(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-248178
(P2012-248178A)
(43)公開日　平成24年12月13日(2012.12.13)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	21/24	166C	5J104
G06F 21/22	(2006.01)	G06F	21/22	110D	
H04L 9/08	(2006.01)	G06F	21/22	112B	
		H04L	9/00	601E	
		H04L	9/00	601D	

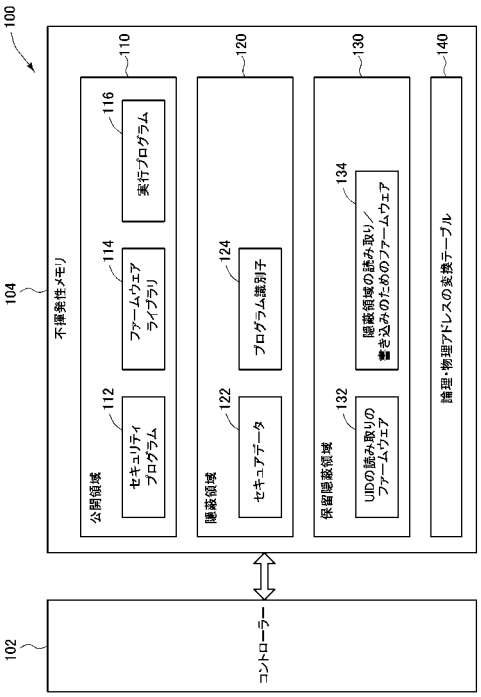
審査請求 有　請求項の数 22　ＯＬ　（全 22 頁）

(21)出願番号　特願2012-12029(P2012-12029)
(22)出願日　平成24年1月24日(2012.1.24)
(31)優先権主張番号　13/115,457
(32)優先日　平成23年5月25日(2011.5.25)
(33)優先権主張国　米国(US)

(71)出願人　512019424
コンデル　インターナショナル　テクノロジーズ　インコーポレイテッド
ＣｏｎＤｅｌ　Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｔｅｃｈｎｏｌｏｇｉｅｓ　Ｉｎｃ．
イギリス領ケイマン諸島　グランドケイマン　ケーワイ１－１２０３　ジョージタウン　ピーオーボックス　３０５９２
Ｐ．Ｏ．　Ｂｏｘ　３０５９２，　Ｇｅｏｒｇｅ　Ｔｏｗｎ，　Ｇｒａｎｄ　Ｃａｙｍａｎ　ＫＹ１－１２０３
(74)代理人　100095751
弁理士　菅原　正倫
(72)発明者　林　育中
台湾彰化縣二林鎮北平里３鄰新民街６號
最終頁に続く

(54)【発明の名称】セキュアリムーバブルメディアとその管理方法

(57)【要約】　（修正有）
【課題】セキュアリムーバブルメディアとその管理方法を提供する。
【解決手段】セキュアリムーバブルメディア１００は、不揮発性メモリとコントローラーを含む。不揮発性メモリは対応するメディア識別子UIDを有し、且つ、公開領域、隠蔽領域、及び、保留隠蔽領域を有して、データを保存し、セキュリティプログラムは公開領域に保存され、メディア識別子を回収する第一ファームウェア１３２と隠蔽領域にアクセスする第二ファームウェア１３４は、保留隠蔽領域に保存される。コントローラーは、外部装置からセキュアデータを受信する。セキュリティプログラムは、第一ファームウェアを用いて、不揮発性メモリから、メディア識別子を回収し、メディア識別子に従って、暗号化キーを生成し、暗号化キーに従って、セキュアデータを暗号化して、且つ、第二ファームウェアを用いて、暗号化セキュアデータを隠蔽領域に書き込む。
【選択図】図１



【特許請求の範囲】
【請求項１】
セキュアリムーバブルメディアであって、
メディア識別子に対応し、公開領域、隠蔽領域、及び、保留隠蔽領域を有して、データを保存し、前記メディア識別子を回収する第一ファームウェアと前記隠蔽領域にアクセスする第二ファームウェアが、前記保留隠蔽領域に保存され、前記メディア識別子は、不揮発性メモリの半導体チップに物理的に登録され、正規のメモリセルに保存されない不揮発性メモリと、
外部装置から、セキュアデータを受信するコントローラーと、
前記公開領域に保存され、前記第一ファームウェアを用いて、前記不揮発性メモリから、前記メディア識別子を回収し、前記第一ファームウェアにより与えられる前記メディア識別子に従って、暗号化キーを生成し、前記暗号化キーに従って、前記セキュアデータを暗号化し、暗号化セキュアデータを得て、且つ、前記第二ファームウェアを用いて、前記暗号化セキュアデータを前記隠蔽領域に書き込むセキュリティプログラムと、
を含むことを特徴とするセキュアリムーバブルメディア。
【請求項２】
前記セキュリティプログラムは、
前記第一ファームウェアを起動し、前記不揮発性メモリから、前記メディア識別子を回収し、前記第二ファームウェアを起動して、前記暗号化セキュアデータを前記隠蔽領域に書き込むファームウェアライブラリと、
前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記暗号化キーを生成する鍵導出機能と、
前記暗号化キーに従って、前記セキュアデータを暗号化し、前記暗号化セキュアデータを得る暗号化/復号機能と、
を含むことを特徴とする請求項1に記載のセキュアリムーバブルメディア。
【請求項３】
前記セキュアデータが、前記セキュアリムーバブルメディアから回収される時、前記セキュリティプログラムは、前記隠蔽領域から、前記暗号化セキュアデータを読み取り、前記不揮発性メモリから、前記メディア識別子を読み取り、前記第一ファームウェアにより与えられる前記メディア識別子に従って、復号キーを生成し、前記復号キーに従って、前記暗号化セキュアデータを復号し、前記セキュアデータを得ることを特徴とする請求項1に記載のセキュアリムーバブルメディア。
【請求項４】
前記セキュリティプログラムは、
前記第二ファームウェアを起動して、前記隠蔽領域から前記暗号化セキュアデータを読み取り、前記第一ファームウェアを起動して、前記不揮発性メモリから、前記メディア識別子を回収するファームウェアライブラリと、
前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記復号キーを生成する鍵導出機能と、
前記復号キーに従って、前記暗号化セキュアデータを復号し、前記セキュアデータを得る暗号化/復号機能と、
を含むことを特徴とする請求項3に記載のセキュアリムーバブルメディア。
【請求項５】
セキュアリムーバブルメディアの管理方法であって、前記セキュアリムーバブルメディアは、不揮発性メモリとコントローラーを含み、前記不揮発性メモリはメディア識別子に対応し、前記不揮発性メモリは、公開領域、隠蔽領域、及び、保留隠蔽領域に分けられ、データを保存し、前記メディア識別子は、前記不揮発性メモリの前記半導体チップに物理的に登録され、正規のメモリセルに保存されず、
前記メディア識別子を回収する第一ファームウェアと前記隠蔽領域にアクセスする第二ファームウェアを、前記保留隠蔽領域に保存するステップと、

外部装置により、セキュアデータを前記セキュアリムーバブルメディアに伝送するステップと、
前記第一ファームウェアを用いて、前記コントローラーにより、前記不揮発性メモリから、前記メディア識別子を回収するステップと、
前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記公開領域に保存されたセキュリティプログラムにより、暗号キーを生成するステップと、
前記暗号化キーに従って、前記セキュリティプログラムにより、前記セキュアデータを暗号化して、暗号化セキュアデータを得るステップと、
前記第二ファームウェアを用いて、前記コントローラーにより、前記暗号化セキュアデータを前記隠蔽領域に書き込むステップと、
を含むことを特徴とする管理方法。
【請求項６】
前記方法は、更に、
前記セキュアデータが前記セキュアリムーバブルメディアから回収される時、前記隠蔽領域から、前記コントローラーにより、前記暗号化セキュアデータを読み取るステップと、
前記コントローラーにより、前記不揮発性メモリから、前記メディア識別子を回収するステップと、
前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記セキュリティプログラムにより、復号キーを生成するステップと、
前記復号キーに従って、前記セキュリティプログラムにより、前記暗号化セキュアデータを復号し、前記セキュアデータを得るステップと、
を含むことを特徴とすることを特徴とする請求項5に記載の方法。
【請求項７】
セキュアリムーバブルメディアであって、
メディア識別子に対応し、公開領域、隠蔽領域、及び、保留隠蔽領域を有して、データを保存し、前記メディア識別子を回収する第一ファームウェアと前記隠蔽領域にアクセスする第二ファームウェアが、前記保留隠蔽領域に保存され、前記メディア識別子は、不揮発性メモリの半導体チップに物理的に登録され、正規のメモリセルに保存されない不揮発性メモリと、
外部装置から実行プログラムを受信し、その後、前記実行プログラムを前記セキュリティプログラムにリンクするコントローラーと、
前記公開領域に保存され、前記第一ファームウェアを用いて、前記不揮発性メモリから、前記メディア識別子を回収し、前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記実行プログラムと前記不揮発性メモリに対応する第一プログラム識別子を生成し、前記第二ファームウェアを用いて、前記第一プログラム識別子を前記隠蔽領域に書き込むセキュリティプログラムと、
を含むことを特徴とするセキュアリムーバブルメディア。
【請求項８】
前記セキュリティプログラムは、前記第一ファームウェアを用いて、前記不揮発性メモリから、前記メディア識別子を回収し、前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記実行プログラムと前記不揮発性メモリに対応する第二プログラム識別子を生成し、前記第二ファームウェアを用いて、前記隠蔽領域から、前記第一プログラム識別子を読み取り、前記第二プログラム識別子と前記第一プログラム識別子を比較し、前記第二プログラム識別子が前記第一プログラム識別子と同一である時、前記実行プログラムの実行を続行し、前記第二プログラム識別子が前記第一プログラム識別子と同一でない時、前記実行プログラムの実行を終了することを特徴とする請求項7に記載のセキュアリムーバブルメディア。
【請求項９】
前記セキュリティプログラムは、

前記第一ファームウェアを起動して、前記不揮発性メモリから、前記メディア識別子を回収し、前記第二ファームウェアを起動して、前記第一プログラム識別子を前記隠蔽領域に書き込み、前記第二ファームウェアを起動して、前記隠蔽領域から、前記第一プログラム識別子を読み取るファームウェアライブラリと、

前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記実行プログラムと前記不揮発性メモリに対応する前記第一プログラム識別子を生成し、前記メディア識別子に従って、前記実行プログラムと前記不揮発性メモリに対応する前記第二プログラム識別子を生成し、前記第二プログラム識別子と前記第一プログラム識別子を比較する認証機能と、

を含むことを特徴とする請求項8に記載のセキュアリムーバブルメディア。

【請求項１０】

セキュアリムーバブルメディアの管理方法であって、前記セキュアリムーバブルメディアは、不揮発性メモリとコントローラーを含み、前記不揮発性メモリはメディア識別子に対応し、前記不揮発性メモリは、公開領域、隠蔽領域、及び、保留隠蔽領域に分けられ、データを保存し、前記メディア識別子は、前記不揮発性メモリの半導体チップに物理的に登録され、正規のメモリセルに保存されず、

前記メディア識別子を回収する第一ファームウェアと前記隠蔽領域にアクセスする第二ファームウェアを、前記保留隠蔽領域に保存するステップと、

外部装置により、実行プログラムを前記セキュアリムーバブルメディアに伝送するステップと、

前記コントローラーにより、前記第一ファームウェアを用いて、前記不揮発性メモリから、前記メディア識別子を回収するステップと、

前記第一ファームウェアにより与えられる前記メディア識別子に従って、セキュリティプログラムにより、前記実行プログラムと前記不揮発性メモリに対応する第一プログラム識別子を生成するステップと、

前記第二ファームウェアを用いて、前記コントローラーにより、前記第一プログラム識別子を前記隠蔽領域に書き込むステップと、

を含むことを特徴とする管理方法。

【請求項１１】

前記方法は、更に、

前記実行プログラムが実行される時、前記第一ファームウェアを用いて、前記コントローラーにより、前記不揮発性メモリから、前記メディア識別子を回収するステップと、

前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記セキュリティプログラムにより、前記実行プログラムと前記不揮発性メモリに対応する第二プログラム識別子を生成するステップと、

前記第二ファームウェアを用いて、前記コントローラーにより、前記隠蔽領域から、前記第一プログラム識別子を読み取り、前記第二プログラム識別子と前記第一プログラム識別子を比較するステップと、

前記第二プログラム識別子が前記第一プログラム識別子と同一である時、前記実行プログラムの実行を続行するステップと、

前記第二プログラム識別子が前記第一プログラム識別子と同一でない時、前記実行プログラムの実行を終了するステップと、

を含むことを特徴とする請求項10に記載の方法。

【請求項１２】

セキュアリムーバブルメディアであって、デジタル著作権管理（DRM）エージェントを含むクライアントエンド装置に装着され、

メディア識別子に対応し、公開領域、隠蔽領域、及び、保留隠蔽領域を含み、データを保存し、前記メディア識別子を回収する第一ファームウェアと前記隠蔽領域にアクセスする第二ファームウェアは、前記保留隠蔽領域に保存され、前記メディア識別子は、不揮発性メモリの半導体チップに物理的に登録され、正規のメモリセルに保存されない不揮発性

メモリと、
前記クライアントエンド装置の前記DRM エージェントから、権利オブジェクトとセキュアデータを受信するコントローラーと、
前記公開領域に保存され、前記第一ファームウェアを用いて、前記不揮発性メモリから、前記メディア識別子を回収し、前記第一ファームウェアにより与えられる前記メディア識別子に従って、暗号化キーを生成し、前記暗号化キーに従って、前記権利オブジェクトと前記セキュアデータを暗号化して、暗号化権利オブジェクトと暗号化セキュアデータを得て、且つ、前記第二ファームウェアを用いて、前記暗号化権利オブジェクトと前記暗号化セキュアデータを、前記隠蔽領域に書き込むセキュアリムーバブルメディア（SRM）エージェントと、
を含むことを特徴とするセキュアリムーバブルメディア。
【請求項１３】
前記SRM エージェントは、
前記第一ファームウェアを起動し、前記不揮発性メモリから、前記メディア識別子を回収し、前記第二ファームウェアを起動して、前記暗号化権利オブジェクトと前記暗号化セキュアデータを、前記隠蔽領域に書き込むファームウェアライブラリと、
前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記暗号化キーを生成する鍵導出機能と、
前記暗号化キーに従って、前記権利オブジェクトと前記セキュアデータを暗号化し、前記暗号化権利オブジェクトと前記暗号化セキュアデータを得る暗号化/復号機能と、
を含むことを特徴とする請求項12に記載のセキュアリムーバブルメディア。
【請求項１４】
前記権利オブジェクトと前記セキュアデータが、前記セキュアリムーバブルメディアから回収される時、前記SRM エージェントは、前記隠蔽領域から、前記暗号化権利オブジェクトと前記暗号化セキュアデータ を読み取り、前記不揮発性メモリから、前記メディア識別子を回収し、前記第一ファームウェアにより与えられる前記メディア識別子に従って、復号キーを生成し、前記復号キーに従って、前記暗号化権利オブジェクトと前記暗号化セキュアデータを復号し、前記権利オブジェクトと前記セキュアデータを得ることを特徴とする請求項12に記載のセキュアリムーバブルメディア。
【請求項１５】
前記SRM エージェントは、
前記第二ファームウェアを起動して、前記隠蔽領域から、前記暗号化権利オブジェクトと前記暗号化セキュアデータを読み取り、前記第一ファームウェアを起動して、前記不揮発性メモリから、前記メディア識別子を回収するファームウェアライブラリと、
前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記復号キーを生成する鍵導出機能と、
前記復号キーに従って、前記暗号化権利オブジェクトと前記暗号化セキュアデータを復号し、前記権利オブジェクトと前記セキュアデータを得る暗号化/復号機能と、
を含むことを特徴とする請求項14に記載のセキュアリムーバブルメディア。
【請求項１６】
前記暗号化権利オブジェクトと前記暗号化セキュアデータが復号されて、前記権利オブジェクトを得た後、前記セキュアリムーバブルメディアが、前記権利オブジェクトを前記クライアントエンド装置に伝送し、前記DRM エージェントは、前記権利オブジェクトを用いて、DRM コンテンツを取得し、前記クライアントエンド装置の前記DRM エージェントは、権利オブジェクト情報を、前記セキュアリムーバブルメディアに戻すことを特徴とする請求項14に記載のセキュアリムーバブルメディア。
【請求項１７】
前記セキュアリムーバブルメディアが、前記クライアントエンド装置から、前記権利オブジェクト情報を受信後、前記SRM エージェントは、前記隠蔽領域から、前記暗号化権利オブジェクトを読み取り、前記不揮発性メモリから前記メディア識別子を回収し、前記第

一ファームウェアにより与えられる前記メディア識別子に従って、前記復号キーを生成し、前記復号キーに従って、前記暗号化権利オブジェクトを復号し、前記権利オブジェクトを得て、前記権利オブジェクト情報に従って、前記権利オブジェクトを修正し、修正された権利オブジェクトを得て、且つ、前記第一ファームウェアを用いて、前記不揮発性メモリから、前記メディア識別子を回収し、前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記暗号化キーを生成し、前記暗号化キーに従って、修正された権利オブジェクトを暗号化し、暗号化された修正権利オブジェクトを得て、且つ、前記第二ファームウェアを用いて、前記暗号化された修正権利オブジェクトを前記隠蔽領域に書き込むことを特徴とする請求項16に記載のセキュアリムーバブルメディア。

【請求項１８】

セキュアリムーバブルメディアの管理方法であって、前記セキュアリムーバブルメディアは、デジタル著作権管理 (DRM) エージェントを含むクライアントエンド装置に結合され、前記セキュアリムーバブルメディアは、不揮発性メモリとコントローラーを含み、前記不揮発性メモリはメディア識別子に対応し、前記不揮発性メモリは、公開領域、隠蔽領域、及び、保留隠蔽領域に分けられ、データを保存し、前記メディア識別子は、前記不揮発性メモリの半導体チップに物理的に登録され、正規のメモリセルに保存されず、

セキュアリムーバブルメディア (SRM) エージェントを、前記不揮発性メモリの前記公開領域に保存するステップと、

前記メディア識別子を回収する第一ファームウェアと前記隠蔽領域にアクセスする第二ファームウェアを、前記保留隠蔽領域に保存するステップと、

前記クライアントエンド装置の前記DRM エージェントから、権利オブジェクトとセキュアデータを、前記セキュアリムーバブルメディアに伝送するステップと、

前記SRMエージェントを実行して、前記第一ファームウェアを使用し、前記不揮発性メモリから、前記メディア識別子を回収するステップと、

前記SRMエージェントを実行して、前記第一ファームウェアにより与えられる前記メディア識別子に従って、暗号化キーを生成するステップと、

前記SRMエージェントを実行して、前記暗号化キーに従って、前記権利オブジェクトと前記セキュアデータを暗号化して、暗号化権利オブジェクトと暗号化セキュアデータを得るステップと、

前記SRMエージェントを実行して、前記第二ファームウェアを用いて、前記暗号化権利オブジェクトと前記暗号化セキュアデータを、前記隠蔽領域に書き込むステップと、

を含むことを特徴とする管理方法。

【請求項１９】

前記方法は、更に、

前記権利オブジェクトと前記セキュアデータが、前記セキュアリムーバブルメディアから回収される時、前記SRMエージェントを実行して、前記隠蔽領域から、前記暗号化権利オブジェクトと前記暗号化セキュアデータを読み取るステップと、

前記SRMエージェントを実行して、前記不揮発性メモリから、前記メディア識別子を回収するステップと、

前記SRMエージェントを実行して、前記第一ファームウェアにより与えられる前記メディア識別子に従って、復号キーを生成するステップと、

前記SRMエージェントを実行して、前記復号キーに従って、前記暗号化権利オブジェクトと前記暗号化セキュアデータを復号し、前記権利オブジェクトと前記セキュアデータを得るステップと、

を含むことを特徴とする請求項18に記載の方法。

【請求項２０】

前記方法は、更に、

前記暗号化権利オブジェクトと前記暗号化セキュアデータが復号されて、前記権利オブジェクトを得た後、前記セキュアリムーバブルメディアにより、前記権利オブジェクトを前記クライアントエンド装置に伝送するステップと、

前記権利オブジェクトを用いて、前記DRM エージェントにより、DRM コンテンツを取得するステップと、
前記DRM エージェントにより、権利オブジェクト情報を前記セキュアリムーバブルメディアに戻すステップと、
を含むことを特徴とする請求項19に記載の方法。
【請求項２１】
前記方法は、更に、
前記セキュアリムーバブルメディアは、前記クライアントエンド装置から、前記権利オブジェクト情報を受信後、前記SRMエージェントを実行して、前記隠蔽領域から、前記暗号化権利オブジェクトを読み取るステップと、
前記SRMエージェントを実行して、前記不揮発性メモリから、前記メディア識別子を回収するステップと、
前記SRMエージェントを実行して、前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記復号キーを生成するステップと、
前記SRMエージェントを実行して、前記復号キーに従って、前記暗号化権利オブジェクトを復号し、前記権利オブジェクトを得るステップと、
前記SRMエージェントを実行して、前記権利オブジェクト情報に従って、前記権利オブジェクトを修正し、修正された権利オブジェクトを得るステップと、
前記SRMエージェントを実行して、前記第一ファームウェアを使用し、前記不揮発性メモリから、前記メディア識別子を回収するステップと、
前記SRMエージェントを実行して、前記第一ファームウェアにより与えられる前記メディア識別子に従って、前記暗号化キーを生成するステップと、
前記SRMエージェントを実行して、前記暗号化キーに従って、修正された権利オブジェクトを暗号化して、暗号化された修正権利オブジェクトを得るステップと、
前記SRMエージェントを実行して、前記第二ファームウェアを用いて、 前記暗号化された修正権利オブジェクトを、前記隠蔽領域に書き込むステップと、
を含むことを特徴とする請求項20に記載の方法。
【請求項２２】
セキュアリムーバブルメディアは、セキュアデジタル (SD) メモリカード、マルチメディアカード(MMC)、又は、USB ディスクであることを特徴とする請求項18に記載のセキュアリムーバブルメディア。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データ保存に関するものであって、特に、セキュアデータの保存に関するものである。
【背景技術】
【０００２】
デジタル著作権管理 (Digital rights management、DRM)は、ハードウェア製造業者、出版社、著作権保有者と個人により使用されて、デジタルコンテンツの使用を制限するアクセス制御技術である。DRM 技術は、エンドユーザーからの未許可のアクセス、複製、又は、他のフォーマットへの転換を防止することにより、デジタルメディア使用の制御を試みる。デジタル著作権管理は、例えば、Sony、Amazon、Apple、及び、Microsoft等の会社に用いられている。下記特許文献１には、マルチメディアにおけるコンテンツの配布や蓄積等に関する技術が開示されている。
【０００３】
エンドユーザーがデジタルコンテンツを再生したい時、エンドユーザーは、DRM サーバから、クライアントエンド装置にデジタルコンテンツをダウンロードし、DRM サーバは、権利オブジェクトをクライアントエンド装置に発する。その後、エンドユーザーは、権利オブジェクトに従って、クライアントエンド装置に保存されるデジタルコンテンツを再生

する。デジタルコンテンツが、承認装置から未承認装置に複製される場合、未承認装置は保存された権利オブジェクトを有さないので、エンドユーザーは、未承認装置に複製されたデジタルコンテンツを再生することができない。一般のDRM サーバは、エンドユーザーが、クライアントエンド装置から別の装置に、権利オブジェクトを移動することを許可しないので、エンドユーザーは、ネットワーク接続により、DRM サーバに接続されたクライアントエンド装置上だけで、デジタルコンテンツを再生し、対応する権利オブジェクトを獲得する。これは、エンドユーザーにとっては不便である。

【０００４】

オープンモバイルアライアンス（Open Mobile Alliance、OMA） は、既に、エンドユーザーが、権利オブジェクトを、クライアントエンド装置からセキュアリムーバブルメディア(SRM)に移動するのを許可するOMA DRM 2.0/2.1 スタンダードを構築している。セキュアリムーバブルメディアの例は、セキュアデジタル (SD)カード、USBディスク、又は、マルチメディアカード (MMC)である。これにより、エンドユーザーは、セキュアリムーバブルメディアに保存された権利オブジェクトを用いて、セキュアリムーバブルメディアに保存されたデジタルコンテンツを再生することができる。このような方法は、ローカル消費と呼ばれる。しかし、SRMスタンダードは、セキュアリムーバブルメディア中、どのように、安全な方式で、権利オブジェクトを保存、回収するかを開示していない。よって、OMADRM2.0/2.1 スタンダードに従って、セキュアリムーバブルメディアに保存される権利オブジェクトを管理する方法が必要である。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】米国公開特許公報US2011/0015985A1

【発明の概要】

【発明が解決しようとする課題】

【０００６】

本発明は、セキュアリムーバブルメディアを提供することを目的とする。

【課題を解決するための手段】

【０００７】

本発明は、セキュアリムーバブルメディアを提出する。一実施例では、セキュアリムーバブルメディアは、不揮発性メモリとコントローラーを含む。セキュアリムーバブルメディアはメディア識別子に対応し、メディア識別子は、不揮発性メモリ半導体チップに物理的に登録される番号で、且つ、正規の不揮発性メモリセル、又は、別のワンタイムプログラム可能メモリ（one-time-programmable memory）、例えば、ROM (read only memory)に保存されず、公開領域、隠蔽領域、及び、保留隠蔽領域を有して、データを保存し、少なくとも一つのセキュリティプログラムが公開領域に保存され、メディア識別子を回収する第一ファームウェアと隠蔽領域にアクセスする第二ファームウェアは、保留隠蔽領域に保存される。コントローラーは、外部装置からセキュアデータを受信する。その後、セキュリティプログラムは、第一ファームウェアを用いて、セキュアリムーバブルメディアから、メディア識別子を回収し、ファームウェアにより与えられたメディア識別に従って、暗号化キーを生成し、暗号化キーに従って、セキュアデータを暗号化し、暗号化セキュアデータを得て、且つ、第二ファームウェアを用いて、暗号化セキュアデータを隠蔽領域に書き込む。

【０００８】

本発明は、セキュアリムーバブルメディアの管理方法も提供する。一実施例では、セキュアリムーバブルメディアは、不揮発性メモリとコントローラーを含み、セキュアリムーバブルメディアはメディア識別子に対応し、メディア識別子は、不揮発性メモリ半導体チップに物理的に登録される番号で、且つ、正規の不揮発性メモリセル、又は、別のワンタイムプログラム可能メモリ、例えば、ROM (read only memory)に保存されない。セキュアリムーバブルメディアは、公開領域、隠蔽領域、及び、保留隠蔽領域に分けられ、データ

を保存する。まず、メディア識別子を回収する第一ファームウェアと隠蔽領域にアクセスする第二ファームウェアが保留隠蔽領域に保存される。セキュアデータが外部装置により、セキュアリムーバブルメディアに伝送される。コントローラーが、第一ファームウェアを用いて、セキュアリムーバブルメディアから、メディア識別子を回収する。ファームウェアにより与えられるメディア識別子に従って、セキュリティプログラムにより、暗号化キーを生成する。セキュアデータは、暗号化キーに従って暗号化され、暗号化セキュアデータを得る。コントローラーが、第二ファームウェアを用いて、暗号化セキュアデータを隠蔽領域に書き込む。

【０００９】

本発明は、更に、セキュアリムーバブルメディアを提供する。一実施例では、セキュアリムーバブルメディアは、不揮発性メモリとコントローラーを含む。セキュアリムーバブルメディアはメディア識別子に対応し、メディア識別子は、不揮発性メモリ半導体チップに物理的に登録される番号で、且つ、正規の不揮発性メモリセル、又は、別のワンタイムプログラム可能メモリ、例えば、ROM (read only memory)に保存されず、セキュアリムーバブルメディアは、公開領域、隠蔽領域、及び、保留隠蔽領域を有して、データを保存し、少なくとも一つのセキュリティプログラムは公開領域に保存され、メディア識別子を回収する第一ファームウェアと隠蔽領域にアクセスする第二ファームウェアは、保留隠蔽領域に保存される。コントローラーは、外部装置から実行プログラムを受信し、その後、実行プログラムはセキュリティプログラムにリンクされる。セキュリティプログラムは、第一ファームウェアを用いて、セキュアリムーバブルメディアから、メディア識別子を回収し、ファームウェアにより与えられるメディア識別子に従って、実行プログラムとセキュアリムーバブルメディアに対応する第一プログラム識別子を生成し、第二ファームウェアを用いて、第一プログラム識別子を隠蔽領域に書き込む。

【００１０】

本発明は、セキュアリムーバブルメディアの管理方法も提供する。一実施例では、セキュアリムーバブルメディアは、不揮発性メモリとコントローラーを含み、セキュアリムーバブルメディアはメディア識別子に対応し、メディア識別子は、不揮発性メモリ半導体チップに物理的に登録される番号で、且つ、正規の不揮発性メモリセル、又は、別のワンタイムプログラム可能メモリ、例えば、ROM (read only memory)に保存されず、セキュアリムーバブルメディアは、公開領域、隠蔽領域、及び、保留隠蔽領域に分けられ、データを保存する。まず、メディア識別子を回収する第一ファームウェアと隠蔽領域にアクセスする第二ファームウェアは、保留隠蔽領域に保存される。その後、実行プログラムは、外部装置により、セキュアリムーバブルメディアに保存される。その後、コントローラーは、第一ファームウェアを用いて、セキュアリムーバブルメディアからメディア識別子を回収する。第一プログラム識別子は実行プログラムに対応し、セキュアリムーバブルメディアが、ファームウェアにより与えられるメディア識別子に従って、セキュリティプログラムにより生成される。コントローラーは、第二ファームウェアを用いて、第一プログラム識別子を隠蔽領域に書き込む。

【００１１】

本発明は、セキュアリムーバブルメディアも提供する。一実施例では、セキュアリムーバブルメディアは、デジタル著作権管理 (DRM) エージェントを含むクライアントエンド装置に装着され、不揮発性メモリとコントローラーを含む。セキュアリムーバブルメディアはメディア識別子に対応し、メディア識別子は、不揮発性メモリ半導体チップ上に物理的に登録される番号で、且つ、正規の不揮発性メモリセル、又は、別のワンタイムプログラム可能メモリ、例えば、ROM (read only memory)に保存されず、セキュアリムーバブルメディアは、公開領域、隠蔽領域、及び、保留隠蔽領域を有して、データを保存し、セキュアリムーバブルメディア(SRM) エージェントは、公開領域に保存され、メディア識別子を回収する第一ファームウェアと隠蔽領域にアクセスする第二ファームウェアは、保留隠蔽領域に保存される。コントローラーは、クライアントエンド装置のDRMエージェントから、権利オブジェクトとセキュアデータを受信する。その後、SRM エージェントは、第一

ファームウェアを用いて、セキュアリムーバブルメディアから、メディア識別子を回収し、ファームウェアにより与えられたメディア識別子に従って、暗号化キーを生成し、暗号キーに従って、権利オブジェクトとセキュアデータを暗号化し、暗号化権利オブジェクトと暗号化セキュアデータを得て、且つ、第二ファームウェアを用いて、暗号化権利オブジェクトと暗号化セキュアデータを、隠蔽領域に書き込む。

【００１２】

本発明は、セキュアリムーバブルメディアの管理方法を提供する。一実施例では、セキュアリムーバブルメディアは、デジタル著作権管理 (DRM) エージェントを含むクライアントエンド装置に装着される。セキュアリムーバブルメディアは、不揮発性メモリとコントローラーを含む。セキュアリムーバブルメディアはメディア識別子に対応し、メディア識別子は、不揮発性メモリ半導体チップに物理的に登録される番号で、且つ、正規の不揮発性メモリセル、又は、別のワンタイムプログラム可能メモリ、例えば、ROM(read only memory)に保存されず、且つ、セキュアリムーバブルメディアは、公開領域、隠蔽領域、及び、保留隠蔽領域に分けられ、データを保存する。まず、セキュアリムーバブルメディア(SRM) エージェントは、セキュアリムーバブルメディアの公開領域に保存される。その後、メディア識別子を回収する第一ファームウェアと隠蔽領域にアクセスする第二ファームウェアが保留隠蔽領域に保存される。その後、権利オブジェクトとセキュアデータは、クライアントエンド装置のDRMエージェントから、セキュアリムーバブルメディアに伝送される。その後、SRM エージェントが実行されて、第一ファームウェアを用い、セキュアリムーバブルメディアから、メディア識別子を回収し、ファームウェアにより与えられたメディア識別子に従って、暗号化キーを生成し、暗号化キーに従って、権利オブジェクトとセキュアデータを暗号化し、暗号化権利オブジェクトと暗号化セキュアデータを得て、且つ、第二ファームウェアを用いて、暗号化権利オブジェクトと暗号化セキュアデータを、隠蔽領域に書き込む。

【発明の効果】

【００１３】

本発明により、OMADRM 2.0/2.1 スタンダードに従って、セキュアリムーバブルメディアに保存される権利オブジェクトを管理する方法が提供される。

【図面の簡単な説明】

【００１４】

【図１】本発明によるセキュアデータを保存できるセキュアリムーバブルメディアを示す図である。

【図２】本発明によるセキュリティプログラムを示す図である。

【図３Ａ】本発明によるセキュアデータをセキュアリムーバブルメディアに書き込む方法のフローチャートである。

【図３Ｂ】本発明によるセキュアリムーバブルメディアからセキュアデータを読み取る方法のフローチャートである。

【図４Ａ】本発明による実行プログラムをセキュアリムーバブルメディアに書き込む方法のフローチャートである。

【図４Ｂ】本発明による実行プログラムを実行する方法のフローチャートである。

【図５】本発明によるデジタル著作権管理 (DRM) システムを示す図である。

【図６】本発明によるDRM システムのセキュアリムーバブルメディアを示す図である。

【図７】本発明によるSRM エージェントを示す図である。

【図８Ａ】本発明による権利オブジェクトとセキュアデータを、セキュアリムーバブルメディアに書き込む方法のフローチャートである。

【図８Ｂ】本発明によるセキュアリムーバブルメディアから、権利オブジェクトとセキュアデータを読み取る方法のフローチャートである。

【図９Ａ】本発明によるDRM コンテンツの地方消費の方法のフローチャートである。

【図９Ｂ】図9Aから続く本発明によるDRM コンテンツの地方消費の方法のフローチャートである。

【発明を実施するための形態】
【００１５】
図1は、本発明によるセキュアデータを保存することができるセキュアリムーバブルメディア100を示す図である。一実施例では、セキュアリムーバブルメディア100は、コントローラー102と不揮発性メモリ104を含む。セキュアリムーバブルメディア100は、セキュアデジタル(SD)メモリカード、マルチメディアカード (MMC)、又は、USB ディスクである。不揮発性メモリ104 は、対応するメディア識別子UIDを有し、これにより、セキュアリムーバブルメディア100は、ファームウェア132により与えられるメディア識別子 UID に従って識別される。メディア識別子 UIDは、不揮発性メモリ104の半導体チップに物理的に登録される番号で、正規の不揮発性メモリセル、又は、別のワンタイムプログラム可能メモリ、例えば、ROM(read only memory)に保存されない。一実施例では、メディア識別子 UID は、不揮発性メモリ104のチップに物理的にマークされるチップシリアルナンバーである。メディア識別子UID は不揮発性メモリ104の正規のメモリセルに保存されないので、メディア識別子 UID は、ビット対ビット（bit-to-bit）ミラーイメージングプロセスにより複製されない。
【００１６】
一実施例では、不揮発性メモリ104の格納スペースは、公開領域（public area）110、隠蔽領域（hidden area）120、及び、保留隠蔽領域（reserved hidden area）130に分割される。公開領域110の格納スペースは、要求に応じて、エンドユーザーによりアクセスされる。隠蔽領域120の格納スペースと保留隠蔽領域130は、エンドユーザーによりアクセスできない。論理・物理アドレスの変換テーブル140は、不揮発性メモリ104に保存される。ファームウェア132と134 は、不揮発性メモリ104の保留隠蔽領域130 に保存される。ファームウェア132が用いられて、不揮発性メモリ104から、メディア識別子UIDを読み取る。一実施例では、ファームウェア132 は、一対一マッピングアルゴリズムを含む。ファームウェア132が、不揮発性メモリ104から、オリジナルのメディア識別子を読み取った後、ファームウェア132は、一対一マッピングアルゴリズムを用いて、オリジナルのメディア識別子から、新しいメディア識別子UIDを導き出す。これにより、ファームウェア132により出力されるメディア識別子 UIDは、安全目的のため、不揮発性メモリ104の半導体チップに登録されるオリジナルのメディア識別子と異なる。この一対一マッピングアルゴリズムは、特別な防護措置を提供することができる。メモリチップ製造業者が、オリジナルのメディア識別子を漏洩しても、暗号化キーと復号キーの生成に用いられるメディア識別子UIDは未許可の装置に知られない。ファームウェア134 が用いられて、隠蔽領域120 からデータを読み取る、又は、隠蔽領域120にデータを書き込む。セキュリティプログラム112とファームウェアライブラリ114は、不揮発性メモリ104の公開領域110に保存される。セキュリティプログラム112が用いられて、セキュアデータを不揮発性メモリ104の隠蔽領域120に保存し、隠蔽領域120からセキュアデータを回収する。セキュリティプログラム112の機能は、更に、図2、3A、及び、3Bで示される。ファームウェアライブラリ114が用いられて、ファームウェア132と134を起動、且つ、呼び出す。一実施例では、ファームウェアライブラリ114は、セキュリティプログラム112の一部である。
【００１７】
図2は、本発明によるセキュリティプログラムを示す図である。セキュアリムーバブルメディア100が、外部装置からセキュアデータを受信する時、セキュアプログラムは、セキュアデータを不揮発性メモリ104の隠蔽領域120に保存する。一実施例では、セキュリティプログラム200は、ファームウェアライブラリ202、鍵導出機能204、暗号化/復号機能 206、及び、認証機能208を含む。ファームウェアライブラリ202が用いられて、ファームウェア132と134を起動し、メディア識別子UIDを読み取るか、又は、隠蔽領域120にアクセスする。メディア識別子UIDがファームウェア132により与えられた後、鍵導出機能 204は、ファームウェア132により与えられるメディア識別子UIDに従って、暗号化キー、又は、復号キーを生成する。キー生成機能204が一対一機能なので、異なる暗号化キーは、異なるセキュアリムーバブルメディアの異なる不揮発メモリに対応し、異なる復号キーも、異な

るセキュアリムーバブルメディアの異なる不揮発メモリに対応する。暗号化/復号機能206が用いられて、暗号化キーに従って、セキュアデータを暗号化する、又は、復号キーに従って、暗号化セキュアデータを復号する。認証機能208が用いられて、実行プログラム116が、認証されたセキュアリムーバブルメディア 100で実行されるか判断する。

【００１８】

図3Aは、本発明によるセキュアデータをセキュアリムーバブルメディア100に書き込む方法300のフローチャートである。セキュアリムーバブルメディア100が、外部装置から、安全に保存する必要があるセキュアデータを受信する時 (ステップ302)、セキュリティプログラム112は、ファームウェアライブラリ114を用いて、ファームウェア132を起動し、不揮発性メモリ104から、メディア識別子UID を回収する (ステップ304)。その後、セキュリティプログラム112は、鍵導出機能204 を用いて、ファームウェア132により与えられるメディア識別子 UID に従って、暗号化キーを生成する (ステップ306)。その後、セキュリティプログラム112は、暗号化/復号機能206を用いて、暗号化キーに従って、セキュアデータを暗号化し、暗号化セキュアデータを得る(ステップ308)。その後、セキュリティプログラム112は、ファームウェアライブラリ114を用いて、ファームウェア134を起動し、暗号化セキュアデータ122 を隠蔽領域120に書き込む(ステップ310)。暗号化セキュアデータ122は隠蔽領域120に保存されるので、エンドユーザーは、直接、暗号化セキュアデータ122にアクセスすることができない。暗号化セキュアデータ122がうまく未承認装置に複製されても、未承認装置は、オリジナルの不揮発性メモリ104のメディア識別子UIDを含まないので、未承認装置は、正しい復号キーを生成して、暗号化セキュアデータを復号することができない。

【００１９】

図3Bは、本発明によるセキュアリムーバブルメディア100から、セキュアデータを読み取る方法350のフローチャートである。まず、セキュアデータが読み取られる時、セキュリティプログラム112は、ファームウェアライブラリ114を用いて、ファームウェア134を呼び、不揮発性メモリ104の隠蔽領域120から、暗号化セキュアデータ122を読み取る(ステップ352)。その後、セキュリティプログラム112は、ファームウェアライブラリ114を用いて、ファームウェア132を呼び、不揮発性メモリ104から、メディア識別子 UIDを回収する(ステップ354)。その後、セキュリティプログラム112は、鍵導出機能204を用いて、ファームウェア132により与えられるメディア識別子UIDに従って、復号キーを生成する(ステップ356)。その後、セキュリティプログラム 112は、暗号化/復号機能を用いて、復号キーに従って、暗号化セキュアデータを復号し、セキュアデータを得る(ステップ358)。その後、セキュリティプログラム 112 は、通信プロトコルに従って、セキュアデータを用いて、又は、セキュアデータを外部装置に伝送する(ステップ360)。

【００２０】

実行プログラムも、安全な保護のもとで保存される必要がある。しかし、実行プログラムは暗号化形式で保存できない。プロセッサは、暗号化実行プログラムを直接実行することができない。実行プログラムが未承認装置で実行されるのを防止するため、実行プログラムが実行される前、セキュリティプログラムは、実行プログラムを保存する装置が未承認装置かどうか判断する必要がある。図4Aは、本発明による実行プログラム116をセキュアリムーバブルメディア 100に書き込む方法400のフローチャートである。まず、実行プログラム116が不揮発性メモリ104の公開領域110に書き込まれる。その後、実行プログラム 116が、動的、又は、静的に、セキュリティプログラム 112にリンクされ(ステップ 402)、セキュリティプログラム112は、ファームウェアライブラリ114を用いて、ファームウェア 132を呼び、不揮発性メモリ 104から、メディア識別子UID を回収する(ステップ 404)。その後、セキュリティプログラム112は、認証機能 208を用いて、ファームウェア132により与えられるメディア識別子UIDに従って、プログラム識別子 UID’を生成し(ステップ 406)、プログラム識別子 UID’は、実行プログラム116 と不揮発性メモリ104に対応する。言い換えると、異なるセキュアリムーバブルメディアの異なる実行プログラム、又は、異なる不揮発メモリは、異なるプログラム識別子に対応する。その後、セキュリティプ

ログラム112は、ファームウェアライブラリ114を用いて、ファームウェア134を呼び、プログラム識別子 UID’を不揮発性メモリ104の隠蔽領域 120に書き込む (ステップ 408)。

【００２１】

図4Bは、本発明による実行プログラム116を実行する方法450のフローチャートである。実行プログラム116は、まず、ファームウェアライブラリ114を用いて、ファームウェア 132を呼び、不揮発性メモリ104から、メディア識別子 UIDを回収する(ステップ 452)。その後、実行プログラム116 は、セキュリティプログラム112の認証機能208を用いて、ファームウェア132により与えられるメディア識別子UIDとプログラム識別子UID’を比較する(ステップ454、456)。一実施例では、実行プログラム116は、認証機能208を用いて、ファームウェア132により与えられるメディア識別子UIDに従って、第二プログラム識別子UID”を生成し、ファームウェアライブラリ114 を用いて、ファームウェア134を呼び、隠蔽領域 120から、プログラム識別子UID’を読み取り、認証機能 208を用いて、隠蔽領域 120に保存されるプログラム識別子 UID’とファームウェア 132により与えられるメディア識別子UIDに従って生成されるプログラム識別子 UID”を比較する。

【００２２】

その後、認証機能 208は、プログラム識別子 UID”がプログラム識別子 UID’と同一であるか判断する。セキュアリムーバブルメディア100が、実行プログラム116を有する最初に保存された認証セキュアリムーバブルメディアである場合、不揮発性メモリ 104のメディア識別子 UID に従って生成されるプログラム識別子UID” は、隠蔽領域120に保存されるプログラム識別子 UID’と同一であると見なされ、実行プログラム116 の実行(ステップ 458)が続行される。セキュアリムーバブルメディア100が、最初に実行プログラム116を保存する認証セキュアリムーバブルメディアでない場合、未許可のセキュアリムーバブルメディア100のファームウェア132により与えられるメディア識別子UID に従って生成されるプログラム識別子 UID”は、隠蔽領域120に保存されるプログラム識別子 UID’と異なり、実行プログラム116の実行 (ステップ460) が終了する。よって、実行プログラム116 が未承認装置の不揮発性メモリに複製されても、実行プログラム116 は、未承認装置で実行されない。

【００２３】

図5は、本発明によるデジタル著作権管理 (DRM) システム 500を示す図である。一実施例では、DRMシステム500 は、DRMサーバ 502、クライアントエンド装置504、及び、セキュアリムーバブルメディア506を含む。DRM サーバ 502は、権利発行 508 とパッケージャー510を含む。クライアントエンド装置 504は、ネットワーク接続により、DRM サーバ 502に接続される。例えば、クライアントエンド装置 504は、PCや携帯電話である。一実施例では、クライアントエンド装置504は、DRMエージェント512とコンテンツビューアー514を含む。クライアントエンド装置504が、DRM コンテンツを再生、又は、使用したい時、クライアントエンド装置504 のDRM エージェント512は、要求をDRMサーバ 504に伝送し、その後、DRM サーバ502のパッケージャー510 が、DRM コンテンツ518をクライアントエンド装置504に伝送し、DRM サーバ502の権利発行508が、権利オブジェクト516とセキュアデータをクライアントエンド装置 504に伝送する。一実施例では、セキュアデータは、公開キー、秘密鍵、又は、認可証である。その後、クライアントエンド装置504のコンテンツビューアー514 は、権利オブジェクト516に従って、DRM コンテンツ518を再生、又は、使用することができる。

【００２４】

セキュアリムーバブルメディア506は、クライアントエンド装置に接続される。例えば、セキュアリムーバブルメディア506は、セキュアデジタル (SD)メモリカード、マルチメディアカード (MMC)、又は、USB ディスクである。一実施例では、セキュアリムーバブルメディアは、USB接続により、クライアントエンド装置に接続され、セキュアリムーバブルメディア(SRM) エージェント522を含む。クライアントエンド装置504は、DRM コンテンツ518をセキュアリムーバブルメディア 506に書き込み、DRM コンテンツ518’で示される。クライアントエンド装置 504は、クライアントエンド装置 504とセキュアリムーバブル

メディア506間の権利オブジェクト516とセキュアデータも移動させる。一実施例では、セキュアリムーバブルメディア506は、DRM エージェント 512’とコンテンツビューアー514’も含む。権利オブジェクト516’がセキュアリムーバブルメディア506に移動する時、セキュアリムーバブルメディア506は、権利オブジェクト516’に従って、DRMコンテンツ 518’を直接再生、又は、使用することができる。

【００２５】

権利オブジェクト516が、クライアントエンド装置504からセキュアリムーバブルメディア506に移動する時、SRMエージェント522は、権利オブジェクト516とセキュアデータを暗号化し、暗号化権利オブジェクト516’と暗号化セキュアデータを得て、暗号化権利オブジェクト516’と暗号化セキュアデータを、セキュアリムーバブルメディア506の隠蔽領域に書き込む。セキュアリムーバブルメディア506に保存される暗号化権利オブジェクト516’が隠蔽領域に保存されるので、ユーザーは、セキュアリムーバブルメディア506から、直接、暗号化権利オブジェクト516’を複製することができない。この他、セキュアリムーバブルメディア506に保存される権利オブジェクト516’が暗号化されるので、ユーザーは、直接、セキュアリムーバブルメディア506から複製される暗号化権利オブジェクト516’を使用することはできない。これにより、DRMシステム 500の権利オブジェクトは、未許可のアクセスと複製が回避される。

【００２６】

図6は、本発明によるDRM システム500のセキュアリムーバブルメディア 600を示す図である。一実施例では、セキュアリムーバブルメディア600は、コントローラー602と不揮発性メモリ604を含む。セキュアリムーバブルメディア600は、セキュアデジタル (SD) メモリカード、マルチメディアカード(MMC)、又は、USB ディスクである。不揮発性メモリ604は、対応するメディア識別子 UID を有し、これにより、セキュアリムーバブルメディア600は、メディア識別子UIDに従って識別される。メディア識別子 UIDは、不揮発性メモリ604の半導体チップに物理的に登録される番号で、正規の不揮発性メモリセル、又は、別のワンタイムプログラム可能メモリ、例えば、ROM(read only memory)に保存されない。一実施例では、メディア識別子UIDは、不揮発性メモリ604のチップに物理的にマークされるチップシリアルナンバーである。メディア識別子UIDは、不揮発性メモリ604のメモリセルに保存されないので、メディア識別子UID は、ビット対ビットミラーイメージングプロセスにより、複製されない。

【００２７】

一実施例では、不揮発性メモリ 604の格納スペースは、公開領域 610、隠蔽領域620、及び、保留隠蔽領域 630に分けられる。公開領域 610の格納スペースは、必要に応じて、エンドユーザーによりアクセスされる。一実施例では、SRM エージェント612、ファームウェアライブラリ614、コンテンツビューアー616、DRMエージェント618、及び、DRM コンテンツ619は、公開領域610に保存される。隠蔽領域620と保留隠蔽領域630の格納スペースは、エンドユーザーによりアクセスできない。論理・物理アドレスの変換テーブル640は、不揮発性メモリ604に保存される。ファームウェア632と634は、不揮発性メモリ604の保留隠蔽領域630に保存される。ファームウェア632が用いられて、不揮発性メモリ604から、メディア識別子UIDを読み取る。一実施例では、ファームウェア632は一対一マッピングアルゴリズムを含む。ファームウェア632が、不揮発性メモリ604から、オリジナルのメディア識別子を読み取った後、安全目的のため、ファームウェア632は、一対一マッピングアルゴリズムを用いて、オリジナルのメディア識別子から、新しいメディア識別子UIDを導き出す。ファームウェア 634が用いられて、隠蔽領域 620からデータを読み取る、又は、隠蔽領域 620にデータを書き込む。権利オブジェクト622とセキュアデータ629が、不揮発性メモリ604の隠蔽領域620に保存される前、SRMエージェント612が用いられて、権利オブジェクト 622とセキュアデータ 629を暗号化する。SRM エージェント 612の機能は、更に、図 7、8A、8B、及び、9で示される。ファームウェアライブラリ614が用いられて、ファームウェア632と634を起動、呼び出しする。一実施例では、ファームウェアライブラリ 614 はSRM エージェント 612の一部である。

【００２８】
図7は、本発明によるSRM エージェント 700 を示す図である。クライアントエンド装置から、セキュアリムーバブルメディア600が権利オブジェクトとセキュアデータを受信する時、SRM エージェント700は、権利オブジェクトとセキュアデータを不揮発性メモリ 604の隠蔽領域620に保存する。一実施例では、SRMエージェント700は、ファームウェアライブラリ702、鍵導出機能704、暗号化/復号機能706、認証機能708、DRM 要求機能710を含む。ファームウェアライブラリ702が用いられて、ファームウェア632と634を起動し、メディア識別子 UID を読み取る、又は、隠蔽領域 620にアクセスする。ファームウェア 632により与えられるメディア識別子 UID が得られた後、ファームウェア632により与えられるメディア識別子UID に従って、鍵導出機能 704が、暗号化キー、又は、復号キーを生成する。キー生成機能 704が一対一機能なので、よって、異なる暗号化キーは、異なるセキュアリムーバブルメディアの異なる不揮発メモリに対応し、異なる復号キーも、異なるセキュアリムーバブルメディアの異なる不揮発メモリに対応する。暗号化/復号機能706が用いられて、暗号化キーに従って、権利オブジェクトとセキュアデータを暗号化する、又は、復号キーに従って、暗号化セキュアデータを復号する。

【００２９】
図8Aは、本発明による権利オブジェクトとセキュアデータをセキュアリムーバブルメディア600に書き込む方法800のフローチャートである。クライアントエンド装置のDRMエージェント は、まず、権利オブジェクトとセキュアデータを、SRM エージェント612に伝送し(ステップ 802)、SRM エージェント 612は、第一暗号化権利オブジェクト、第一暗号化セキュアデータ、及び、セクション暗号化キーを受信する(ステップ 804)。その後、SRM エージェントは、セクション復号キーを用いて、第一暗号化権利オブジェクトと第一暗号化セキュアデータを復号し、権利オブジェクトとセキュアデータを得る(ステップ 806)。その後、SRM エージェント612 は、ファームウェアライブラリ614 を用いて、ファームウェア632を起動し、不揮発性メモリ604から、メディア識別子UID を回収する (ステップ 808)。その後、SRM エージェント 612は、鍵導出機能 704 を用いて、ファームウェア632により与えられるメディア識別子UID に従って、暗号化キーを生成する(ステップ 810)。その後、SRM エージェント612は、暗号化/復号機能706 を用いて、暗号化キーに従って、権利オブジェクトとセキュアデータを暗号化し、第二暗号化権利オブジェクトと第二暗号化セキュアデータを得る(ステップ 812)。その後、SRM エージェント612 は、ファームウェアライブラリ614 を用いて、ファームウェア634を起動し、第二暗号化権利オブジェクト622と第二暗号化セキュアデータ629を、隠蔽領域620に書き込む(ステップ814)。第二暗号化権利オブジェクト 622 と第二暗号化セキュアデータ629 は隠蔽領域620に保存されるので、エンドユーザーは、直接、第二暗号化権利オブジェクト622と第二暗号化セキュアデータ 629にアクセスすることができない。第二暗号化権利オブジェクト622と第二暗号化セキュアデータ 629がうまく未承認装置に複製されても、未承認装置は、オリジナルの不揮発性メモリ604のメディア識別子 UIDを含まないので、未承認装置は、正しい復号キーを生成して、第二暗号化権利オブジェクト 622と第二暗号化セキュアデータ 629を復号することができない。

【００３０】
図8Bは、本発明によるセキュアリムーバブルメディア 600から権利オブジェクトとセキュアデータを読み取る方法850のフローチャートである。SRMエージェント 612は、ファームウェアライブラリ 614を用いて、ファームウェア 634を呼び出し、不揮発性メモリ604の隠蔽領域 620から、第一暗号化権利オブジェクト622と第一暗号化セキュアデータ629を読み取る(ステップ852)。その後、SRM エージェント612は、ファームウェアライブラリ 614 を用いて、ファームウェア 632を呼び出し、不揮発性メモリ 604からメディア識別子UID を回収する (ステップ 854)。その後、SRM エージェント 612 は、鍵導出機能 704を用いて、ファームウェア632により与えられたメディア識別子UID に従って、復号キーを生成する (ステップ 856)。その後、SRM エージェント612 は、暗号化/復号機能 706を用いて、復号キーに従って、暗号化権利オブジェクトと暗号化セキュアデータを暗号化し、

権利オブジェクトとセキュアデータを得る(ステップ 858)。その後、権利オブジェクトとセキュアデータに従って、SRM エージェント662は、第二権利オブジェクトと第二セキュアデータを暗号化し、第二権利オブジェクト、第二セキュアデータ、及び、セクション復号キーを、クライアントエンド装置のDRMサーバに伝送する (ステップ 860)。最後に、DRM サーバは、第二権利オブジェクト、第二セキュアデータ、及び、セクション復号キーを受信する(ステップ862)。

【００３１】

図9は、本発明によるDRM コンテンツのローカル消費の方法900のフローチャートである。まず、SRMエージェント 612は、ファームウェアライブラリ614を用いて、隠蔽領域 620から、第一暗号化権利オブジェクト622と第一暗号化セキュアデータ 629を読み取る(ステップ901)。その後、SRM エージェント 612は、ファームウェアライブラリ 614を用いて、セキュアリムーバブルメディア 600に対応するメディア識別子 UIDを回収する(ステップ902)。その後、SRM エージェント612は、ファームウェア632により与えられた鍵導出機能704とメディア識別子 UID を用いて、復号キーを生成する(ステップ 903)。その後、SRM エージェント612は、復号キーと暗号化/復号機能706を用いて、第一暗号化権利オブジェクトと第一暗号化セキュアデータを復号し、権利オブジェクトとセキュアデータを得る(ステップ 904)。その後、SRM エージェント 612は、権利オブジェクト、セキュアデータ、及び、セクション復号キーを、クライアントエンド装置504のDRMエージェント512に伝送する (ステップ 905)。その後、DRM エージェント512は、第二暗号化権利オブジェクト、第二暗号化セキュアデータ、及び、セクション復号キーを受信する(ステップ 906)。その後、DRMエージェント512は、セクション復号キーを用いて、第二暗号化権利オブジェクトと第二暗号化セキュアデータを復号して、権利オブジェクトとセキュアデータを得て、それらを使用して、DRMコンテンツを取得する(ステップ907)。その後、DRMエージェント512は、暗号化権利オブジェクト情報とセクション復号キーを、SRM エージェント 612 に伝送する(ステップ 908)。その後、SRM エージェント612は、セクション復号キーを用いて、暗号化権利オブジェクト情報を復号し、権利オブジェクト情報を得る(ステップ 909)。

【００３２】

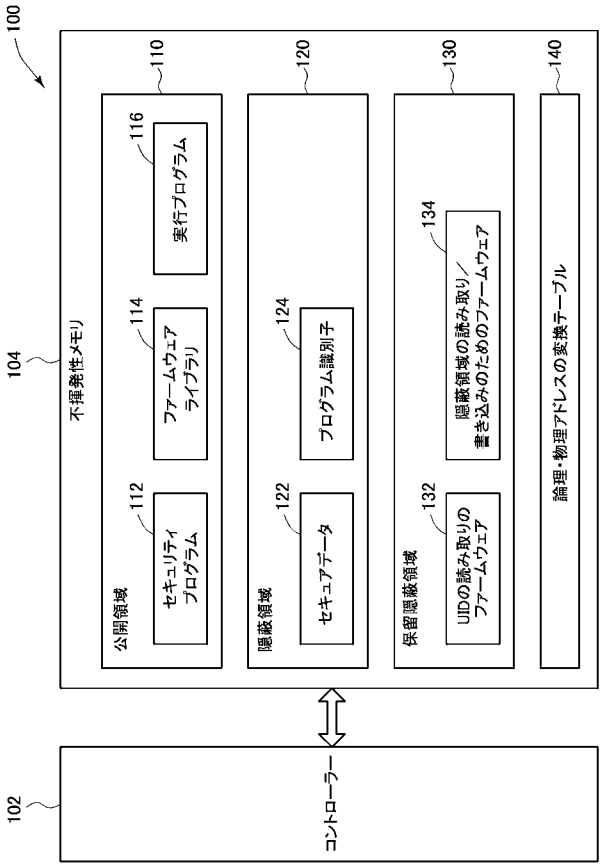
その後、SRM エージェント 612は、ファームウェアライブラリ614を用いて、隠蔽領域620 から、第一暗号化権利オブジェクト 622と第一セキュアデータ 629を読み取る(ステップ 910)。その後、SRM エージェント 612 は、ファームウェアライブラリ614 を用いて、セキュアリムーバブルメディア600に対応するメディア識別子 UIDを回収する (ステップ911)。その後、SRM エージェント 612は、鍵導出機能704とファームウェア632により与えられるメディア識別子UID を用いて、復号キーを生成する (ステップ 912)。その後、SRM エージェント612は、復号キーと暗号化/復号機能706を用いて、第一暗号化権利オブジェクトと第一セキュアデータを復号し、権利オブジェクトとセキュアデータを得る(ステップ 913)。その後、SRMエージェント 612は、権利オブジェクト情報を用いて、権利オブジェクトを修正し、修正された権利オブジェクトを得る(ステップ914)。その後、SRM エージェント 612はファームウェアライブラリ 614 を用いて、ファームウェア632により与えられるメディア識別子 UIDを回収する(ステップ 915)。その後、SRM エージェント612は、鍵導出機能704とファームウェア632により与えられるメディア識別子 UID を用いて、暗号化キーを生成する(ステップ 916)。SRM エージェント 612は、暗号化キーと暗号化/復号機能 706を用いて、修正された権利オブジェクトとセキュアデータに従って、第三暗号化権利オブジェクトと第三セキュアデータを暗号化する(ステップ 917)。その後、SRM エージェント612 は、ファームウェアライブラリ614を用いて、第三暗号化権利オブジェクトと第三セキュアデータを、隠蔽領域620 に書き込む(ステップ 918)。

【００３３】

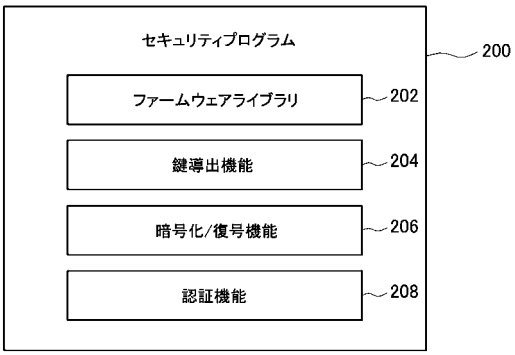
本発明では好ましい実施例を前述の通り開示したが、これらは決して本発明を限定するものではなく、当該技術を熟知する者なら誰でも、本発明の精神と領域を脱しない範囲内で各種の変更や潤色を加えることができ、従って本発明の保護範囲は、特許請求の範囲で

指定した内容を基準とする。
【符号の説明】
【００３４】
100、506～セキュアリムーバブルメディア；
102、602～コントローラー；
104～不揮発性メモリ；
110、610～公開領域；
112、200～セキュリティプログラム；
114、202、614、702～ファームウェアライブラリ；
116～実行プログラム；
120、620～隠蔽領域；
122、629～セキュアデータ；
124～プログラム識別子；
130、630～保留隠蔽領域；
132、134、632、634～ファームウェア；
140、640～論理対物理のアドレス変換テーブル；
204、704～鍵導出機能；
206、706～暗号化/復号機能；
208、708～認証機能；
300、350、400、450、800、850、900～フローチャート；
500～デジタル著作権管理（DRM）システム；
502～DRMサーバ；
508～権利発行；
510～パッケージャー；
512、512’、618～ DRMエージェント；
514、514’、616～コンテンツビューアー；
516、516’～ 権利オブジェクト /セキュアデータ；
622～権利オブジェクト；
518、518’、619～DRMコンテンツ；
522、612、700～SRM エージェント；
710～DRM 要求機能。

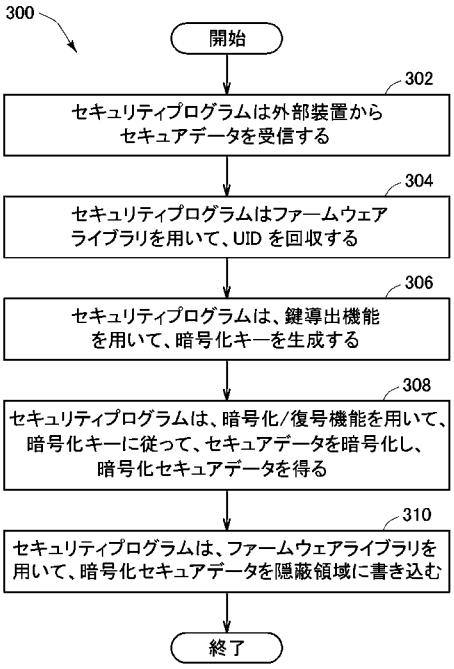
【図１】


100
104
不揮発性メモリ
110
公開領域
112
セキュリティプログラム
116
実行プログラム
114
ファームウェアライブラリ
120
隠蔽領域
122
セキュアデータ
124
プログラム識別子
130
保留隠蔽領域
132
UIDの読み取りのファームウェア
134
隠蔽領域の読み取り／書き込みのためのファームウェア
140
論理・物理アドレスの変換テーブル
102
コントローラー

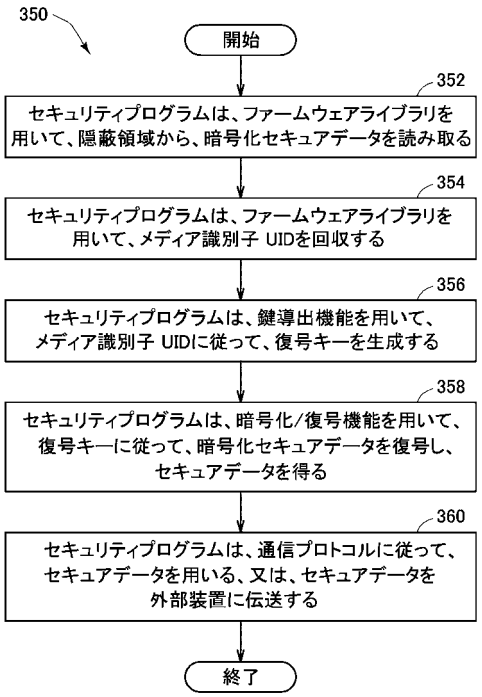
【図２】


セキュリティプログラム
200
ファームウェアライブラリ
202
鍵導出機能
204
暗号化/復号機能
206
認証機能
208

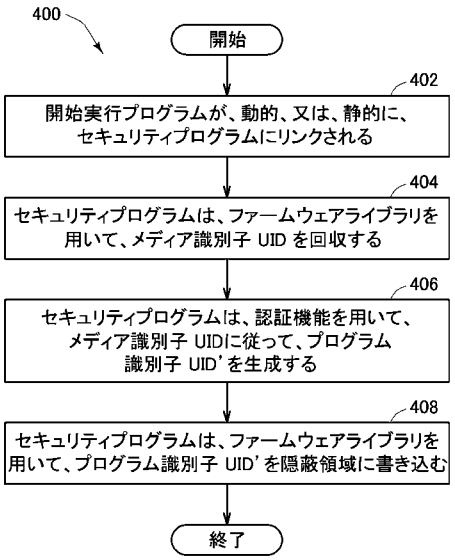
【図３Ａ】


300
開始
302
セキュリティプログラムは外部装置から
セキュアデータを受信する
304
セキュリティプログラムはファームウェア
ライブラリを用いて、UID を回収する
306
セキュリティプログラムは、鍵導出機能
を用いて、暗号化キーを生成する
308
セキュリティプログラムは、暗号化/復号機能を用いて、
暗号化キーに従って、セキュアデータを暗号化し、
暗号化セキュアデータを得る
310
セキュリティプログラムは、ファームウェアライブラリを
用いて、暗号化セキュアデータを隠蔽領域に書き込む
終了

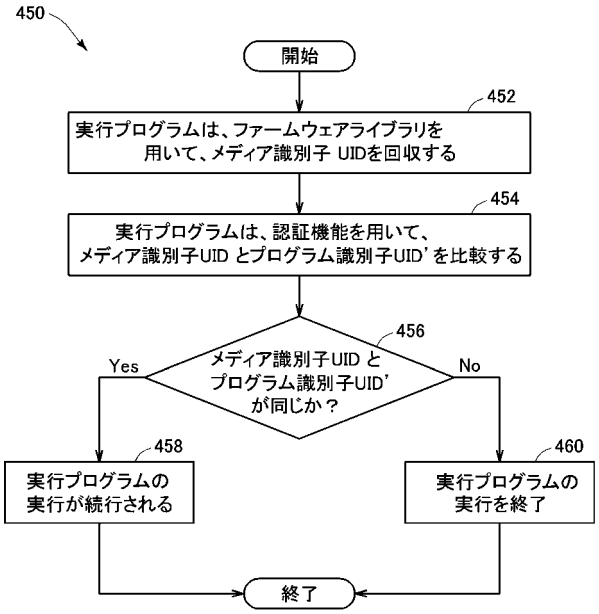
【図３Ｂ】


350
開始
352
セキュリティプログラムは、ファームウェアライブラリを
用いて、隠蔽領域から、暗号化セキュアデータを読み取る
354
セキュリティプログラムは、ファームウェアライブラリを
用いて、メディア識別子 UIDを回収する
356
セキュリティプログラムは、鍵導出機能を用いて、
メディア識別子 UIDに従って、復号キーを生成する
358
セキュリティプログラムは、暗号化/復号機能を用いて、
復号キーに従って、暗号化セキュアデータを復号し、
セキュアデータを得る
360
セキュリティプログラムは、通信プロトコルに従って、
セキュアデータを用いる、又は、セキュアデータを
外部装置に伝送する
終了

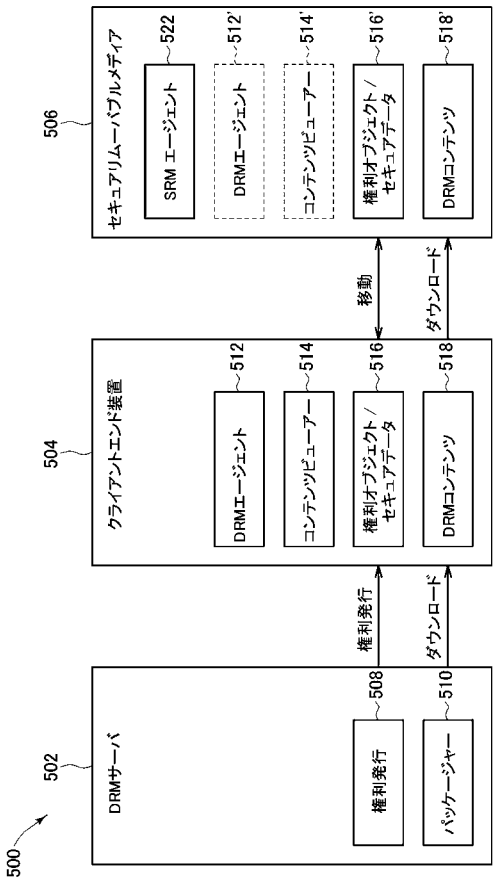
【図４Ａ】


400
開始
402
開始実行プログラムが、動的、又は、静的に、
セキュリティプログラムにリンクされる
404
セキュリティプログラムは、ファームウェアライブラリを
用いて、メディア識別子 UID を回収する
406
セキュリティプログラムは、認証機能を用いて、
メディア識別子 UIDに従って、プログラム
識別子 UID'を生成する
408
セキュリティプログラムは、ファームウェアライブラリを
用いて、プログラム識別子 UID'を隠蔽領域に書き込む
終了

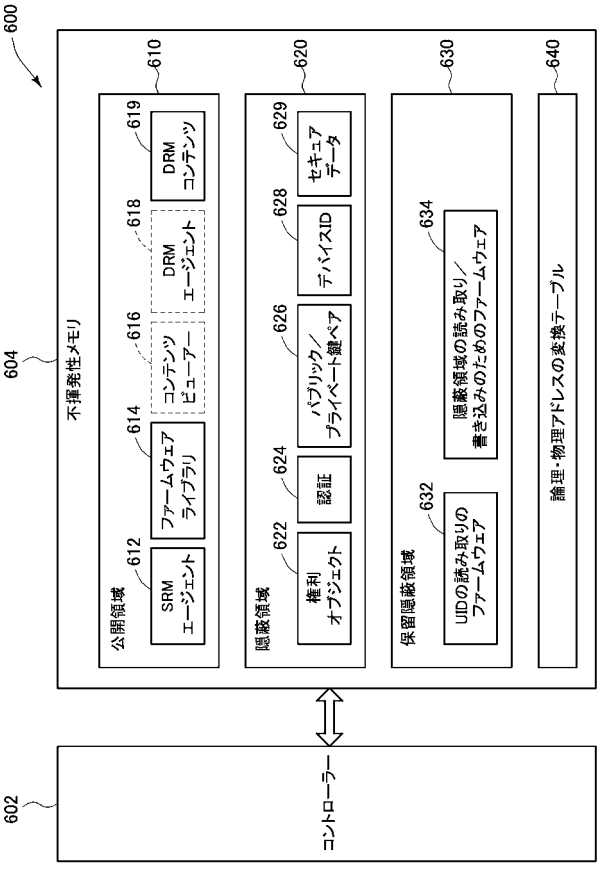
【図４Ｂ】


450
開始
452
実行プログラムは、ファームウェアライブラリを
用いて、メディア識別子 UIDを回収する
454
実行プログラムは、認証機能を用いて、
メディア識別子UID とプログラム識別子UID'を比較する
456
メディア識別子UID と
プログラム識別子UID'
が同じか？
Yes
No
458
実行プログラムの
実行が続行される
460
実行プログラムの
実行を終了
終了

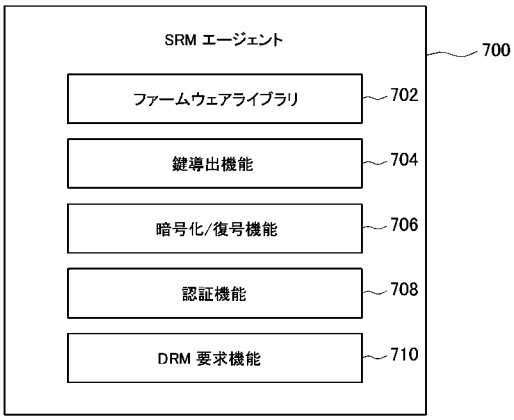
【図５】


500
DRMサーバ
502
権利発行
508
パッケージャー
510
権利発行
ダウンロード
クライアントエンド装置
504
DRMエージェント
512
コンテンツビューアー
514
権利オブジェクト／
セキュアデータ
516
DRMコンテンツ
518
移動
ダウンロード
セキュアリムーバブルメディア
506
SRM エージェント
522
DRMエージェント
512'
コンテンツビューアー
514'
権利オブジェクト／
セキュアデータ
516'
DRMコンテンツ
518'

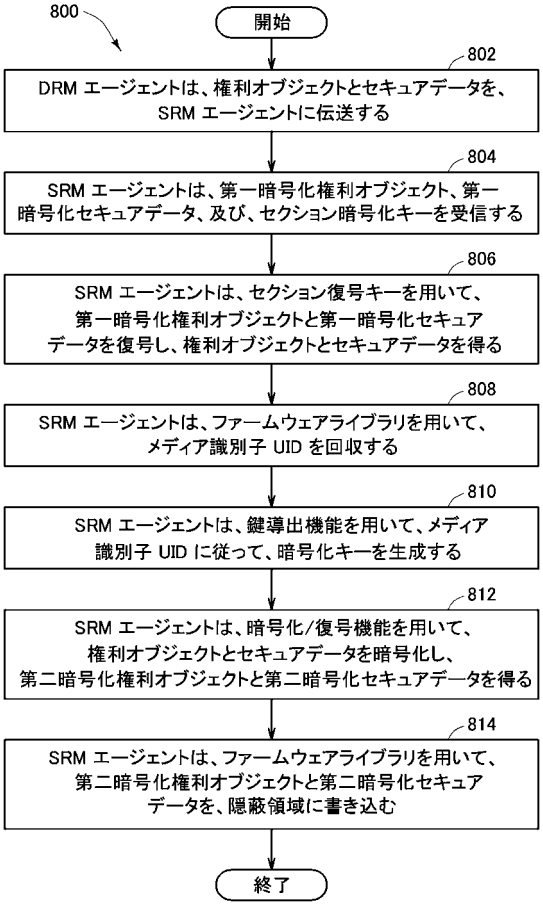
【図６】


600
不揮発性メモリ
604
公開領域
SRM
エージェント
612
ファームウェア
ライブラリ
614
コンテンツ
ビューアー
616
DRM
エージェント
618
DRM
コンテンツ
619
610
隠蔽領域
権利
オブジェクト
622
認証
624
パブリック／
プライベート鍵ペア
626
デバイスID
628
セキュア
データ
629
620
保留隠蔽領域
UIDの読み取り
ファームウェア
632
隠蔽領域の読み取り／
書き込みのためのファームウェア
634
630
論理・物理アドレスの変換テーブル
640
コントローラー
602

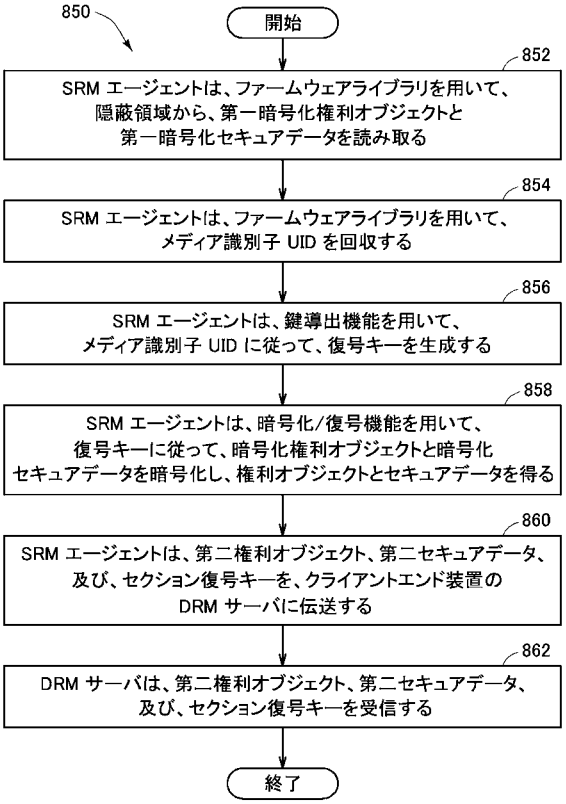
【図７】



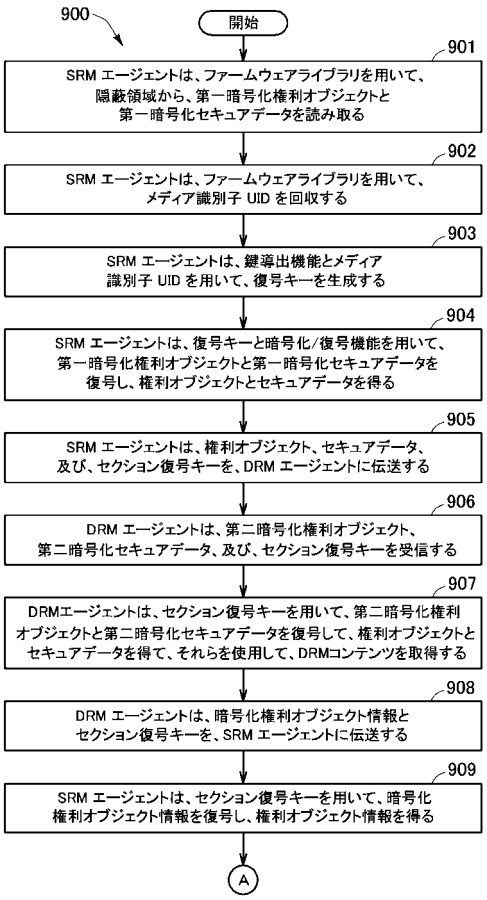
【図８Ａ】



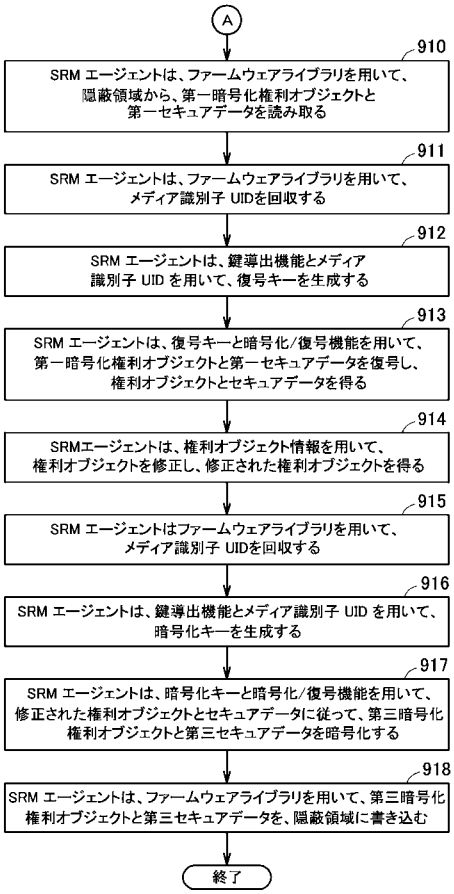
【図８Ｂ】



【図９Ａ】



【図９Ｂ】


A
910
SRM エージェントは、ファームウェアライブラリを用いて、
隠蔽領域から、第一暗号化権利オブジェクトと
第一セキュアデータを読み取る
911
SRM エージェントは、ファームウェアライブラリを用いて、
メディア識別子 UIDを回収する
912
SRM エージェントは、鍵導出機能とメディア
識別子 UID を用いて、復号キーを生成する
913
SRM エージェントは、復号キーと暗号化/復号機能を用いて、
第一暗号化権利オブジェクトと第一セキュアデータを復号し、
権利オブジェクトとセキュアデータを得る
914
SRMエージェントは、権利オブジェクト情報を用いて、
権利オブジェクトを修正し、修正された権利オブジェクトを得る
915
SRM エージェントはファームウェアライブラリを用いて、
メディア識別子 UIDを回収する
916
SRM エージェントは、鍵導出機能とメディア識別子 UID を用いて、
暗号化キーを生成する
917
SRM エージェントは、暗号化キーと暗号化/復号機能を用いて、
修正された権利オブジェクトとセキュアデータに従って、第三暗号化
権利オブジェクトと第三セキュアデータを暗号化する
918
SRM エージェントは、ファームウェアライブラリを用いて、第三暗号化
権利オブジェクトと第三セキュアデータを、隠蔽領域に書き込む
終了

フロントページの続き

(72)発明者　蘇　志勝
台湾新竹縣竹北市嘉豐二街二段８８巷２７號９樓

Ｆターム(参考) 5J104 AA16　EA26　NA27　NA36　NA42　PA14