号する段階と、

前記復号された権利オブジェクトをセッション鍵により暗号化する段階と、

前記権利オブジェクトを前記セッション鍵を使用して復号する段階と、

前記復号された権利オブジェクトを鍵により暗号化し、前記暗号化された権利オブジェクトをバックアップ記憶領域に記憶する段階とを含んでいる、前記権利オブジェクトが暗号化されている、請求項 66 に記載の方法。

【請求項 69】

前記バックアップする段階は、前記権利オブジェクトを前記デバイスから削除する段階を含んでいる、請求項 66 に記載の方法。

【請求項 70】

前記バックアップする段階は、前記権利オブジェクトをバックアップ記憶領域に記憶する段階を含み、前記復元する段階は、更に、前記権利オブジェクトを前記バックアップ記憶領域から削除する段階を含んでいる、請求項 66 に記載の方法。

【請求項 71】

不揮発性書換可能メモリデバイス内の権利オブジェクトを制御するための方法であって、前記権利オブジェクトは、第 1 の証明書が前記デバイスに提示されたときには、読取専用機能についてアクセス可能になり、前記第 1 証明書とは異なる第 2 の証明書が前記デバイスに提示されたときには、変更又は消去するためにアクセス可能になるような方法で、前記デバイスに記憶され、

前記第 2 の証明書を前記デバイスに提示する段階と、

前記権利オブジェクトを変更し又は消去する段階と、から成る方法。

【請求項 72】

前記デバイスは前記権利オブジェクトにより制御される暗号化されているメディアコンテンツを記憶し、前記権利オブジェクトは、前記コンテンツがどの様に使用され及び／又はアクセスされるかを指定し、且つ n を正の整数として、前記権利オブジェクトからコピーが n 個だけ作成されることを指定している規則を含み、前記方法は、前記権利オブジェクトを記憶領域にコピーし、 m をゼロ又は n より小さい正の整数として、 $(n - m)$ 個だけの前記権利オブジェクトのコピーが前記記憶領域内に前記コピーされた権利オブジェクトから更に作成される、ということを指定する規則を、前記記憶領域にコピーされた前記オブジェクトが含むようにする段階を更に含んでいる、請求項 71 に記載の方法。

【請求項 73】

前記権利オブジェクトが 1 つ又は複数の記憶領域にコピーされる時、前記デバイス内の前記権利オブジェクトの前記規則は、前記権利オブジェクトのコピーが m 個だけ作成されることを指定するように更新される、請求項 72 に記載の方法。

【請求項 74】

前記権利オブジェクトは、それからは一切コピーが作成されないことを指定し、前記方法は、当該オブジェクトがコピーされた後には、当該オブジェクトを削除し又は当該オブジェクトを変更し、当該オブジェクトにより制御されている前記メディアコンテンツは、当該コンテンツにアクセスしてレンダリング又は再生を行うために読み取ることはできないと表示する段階を更に含んでいる、請求項 72 に記載の方法。

10

20

30

40

50

【請求項 75】

前記コピーする段階及び更新する段階は、DRM性能を有するアプリケーションによって実行される、請求項72に記載の方法。

【請求項 76】

前記方法は、

前記権利オブジェクトを復号する段階と、

前記復号された権利オブジェクトをセッション鍵により暗号化する段階と、

前記権利オブジェクトを、前記セッション鍵を使って記憶領域で復号する段階と、

前記復号された権利オブジェクトを鍵により暗号化し、前記暗号化された権利オブジェクトを前記記憶領域に記憶する段階を更に含んでいる、前記権利オブジェクトが暗号化されている、請求項71に記載の方法。

10

【請求項 77】

不揮発性書換可能メモリカードを使用してメディアコンテンツを配信できるようにするための方法であって、

不揮発性書換可能メモリカードにアクセスしているアプリケーションの証明書を、それがそうすることを認可されているか否かを判定するために照合する段階と、

前記アプリケーションの前記証明書が要件を満たさない場合は、前記アプリケーションが前記不揮発性書換可能メモリカードにアクセスすることを認可されていないことを示す表示を提供する段階と、から成る方法。

20

【請求項 78】

コンピュータシステムにより実行され、前記システムは、エンティティにより提供されているアプリケーションの事前に決められている証明書の一覧を保存し、前記コンピュータは、前記アプリケーションの証明書を前記事前に決められている証明書の一覧と照合する、請求項77に記載の方法。

【請求項 79】

セキュアメモリ領域と少なくとももう一つのメモリ領域を有している不揮発性書換可能メモリデバイスであって、前記デバイスは、

前記セキュアメモリ領域に記憶されている1つ又は複数のコンテンツ暗号化鍵（複数鍵）と、

前記デバイスのメモリ領域に記憶されているコンテンツであって、前記コンテンツ暗号化鍵（複数鍵）により暗号化されているメディアタイトルの第1セットと、前記第1セット内の前記メディアタイトルの選択された部分及び／又は当該タイトルの制約無しにアクセスできる低品質バージョンと、を含み

30

前記第1セット内の前記メディアタイトルへのアクセスを制御するコントローラと、を備えているメモリデバイス。

【請求項 80】

前記暗号化されているメディアタイトルの第1セットは、購入の証明無しにアクセスすることはできない、請求項79に記載のデバイス。

【請求項 81】

前記コントローラは、前記コンテンツ暗号化鍵（複数鍵）にアクセスを提供し、当該権利及び／又は規則を前記デバイスの前記セキュアメモリ領域に記憶することによって前記第1セット内の前記暗号化されているメディアタイトルを復号するために認証情報及び当該権利及び／又は規則に関する情報に応答する、請求項80に記載のデバイス。

40

【請求項 82】

前記デバイスを操作するホスト上のアプリケーションは、購入の証明が与えられた後に、前記認証情報が提供される、請求項81に記載のデバイス。

【請求項 83】

前記権利及び／又は規則は、前記第1セット内の1つ又は複数の暗号化されているメディアタイトルを復号するための1つ又は複数のコンテンツ暗号化鍵へのアクセスを許可する、請求項81に記載のデバイス。

50

【請求項 8 4】

ホスト上のアプリケーションは前記デバイス进行操作し、前記権利及び／又は規則は、前記アプリケーションが前記復号されたメディアタイトルを再生するのを許可する、請求項 8 3 に記載のデバイス。

【請求項 8 5】

ホスト上のアプリケーションは前記デバイス进行操作し、前記権利及び／又は規則は、前記アプリケーションが、前記復号されたメディアタイトルを制限回数エクスポートするか又は制限部数のコピーを記憶用に作成することを許可する、請求項 8 3 に記載のデバイス。

【請求項 8 6】

前記デバイスの正常な動作中に、事前に決められている証明書が提示される時、前記デバイスの外部のエンティティにとってアクセス可能となる前記セキュアメモリ領域のパーティションに、前記権利及び／又は規則が記憶される、請求項 8 1 に記載のデバイス。

【請求項 8 7】

前記デバイスは、フラッシュメモリカードを備えている、請求項 7 9 に記載のデバイス。

【請求項 8 8】

前記第 1 セット内の前記メディアタイトルの前記選択された部分又は当該タイトルの低品質バージョンのコピーは、前記第 1 セット内の前記暗号化されているメディアタイトルとは別のファイルに記憶される、請求項 7 9 に記載のデバイス。

【請求項 8 9】

前記デバイスの正常な動作中には前記デバイスの外部のエンティティにとってアクセス可能ではない前記セキュアメモリ領域のパーティションに、前記 1 つ又は複数のコンテンツ暗号鍵（複数鍵）が記憶される、請求項 7 9 に記載のデバイス。

【請求項 9 0】

前記コンテンツは、前記コンテンツ暗号化鍵（複数鍵）により暗号化されているメディアタイトルの第 2 セットを更に備え、前記デバイスは、前記デバイスの前記セキュアメモリ領域に記憶されている前記メディアタイトルの第 2 セットに関する権利及び／又は規則を更に備え、当該権利及び／又は規則は、前記メディアタイトルの前記第 2 セットが、制限回数だけアクセス可能であることを指定している、請求項 7 9 に記載のデバイス。

【請求項 9 1】

前記メディアタイトルの第 2 セットに関する前記権利及び／又は規則は、前記第 2 セット内の 1 つ又は複数の暗号化されているメディアタイトルを復号するために、前記 1 つ又は複数のコンテンツ暗号化鍵への制限回数だけのアクセスを許可する、請求項 9 0 に記載のデバイス。

【請求項 9 2】

ホスト上のアプリケーションは前記デバイス进行操作し、前記権利及び／又は規則は、前記アプリケーションが、前記復号されたメディアタイトルを前記制限回数だけレンダリングすることを許可する、請求項 9 1 に記載のデバイス。

【請求項 9 3】

前記メディアタイトルはファイルに編成され、各ファイルは対応するコンテンツ暗号化鍵により暗号化され、前記デバイスは、前記ファイルの内の少なくとも幾つかのそれぞれにつき、当該ファイルの前記対応するコンテンツ暗号鍵へのアクセスを制御するアクセス制御記録を更に備えている、請求項 7 9 に記載のデバイス。

【請求項 9 4】

前記アクセス制御記録のそれぞれは、それにより制御される前記コンテンツ暗号化鍵へのアクセス、及び当該鍵を使用するための許可及び／又は制約を得るために必要となる証明書に関する情報を備えている、請求項 9 3 に記載のデバイス。

【請求項 9 5】

前記アクセス制御記録の少なくとも 1 つの前記許可（複数の許可）は、コンテンツ暗号

10

20

30

40

50

化鍵にアクセスする許可を別のアクセス制御記録に委譲する許可を備えている、請求項 9 4 に記載のデバイス。

【請求項 9 6】

前記メディアタイトルの第 1 セットが関与する前記セキュアメモリ領域に記憶されている、権利及び／又は規則を更に備え、

前記権利及び／又は規則は、前記第 1 セット内の前記メディアタイトルの少なくとも幾つかの選択された部分又は当該タイトルの低品質バージョンだけが制約無しにアクセスできることを、又は当該タイトルは制限回数だけ再生できることを指定し、

前記コントローラは、前記デバイスに記憶されている前記第 1 セット内の何れのメディアタイトルに関する前記権利及び／又は規則でも実行する、請求項 7 9 に記載のデバイス。

10

【請求項 9 7】

ホスト上のアプリケーションは前記デバイスを操作し、前記権利及び／又は規則は、前記アプリケーションが、前記第 1 セット内の前記復号されたメディアタイトルを制限回数だけエクスポートすることを許可する、請求項 9 6 に記載のデバイス。

【請求項 9 8】

前記デバイスに記憶されている前記第 1 セット内の 1 つ又は複数の暗号化されているメディアタイトルへのアクセスを許可するために、前記コントローラは、認証情報に応答して前記コンテンツ暗号化鍵（複数鍵）へのアクセスを提供するための前記権利及び／又は規則を変更する、請求項 9 6 に記載のデバイス。

20

【請求項 9 9】

前記コントローラは、前記認証情報に応答して、前記第 1 セット内の 1 つ又は複数の暗号化されているメディアタイトルを復号するために、前記 1 つ又は複数のコンテンツ暗号化鍵へのアクセスを許可するための、前記権利及び／又は規則を変更する、請求項 9 6 に記載のデバイス。

【請求項 1 0 0】

前記コントローラは、前記認証情報に応答して、前記第 1 セット内の前記 1 つ又は複数のメディアタイトルを復号するために、前記コンテンツ暗号化鍵（複数鍵）の 1 つ又はそれ以上への無制約のアクセスを許可するための、前記権利及び／又は規則を変更する、請求項 9 9 に記載のデバイス。

30

【請求項 1 0 1】

前記第 1 セット内の前記メディアタイトルの選択された部分又は当該タイトルの低品質バージョンのコピーは、制約無しにアクセス可能であり、前記暗号化されているメディアタイトルとは別のファイルに記憶される、請求項 9 6 に記載のデバイス

【請求項 1 0 2】

前記権利及び／又は規則は、前記 1 つ又は複数のコンテンツ暗号化鍵（複数鍵）へのアクセスが、暗号化されているコンテンツの購入の証明が提供された後にしか許可されないことを指定する、請求項 9 6 に記載のデバイス。

【請求項 1 0 3】

前記権利及び／又は規則は、暗号化されているコンテンツの購入の証明が提供された後に、前記 1 つ又は複数のコンテンツ暗号化鍵（複数鍵）へのアクセスを許可するために変更され得る、請求項 9 6 に記載のデバイス。

40

【請求項 1 0 4】

前記コントローラは、前記コンテンツ暗号鍵（複数鍵）へのアクセスを提供し、前記第 1 セット内の前記暗号化されているメディアタイトルを復号するために、前記デバイスの前記セキュアメモリ領域内の当該権利及び／又は規則を更新することによって、認証情報、及び前記権利及び／又は規則の更新に関する情報に応答する、請求項 9 6 に記載のデバイス。

【請求項 1 0 5】

前記更新された権利及び／又は規則は、前記第 1 セット内の前記暗号化されているメデ

50

ィアタイトルを復号するために、前記コンテンツ暗号化鍵（複数鍵）へアクセスする際の無制約又は更に緩い制約を許可する、請求項 9 6 に記載のデバイス。

【請求項 1 0 6】

暗号化されているメディアコンテンツを記憶する第 1 メモリ領域、及び 1 つ又は複数の制御構造を記憶する第 2 安全メモリ領域と、

前記デバイスに記憶され、サービスプロバイダが、前記第 1 メモリ領域に記憶されている、暗号化されているコンテンツへのアクセスを制御するために、前記デバイスの前記セキュアメモリ領域内に制御構造を作成できるようにする、システムエージェントと、

前記デバイスの前記セキュアメモリ領域内に前記制御構造を作成するためのセッション内で前記サービスプロバイダと通信するコントローラと、を備えている不揮発性書換可能メモリデバイス。

10

【請求項 1 0 7】

前記制御構造を作成するための前記サービスプロバイダとのセキュアセッションを可能とする証明書を更に備え、前記証明書は前記デバイスの前記セキュアメモリ領域に記憶される、請求項 1 0 6 に記載の不揮発性書換可能メモリデバイス。

【請求項 1 0 8】

前記デバイスを認証可能とする証明書を更に備えている、請求項 1 0 6 に記載のデバイス。

【請求項 1 0 9】

前記エージェントは、2 つ以上のサービスプロバイダが、対応する制御構造を前記デバイスの前記セキュアメモリ領域内に作成できるようにする、請求項 1 0 6 に記載のデバイス。

20

【請求項 1 1 0】

前記デバイスは、対応する複数のサービスプロバイダのために作成された複数の制御構造を前記デバイスの前記セキュアメモリ領域に記憶し、前記複数のサービスプロバイダは互いに独立して前記デバイスとやりとりをする、請求項 1 0 9 に記載のデバイス。

【請求項 1 1 1】

前記デバイスは、異なるサービスプロバイダにより作成された、対応する制御構造を記憶するために、前記セキュアメモリ領域内に別々のパーティションを備え、各パーティションはその対応するサービスプロバイダの前記制御構造だけを記憶する、請求項 1 1 0 に記載のデバイス。

30

【請求項 1 1 2】

前記パーティションは、前記パーティションの内の少なくとも幾つかのそれぞれには、当該パーティションに記憶されている前記制御構造の前記対応するサービスプロバイダはアクセスできるが、他のサービスプロバイダはアクセスできないようになっている、請求項 1 1 1 に記載のデバイス。

【請求項 1 1 3】

前記デバイスは、前記第 1 メモリ領域内の前記複数のサービスプロバイダの内の少なくとも幾つかと関係付けられている、暗号化されているメディアコンテンツを記憶し、前記サービスプロバイダのそれぞれと関係付けられている、暗号化されているメディアコンテンツへのアクセスは、当該サービスプロバイダによりその対応する制御構造を介して排他的に制御される、請求項 1 1 0 に記載のデバイス。

40

【請求項 1 1 4】

前記サービスプロバイダのそれぞれと関係付けられている、前記暗号化されているメディアコンテンツには、他の何れのサービスプロバイダもアクセスできない、請求項 1 1 3 に記載のデバイス。

【請求項 1 1 5】

前記コントローラは、前記制御構造が作成された後に、前記サービスプロバイダによって提供されるメディアコンテンツを、前記デバイスに記憶する、請求項 1 0 6 に記載のデバイス。

50

【請求項 1 1 6】

前記サービスプロバイダにより提供された前記コンテンツへのアクセスは、前記制御構造により制御されている、請求項 1 1 5 に記載のデバイス。

【請求項 1 1 7】

前記デバイスは、異なるデジタル権利管理システムをサポートすることができるインターフェースを備えている、請求項 1 0 6 に記載のデバイス。

【請求項 1 1 8】

ホストは、前記デバイスに記憶されている、前記暗号化されているコンテンツをレンダリングするために前記デバイスを操作し、前記インターフェースは、異なるデジタル権利管理システムをサポートすることができ、これにより、前記ホストが当該能力を欠いていても、前記デバイスとホストが前記暗号化されたコンテンツをレンダリングできるようにする、請求項 1 1 7 に記載のデバイス。

10

【請求項 1 1 9】

前記制御構造は、前記第 1 メモリ領域に記憶されている、暗号化されたコンテンツにアクセスするための権利及び／又は規則を含み、前記権利及び／又は規則は、ユーザー又はホスト、又はユーザー又はホストのグループが、前記暗号化されているコンテンツにアクセスすることを許可する、請求項 1 0 6 に記載のデバイス。

【請求項 1 2 0】

前記デバイスは、固有の ID を備えている、請求項 1 0 6 に記載のデバイス。

【請求項 1 2 1】

前記デバイスに記憶されているコンテンツを暗号化するために、前記デバイスに記憶されている 1 つ又は複数のコンテンツ暗号化鍵を更に備え、前記制御構造は、前記 1 つ又は複数のコンテンツ暗号化鍵へのアクセスを制御する、請求項 1 0 6 に記載のデバイス。

20

【請求項 1 2 2】

前記デバイスに記憶されているメディアタイトルを更に備え、前記メディアタイトルの少なくとも幾つかは、前記 1 つ又は複数のコンテンツ暗号化鍵の内の少なくとも 1 つを使用して暗号化されている、請求項 1 2 1 に記載のデバイス。

【請求項 1 2 3】

前記制御構造は、前記少なくとも 1 つのコンテンツ暗号化鍵へのアクセスの権利及び／又は規則を含み、前記権利及び／又は規則は、ユーザー又はホスト、又はユーザー又はホストのグループが、前記少なくとも 1 つのコンテンツ暗号化鍵にアクセスすることを許可する、請求項 1 2 2 に記載のデバイス。

30

【請求項 1 2 4】

前記制御構造は、前記第 1 メモリ領域に記憶されている、暗号化されたメディアコンテンツへのアクセスは、事前に決められている証明書が提示されたときに、暗号化されているメディアコンテンツへのアクセスのために、単一又は複数のエンティティに対して許容されることを指定する、請求項 1 0 6 に記載のデバイス。

【請求項 1 2 5】

前記制御構造は、対応するエンティティのセットによる、前記第 1 メモリ領域に記憶されている、暗号化されているメディアコンテンツへのアクセスを制御する、異なるレベルのノードを備えている階層ツリーを備え、前記ツリーのノードは、事前に決められている証明書が提示されたときに、対応する単数又は複数のエンティティが暗号化されているメディアコンテンツにアクセスする許可（複数の許可）を指定し、前記ツリーの或るノードにおける許可（複数の許可）は、前記同じツリー内の上位又は下位レベルの別のノードにおける許可（複数の許可）に対する事前に決められた関係を有する、請求項 1 2 4 に記載のデバイス。

40

【請求項 1 2 6】

前記ツリーの或るノードは、前記サービスプロバイダにより信頼されている対応するアプリケーションが暗号化されているメディアコンテンツにアクセスする許可（複数の許可）を指定する、請求項 1 2 5 に記載のデバイス。

50

【請求項 1 2 7】

前記デバイスに記憶されている、前記暗号化されたメディアコンテンツを復号するのに有用な 1 つ又は複数のコンテンツ暗号化鍵を更に備え、対応する信頼されているアプリケーションの前記許可（複数の許可）は、当該アプリケーションに対して事前に決められている証明書が前記デバイスに提示されると、当該アプリケーションが、前記暗号化されているメディアコンテンツを復号するために、前記 1 つ又は複数のコンテンツ暗号化鍵にアクセスすることを許可する、請求項 1 2 6 に記載のデバイス。

【請求項 1 2 8】

前記エージェントは、複数のサービスプロバイダそれぞれが、前記デバイスの前記第 2 安全メモリ領域に対応する制御構造を作成できるようにし、各制御構造は対応する階層ツリーを備え、前記ツリーの内の少なくとも 2 つの間にはクロストークが存在せず、当該 2 つのツリーを作成した前記 2 つの対応するサービスプロバイダは、互いに独立して前記デバイスと対話する、請求項 1 2 5 に記載のデバイス。

【請求項 1 2 9】

暗号化されているメディアコンテンツを記憶するための第 1 メモリ領域、及び 1 つ又は複数の制御構造を記憶するための第 2 安全メモリ領域と、

前記装置に記憶されているシステムエージェントであって、サービスプロバイダが、前記第 1 メモリ領域に記憶されている、暗号化されたコンテンツへのアクセスを制御するために、前記デバイスの前記セキュアメモリ領域内に制御構造を作成できるようにする機能を有し、

前記デバイスの前記セキュアメモリ領域内に前記制御構造を作成するためのセッションで前記サービスプロバイダと通信することができるコントローラと、を備えている不揮発性書換可能メモリデバイス。

【請求項 1 3 0】

複数のホストによりレンダリングされるメディアタイトルを記憶している不揮発性書換可能メモリデバイスであって、

暗号化されているメディアコンテンツを記憶するための第 1 メモリ領域および前記暗号化されているメディアタイトルへのアクセスを制御する制御情報を記憶するための第 2 安全メモリ領域であって、前記制御情報は、1 つ又は複数のアカウントに関する情報を含み、各アカウントは前記第 1 メモリ領域に記憶されている、暗号化されたメディアタイトルのセットと関係付けられ、各アカウントは対応する証明書を有し、

前記セキュアメモリ領域に記憶されている制御構造であって、特定のアカウントと関係付けられている、暗号化されたメディアタイトルの前記セットが、当該アカウントに対応する証明書を提示するユーザーだけに見えてアクセスできるようになるのを許可し、

前記ホストと通信し及び前記ホストによって提示された証明書を照合し、特定のアカウントと関係付けられている、暗号化されているメディアタイトルを、見ることができアクセスすることができるようにすべきか否かを判定するコントローラと、を備えているメモリデバイス

【請求項 1 3 1】

サービスプロバイダと関係付けられ且つサービスプロバイダによって許容される前記アカウントそれぞれに、関係付けられている証明書を有する固有の ID を更に備えている、請求項 1 3 0 に記載のデバイス。

【請求項 1 3 2】

前記サービスプロバイダは、前記第 1 メモリ領域の暗号化されているメディアタイトルへのアクセスを、前記アカウントによって、それらの ID、関係付けられている証明書及び前記制御構造を介して制御する、請求項 1 3 1 に記載のデバイス。

【請求項 1 3 3】

前記デバイスは、その中の前記メディアタイトルをレンダリングするために異なるホストにより作動させることができ、前記制御構造は、当該アカウントの証明書が当該ホストを通して前記デバイスに提示されると、前記異なるホストが特定のアカウントと関係付け

10

20

30

40

50

られている前記メディアタイトルをレンダリングすることを許可する、請求項 130 に記載のデバイス。

【請求項 134】

メモリ領域を有している不揮発性書換可能メモリカードであって、
前記カードは、

少なくとも幾つかのメディアタイトルの選択された暗号化されていない部分又は当該メディアタイトルの低品質の暗号化されていないバージョンだけを含み、前記カードの前記メモリ領域に記憶されているコンテンツと、

前記カードに記憶されている前記メディアコンテンツへアクセスでき、前記メディアコンテンツがホストによりレンダリングされることができるようにするコントローラと、を備えているメモリカード。

10

【請求項 135】

前記カードは、

セキュアメモリ領域と、

前記カードに記憶されることになる暗号化されているメディアコンテンツに関与する、1つ又は複数のコンテンツ暗号化鍵（複数鍵）及び権利及び／又は規則であって、前記権利及び／又は規則は前記セキュアメモリ領域に記憶されているコンテンツ暗号化鍵（複数鍵）及び権利及び／又は規則を更に備え、

前記コントローラは、前記カードに記憶されている何れかの暗号化されているメディアタイトルに関して、前記権利及び／又は規則を実行する請求項 134 に記載のカード。

20

【請求項 136】

前記カードは、前記 1つ又は複数のコンテンツ暗号化鍵（複数鍵）により暗号化され且つ前記カードに記憶されている少なくとも幾つかのメディアタイトルを更に備え、前記権利及び／又は規則は、当該タイトルが前記 1つ又は複数のコンテンツ暗号化鍵（複数鍵）を使用して、制限回数だけ再生できることを指定する、請求項 135 に記載のカード。

【請求項 137】

前記カードは、1つ又は複数のコンテンツ暗号化鍵（複数鍵）により暗号化されている少なくとも幾つかのメディアタイトルを更に備えている、請求項 134 に記載のカード。

【請求項 138】

前記カードは、セキュアメモリ領域を更に備えて、前記コントローラは、前記暗号化されているメディアタイトルが関与する前記 1つ又は複数のコンテンツ暗号化鍵（複数鍵）と権利及び／又は規則を受け取り、前記コントローラは、前記権利及び／又は規則を前記セキュアメモリ領域に記憶し、及び前記暗号化されているメディアタイトルに関して、前記権利及び／又は規則を実行する、請求項 137 に記載のカード。

30

【請求項 139】

前記権利及び／又は規則は、前記コントローラが、認証情報に応じて、前記コンテンツ暗号化鍵（複数鍵）へのアクセスを提供することを許可し、前記暗号化されているメディアタイトルへのアクセスが許可されるようにする、請求項 138 に記載のカード。

【請求項 140】

メモリ領域を有する不揮発性書換可能メモリカードであって、

40

前記カードの前記メモリ領域に記憶され、1つ又は複数のコンテンツ暗号化鍵（複数鍵）を使用して暗号化されている少なくとも幾つかのメディアタイトルを含んでいるメディアコンテンツと、

前記 1つ又は複数のコンテンツ暗号化鍵（複数鍵）が前記カードに提供されたとき、前記カードに記憶されている前記第 1 コンテンツへアクセスできるようにするコントローラと、を備えているメモリカード。

【請求項 141】

前記カードは、

セキュアメモリ領域と、

前記カードに記憶されている暗号化されているメディアコンテンツに関与する、前記 1

50

つ又は複数のコンテンツ暗号化鍵（複数鍵）及び権利及び／又は規則であって、前記権利及び／又は規則は前記セキュアメモリ領域に記憶されているコンテンツ暗号化鍵（複数鍵）及び権利及び／又は規則と、
を更に備える、請求項 1 4 0 に記載のカード。

【請求項 1 4 2】

前記コントローラは、前記少なくとも幾つかの暗号化されたメディアタイトルに関して、前記権利及び／又は規則を実行する、請求項 1 4 1 に記載のカード。

【請求項 1 4 3】

前記カードに記憶されている前記メディアコンテンツへのアクセスを追跡し、前記メディアコンテンツに関して前記カード内にアクセスプロファイルを記録する追跡エージェントを更に備えており、前記権利及び／又は規則は、前記アクセスプロファイルをダウンロードするために、周期的に前記カードとサーバの間の接続を要求する、請求項 1 4 1 に記載のカード。

10

【請求項 1 4 4】

前記権利及び／又は規則は、前記カードに記憶されているメディアコンテンツへの時間限定アクセスを許容し、前記時間限定アクセスは、前記カードとサーバの接続に成功し、及び前記アクセスプロファイルのダウンロードに成功すると、延長可能となる、請求項 1 4 3 に記載のカード。

【請求項 1 4 5】

前記権利及び／又は規則は、前記 1 つ又は複数のコンテンツ暗号化鍵（複数鍵）へのアクセスを許容することにより、前記カードに記憶されているメディアコンテンツへのアクセスを許容する、請求項 1 4 3 に記載のカード。

20

【請求項 1 4 6】

メモリ領域を有する不揮発性書換可能メモリカードであって、

前記カードは、

セキュアメモリ領域と、

前記カードに記憶されている暗号化されているメディアコンテンツに関与する、1 つ又は複数のコンテンツ暗号化鍵（複数鍵）及び権利及び／又は規則であって、前記権利及び／又は規則は前記セキュアメモリ領域に記憶されているコンテンツ暗号化鍵（複数鍵）及び権利及び／又は規則と、
を備えているメモリカード。

30

【請求項 1 4 7】

前記カードの前記メモリ領域に記憶され、前記 1 つ又は複数のコンテンツ暗号化鍵（複数鍵）を使用して暗号化された少なくとも幾つかのメディアタイトルを含んでいる、メディアコンテンツと、

前記 1 つ又は複数のコンテンツ暗号化鍵（複数鍵）が前記カードに提供されると、前記カードに記憶されている前記第 1 コンテンツへアクセスできるようにするコントローラと、
を備えている、請求項 1 4 6 に記載のカード。

【請求項 1 4 8】

暗号化されているメディアコンテンツを記憶するための第 1 メモリ領域と、

第 2 安全メモリ領域と、

前記第 1 メモリ領域に記憶されている、暗号化されているメディアコンテンツへのアクセスを制御するための、前記第 2 メモリ領域に記憶されている少なくとも 1 つの権利オブジェクトと、を備え、

40

前記第 2 メモリ領域には、前記少なくとも 1 つの権利オブジェクトのバックアップと復元のために、認可されているアプリケーションだけがアクセスすることができる、不揮発性書換可能メモリデバイス。

【請求項 1 4 9】

前記第 2 メモリ領域は、事前に決められている証明書を有するものを除き、全てのアプリケーションから隠されアクセスすることができないパーティションである、請求項 1 4

50

8に記載のデバイス。

【請求項150】

前記少なくとも1つの権利オブジェクトのバックアップと復元のために前記第2メモリ領域へアクセスするためには、読取機能のために前記第2メモリ領域へアクセスするのに提示することが要求されるものとは異なる証明書の提示を必要とする、請求項149に記載のデバイス。

【請求項151】

前記第2メモリ領域は、読取機能のために第1アプリケーションによってアクセスすることができ、前記少なくとも1つの権利オブジェクトのバックアップ及び復元のためには、前記第1アプリケーションとは異なる第2アプリケーションだけがアクセスすることができる、請求項148に記載のデバイス。

10

【請求項152】

前記権利オブジェクトは、第1の証明書が前記デバイスに提示されると、読取専用機能がアクセスできるようになり、前記第1の証明書とは異なる第2の証明書が前記デバイスに提示されると、変更又は消去のため、又はバックアップ／復元のためにアクセスできるようになる、請求項148に記載のデバイス。

【請求項153】

前記第2メモリ領域は、前記少なくとも1つの権利オブジェクトの変更、消去、更新、及び／又はバックアップ及び復元のためには、DRM及び／又はCPRM能力を有するホストアプリケーションだけがアクセスできる、請求項148に記載のデバイス。

20

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、メディアコンテンツを安全に記憶し、当該コンテンツを消費者に安全に配信するための、モバイルストレージデバイスを採用したシステムを対象としている。

【背景技術】

【0002】

現在、消費者は、音楽、映像、及びゲームの様なメディアコンテンツをレンダリングするのに様々なデジタルデバイスを使用している。その様なデバイスには、携帯電話機、携帯情報端末（PDA）、デスクトップ型、ノートブック型、又はラップトップ型のコンピュータ、及びMP3プレーヤー、ビデオゲーム機などの様な各種メディアプレーヤー（以下、総称的に端末という）が含まれる。エンドユーザーの視点から言えば、あらゆるメディアコンテンツに対して購入申込は1つだけであるのが望ましい。例えば、音楽メディアコンテンツの場合、音楽の購入申込を1つだけにして、当該デバイスのどれを介してもその購入申込から音楽を再生できるようになっているのが望ましい。モバイルネットワークオペレータ（MNO）は、実際に携帯電話のユーザーが送受話器を介してメディアコンテンツにアクセスできるようにしてはいるが、その様なコンテンツサービスは、通常、送受話器に対してロックされているため、ユーザーは自分が所有している他の端末を介して当該コンテンツにアクセスすることは許されていない。

30

【0003】

現在の市場環境では、音楽、映画、及びビデオゲーム業界の会社は、彼らが提供しているメディアコンテンツが無認可で使用されることを懸念している。デジタルファイルの複製及び配信が容易になったので、メディアコンテンツの無認可利用に対する従来のバリアは崩壊しつつあり、今日、我々は、上記会社が所有する著作権の深刻な侵害を目の当たりにしている。しかしながら、既存のメディア記録及びレンダリング用システムは、今なお、メディア業界にとって完全に納得のいく方法で、エンドユーザーが上記各種デジタルデバイス又は端末を使用し、メディアコンテンツをレンダリングできるようにするための適切な安全性を提供していない。

40

【0004】

従って、デジタルデバイス又は端末のどれを介しても、メディアコンテンツを安全に記

50

憶し、当該コンテンツを認可されたエンドユーザーだけに引き渡すために使用できるモバイルメモリシステム及び方法を提供することが望ましい。

【特許文献1】米国仮特許出願第60／638,804号

【発明の開示】

【課題を解決するための手段】

【0005】

メディアコンテンツを記憶するための媒体としては、不揮発性書換可能メモリデバイスが特に適している。例えば、フラッシュメモリカードは、現在、数ギガバイト程度の容量を有しており、これはスマートカードの様な他の記憶媒体より遙かに大きく、映画、ビデオゲーム、及び多数の楽曲を記憶するのに使用することができる。更に、フラッシュメモリは書換可能であるため、コンパクトディスクの様な大容量書換不能メモリに比べ柔軟性が高い。既存のフラッシュメモリデバイスの1つの欠点は、カードに記憶されているメディアコンテンツの無認可の使用又はアクセスを防止する適切な安全性が提供できていないことである。このようにして、不揮発性書換可能メモリデバイスのメディアコンテンツが、コンテンツ所有者によって又は所有者に代わって、安全に保護され制御できたなら、メディア会社にとってはメディアコンテンツを配信する新しい手段が提供されることになり、そのときには、エンドユーザーは、複数のメディアサービスに購買申込をしなくても、異なるモバイルデジタルデバイスを介して当該デバイス内のメディアコンテンツにアクセスすることができることになる。MNOなどのサービスプロバイダは、更に、メディアコンテンツを安全に記憶し、メディアコンテンツを制御された方法で配信する、というサービスに対して課金できるようになることで、追加収益を得ることになる。

【0006】

メディアコンテンツを配信するための1つの新たな手段として、1つの実施形態では、不揮発性書換可能メモリデバイスには、暗号化されたメディアタイトルが事前にロードされており、当該タイトルは何らの制約無しにプレビューできるようになっている。

【0007】

上記実施形態の1つの実施例では、当該プレビューは、暗号化されたメディアタイトルの暗号化されていない部分又は当該タイトルの暗号化されていない低品質バージョンを備えている。プレビューは、更に、ノーカットのメディアタイトルの回数限定の再生又はレンダリングを備えている。しかしながら、エンドユーザーが、彼らのプレビューに加え、何らの制約や減損も無く、暗号化されたメディアタイトルにアクセスしたいと望む場合、エンドユーザーは、暗号化され且つ省略化されていないメディアタイトルにアクセスする権利を購入せねばならない。エンドユーザーは、この暗号化されたメディアタイトルにアクセスする権利を購入した後、当該タイトルにアクセスできるようになる。

【0008】

本実施形態のこの実施例では、プレビュー用として利用可能である暗号化されたメディアタイトルにアクセスするための証明書（クレデンシャル）又は他の種類の認証情報及び権利及び／又は規則は、デバイスに前以てロードされていない。それらは、エンドユーザーに対しては購入後にしか利用可能とならず、即ち、購入後に、その様な情報がメモリデバイスに記憶される。

【0009】

本実施形態の代わりの実施例では、上記不揮発性書換可能メモリデバイスへは、暗号化されたメディアタイトルのみならず、暗号化されたメディアタイトルの選択された部分だけ又は当該タイトルの低品質バージョンだけが制約無しにアクセス可能であることを、又は当該タイトルが限定回数だけ再生できることを、指定する権利及び／又は規則も事前にロードされる。エンドユーザーが支払いを済ますと、そこで、メモリデバイスに記憶されている権利及び／又は規則は更新されて、メモリデバイスに記憶されている暗号化されたメディアタイトルへのアクセスが、それ以上の制約無しに、又はもっと緩い制約付きで、の何れかで許可される。

【0010】

安全特性を備えた不揮発性書換可能メモリデバイスは、サービスプロバイダがメディアコンテンツの配信を制御するために使用するのに有利である。従って、メディア配信の別の新たな手段として、不揮発性書換可能メモリデバイスには、サービスプロバイダがデバイス上にプロバイダ自身の安全環境を構築できるようにする安全特性が提供される。サービスプロバイダは、デバイスに記憶されているメディアコンテンツが当該環境でどのように使用されるかを制御することができる。1つの実施形態では、不揮発性書換可能メモリデバイスには、サービスプロバイダが、デバイスに記憶されている暗号化されたコンテンツへのアクセスを制御するためにデバイスのセキュアメモリ領域内に制御構造を構築できるようにする、システムエージェントが提供されている。制御構造は、サービスプロバイダが、柔軟な方法でメディアコンテンツを配信する仕組みを設定できるようにする。制御構造は、メディアコンテンツがどのように使用され、どのようにアクセスされるかを制御する際に、サービスプロバイダが多くのオプションを持てるようにする階層ツリーの形態を採ってもよい。制御構造は、以下で「権利オブジェクト」とぶオブジェクトの形態を採ってもよく、そこでは、権利及び／又は規則は、特定のメディアコンテンツへのアクセスと或る特定の認証要件（複数の要件）に関係付けられており、当該コンテンツへのアクセスは、当該認証要件（複数の要件）が満たされたときに許容される。制御構造によって、多数のアプリケーション又はエンドユーザーは、同一コンテンツに、鍵又は証明書を共有すること無しに、アクセスすることができ、コンテンツを復号及び／又は暗号化するために使用される或る特定の鍵へのアクセス権を委託することができる。

10

【0011】

20

制御構造は、サービスプロバイダが、端末及びアカウントを或る特定の種類のコンテンツにアクセスできるようにする制御もできるようにしている。例えば、メモリデバイスの第1類では、デバイス内のメディアコンテンツには、何れのエンドユーザー端末を介しても制約無しにアクセスすることができる。メモリデバイスの第2類では、安全特性を備えたそれらのデバイスには、特定のサービスプロバイダ（例えば、MNO）の識別子又はIDの様な特定の証明書を有する端末でしかアクセスできない。更に、安全特性を備えているメモリデバイスの第3類では、家族の様な、エンドユーザーの或る特定のグループだけが、モバイルネットワークオペレータのIDの様な特定の証明書を有する端末で、デバイス内のコンテンツにアクセスできるようになっている。更に、書換可能不揮発性メモリデバイスの第4類では、デバイスに記憶されているコンテンツには、自身の固有の証明書と、モバイルネットワークオペレータのIDの様な特定のサービスプロバイダの証明書とを併せ持っている端末でしかアクセスできないようになっている。

30

【0012】

サービスプロバイダ又は何か他のエンティティにより構築される制御構造は、不揮発性書換可能メモリデバイスに記憶されているメディアコンテンツを暗号化するのに使用される1つ又は複数のコンテンツ暗号化鍵へのアクセスに対する或る特定の許可を規定するものである。例えば、制御構造は、事前に決められている証明書がデバイスに提示されたときに、1つ又は複数の（或る特定の目的のためだけの）コンテンツ暗号化鍵へのアクセスを許可する。このようにして、その様なデバイスが作動しているとき、デバイスは、事前に決められた証明書が提示されたときには、デバイスに提示された証明書が事前に決められた証明書であるか否かを判定し、1つ又は複数のコンテンツ暗号化鍵へのアクセスが、暗号化されているコンテンツを復号するための許可に従って許容されるか否かを判定する。

40

【0013】

不揮発性書換可能メモリデバイスは、更に、2人以上のエンドユーザーが、デバイスに記憶されている暗号化されたメディアコンテンツにアクセスできるようにしているが、その場合、それぞれのエンドユーザーは、同一コンテンツ又は異なるコンテンツにアクセスするのに異なる権利を有していてもよい。このようにして、1人のユーザーにとって目に見え且つアクセスすることのできるコンテンツが、別のエンドユーザーにはアクセスできなかったり、或いは目に見えないことすらある。デバイスは、それぞれがデバイスに記憶

50

されている暗号化された1組のメディアタイトルと関係付けられる複数のアカウントの情報を含む制御情報を記憶し、そこでは、各アカウントは対応する証明書を有している。或るアカウントと関係付けられた証明書が、ホスト又は端末によってデバイスに提示されると、デバイスは、特定のアカウントと関係付けられる暗号化されたメディアタイトルをアクセス可能とするべきか及び／又は目に見えるようにするべきか否かを判定するために、提示された証明書を照合するホストによって提示された資格証明物が正しいかどうか照合し、提示された資格証明物がデバイスに記憶されているそれらの資格証明物と当該アカウントについて一致するというような場合には、デバイスは、そこで、特定のアカウントと関係付けられる暗号化されたメディアタイトルを復号して、復号されたメディアタイトルをホストに供給してレンダリングできるようにする。従って、デバイスに対して、ホスト又は端末が証明書を提示しないか又は誤った証明書を提示したときには、アクセスする特定のアカウントと関係付けられる暗号化されたメディアタイトルは、目に見えることすら無く、アクセスすることもできない。本出願では、「ホスト」及び「端末」という用語は入れ替えて使用できる。

【0014】

安全特性を備えた不揮発性書換可能メモリデバイスとは、デバイスに記憶されている各メディアファイルが自身のコンテンツ暗号化鍵又は当該鍵へのアクセスが許容される前に要求される自身の証明書、及び復号されたメディアファイル又はタイトルがどの様に使用されるかに関する権利及び／又は規則、を有しているようなメモリデバイスである。1つの実施形態では、権利オブジェクトは、或る特定の暗号化されたメディアコンテンツに関する権利及び／又は規則、当該コンテンツを復号及び／又は暗号化するためのコンテンツ暗号化鍵、及び当該鍵にアクセスするのに必要な証明書を含んでいる。その様な権利オブジェクトは、上記で言及した制御構造の形態として使用される。このようにして、権利オブジェクトのこの実施形態を採用すれば、メモリデバイスは、デバイスに記憶されている多数の対応するメディアファイルを復号するのに利用できる多数のコンテンツ暗号化鍵を記憶することができ、且つ対応する権利オブジェクトを記憶することができる。不揮発性書換可能メモリデバイスそれぞれは、他のどのメモリデバイスの鍵とも異なる固有鍵を有するように製造することができる。これには、メモリデバイスそれぞれに対してコンテンツ暗号化鍵の固有セットを生成することが必要になる。しかしながら、幾つかのアプリケーションでは、及び安全実行の場合には、権利オブジェクトはコンテンツ暗号化鍵を含んでいないことが望ましい。代わりに、それは、コンテンツ暗号化鍵にアクセスするのに必要な認証情報（例えば、証明書）を含んでいる。このようにして、更に層の厚い安全策が提供される。

【0015】

しかしながら、幾つかのアプリケーションでは、不揮発性書換可能メモリデバイスの各バッチに、コンテンツ暗号化鍵（及び対応する権利オブジェクト）の同一セットをインストールすることが望ましく、そうすれば、製造中にバッチ内の異なるデバイスに異なる鍵をインストールする必要は無くなる。製造された不揮発性書換可能メモリデバイスの各バッチは、メモリデバイスの他のどのバッチのものとも異なる自身に固有のコンテンツ暗号化鍵及び対応する権利オブジェクトのグループを有することになる。

【0016】

この方式によれば、上記メモリデバイスを大量に製造する場合、デバイスは、それぞれが、Nが正の整数であるN個のデバイスを有する複数のグループに分けられる。それぞれが対応するコンテンツ暗号化鍵のセットを含んでいる、N個の権利オブジェクトセットが生成される。N個の権利オブジェクトセットは、それぞれ更に、製造中に当該権利オブジェクトセットがロードされるグループそれぞれの中で或るデバイスを識別するための対応するセット識別コードを有している。このようにして、N個の異なるセット識別コードが存在する。各デバイスは、固有の識別コードと、その識別コードから導き出されるのが望ましいセット識別コードを有している。従って、製造中、インストール処理では、先ず、製造されるデバイスそれぞれのセット識別コードをその固有識別コードから導き出す。次

に、セット識別コードから、対応する権利オブジェクトが識別され、デバイスにロードされる。当該権利オブジェクト内の鍵を使用して復号できる対応するメディアファイルも、デバイスにロードされる。ロードされたメディアファイルは、支払い済みのメディアコンテンツのみならず、アクセスできるようになる前に支払いが要求される未払いのメディアコンテンツを備えていてもよいし、無制約のアクセスが利用できる当該未払いメディアコンテンツのプレビューを備えていてもよい。

【0017】

本発明の更に別の態様の実施形態では、不揮発性書換可能メモリデバイスに記憶されるメディアコンテンツは暗号化されている。これは、暗号化されたメディアコンテンツのローディングは、安全が担保されていないファシリティで行うことができることを意味しており、これによりデバイスの製造工程は大いに単純になる。1つの実施形態では、例えば、コンテンツ暗号化鍵を含んでいる権利オブジェクトが、最初に、セキュアファシリティでデバイスにロードされる。その後、デバイスは安全が担保されていないファシリティに出荷されて、暗号化されたメディアコンテンツのローディングが行われるが、そのメディアコンテンツへのアクセスはメモリデバイスに既にロードされている権利オブジェクトによって制御されており、オブジェクト内のコンテンツ暗号化鍵を使用して、暗号化されたメディアコンテンツを復号することができることになる。

【0018】

上記で指摘したように、暗号化されたメディアタイトルとその様なタイトルのプレビューを有する不揮発性書換可能メモリデバイスは、メディア会社にメディアコンテンツ配信の新しい手段と新たな収益を提供する。上記種類とは異なるコンテンツが記憶されている不揮発性書換可能メモリは、更に、メディア会社並びに他の関連プロバイダに他の収益の道筋を提供する。1つのその様な構成では、メディアコンテンツは、不揮発性書換可能メモリカードのメモリ領域に記憶されるが、この場合、コンテンツは、少なくとも幾つかのメディアタイトルの選択された及び暗号化されていない部分又は当該タイトルの低品質で暗号化されていないバージョンしか含んでいない。その様なカードは、販売促進の目的に有用であり、また、エンドユーザーが購入前にメディアコンテンツをプレビューするのにも有用である。エンドユーザーは、当該コンテンツをプレビューした後、ノーカットのメディアタイトル又は当該タイトルの高品質バージョンの何れかを購入する。購入後、エンドユーザーは、当該メディアタイトルをメモリデバイスにダウンロードすると共に、支払い後は権利オブジェクトもダウンロードされる。

【0019】

このようにして、プレビューコンテンツを有する上記型式のメモリデバイスでは、デバイスは、メディアタイトルの暗号化されていない部分又はタイトルの低品質で暗号化されていないバージョンをレンダリングするか、限られた期間だけ又は限られた回数だけレンダリングすることによって、エンドユーザーからの要求に応答する。デバイスは、更に、ユーザーがノーカットの又は高品質バージョンのタイトルにアクセスする権利を購入したか否かを、ユーザーに問い合わせる。プレビューコンテンツが、ユーザーがノーカットのタイトルに限られた回数だけアクセスできるものである場合、メモリデバイスは、エンドユーザーが当該タイトル（複数のタイトル）にアクセスした後、ユーザーが当該タイトル（複数のタイトル）に無制約にアクセスする権利を購入したか否かをエンドユーザーに問い合わせる。1つの実施形態では、ユーザーがそこで当該タイトル（複数のタイトル）を購入することにより応答した場合、適切な権利オブジェクトが次にインストールされ、ノーカットの又は高品質なメディアタイトルも、まだデバイスに記憶されていないのであれば、インストールされる。そのような処理が完了したら、そこで、ユーザーは、レンダリングされたノーカットの又は高品質なメディアタイトル（複数のタイトル）を楽しむことができ、又は当該タイトルを一切の制約無しに楽しむことができる。

【0020】

更に別の代わりの実施形態は、暗号化されたメディアタイトルを、それらタイトルを復号するのに必要な鍵を記憶すること無しに、不揮発性書換可能メモリカードに記憶する実

施形態である。レンダリングの権利を購入した後、エンドユーザーは、次に、適切な鍵（又はその様な鍵にアクセスするための証明書）を使って、適切な権利オブジェクトをダウンロードし、メディアタイトルを復号して楽しむ。

【0021】

更に別の実施形態では、暗号化されていないメディアタイトルが記憶されている不揮発性書換可能メモリカードは、市場調査の目的で使用されている。このようにして、カードには、或る一定期間又は制限回数分の何れかの条件付でメディアタイトルへのアクセスを許可する権利オブジェクト又は他の制御構造も記憶され、カードは、メディアタイトルへのアクセスを追跡し、追跡されたアクセスに基づいてアクセスプロファイルをコンパイルする。メディアタイトルを再生又はレンダリングできる制限時間又は制限回数は、既にコンパイルされたアクセスプロファイルが市場調査の様な目的のためにサーバにダウンロードされると、延長される。

【0022】

更に別の実施形態では、不揮発性書換可能メモリカードは、アクセスできる或る特定の暗号化されたメディアコンテンツに適用される1つ又は複数の権利オブジェクト（複数のオブジェクト）又は他の制御構造を記憶しているが、但し、ここでは、当該コンテンツはカードに記憶されていない。その様なメモリカードは、エンドユーザーによる購入に利用できるプリペイド式メディアコンテンツカードとして使用される。コンテンツ暗号化鍵（又は当該鍵にアクセスするための証明書）及び権利及び／又は規則は既にカードに記憶されているので、エンドユーザーは、カード内の権利及び／又は規則の下で規定されている暗号化されたコンテンツをダウンロードし、1つ又は複数のコンテンツ暗号化鍵を使用して当該コンテンツを復号することができ、そのコンテンツはレンダリングのためにカードによってアクセスされるか、又はカード内に記憶される。その様なカードの1つの利点は、エンドユーザーが、権利及び／又は規則によって規定されている暗号化されたコンテンツを繰り返しダウンロードすることを許可していることであり、これにより、エンドユーザーは、暗号化されているコンテンツを削除し、同一コンテンツを後でダウンロードすることができるようになる。これは、ユーザーが、アクセスする権利を放棄すること無しに大量のメディアコンテンツに、アクセスできるようにする。

【0023】

ユーザーが、複数の証明書を提供する必要なしに、多数の異なる保護されたメディアファイルに容易にアクセスできるようにするために、それらファイルへのアクセスを制御する制御構造は、特定のセットの証明書が提示されたときに、ユーザーに当該メディアファイルの全てにアクセスすることを許可するように指定された制御構造の様な、別の制御構造に、それらファイルにアクセスするための許可又は権限を、委譲できるようにしている。1つの実施形態では、その様な指定された制御構造は、プレイバックアクセス制御記録又は権利オブジェクトであってもよい。別の実施形態では、委譲される許可は、暗号化されているメディアファイルを復号するための鍵にアクセスする許可である。

【0024】

権利オブジェクトを採用している上記各種実施形態では、権利オブジェクトは、コンテンツを復号及び／又は暗号化するのに使用される鍵、及び鍵にアクセスするための認証要件を含んでいる。上記各実施形態と類似している別の実施形態は、権利オブジェクトの別の実施形態を使用して実施されており、そこでは、メモリデバイスの或る特定の保護された領域にアクセスするための権利及び／又は規則は、対応する認証要件と関係付けられており、その様な要件を満たしている認可されたエンティティだけが、当該領域に記憶されているコンテンツへアクセスすることができるようになっている。権利オブジェクトの当該実施形態は、鍵を含んでいてもいなくてもよい。権利オブジェクトの当該実施形態が鍵を含んでいる場合には、鍵は、保護されている領域又は保護されていない領域に記憶されているコンテンツを復号及び／又は暗号化するために使用され、その場合、認証要件は、保護された領域にアクセスするために使用されるものとは異なっていることが望ましく、その認証要件との整合性が、鍵にアクセスするのに必要とされる。

【0025】

上記指摘したように、有用な権利及び／又はコンテンツがメモリデバイスにロードされる。このために、当該貴重なコンテンツがロードされる前に、カードの証明書を調べるのが肝要である。このようにして、本発明の別の態様によれば、不揮発性書換可能フラッシュメモリカードの証明書は、カードが正規であるか又は偽造品であるかを判定するために照合され、そこで、照合に応じてカードが正規であるか否かに関する情報が提供される。この能力は、認証サーバからサービスプロバイダサーバへという様に、サーバからサーバへと伝送される。

【0026】

もう1つの実施形態では、権利オブジェクトは、権利オブジェクトによるコンテンツの制御を迂回する方法を防止するように、バックアップされ復元される。メディアコンテンツは第1メモリ領域に記憶されている。第1メモリ領域に記憶されているメディアコンテンツへのアクセスを制御するために、少なくとも1つの権利オブジェクトが第2メモリ領域に記憶されている。第2メモリ領域には、当該の少なくとも1つの権利オブジェクトのバックアップ及び復元のために、そうすることが認可されているアプリケーションしかアクセスできないことが望ましい。1つの実施例では、第2メモリ領域は、読取り専用機能のパーティションにアクセスするのに使用されるものとは異なる証明書を有するアプリケーションしかアクセスできない保護されたパーティションである。

更に別の実施形態では、権利オブジェクトは、第1証明書がデバイスに提示されたときには、読取り専用機能にとってアクセス可能であり、第1証明書とは異なる第2証明書がデバイスに提示されたときには、アクセスしてコピーし、変更し、又は消去することができる。1つの実施形態では、第2証明書がデバイスに提示されると、権利オブジェクトがコピーされ、変更され、又は消去される。この処理によって、権利オブジェクトのコピー元のソースメモリデバイスと権利オブジェクトのコピー先のレシピエントデバイスの両方において、権利オブジェクトから作られる複数のコピーを有効に制御できるようになる。コピーに先立ち、許可されるコピーの総数は、同じ数に維持され、コピーによって変わることはない。これは、ソースメモリデバイス内の権利オブジェクトを変更するか消去するかの何れかによって、及び必要に応じて、レシピエントメモリデバイスへコピーする前に権利オブジェクトを変更することによって、制御される。

更に別の実施形態では、不揮発性書換可能メモリカードにアクセスしようとしているアプリケーションの証明書は、そうするよう認可されているか否かを判定するために照合される。アプリケーションの証明書が要件に合致しないときには、当該アプリケーションは不揮発性書換可能メモリカードにアクセスするよう認可されていないことが示される。

【0027】

上に述べた特性は、メディアコンテンツを安全で制御された方法で配信するための異なる手段を提供するため、個別に又は何らかの組み合わせで使用されてもよい。

【発明を実施するための最良の形態】

【0028】

説明を分かり易くするために、本出願中、同一の構成要素には同じ符号を付して表示している。

【0029】

本発明の様々な態様が実施される一例的なメモリシステムを図1のブロック図で示している。図1に示すように、メモリシステム又はデバイス10は、中央演算処理装置(CPU)12、バッファ管理装置(BMU)14、ホストインターフェースモジュール(HIM)16及びフラッシュインターフェースモジュール(FIM)18、フラッシュメモリ20、及び周辺アクセスモジュール(PAM)22を含んでいる。メモリシステム10は、ホストインターフェースバス26とポート26aを介してホストデバイス24と通信する。NAND型であるフラッシュメモリ20は、ホストデバイス24用のデータ記憶部である。CPU12用のソフトウェアコードもフラッシュメモリ20に記憶される。FIM18は、フラッシュインターフェースバス28とポート28aを介してフラッシュメモリ

20に接続される。HIM16は、デジタルカメラ、パーソナルコンピュータ、携帯情報端末(PDA)、デジタルメディアプレーヤー、MP-3プレーヤー、携帯電話、又は他のデジタルデバイスの様なホストシステムへの接続に適している。周辺アクセスモジュール22は、CPU12と通信するために、FIM、HIM、及びBMUの様な適切なコントローラモジュールを選択する。1つの実施形態では、点線のボックス内のシステム10の構成要素の全てが、メモリカード又はスティック10'の様な単一のユニット内に囲われ、カプセル化されるのが望ましい。

【0030】

本発明は、ここでは、カード形態のフラッシュメモリに関して説明しているが、本発明は、カード形態か否かを問わず、磁気ディスク、光学式CDの様な他の型式のメモリ、並びに他の型式の書換可能揮発性メモリシステムにも適用可能である。

10

【0031】

バッファ管理ユニット14は、ホストダイレクトメモリアクセス(HDMA)32、フラッシュダイレクトメモリアクセス(FDMA)34、アービタ36、バッファランダムアクセスメモリ(BRAM)38、及びクリプトエンジン40を含んでいる。アービタ36は、共用バスアービタなので、常時1つのマスタ又はイニシエータ(HDMA32、FDMA34、又はCPU12が考えられる)しかアクティブにならず、スレーブ又は標的はBRAM38である。アービタは、BRAM38に対する適切なイニシエータ要求のチャネリングの任を負っている。HDMA32とFDMA34は、HIM16とFIM18とBRAM38又はCPUランダムアクセスメモリ(CPU RAM)12aの間で伝送されるデータに責任を負っている。HDMA32とFDMA34の動作は、従来通りなので、ここでは詳しく説明する必要はない。BRAM38は、ホストデバイス24とフラッシュメモリ20の間を通過するデータを記憶するのに使用される。HDMA32とFDMA34は、HIM16/FIM18とBRAM38又はCPU RAM12aの間でデータを伝送すること、及びセクター完了を表示することに責任を負っている。

20

【0032】

メモリ20に記憶されているコンテンツの安全性を改善するために、メモリシステム10は、暗号化及び／又は復号に使用される鍵値(複数鍵値)を生成する。しかしながら、ホストデバイスは、メモリシステム10に対してデータをファイル形式で読み取り、書き込むので、暗号化と復号は、通常、ファイル毎に行われる。多くの他の型式の記憶装置の様に、メモリデバイス10は、ファイル又はファイルシステムを認識できない。メモリ20が、ファイルの論理アドレスが識別できるファイルアロケーションテーブル(FAT)を実際に記憶しているにもかかわらず、FATは、通常、コントローラ12ではなくホストデバイス24によってアクセス及び管理される。従って、特定のファイル内のデータを暗号化するために、コントローラ12は、ホストデバイスを信頼してメモリ20のファイル内のデータの論理アドレスを送信せねばならないので、特定のファイルのデータは、システム10だけに利用可能な鍵値(複数鍵)を使用して、システム10により、認識及び暗号化及び／又は復号される。

30

【0033】

ファイル内のデータを暗号手法で処理し、ホストデバイス24とメモリシステム10の両方が同じ鍵(複数鍵)を参照できるようにするハンドルを提供するため、ホストデバイスは、システム10によって生成された鍵値のそれぞれのリファレンスを提供しており、その様なリファレンスは単純に鍵IDであってもよい。このようにして、ホスト24は、システム10によって暗号手法的に処理された各ファイルと鍵IDを関係付け、システム10は、データを暗号手法で処理するために使用される各鍵値を、ホストにより提供された鍵IDと関係付ける。このようにして、ホストが、ファイルを暗号手法で処理することを要求するとき、この要求を、メモリ20から取り出された、又はメモリ20に記憶されているデータの論理アドレスを伴う鍵IDと共に、この要求をシステム10に送る。システム10は、鍵値を生成し、ホスト24によって提供された鍵IDを当該値と関係付け、暗号手法の処理を行う。この方法では、メモリシステム10が鍵(複数鍵)を使用して暗

40

50

号手法の処理を制御できるようにしながらも、メモリシステム 10 が作動するやり方を変更する必要はない。換言すると、システム 10 は、引き続き、暗号方式の処理に使用される鍵値の生成と管理に対する制御を維持しながら、ホスト 24 が、F A T の排他的制御を有することによりファイルを管理できるようにしている。

【0034】

ホスト 24 により提供される鍵 I D と、メモリシステムにより生成される鍵値は、以下で「コンテンツ暗号化鍵」又は「C E K」と呼んでいる 2 つの量の属性を形成する。ホスト 24 は、各鍵 I D を 1 つ又はそれ以上のファイルと関係付けるが、ホスト 24 は、更に、各鍵 I D を、未編成のデータ又は何らかの方法で編成されたデータ、そして完全なファイルに編成されたデータに限定せず、関係付ける。

10

【0035】

ユーザー又はアプリケーションがシステム 10 内の保護されているコンテンツ又は領域にアクセスを得るためには、システム 10 に事前登録されている証明書を使用して認証される必要がある。証明書は、当該証明書を有する特定のユーザー又はアプリケーションに許容されているアクセス権に結びつけられている。事前登録のプロセスでは、システム 10 は、ユーザー又はアプリケーションの身分と証明書、及びユーザー又はアプリケーションによって決められホスト 24 を通して提供された、当該身分と証明書に関係付けられたアクセス権の記録を記憶する。事前登録の完了後、ユーザー又はアプリケーションがメモリ 20 にデータを書き込むことを要求するとき、ホストデバイスを通して、その身分と証明書、データを暗号化するための鍵 I D、及び暗号化されたデータが記憶される論理アドレスを提供することが必要になる。システム 10 は、鍵値を生成し、その値をホストデバイスによって提供された鍵 I D と関係付け、当該ユーザー又はアプリケーション用のシステム自身の記録又は表に、書き込まれるデータの暗号化に使用される鍵値の鍵 I D を記憶する。次いで、システムはデータを暗号化し、暗号化されたデータ並びにシステムが生成した鍵値を、ホストによって指定されたアドレスに記憶する。

20

【0036】

ユーザー又はアプリケーションが、システム 20 から暗号化されているデータを読み取することを要求するとき、ユーザー又はアプリケーションは証明書を提供することによってその身分を証明することと、要求されているデータの暗号化に以前使用した鍵の鍵 I D 及び暗号化されたデータが記憶されている論理アドレスを提供することが必要となる。次いで、システム 10 は、ホストによって提供されたユーザー又はアプリケーションの身分と証明書を、その記録に記憶されているものと照合する。それらが一致すれば、システム 10 は、そこで、そのメモリから、ユーザー又はアプリケーションによって提供された鍵 I D と関係付けられている鍵値を取り出し、その鍵値を使用して、ホストデバイスによって指定されたアドレスに記憶されているデータを復号し、復号されたデータをユーザー又はアプリケーションに送る。

30

【0037】

認証証明書を暗号化処理に使用される鍵の管理から切り離すことによって、証明書を共有すること無しに、データにアクセスする権利を共有することが可能になる。このようにして、異なる証明書を有するユーザー又はアプリケーションのグループは、同一データにアクセスするのに同一鍵へのアクセスを有することができ、一方、このグループ外のユーザーはアクセスを有しない。グループ内の全てのユーザー又はアプリケーションは、同一データへのアクセスを有しているが、それらは異なる権利をなお有している。このようにして、或るものは読取り専用アクセスを有し、他のものは書込みアクセスしか持たず、また他のものは両方を有している。システム 10 は、ユーザー又はアプリケーションの身分と証明書、それらがシステムにアクセスできる鍵 I D、及び鍵 I D のそれぞれに関係付けられたアクセス権の記録を維持しているので、システム 10 は、特定のユーザー又はアプリケーションについて、鍵 I D を追加又は削除し、鍵当該 I D と関係付けられているアクセス権を変更すること、或るユーザー又はアプリケーションから別のユーザー又はアプリケーションへアクセス権を委譲すること、或いはユーザー又はアプリケーションの記録又

40

50

は表を削除又は追加することさえ可能であり、それらは全て適正に認証されたホストデバイスによって制御される。記憶されている記録は、或る特定の鍵にアクセスするのにセキュアチャンネルが必要であることを指定しているかもしれない。認証は、対称又は非対称アルゴリズム並びにパスワードを使用して行われる。

【0038】

特に重要なことは、メモリシステム10内の保護されたコンテンツの可搬性である。鍵値は、メモリシステムにより生成され、実質的には外部システムには利用できないため、メモリシステム又はこのシステムを組み込んでいる記憶装置が、或る外部システムから別の外部システムに移転されるとき、そこに記憶されているコンテンツの安全性は維持されており、外部システムは、メモリシステムによって完全に制御された方法で認証されない限り、当該コンテンツにアクセスすることはできない。そのように認証された後でさえ、アクセスはメモリシステムにより制御され、外部システムは、メモリシステム内の事前に設定されている記録に従って制御される方法でしかアクセスできない。要求が当該記録に適合しなければ、要求は拒絶される。

【0039】

コンテンツを保護する場合の柔軟性をより高めるために、以下でパーティションと呼んでいるメモリの或る特定の領域は、適正に認証されたユーザー又はアプリケーションしかアクセスできないように目論まれている。鍵に基づくデータ暗号化の上記特性と組み合わせると、システム10は、更に優れたデータ保護能力を発揮する。図2に示すように、フラッシュメモリ20は、その記憶容量が複数のパーティション、即ちユーザーの領域又はパーティションP0は、認証なしで全ユーザー及びアプリケーションにとってアクセス可能となっている。ユーザー領域に記憶されているデータの全てのビット値は、あらゆるアプリケーション又はユーザーによって読み取られ又は書き込まれるが、読取りデータが暗号化されている場合は、復号する権限のないユーザー又はアプリケーションは、ユーザー領域に記憶されているビット値により表される情報にアクセスすることはできない。このことは、例えば、ユーザー領域P0に記憶されているファイル102及び104によって説明されている。更に、ユーザー領域には、全てのアプリケーション及びユーザーによって読み取られ理解されるファイル106の様な暗号化されていないファイルも記憶されている。このようにして、象徴的に、暗号化されているファイルは、ファイル102と104の場合の様に錠前を付けて示している。

【0040】

ユーザー領域P0の暗号化されているファイルが認可されていないアプリケーション又はユーザーによって理解されることはないとしても、その様なアプリケーション又はユーザーが当該ファイルを削除又は汚染することは依然として可能であり、それは幾つかのアプリケーションにとっては望ましくないことである。そのため、メモリ20は、事前の認証なしにアクセスすることができないパーティションP1及びP2の様な保護されたカスタムパーティションも含んでいる。本出願の実施形態で許可されている認証プロセスをこれより説明する。

【0041】

これも図2に示すように、様々なユーザー又はアプリケーションが、メモリ20内のファイルにアクセスする。ユーザー1と2及び（デバイス上で実行中の）アプリケーション1～4を図2に示している。それらのエンティティがメモリ20内の保護されたコンテンツにアクセスできるようになる前に、それらは、先ず認証プロセスによって以下に説明する方法で認証される。このプロセスでは、アクセスを要求しているエンティティは、役割ベースのアクセス制御のためにホスト側で識別される必要がある。このようにして、アクセスを要求しているエンティティは、先ず、「私はアプリケーション2であり、ファイル1の読み取りを希望する」というような情報を供給することによって自身の身分を明らかにする。そこで、コントローラ12は、身分、認証情報、及び要求を、メモリ20又はコントローラ12に記憶されている記録と照合する。全ての要件が合致すれば、そこで、当

該エンティティに対してアクセスが許容される。図2に示すように、ユーザー1は、パーティションP1のファイル101に対する読取り及び書込みが許可されており、加えて、P0内のファイル106からの読取りと当該ファイルへの書込みについてユーザー1は無制約の権利を有するが、ファイル102と104に関しては読取りしか許可されていない。他方ユーザー2は、ファイル101と104へのアクセスは許可されていないが、ファイル102に対する読取り及び書込みアクセスは有している。図2に表示している、ユーザー1と2は同じログインアルゴリズム(AES)を有しているが、一方、アプリケーション1と3は、異なるログインアルゴリズム(例えばmRSAと001001)を有しており、それらは、ユーザー1及び2のものとも異なっている。ユーザー1と2は共に、証明書を一切提示すること無しに、また一切の制約無しに、ファイル106にアクセスすることができる。

10

【0042】

安全記憶アプリケーション(SSA)は、メモリシステム10のファームウェア内の安全アプリケーションであり、上で特定した特性の多くを実施するのに使用される本発明の或る実施形態を例証している。SSAは、メモリ20又はCPU12内の不揮発性メモリ(図示せず)に記憶されているデータベースでソフトウェア又はコンピュータコードとして具現化されており、RAM12a内に読み込まれ、CPU12によって実行される。SSAに関して使用される各頭字語を下表に示す。

【表1】

定義、頭字語、及び略語

20

ACR	アクセス制御記録
AGP	ACRグループ
CBC	チェーンブロック暗号
CEK	コンテンツ暗号化鍵
ECB	電子コードブック
ACAM	ACR属性管理
PCR	許可制御記録
SSA	安全記憶アプリケーション
エンティティ	SSAにログインし、而してその機能を利用する、現実且つ個別的に存在するあらゆるもの(ホスト側)

30

【0043】

(SSAシステムの説明)

データの安全性、完全性、及びアクセス制御が、SSAの主な役割である。データとは、そうでなければ或る種の大記憶装置に単にそのまま記憶されることになるファイルである。SSAシステムは、記憶システムの頂上に座し、記憶されるホストファイルに安全層を追加する。

【0044】

40

SSAの主要タスクは、メモリに記憶され(及び保護され)ているコンテンツと関係付けられている異なる権利を管理することである。メモリアプリケーションは、記憶されている複数のコンテンツに対する複数のユーザーとコンテンツ権を管理する必要がある。ホストアプリケーションは、それらの側から、当該アプリケーションにとって目に見えるドライブとパーティション、及び記憶装置に記憶されているファイルの場所を管理し表現しているファイル割振り表(FAT)を観察する。

【0045】

この場合、記憶装置は、パーティションに分割されたNANDフラッシュチップを使用するが、他のモバイル記憶装置も使用でき、それらも本発明の範囲内にある。それらパーティションは、論理アドレスの連続したスレッドであり、そこでは、スタートとエンドア

50

ドレスがそれらの境界を画定する。従って、必要に応じて、隠れたパーティションへのアクセスには、制約を果たすことができるが、それは当該制約を当該境界内のアドレスと関係付けるソフトウェア（メモリ 20 に記憶されているソフトウェアなど）によって課される。SSA によって管理されている論理アドレス境界によって、SSA にとっては完全にパーティションを認識可能である。SSA システムは、認可されていないホストアプリケーションからのデータを物理的に保護するためにパーティションを使用する。ホストにとっては、パーティションは、データファイルを記憶するための独占空間を画定する機構である。それらパーティションは、記憶装置へのアクセスを有するものは誰でも見ることができ、デバイス上のパーティションの存在に気づくパブリックなもの、又は選択されたホストアプリケーションだけがアクセスを有し、記憶装置内のそれらの存在に気づくプライベート又は隠されたもの、の何れであってもよい。

【0046】

図 3 は、メモリのパーティション、P0、P1、P2、及び P3（パーティションは 4 個より少なくとも多くてもよいことは明らかである）を説明しているメモリの概略図であり、ここで、P0 は、あらゆるエンティティが認証無しにアクセスできるパブリックパーティションである。

【0047】

プライベートパーティション（P1、P2、又は P3）は、その内部のファイルへのアクセスを隠している。ホストがパーティションにアクセスすることを妨げることによって、フラッシュデバイス（例えば、フラッシュカード）は、パーティションの内部のデータファイルの保護を実現している。しかしながら、この種の保護は、隠れたパーティションに置かれているファイルの全てを巻き込み、パーティション内の論理アドレスに記憶されているデータへのアクセスに制約を課することになる。。言い換えると、制約は論理アドレスの範囲と関係付けられている。当該パーティションに対するアクセスを有するユーザー／ホストの全ては、内部のファイルの全てに対する無制限のアクセスを有することになる。それぞれのファイル又はファイルのグループを互いに分離させるために、SSA システムは、鍵及び鍵リファレンス又は鍵 ID を使用して、ファイル又はファイルのグループ毎にもう一つ別のレベルの安全性及び完全性を提供している。異なるメモリアドレスのデータの暗号化に使用される特定の鍵値の鍵リファレンス又は鍵 ID は、暗号化されたデータが入っているコンテナ又はドメインと類比して説明させることができる。この理由から、図 4 では、鍵リファレンス又は鍵 ID（例えば、「鍵 1」及び「鍵 2」）は、鍵 ID と関係付けられている鍵値を使用して暗号化されたファイルを取り囲んでいる領域として図形的に示されている。

【0048】

図 4 に関して、例えば、ファイル A は、何れの鍵 ID にも囲まれていないことが図示されていることから、一切の認証無しに全てのエンティティにとってアクセス可能となっている。パブリックパーティションのファイル B は、全てのエンティティによって読取り又は上書きされるが、ID「鍵 1」を有する鍵で暗号化されているデータを含んでいるので、ファイル B に入っている情報は、エンティティが当該鍵に対するアクセスを有していない限り、そのエンティティにとってはアクセス可能にならない。この方法では、鍵値と鍵リファレンス又は鍵 ID を使用することは、上で説明したパーティションにより提供される類の保護とは反対に、論理的な保護しか提供しない。従って、パーティション（パブリック又はプライベート）にアクセスすることのできるホストは何れも、暗号化されているデータを含め、全パーティション内のデータの読取り又は書込みが可能である。しかしながら、データは暗号化されているので、認可されていないユーザーはそれに悪影響を与えることができるだけである。ユーザーらは、検知されずにデータを変更することも使用することもできないのが望ましい。暗号化及び／又は復号鍵へのアクセスを制約することによって、この特性は、認可されたエンティティだけがデータを使用できるようにしている。ファイル B 及び C は、更に、P0 内の鍵 ID「鍵 2」を有する鍵を使用して暗号化される。

10

20

30

40

50

【0049】

データの機密性及び完全性は、コンテンツ暗号化鍵（CEK）をCEK毎に1つ使用する対称暗号化法によって提供される。SSA実施形態<17>では、CEKは、フラッシュデバイス（例えば、フラッシュカード）によって生成され、内部的にしか使用されず、秘密裏に維持される。暗号化され又は暗号にされたデータは、データの完全性を確保するために、更に、ハッシュ化されても、暗号がチェーンブロックであっても、何れでもよい。CEKは、正常操作時はカードの外部のエンティティにとってアクセスできないメモリの保護された領域に記憶されているのが望ましい。

【0050】

パーティション内の全てのデータが、異なる鍵を使って暗号化され、異なる鍵IDと関係付けられているわけではない。パブリック又はユーザーファイル内か、オペレーティングシステム領域（即ちFAT）内かを問わず、或る特定の論理アドレスは、何れの鍵又は鍵リファレンスにも関係付けられず、このようにして、あらゆるエンティティがパーティション自体を利用できる。

【0051】

鍵及びパーティションを作成する並びにそれらからデータを書き込み及び読み取るかは鍵を使用する能力を求めるエンティティは、アクセス制御記録（ACR）を通してSSAシステムにログインする必要がある。SSAシステムのACRの特権はアクションと呼ばれている。全てのACRは、次の3つのカテゴリ、即ち、パーティション及び鍵／鍵IDを作成する、パーティション及び鍵にアクセスする、他のACRを作成／更新する、というアクションを行う許可を有している。

【0052】

ACRは、ACRグループ又はAGPと呼ばれるグループに編成されている。ACRが首尾よく認証されると、SSAシステムは、ACRアクションの何れかが実行されるセッションを開く。

【0053】

（ユーザーパーティション）

SSAシステムは、1つ又は複数のパブリックパーティションを管理しており、このパーティションはユーザーパーティション（複数パーティション）とも呼ばれる。このパーティションは記憶装置上に存在しており、記憶装置の標準的な読取り書き込みコマンドを介してアクセスできる単一又は複数のパーティションである。パーティション（複数パーティション）の大きさ並びにデバイス上のその存在に関する情報を取得することは、ホストシステムから隠せないのが望ましい。

【0054】

SSAシステムは、標準的な読取り書き込みコマンド又はSSAコマンドの何れかを介して、このパーティション（複数パーティション）へのアクセスを可能にする。従って、パーティションへのアクセスは特定のACRに制約されないことが望ましい。しかしながら、SSAシステムは、ホストデバイスがユーザーパーティションへのアクセスを制約できるようにしている。読取り及び書き込みアクセスは、個々に可能にされ／不能にされる。全4つの組み合わせ（例えば、書き込み専用、読取り専用（書き込み保護）、読取り及び書き込み、アクセス無し）が許容されている。

【0055】

SSAシステムは、ACRが、鍵IDをユーザーパーティション内のファイルと関係付けできるようにし、当該鍵IDに関係付けられた鍵を使用して個々のファイルを暗号化できるようにしている。ユーザーパーティション内の暗号化されたファイルにアクセスすること並びに当該パーティションへのアクセス権を設定することは、SSAコマンドセット（SSAコマンドの詳細説明に付いては付録A参照—付録では、鍵IDは「ドメイン」と呼ばれている）を使用して行われる。

【0056】

上記特性は、フィルに編成されていないデータにも適用される。

10

20

30

40

50

【0057】

(SSAパーティション)

これらは、SSAコマンドを介してのみアクセスできる（ホストのオペレーティングシステム又はOSから）隠されたパーティションである。SSAシステムは、ホストデバイスが、ACRに対してログインすることによって確立されるセッション（下記で説明）以外を介してSSAパーティションにアクセスすることを許容しないのが望ましい。同様に、SSAは、SSAパーティションの存在、大きさ、及びアクセス許可に関する情報については、それらの要求が確立されたセッションを介して入ってくるのでなければ、情報を提供しないのが望ましい。

【0058】

パーティションへのアクセス権は、ACR許可から導き出される。ACRは、一旦SSAシステムにログインされると、当該パーティションを他のACRと共有することになる（下記で説明）。或るパーティションが作成される時、ホストは、そのパーティションのレファレンス名又はID（例えば、図3及び図4のP0-P3）を与える。このリファレンスは、更にパーティションに対する読取り及び書込みコマンドに使用される。

【0059】

(記憶装置のパーティション化)

デバイスの全利用可能記憶容量は、ユーザーパーティションと現在設定されているSSAに割り振られるのが望ましい。従って、再パーティション化動作には、既存のパーティションの再設定が伴う。デバイス容量（全パーティションの大きさの総和）への正味の変更はゼロである。デバイスメモリ空間内のパーティションのIDは、ホストシステムによって定義される。

【0060】

ホストシステムは、既存パーティションの1つを、2つのより小型のパーティションに再パーティション化するか、2つの既存パーティション（隣接していてもいなくてもよい）を1つにマージするかの何れかを行うことができる。分割された又は併合されたパーティション内のデータは、ホストの裁量により消去されるか触れずに残されるかの何れでもよい。

【0061】

記憶装置の再パーティション化では、（データが記憶装置の論理アドレス空間内で消去されたか、移動されたかの何れかが原因で）データの損失が発生することから、再パーティション化に対する厳格な制約がSSAシステムにより施行されている。ルートAGP（下記で説明）に存在しているACRだけが、再パーティション化コマンドの発行を許されており、それが所有しているパーティションしか参照できない。SSAシステムは、データがパーティション内でどの様に（FAT又は他のファイルシステム構造）編成されるかには気づかないために、デバイスが再パーティション化されるときは常にそれらの構造を再構築することはホストの責任である。

【0062】

ユーザーパーティションの再パーティション化は、ホストOSに見えるこのパーティションの大きさと他の属性を変化させることになる。

【0063】

再パーティション後、SSAシステム内のACRが存在していないパーティションを参照することがないようにするのは、ホストシステムの責任である。それらACRが適切に削除又は更新されていなければ、それらACRに成り代って、存在していないパーティションへアクセスしようとする試みは、システムによって検知され拒絶される。鍵及び鍵IDの削除に関しても同様の配慮がなされることが望ましい。

【0064】

(鍵、鍵ID、及び論理的保護)

ファイルが或る特定の隠されたパーティションに書き込まれるとき、それは一般のパブリックから物理的に隠されている。しかし、エンティティ（敵対的であるか否かを問わず

10

20

30

40

50

）が一旦このパーティションに対する知識とアクセスを得てしまうと、ファイルは利用可能となり簡単に見えてしまう。ファイルを更に安全に護るために、SSAは、隠されたパーティションで暗号化することができるが、その際、ファイルを復号するために鍵にアクセスする証明書は、当該パーティションにアクセスするためのものとは異なっているのが望ましい。ファイルはSSAが気づくものではない（ホストによって全面的に制御され管理されている）ため、CEKとファイルの関係付けが問題である。ファイルを何かとリンクさせる場合、SSAの承認ー鍵IDが、これを是正する。このようにして、SSAによって鍵が作成されると、ホストはこの鍵の鍵IDを、SSAによって作成された鍵を使用して暗号化されたデータと関係付ける。

【0065】

鍵値と鍵IDは論理的な安全を提供する。所与の鍵IDに関係付けられている全てのデータは、その場所を問わず、同じコンテンツ暗号化鍵（CEK）で暗号にされるが、そのリファレンス名又は鍵IDはホストアプリケーションによる作成時に固有に提供される。或るエンティティが、隠されているパーティションへのアクセスを（ACRを介した認証によって）獲得し、このパーティション内の暗号化されているファイルの読取り又は書き込みの何れかをしたいと希望した場合には、ファイルと関係付けられている鍵IDへのアクセスを有する必要がある。この鍵IDの鍵へのアクセスを許容する際、SSAは、この鍵IDに関係付けられているCEKの鍵値をロードして、ホストに送る前にデータを復号するか、フラッシュメモリ20に書き込む前にデータを暗号化するか、の何れかを行う。鍵IDに関係付けられているCEKの鍵値は、SSAシステムによって一度ランダムに作成され、SSAシステムによって維持される。鍵値は、SSAによって全面的に管理される。

【0066】

SSAシステムは、以下の暗号モードの何れか（ユーザーが定義）を使用して、鍵IDに関係付けられているデータを保護する（CEKの鍵値に加え、使用される実際の暗号アルゴリズムは、システム制御されており、外界には露呈されない）。

【0067】

ブロックモードデータはブロックに分割され、1つずつが個別に暗号化される。このモードは、一般に安全性が高いとはいえず、辞書攻撃を受け易い。しかしながら、これは、ユーザーがデータブロックの何れにでもランダムにアクセスできるようにしている。

【0068】

チェーンモードデータはブロックに分割され、暗号化処理の間に連鎖される。各ブロックは、次のブロックの暗号化処理に対する入力として使用される。このモードは、安全性はより高いと考えられるが、データは、スタートからエンドまで常に順に書き込まれ読み出される必要があり、常にユーザーに受け入れられるとは限らないオーバーヘッドができる。

【0069】

ハッシュ式データの完全性の検証に使用されるデータダイジェストの追加作成を伴うチェーンモード。

【0070】

（ACR及びアクセス制御）

SSAは、それぞれがシステムデータベース内でノードのツリーとして表されている複数のアプリケーションを取り扱うように設計されている。アプリケーション間の相互排除は、ツリーの枝同士の間クロストークが確実に無いようにすることによって実現される。

【0071】

SSAシステムへのアクセスを得るためには、エンティティは、システムのACRの1つを介して接続を確立する必要がある。ログイン手続きは、ユーザーが接続相手に選定したACRに埋め込まれている定義に従って、SSAシステムにより管理される。

【0072】

ACRは、SSAシステムへの個別のログインポイントである。ACRは、ログイン証明書と認証方法を保持している。記録には、SSAシステム内のログイン許可も含まれており、その中には読取り及び書き込み特権も含まれている。これを図5に示しているが、これは、同じAGP内のn個のACRを示している。これは、n個のACRの内の少なくとも幾つかは、同じ鍵へのアクセスを共有していることを意味する。このようにして、ACR#1とACR#nは、鍵ID「鍵3」を有する鍵へのアクセスを共有しており、ここで、ACR#1とACR#nはACRのIDであり、「鍵3」は「鍵3」に関係付けられているデータを暗号化するのに使用される鍵の鍵IDである。同じを使用して複数のファイル又は複数のデータセットを暗号化及び／又は復号することもできる。

【0073】

10

SSAシステムは、システムに対する数種類のログインをサポートしており、そこでは、認証アルゴリズムとユーザー証明書は様々で、ユーザーが一旦首尾よくログインしてしまえばシステム内でのユーザーの特権である。図5で、再度、異なるログインアルゴリズムと証明書を示している。ACR#1は、パスワードログインアルゴリズムとパスワードを証明書として要求しているが、一方、ACR#2は、PKI（公開鍵インフラストラクチャ）ログインアルゴリズムと公開鍵を証明書として要求している。このようにして、ログインするには、エンティティは、有効なACRのID、並びに現在のログインアルゴリズムと証明書を提示する必要がある。

【0074】

20

エンティティが一旦SSAシステムのACRにログインしてしまうと、その許可（そのSSAコマンドを使用する権利）は、当該ACRに関係付けられている許可制御記録（PCR）内に定義される。図5では、図示のPCRによると、ACR#1は、「鍵3」と関係付けられているデータに対する読取り専用許可を許容しており、ACR#2は、「鍵5」と関係付けられているデータを読み取り及び書き込む許可を許容している。

【0075】

異なるACRは、読取り及び書き込みに使用する鍵の様なシステム内での共通の利益と特権を共有する。これを成し遂げるために、何か共通のものを有するACRがAGP-ACPグループ内にグループ分けされている。このようにして、ACR#1とACR#3は、鍵ID「鍵3」を有する鍵へのアクセスを共有している。

【0076】

30

AGP及びその中のACRは、階層ツリーに編成されており、よって、機密データの安全を守る安全鍵の作成の他にも、ACRは、自身の鍵ID／パーティションに対応する他のACRエントリも作成できるのが望ましい。それら子であるACRは、親（つまり作成者）と同じかそれよりも少ない許可を有することになり、親のACR自身が作成した鍵の許可が与えられる。付け加えるまでもなく、子であるACRは、彼らが作成するあらゆる鍵に対するアクセス許可を得る。これを図6に示す。このようにして、AGP120内のACRの全てはACR122によって作成され、当該ACRの内の2つは「鍵3」と関係付けられているデータへアクセスするための許可（複数の許可）をACR122から継承している。

【0077】

40

(AGP)

SSAシステムへのログオンは、AGPとAGP内のACRを指定することによって行われる。

【0078】

各AGPは固有のID（リファレンス名）を有しており、これがSSAデータベースへのエントリに対するインデクスとして使用される。AGPが作成されるとき、AGP名がSSAシステムに提供される。提供されたAGP名が既にシステム内に存在していれば、SSAは作成操作を拒絶する。

【0079】

次の欄で説明するように、AGPは、アクセス及び管理許可の委譲に関する制約を管理

50

するために使用される。図 6 の 2 つのツリーが果たす機能の内の 1 つは、2 つの異なるアプリケーション又は 2 つの異なるコンピュータユーザーのような、全く別々のエンティティによるアクセスを管理することである。そのためには、2 つのアクセスプロセスが、同時に起こったとしても、両者は実質的に互いに独立している（即ち、実質的にはクロストークが無い）ことが重要である。このことは、各ツリーにおける追加的な A C R 及び A G P の認証、許可、並びに作成が、他のツリーのそれらに結び付けられておらず、依存していないことを意味する。従って、メモリ 10 内で S S A システムを使用すると、これにより、メモリシステム 10 は、複数のアプリケーションを同時に対応できるようになる。更に、2 つのアプリケーションが、互いに独立している 2 つの別々のデータセット（例えば、写真のセットと歌曲のセット）にアクセスできるようになる。これを図 6 に示している。このようにして、図 6 の最上部のツリーのノード（A C R）を経由してアプリケーション又はユーザーがアクセスするための「鍵 3」、「鍵 X」、及び「鍵 Z」と関係付けられたデータは、写真を備えていてもよい。図 6 の最下部のツリーのノード（A C R）を経由してアプリケーション又はユーザーがアクセスするための「鍵 5」及び「鍵 Y」と関係付けられたデータは、歌曲を備えていてもよい。A G P を作成した A C R は、望ましくは A G P の A C P エントリが空である場合にのみ、それを削除する許可を有している。

10

【0080】

（エンティティの S S A エントリポイント：アクセス制御記録（A C R））

S S A システム内の A C R は、エンティティがシステムにログインを許可される方法を記述している。エンティティが S S A システムにログインするとき、行われるべき認証プロセスに対応する A C R を指定することが必要である。A C R は、図 5 に示している A C R 内で定義された方法で一旦認証されると、ユーザーが実行することのできる許容されたアクションを説明する、許可制御記録（P R C）を含んでいる。ホスト側のエンティティは、A C R データフィールドの全てを提供している。

20

【0081】

エンティティが首尾よく A C R にログオンされると、エンティティは、A C R パーティション及び鍵アクセス許可及び A C A M 許可（下で説明）の全てを問い合わせることができるようになる。

【0082】

（A C R の I D）

S S A システムエンティティがログインプロセスを開始するときには、全てのログイン要求が一致すると、S S A が正しいアルゴリズムを設定して正しい P C R を選択することができるようにするために、ログイン方法に対応する A C R の I D（A C R が作成されたときにホストによって提供されている）を指定する必要がある。A C R の I D は、A C R が作成されたときに、S S A システムに提供される。

30

【0083】

（ログイン／認証アルゴリズム）

認証アルゴリズムは、どんな種類のログイン手続きがエンティティによって使用されるか、及びユーザーの身分を証明するのにどんな種類の証明書が必要とされるかを指定する。S S A システムは、手続き無し（及び証明書無し）及びパスワードに基づく手続きから対称又は非対称何れかの暗号に基づくツーウェイ認証プロトコルまでに及ぶ幾つかの標準的な論理アルゴリズムをサポートする。

40

【0084】

（証明書）

エンティティの証明書は、ログインアルゴリズムに対応しており、ユーザーを確認し認証するために S S A によって使用される。証明書の一例は、パスワード認証の場合にはパスワード／P I N 番号、A E S 認証の場合には A E S 鍵、などである。証明書の種類／フォーマット（即ち、P I N、対称鍵など）は、事前に定義されており、認証モードから導き出され、即ち、A C R が作成されるときに S S A システムに提供される。S S A システムは、それら証明書の定義、分配、及び管理には関わっていないが、唯一例外として、P

50

K Iに基づく認証の場合には、R S A鍵ペアを生成するのにデバイス（例えば、フラッシュカード）が使用され、公開鍵が証明生成のためにエクスポートされる。

【0085】

（許可制御記録（PCR））

PCRは、SSAシステムにログインし、ACRの認証プロセスに首尾よく合格した後、エンティティに何が許容されるかを示す。3種類の認可カテゴリ、即ち、パーティション及び鍵の作成許可、パーティション及び鍵へのアクセス許可、及びエンティティ-ACR属性の管理許可がある。

【0086】

（アクセス用パーティション）

10

PCRのこの欄には、エンティティがACR段階を首尾よく完了するとアクセスできるパーティションの一覧が入っている（SSAシステムに提供されているそれらのIDを使用）。各パーティション毎に、アクセスの種類は、書込み専用又は読み取り専用に制約されることもあれば、完全な書込み／読取りアクセス権を指定することもある。このようにして、図5のACR#1は、パーティション#2へのアクセスを有しているが、パーティション#1へのアクセスは有していない。PCRで指定されている制約は、SSAパーティション及びパブリックパーティションに適用される。

【0087】

パブリックパーティションは、SSAシステムのホストであるデバイス（例えば、フラッシュカード）に対する通常の読取り及び書込みコマンド又はSSAコマンドの何れかによってアクセスされる。ルートACR（下記で説明）がパブリックパーティションを制約する許可付きで作成された場合、ルートACRはそれを自身の子に引き渡すことができる。ACRは、通常の読取り及び書込みコマンドがパブリックパーティションにアクセスすることだけを制約しているのが望ましい。SSAシステム内のACRは、作成時のみ制約されるのが望ましい。ACRは一旦パブリックパーティションから／に対する、読取り／書込みの許可を得たら、許可を取り上げられないことが望ましい。

20

【0088】

（アクセス用鍵ID）

30

PCRのこの欄には、エンティティのログインプロセスがACRポリシーを満たしたときにエンティティがアクセスできる鍵ID（ホストによってSSAシステムに提供されている）の一覧と関係付けられているデータが入っている。指定されている鍵IDは、PCRに現われるパーティション内に置かれている単一ファイル／複数ファイルと関係付けられている。鍵IDは、デバイス（例えば、フラッシュカード）内の論理アドレスとは関係付けられていないので、2つ以上のパーティションが特定のACRに関係付けられている場合、ファイルはそれらパーティションの内の何れか一方に在ることになる。PCR内で指定されている鍵IDは、それぞれが、異なるアクセス権のセットを有している。鍵IDによって指し示されるアクセス可能データは、書込み専用又は読取り専用に制約されることもあれば、又は完全な書込み／読取りアクセス権を指定していることもある。

【0089】

ACR属性管理（ACAM）

40

この欄では、或る特定の事例で、どのようにACRシステム属性が変更されるかを説明する。

【0090】

SSAシステム内で許可されるACAMアクションは、
AGP及びACRの作成／削除／更新、
パーティション及び鍵の作成／削除、
鍵及びパーティションへのアクセス権の委譲、
である。

【0091】

親ACRは、ACAM許可を編集できないのが望ましい。これには、ACRの削除と再

50

作成を必要とするのが望ましい。更に、ACRにより作成された鍵IDに対するアクセス許可は取り上げられないのが望ましい。

【0092】

(AGP及びACRの作成／削除／更新)

ACRは、他のACR及びAGPを作成する能力を有している。ACRを作成することは、更に、ACRクリエイタによって保有されているACAM許可の幾つか又は全てをACRに委譲することを意味する。ACRを作成する許可を有しているということは、以下のアクションの許可を有していることを意味する。

1. 子の証明書を定義し編集する－認証方法は、ACRを作成することによって一旦設定されたら編集できないのが望ましい。証明書は、子にとって既に定義されている認証アルゴリズムの境界内で変更される。

2. ACRを削除する。

3. 作成許可を子ACR（このようにして孫を有する）に委譲する。

【0093】

他のACRを作成する許可を有するACRは、それが作成する他のACRに非ブロック化の許可を委譲する許可を有している（が、他のACRを非ブロック化する許可は恐らく有していない）。父ACRは、子ACR内に親のアンブロッカに対するリファレンスを置く。

【0094】

父親のACRは、自身の子のACRを削除する許可を有する唯一のACRである。ACRが自身の作成した下位のACRを削除するとき、この下位ACRにより生み出された全ACRも自動的に削除される。ACRが削除されると、次いで、それが作成した鍵IDとパーティションが削除される。

【0095】

ACRが自身の記録を更新することができる2つの例外がある。即ち、パスワード／PINは、クリエイタACRによって設定されるが、更新はそれらを含んでいるACRだけができる。

ルートACRは、自身とそれが入っているAGPを削除できる。

【0096】

(鍵及びパーティションへのアクセス権の委譲)

ACRとそれらのAGPは、階層ツリーに組み立てられており、そこでは、ルートAGPと内部のACRは、ツリーの頂上にある（例えば、図6のルートAGP130と132）。SSAシステム内には幾つかのAGPツリーがあるが、それらは互いに完全に分離されている。AGP内のACRは、その鍵に対するアクセス許可を、それが入っている同じAGP内の全ACR及びそれらによって作成された全てのACRに委譲することができる。鍵を作成する許可は、鍵を使用するためのアクセス許可を委譲する許可を含んでいるのが望ましい。アクセス権を委譲する許可は、対応するACRの許可制御記録に属性として記憶される。

【0097】

鍵への許可は3つのカテゴリに分類される。

1. アクセス－これは、鍵、即ち読取り、書込みについてのアクセス許可を定義している。

2. 所有権－鍵を作成したACRは、定義により、その所有者である。この所有権は、1つのACRから別のACR（同一AGPに入っているか子のAGPに入っていることを条件とする）に委譲される。鍵の所有権は、それを削除する許可並びに各許可をそれに委譲する許可を提供する。

3. アクセス権委譲－この許可は、ACRが自身の保持する権利を委譲できるようにする。

【0098】

ACRは、自身が作成したパーティション並びに自身がアクセス許可を有している他の

10

20

30

40

50

パーティションへのアクセス許可を委譲することができる。

【0099】

許可委譲は、パーティションの名前及び鍵IDを指定されたACRのPCRに加えることによって行われる。鍵アクセス許可の委譲は、鍵IDによって、又はアクセス許可が委譲しているACRの作成された鍵全てを対象としていることを述べることによって、の何れかによる。

【0100】

(ACRのブロック化及び非ブロック化)

ACRは、システムとエンティティのACR認証プロセスが不成功に終わった場合に増分されるブロック化カウンタを有している。認証失敗が或る特定の最大数(MAX)に到達すると、ACRはSSAシステムによってブロックされる。

【0101】

ブロックされたACRは、ブロックされたACRによって参照される別のACRによって非ブロック化することができる。非ブロック化されたACRへの参照は、その作成者により設定される。非ブロック化ACRは、ブロックされたACRのクリエイタと同じAGP内にあり、「非ブロック化」許可を有することが望ましい。

【0102】

システム内の他のACRはどれも、ブロックされたACRを非ブロック化することはできない。ACRは、ブロック化カウンタを備えているが、アンブロックACRは備えていない構成であってもよい。

【0103】

(ルートAGP—アプリケーションデータの作成)

SSAシステムは、複数のアプリケーションを取り扱い、それら各々のアプリケーションのデータを孤立させるように設計されている。AGPシステムのツリー構造は、アプリケーション特定データを識別し孤立させるために使用される主要ツールである。ルートAGPは、アプリケーションSSAデータベースツリーの先端にあり、幾分異なる動作規則に従っている。SSAシステム内には幾つかのルートAGPが構成される。図6には2つのAGP130と132を示している。使用されるAGPの個数はこれより少なくとも多くてもよく、それらも本発明の範囲内にあることは明白である。

【0104】

新しいアプリケーションに備えてデバイス(例えば、フラッシュカード)を登録及び／又はデバイスに対する新しいアプリケーションの証明書の発行は、新しいAGP／ACRツリーをデバイスに追加するプロセスを通して行われる。

【0105】

SSAシステムは、ルートAGP作成(並びに、ルートAGPのACRの全て及びそれらの許可)の3つの異なるモードをサポートしている。

1. オープン: どんな種類の認証も要求されないあらゆるユーザー又はエンティティ、又はシステムACR(下記で説明)を通して認証されたユーザー／エンティティは、新しいルートAGPを作成することができる。オープンモードは、全データ転送がオープンチャンネルで行われるが何の安全対策も無しで(即ち、発行エージェンシーの安全な環境内で)、又はシステムACR認証を通して確立されたセキュアチャンネルを通して(即ち、無線(OTA)又は発行後手続き)、の何れかで、ルートAGPの作成を可能にする。

【0106】

システムACRが構成されていない(これはオプション特性である)場合、及びルートAGP作成モードがオープンに設定されている場合には、オープンチャンネルオプションしか利用できない。

2. 制御: システムACRを通して認証されたエンティティだけが、新しいルートAGPを作成することができる。システムACRが構成されていない場合は、SSAシステムがこのモードに設定されることはない。

3. ロック: ルートAGPの作成は使用禁止であり、システムへそれ以上ルートAGP

10

20

30

40

50

を追加することはできない。

【0107】

2つのSSAコマンドが、この特性を制御する（それらコマンドは認証無しであらゆるユーザー／エンティティにとって利用可能である）。

1. 方法構成コマンドー上記3つのルートAGP作成モードの何れか1つを使用するためにSSAシステムを構成するのに使用される。以下のモード変更、即ち：オープン→制御、制御→ロックしか許されていない（即ち、SSAシステムが現在は制御モードに構成されているのであれば、ロックモードへの変更しかできない）。

2. 方法構成ロックコマンドー方法構成コマンドを使用禁止にし、現在選択されている方法を永久的にロックするために使用される。

10

【0108】

ルートAGPが作成されると、それは、そのACRの作成と構成を可能にする特別な初期化モードになる（ルートAGPの作成に適用されたものと同じアクセス制約を使用）。ルートAGP構成プロセスが終わり、エンティティが明示的に動作モードに切り替わると、既存のACRはそれ以後更新できなくなり、追加的なACRはそれ以後作成できなくなる。

【0109】

ルートAGPは一旦標準モードに置かれると、ルートAGPを削除する許可を割り当てられているそのACRの1つを通してシステムにログインすることによってしか削除できない。これは、特別初期化モードに加え、ルートAGPのもう一つの例外であり、次のツリー階層内のAGPとは対照的に、それ自身のAGPを削除する許可を有するACRが入っているAGPだけであるのが望ましい。

20

【0110】

ルートACRと標準ACRの間の3番目で最後の違いは、パーティションを作成及び削除する許可を有するのはシステム内のACRだけである、ということである。

【0111】

（SSAシステムACR）

システムACRは、次の2つのSSA動作に使用される。

1. 適さない環境内で安全が確保されているチャンネルの保護下でACR／AGPツリーを作成する。

30

2. SSAシステムのホストであるデバイスを識別し認証する。

【0112】

SSA内には唯1つのシステムACRしかないのが望ましく、それが一旦定義されると変更されないのが望ましい。システム認証にとってシステムACRを何時作成するかは必要でない。即ち、SSAコマンドしか必要ない。システムACR作成特性は、使用禁止にすることができる（ルートAGP作成特性と同様）。唯1つのシステムACRしか許されないことが望ましいので、システムACRが作成された後は、システムACR作成コマンドには効力がない。

【0113】

作成プロセスの間、システムACRは動作できない。終了すると、システムACRが作成され、作動する用意が整ったことを示す特別なコマンドを発行する必要がある。この時点以後、システムACRは、更新も置換もできないのが望ましい。

40

【0114】

システムACRは、SSA内でACR／AGPを作成する。それは、ホストがそれに満足してそれをブロックするような時まで、ルートレベルを追加／変更する許可を有する。ルートAGPがブロックされると、基本的に、システムACRへのその接続が切断され、それを状態の証明に変える。この時点では、何者もAGP及びその中のACRを変更／編集できない。これはSSAコマンドを通して行われる。ルートAGPの作成の使用禁止は、永久的効果を有し、覆すことはできない。システムACRが関わる上記特性を図7に示している。システムACRは、3つの異なるルートAGPを作成するのに使用されている

50

。それらが作成された後の或る特定の時点で、SSAコマンドがホストから送られ、ルートAGPをシステムACRからブロックし、これにより、図7でシステムACRをルートAGPに接続している点線に示すように、ルートAGP作成特性が使用禁止にされる。これは、3つのルートAGPを状態証明に変える。3つのルートAGPは、ルートAGPがブロックされる前又は後に、子のAGPを作成して3つの別々のツリーを形成するのに使用される。

【0115】

上記特性は、コンテンツを有する安全な製品を作る際にコンテンツ所有者に高い柔軟性を提供する。安全な製品は「発行される」必要がある。発行は、デバイスがホストを識別しその逆もできるようにする識別鍵を付けるプロセスである。デバイス（例えば、フラッシュカード）の識別は、ホストがデバイスが有する機密を信用できる否かを決定できるようにする。他方、ホストの識別は、デバイスが安全ポリシーを実行する（特定のホストコマンドを許容し実行する）ことができるようにするが、それは、ホストがそうすることを許された限りの場合である。

【0116】

複数のアプリケーションに役立つように設計されている製品は、幾つかの識別鍵を有することになる。製品は、「事前発行」－出荷前の製造時に鍵が記憶されるか、又は「事後発行」－出荷後に新しい鍵が追加されることになる。事後発行の場合、メモリデバイス（例えば、メモリカード）には、アプリケーションをデバイスに追加することが許されているエンティティの識別に使用されている、何らかの種類のマスター又はデバイスレベルの鍵が入っている必要がある。

【0117】

上記特性は、製品が事後発行を可能／使用禁止にするように構成されることを可能にする。また、事後発行構成は、出荷後に安全に行われる。デバイスは、上記マスター又はデバイスレベルの鍵の他に何らの鍵も持っていない小売製品として買われ、その後、新しい所有者によって、更なる事後発行アプリケーションを可能にするかそれらを使用禁止にするように構成される。

【0118】

このようにして、システムACR特性は、上記目的を達成する能力を提供し

－システムACRを有していないメモリデバイスは、無制限且つ無制御なアプリケーション追加を許容することになる。

－システムACRを有していないメモリデバイスは、システムACRの作成を使用禁止にするように構成され、これは、（新しいルートAGP作成の特性も使用禁止されない限り）新しいアプリケーションの追加を制御する方法が無いことを意味する。

－システムACRを有するメモリデバイスは、システムACR証明書を使用した認証手続きを通して、セキュアチャネルを介した制御されたアプリケーションの追加だけが確立されることを許容する。

－システムACRを有するメモリデバイスは、アプリケーションが追加される前又は後に、アプリケーション追加特性を使用禁止にすることができるように構成される。

【0119】

（鍵ID一覧）

鍵IDは、特定のACR要求毎に作成されるが、メモリシステム10では、それらはSSAシステムだけによって使用されている。鍵IDが作成されるとき、以下のデータがACR作成によって又はACR作成に対して提供される。

1. 鍵ID。IDは、エンティティによりホストを通して提供され、鍵と、その後の全ての読取り又は書込みアクセスの際にその鍵を使用して暗号化され又は復号されるデータと、を参照するのに使用される。

2. 鍵暗号及びデータ完全性モード（上記のブロック化され、チェーン化され、ハッシュ化された各モードであり、下記で説明する）

【0120】

ホストによって提供されている属性に加え、以下のデータがSSAシステムによって保守されている。

1. 鍵ID所有者。所有者であるACRのID。鍵IDが作成されると、クリエイターであるACRがその所有者になる。しかしながら、鍵ID所有権は、別のACRに移転されてもよい。鍵ID所有者だけが、鍵IDの所有権を移転させること、及び鍵IDを委譲することができるようになってるのが望ましい。関係付けられている鍵へのアクセス許可の委譲、及びそれら権利の取消は、鍵ID所有者又は委譲許可を割り当てられた他のACRの何れかによって管理されることになる。上記動作の何れかを実行しようという試みがなされた場合には、SSAシステムは、要求しているACRが認可されたときに限り、何時でもそれを許容することになる。

2. CEK。これは、鍵IDに関係付けられる又は指し示されているコンテンツを暗号化するのに使用される。CEKは、SSAシステムによって生成される128ビットAESランダム鍵である。

3. MAC及びIV値。チェーン化ブロック暗号(CBC)方式暗号化アルゴリズムに使用される動的情報(メッセージ認証コード及び開始ベクトル)。

【0121】

図8A～図16のフローチャートを参照しながら、更に、SSAの様々な特性を説明してゆくが、ここで、ステップの左の「H」は、動作がホストによって行われることを意味し、「C」は、動作がカードによって行われることを意味する。システムACRを生成するために、ホストはメモリデバイス10内のSSAに、システムACRを生成するコマンドを発行する(ブロック202)。デバイス10は、システムACRが既に存在するか否かを調べることによって応答する(ブロック204、菱形206)。既に存在している場合は、デバイス10は、失敗を返し、停止する(長方形208)。存在していない場合、メモリ10は、システムACR作成が許されているか否かを調べて確かめ(菱形210)、許されていなければ失敗状態を返す(ブロック212)。システムACRを必要としないように、必要な安全特性が事前に決められている場合、システムACRの作成をデバイスの発行者が許していない事例もある。これが許されている場合は、装置10はOK状態を返し、ホストからのシステムACR証明書を待つ(ブロック214)。ホストは、SSA状態と、装置10がシステムACRの作成が許されていることを示しているか否かとを調べる(ブロック216及び菱形218)。作成が許されていない場合、又はシステムACRが既に存在している場合には、ホストは停止する(長方形220)。装置10が、システムACRの作成が許されていることを示している場合、ホストは、そのログイン証明書を定義し、それを装置10に送るSSAコマンドを発行する(ブロック222)。装置10は、受け取った証明書を使ってシステムACR記録を更新し、OK状態を返す(ブロック224)。この状態信号に応じて、ホストは、システムACRの準備が整っていることを示すコマンドを発行する(ブロック226)。装置10は、システムACRが更新も置換もできないようにロックすることによって応答する(ブロック228)。これにより、システムACRの特性、及びホストに対して装置10を識別するためのその身分、がロックされる。

【0122】

新しいツリー(新ルートAGP及びACR)を作成するための手続きは、それらの機能が装置内で構成される方法によって決まる。図9は、その手続きを説明している。ホスト24とメモリシステム10は共にそれに従う。新ルートAGPの追加が完全に禁止にされている場合、新ルートAGPは追加されない(菱形246)。それが可能でありシステムACRを求めている場合、ルートAGP作成コマンドを発行する(ブロック254)前に、ホストは、システムACRを通して認証し、セキュアチャネルを確立する(菱形250、ブロック252)。システムACRが求められていない(菱形248)場合、ホスト24は、ルートAGP作成コマンドを認証無しで発行し、ブロック254に進むことができる。システムACRが現実に存在している場合、ホストは、要求されていなくともそれを使用する(フローチャートには図示していない)。装置(例えば、フラッシュカード)は

10

20

30

40

50

、当該機能が使用禁止になっている場合は新ルートAGPを作成するというあらゆる試みを拒絶することになり、システムACRが求められている場合は認証無しに新ルートAGPを作成するという試みを拒絶することになる（菱形246と250）。ブロック254で新たに作成されたAGP及びACRは、当該AGPのACRが更新されるか別の方法で変更されることがないように、今度は動作モードに切り替えられ、どんなACRもそれらに追加することはできなくなる（ブロック256）。次に、システムは、追加的なルートAGPが作成されることのないように随意的にロックされる（ブロック258）。点線のボックス258は、このステップが随意的なステップであることを示しているという約束事である。本出願の各図面のフローチャートにおいて点線で示されている全てのボックスは随意的なステップである。これは、正規のコンテンツを備えた正規のメモリデバイス
10
を模倣するという他の違法目的のために、装置10が使用されるのを、コンテンツ所有者が防げるようにする。

【0123】

（上記ルートAGP内のACR以外の）ACRを作成する場合、図10に示す様に、ACRを作成する権利を有する何れのACRから開始してもよい（ブロック270）。エンティティは、ホスト24を通して、エントリポイントACR身分と、作成を希望する必要な属性を、全て備えているACRとを提供することによって、進入を試みる（ブロック272）。SSAは、ACR身分との一致、及び当該身分を有するACRがACRを作成する許可を有しているか否かを調べる（菱形274）。要求が認可されていると確認されると、装置10のSSAはACRを作成する（ブロック276）。
20

【0124】

図11は、図10の方法を使用した安全アプリケーションに有用なツリーを説明している2つのAGPを示している。このようにして、マーケティング用AGP内の身分m1を有するACRは、ACRを作成する許可を有している。ACR m1は、更に、鍵ID「マーケティング情報」と関係付けられているデータ及び鍵ID「価格一覧」と関係付けられているデータの読取り及び書込みのための鍵を使用する許可を有している。図10の方法を使用して、鍵ID「マーケティング情報」と関係付けられているデータにアクセスするのに必要な鍵に対する許可は有しておらず、鍵ID「価格一覧」と関係付けられている価格データにアクセスするための鍵に対する読取り許可しか有していない、2つのACR、すなわちs1とs2、を有するセールスAGPを作成する。この方法では、ACR s1とs2を有するエンティティは、価格データを読み取ることができただけで、それを変更することはできず、マーケティングデータに対するアクセスは有していない。他方、ACR m2は、ACRを作成する許可を有しておらず、鍵ID「価格一覧」及び鍵ID「マーケティング情報」と関係付けられているデータにアクセスするための鍵に対する読取り許可しか有していない。
30

【0125】

このようにして、アクセス権は上で説明した方法で委譲され、ここで、m1は、価格データを読み取る権利をs1とs2に委譲する。これは、大きなマーケティング及びセールスグループが関与している場合に特に有用である。販売人がいても一人か数人しかいない場合は、図10の方法を使用する必要はない。代わりに、アクセス権は、図12に示すように、ACRによって同一AGP内の下位又は同位のACRに委譲してもよい。最初に、エンティティは、ホストを通して、ツリー内で上記に説明した方法でACRを指定することによって、当該AGPのツリーに入る（ブロック280）。次に、ホストは、委譲相手のACRと委譲する権利を指定する。SSAは、その様なACRのツリーと、当該ACRが指定された別のACRに権利を委譲する許可を有しているか否かを調べる（菱形282）。そうであれば、権利は委譲され（ブロック284）、そうでなければ停止される。結果を図13に示している。この事例のACR m1は、読取り許可をACR s1に委譲する許可を有しているので、s1は、委譲後に、鍵を使用して価格データにアクセスすることができる。これは、m1が価格データにアクセスするための同一又はより大きな権利と、その様に委譲する許可を有している場合に行われる。1つの実施形態<18>では、
40
50

m 1 は、委譲後もそのアクセス権を保持している。アクセス権は、制限された期間中、制限されたアクセス回数など、制約された条件下で（永久的にはなく）委譲されるのが望ましい。

【0126】

鍵及び鍵IDを作成するプロセスを図14に示している。エンティティはACRを通して認証する（ブロック302）。エンティティは、ホストによって指定されたIDを使って鍵の作成を要求する（ブロック304）。SSAは、指定されているACRがそうする許可を有しているか否かを調べて確かめる（菱形306）。例えば、特定のパーティションのデータにアクセスするために鍵が使用されようとしている場合、SSAは、当該ACRがその様なパーティションにアクセスするか否かを調べて確かめる。ACRが認可されておれば、メモリ装置10は、ホストによって提供されている鍵IDと関係付けられている鍵値を作成し（ブロック308）、鍵IDをACRに記憶し、鍵値を自身のメモリ（コントローラに關係付けられているメモリ又はメモリ20の何れか）に記憶し、エンティティによって供給されている情報に従って権利と許可を割り当て（ブロック310）、当該ACRのPCRに当該割り当てられた権利と許可を加えて変更する（ブロック312）。このようにして、鍵のクリエイタは、書込み及び読取り許可、同一AGP内の他のACR又は下位のACRに委譲しそれらと共有する権利、及び鍵の所有権を移転する権利の様な、全ての利用可能な権利を有している。

10

【0127】

ACRは、図15に示すように、SSAシステム内の別のACRの許可を（又は存在も含め）変えることができる。エンティティは、前述の様にACRを通してツリーに入ることができ、1つの事例では、エンティティは認証され、次にACRを指定する（ブロック330、332）。それは、標的ACR又は標的ACR内の許可の削除を要求する（ブロック334）。指定されたACR又はこのときアクティブであるACRは、そうする権利を有し（菱形336）、標的ACRは削除されるか、標的ACRのPCRがその様な許可を削除するように変更される（ブロック338）。これが認可されない場合、システムは停止する。

20

【0128】

上記プロセスの後、標的は、このプロセス前にはアクセスできたデータにもはやアクセスできなくなる。図16に示すように、エンティティは、標的ACRに進入を試み（ブロック350）、以前は存在していたACRのIDがもはやSSA内に無いため、認証プロセスは失敗し、従ってアクセス権は否認されることが分かる（菱形352）。ACRのIDが削除されていないと仮定すると、エンティティが、ACRを指定し（ブロック354）、鍵ID及び／又は特定のパーティション内のデータを指定する（ブロック356）と、そこでSSAが、その様なACRのPCRに従って、鍵ID又はパーティションアクセス要求が許可されているかを調べて確認する（菱形358）。許可が削除されているか有効期限切れである場合、要求は再度否認される。そうでなければ、要求は許容される（ブロック360）。

30

【0129】

上のプロセスは、ACR及びそのPCRが別のACRによって変更されたばかりであったか、或いはその状態で開始されるように構成されていたかには関係なく、保護されているデータへのアクセスが装置（例えば、フラッシュカード）によってどの様に管理されるかを説明している。

40

【0130】

（セッション）

SSAシステムは、同時にログインした複数のユーザーを扱うことができるように設計されている。この特性は、SSAによって受け取られた全てのコマンドが特定のエンティティと関係付けられ、このエンティティを認証するのに使用されたACRが要求されているアクションへの許可を有している場合に限り実行されることを必要とする。

【0131】

50

複数のエンティティは、セッション概念を介してサポートされている。セッションは、認証プロセス中に確立され、SSAシステムによってセッションIDが割り当てられる。セッションIDは、システムへのログインに使用されるACRと内部的に関係付けられ、それ以降の全てのSSAコマンドに使用するためにエンティティにエクスポートされる。

【0132】

SSAシステムは、2つの型式のセッション、即ち、オープンセッションとセキュアセッションをサポートしている。特定の認証プロセスと関係付けられるセッションの型式は、ACR内で定義される。SSAシステムは、それが認証自体を実行する方法と同様の方法でセッションの確立を実行する。ACRはエンティティ許可を定義するので、この機構は、システムデザイナーが、セキュアトンネリングを、特定の鍵IDにアクセスすること又は特定のACR管理動作を実施すること（即ち、新ACRの作成及び証明書の設定）の何れかと関係付けることができるようにする。

【0133】

（オープンセッション）

オープンセッションは、セッションIDで識別され、パス暗号化を持たず、全てのコマンドとデータは暗号化されずに引き渡されるセッションである。この動作モードは、複数ユーザー又は複数エンティティ環境で使用されるのが望ましく、そこでは、エンティティは、脅威モデルの一部になることもパスを盗聴することもない。

【0134】

ホスト側のアプリケーション同士の間で、データの伝送を保護することも効率的なファイウォール化を可能にすることもないにもかかわらず、オープンセッションモードは、SSAシステムが、現在認証されているACRに許されている情報にのみアクセスすることができるようにしている。

【0135】

オープンセッションは、パーティション又は鍵が保護される必要がある場合にも使用される。しかしながら、有効な認証プロセスの後、アクセスはホスト上の全てのエンティティに対して許容される。認証されたACRの許可を得るために様々なホストアプリケーションが共有する必要があるものは、セッションIDである。これを図17Aに示している。線400より上のステップは、ホスト24が行うものである。ACR1に対してエンティティが認証された（ブロック402）後、それはメモリ装置10内の鍵ID Xと関係付けられているファイルへのアクセスを要求する（ブロック404、406、408）。ACR1のPCRが当該アクセスを許容すると、装置10は要求を許容する（菱形410）。そうでない場合は、システムはブロック402に戻る。認証が完了した後、メモリシステム10は、割り当てられたセッションID（ACR証明書ではない）だけによってコマンドを発行しているエンティティを識別する。オープンセッションにおいて、一旦ACR1がそのPCR内の鍵IDと関係付けられているデータへのアクセスを得ると、その他のアプリケーション又はユーザーは、ホスト24上の異なるアプリケーションの間で共有されている、正しいセッションIDを指定することによって、同じデータにアクセスすることができる。この特性は、1回だけログインできること、及び異なるアプリケーションにログインできるアカウントに結び付けられた全データにアクセスできることが、アプリケーションで好都合であり、ユーザーにとって更に便利である。従って、携帯電話ユーザーは、何度もログインすること無く、記憶されているEメールにアクセスして、メモリ20に記憶されている音楽を聴くことができる。他方、ACR1の範囲に含まれていないデータは、アクセスすることができない。このようにして、同じ携帯電話ユーザーは、別のアカウントACR2を通してアクセス可能であるゲーム及び写真の様な貴重なコンテンツを有している。たとえユーザーが、ユーザーの電話を借用する他人がユーザーの第1アカウントACR1を通して利用できるデータにアクセスすることは気に掛けなくても、先のコンテンツはユーザーがその他人にアクセスしてほしくないデータである。ACR1へのアクセスはオープンセッションで許容しながら、一方でデータへのアクセスを2つの別々のアカウントに切り離すことで、使用が簡単になると同時に貴重なデータの保護を与

10

20

30

40

50

えることもできる。

【0136】

ホストアプリケーション間でセッションIDを共有するプロセスをなお一層簡単にするため、ACRは、オープンセッションを要求しているとき、セッションに「0（ゼロ）」IDが割り当てられることを具体的に要求してもよい。このように、アプリケーションは、事前に定義されたセッションIDを使用するように設計することができる。唯一の制約は、明白な理由で、セッションを要求している1つのACRしか、ノーカット又は高品質バージョンのタイトルにアクセスする権利の購入を希望することができないことである。プレビューコンテンツは、エンドユーザーがノーカットのタイトルにアクセスできるものである場合は、限定されたn、0が特定の時期に認証される。セッション0を要求している別のACRを認証する試みは、拒絶されることになる。

10

【0137】

（セキュアセッション）

安全な層を追加するために、セッションIDは図17Bに示すように使用される。ここで、メモリ10はアクティブなセッションのセッションIDも記憶する。図17Bでは、例えば、鍵ID Xと関係付けられているファイルにアクセスできるようになるためには、エンティティは、ファイルにアクセスすることを許される前に、セッションID「A」の様なセッションIDも提供する必要がある（ブロック404、406、412、414）。この方法では、要求しているエンティティが正しいセッションIDに気づかない限り、メモリ10にアクセスすることはできない。セッションIDは、セッションが終了すると削除され、且つセッション毎に異なるために、エンティティは、セッション番号を提供することができたときにのみ、アクセスを得ることができる。

20

【0138】

コマンドが、認証された正しいエンティティから実際に来ていることを確認する方法は、SSAシステムにはセッション番号の使用以外には無い。アタッカーがオープンチャネルを使用して悪意のあるコマンドを送りつける脅威があるアプリケーション及びユーザーの場合は、ホストアプリケーションは、セキュアセッション（セキュアチャネル）を使用する。

【0139】

セキュアチャネルを使用する場合、セッションID並びにコマンド全体が安全チャネル暗号化（セッション）鍵で暗号化され、セキュアレベルは、ホスト側の実施と同じ程度に高い。

30

【0140】

（セッションの終結）

セッションが終結すると、ACRは以下のシナリオの何れか1つでログオフされる。

1. エンティティは明示的なエンドセッションコマンドを発行する。
2. 通信を時間切れにする。ACRパラメータの1つとして定義される期間中にコマンドを発行しなかった特定のエンティティ。
3. 全てのオープンセッションは、装置（例えば、フラッシュカード）がサイクルをリセット及び／又はパワー供給した後終結される。

40

【0141】

（データ統合化サービス）

SSAシステムは、SSAデータベース（全てのACR、PCRなどが入っている）の完全性を検証する。更に、データ統合化サービスは、鍵ID機構を通してエンティティデータに供される。

【0142】

鍵IDが、その暗号化アルゴリズムとしてハッシュされて構成されている場合、ハッシュ値は、CEK及びCEK記録内のIVと共に記憶される。ハッシュ値は、書込み動作中に計算され記憶される。ハッシュ値は、読取り動作中に再度計算され、それまでの読取り

50

動作中に記憶された値と比較される。エンティティが鍵IDにアクセスする度に、追加的なデータが古いデータに（暗号的に）連結され、適切なハッシュ値（読取り又は書込み用）が更新される。

【0143】

鍵IDと関係付けられているか鍵IDによって指し示されているデータファイルはホストしか知らないために、ホストは次の方法でデータ統合化機能の幾つかの態様を明示的に管理する。

1. 鍵IDと関係付けられているか鍵IDによって指し示されているデータファイルは、開始から終了まで書き込まれ又は読み取られる。SSAシステムはCBC暗号化方法を使用しており、データ全体をハッシュされたメッセージダイジェストとして生成するので、ファイルの一部にアクセスしようという試みは何れも混乱してしまう。

2. 中間のハッシュ値はSSAシステムによって保守されているので、連続的なストリームでデータを処理する必要は無い（データストリームは、他の鍵IDのデータストリームをインターリーブすることもこともできるし、複数のセッションを跨いで分割することもできる）。しかしながら、エンティティは、データストリームが再スタートされる場合は、SSAシステムにハッシュ値をリセットするように明示的に命令する必要がある。

3. 読取り動作が完了すると、ホストは、SSAシステムに、読み取られたハッシュを書込み動作時に計算されたハッシュ値と比較することによって、読み取られたハッシュを有効にするよう明示的に要求せねばならない。

4. SSAシステムは「ダミーの読取り」動作も提供する。この特性は、暗号化エンジンを通してデータを流すが、それをホストへ送り出すことはしない。この特性は、データが実際に装置（例えば、フラッシュカード）から読み出される前にデータの完全性を検証するのに使用される。

【0144】

（乱数の生成）

SSAシステムは、外部エンティティが、内部乱数生成器を利用し、乱数がSSAシステムの外部で使えるように要求することができるようにする。このサービスは、何れのホストにも利用可能であり、認証を必要としない。

【0145】

（RSA鍵ペアの生成）

SSAシステムは、外部ユーザーが、内部RSA鍵ペア生成特性を利用し、RSA鍵ペアがSSAシステムの外部で使えるように要求することができるようにする。このサービスは、何れのホストにも利用可能であり、認証を必要としない。

【0146】

SSAシステム及び付帯する特性の以上の詳細な説明は、主に、2004年12月21日出願の米国仮特許出願第60/638,804号からの抜粋である。

【0147】

（メディアコンテンツ配信の手段）

（環境及び異なる配信モデル）

図18は、上記メモリ装置10がメディアコンテンツを安全に記憶するために使用され、そこに記憶されたメディアコンテンツを制御された方法で配信するために使用される環境を説明している。図18に示すように、装置10内のメディアコンテンツは、携帯情報端末、ビデオゲーム機、携帯電話機502、MP3プレーヤーの様なメディアプレーヤー506、デスクトップ、ノートブック、又はラップトップの様なコンピュータ508を含め、多種多様なエンドユーザー端末又はホストによってレンダリングされる。メディアコンテンツ配信の新しい手段は、MNO504の様なサービスプロバイダによって、装置10を使用して実現される。MNO504は、送受話器502を通して装置10にメディアコンテンツを供給する。代わりに、装置10に記憶されているメディアコンテンツへのアクセスが制約されている場合は、装置10に記憶されているメディアコンテンツにアクセスするために、オペレータ504から送受話器502に権利及び／又は規則がダウンロー

ドされる。装置 10 内の暗号化されているメディアコンテンツに対するアクセスを規制している権利及び／又は規則は、装置 10 内のメディアコンテンツが送受話器 502 ではなくメディアプレーヤー 506 やコンピュータ 508 の様な他の種類の端末によってアクセスされる場合にも適用される。オペレータ 504 からメディアコンテンツ及び権利及び／又は規則を受け取るのではなく、装置 10 は、代わりに、その様なコンテンツ及び権利及び／又は規則を、インターネット経由でアカウント管理サーバ 510 の様な他のサーバ及びコンピュータ 508 を通して受け取ってもよい。その様なコンテンツ及び権利及び／又は規則は、オペレータ 504 によってコンピュータ 508 及びサーバ 510 に提供される。

【0148】

図 18 の環境では、メモリシステム又は装置 10 をメディアコンテンツの記憶及び配信のための手段として使用する複数の新しい手段が可能になる。このことを図 19A～図 19D に示している。購入コンテンツが事前にロードされているメモリ装置を使用してメディアコンテンツを配信する手段を、図 19A に示している。図 19A～図 19D では、フラッシュカードを例に使用しているが、同じ考察は、カード以外のフォーマット及び他の種類の不揮発性書込可能メモリにも適用できるものと理解頂きたい。このようにして、フラッシュメモリカード製造者 CM は、カードをコンテンツ発行者 CI に販売し、CI は更にメディアコンテンツをコンテンツプロバイダ CP から買い、その様なコンテンツを制御するための権利オブジェクトを権利オブジェクト (RO) サーバから受け取る。その様なコンテンツ及び権利オブジェクトがカードにロードされる前に、CI は、先ず認証サーバへの接続によってカードが正規であるか否かを検証する。コンテンツ及び権利オブジェクトは、カードが正規であると確かめられた後にロードされる。

【0149】

図 19A から分かるように、コンテンツ発行者 (CI) から向きを表している矢印は 2 つの分枝を有しており、一方はサービスプロバイダ SP へと上側を指しており、下側の矢印はエンドユーザー EU を指している。CI は、コンテンツを備えたカードを、図 19A の CI と EU の間の下側の矢印に沿ってエンドユーザー EU に直接販売するか、或いは、CI と SP の間の上側の矢印に沿ってサービスプロバイダ SP に販売するか、何れかの方法で販売する。上側の矢印に沿った取引をこれから説明する。

【0150】

従って、コンテンツ発行者は、カード製造者 CM であってもよいが、カードを MNO の様なサービスプロバイダに販売する。すると、サービスプロバイダは、このカードを、元の機器製造者 (以下「OEM」と呼ぶ) によって提供されている携帯電話機の様なエンドユーザー端末と一緒にエンドユーザーに販売する。図 19A～図 19D では、隣にドル記号が付いている矢印は、各図に示されている矢印の方向に沿った当事者間での可能な収益の流れを示している。コンテンツ発行者がカードをサービスプロバイダに販売する前に、コンテンツ発行者は、ここに説明している型式の制御構造をインストールする。しかしながら、その様な制御構造は、サービスプロバイダが適切だと思ふ方法でコンテンツの配信を制御できるように、サービスプロバイダが自身の安全環境を作成し、下記で説明するようにサービスプロバイダによってインストールされるのが望ましい。これが起こる前に、カードは、正規であることを再度検証される。このようにして、サービスプロバイダ側のファシリティで、カードは、認証サーバへの接続によって再度認証される。カードは、更に、カード内であらゆる特定の特性又はアプリケーション (例えば、メディアプレーヤーの様なメディアコンテンツレンダリングアプリケーション) を使用可能に又はアクティブにするために、端末を介して認証サーバに接続される。次に、サービスプロバイダは、カード内のコンテンツへのアクセスを制御するために、下で説明する型式の制御構造をインストールする。制御構造は、確実に、認証されたユーザーだけがコンテンツにアクセスすることができ、その様なアクセスが、制御構造内の或る特定の許可又は或る特定の権利及び／又は規則に準じるようにする。

【0151】

代わりに、コンテンツ発行者からエンドユーザーに向かっている下側の矢印により示すように、コンテンツ発行者は、カードをエンドユーザーに直接販売してもよい。エンドユーザーは、携帯電話機のような端末をOEMから入手する。その様な端末及びカードは下で説明する方法で相互に認証されることを前提として、エンドユーザーは、ここでその端末を使用してコンテンツにアクセスすることができる。相互認証の1つのプロセスを下に説明する。

【0152】

メディア配信の上記手段は、カードにはエンドユーザーが既に購入したコンテンツしか入っていない場合の方法である。この構成では、エンドユーザーには、コンテンツにアクセスするための証明書の様な必要な認証情報が提供される。これにより、その様な認証手段を提供されていない他者が認可されていない方法でコンテンツにアクセスすることが防止される。

【0153】

図19Bは、本発明の別の実施形態を示すメディアコンテンツ配信の別の手段を説明しているフロー図である。コンテンツをカードにインストールし、これによりカードがエンドユーザーに届く段階は、図19Aのものと同様である。図19Bの方式は、図19Aの方式で無制約のレンダリングが可能になっているのとは違い、カードにロードされたコンテンツは、プレビュー目的で或る特定の制約付きでレンダリングすることしかできないこと（例えば、コンテンツの一部又は低品質バージョンのレンダリングのためのアクセス、又は制限された回数又は期間だけのアクセス）が、図19Aのものと相違している。換言すると、エンドユーザーがメディアコンテンツを完全に楽しみたいと願うなら、ユーザーは、プレビュー付きのコンテンツとしてではなく、制約無しにその様なメディアコンテンツの省略されていないバージョンにアクセスしてレンダリングする権利を最初に購入せねばならない。このようにして、購入後に、エンドユーザーはサービスプロバイダから省略されていない完全なバージョンに制約無しにアクセスしレンダリングする。しかしながら、エンドユーザーが、前記目的に適切な権利をダウンロードできるようになる前に、カードは認証サーバによって再度正規であることが検証される。その様な認証の後、権利発行者は、権利オブジェクトの様な制御構造をサービスプロバイダに提供し、サービスプロバイダは、これをエンドユーザーに提供してダウンロードできるようににする。1つの実施形態では、権利オブジェクトは、エンドユーザー（又は、ホスト上のアプリケーションの様な他のエンティティ）が暗号化されているメディアコンテンツにアクセスするための証明書、及びその様なアクセスを規制している権利及び／又は規則を備えている。異なる実施形態では、権利オブジェクトには、暗号化されているメディアコンテンツを復号するのに使用できる実際のコンテンツ暗号化鍵が入っている。権利オブジェクトに実際のコンテンツ暗号化鍵が入っている場合、権利オブジェクト内の証明書は、秘密コードとメモリ装置IDを、ハッシュ機能の様な機能によるシード値として使用して、オンザフライで生成されるものである。この様式は、権利オブジェクトに実際のコンテンツ暗号化鍵が入っていない場合にでも適用することができる。エンドユーザーには、更に、購入時に、プレビューコンテンツの省略されていない高品質バージョンをダウンロードすることなどによって、事前にロードされているコンテンツをアップグレードするというオプションもある。

【0154】

代わりに、プレビューコンテンツが、コンテンツ発行者によって図19Aに説明している方法でロードされている場合には、その様なコンテンツは、更に、メディアコンテンツの暗号化され且つ省略化されていないバージョンを含んでいる。このようにして、エンドユーザーがその様なカードを購入するとき、カードには、ユーザーが購入したいと希望するメディアコンテンツの暗号化されているバージョンが既に記憶されていることになる。カードには、カード内のコンテンツの省略化されたバージョン又は一部分にしかアクセスできないようにエンドユーザーの権利を制約する権利及び／又は規則も記憶されている。その様な環境では、その様なコンテンツをカードに再度ダウンロードする必要は無い。代わりに、エンドユーザーが必要なのは、メディアコンテンツを復号するためのコンテンツ

暗号化鍵と、制約されていない又はより緩いアクセスを許可するための、その様なアクセスを規制している権利及び／又は規則への更新だけである。その様な情報は、認証後に権利発行者からサービスプロバイダを通してダウンロードされることになる。

【0155】

図19Cは、メディアコンテンツ配信の更に別の手段を説明しているフロー図である。図19A及び図19Cを比較すると、図19Cの方式では、カード内のコンテンツは、エンドユーザーがサービスプロバイダによって提供されている様なサービスのサブスクリプションをした後にしかアクセスできないという点以外、2つの方式が実質的に同じであることが明らかである。このように、エンドユーザーによって購入されたカードには、エンドユーザーがサブスクリプションをするまではエンドユーザーがコンテンツへアクセスするのを許可しないという制御情報が入っている。図19Cに示すように、エンドユーザーは、最初にカードをコンテンツ発行者から購入するが、サービスプロバイダからサブスクリプションを購入するまでは、中のメディアコンテンツにアクセスすることはできない。それより以前、サブスクリプションの確認に先立ち、エンドユーザー所有のカードは、認証サーバと、認証サーバによって随意的に使用可能又はアクティブにされる内部のアプリケーション（例えば、メディアプレーヤーの様なメディアコンテンツレンダリングアプリケーション）とによって、正規であることが検証される。サブスクリプションのプロセスでは、権利発行者によって提供されている権利オブジェクトは、サービスプロバイダによってエンドユーザーに送信され、カードへダウンロードできるようになる。取引はサブスクリプションに基づいているので、収益の流れがエンドユーザーからサービスプロバイダを通して権利発行者に循環するように、エンドユーザーは、サブスクリプションの支払いを定期的に行う必要がある。

【0156】

図19Dは、メディアコンテンツ配信の別の手段を説明しているフロー図である。この方式では、エンドユーザーによって購入されたカードには、メディアコンテンツが事前にロードされていない。このように、エンドユーザーは、サービスプロバイダからコンテンツを購入せねばならず、サービスプロバイダは、コンテンツプロバイダサーバからコンテンツを入手することになる。それより以前、コンテンツのカードへのローディングに先立ち、カードは認証サーバによって認証される。特性及びアプリケーション（例えば、メディアプレーヤーの様なメディアコンテンツレンダリングアプリケーション）は、認証サーバによって随意的に使用可能にされる。プロセスの一部として、権利発行者を起源とする権利オブジェクトは、サービスプロバイダを通してエンドユーザーに送信され、カードへダウンロードされる。この処理は、エンドユーザーが権利発行者とサービスプロバイダに定期的に支払いを行わねばならないようなサブスクリプションに基づいている。エンドユーザーによって購入されたカードには、メディアコンテンツが事前にロードされていないが、カードは、エンドユーザーにその様なコンテンツをダウンロードする資格を与える権利オブジェクト（複数のオブジェクト）が記憶されている。これは、この場合はプリペイドカードであり、エンドユーザーが、購入したコンテンツを繰り返しダウンロードできるようにする。

【0157】

（装置10の異なるモジュールと機能）

図20は、装置の異なる領域に異なる機能が記憶されているメモリ装置10の1つの実施形態のブロック図である。図20に示すように、装置10は、図18のオペレータ504の様なMNOによって関係付けられるか所有されている暗号化されたコンテンツの様な保護されているオペレータコンテンツを記憶しているコンテンツ領域を有している。コンテンツ領域には、下で更に詳しく説明するが、暗号化されている及び／又は暗号化されていない事前にロードされたコンテンツも記憶されている。コンテンツ領域には、制約されていないユーザーコンテンツ、並びに暗号などにより制約されロックされているユーザーコンテンツも記憶されている。

【0158】

装置 10 のセキュア領域は、下で更に詳しく説明する D R M エージェントの様なソフトウェアコードによって実施される複数の異なる機能を含んでいる。装置 10 のセキュア領域は、上で説明している隠されたパーティションを使用して実施されている。コンテンツ暗号化鍵、証明書、及び認証マネージャも、セキュア領域に記憶されている。上で説明した A G P / A C R の様な制御構造は、認証マネージャの一部を形成している。セキュア領域には、M N O オペレータ用のアプリケーションと管理も記憶される。装置 10 は、通信領域に、携帯電話機概念部とサーバエージェントを記憶している。それらは、装置 10 が送受話器によって操作される場合に有用である。

【0159】

図 21 は、図 19 A ~ 図 19 D の異なるメディアコンテンツ配信方式を実施するためのシステムアーキテクチャのブロック図である。図 21 に示すように、メモリ装置 10 は、可能な実施形態として、セキュア記憶部を備え、それはアクセス制御記録 (A C R) 又は権利オブジェクト (「R O」) と共にコンテンツ暗号化鍵を使用した、隠されているパーティションと暗号化の上記特性を活用しているのが望ましい。装置 10 は、更に、(装置のセキュア領域に記憶されている D R M を含んでいるかその一部である) アクセスマネージャを含んでおり、アクセスマネージャは、現在商業的に使用されている異なるデジタル権利管理 (D R M) エージェントとインターフェースすることができる。それらには、例えば、携帯電話の送受話器に一般に使用されているモバイル D R M エージェント、及びパーソナルコンピュータ上で現在一般に使用されている W i n d o w s (登録商標) 3 2 D R M エージェントが含まれる。この方式では、装置 10 のアクセスマネージャは、コンテンツ及び権利オブジェクトのダウンロード (又は権利オブジェクトの更新) 並びに装置 10 内のアクセス制御記録又は権利オブジェクト内の許可の変更を目的として、エンドユーザー端末の様々な種類の D R M エージェントとインターフェースすることができる。

【0160】

このように、メディアコンテンツが、図 19 A ~ 図 19 D の S P サーバから装置 10 にダウンロードされようとするとき、図 21 のアーキテクチャは、最初にメディアコンテンツをコンテンツサーバ 5 2 2 から D R M サーバ 5 2 4 に送ることによって、その様なダウンロードを実施する。コンテンツサーバ 5 2 2 は、コンテンツプロバイダサーバからコンテンツを受け取るサービスプロバイダに設置されている。代わりに、メディアコンテンツが、サービスプロバイダを経由すること無しにコンテンツプロバイダから直接ダウンロードされる場合は、コンテンツサーバ 5 2 2 は、コンテンツプロバイダ側のファシリティに配置されている。D R M サーバ 5 2 4 は、M N O、及び図 18 及び図 19 A ~ 図 19 D に関して上で説明した送受話器、パーソナルコンピュータ、及び他の端末を通してメディアコンテンツをダウンロードするための他のエンティティ、への支払いを管理する支払いサーバ 5 2 6 と通信している。このようにして、複数の支払いサーバ 5 2 6 の内の 1 つによって支払いの証明が提供された後、D R M サーバ 5 2 4 は、権利オブジェクトとメディアコンテンツをコンテンツサーバ 5 2 2 から端末 (図 21 の送受話器 5 2 8 又はパーソナルコンピュータ 5 3 0) に送信する。D R M エージェント 5 2 8 a 又は 5 3 0 a は、次いでメディアコンテンツと権利オブジェクトを装置 10 のアクセスマネージャに送信し、そこで、アクセスマネージャは、上記メディアコンテンツを装置 10 の或るパーティションに記憶する。権利オブジェクトは、図 21 には図示していない権利発行者からサーバ 5 2 4 によって入手される。上で説明した権利オブジェクトを送信する代わりに、D R M エージェント及びアクセスマネージャは、既に装置 10 に記憶されている権利オブジェクトを変更又は更新してもよい (例えば、新規又は追加の権利の購入後)。A C R、A G P、及び R O の様な制御構造のインストール及び変更は、同様の方法で行われる。ここで説明している、メディアコンテンツと権利オブジェクトが送信されるか変更されるプロセスは、セッション鍵を使った上記型式のセキュアセッションを介して行われるのが望ましい。このようにして、証明書又は他の認証情報並びに復号されたメディアファイルは、それらが送信される前にセッション鍵で暗号化される。これは、A C R、A G P、及び階層ツリーの様な他の型の制御構造が、メモリ装置内で、サーバと通信している端末を介して作成されるか変

更される場合にも当てはまる。

【0161】

図20に明白に示しているように、装置10のアクセスマネージャは、DRMサーバ524とインターフェースし、そこからのコマンドを直接取り扱うことができるDRMエージェントを含んでいるので、送受話器528及びコンピュータ530の様なエンドユーザー端末がDRMエージェントを含んでいなくても、装置10のアクセスマネージャは、制御構造のインストール又は変更及びメディアコンテンツと権利オブジェクトのダウンロードの様な上記機能をなお実施することができる。

【0162】

(プレビューコンテンツを備えたメモリ装置)

図22は、支払われたメディアコンテンツと未払いのカタログメディアコンテンツが入っているメモリ装置を示しているブロック図であり、メディアコンテンツを配信するための1つの可能な手段を説明している。先に図19Aに関して説明したように、支払われたメディアコンテンツと未払いのカタログメディアコンテンツを含むコンテンツはメモリ装置10にダウンロードされるので、その様なコンテンツを含んでいるメモリ装置は、図22で符号10"を付けられている。メモリ装置には、支払われたコンテンツへのアクセスを制御するための対応する権利オブジェクトもロードされる。図22に示すように、1つの実施例では、権利オブジェクトは、携帯電話機又はパーソナルコンピュータの様な端末を介した、支払われたコンテンツへの無制限のアクセスを許可するが、パーソナルコンピュータライブラリへのコンテンツの移動は3回しか許可せず、これは随意的な特性である。代わりに、随意的な特性は、適切な証明書を有するものは誰でも、支払われたメディアコンテンツを、端末又は他の端末で動作しているソフトウェアアプリケーションによって、3回までならエクスポートして記憶させることができるようになっていてもよい。

【0163】

しかしながら、カタログメディアコンテンツに関しては、装置10"を購入することで、購入者がカタログメディアコンテンツへの完全な権利を有することが許可されるわけではない。代わりに、購入者の権利は、多種多様な方法で制限され又は省略化される。例えば、図22に示すように、カタログメディアコンテンツをプレビューする権利は、持続時間又は回数又は計数によって制限される。代わりに、メディアタイトルの選択された部分(例えば、歌曲又は映像の15秒分)だけが制約無くアクセスされるか、或いはアクセスできるものが低品質バージョンだけであってもよい。このように、省略化されていない完全な品質のカタログ化されたメディアタイトルへの無制約のアクセスを得るためには、購入者は、先ずその様な権利を購入する必要がある。購入される権利は、単一のメディアコンテンツファイル又はコンテンツファイルの完全なアルバムであってもよい。図22に示す実施形態では、カタログ化されたメディアタイトルの省略化されていない完全なバージョンは、装置10"に実際に記憶されているが、購入者がメディアタイトルの省略化されていない完全なバージョンにアクセスすることができないように暗号化されている。購入後、購入されたメディアコンテンツファイルは、ロックを解除され、購入者によるアクセスが許可される。

【0164】

代わりの実施形態では、装置10"内のカタログ化されているメディアタイトルの省略化されていない完全なバージョンは、装置10"内に前以て記憶されていない。このようにして、購入者が、完全なアクセスの権利を購入した後、その様なメディアタイトルは、上記方法などで、その様なタイトルへのアクセスを制御する権利オブジェクトと共にダウンロードされねばならない。装置10"が関与するコンテンツのロック解除プロセスを図23A～図23Cのフローチャートに示している。図23A～図23Cではフラッシュメモリカードが例として使用されているが、同じ考えは、カード以外のフォーマット及び他の種類の不揮発性書込可能メモリにも適用できるものと理解頂きたい。

【0165】

エンドユーザーが装置10"内のカタログ化された暗号化されているメディアコンテン

ツの様な、制約されているメディアコンテンツのサンプルへのアクセスを要求したことに
対して、端末の様なレンダリング装置が応答する（ブロック552）。フラッシュメモリ
カードの様な装置10”は、その様な要求に応答して、レンダリング装置又は端末に、要
求されているメディアサンプルを提供する（ブロック554）。メディアサンプルファイル
には、図19A～図19Dに関して示しているサービスプロバイダのサーバのアドレス
又は図21に示しているDRMサーバのアドレスの様な、ロック解除の権利を購入するこ
とができるようなサーバのインターネットアドレスに関係している情報が入っているのが
望ましい。レンダリング装置は、装置内で動作しているソフトウェアアプリケーションに
より、フラッシュカード10”からメディアサンプルを再生又はレンダリングし、ユーザ
ーにサンプル化されているメディアタイトルに対する無制約な権利を購入することを促し
、ユーザーのために購入を取り扱うサーバのインターネットアドレス情報を提供する。そ
の様なソフトウェアにより、レンダリング装置又は端末は、次に、ユーザーが、サンプ
ル化された省略化されていない完全なメディアタイトルのロックを解除するための権利を購
入したいかどうかについて、ユーザーに問い合わせる（ブロック556）。ユーザーが購
入を希望しない旨を返答すると、プロセスは終了する。しかしながら、ユーザーが購入の
意思を示すと、レンダリング装置又は端末は、次いで、ユーザーコマンドに応答して購入
を取り扱うサーバに接続する（ブロック558）。レンダリング装置又は端末は、次いで
、ユーザーによって入力されたユーザー購入認可及び他の情報をサーバ（SPサーバ又は
DRMサーバ）に送る（ブロック560）。

10

【0166】

20

上で指摘したように、権利オブジェクトには、コンテンツ暗号化鍵とその様な鍵へのア
クセスが許容される前に適切な証明書の提示を要求する認証情報、及び復号されたメデ
ィアファイル又はタイトルがどのように使用できるかに関する権利及び／又は規則が入っ
ている。1つの実施形態では、装置10”内のカタログメディアタイトルの何れについても
権利オブジェクトは一切記憶されていない。その様な状況では、カタログメディアタイ
トルを復号し制御するための権利オブジェクトは、SPサーバ又はDRMサーバなどからダ
ウンロードされねばならない。

【0167】

別の方法では、装置10”には、カタログメディアタイトルの制約されたプレビューし
か許可しない権利が既に入っている。プレビューされるカタログの省略化されているメ
ィアタイトルは、ロックされているカタログの省略化されていない暗号化されているメ
ィアタイトルとは別のファイルとして記憶される。このように、プレビューメディアタイ
トルは、完全なメディアタイトルの一部分（例えば、15秒分）又はその様なタイトルの
低品質バージョンから構成されている。別の方法では、プレビューメディアタイトルは、
別個のファイル内に記憶されておらず、その場合、ロックされているカタログの暗号化さ
れているメディアタイトルの一部又は品質を下げたものは、プレビューとして制約無しに
利用可能にされている。プレビューメディアタイトルは、更に、完全な長さのメディアタ
イトルを備えているが、その場合、プレビュー動作は持続時間又は回数の何れかによっ
て制限されている。上記制約は、装置10”内に既に記憶されている権利オブジェクトによ
って課される。このようにして、カタログメディアタイトルの権利オブジェクトが装置1
0”内に既に記憶されている場合、その様な権利オブジェクトは、購入者によって購入さ
れた後にロック解除の権利を使って更新される必要があり、これにより、更新後の権利
オブジェクトは、装置10”内の暗号化されている省略化されていないカタログメディア
タイトルへの完全なアクセスを許可することになる。このように、ユーザーが認証を購
入し、ブロック560で他のユーザー情報がSP/DRMサーバに送られた後、レンダリング
装置又は端末は、装置10”がまだ権利オブジェクトを有していない場合は、ダウンロ
ードされた権利オブジェクトが（例えば、DRMエージェントにより）装置10”のセキュ
ア領域に記憶されるようにし、或いは装置10”内に既に在る権利オブジェクトが更新さ
れて、現在の更新された権利オブジェクトに従って購入されるメディアタイトルへのアク
セスが許可されるようにする（ブロック562及び564）。

30

40

50

【0168】

ブロック560で、レンダリング装置又は端末からのユーザー要求に応答して、サーバ（例えば、SP又はDRMサーバ）は、エンドユーザーから支払いを得るためにユーザー情報を図21の請求書作成サーバ526に送ることによって応答する（ブロック566）。サーバ（例えば、SP/DRM）は、レンダリング装置又は端末に、カード上に記憶させるため又はカード上の権利オブジェクトを更新するための権利オブジェクト情報を提供する。権利オブジェクトは、鍵と、望ましくは、購入されたロックされている（暗号化されている）メディアタイトルを復号するための鍵にアクセスするための証明書を作成するための情報とを含んでいる（ブロック568）。

【0169】

上記プロセスでは、権利オブジェクトは、カタログメディアタイトルを復号するためのコンテンツ暗号化鍵を含んでいる。そのような事象では、鍵は、タイトルを復号するために装置10”に記憶される。しかしながら、認可されていない使用の可能性を減らすために、そのような鍵へのアクセスは、そのような鍵にアクセスするための正しい証明書を有するエンドユーザーに限定される。そのような証明書は、端末により、及び装置10”によって、端末の固有IDを、装置10”と端末両方のハッシュ関数のような関数によるシード値として使用して、オンザフライで生成される。このようにして、端末が装置10”により認証されていれば、装置10”はそのような証明書を生成することもでき、鍵へのアクセスは（装置10”と端末によって生成された）証明書の2つのセットが一致したときに限り許容される。装置10”の固有IDを使用して装置10”を認証する場合に、同様のプロセスが使用される。両方のプロセスが実行される場合、方式は相互認証方式になる。

【0170】

他の更に安全な代替案として、権利オブジェクトは、カタログメディアタイトルを復号するためのコンテンツ暗号化鍵自体ではなく、そのような鍵にアクセスするための或る特定の証明書しか含んでいない。例えば、証明書は、上記ACR構造により規制されているアクセスを可能にするものである。このようにして、各カタログメディアタイトルが、タイトルの復号に使用できる対応するコンテンツ暗号化鍵を有する対応するACRを有している場合、権利オブジェクトからそのようなACRへ証明書を供給することによって、タイトルの復号が可能になる。そのような事象では、エンドユーザーは、そのようなタイトルが復号されレンダリングできるようになる前に、全てのカタログタイトルのACRのそれぞれに証明書（並びに、支払済みのコンテンツが同様にACRによって保護されている場合には、支払済みコンテンツのACRにアクセスするための証明書）を入力することが必要になる。エンドユーザーは、そこで、多数の証明書を見失わないようにする必要がある。これより、図24を見ながら、更に使いやすい機構を説明する。

【0171】

図24は、上記アクセス制御記録（ACR）及び委譲属性を使用して、装置10”内のロックされているカタログメディアコンテンツをロック解除するための更に別の実施形態を説明しているブロック図である。このように、装置10”の制御構造は、2つのAGP572と574を含んでいる。AGP572は、DRM__ACRを含んでいる。DRM__ACRは、3つの異なる支払済みコンテンツメディアファイルの権利オブジェクトを制御する。それら権利オブジェクトは、例えば、コンテンツをパーソナルコンピュータライブラリに移動させるための、又はコンテンツを別の端末にエクスポートするための限定された権利を制御している。

【0172】

AGP574には、playback__ACR576と、3つの支払済みメディアコンテンツタイトルのコンテンツ暗号化鍵へのアクセスを制御するための3つのpaid__ACR578と、まだ支払われていない3つの対応するカタログメディアタイトルのコンテンツ暗号化鍵へのアクセスを制御するための3つのcatalog__ACR580を含む、7つのアクセス制御記録が入っている。図24に示すように、playback__ACR576からpaid__ACR578に向かう矢印582は、3つのpaid__ACR5

78が自分たちのコンテンツ暗号化鍵に対する権利をplayback__ACR576に委譲したことを示しているので、3つのpaid__ACR578によって制御されている3つの支払済みのメディアタイトルを復号するのに使用されるコンテンツ暗号化鍵にアクセスするために、3つのpaid__ACR578に証明書を提示する必要はない。代わりに、正しい証明書をplayback__ACR576に提示することによって、3つの支払済みメディアタイトルを復号するためのコンテンツ暗号化鍵にアクセスできるので、エンドユーザーにとっては、証明書は3つ又はそれ以上のセットではなく1セットだけ覚えておけばよく、更に好都合である。

【0173】

上記実施形態では、ダウンロードされるか更新された権利オブジェクトには、個々のカタログ又は支払済みメディアタイトルを復号するための鍵にアクセスするためのACR内の証明書が入っている。代替の実施形態では、ダウンロードされるか更新された権利オブジェクトには、代わりに、DRM__ACRに対する証明書が入っている。DRM__ACRは、catalog__ACR580に、3つの未払いのカタログメディアタイトルを復号するためのコンテンツ暗号化鍵にアクセスする自身の権利をも、やはりplayback__ACR576に委譲させる、許可を有している。このようにして、権利オブジェクトがダウンロードされるか更新された後、端末又は装置10”の何れかのDRMエージェントは、権利オブジェクトからの証明書を提示することによってDRM__ACRにアクセスして、DRM__ACRにその権利を実行させ、委譲を起こさせる。図24に説明している実施形態では、請求書作成サーバが、図23のブロック566のエンドユーザーから支払いを受けたことを確認した後、catalog__ACR580は、次に、3つの未払いのカタログメディアタイトルを復号するためのコンテンツ暗号化鍵へアクセスする自身の権利を、やはりplayback__ACR576に委譲する。このことは、図24の点線584によって示されている。このようにして、委譲後、適切な証明書の単一セットだけをplayback__ACR576に提示することによって、catalog__ACR580によって制御されているメディアタイトルを復号するためのコンテンツ暗号化鍵にアクセスし、同時に、ACR578によって制御されている支払済みメディアタイトルを復号するための鍵もアクセスできるようになる。

【0174】

図24に示しているように、更に安全を追加した策として、権利オブジェクトには、DRM__ACRの証明書の代わりに秘密コードが入っている。DRM__ACRの証明書は、関数を使って、この秘密コードと装置10”のIDからオンザフライで生成される。playback__ACRの証明書は、関数を使って、秘密コードと装置10”のIDから同様の方法で生成される。エンドユーザーが入力する必要があるのは、playback__ACR576の証明書を生成するための秘密コードだけである。ACRの代わりに、上記方式は、権利オブジェクトを使用して実現することもでき、その場合、メディアファイルへのアクセスを制御している異なる権利オブジェクトには、その様なファイルにアクセスする許可を再生権利オブジェクトに委譲する権利が入っている。

【0175】

コンテンツレンダリングのプロセスは、図25Aと図25Bのフローチャートに示されている。レンダリング装置又は端末上の信頼されているアプリケーションは、メディアタイトルへアクセスしたいというユーザー要求とアクセスのための証明書又は秘密コードを装置10”に提示する(ブロック590)。すると、装置10”は、正しい証明書又は秘密コードがレンダリング装置によって装置10”に提示されたか否かを判定する(菱形592)。正しい証明書又は秘密コードが提示されていなければ、装置10”は、その様な証明書が提示されるまで待つ。正しい証明書又は秘密コードが提示されたら、装置10”に記憶されているコンテンツ暗号化鍵へのアクセスがここで許可される。次いで、鍵が使用され、要求されている暗号にされたメディアタイトルが復号される。次いで、復号されたメディアタイトルは、信頼されているアプリケーションに送られる(ブロック594)。レンダリング装置又は端末は、次いで、復号されたメディアタイトルをレンダリングす

る（ブロック596）。

【0176】

（サービスプロバイダがセキュア環境を作成可能にする）

図26は、本発明の追加の特性を説明するための、不揮発性書換可能メモリ装置内の安全アーキテクチャ又は制御構造のブロック図である。図26の安全アーキテクチャ600は、図20に示すようなセキュア領域に記憶されているサービスプロバイダ（SP）の証明書を含んでいる。SP証明書602は、矢印604を介して、事前にロードされているメディアコンテンツ606を指しており、コンテンツ606には、写真606a、楽曲606b、ゲーム606c、及び映像606dが含まれている。サービスプロバイダ（SP）がMNOである場合、事前にロードされているコンテンツ606は、着信音の様な送受話器特定メディアコンテンツ606eも含んでいる。矢印604は、端末内で動作しているアプリケーションがSP証明書602を有している場合は、アプリケーションは、事前にロードされているコンテンツ606a～606eにアクセスすることができることを示している。このようにして、サービスプロバイダSPがSprint又はVerizonの様なモバイルネットワークオペレータである場合には、オペレータは、その証明書をそれによって発行された携帯電話機にロードする。そこで、全てのその様な送受話器は、その様なオペレータの証明書をその様な事前にロードされているコンテンツを有するメモリ装置に供給することによって、事前にロードされているコンテンツ606a～606eにアクセスするのに使用される。

【0177】

サービスプロバイダの証明書を有する全てのアプリケーションによってアクセスできるメディアコンテンツに加えて、メモリ装置は、或る特定のサブスクリバしかアクセスできないメディアコンテンツも記憶している。従って、図26に示すように、写真610a、楽曲610b、ゲーム610c、映像610d、送受話器特定情報610e、及びパーソナルメディアコンテンツ610fは、サブスクリバ1又はサブスクリバ1の証明書を有するものにしか利用できない。サブスクリバ1の証明書を供給できるアプリケーションだけが、メディアコンテンツ610a～610fへアクセスすることができる。このようにして、サブスクリバ1がファイル610a～610fの何れかにアクセスを希望した場合、サブスクリバ1は自身の証明書を、送受話器の様な端末内のアプリケーションによって入力すると、その様なファイルの何れにでもアクセスすることができる。サブスクリバ1のアカウント608は、個人のアカウントであってもよいし、ファミリーアカウントのメンバーアカウントの様なグループ内の共有アカウントであってもよい。その様な事象では、ファイル610a～610fにアクセスするのに使用できる証明書は2セット以上存在することになる。証明書のセットの内の何れか1つがアーキテクチャ600を有するメモリ装置に送信されると、ファイル610a～610fにアクセスすることができる。

【0178】

アーキテクチャ600は、サブスクリバ1の証明書が要求される段階にサブスクリバ1が実際に到達する以前に、SP証明書がまず提示されるべきであるというポリシーを実行することに留意されたい。SP証明書がメモリ装置に提示された後、サブスクリバは、制約されているファイル610a～610fの何れか1つにアクセスを希望する場合、サブスクリバ1の証明書を入力するように求められる。

【0179】

サブスクリバ1のアカウント608は、矢印612によりファイル610a～610fを指している。矢印612は、ファイル610a～610fのコンテンツを使用するための権利及び／又は規則を含んでいる権利オブジェクトによるなど、上記型式の1つの制御構造を象徴化している。権利オブジェクトは、暗号化されているファイル610a～610fを復号するための鍵も含んでいる。しかしながら、権利オブジェクトは、ファイル610a～610fを復号するためにコンテンツ暗号化鍵を入手できるアクセス制御記録にアクセスするための証明書を含んでいることが望ましい。

【0180】

アーキテクチャ600は、複数のサブスクリバによってアクセスできる暗号化されているメディアコンテンツを記憶するために使用され、その場合、或るサブスクリバがアクセスできるメディアコンテンツは、異なるサブスクリバがアクセスできる場合もあればできない場合もある。このようにして、アーキテクチャ600は、サブスクリバXのアカウントも含んでいる。図26には示していないが、サブスクリバXに関係付けられているメディアコンテンツファイルには、サブスクリバXの正しい証明書がアーキテクチャ600の入っているメディア装置に提示された場合に限り、アクセスすることができる。この方法では、メモリ装置10は、複数のサブスクリバによって使用される。サブスクリバのそれぞれは、自身のアカウントに関係付けられているメディアコンテンツに対し、異なるサブスクリバがその様なコンテンツに対する認可されていないアクセスを得る恐れ無しに、独立的にアクセスすることができる。同時に、SP証明書を有している限り、全てのサブスクリバがアーキテクチャ600を介してアクセスできるファイル610a~610fの様な共有コンテンツが存在している。更に、2人又はそれ以上のサブスクリバがアクセスすることのできるメディアコンテンツファイルの間に部分的な重なりがあってもよい。例えば、或る特定のメディアコンテンツファイルは、2人以上のサブスクリバアカウントと関係付けられているので、その様なメディアコンテンツファイルは、サブスクリバの誰かの証明書がメモリ装置に提示されると、アクセスし復号することができる。これは、サブスクリバが彼らの証明書又は鍵の何れかを共有する必要なしに行われる。

10

20

【0181】

上で指摘したように、図26の安全構造600にとって1つの可能な制御構造は、上記アクセス制御記録(ACR)である。通常、暗号化されているメディアコンテンツを復号するためのCEKを制御するACRは、図24のACRの様に、メモリ装置が作成されたときに作成される。次に、サブスクリバアカウントが作成されると、適切なACR内の証明書がそのサブスクリバに供給され、サブスクリバがCEKにアクセスできるようになる。

【0182】

上で説明したように、システムACRは、AGPとACRを作成する能力を有している。一般に、ACRを作成する権限を有するACR又はAGPは、何れも、サブスクリバACRを作成するのに使用できる。その様なACR又はAGPは、製造時に既に装置10内に作成されている。ACRは、メディアコンテンツが装置にロードされる前又は後に、メモリ装置の制御構造として作成される。装置にロードされたコンテンツは、装置によって生成されるか供給されたコンテンツ暗号化鍵を使用して暗号化され、その場合、コンテンツ及び暗号化鍵は、関係付けられ、サブスクリバACRによって制御される。その様な方法では、サブスクリバが関係付けられている制御構造が、その様な暗号化されているメディアコンテンツへのアクセスを制御するために使用される。

30

【0183】

図26の安全アーキテクチャは、メディアコンテンツ配信の1つの手段を説明しており、ここでは、メモリ装置は特定のサービスプロバイダに結合されているので、異なるサービスプロバイダが、このメモリ装置を使用して、メディアコンテンツを装置内に記憶し、装置内のメディアコンテンツを制御することはできない。図26の安全構造に代わるものとして、メモリ10内の安全アーキテクチャはSP証明書602を含んでいないので、その様な証明書は、装置内のコンテンツにアクセスするのに必要ない。その様な代替りの実施形態では、複数の異なるサービスプロバイダのそれぞれは、同じメモリ装置内の他のサービスプロバイダから独立して自身の制御構造を作成することができる。各サービスプロバイダは、他のプロバイダによるクロストーク又は干渉無しに、メモリ装置と対話することができる。装置10に事前にロードされている上記SSAシステムのシステムACRは、異なるサービスプロバイダのそれぞれが、上記の方法でAGP-ACR構造の形式で自身の階層ツリーを作成するのを支援する。

40

50

【0184】

この様に、上記制御構造は、権利オブジェクトと、ACRと、関係付けられている階層ツリーを含んでいる。権利オブジェクトは、上で指摘したように、通常は、メモリ装置の外部に作成され、装置にダウンロードされる。1つの実施形態では、その様なオブジェクトは、DRMサーバ又は端末内のDRMエージェントによって、及びメモリ装置内のDRM ACRの様な構造によって、管理される。他方、ACR及び関係付けられている階層ツリーは、メモリ装置内に作成された構造であり、その外部には存在していない。一般には、それらのコンテンツ又は特性が装置外部のエンティティにエクスポートされるのは望ましくない。ACRは、CEKがどの様に使用されるか、例えば機能の読取り、書込み、又は委譲について、の許可を含んでいる。他方、権利オブジェクトは、CEK及びそれにより暗号化されているコンテンツがどの様に使用されるかを、例えばアクセスが許容される持続時間又はアクセスの回数などを限定することにより、更に厳密に指定することができる。

10

【0185】

別の特性として、メモリ装置の（例えば、セキュア領域に）記憶されている再生リストマネージャを実行しているソフトウェアコードは、エンドユーザーが再生又は他のレンダリングプロセスを停止したメディアタイトル内の場所を登録するのに使用される。これにより、エンドユーザーは、メモリ装置を1つの端末から外して、それを別の端末に接続し、自分が停止した地点から再生又はレンダリングを再開することができる。

20

【0186】

（認証に使用される証明書）

メディアコンテンツプロバイダとサービスプロバイダが取り組む必要がある1つの重要な問題は、コンテンツがロードされることになる特定のメモリ装置が純正装置であるか否かということである。他方、メモリ装置の側から見れば、コンテンツ又は権利情報を記憶又は取り出そうと試みているホスト又は端末（又はサーバ）が純正か否かを判定することが有用又は必要である。このため、安全アーキテクチャ600は、更に、証明の様な認証及び設定特性622を含んでいる。次はそれについて説明する。

【0187】

異なるサービスプロバイダによって作成された制御構造は、各パーティションにはその対応するサービスプロバイダの制御構造（例えば、AGP-ACR及び／又は権利オブジェクト）しか記憶されないように、別々のパーティションに記憶されるのが望ましい。その様なパーティションは、それらパーティションの少なくとも幾つかのそれぞれに、そこに記憶されている制御構造の対応するサービスプロバイダがアクセスすることができ且つ他のプロバイダはアクセスできないように、プライベートであり隠されているのが望ましい。異なるサービスプロバイダに対して作成された階層ツリー同士の間にはクロストークの無いことが望ましい。

30

【0188】

エンドユーザー端末とメモリ装置の間の相互認証のためのアーキテクチャ全体を図27に示している。図27に示すように、メモリ装置630が正規であることの証明、及びエンドユーザー端末632が正規であることの証明は、共にルートCAサーバ634の権限から導き出される。装置630は、生産CAサーバ636が配置されている生産ファシリティによって製造される。一方、端末632は、端末CAサーバ638（サーバ634と同じでもよい）が配置されているファシリティで製造される。このようにして、装置630は、サーバ636に、装置ID、型式、及び装置の公開鍵を提供する。サーバ636は、プロダクションサーバIDとプロダクションサーバ公開鍵をサーバ634に提供する。サーバ634は、ルートCA証明及び生産CA証明をサーバ636に提供する。すると、サーバ636は、サーバ634からの2つの証明を、サーバ636のプライベート鍵によって署名された装置証明と共に、装置630に提供する。同様のプロセスが、サーバ634、638と端末632の間で実行される。上記プロセスの結果として、端末632と装置630それぞれは、図28に示すように3つの証明を保有する。

40

50

【0189】

図28に示すように、メモリ装置は、3つの証明、即ち、ルートCA証明、生産CA証明、及びメモリ装置証明を含んでいる。装置630と端末632は、共にルートCA証明とルート公開鍵を有しているので、最初の設定プロセス時に、この鍵を使用して、公開鍵と、装置及び端末内にそれら鍵を保有している証明とが純正であることが、下の方法で検証される。

【0190】

図29に示すように、端末632と装置630は、設定プロセスのために装置が初めて端末に挿入されたときに、証明を交換する。装置は、装置証明と生産CA証明を端末に送り、端末は、端末証明と端末CA証明を装置に送る。装置630と端末632内に入っている異なる鍵及び証明を、図30に示している。

10

【0191】

生産CA証明は、生産CA公開鍵と、その様な公開鍵のルートCAプライベート鍵によって署名されている（即ち、暗号化されている）バージョンとを含んでいる。端末632は、この生産CA証明が純正であるか否かを、それが所有しているルート公開鍵を使用して、暗号化されている生産CA公開鍵を復号し、その結果を装置630から受け取った生産CA証明内の生産CA公開鍵と比較することによって検証する。それらが一致すれば、そのことは、受け取った生産CA証明は細工されておらず純正であることを示している。端末632は、次いで、その様に確認された生産CA公開鍵を使用して、装置公開鍵の暗号化されているバージョンを復号し、その結果を装置630から受け取った装置証明内の装置公開鍵と比較する。それらが一致すれば、そのことは、受け取った装置証明が細工されておらず純正であることを示している。装置630は、端末から受け取った証明が純正で細工されていないことを検証するために同様のプロセスを実行する。上記より、更に多くのレベルの鍵と証明のが活用できれば、システムは更に安全になることが明白である。図27～図32には3つのレベルが使用されている。高レベルの安全が求められているか低レベルの安全が求められているかによって、上記方針はしかるべく変更されることは自明である。

20

【0192】

装置と端末が上記相互認証プロセスを実行した後、端末は、製造中に装置内に作成されたACRを使用して、図31に示すように、装置630内にACRを作成する。作成されたこのACRには、ルート公開鍵を有するルートCA証明が入っているので、次に端末が装置と接続されたとき、装置は、ルート公開鍵を使用して、端末によって提供された端末証明が純正であることを、上記プロセスと同様のプロセスで検証する。端末によって提供された端末証明が純正であると確認されると、メモリ装置は、ACR内の許可に従って端末がコンテンツにアクセスすることを許す。

30

【0193】

図32に示すように、次にメモリ装置が端末と接続されたとき、端末は、ログインしてその証明を装置に送る。装置は、次いで、上記検証プロセスを実行する。オプションとして、メモリ装置630も、図32に示すように検証するためにその証明を端末632に送る。

40

【0194】

装置630に記憶されている証明は、装置が正規であるか否かを調べるために、図19A～図19Dに示しているサーバのうちの何れかの様な認証サーバのために使用することもできる。サーバもルートCA証明と証明内のルート公開鍵とを有している場合は、この鍵は、装置が正規であるか偽造品であるかを検証するために、上で説明したのと同様の方法で使用される。装置630も、サーバが正規であるか否かを同様のプロセスで検証する。認証サーバは、ルートCA証明と調査を実行するためのソフトウェアを、サービスプロバイダのサーバの様な異なるサーバに転送して、サービスプロバイダサーバが代わりに検証プロセスを実行できるようにしてもよい。そうすると、図19A～図19Dのプロセスは、サービスプロバイダサーバが認証サーバの機能も行えるようになるという点で、単純

50

化されることになる。

【0195】

(事前ロードされるコンテンツのパッケージ化)

図22のメモリ装置10”には、歌曲の様なメディアコンテンツだけでなく未払いのカタログメディアコンテンツも事前にロードされている。そのようなカタログメディアコンテンツは、暗号化されているノーカットの高品質バージョン、並びにその様なバージョンのプレビューを備えている。装置10”には、更に、プロモーション品目並びに各種アプリケーションが記憶されている。図20に関して上で説明したように、メモリ装置10”は、コンテンツ領域及びセキュア領域を含む複数の異なる領域を備えている。セキュア領域は、セキュア生産ファシリティでの装置生産中にしかアクセスできないのが望ましい。例えば、権利オブジェクト及びAGP/ACR構造及び他のデジタル権利管理ソリューションは、セキュア生産ファシリティで、装置10又は10”のセキュア領域に記憶される。コンテンツ暗号化鍵は、セキュアファシリティで、セキュア領域にロードされるか、生産後に装置自身によって生成される。

10

【0196】

コンテンツ領域内のオペレータコンテンツ及び他の保護されているコンテンツの様なコンテンツは、通常、映像ファイルの様な大きなファイルを有している。安全なデータをセキュア領域にロードするためのセキュアファシリティには、大量生産で多数の大きなファイルをロードする能力がないかもしれない。この理由から、ロックされているコンテンツ並びにロック解除されているコンテンツは、生産ファシリティの安全でない領域でロードされるのが望ましい。ロックされているメディアコンテンツは、通常は暗号化されているので、その様なコンテンツは、認可を受けずに利用される可能性を減らすために、暗号化されている形式で安全でないファシリティに送られる。各メモリ装置は、順番になっているシリアル番号のような固有の識別を有している。従って、暗号化されているメディアコンテンツ並びに暗号化されていないコンテンツをロードするために装置が安全でないファシリティに回される前に、先ず安全関連データとオブジェクトをセキュア領域に記憶することが可能である。セキュア領域にロードされるデータは、コンテンツ領域に記憶されているメディアコンテンツの使用を制御するための制御構造を含んでいるので、暗号化されているコンテンツをロードする前に、上記制御構造をセキュア領域にまずロードすることによって、メディアコンテンツが許可を受けずに利用されるのを防止する追加的な安全性が提供される。

20

30

【0197】

製造されたメモリ装置のそれぞれにコンテンツを暗号化するのに使用される鍵は、それ以外の装置に事前にロードされている鍵とは異なっている。実際にそうになっている事例では、1つのメモリ装置の暗号化鍵を入手することができるハッカーでも、それ以外のメモリ装置に記憶されているコンテンツにはアクセスできない。しかしながら、多数の異なるコンテンツ暗号化鍵を生成して各装置にロードすることは、厄介である。妥協案として、或るバッチのメモリ装置には、それらが同じ鍵セットを有するように、同じ鍵セットがロードされる。従って、或るバッチの内のメモリ装置の1つの鍵セットが認可を受けていない方法で入手されると、その様なバッチのメモリ装置に記憶されているメディアコンテンツは認可無しにアクセスできるようになる。しかしながら、その様な鍵セットを入手した人物も、異なるバッチのメモリ装置に記憶されているメディアコンテンツに対しては、その様な装置のメディアコンテンツはその人物が違法に入手したものとは異なる鍵セットによって暗号化されているので、アクセスすることができない。

40

【0198】

このようにして、50,000個のメモリ装置が生産される場合、50,000個の装置は、それぞれ50個のメモリ装置を有する1,000個のセットに分けられ、当該セット内の各装置には50個の異なる鍵セットの内の1つがロードされる。このように、50,000個の装置が50のバッチに分けられ、1,000個の装置からなる各バッチは、同じ鍵セットがロードされ即ち同じ鍵セットを使用することになる。例えば、50個の鍵

50

セットはK O m nと表され、ここに、mは、サウンドトラックの様な最大20個までの購入されたメディアタイトルに対して1から20までを範囲とし、nは、1からNであり、Nはこの事例では50である。Nセットの鍵セットK P l nも提供され、ここに、lは、サウンドトラックの様な最大50個までの未払いメディアタイトルに対して1から50を範囲とし、nは、1からNを範囲とする。この鍵K P l nのセットは、権利発行者であるサーバに安全に送信され、上記トラックが購入されるときに権利オブジェクトが発行される。

【0199】

更に、セキュアファシリティでは、購入されたタイトル又はトラックのコンテンツ暗号化鍵K O m nは、無制限の再生及び例えば上で説明した3つのエクスポートのためのビジネス規則を追加するためのN個のオブジェクトのセットにパッケージ化される。N個の権利オブジェクトのセット（購入されたメディアタイトル毎に1つ）はR O m nとして表され、ここに、mは、最大20個までの購入されたメディアタイトルに対する1から20までを範囲とし、nは、1からNを範囲とする。N個の権利オブジェクトのセットは、セキュアファシリティに安全に転送される。生産時、メモリ装置の固有シリアル番号は、50個の権利オブジェクトのセットの内のどの1つがカート、R O 1 n、R O 2 n、... R O m n、にロードされるかを決めるために使用され、ここに、mは、最大20個までの購入されたメディアタイトルに対する20である。それら20個の権利オブジェクトは、10,000個のメモリ装置の第n番目のセット又はバッチ内の各装置にロードされ、ここに、nは、メモリ装置シリアル番号を1,000で割った逐次部分により決まる（即ち、メモリ装置シリアル番号/1,000の整数部+1）。例えば、メモリ装置シリアル番号が5の場合、nは値1になる。シリアル番号1200では、nは2となる。シリアル番号が35870であれば、nは36ということになる。

【0200】

購入されたメディアタイトル（最大20）は、N個の暗号化されたファイルのセットC O m nに暗号化され、ここに、mは1~20を範囲とし、nは1~nを範囲とする。最大50個までのカタログメディアタイトルが入手された後、それらタイトルは、ファイルP C L R 1、P C L R 2、... P C L R Lとして暗号化されることになり、ここに、Lは最大50までである。最大50個までのカタログメディアタイトルから、その様なタイトルのそれぞれの15秒分の映像断片又は低品質バージョンが作られ、S N I P 1、S N I P 2、S N I P Lと標示され、ここに、Lは最大50までである。次いで、ノーカットのカタログメディアタイトルが、N個の暗号化されたファイルのセットP O l nに暗号化され、ここに、lは1~Lを範囲とし、nは1~Nを範囲とする。カタログメディアタイトルファイル用のN個の暗号化鍵のセットは、権利発行者に送られる。コンテンツをロードするためのマスターコピーには以下のものが入っている。

（1）N個の暗号化されている購入されたメディアタイトルのセットC O m n、ここに、mは1~20を範囲とし、nは1~Nを範囲とする。

（2）1個のカタログメディアタイトルのプレビュー断片のセットであり、断片は暗号化されておらず、N個のメディア装置全般に亘って同じであり、S N I P 1、S N I P 2、... S N I P Lと表わされ、ここにLは最大50までである。

（3）プレビュー断片に対応するN個の暗号化されたカタログメディアタイトルのセットであり、それらはN個のメモリ装置のセットについて異なるコンテンツ暗号化鍵を使って暗号化されている。

（4）コンピュータクリップ、写真、着信音の様な、1個の全ての他のプロモーション用コンテンツのセット。

【0201】

サードパーティーの請負によるファシリティの様な安全でないコンテンツローディングファシリティでは、コンテンツをメモリ装置にロードするのにマスターコピーとコンテンツローディングスクリプトが使用される。コンテンツローディングスクリプトは、メモリ装置シリアル番号を最初に読み取り、シリアル番号に基づいて、1からNの間のバッチ又

はセット数を計算する。次いで、このセット数 n に基づいて、コンテンツローディングスクリプトは、購入された、メディアタイトルファイルの n 番目のセット $CO1n$ 、 $CO2n$ 、 $\dots$ $COmn$ を読み取り、ここに、 m は購入されたメディアコンテンツ内のメディアタイトルの個数である。コンテンツローディングスクリプトは、カタログメディアタイトルの n 番目のセット $PO1n$ 、 $PO2n$ 、 $\dots$ $POLn$ も読み取り、ここに、 L は装置に載せるカタログメディアタイトルファイルの個数である。ポストアプリケーションのプレビュー断片ファイルのセットとプロモーション用品目のセットも、各メモリ装置にロードされる。コンテンツローディングスクリプトは、次いで、上で選択されたファイルを、図 20 に示すメモリ装置のコンテンツパブリック領域に書き込む。

【0202】

プリペイドコンテンツの鍵を生成しタイトルをロードするためのプロセス、及び権利発行者による権利オブジェクト発行のプロセスを、図 33A と図 33B を参照しながら説明する。ファシリティでは、ロードされる装置又はカードは N 個の装置又はカードを有するグループに分けられ、各グループの N 個の装置それぞれは、異なるセット番号及び対応する鍵と権利のセットを有しており（ブロック 631）、ここに、セット番号は装置のシリアル番号から導き出すことができる（ブロック 632）。 N 個のコンテンツ暗号化鍵のセットが生成され権利発行者に送られる（ブロック 634）。権利発行者は、メモリカードの様な各メモリ装置のセット識別番号をそのシリアル番号から導き出す。導き出されたセット識別番号と受け取った N 個の鍵のセットから、コンテンツに対する制御されたアクセスのための権利オブジェクトがコンパイルされ、識別され、ローディング用のファシリティに送られる（ブロック 638、640）。それらは、ローディングのファシリティで受け取られる（ブロック 642）。メモリカードの様な各装置毎に、ファシリティでセット識別番号がその固有のシリアル番号及び鍵と識別された権利オブジェクトの対応するセットから導き出される（ブロック 644）。次いで、対応する権利オブジェクトがメモリカードの様な装置にロードされる。購入されたメディアタイトルは、セキュアファシリティで暗号化され、マスターコピーが請負業者のファシリティに送られ、暗号化されたタイトルがロードされる（ブロック 646、648）。

【0203】

上で指摘したように、メモリ装置及び／又は端末の何れかの DRM エージェントは、装置及び／又は端末のため上記アクションを取り扱うために使用される。

【0204】

カタログコンテンツ用の鍵を生成しタイトルをロードするプロセス、及び権利発行者による権利オブジェクト発行のプロセスを、図 34 と図 35 を参照しながら説明する。ファシリティでは、ロードされる装置は N 個の装置又はカードを有するグループに分けられ、各グループの N 個の装置それぞれは、異なるセット番号と、対応する鍵と権利オブジェクトのセットを有しており、ここに、セット番号は装置のシリアル番号から導き出すことができる（ブロック 652）。このようにして、カタログメディアタイトル用の N 個の CEK のセットはセキュアファシリティにより生成され、 CEK と装置 ID 番号は権利発行者に送られる（ブロック 654、656）。メモリカードの様な各装置毎に、セット識別番号がその固有シリアル番号と識別された鍵の対応するセットから導き出される（ブロック 658）。次いで、識別された鍵の対応するセットを使用して、カタログメディアタイトルが暗号化される（ブロック 660）。次いで、カタログメディアタイトルは、メモリカードの様な装置に記憶される（ブロック 662）。

【0205】

購入取引中に、図 35 に示すように、エンドユーザーによる購入が確認されると（ブロック 670）、セット識別番号が、権利発行者によって、装置シリアル番号から導き出され（ブロック 672）、このセット番号とブロック 656 でファシリティから受け取った CEK を使用して、適切な権利オブジェクトがコンパイルされる（ブロック 674）。権利発行者は、対応する権利オブジェクトをセキュアファシリティに提供する（ブロック 660）。エンドユーザーがカタログメディアタイトルを購入するとき、DRM エージェン

トは、メモリ装置のシリアル番号と購入されたメディアタイトルのIDを、権利発行者サーバに送る（ブロック670）。権利発行者サーバは、そこで、メモリ装置のシリアル番号に基づいて、メモリ装置のセット番号を計算する（ブロック672）。権利発行者は、既にカタログメディアタイトルファイル用のN個の暗号化鍵セットを有しているはずである。セット番号とメディアタイトルIDに基づいて、権利発行者は、購入後にメモリ装置にダウンロードされることになる対応するコンテンツ暗号化鍵を有する正しい権利オブジェクトを発行することができるようになる。

【0206】

（メディアコンテンツ配信の手段として他のコンテンツを有するメモリ）

暗号化されているメディアタイトル及びその様なタイトルのプレビューを有するメモリ装置の事例を上記に説明している。これらの型式の装置を図36A～図36Dに示しており、装置はプリペイドコンテンツも含んでいる。これらの図中、PREVは、省略化されているメディアコンテンツ（例えば、一部又は低品質バージョン）を備えているプレビューコンテンツを意味し、FULLは、PREVの省略化されていない暗号化されているバージョンを意味し、ROは、PREVの権利オブジェクトを意味する。PREPAIDは、メモリ装置を取得する際に支払いが済んでいるコンテンツを意味する。明解さを期して、プリペイドコンテンツ用の権利オブジェクトは図から省略している。

【0207】

代わりに、装置10の様なメモリ装置は、図37A～図37C、図38A、図38B、図39A、及び図39Bに示すように、他の型式のコンテンツも記憶することができる。図37Aに示すように、装置は、PREVだけを記憶していてもよいし、或いは図37Bに示すように、PREVとFULLの両方を記憶していてもよい。装置は、更に図37Cに示す様にPREVとROを記憶していてもよい。このようにして、図37A～図37Cでは、装置は全ての構成でPREVを記憶している。

【0208】

別の代替例では、装置10の様なメモリ装置は、図38A及び図38Bに示すように、全ての構成でFULLを記憶している。図38Bでは、これもROを記憶している。

【0209】

更に別の代替例では、装置10の様なメモリ装置は、図39A及び図39Bに示すように、全ての構成でROを記憶している。図39Bでは、これもFULLを記憶している。

【0210】

図37A～図37C、図38A、図38B、図39A、及び図39Bの構成の全てにおいて、PREPAIDと権利オブジェクトは上記により示していないが、必要に応じて含ませてもよい。

【0211】

従って、図37Aと図40に示すように、装置10には、メディアタイトルの断片又は低品質バージョンの様なプレビューコンテンツしかロードされない。その様なタイトルは702で表示している。エンドユーザーがメモリ装置702によってプレビューされたメディアタイトルの省略化されていないバージョンを見る権利を購入した後、権利オブジェクト704は、図40の矢印706によって示されているように、コンテンツ702の購入後にダウンロードされる。権利オブジェクトが装備されると、エンドユーザーは、プレビューされたメディアタイトルの省略化されていないバージョン（FULL）をダウンロードする権利を有する。省略化されていないメディアタイトルを有していない装置からそれを有する装置への転換を図40の矢印710で示している。代わりに、エンドユーザーは、図40の矢印712によって表示されているように、メディアタイトル708の完全で省略化されていないバージョン（FULL）を最初にダウンロードしてもよい。しかしながら、この時点で、エンドユーザーは、完全なメディアタイトル708にアクセスする権利は、その様なタイトルが暗号化されているので、まだ有しておらず、エンドユーザーに提供されているその様なタイトルを復号するのに必要なコンテンツ暗号化鍵にアクセスする権利も持っていない。しかしながら、エンドユーザーが購入した後、エンドユーザー

10

20

30

40

50

は、図 40 の矢印 714 によって示すように、権利オブジェクト 704 をダウンロードする権利を有することになる。

【0212】

図 40 のフローを使用してメディアコンテンツを配信するプロセスは、図 23 のものと幾分似ており、図 41 に示している。このように、プレビューコンテンツ 702 は、ユーザーが最初にカタログメディアタイトルをプレビューできるようにする。メモリ装置は、従って、PREV をレンダリングし、次いで、エンドユーザーの端末を介してエンドユーザーにプレビューされているカタログメディアタイトルを購入するように促す（ブロック 722、724）。購入が受信されると、次いで、完全なメディアタイトルと権利オブジェクトがメモリ装置に記憶するために供給される（ブロック 726、728）。その後、エンドユーザーは、タイトルを復号することによって、購入されたメディアタイトルにアクセスし、それをレンダリングすることができるようになる。図 42 では、プレビューコンテンツ 702 は、ユーザーが最初にカタログメディアタイトルをプレビューできるようにする。完全なメディアタイトルがダウンロードされ、引き続き、購入後に権利オブジェクトが受信される（この順は逆でもよい）。そこで鍵を使用して、完全なタイトルが復号されレンダリングされる。

10

【0213】

代わりに、メモリ装置 10 には、図 38A に示すように完全な暗号化され且つ省略化されていないメディアタイトルしか配信されなくてもよい。エンドユーザーが既にその様なメディアタイトルへの権利を購入しておれば（図 38B）、メモリ装置には、メディアタイトルの復号に必要なコンテンツ暗号化鍵への権利オブジェクトとアクセスも提供されることになる。しかしながら、完全なメディアタイトル用のメモリ装置が購入前に配信される場合は、エンドユーザーはアクセスする権利を購入せねばならない。購入後、適切な権利オブジェクトがダウンロードされ（図 43 の矢印 732）、購入されたメディアタイトルの復号に必要なコンテンツ暗号化鍵へのアクセスが提供される。

20

【0214】

コンテンツ配信のその様は手段の変型として、完全な省略化されておらず且つ暗号化されているメディアタイトルを有するメモリ装置は、その様なメディアタイトルの制約付き閲覧又はアクセスしか許可しない権利オブジェクトと共に記憶される。更に、装置には、エンドユーザーの使用パターンを追跡し、ユーザープロファイルをコンパイルする追跡エージェントが記憶されている。図 44 を参照されたい。制約として、メディアタイトルにアクセスする持続時間又は回数の制約が課されている（図 45 のブロック 742）。ユーザーがタイトルをレンダリングするとき、アクセスが追跡され、ユーザーアクセスプロファイルがコンパイルされる（図 45 のブロック 744）。持続時間又は回数が失効した時点で、エンドユーザーは、メモリ装置をサーバに接続しない限り、メディアタイトルにもはやアクセスすることができなくなる。メモリ装置が、ホスト又は端末を介してサーバに接続されたとき、その様なユーザープロファイルは、ここで、市場調査の様な目的でサーバにダウンロードされる。アクセスプロファイルがダウンロードされた後、権利オブジェクトは修正されるか更新され、エンドユーザーがメモリ装置上のメディアタイトルにアクセスして楽しめる持続時間又は回数の拡大が許可される（図 45 のブロック 746）。

30

40

【0215】

メディアコンテンツ配信のための更に別の可能な手段として、メモリ装置 10 は、図 39 に示す権利オブジェクトだけがロードされた状態で配信されるようにしてもよい。その様なメモリ装置は、購入されねばならず、それは、電話サービス用の SIM カードの様なプリペイドサービスカードと似た機能を持つ。権利オブジェクトは、エンドユーザーが、完全な省略化されていないメディアタイトルをダウンロードして楽しむのを許可する（図 46 のブロック 752）。権利オブジェクトは、エンドユーザーが、多数のメディアタイトルをダウンロードするのを許可する。このようにして、エンドユーザーは、多数のダウンロードされたタイトルを楽しんだ後、それらを一旦メモリ装置から削除し、次に、同じタイトルを後でダウンロードすることが可能である。この方法では、エンドユーザーは、

50

メモリ装置の記憶容量に対する制約は課されておらず、メモリ装置に対するメディアタイトルのダウンロードと削除を繰り返すことができる。

【0216】

(バックアップと再ロード制御)

状況によっては、フラッシュカードの様な不揮発性メモリ装置上のコンテンツを、存在しているメディアコンテンツのみならず、アクセス及び一旦アクセスされた後コンテンツに行えることを制御するあらゆる権利オブジェクトを含めて、バックアップする能力を有するのが望ましい場合もある。しかしながら、適切な制御無しにこれが行われると、権利オブジェクトを使用した制御を巧みに回避する裏口を提供することになりかねない。例えば、権利オブジェクトが、3部のコピーの様な限定された部数のコピー作成を許可した場合、権利オブジェクトは作成された部数分のコピーを見失わないようにする。設定された限定枚数のコピーが一旦作成されたら、権利オブジェクトはそれ以上のコピー作成を禁止することになる。この制約は、権利オブジェクトのバックアップコピーが、コピー作成前に記憶領域に作られ、3部のコピーが作成された後にメモリ装置に復元されてしまうと、回避される恐れがある。3部のコピーを許す元の権利オブジェクトを復元することによって、ユーザーは再度コピーを更に3部作成することができる。このプロセスは、自明の通り繰り返すことができるので、権利オブジェクトの制約は完全に回避される。この記憶領域は、権利オブジェクトのバックアップコピー製作元と同じ装置内に在っても、異なる装置内にあってもよい。

【0217】

これが起こるのを防止するため、権利オブジェクトは、図2～図4に関して上で説明したものの様な保護されているパーティションに記憶される。その様な保護されているパーティションにアクセスするために、ホスト上のアプリケーションの様なアプリケーションは、アクセスが許容される前に、適切な事前に決められている証明書をメモリ装置に供給する必要がある。エンドユーザーは、通常、権利オブジェクトによって制御されているコンテンツをレンダリングしたり再生する目的で、権利オブジェクトにアクセスすることができる。エンドユーザーが、バックアップ又は復元を目的として権利オブジェクトにアクセスするのを防止するために、エンドユーザーの証明書は、エンドユーザーが権利オブジェクトを当該パーティションから読み取ることしか許可せず、権利オブジェクトをバックアップして当該パーティションに復元することを許可しない。権利オブジェクトをバックアップし復元するためには、エンドユーザーにとって入手可能なものとは異なる証明書が使用される。その様な証明書を有するアプリケーションだけが、権利オブジェクトをバックアップして当該パーティションに復元することができる。権利オブジェクトは保護されているパーティションに復元されるので、復元された権利オブジェクトは、この場合も、一方のセットは権利オブジェクトの読取りだけを許可し、他方のセットはバックアップと復元を許可する、2つの異なる証明書のセットを手段とするなどして、対応するコンテンツへのアクセスの制御に効果を発揮することになる。

【0218】

権利オブジェクトは、バックアップされバックアップ記憶領域に記憶された後、メモリ装置から削除されるのが望ましい。権利オブジェクトは、メモリ装置に復元された後、バックアップ記憶領域から削除されるのが望ましい。

【0219】

上記特性は、多種多様な不揮発性メモリ記憶装置に適用することができ、そこでは、無制約のメモリ領域に加えてセキュアメモリ領域が提供されている。

【0220】

上記方式に代わるものでは、証明書の第1セットを有する或る特定の認可されたアプリケーションだけが、バックアップと復元の機能を行うことができるようになっており、第1セットとは異なる証明書の第2セットを有する他のアプリケーションは、権利オブジェクトを読み取ることしかできない。その様な認可は、メモリ装置により制御されるか、例えば、登録プロセスを通すなどしてサーバにより外部的に制御されるかの何れかである。

DRM及び／又はCPRM能力を有するアプリケーションだけが、権利オブジェクトを変更、更新、又は消去、及び／又はバックアップ及び復元する権限を有することになると期待される。この代わりの方式は、セキュアメモリ領域が提供されているか否かに関わらず有用である。

【0221】

上で指摘したように、権利オブジェクトは、3部のコピーの様な限定部数のコピー作成を許可する。その様な規則を実行するために、権利オブジェクトは、作成された部数のコピーを見失わないようにする。アプリケーションが権利オブジェクトをコピーしたとき、メモリ装置上に留まっている権利オブジェクトは、仮にコピーが作成された後に更に許可されているコピーがあれば、それら当該部数のコピーを見失わないように更新される必要がある。更に、コピーされる権利オブジェクトは、その様なコピーから別のコピーが作成できるか否かを正確に反映させるために、コピー中に変更される必要がある。このように、エンドユーザーがその様なコピーから更にコピーを作成する許可を望む場合は、これを可能にするため、コピーされる権利を変更するのが望ましい。例えば、権利オブジェクトは、オリジナルから合計 n 部のコピーが作成されることを許可し、ここに、 n は正の整数である。コピーされた権利オブジェクトは、合計 m 部のコピーがコピーされた権利オブジェクトから作成されることを指定し、ここに、 m はゼロ又は n より小さい正の整数である。その様な事象では、元の権利オブジェクトの規則は、オリジナルから $(n-m)$ 部のコピーが作成されることしか許可しないように更新される。このように、権利オブジェクト（オリジナル及びコピーされたもの）は、それから作成されるコピーの計数又は部数、並びにコピー計数がその後の転送時にしかるべく変更される必要がある要件を含んでいる。それ以上コピーが作成できない場合は、この計数又は部数はゼロになる。

【0222】

メディアコンテンツを制御するための権利オブジェクトは、無制限のレンダリング又は再生の権利を指定する。或いは、レンダリング又は再生の回数も制限される。その場合には、権利オブジェクトは、なお行われ得るレンダリング又は再生の計数又は回数を含んでいることになる。

【0223】

バックアップ及び復元の場合には、変更、更新、又は削除を目的として権利オブジェクトにアクセスするのに必要な証明書が、読取り専用機能に必要なものとは異なる。変更、更新、又は削除を目的として権利オブジェクトにアクセスするのに必要な証明書は、バックアップ及び復元用のものと同じであってもよい。

【0224】

幾つかの実施形態では、その様なオブジェクト（即ち、そこからコピーが作成できないオブジェクト）のコピーを作成する試みが行われた場合、この試みは、コピーが例えば権利オブジェクトによって指定されている、別の装置に作成されたときに、その様なオブジェクトがメモリ装置（又は他の記憶装置）から削除される結果となる。削除後、コンテンツは、レンダリング、再生、又はその他の目的でそれ以上アクセスできなくなる。他の実施形態では、その様なオブジェクトのコピーを作成するという試みが行われた場合、制限付き又は無制限のレンダリング又は再生の権利が更新され、レンダリングも再生も一切行えないこと、又は権利オブジェクトへのアクセスが、単に、診断又は故障分析の様な限られた目的以外は全面的に遮断される旨表示される。

【0225】

権利オブジェクトは、鍵によって暗号化されるのが望ましく（装置10内で行われるのが望ましい）、メモリ装置に提示される正しい証明書は、上に述べた方法で、その様な鍵が読取り専用又は書込みに利用できるようにする（これは、削除、変更又は更新、バックアップ、及び復元を可能にするという意味）。このようにして、コピー作成又は変更に先立ち、権利オブジェクトが先ず復号される。次いで、上に述べた方法で変更又は削除が行われ、権利オブジェクトが暗号化される。暗号化を行うのにクリプトエンジン40が使用される。権利オブジェクトの暗号化が求められていない場合は、データストリーム上に何

らの暗号動作も無しに迂回経路（図 1 には図示せず）が、あたかもクリプトエンジン 40 が存在しないかのようにできて、H DMA と F DMA がこの迂回経路に沿ってアービタ 36 を介して B R A M 38 に直接接続される。

【0226】

その後、コピー作成が求められており、権利オブジェクトの規則によって許可されている場合は、権利オブジェクトはコピーできる。しかしながら、これをセキュアプロセスにするため、コピーされることになる復号された権利オブジェクトは、セッション ID 又は鍵を使って暗号化され、別の記憶装置に送信される。その様な別の記憶装置では、権利オブジェクトは、セッション ID 又は鍵を使って復号され、更に（別の記憶装置又は別のソースからの）別の鍵を使って再度暗号化され、その別の記憶装置に記憶される。このプロセスは、バックアップされ復元される権利オブジェクトについて実施される。

10

【0227】

上記特性は、制約されていないメモリ領域の他にセキュアメモリ領域が提供されているか否かに関わらず、多種多様な不揮発性記憶装置に適用される。

【0228】

以上、様々な実施形態を参照しながら本発明を説明してきたが、本発明の範囲を逸脱すること無く変更及び修正を加えることができ、本発明の範囲は、特許請求の範囲及びその等価物によってのみ定義されるものと理解されたい。ここで言及した全ての参考文献は、参考文献として援用される。このようにして、実施形態の幾つかは、ここではカード形態のフラッシュメモリを例にとって説明しているが、本発明は、カード形態であるか否かを問わず、磁気ディスク、光学 CD の様な他の型式のメモリ、並びに他の型式の書換可能不揮発性メモリシステムにも適用可能である。上で説明した段階又はアクションは、上に述べたメモリ装置及び／又は端末又はホスト装置及び／又はサーバに記憶されているソフトウェアコード（例えば、アプリケーションソフトウェア）によって実施することができる。

20

【図面の簡単な説明】

【0229】

【図 1】本発明を説明するのに有用な、ホスト装置と通信しているメモリ装置のブロック図である。

【図 2】本発明の態様を説明するのに有用な、メモリの異なるパーティション及び異なるパーティションに記憶されている暗号化されていないファイル及び暗号化されているファイルの概略図であり、或る特定のパーティション及び暗号化されているファイルへのアクセスは、アクセスポリシー及び認証手順によって制御されている。

30

【図 3】メモリ内の異なるパーティションを示しているメモリの概略図である。

【図 4】図 3 に示すメモリの異なるパーティションのファイル場所表の概略図であり、パーティション内のファイルの内の幾つかは暗号化されている。

【図 5】本発明の態様を説明するのに有用である、アクセスが制御された記録グループ内のアクセス制御記録及び関係付けられた鍵リファレンスの概略図である。

【図 6】本発明の態様を説明するのに有用である、アクセスが制御された記録グループによって形成されたツリー構造及びアクセスが制御された記録の概略図である

40

【図 7】ツリー形成のプロセスを説明するために、アクセスが制御された記録グループの 3 つの階層ツリーを示している概略図である。

【図 8 A】図 8 A は、システムアクセス制御記録を作成し使用するために、ホスト装置とメモリカードの様なメモリ装置によって実行されるプロセスを説明しているフローチャートである。

【図 8 B】図 8 B は、システムアクセス制御記録を作成し使用するために、ホスト装置とメモリカードの様なメモリ装置によって実行されるプロセスを説明しているフローチャートである。

【図 9】本発明の態様を説明するために、システムアクセス制御記録を使用してアクセスが制御された記録グループを作成するプロセスを説明しているフローチャートである。

50

【図 10】アクセス制御記録を作成するためのプロセスを説明しているフローチャートである。

【図 11】階層ツリーの特定のアプリケーションを説明するのに有用な、2つのアクセス制御記録グループの概略図である。

【図 12】特定の権利の委託のプロセスを説明しているフローチャートである。

【図 13】図 12 の委託のプロセスを説明するための、アクセスが制御された記録グループ及びアクセス制御記録の概略図である。

【図 14】暗号化及び／又は復号を目的として鍵を作成するためのプロセスを説明しているフローチャートである。

【図 15】アクセスされた制御記録に従って、アクセス権及び／又はデータアクセスの許可を削除するプロセスを説明しているフローチャートである。

【図 16】アクセス権及び／又はアクセスに対する許可が抹消されるか期限切れになったときにアクセスを要求するプロセスを説明しているフローチャートである。

【図 17 A】図 17 A は、認証及びアクセスのセッションの、幾つかのセッションが開いているときのセッションを説明しているフロー図である。

【図 17 B】図 17 B は、認証及びアクセスのセッションの、幾つかのセッションが開いているときのセッションを説明しているフロー図である。

【図 18】メディアコンテンツを安全に記憶し、そこに記憶されているメディアコンテンツを制御された方法で送付するために、メモリ装置が使用されている環境を示している。

【図 19 A】図 19 A は、本発明の様々な実施形態を説明するのに有用な、メディアコンテンツ配信用の異なる手段を説明しているフロー図である。

【図 19 B】図 19 B は、本発明の様々な実施形態を説明するのに有用な、メディアコンテンツ配信用の異なる手段を説明しているフロー図である。

【図 19 C】図 19 C は、本発明の様々な実施形態を説明するのに有用な、メディアコンテンツ配信用の異なる手段を説明しているフロー図である。

【図 19 D】図 19 D は、本発明の様々な実施形態を説明するのに有用な、メディアコンテンツ配信用の異なる手段を説明しているフロー図である。

【図 20】異なる機能が装置の異なる領域に記憶されているメモリ措置の 1 つの実施形態のブロック図である。

【図 21】図 19 A から図 19 D 及び本出願の他の図の異なるメディアコンテンツ配信スキームを実施するために使用されているシステムアーキテクチャのブロック図である。

【図 22】メディアコンテンツ配信のための 1 つの可能な手段を説明するため、支払い済みメディアコンテンツ及び未払いのカタログメディアを含んでいるメモリ装置を説明しているブロック図である。

【図 23 A】図 23 A は、図 22 の装置が関与するコンテンツロック解除プロセスを説明しているフローチャートである。

【図 23 B】図 23 B は、図 22 の装置が関与するコンテンツロック解除プロセスを説明しているフローチャートである。

【図 23 C】図 23 C は、図 22 の装置が関与するコンテンツロック解除プロセスを説明しているフローチャートである。

【図 24】アクセス制御記録 (ACR) と委託属性を使用して、図 22 の装置内のロックされているカタログメディアコンテンツをロック解除する更に別の実施形態を説明しているブロック図である。

【図 25 A】図 25 A は、コンテンツレンダリングのプロセスを説明しているフローチャートである。

【図 25 B】図 25 B は、コンテンツレンダリングのプロセスを説明しているフローチャートである。

【図 26】本発明の更なる特徴を説明する、不揮発性書換可能メモリ装置の安全アーキテクチャ又は制御構造のブロック図である。

【図 27】図 27 は、エンドユーザー端末とメモリ装置の間の相互認証のためのアーキテ

10

20

30

40

50

クチャ全体を示している。

【図 28】図 28 は、エンドユーザー端末とメモリ装置の間の相互認証のためのアーキテクチャ全体を示している。

【図 29】図 29 は、エンドユーザー端末とメモリ装置の間の相互認証のためのアーキテクチャ全体を示している。

【図 30】図 30 は、エンドユーザー端末とメモリ装置の間の相互認証のためのアーキテクチャ全体を示している。

【図 31】図 31 は、エンドユーザー端末とメモリ装置の間の相互認証のためのアーキテクチャ全体を示している。

【図 32】図 32 は、エンドユーザー端末とメモリ装置の間の相互認証のためのアーキテクチャ全体を示している。

【図 33 A】図 33 A は、プリペイド並びにカタログコンテンツのための鍵と権利オブジェクトの生成とローディングのプロセスを説明しているフローチャートである。

【図 33 B】図 33 B は、プリペイド並びにカタログコンテンツのための鍵と権利オブジェクトの生成とローディングのプロセスを説明しているフローチャートである。

【図 34】図 34 は、プリペイド並びにカタログコンテンツのための鍵と権利オブジェクトの生成とローディングのプロセスを説明しているフローチャートである。

【図 35】図 35 は、プリペイド並びにカタログコンテンツのための鍵と権利オブジェクトの生成とローディングのプロセスを説明しているフローチャートである。

【図 36 A】図 36 A は、本発明の実施形態を説明するための、暗号化されたメディアタイトルとその様なタイトルのプレビューを有するメモリ装置の概略図である。

【図 36 B】図 36 B は、本発明の実施形態を説明するための、暗号化されたメディアタイトルとその様なタイトルのプレビューを有するメモリ装置の概略図である。

【図 36 C】図 36 C は、本発明の実施形態を説明するための、暗号化されたメディアタイトルとその様なタイトルのプレビューを有するメモリ装置の概略図である。

【図 36 D】図 36 D は、本発明の実施形態を説明するための、暗号化されたメディアタイトルとその様なタイトルのプレビューを有するメモリ装置の概略図である。

【図 37 A】図 37 A は、本発明の更なる実施形態を説明するための、プレビューを有するメモリ装置の概略図である。

【図 37 B】図 37 B は、本発明の更なる実施形態を説明するための、プレビューを有するメモリ装置の概略図である。

【図 37 C】図 37 C は、本発明の更なる実施形態を説明するための、プレビューを有するメモリ装置の概略図である。

【図 38 A】図 38 A は、本発明の更なる実施形態を説明するための、暗号化されたメディアタイトルを有するメモリ装置の概略図である。

【図 38 B】図 38 B は、本発明の更なる実施形態を説明するための、暗号化されたメディアタイトルを有するメモリ装置の概略図である。

【図 39 A】図 39 A は、本発明の更なる実施形態を説明するための、権利オブジェクトを有するメモリ装置の概略図である。

【図 39 B】図 39 B は、本発明の更なる実施形態を説明するための、権利オブジェクトを有するメモリ装置の概略図である。

【図 40】図 40 は、本発明の実施形態を説明するため、図 36 A から図 39 B のメモリ装置を使用してメディアコンテンツを配信するためのプロセスを説明しているフローチャートである。

【図 41】図 41 は、本発明の実施形態を説明するため、図 36 A から図 39 B のメモリ装置を使用してメディアコンテンツを配信するためのプロセスを説明しているフローチャートである。

【図 42】図 42 は、本発明の実施形態を説明するため、図 36 A から図 39 B のメモリ装置を使用してメディアコンテンツを配信するためのプロセスを説明しているフローチャートである。

10

20

30

40

50

【図４３】図４３は、本発明の実施形態を説明するため、図３６Ａから図３９Ｂのメモリ装置を使用してメディアコンテンツを配信するためのプロセスを説明しているフローチャートである。

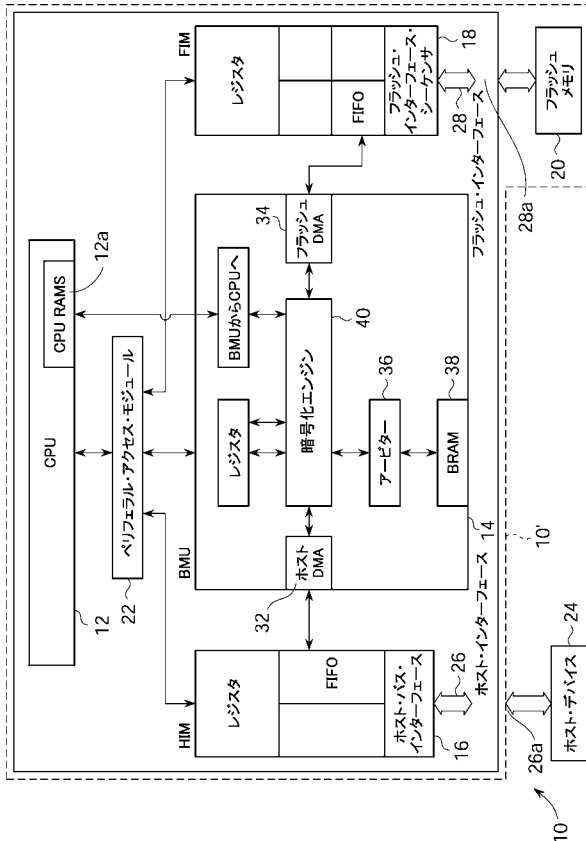
【図４４】図４４は、本発明の実施形態を説明するため、図３６Ａから図３９Ｂのメモリ装置を使用してメディアコンテンツを配信するためのプロセスを説明しているフローチャートである。

【図４５】図４５は、本発明の実施形態を説明するため、図３６Ａから図３９Ｂのメモリ装置を使用してメディアコンテンツを配信するためのプロセスを説明しているフローチャートである。

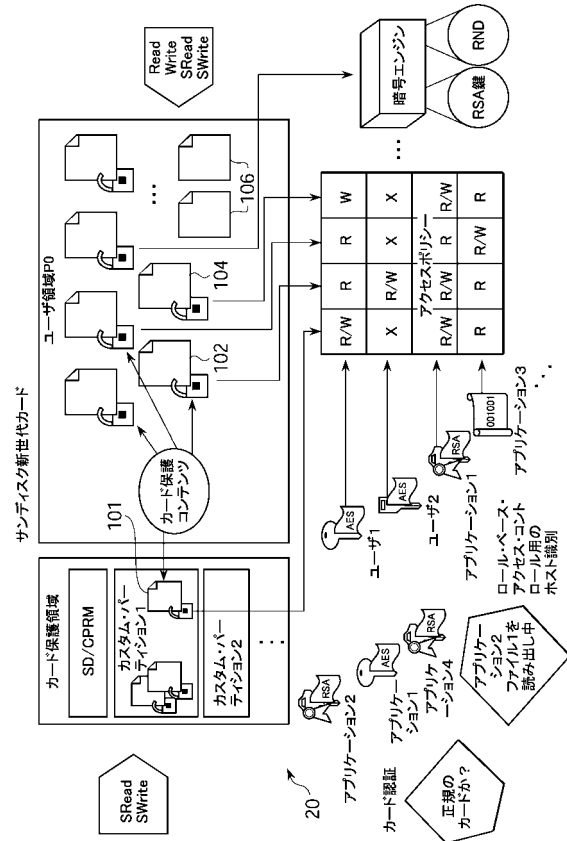
【図４６】図４６は、本発明の実施形態を説明するため、図３６Ａから図３９Ｂのメモリ装置を使用してメディアコンテンツを配信するためのプロセスを説明しているフローチャートである。

10

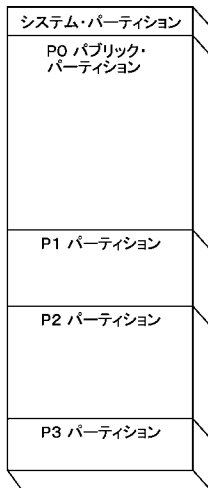
【 図 1 】



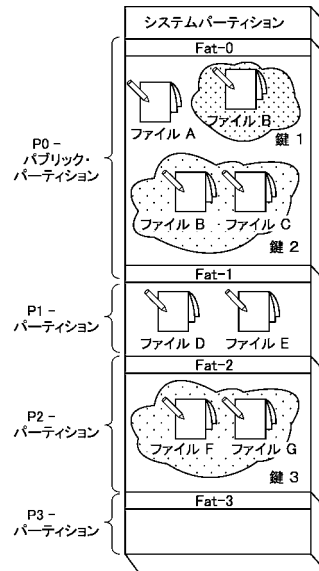
【图 2】



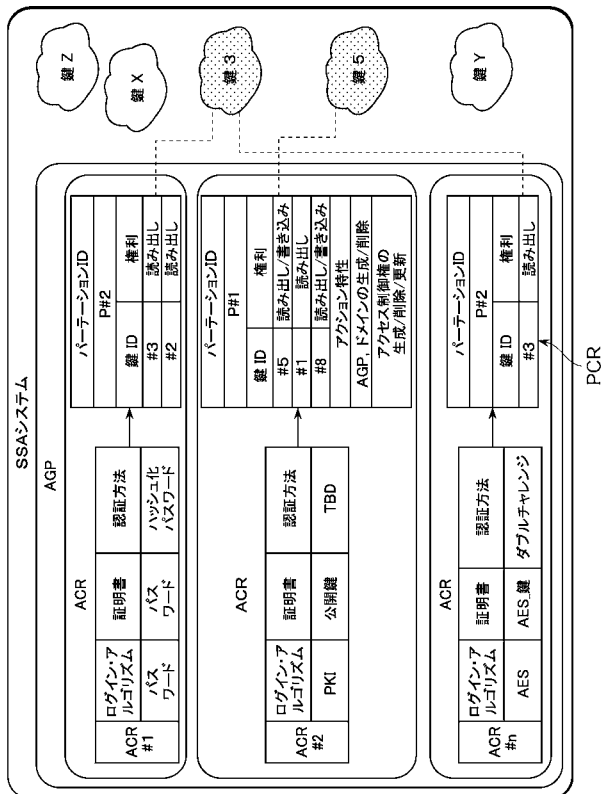
【 図 3 】



【図 4】



【図 5】



【 図 6 】

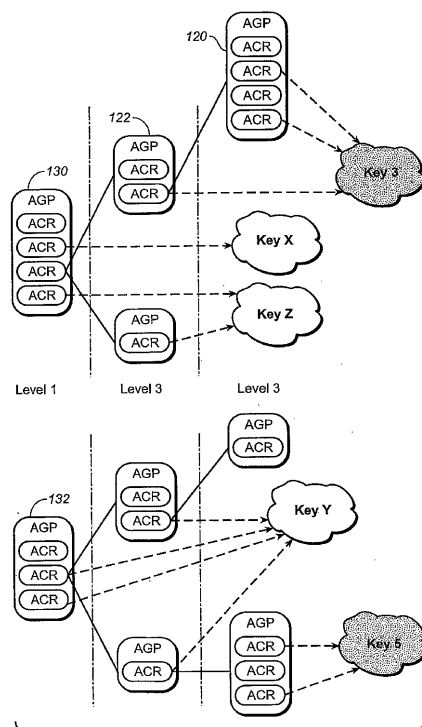
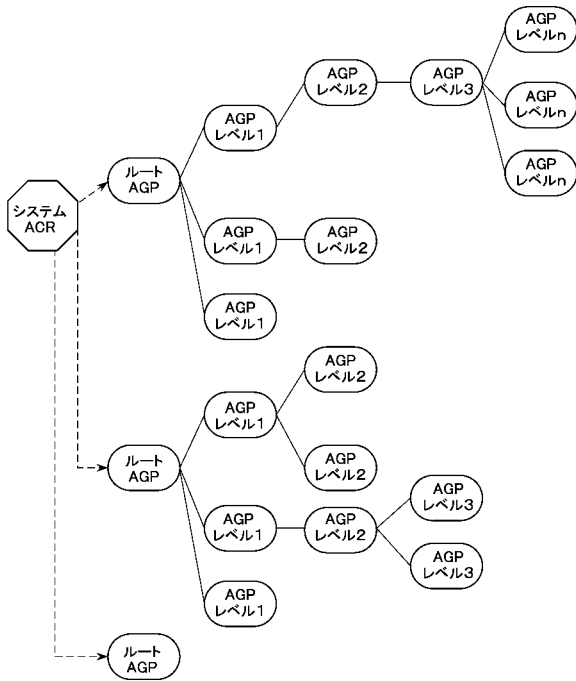
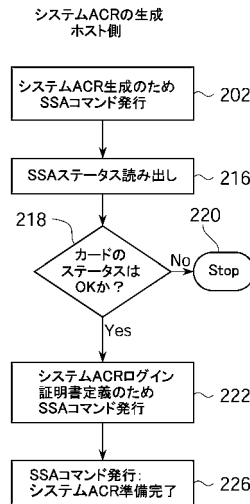


FIG. 6

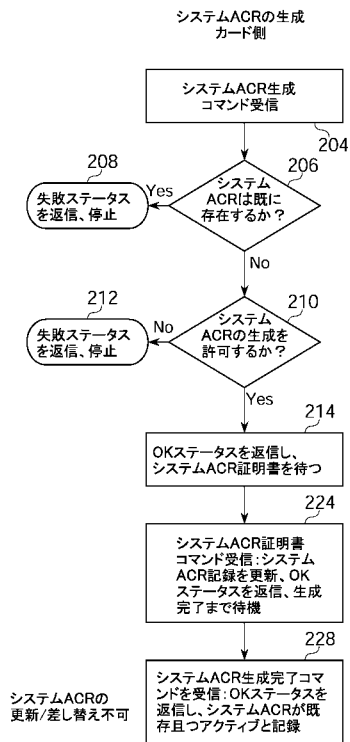
【图 7】



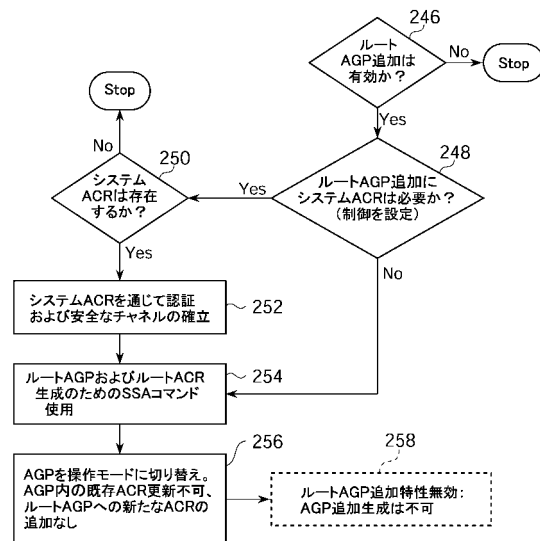
【図 8 A】



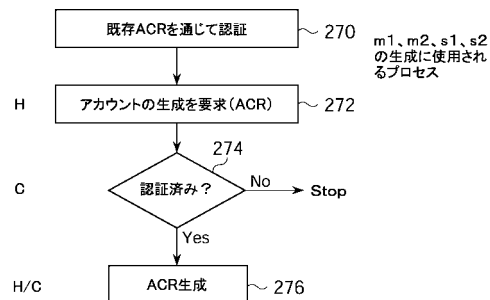
【 図 8 B 】



【図 9】

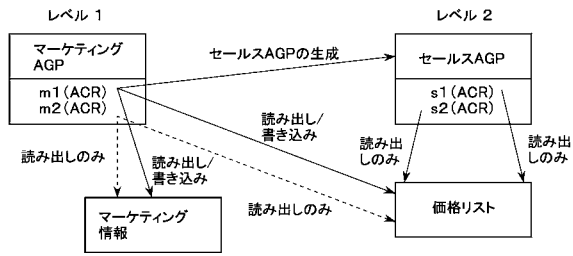


【 図 1 0 】

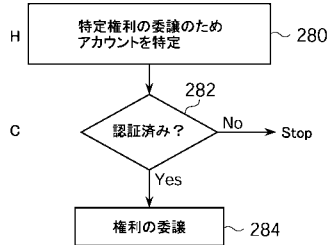


【図 1 1】

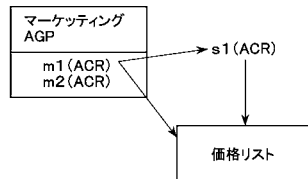
マーケティングAGP内に2つのACR(m1、m2)を、
セールスAGP内に2つのACR(s1、s2)を、それぞれ生成



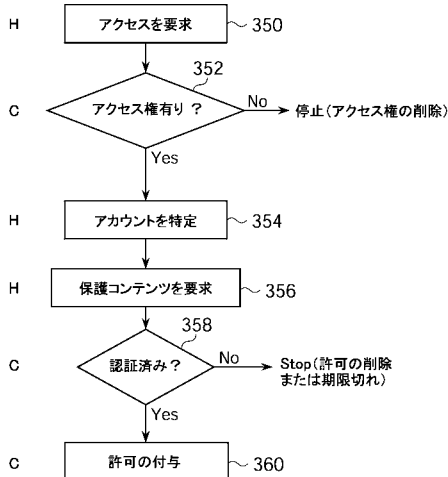
【図 1 2】



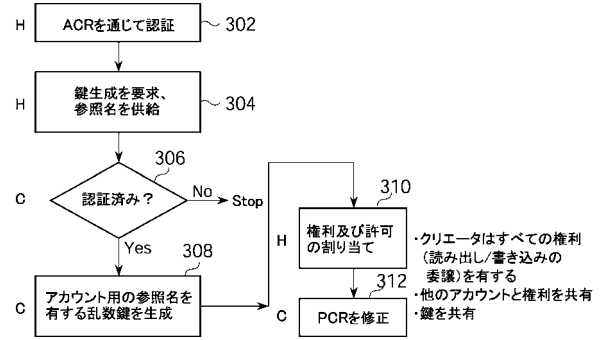
【図 1 3】



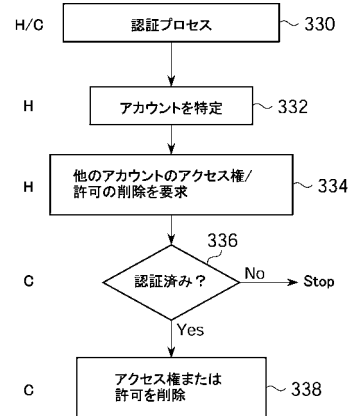
【図 1 6】



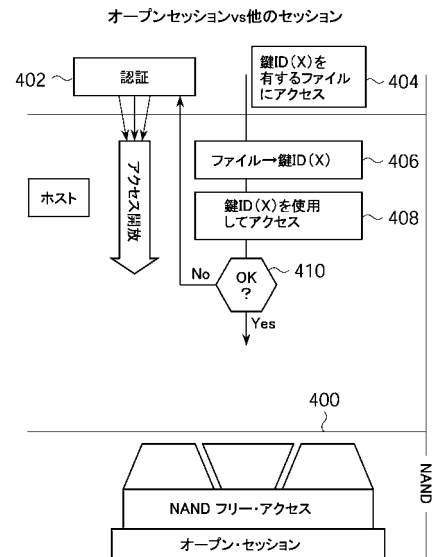
【図 1 4】



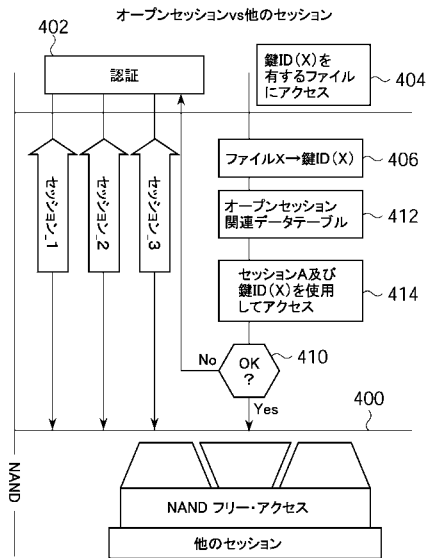
【図 1 5】



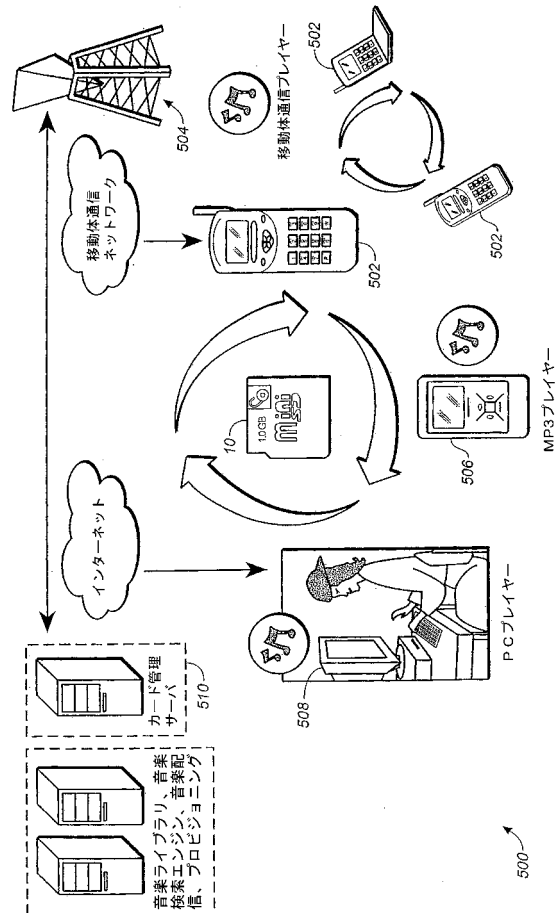
【図 1 7 A】



【図 17 B】

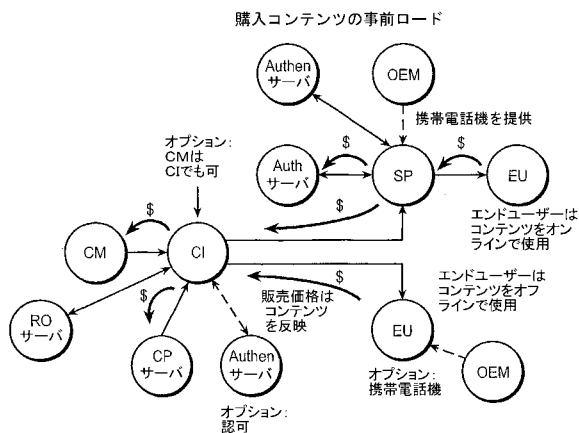


【図 18】

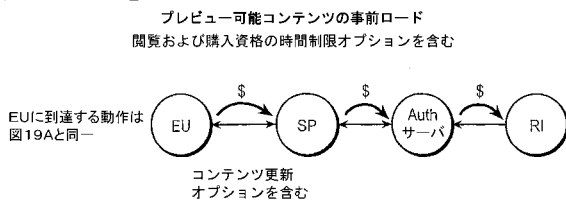


【図 19 A】

SP - サービスプロバイダ (例えば、MNO - 移動体通信ネットワークオペレータ);
 OEM - 機器製造業者 (例えば、携帯電話機、PC);
 Authenサーバ - 認証サーバ (カードが正規で信頼できるフラッシュカードであることを確認する);
 Authサーバ - 認可サーバ (特性を使用可能化又は活性化);
 CPサーバ - コンテンツプロバイダサーバ; ROサーバ - コンテンツ権利オブジェクトサーバ

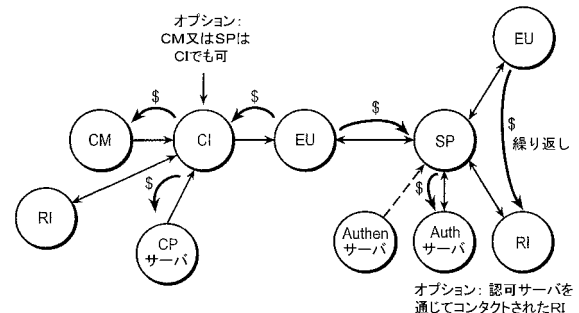


【図 19 B】



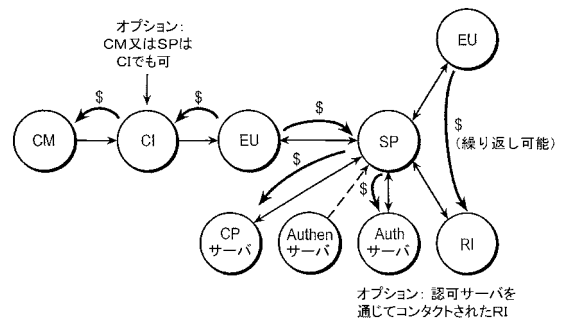
【図 19 C】

購入時のみ閲覧可能な事前ロードコンテンツ
 (オプションとしての時間制限プレビュー)

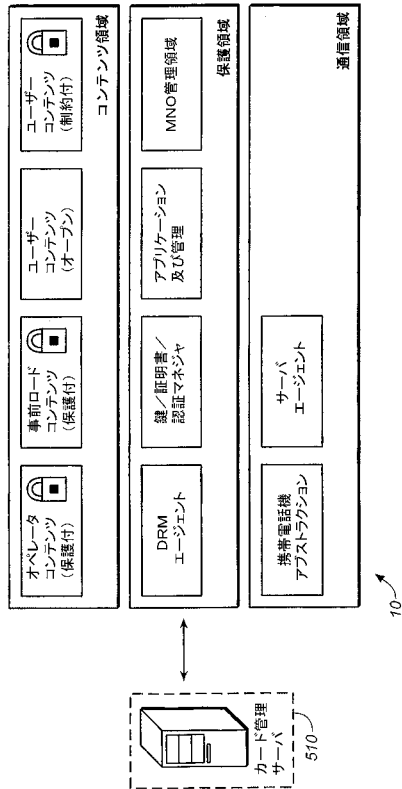


【図 19 D】

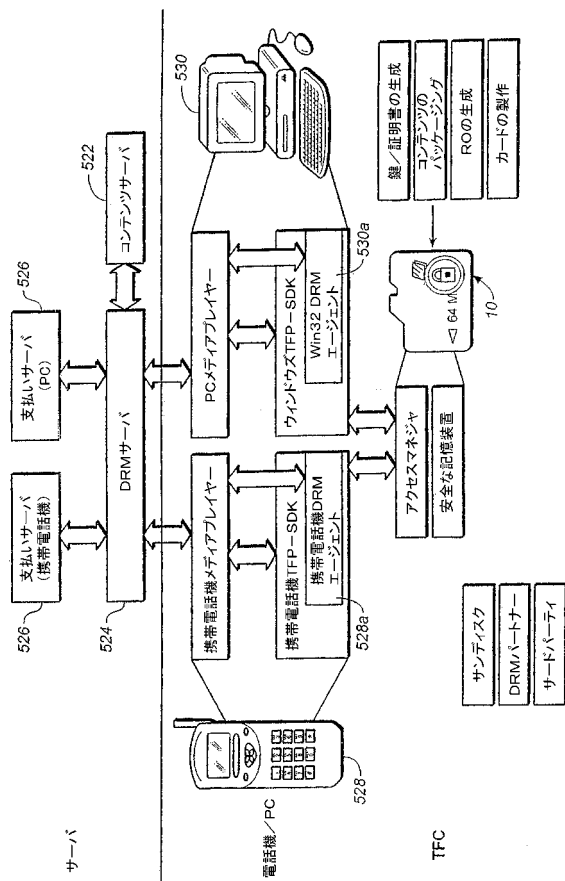
事前ロードコンテンツの無い使用可能カード
 (初期CPサーバとRIの除去以外図19Cと同一)



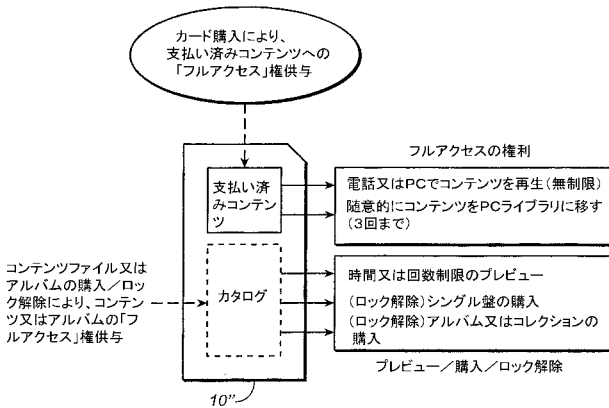
【図 20】



【図 21】

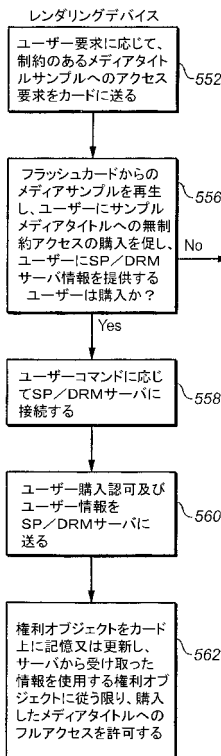


【図 22】



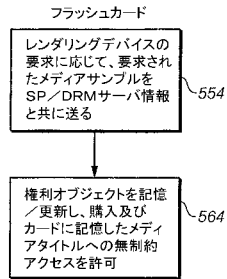
【図 23 A】

プレビュー、ノーカットコンテンツ、
権利オブジェクトを有するカード
コンテンツロック解除



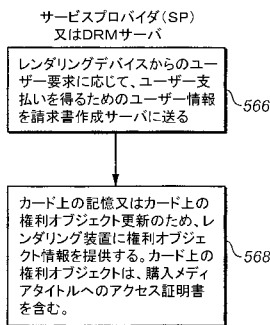
【図 2 3 B】

プレビュー、ノーカットコンテンツ、
権利オブジェクトを有するカード
コンテンツロック解除



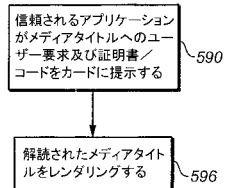
【図 2 3 C】

プレビュー、ノーカットコンテンツ、
権利オブジェクトを有するカード
コンテンツロック解除



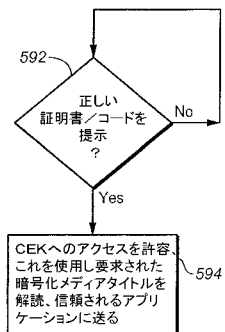
【図 2 5 A】

コンテンツレンダリング
レンダリングデバイス
（ホスト）

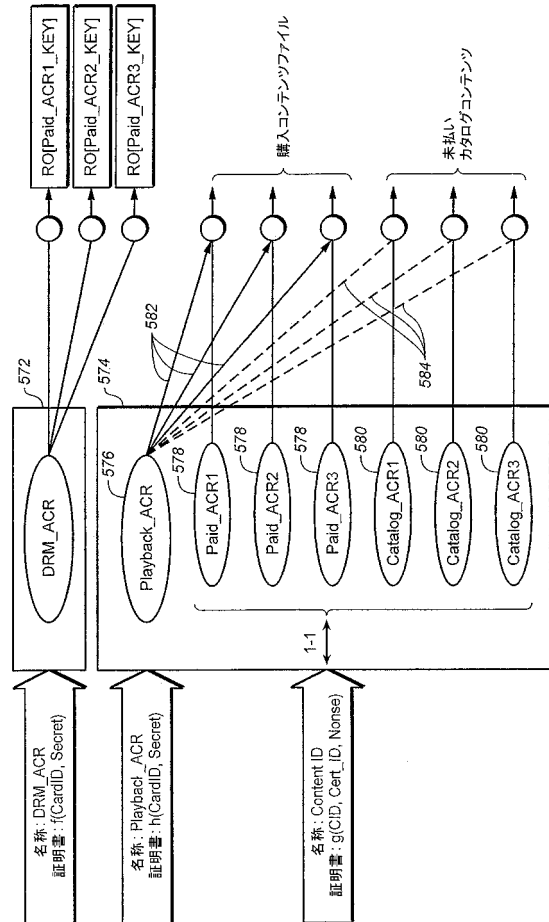


【図 2 5 B】

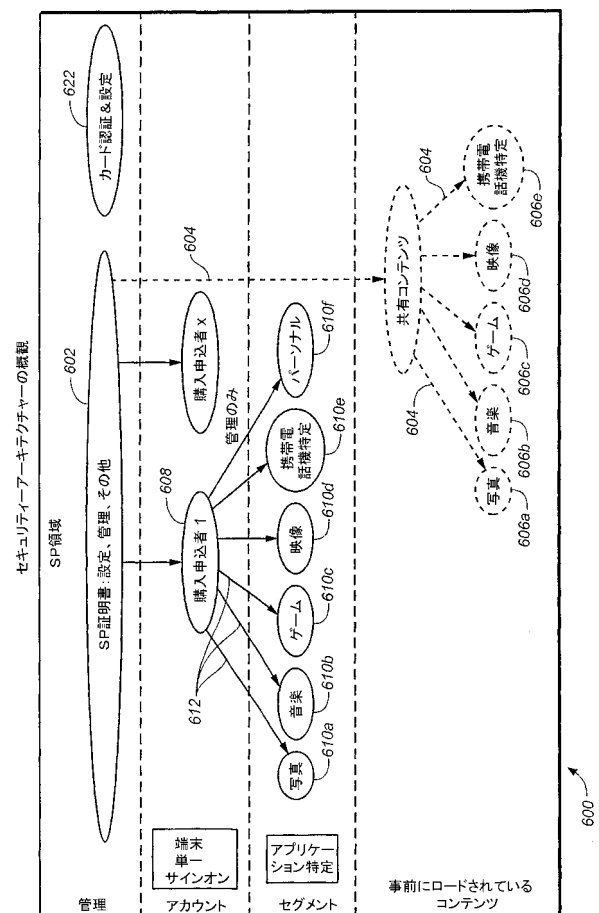
コンテンツレンダリング
フラッシュカード



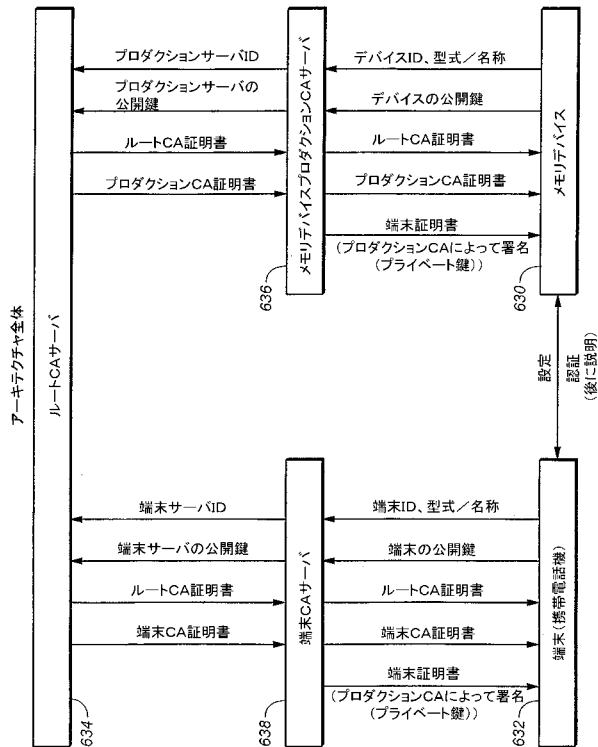
【図 2 4】



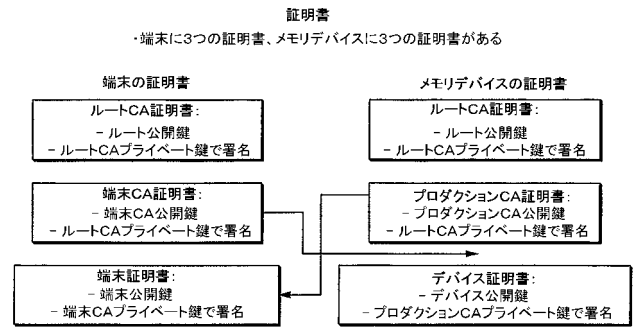
【図 2 6】



【図 27】



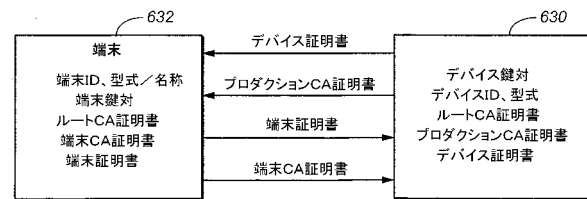
【図 28】



【図 29】

デバイスとカードの最初の設定

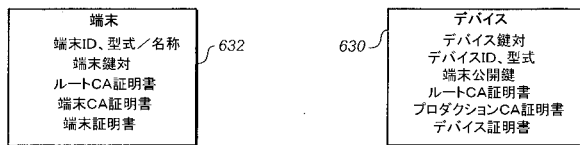
- 最初にデバイスを端末に挿入し、証明書の交換を行う。
- 端末は、デバイス証明書とプロダクションCA証明書を入手する。デバイスは、端末証明書と端末CA証明書を入手する。



【図 30】

デバイスとカードの最初の設定(続き)

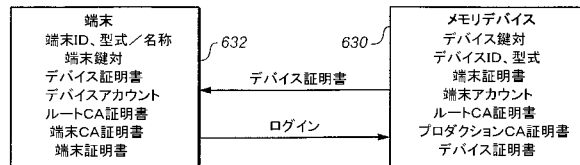
- ・端末は、ルートCA公開鍵を使って生産CA証明書の生産CA公開鍵を検証する。プロダクションCAが同じルートCAによって署名されていれば、検証は合格する。公開鍵を使用してもよい。
- ・端末は、公開鍵を使って検証し、デバイス公開鍵を入手する。
- ・同じ端末をデバイス内で実行する。デバイスは、有効な(端末公開鍵付の)端末証明書を得る。



【図 31】



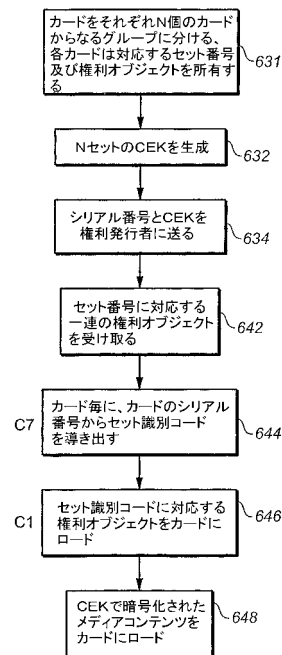
【図 32】



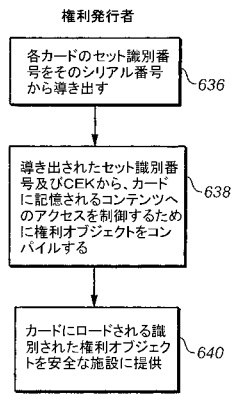
【図 33A】

セキュアファシリティにおいて

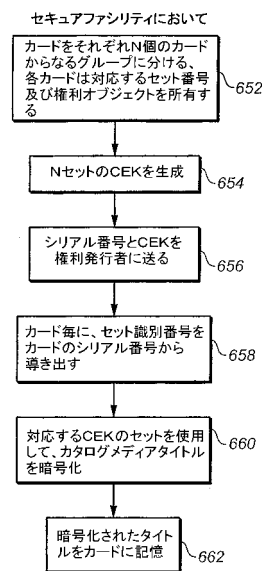
GEKを生成
ROを入手及びロード



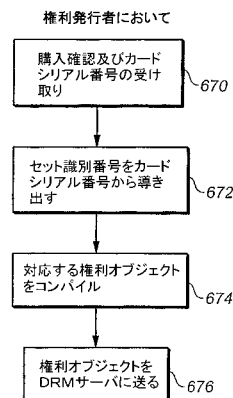
【図 3 3 B】



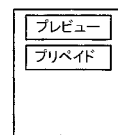
【図 3 4】



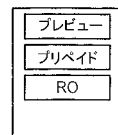
【図 3 5】



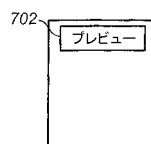
【図 3 6 C】



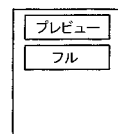
【図 3 6 D】



【図 3 7 A】



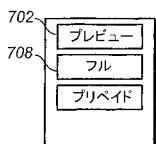
【図 3 7 B】



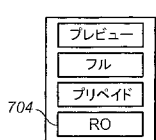
【図 3 7 C】



【図 3 6 A】



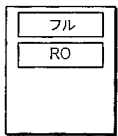
【図 3 6 B】



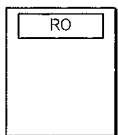
【図 38 A】



【図 38 B】



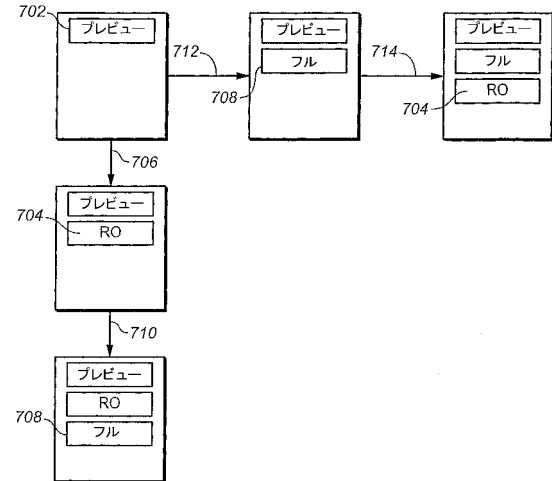
【図 39 A】



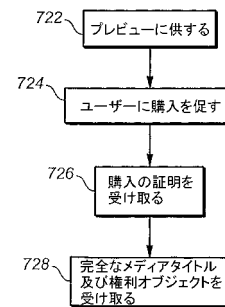
【図 39 B】



【図 40】

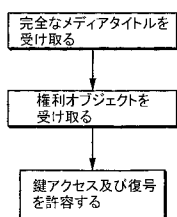


【図 41】



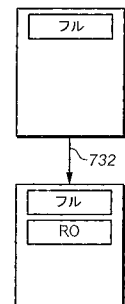
【図 42】

最初はプレビューのみのカード



【図 43】

最初はノーカットコンテンツのみのカード



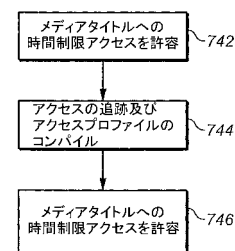
【図 44】

最初はノーカットコンテンツのみのカード



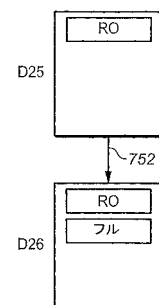
【図 45】

最初はノーカットコンテンツのみのカード



【図 46】

最初は権利オブジェクトのみのカード



フロントページの続き

(51)Int.Cl.	F I	テーマコード (参考)
G 0 6 F 21/24 (2006.01)	G 0 6 F 17/60 5 1 2	
G 0 6 F 21/00 (2006.01)	G 0 6 F 12/14 5 2 0 D	
	G 0 6 F 12/14 5 4 0 A	
	G 0 6 F 12/14 5 2 0 F	
	G 0 6 F 15/00 3 3 0 Z	

(81)指定国 AP(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), EP(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW

(72)発明者 ジャゴソークーロン, ファブリス
アメリカ合衆国 9 4 0 7 0 カリフォルニア州, サンカルロス, バックランド アヴェニュー 8 5 5

(72)発明者 サベットーシャルギ, ファルシッド
アメリカ合衆国 9 4 0 2 4 カリフォルニア州, ロス アルトス ヒルズ, マグダレン アヴェニュー 1 1 1 9 8

(72)発明者 ホルツマン, マイケル
アメリカ合衆国 9 5 0 1 4 カリフォルニア州, クパティーノ, バーンハート プレイス 7 6 0 2

(72)発明者 ケイロン, パスカル
アメリカ合衆国 1 0 0 1 4 ニューヨーク州, ニューヨーク, グリニッチ ストリート 6 6 6, # 5 4 4

(72)発明者 ドワイヤー, パトリシア
アメリカ合衆国 9 4 0 7 0 カリフォルニア州, サンカルロス, シーダー ストリート 1 9 8

(72)発明者 ムカヴォイ, ポール
アメリカ合衆国 9 4 1 1 0 カリフォルニア州, サンフランシスコ, ドロレス ストリート 5 3 9

(72)発明者 ヴァルガス, ペドロ
アメリカ合衆国 9 5 1 3 0 カリフォルニア州, サンノゼ, グリーソン アヴェニュー 3 6 4 8

(72)発明者 ユアン, ポ
アメリカ合衆国 9 5 1 3 4 カリフォルニア州, サンノゼ, リオ ロブルス イースト 8 5, ユニット 2 1 1 3

(72)発明者 チャン, ロバート, シー.
アメリカ合衆国 9 4 5 0 6 カリフォルニア州, ダンヴィル, スタントン コート 1 0

F ターム(参考) 5B017 AA03 BA06 BA07 BB09 BB10 CA16
5B285 AA02 AA03 BA06 BA09 CA18 CA42 CA44 CB02 CB62 CB64
CB73 CB85 CB92 DA05
5C164 MB34S PA09 SC02P UC22P
5J104 AA15 AA16 EA16 EA20 PA07 PA10

【要約の続き】

ンツ、当該コンテンツへのアクセスを管理する権利及び／又は規則）は、安全且つ効率的な方法で生成されロードされる。