(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5572209号
(P5572209)

(45)発行日　平成26年8月13日(2014.8.13)　(24)登録日　平成26年7月4日(2014.7.4)

(51)Int.Cl.		F I		
G06Q 50/10	(2012.01)	G06Q	50/10	140
H04L 9/08	(2006.01)	H04L	9/00	601B
G06F 21/62	(2013.01)	H04L	9/00	601E
		G06F	21/24	166A

請求項の数 18　(全 22 頁)

(21)出願番号	特願2012-505119(P2012-505119)
(86)(22)出願日	平成22年3月31日(2010.3.31)
(65)公表番号	特表2012-524309(P2012-524309A)
(43)公表日	平成24年10月11日(2012.10.11)
(86)国際出願番号	PCT/EP2010/054297
(87)国際公開番号	WO2010/118957
(87)国際公開日	平成22年10月21日(2010.10.21)
審査請求日	平成25年3月4日(2013.3.4)
(31)優先権主張番号	12/425,490
(32)優先日	平成21年4月17日(2009.4.17)
(33)優先権主張国	米国(US)

(73)特許権者　598036300
テレフオンアクチーボラゲット　エル　エム　エリクソン(パブル)
スウェーデン国　ストックホルム　エス－１６４　８３
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】電子チケット処理の方法及び装置

(57)【特許請求の範囲】

【請求項１】

ネットワーク化された既存のデジタル著作権管理システムの一部として動作するデジタル著作権管理エージェントをインストールした電子デバイスにおいて使用される電子チケット処理の方法であって、

前記デジタル著作権管理システムに従って、コンテンツ暗号化鍵で暗号化されたチケット鍵を含むチケットオブジェクトを受信するステップと、

前記著作権管理システムと互換性のある権利オブジェクトであって、前記チケットオブジェクトに対応する１つ以上の使用制限を含み、前記デジタル著作権管理エージェントに関連するデジタル著作権管理鍵で暗号化された前記コンテンツ暗号化鍵を含む前記権利オブジェクトを受信するステップと、

前記チケットオブジェクト、及び関連する前記権利オブジェクトが前記既存のデジタル著作権管理システムに従ってフォーマットされ、他のデジタル著作権管理制限されたオブジェクトである音楽ファイル及び動画ファイルと同じ方法で前記デジタル著作権管理エージェントによって扱われ、前記デジタル著作権管理エージェントが、前記チケットオブジェクトの使用制限を確認し、チケットの使用が許可されていれば、前記チケットオブジェクトを復号化するように、チケットエージェントによって要求するステップと、

前記チケットエージェントによって、前記１つ以上の使用制限に従って、前記デジタル著作権管理エージェントから前記チケット鍵を取り出すステップと、

前記チケットエージェントによって、前記チケット鍵を外部エージェントに公開する

ことなく、該チケット鍵の所有を検証するために、予め定義された検証プロトコルに従って前記外部エージェントと通信するステップと
を実行することによって、前記電子デバイスにインストールされた少なくとも１つの前記チケットエージェントを用いて前記チケットオブジェクトを引き換えるステップと
を含むことを特徴とする方法。

【請求項２】
前記チケット鍵の所有を検証するために、前記外部エージェントと通信する前記ステップは、前記外部エージェントへの前記チケット鍵の所有を検証するように、共有のシークレット又は非対称鍵対を用いるステップを含むことを特徴とする請求項１に記載の方法。

【請求項３】
前記チケットオブジェクトを受信する前記ステップは、
両方が前記コンテンツ暗号化鍵によって保護された、組込み型チケットエージェントと前記チケット鍵とを含む複合チケットオブジェクトを受信するステップを含み、
前記チケットオブジェクトを引き換える前記ステップは、
前記組込み型チケットエージェントと、前記チケット鍵とを前記デジタル著作権管理エージェントから取り出すステップと、前記予め定義された検証プロトコルに従って前記外部エージェントと通信するために前記組込み型チケットエージェントを用いるステップとを含むことを特徴とする請求項１に記載の方法。

【請求項４】
マスタチケットエージェントの制御の下で安全に前記チケット鍵を保持する一方で、前記組込み型チケットエージェントによって該チケット鍵を引き換えるのに使用するために、前記デジタル著作権管理エージェントから前記組込み型チケットエージェントと前記チケット鍵とを取り出し、該組込み型チケットエージェントをインストールするか又は開始し、該チケット鍵の参照を前記組込み型チケットエージェントに与える前記電子デバイスにインストールされた前記マスタチケットエージェントを用いるステップをさらに含むことを特徴とする請求項３に記載の方法。

【請求項５】
前記チケットオブジェクトを受信する前記ステップは、
前記デジタル著作権管理エージェントによって著作権管理されたオブジェクトとして扱うために、予め定義されたデジタル著作権管理フォーマットに従ってタグ付けされるか、又はパッケージ化されるコンテンツファイルを受信するステップを含むことを特徴とする請求項１に記載の方法。

【請求項６】
前記外部エージェントは、電子検証システムを備え、
前記チケットオブジェクトを引き換える前記ステップは、
前記電子検証システムのための検証情報を生成するステップと、
前記チケットエージェントと前記電子検証システムとの間の共有のシークレットとして前記チケット鍵に基づき、前記電子検証システムから反検証情報を検証するステップと
を含むことを特徴とする請求項１に記載の方法。

【請求項７】
前記電子デバイスと前記電子検証システムとの間のローカル通信インタフェースを介して、前記検証情報を前記電子検証システムへ送信するステップと、前記電子検証システムからの前記反検証情報を受信するステップと、をさらに含むことを特徴とする請求項６に記載の方法。

【請求項８】
前記チケットオブジェクトを引き換える前記ステップは、
前記チケットエージェントが、前記電子検証から前記チケットオブジェクトに対応するチケット識別子を受信するステップと、
前記チケットエージェントが、前記チケット識別子を前記デジタル著作権管理エージェントに渡し、応答として前記チケット鍵及び暗号化アルゴリズムを受信するステップと、

前記チケットエージェントが、前記電子検証システムのための前記検証情報を生成するために前記チケット鍵及び前記暗号化アルゴリズムを用いるステップとを含むことを特徴とする請求項６に記載の方法。

【請求項９】

前記外部エージェントは、人間の操作者を含み、

前記チケットオブジェクトを引き換える前記ステップは、

前記チケットエージェントが、前記電子デバイスのユーザインタフェースを介して、前記チケットオブジェクトに対応するチケット識別子を受信するステップと、

前記チケットエージェントが、前記チケット識別子を前記デジタル著作権管理エージェントに渡し、応答として前記チケット鍵及びチケットレンダリング情報を受信するステップと、

前記チケットエージェントが、前記レンダリング情報に従って前記電子デバイスの前記ユーザインタフェースを介して人間が検証可能な形式にチケット情報をレンダリングするステップとを含むことを特徴とする請求項１に記載の方法。

【請求項１０】

ネットワーク化された既存のデジタル著作権管理システムにおいて使用されるデジタル著作権管理エージェントをインストールした電子デバイスであって、

前記デジタル著作権管理システムに従って、コンテンツ暗号化鍵で暗号化されたチケット鍵を含むチケットオブジェクトを受信し、前記著作権管理システムと互換性のある権利オブジェクトであって、前記チケットオブジェクトに対応する１つ以上の使用制限を含み、前記デジタル著作権管理エージェントに関連するデジタル著作権管理鍵で暗号化された前記コンテンツ暗号化鍵を含む前記権利オブジェクトを受信するための１つ以上の通信インタフェースと、

前記チケットオブジェクト及び前記権利オブジェクトを格納するメモリと、

前記１つ以上の通信インタフェースと前記メモリとに関連して動作可能な１つ以上の処理回路であって、前記デジタル著作権管理エージェントを実行し、前記チケットオブジェクト、及び関連する前記権利オブジェクトが前記既存のデジタル著作権管理システムに従ってフォーマットされ、他のデジタル著作権管理制限されたオブジェクトである音楽ファイル及び動画ファイルと同じ方法で前記デジタル著作権管理エージェントによって扱われ、前記デジタル著作権管理エージェントが、前記チケットオブジェクトの使用制限を確認し、チケットの使用が許可されていれば、前記チケットオブジェクトを復号化するように要求し、前記１つ以上の使用制限に従って、前記デジタル著作権管理エージェントから前記チケット鍵を取り出し、前記チケット鍵を外部エージェントに公開することなく、該チケット鍵の所有を検証するために、予め定義された検証プロトコルに従って前記外部エージェントと通信することによって、前記チケットオブジェクトを引き換える少なくとも１つのチケットエージェントを実行する前記処理回路と

を備えることを特徴とする電子デバイス。

【請求項１１】

前記チケットエージェントは、

前記外部エージェントへの前記チケット鍵の所有を検証するように、共有のシークレット又は非対称鍵対を用いることを特徴とする請求項１０に記載の電子デバイス。

【請求項１２】

前記チケットオブジェクトは、両方が前記コンテンツ暗号化鍵によって保護された、組込み型チケットエージェントと前記チケット鍵とを含む複合チケットオブジェクトを受信し、

前記１つ以上の処理回路は、前記組込み型チケットエージェントと、前記チケット鍵とを前記デジタル著作権管理エージェントから取り出し、前記予め定義された検証プロトコルに従って前記外部エージェントと通信するために前記組込み型チケットエージェントを用いることによって前記チケットオブジェクトを引き換えることを特徴とする請求項１０に記載の電子デバイス。

【請求項１３】
前記１つ以上の処理回路は、マスタチケットエージェントを実行し、
前記マスタチケットエージェントは、
前記マスタチケットエージェントの制御の下で安全に前記チケット鍵を保持する一方で、前記組込み型チケットエージェントによって該チケット鍵を引き換えるのに使用するために、前記デジタル著作権管理エージェントから前記組込み型チケットエージェントと前記チケット鍵とを取り出し、該組込み型チケットエージェントをインストールするか又は開始し、該チケット鍵の参照を前記組込み型チケットエージェントに与えることを特徴とする請求項１２に記載の電子デバイス。
【請求項１４】
前記チケットオブジェクトは、前記デジタル著作権管理エージェントによって著作権管理されたオブジェクトとして扱うために、予め定義されたデジタル著作権管理フォーマットに従ってタグ付けされるか、又はパッケージ化されるコンテンツファイルを含むことを特徴とする請求項１０に記載の電子デバイス。
【請求項１５】
前記外部エージェントは、電子検証システムを備え、
前記チケットエージェントは、
前記電子検証システムのための検証情報を生成し、
前記チケットエージェントと前記電子検証システムとの間の共有のシークレットとして前記チケット鍵に基づき、前記電子検証システムから反検証情報を検証することによって前記チケットオブジェクトを引き換えるように構成されることを特徴とする請求項１０に記載の電子デバイス。
【請求項１６】
前記チケットエージェントは、
前記検証情報を前記電子検証システムへ送信し、前記電子検証システムからの前記反検証情報を受信するために、前記１つ以上の通信インタフェースの１つとしてローカル通信インタフェースを用いるように構成されることを特徴とする請求項１５に記載の電子デバイス。
【請求項１７】
前記チケットエージェントは、
前記電子検証から前記チケットオブジェクトに対応するチケット識別子を受信することに応じて前記チケットオブジェクトを引き換え、
前記チケット識別子を前記デジタル著作権管理エージェントに渡し、
応答として前記チケット鍵及び暗号化アルゴリズムを受信し、
前記電子検証システムのための前記検証情報を生成するために前記チケット鍵及び前記暗号化アルゴリズムを用いるように構成されることを特徴とする請求項１５に記載の電子デバイス。
【請求項１８】
前記外部エージェントは、人間の操作者を含み、
前記チケットエージェントは、
前記電子デバイスのユーザインタフェースを介して、前記チケットオブジェクトに対応するチケット識別子を受信することに応じて前記チケットオブジェクトを引き換え、
前記チケット識別子を前記デジタル著作権管理エージェントに渡し、
応答として前記チケット鍵及びチケットレンダリング情報を受信し、
前記レンダリング情報に従って前記電子デバイスの前記ユーザインタフェースを介して人間が検証可能な形式にチケット情報をレンダリングするように構成されることを特徴とする請求項１０に記載の電子デバイス。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、一般に電子チケッティングに関し、特に電子チケットの発行、格納及び引換えを簡略化するためにデジタル著作権管理（ＤＲＭ）システムを有利に使用することに関する。

【背景技術】

【０００２】

電子チケットは、ユーザの利便性を向上させ、物理チケットの製造及び配達に関連する無駄をなくす。また、スマートフォン等のハンドヘルドインテリジェント端末の使用が増加するにつれ、安全で且つ簡単に使用できる電子チケッティングシステムに対応するユーザベースが拡張し続けている。

【０００３】

電子チケッティングシステムは、電子財布及び他の安全な電子支払いシステムとある特定の類似点を共有するが、一般にこれらのシステムは、行う取引に関連してお金を入金し且つ引き落とすためのユーザの金融口座へのリンケージに依存する。電子チケットを使用する場合、電子チケットオブジェクト自体は「値」オブジェクトとして機能する。この手法により、電子チケットは、紙のチケットと同様に購入され、発行され、格納され且つ引き換えられる。紙のチケットと同様に、不正使用防止が中心的な目的であり、ユーザの利便性を維持しつつ電子チケットの不正使用を防止するために多くの研究が行われてきた。Ｄｕｔｔａ他の米国特許第７，３１５，９４４Ｂ２号明細書において、電子チケット及び他の種類の「ストアドバリューデータオブジェクト」を発行し、一時的に格納し、且つ引き換える総合システムが開示される。この特許は、特許及び同時係属出願のより大きな集合に属し、その全ては、全体的なストアドバリューデータオブジェクト発行及び引換えシステムの種々の態様に関する。関連出願には、双方ともＤｕｔｔａの米国出願第２００３／００９３６９５号公報及び米国出願第２００８／００６１１３７号公報がある。

【０００４】

また、Ｔａｋａｈａｓｈｉ他の米国特許第６，２６０，０２７Ｂ１号明細書において、電子チケット発行システム、チケット収集システム及び電子チケットを取得し且つ引き換えるように構成されたユーザ端末の例が開示される。更に、Ｓａｋａｍｕｒａの一連の公開された米国特許出願において、安全な電子チケット発行及び引換え処理で使用される安全な集積回路カードの使用法が開示される。これらの公開された出願には、米国出願２００４／００３０８９６Ａ１号明細書、米国出願２００４／００５９６８５Ａ１号明細書及び米国出願２００８／０１０９３７１Ａ１号明細書が含まれる。電子チケッティングシステムの更に有用な説明のため、興味のある読者は、Ｐａｔｅｌ、Ｂｈｒａｔ及びＣｒｏｗｃｒｏｆｔ，Ｊｏｎ、Ｔｉｃｋｅｔ Ｂａｓｅｄ Ｓｅｒｖｉｃｅ Ａｃｃｅｓｓ ｆｏｒ ｔｈｅ Ｍｏｂｉｌｅ Ｕｓｅｒ、ＭＯＢＩＣＯＭ９７ （Ｂｕｄａｐｅｓｔ Ｈｕｎｇａｒｙ、１９９７年）及びＨｕｓｅｍａｎｎ他の米国特許第６，１９２，３４９Ｂ１号明細書を参照すべきである。

【０００５】

電子チケッティングに対して既知の手法は、デジタル著作権管理（ＤＲＭ）のある特定の態様を更に含む。例えばオープンモバイルアライアンス（ＯＭＡ）は、「モバイル」環境でＤＲＭを実現するプロトコル、メッセージ及び機能のパッケージとして「ＤＲＭ ｖ２．０」を開発し且つリリースした。電子チケッティングに関するＤＲＭ概念の更なる説明のため、読者は、Ｇｕｔｈ他、Ｔｏｗａｒｄ ａ Ｃｏｎｃｅｐｔｕａｌ Ｆｒａｍｅｗｏｒｋ ｆｏｒ Ｄｉｇｉｔａｌ Ｃｏｎｔｒａｃｔ Ｃｏｍｐｏｓｉｔｉｏｎ ａｎｄ Ｆｕｌｆｉｌｌｍｅｎｔ、Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｗｏｒｋｓｈｏｐ ｆｏｒ Ｔｅｃｈｎｏｌｏｇｙ，Ｅｃｏｎｏｍｙ，Ｓｏｃｉａｌ ａｎｄ Ｌｅｇａｌ Ａｓｐｅｃｔｓ ｏｆ Ｖｉｒｔｕａｌ Ｇｏｏｄｓ、Ｉｌｌｍｅｎａｕ、Ｇｅｒｍａｎｙ （２００３年）及びＳａｉｔｏの米国出願２００６／０２８８４２４Ａ１号明細書を更に参照してもよい。

【発明の概要】

【発明が解決しようとする課題】

【０００６】
本明細書は、電子チケッティング取引でのセキュリティ及び著作権管理のために電子デバイスに対して既に使用可能なデジタル著作権管理（ＤＲＭ）システムを使用する有利な手法を開示する。既存の「規格化された」ＤＲＭソリューションであってもよいデジタル著作権管理システムを利用することにより、確立されたＤＲＭシステムの実証済みのセキュリティを有利に獲得しつつ、電子チケッティングアプリケーションを実現するのに電子デバイスで必要な処理リソース及びメモリリソースを減少させる。
【０００７】
限定しない一例として、携帯電話機又は他の電子デバイスには、内部に規格化されたＤＲＭソリューションが設置される。例えば、音楽再生機能を含む電子デバイスは、ネットワーク化されたＤＲＭシステムの一部としてＭＩＣＲＯＳＦＴ　ＰＬＡＹＲＥＡＤＹ、ＯＭＡ　ＤＲＭ、ＭＡＲＬＩＮブロードバンド（ＢＢ）又はリモートＤＲＭサーバと対話するように構成される他の規格化されたＤＲＭエージェント等を更に含む。本明細書で提案された教示によると、電子デバイスは、標準的なＤＲＭオブジェクトとして見えるようにパッケージ化される電子チケットオブジェクトを受信する。
【０００８】
このように、チケット発行器は、ＤＲＭオブジェクトとして電子チケットを発行することにより、チケットコンテンツをセキュリティ保護し且つ使用制限を実施する確立されたＤＲＭシステムに依存する。また、電子デバイスに設けられたチケットエージェントは、ＤＲＭによる使用制限を受け、受信した電子チケットを復号化するために確立されたＤＲＭシステムの一部として電子デバイスに設けられたＤＲＭエージェントを有利に使用する。従って、電子チケットオブジェクトを取得し、格納し且つ復号化する機能が既存のネットワーク化されたＤＲＭシステムに既に「内蔵」されているため、チケットエージェントは、これらの機能に対するセキュリティ機構を含む必要はない。従って、電子チケットオブジェクトは、例えば音楽ファイル等の標準的なＤＲＭオブジェクトのようにパッケージ化され、発行され且つ処理されてもよい。
【課題を解決するための手段】
【０００９】
本明細書で開示される一実施形態は、デジタル著作権管理エージェントが設けられた電子デバイスでの電子チケット処理の方法に関する。本明細書において、デジタル著作権管理エージェントは、ネットワーク化されたデジタル著作権管理システムの一部として動作し、方法は、デジタル著作権管理システムに従ってコンテンツ暗号鍵で暗号化されたチケット鍵を含むチケットオブジェクトを受信するステップを含む。方法は、デジタル著作権管理システムと互換性のある権利オブジェクトを受信するステップと、デジタル著作権管理エージェントと関連付けられたデジタル著作権管理鍵で暗号化されたコンテンツ暗号鍵及びチケットオブジェクトに対応する１つ以上の使用制限を含むステップと、電子デバイスに設けられた少なくとも１つのチケットエージェントを使用してチケットオブジェクトを引き換えるステップとを更に含む。引き換え動作は、１つ以上の使用制限を受け、デジタル著作権管理エージェントからチケット鍵を取り出すことを含む。
【００１０】
別の実施形態は、デジタル著作権管理エージェントが設けられた電子デバイスに関する。上述の方法と同様に、デジタル著作権管理エージェントは、ネットワーク化されたデジタル著作権管理システムの一部として動作し、電子デバイスは、１つ以上の通信インタフェースと、メモリと、ＣＰＵ又は他のマイクロプロセッサベースのデジタル処理回路等の１つ以上のプロセッサとを含む。プロセッサは、メモリ及び通信インタフェースと動作可能に関連付けられる。
【００１１】
それに対応して、１つ以上の通信インタフェースは、デジタル著作権管理システムに従ってコンテンツ暗号鍵で暗号化されたチケット鍵を含むチケットオブジェクトを受信し、且つ前記デジタル著作権管理システムと互換性のある権利オブジェクトを受信するように

構成される。本明細書において、権利オブジェクトは、チケットオブジェクトに対応する１つ以上の使用制限及びデジタル著作権管理エージェントと関連付けられたデジタル著作権管理鍵で暗号化されたコンテンツ暗号鍵を含む。

【００１２】

また、メモリはチケットオブジェクト及び権利オブジェクトに記憶装置を提供し、１つ以上の処理回路は、チケットオブジェクトを引き換えるように構成される少なくとも１つのチケットエージェント及びデジタル著作権管理エージェントを実行するように構成される。チケットエージェントは、１つ以上の使用制限を受け、デジタル著作権管理エージェントからチケット鍵を取り出すことと、チケット鍵を外部エージェントに公開せずにチケット鍵の所有を検証するように、予め定義された検証プロトコルに従って外部エージェントと通信することとに基づいてチケットオブジェクトを引き換える。

【００１３】

当然、本発明は上記の特徴及び利点に限定されない。実際には、以下の詳細な説明を読み且つ添付の図面を参照することにより、追加の特徴及び利点が当業者には認識されるだろう。

【図面の簡単な説明】

【００１４】

【図１】電子チケット処理を実現し且つ既存のネットワーク化されたデジタル著作権管理（ＤＲＭ）システムの一部として動作する電子デバイスの一実施形態を示すブロック図である。

【図２】ＤＲＭシステムを利用する電子チケット処理の一実施形態を示す論理フローチャートである。

【図３】電子チケットオブジェクトの一実施形態を示すブロック図である。

【図４】電子チケット処理を実現する電子デバイスの別の実施形態を示すブロック図である。

【図５】外部電子検証システムによる検証と関連付けられたチケット引換えデータフローを強調する電子チケット処理を実行する電子デバイスの別の実施形態を示すブロック図である。

【図６】オペレータによる検証と関連付けられたチケット引換えデータフローを強調する電子チケット処理を実行する電子デバイスの別の実施形態を示すブロック図である。

【図７】２種類の電子チケットオブジェクトのコンテンツの詳細な例で示された電子チケット処理を実行する電子デバイスの別の実施形態を示すブロック図である。

【図８】電子チケット引換えプロトコルの一実施形態を示す処理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、デジタル著作権管理（ＤＲＭ）エージェント１２が設けられた電子デバイス１０を示す。ＤＲＭエージェント１２は、「ネットワーク化されたデジタル著作権管理システム」の一部として動作する。ネットワーク化されたデジタル著作権管理システムは、ＤＲＭエージェント１２及びリモートのネットワークアクセス可能ＤＲＭサーバ１４を含み、著作権管理されたデータオブジェクトを発行し且つ使用する全体的な「ＤＲＭソリューション」を実現するものとして理解されるべきである。本明細書で開示される電子チケット処理の有利な方法及び装置が電子チケット処理をこの既存のＤＲＭソリューションに「便乗する」ことにより、セキュリティ及びオーバヘッドの処理の点で多くを電子デバイス１０に追加せずに、且つ規格化されたＤＲＭ動作を変更又は変形せずに、電子チケットの発行、格納及び引換え処理のセキュリティを確保する。

【００１６】

更に詳細には、権利発行器（ＲＩ）１６及びチケット発行器（ＴＩ）１８として識別されたネットワーク化されたコンピュータシステムをＤＲＭサーバ１４が備えることが分かる。既知であるように、ＲＩ１６及びＴＩ１８は、インターネット又は他のネットワーク接続を介して入手可能であり、別個に実現されてもよく（示されるように）、あるいは同

一のコンピュータ／サーバシステムに組み込まれてもよいことが理解されるべきである。また、ＴＩ１８は、ＤＲＭサーバ１４の構成要素として実現されなくてもよいことが理解されるべきである。しかし、ＴＩ１８がＤＲＭサーバ１４の構成要素として実現される場合、本明細書で開示される電子チケット処理の利点によれば、規格化された既存のＤＲＭソリューションが適切であるため、ＤＲＭソリューションがそのＤＲＭソリューションに対して標準的な著作権管理されたオブジェクトは何でも処理するように電子デバイス１０が「パッケージ化された」電子チケットを適切に処理できる、例えば、これらの適切にパッケージ化された電子チケットが標準的な著作権管理された音楽ファイル、ビデオファイル等のようにＤＲＭソリューション内で透過的に管理されると仮定することである。

【００１７】

換言すると、本明細書で開示される電子チケット処理は、ＤＲＭソリューションに対して透過的であるように電子チケットを発行し、セキュリティ保護し且つ引き換える既存のＤＲＭソリューションを使用する。規格化されたＤＲＭソリューションの限定しない例には、ＯＭＡ　ＤＲＭ、ＭＩＣＲＯＳＯＦＴ　ＰＬＡＹＲＥＡＤＹ及びＭＡＲＬＩＮ　ＢＢ（Ｍａｒｌｉｎ　Ｔｒｕｓｔ　Ｍａｎａｇｅｍｅｎｔ　Ｏｒｇａｎｉｚａｔｉｏｎを示す）が含まれ、その全ては、権利保護されたデータオブジェクトを発行し且つ使用する既定のプロトコル、メッセージ、機能及び暗号鍵／認証を提供する。

【００１８】

図１に示された更なる詳細な例において、電子デバイス１０は、例えば１つ以上の通信ネットワーク２４を介してＤＲＭサーバ１４から直接又は間接的にチケットオブジェクト２２を受信する１つ以上の通信インタフェース２０を備える。少なくとも一実施形態において、通信ネットワーク２４がセルラ通信ネットワークを含み、且つ通信インタフェース２０がセルラ送受信機を含むことにより、セルラ通信リンクを介して電子チケット及び対応する使用権を取得できる。当然、セルラコアネットワークは、一般にインターネットへのアクセスを提供でき且つ／あるいは他の公衆データネットワーク又は専用データネットワークとインタフェースできることが理解されるだろう。また、電子デバイス１０の同一の実施形態又は他の実施形態において、通信インタフェース２０は、ローカル無線通信リンクを提供するＢｌｕｅｔｏｏｔｈ（登録商標）又は他の狭域無線通信インタフェースを更に含む。いずれの場合も、チケットオブジェクト２２は、ＤＲＭシステムに従ってコンテンツ暗号鍵２８で暗号化されたチケット鍵２６を含む。電子デバイス１０は、通信インタフェース２０を介してＤＲＭシステムと互換性のある権利オブジェクト３０を更に受信する。すなわち、権利オブジェクト３０は、チケットオブジェクト２２のライセンスとして動作し、チケットオブジェクト２２に対応する１つ以上の使用制限を規定するデータを含む。少なくとも一実施形態において、権利オブジェクト３０は、デジタル著作権管理鍵３２で暗号化されたようなコンテンツ暗号鍵２８又はＤＲＭエージェント１２と関連付けられた他の鍵を更に含む。上述したように、チケットオブジェクト２２及び権利オブジェクト３０は、ＤＲＭソリューションと互換性のあるフォーマッティング構造を使用して電子ファイル又は他の電子データオブジェクトとして規定される。

【００１９】

電子デバイス１０は、チケットオブジェクト２２及び権利オブジェクト３０を格納するメモリ３４を更に含む。メモリ３４は、電子デバイス１０の全体的な機能性、例えば音楽プレーヤ機能性、携帯電話／スマートフォン機能性等と共に電子チケット処理を実現するプログラム命令に加え、本明細書で開示されるその電子チケット処理が利用する規格化されたＤＲＭ機能を実現するプログラム命令を格納するために更に使用されてもよい。

【００２０】

この点に関して、メモリ３４は、２つ以上のメモリ回路又はメモリ素子を備えてもよい。例えばメモリ３４は、電子デバイス１０の動作中にスクラッチパッドとして使用されるワーキングＲＡＭを含んでもよく、プログラム命令を格納するＥＥＰＲＯＭ、ＦＬＡＳＨ等の１つ以上の不揮発性メモリ素子を含んでもよい。更にメモリ３４は、電子デバイス１０のケース内の改竄防止封止パッケージ等の物理的に且つ電子的に安全な揮発性メモリ及

び／又は不揮発性メモリを含んでもよい。安全なメモリは、ＤＲＭ鍵３２等の機密データを保持するために使用されてもよい。

【００２１】

更なる詳細な例において、電子デバイス１０は１つ以上の処理回路４０を含む。一実施形態において、これらの回路は、格納されたプログラム命令の実行に少なくとも部分的に基づいて、特に本明細書で説明される電子チケット処理を実行するように構成される１つ以上のマイクロプロセッサ回路を備える。いずれの場合も、１つ以上の処理回路４０は、１つ以上の通信インタフェース２０及びメモリ３４と動作可能に関連付けられ、チケットオブジェクト２２を引き換えるように構成される少なくとも１つのチケットエージェント（ＴＡ）４２及びデジタル著作権管理（ＤＲＭ）エージェント１２を実現するように構成される。

【００２２】

少なくとも１つのチケットエージェント４２により実行されるようなチケット引換えは、権利オブジェクト３０により課された１つ以上の使用制限を受け、ＤＲＭエージェント１２からチケット鍵２６を取り出す（検索する）ことを含む。尚、チケット鍵２６を取り出すことは、ＤＲＭ使用制限を受け、一般にチケットオブジェクト２２を取り出すことを含み、ＤＲＭエージェント１２は、チケットオブジェクト２２を使用可能な形式に復号化する。引換えは、チケット鍵２６をチケット検証器４４に公開せずにチケット鍵２６の所有を検証するように、予め定義された検証プロトコルに従ってチケット検証器４４と通信することを更に含む。

【００２３】

図１において、チケット検証器４４は、「チケット検証器」を示すように「ＴＶ」とラベル付けされる。チケット検証器４４を更に参照するために、「チケット検証器４４」という用語が使用される。図１は、電子デバイス１０とチケット検証器４４との通信を実行する「ローカルリンク」４６を更に示す。

【００２４】

１つ以上の実施形態において、ローカルリンク４６は、自社開発のプロトコル又は標準的なプロトコルに従う低電力無線信号伝送等の近距離無線通信（ＮＦＣ）リンクである。更にローカルリンク４６は、Ｂｌｕｅｔｏｏｔｈ（登録商標）接続、光接続又はケーブル接続であってもよい。図示された電子デバイス１０は、電子デバイス１０のユーザと対話するためのキーパッド、ディスプレイ及び１つ以上のスピーカ等を提供するユーザインタフェース４８を含むことが更に分かる。次に、ユーザインタフェース４８がチケット引換え処理を含む電子チケット処理の種々の実施形態を支援するために使用される種々の方法を詳細に説明する。図１の詳細な例に基づき、電子デバイス１０の１つ以上の実施形態は、図２に示されるような電子チケット処理の方法を実現するように構成される。特に、電子デバイス１０の処理回路４０は、プログラム実行を介して示された方法を実現するように構成されてもよい。示された処理は、複数のチケット取引に対して繰り返されてもよく、他の処理動作の一部として又は他の処理動作と組み合わせて実行されてもよいことが理解されるべきである。一般に、チケットサービスが商業的に提供され且つデバイス１０のユーザがチケットを購入したウェブサイト上のブラウジングセッションにより、所定のチケットオブジェクト２２を受信する。当然、この例は限定するものではなく、電子チケットを購入するため、あるいは電子チケットをデバイス１０に配信し始めるための他の種類の取引が考えられる。従って、デバイス１０への電子チケットの配信が開始されるが、示された処理は、ＤＲＭ暗号化されたチケット鍵２６を含むチケットオブジェクト２２を受信すること（ブロック１００）から「開始する」。処理は、ＤＲＭ互換の権利オブジェクト３０を受信すること（ブロック１０２）に継続する。本明細書において、権利オブジェクト３０は、電子デバイス１０に導入されたＤＲＭソリューションの詳細に従ってフォーマットされ、構造化されあるいは構成されたという意味で「ＤＲＭ互換性がある」。例えば、ＤＲＭサーバ１４及びＤＲＭエージェント１２を含むネットワーク化されたＤＲＭシステムがＭＩＣＲＯＳＯＦＴ　ＰＬＡＹＲＥＡＤＹに基づく場合、権利オブジェクト３０

はＰＬＡＹＲＥＡＤＹ権利オブジェクトとして構成され、その違いは、より慣例的な音楽ファイル制御ではなく、チケットオブジェクト２２に使用制限を課すその使用法である。当然、本明細書に開示される利点として、その使用法の違いはＤＲＭエージェント１２に対して透過的である。

【００２５】

上記の実現例の場合、権利オブジェクト３０は、チケットオブジェクト２２の許可された使用法を管理するチケット使用制限を含む（ブロック１０２）。また、少なくとも一実施形態において、権利オブジェクト３０は、チケット鍵２６を復号化するための暗号化された鍵を含む。例えば権利オブジェクト３０は、図１に示されたコンテンツ鍵２８を含む。ネットワークＤＲＭシステムの詳細に依存して、コンテンツ鍵２８は、所有されるか又はＤＲＭエージェント１２と一意に関連付けられるＤＲＭ鍵３２で直接暗号化されてもよく、あるいはＤＲＭエージェントの鍵３２で暗号化されるＤＲＭ「ドメイン」鍵で暗号化されてもよい。どちらの場合でも、コンテンツ鍵２８は、ＤＲＭエージェント１２と関連付けられるデジタル著作権管理鍵で暗号化されるのが有利である。

【００２６】

従って、電子デバイス１０は、チケットオブジェクト２２及び対応する権利オブジェクト３０を受信し、電子デバイス１０のユーザによる引換えのためにそれらを格納する。処理は、チケットオブジェクト２２及び権利オブジェクト３０を受信した後しばらく継続し、設けられたチケットエージェント４２を使用してチケットオブジェクト２２を引き換える（ブロック１０４）。図２において、ブロック１０４は、ＤＲＭエージェント１２から復号化されたチケットオブジェクトを取り出すこと（ブロック１０４Ａ）と、チケット検証器４４と通信し、チケットオブジェクト２２を引き換えること（ブロック１０４Ｂ）とを含むより詳細な動作に分類される。

【００２７】

上記の電子チケット処理により、対応する権利オブジェクト３０により課された制限に従って、ＤＲＭエージェント１２がチケットオブジェクト２２を受信、格納、処理及び復号化できるようになるのが有利である。チケットエージェント４２は、ＤＲＭエージェント１２からチケットオブジェクト２２を要求し、且つＤＲＭエージェント１２が復号化されたチケットオブジェクトコンテンツを提供した後でチケットオブジェクト２２を引き換える引換えプロトコルを実現するように構成されればよい。従って、方法は、１つ以上の使用制限を受け、ＤＲＭエージェント１２からチケット鍵２６を取り出すことと、チケット鍵２６をチケット検証器４４に公開せずにチケット鍵２６の所有を検証するように、予め定義された検証プロトコルに従ってチケット検証器４４と通信することとを備える。

【００２８】

更なる利点として、少なくとも一実施形態において、チケットオブジェクト２２は、対価引換えトークンとしてチケット鍵２６を含み、組込み型チケットエージェントを更に含む。チケットエージェントをチケットオブジェクト２２に組み込むことにより、多くの利点を提供する。例えば組込み型チケットエージェントは、使い捨てのアプリケーションであってもよく、更に引換えのセキュリティを向上させ且つ不正使用防止を支援する。また、小型の組込み型アプレットである組込み型チケットエージェントは、特定の引換えプロトコルに対して容易に調節され、種々のチケットベンダ及び／又は種々のチケット検証システムに対して容易に変更される。

【００２９】

図３は、チケット鍵２６及び組込み型チケットエージェント４２－１を含むチケットオブジェクト２２の一実施形態を示す。（尚、本明細書の命名法において、組込み型チケットエージェントを含むチケットオブジェクト２２は「複合」チケットオブジェクトと呼ばれる場合もあるが、チケットオブジェクトは、組込み型チケットエージェントを含まない場合であっても、例えばチケット鍵２６等の多数の構成要素を含んでもよいことが理解されるべきである。）限定しない例として、少なくとも一実施形態において、組込み型チケットエージェント４２－１は、電子デバイス１０内で実現されたＪＡＶＡ（登録商標）仮

想機械で実行するＪＡＶＡアプレット又はミドレットとして実現される。従って、電子デバイス１０のユーザは、ウェブブラウザアプリケーションを介してチケット販売ウェブサイトにナビゲートし、チケット購入リンクを起動し、支払いをし、著作権管理オブジェクト３０と共に複合チケットオブジェクト２２を受信する。そのような実施形態において、後続の引換えは、ダウンロードされたチケットオブジェクトファイルを開こうとすること、それに対してポインタを選択すること等によりトリガされてもよい。

【００３０】

いずれの場合も、開始されると、ＤＲＭエージェント１２は、複合チケットオブジェクト２２に対応するものとして権利オブジェクト３０を識別し、特定された使用条件を満たす場合、複合チケットオブジェクト２２を復号化することにより、チケット引換えを支援するために組込み型チケットエージェント４２－１を使用できるようになる。

【００３１】

従って、少なくとも一実施形態において、チケットオブジェクト２２は、共にコンテンツ暗号鍵２８により保護された組込み型チケットエージェント４２－１及びチケット鍵２６を含む複合チケットオブジェクトを備える。更に１つ以上の処理回路４０は、ＤＲＭエージェント１２から組込み型チケットエージェント４２－１及びチケット鍵２６を検索し、且つチケットオブジェクト２２を引き換えるために組込み型チケットエージェント４２－１を使用することにより、チケットオブジェクト２２を引き換えるように構成される。少なくともそのような一実施形態において、１つ以上の処理回路４０は、図４に示すようにマスタチケットエージェントを実現するように構成される。本明細書において、マスタチケットエージェント４２－２は、ＤＲＭエージェント１２から組込み型チケットエージェント４２－１及びチケット鍵２６を取り出すように構成される。すなわち、マスタチケットエージェント４２－２は、権利オブジェクト３０により課された使用制限に従って、ＤＲＭエージェント１２による安全なチケットオブジェクト２２の復号化／解凍を開始するように構成される。

【００３２】

更にマスタチケットエージェント４２－２は、組込み型チケットエージェント４２－１を設置するかあるいは開始するように構成され、マスタチケットエージェントの制御下でチケット鍵２６を安全に保持しつつ、組込み型チケットエージェント４２－１によりチケット鍵２６を引き換えるのに使用するためにチケット鍵２６に関連して組込み型チケットエージェント４２－１を提供する。例えばマスタチケットエージェント４２－２は、安全な処理環境で実行する安全なアプリケーションを備える。実際のチケット鍵２６を組込み型チケットエージェント４２－１に公開するのではなく、マスタチケットエージェント４２－２はチケット鍵２６を制御し続ける。例えばマスタチケットエージェント４２－２は、ＤＲＭエージェント１２がチケットオブジェクト２２を復号化した後チケット鍵２６を安全なメモリに保持し、組込み型チケットエージェント４２－１に渡された他のプログラム参照又はポインタ介してチケット鍵２６への制御されたアクセスを提供する。

【００３３】

このように、マスタチケットエージェント４２－２は、電子デバイス１０に予め導入されてもよく、あるいは少なくともチケット引換えの前に導入されてもよく、チケット引換えプロトコルを実現するのを負担する必要はない。その代わり、マスタチケットエージェント４２－２は、チケット鍵情報をダウンロードできるようにする合意されたプロトコル及び組込み型チケットエージェント４２－１を提供すればよく、変形した、場合によっては変化する引換えプロトコルを実現することは、組込み型チケットエージェント４２－１に委ねられる。マスタチケットエージェント４２－２を有することは、マスタチケットエージェント４２－２のみがチケットオブジェクトデータに直接アクセスできるようにすることにより、組込み型チケットエージェント４２－１に対して設けられる可能性のあるセキュリティ制限のうちのいくつかを更に解除する。引換えに使用されるのが１つのチケットエージェント又は複数のチケットエージェントであっても、一実施形態において、図１に示されたチケット検証器４４はオペレータである。この場合、図１に示されたローカル

リンク４６は一般に存在しない。その代わり、引換え動作は、電子デバイス１０のユーザインタフェース４８に依存する。そのような一実施形態において、図５に示されるように、チケットエージェント４２は、電子デバイス１０のユーザインタフェースを介してチケット識別子（ＩＤ）５０を受信することに応答してチケットオブジェクト２２を引き換えるように構成される。例えばチケット検証者は、ユーザインタフェース４８のキーパッドを介して数字コード値を入力してもよく、あるいはそのようなデータは、電子ホブ等を使用して電子デバイス１０に「通して読まれ」てもよい。

【００３４】

いずれの場合も、チケットＩＤ５０は電子デバイス１０に格納された特定のチケットオブジェクト２２に応答し、チケットエージェント４２は、チケットＩＤ５０に対応するチケットオブジェクト２２をＤＲＭエージェント１２に渡すように構成されるか、あるいは参照をチケットオブジェクト２２に渡すように構成される。その結果、ＤＲＭエージェント１２は、使用制限に対して対応する著作権管理オブジェクト３０をチェックし、チケット使用が許可される場合にチケットオブジェクト２２を復号化する。従って、チケットエージェント４２は、返答としてチケット鍵２６及びチケットレンダリング情報（ＴＲＩ）５２を受信する。チケットエージェント４２は、ＴＲＩ５２に従って電子デバイス１０のユーザインタフェース４８を介してチケット情報をユーザが検証可能な形式にレンダリングする。例えばＴＲＩ５２は、２次元バーコード又はユーザインタフェース４８の表示画面上の他の規定のパターンをチケット検証者による検証のための引換え出力データとしてレンダリングする電子データを備えてもよい。

【００３５】

当然、多数の実施形態において、チケット検証器４４は電子検証システムを備える。図６は、チケットエージェント４２が、チケットエージェント４２と電子検証システムとの共有の秘密鍵としてチケット鍵２６を使用することに基づいて、電子検証システムに対して検証情報５４を生成し且つ電子検証システムからの反検証情報５６を検証することにより、チケットオブジェクト２２を引き換えるように構成される一例を示す。あるいは、検証は、一方がチケットエージェント２６用であり、他方が電子検証システム用である非対称鍵対を使用することに基づく。そのような実施形態において、チケットエージェント４２は、検証情報５４を電子検証システムに送出し且つ電子検証システムから反検証情報５６を受信する１つ以上の通信インタフェース２０のうちの１つを使用するように構成される。そのような処理の一部として、チケットエージェント４２は、通信インタフェース２０を介してチケット検証器４４からチケットエージェント４２に電子的に搬送されるチケットＩＤ５０を受信する。

【００３６】

少なくともそのような一実施形態において、チケットエージェント４２は、電子検証システムとして動作するチケット検証器４４からチケットＩＤ５０を受信することに応答してチケットオブジェクト２２を引き換えるように構成される。上述したように、チケットＩＤ５０は特定のチケットオブジェクト２２に対応し、電子デバイス１０は、あらゆる所定の時間に複数のチケットオブジェクトを保持してもよい。チケットエージェント４２は、チケットＩＤ５０に対応するチケットオブジェクト２２を検索してＤＲＭエージェント１２に渡し、且つ返答としてチケット鍵２６及び暗号化アルゴリズム５８を受信するように構成される。チケットエージェント４２は、電子検証システムに対して検証情報５４を生成するために、暗号化アルゴリズム５８等の暗号処理に必要とされるチケット鍵２６及び他のデータを使用する。

【００３７】

チケットオブジェクト２２に対して使用されるデータ構造及び暗号化方法は、上述の処理及びその変形例を補完する。概括的に言えば、チケットオブジェクト２２は、ＤＲＭエージェント１２により著作権管理されたオブジェクトとして処理する予め定義されたデジタル著作権管理形式に従ってタグ付けされるかあるいはパッケージ化されるコンテンツファイルを備える。すなわち、ＤＲＭエージェント１２は、ＤＲＭエージェント１２が理解

するようにプログラムされる他のあらゆる種類の著作権管理されたオブジェクトに見えるようにチケットオブジェクト２２がパッケージ化されるため、音楽ファイル等と比較してチケットオブジェクト２２が電子チケットであると認識する必要はない。

【００３８】

図７は、チケットオブジェクト２２の２つの実施形態に対するより詳細な例を示す。一方は、組込み型チケットエージェント４２－１を含まない２２－１として示され、他方は、示されたチケットオブジェクトで「ＴＡコード」と呼ばれる組込み型チケットエージェント４２－１を含む２２－２として示される。図７は、共に電子デバイス１０内にあるＤＲＭエージェント１２、チケットエージェント４２、権利発行器１６、チケット発行器１８及びチケット検証器（外部エージェント）４４を更に示す。

【００３９】

示されるように、チケットエージェント４２は、主に既定のチケット検証プロトコル（ＴＶＰ）を実行するためにチケット検証器４４と通信する役割を担う。チケットエージェント４２だけが検証期間中にチケットの信用証明書にアクセスすることをＤＲＭエージェント１２が保証するため、チケットエージェント４２は、チケットの妥当性を全くチェックする必要はない。外部から見ると、チケット検証器４４は、チケットオブジェクト２２を検証する役割を担うため、一般に電子デバイス１０の所有者であるチケット所有者がチケットオブジェクト２２と関連付けられた場所又はサービスへのアクセスを許可されるかを判定する。

【００４０】

図７は、ＤＲＭエージェント１２及びチケットエージェント４２が電子デバイス１０内に共に配置されているものとして示しているが、ＤＲＭエージェント１２及びチケットエージェント４２は種々のデバイスに配置されてもよい。例えばＤＲＭエージェント１２は、ＰＣ又は「ホームゲートウェイ」との通信機能を有する電話又は他のポータブルデバイス等の電子デバイス１０にチケットエージェント４２が配置された状態で、ＰＣ又はホームゲートウェイに配置されてもよい。いずれの場合も、ユーザが電子チケットの購入を開始するかあるいは実行することにより、ＴＩ１８は、ＲＩ１６を介して送出されてもよい権利オブジェクト３０で識別されたような適当な制約と共に、電子デバイス１０に発行するための電子チケットオブジェクト２２を発行する。尚、ＤＲＭエージェント１２とチケットエージェント４２との間の通信回線又はチャネルが安全でない場合、通信自体は暗号化等を介してセキュリティ保護される。実際の配置に依存して、少なくとも３種類のデジタルチケットが考えられる。チケットエージェント４２が電子デバイス１０に設置され既に存在する場合、ＴＩ１８は、チケット検証器４４を介して所定のイベントにアクセスするのに必要な信用証明書のみを配信する。これらの信用証明書は、ネットワーク化されたＤＲＭシステムにより暗号化される等して保護される。すなわち、チケットエージェント４２が電子デバイス１０に既に設置されている場合、チケットオブジェクト２２は、引換えに必要な信用証明書を搬送すればよい。図７において、この構成はチケットオブジェクト２２－１として示される。

【００４１】

一方、電子デバイス１０に既に設けられたチケットエージェント４２がない場合、チケットオブジェクト２２は、図３に示された複合チケットオブジェクトのようなものであってもよく、デジタルチケット及びチケットの実行可能なコードの引換え信用証明書は、共にパックされ、電子デバイス１０に配信される。図７において、この構成はチケットオブジェクト２２－２として示される。チケットエージェント４２がデバイス１０に設置されている場合、複合チケットオブジェクト２２－２で示されるような組込み型チケットエージェント４２－１を含む例を更に支援してもよい。そのような場合、パッケージ全体はネットワーク化されたＤＲＭシステムにより保護され、電子デバイス１０は、受信したチケットエージェントソフトウェア、例えば組込み型チケットエージェント４２－１が実行されるＪＡＶＡ仮想機械等の実行環境を提供する。しかし、ＤＲＭエージェント１２がチケットオブジェクト２２を復号化して信用証明書及びチケットエージェントソフトウェアに

アクセスするために、有効なＤＲＭライセンスが必要である。
【００４２】
同様の例において、電子デバイス１０には、図４のマスタチケットエージェント４２－２等のマスタチケットエージェントが設置される。従って、電子デバイス１０の実行環境は、チケット引換えを開始するためにマスタチケットエージェント４２－２を「呼び出す」。しかし、チケットオブジェクト２２のコンテンツは、組込み型チケットエージェント４２－１に自由に配信されない。その代わり、マスタチケットエージェント４２－２は、組込み型チケットエージェント４２－１とＤＲＭエージェント１２との間を仲介するものとして動作する。すなわち、組込み型チケットエージェント４１－１はチケットオブジェクト２２の使用を制御するが、チケットオブジェクト２２上の動作を実行するのはマスタチケットエージェント４２－２である。機密チケットデータをそのように保護することは、安全でなく／信用できない環境で実行するために組込み型チケットエージェント４２－１が複合チケットオブジェクト２２から取り出される場合に有利である。
【００４３】
いずれの場合も、全体的なチケット処理の一部として、ＴＩ１８は、所定のチケット購入に係るライセンスが電子デバイス１０にダウンロードされることをＲＩ１６に通信する。それに応答して、ＲＩ１６は、規定のライセンスダウンロードプロトコルを実行する。プロトコルは、ＯＭＡ　ＤＲＭ１．０に対する無線アプリケーションプロトコル（ＷＡＰ）プッシュ又はＯＭＡ　ＤＲＭ２．０／２．１に対する権利オブジェクト取得プロトコル（ＲＯＡＰ）等の適切な特定のＤＲＭソリューションにより規定される。
【００４４】
それにもかかわらず、チケット取得は完了し、電子デバイス１０は、チケットを引き換えるか又は使用するための使用ライセンス情報を搬送する対応する権利オブジェクト３０及びチケットオブジェクト２２を格納する。この情報は、ＤＲＭサーバ１４／ＤＲＭエージェント１２を含むネットワーク化されたＤＲＭシステムにより保護される。
【００４５】
この点に関して、それぞれ、電子デバイス１０とＴＩ１８とＲＩ１６との間で実行されるプロトコルは、使用されるＤＲＭソリューションにより規定された「標準的な」実現例である。ＤＲＭエージェント１２は、チケットオブジェクト２２が引換え可能な電子チケットであることを知るかあるいは認識する必要はない。実際には、有利な実現例において、チケットオブジェクト２２及び関連する権利オブジェクト３０は、標準的なＤＲＭソリューションに従ってフォーマットされる。これは、ＤＲＭエージェント１２が他のＤＲＭ制限されたオブジェクトを処理するのと同一の方法で、チケットオブジェクト２２及び関連する権利オブジェクト３０がＤＲＭエージェント１２により処理されることを意味する。
【００４６】
従って、図７に示すように、権利オブジェクト３０は、ＤＲＭソリューションにおいてライセンスとコンテンツとの間に論理結合を作成する一般的な構成要素であるコンテンツ識別子（ＣＩＤ）６０を含む。チケットが使用されてもよい制約を説明する使用権（ＵＲ）要素６２及びチケットオブジェクト２２を復号化するために使用されるコンテンツ暗号鍵（ＣＥＫ）６４が更に存在する。尚、ＣＥＫ６４は、図１で採用されたのと同一のコンテンツ鍵２８であってもよい。
【００４７】
殆どのＤＲＭシステムの場合、ＣＥＫ６４は、図１に示されたＤＲＭ鍵３２等の中間鍵を介してあるいはＤＲＭエージェント１２専用の鍵により直接暗号化される。しかし、権利オブジェクト３０を送信するために安全なチャネルに依存するＯＭＡ　ＤＲＭ１．０等のＤＲＭシステムが更にある。尚、権利オブジェクト３０及び／又はチケットオブジェクト２２の整合性を検証するのにＤＲＭエージェント１２により使用される更なる権利オブジェクトフィールド、例えばデジタル署名又は同様のデータを含むフィールドがあってもよい。

【００４８】
更にチケットオブジェクト２２（２２－１実施形態又は２２－２実施形態のいずれか）は、権利オブジェクト３０と同一のＣＩＤ６０を搬送し、デフォルトチケットプルーフ（ＤＴＰ）７２構成要素で発見された復号化データの媒体の種類を説明するＭＩＭＥタイプ７０がある。すなわち、このＭＩＭＥタイプフィールドはＤＲＭエージェント１２によりアクセス可能であり、ＤＲＭオブジェクトの非暗号化部分にあり且つチケットオブジェクトを含んでいるものとして保護されたファイルを説明するＤＲＭメタデータで一般に発見されるＭＭＥタイプフィールドと混同されるべきではない。この後者のＭＭＥタイプ情報は、ＤＲＭエージェント４２によりアクセス可能である。ＤＴＰ７２の暗号化、使用された暗号化アルゴリズム（Ａｌｓｏ）７４、チケット鍵識別子（ＴＫＩＤ）７６、チケット鍵（ＴＫ）２６（図１で採用されたような）及び開始ベクトル（ＩＶ）７８に関連した情報が更にある。ＣＩＤ６０を除く全てのそのような構成要素はＣＥＫ６４により暗号化され、ＤＴＰ７２はＴＫ２６により更に暗号化される。更にチケットオブジェクト２２－２は、ＤＲＭシステムにより更に保護される組込み型チケットエージェント４２－１の実行可能コードを含む。

【００４９】
少なくとも一実施形態において、チケットオブジェクト２２の記憶装置はチケットエージェント４２により制御される。例えばチケットエージェント４２は、電子デバイスのファイルシステム内でチケットオブジェクト２２が格納される場所を示すデータベースを維持する。少なくともそのような一実施形態において、データベースは、格納されたチケットオブジェクト２２のチケットＩＤ５０を格納するチケットＩＤフィールドを含む。チケットＩＤ５０は、チケットが適用するイベントの汎用識別子であり、チケットエージェント４２は、チケット検出器４２からこの識別子を受信する場合、データベースを探索して対応するチケットオブジェクト２２を発見するためにその識別子を使用する。チケットＩＤ５０とチケットオブジェクト２２との間の論理結合を確立し且つ維持するために、チケットオブジェクト２２がチケットＩＤ５０を含むのが有利である。この構成はいくつかの方法で実現される。例えばチケットＩＤ５０は、イベントを示す初期部分を有してもよいＣＩＤ６０の一部であってもよく、あるいは他の何らかのＤＲＭメタデータフィールドに配置されてもよい。

【００５０】
チケットエージェント４２は、受信したチケットオブジェクト２２の記憶装置を処理してもよく、１つ以上の実施形態において、ＤＲＭエージェント１２は、対応する権利オブジェクト３０の記憶装置を処理する。例えばＤＲＭエージェント１２は、権利オブジェクト３０が格納される場所を示すデータベースを維持する。この権利オブジェクトデータベースは、ＣＩＤフィールドに従って含むかあるいは索引を付けられる。すなわち、チケットエージェント４２の１つ以上の実施形態は、対応するチケットオブジェクト２２を取り出すかあるいは参照するためにチケットＩＤ５０を使用し、ＤＲＭエージェント１２の１つ以上の実施形態は、チケットオブジェクト２２からのＣＩＤ６０を分析し、対応する権利オブジェクト３０を取り出すためにそのような情報を使用する。

【００５１】
上記のデータ要素を用いて、多数のチケット検証の手法が考えられる。図８は、詳細な限定しない検証例を提供し、電子チケット引換えが必要となる所定の事象に電子デバイス１０及びそのユーザがあると仮定する。図８は、チケット検証器４４が電子システムであると仮定し、チケット検証器４４がＡｌｇｏ７４、ＴＫＩＤ７６、ＴＫ２６、ＩＶ７８及びチケットＩＤ５０をＴＩ１８から直接又は間接的に安全に受信したと更に仮定する。

【００５２】
チケット検証器４４及び電子デバイス１０は、図１に示されたローカルリンク４６等の接続を確立し、それを介してチケット検証プロトコルが実行される。この接続はどんな種類であってもよいが、一般にＢｌｕｅｔｏｏｔｈ（登録商標）又はＮＦＣ等の狭域無線接続である。接続を介して送出されたデータが十分にセキュリティ保護されるため、接続自

体はセキュリティ保護される必要はない。上記の状況に基づき、例示的な検証処理は以下のステップを含む。

【００５３】

ステップ１：チケット検証器４４は、チケットＩＤ５０を電子デバイス１０のチケットエージェント４２に送出することにより引換えプロトコルを開始する。

【００５４】

ステップ２：チケットエージェント４２は、対応するチケットオブジェクト２２を取り出すためにチケットＩＤ５０を使用する。例えばチケットエージェント４２は、チケットＩＤ５０に基づいて検索すべき適切な格納されたチケットオブジェクト２２を識別し、その特定のチケットオブジェクト２２をレンダリングするようＤＲＭエージェント１２に要求する。そうするために、ＤＲＭエージェント１２は、対象のチケットオブジェクト２２からのＣＩＤ６０を分析し、データベースで一致するＣＩＤを探索することにより関連する権利オブジェクト３０を取り出す。一致する権利オブジェクト３０を発見すると、ＤＲＭエージェント１２は、使用権をチェックし、レンダリングが許可されることを確認する。レンダリングが許可される場合、ＤＲＭエージェント１２は、チケットオブジェクト２２の復号化されたコンテンツをチケットエージェント４２に渡す。使用権によりレンダリングが許可されない場合、チケットエージェント４２は、ＴＩ１８に接続し、チケットオブジェクト２２に対して権利を更新しなければならない。特に、ＤＲＭエージェント１２によるこれらの動作が、ＤＲＭエージェント１２がＭＰ３サウンドファイル等の他のあらゆる種類のコンテンツをレンダリングする際に実行するものと同一であるため、チケット引換え処理は、ＤＲＭエージェント１２により実行された「標準的な」ＤＲＭ処理に新たな要求を追加しない。

【００５５】

ステップ３：チケットオブジェクト２２がＤＲＭエージェント１２によりレンダリングされたと仮定すると、チケットエージェント４２は、ＴＫＩＤ７６及び乱数ＲＮ１をチケット検証器４４に送出することにより、チケット検証器の開始メッセージに応答する。

【００５６】

ステップ４：チケット検証器４４は、データベースから一致する鍵を取り出すためにＴＫＩＤ７６を使用する。すなわち、チケット検証器４４は、ＴＫ２６に対する一致を取り出す。しかし、ＴＫＩＤ７６をこのように使用することにより、同一のチケットアプリケーション内でいくつかの異なる鍵を使用する手段を更に提供する。これは、異なる鍵が所定の事象内の種々の領域／機能にアクセスするために使用されてもよいことを意味する。更にチケット検証器４４は、H_1（ＲＮ１）を取得するように、例えばＳＨＡ１等の安全なハッシュ関数であってもよいある予め定義された関数H_1に従ってＲＮ１を変形する。次にチケット検証器４４は、H_1（ＲＮ１）を暗号化し、別のランダム値ＲＮ２と共にＥ［ＴＫ］（H_1（ＲＮ１））を送出する。

【００５７】

ステップ５：チケットエージェント４２は、先に送出されたＲＮ１に基づいて、Ｅ［ＴＫ］（H_1（ＲＮ１））を復号化し、それがチケットエージェント４２により算出されたH_1（ＲＮ１）に一致することをチェックする。一致しない場合、チケット検証器４４は適切なＴＫ２６を有さないか、あるいは接続は他の何らかの方法で失敗した。どちらの場合でも、そのような失敗により引換え処理は終了する。

【００５８】

ステップ６：チェックするステップ５により一致が判明する場合、チケットエージェント４２は、H_1とは異なる何らかの予め定義された関数H_2に従ってＲＮ２を変形する。次にチケットエージェント４２は、H_2（ＲＮ２）値をＥ［ＴＫ］（H_2（ＲＮ２））に暗号化し、別のランダム値ＲＮ３と共にＥ［ＴＫ］（H_2（ＲＮ２））を送出する。

【００５９】

ステップ７：チケット検証器４４は、チケットエージェント４２から受信したようなＥ［ＴＫ］（H_2（ＲＮ２））を復号化し、それが先に送出されたＲＮ２を使用して算出さ

れたH_2（ＲＮ２）に一致するかをチェックする。チェックにより一致が判明する場合、電子デバイス１０が所有するＴＫ２６が検証される。

【００６０】

デバイスのチケット鍵２６が検証される場合であっても、チケット検証器４４は、最後の正の検証に対して更なるチェックを実行してもよい。例えばチケット検証器４４は、引き換えられたチケットオブジェクト２２の数を追跡してもよく、その数を総合許可又は他の何らかの承認制限と比較してもよい。従って、最後の検証は、現在の検証が許可された検証数を上回るかを判定することを含んでもよい。最後の検証が負である場合、チケット検証器４４は、ＲＮ３をＥ［ＴＫ］（H_1（ＲＮ３））に暗号化し、これをチケットエージェント４２に送出する。

【００６１】

チケットエージェント４２は、Ｅ［ＴＫ］（H_1（ＲＮ３））を含むメッセージを受信する場合、これは送出されたＲＮ３と一致するため、チケット引換えを成功したものとしてログ記録するようＤＲＭエージェント１２に要求しない。逆に、最後の引換え検証がチケット検証器４４により成功するためにＥ［ＴＫ］（H_1（ＲＮ３））を含むメッセージが送出されない場合、チケットエージェント４２は、引換えをログ記録するようＤＲＭエージェント１２に要求する。チケットエージェント４２は、引換えを成功したものとしてログ記録する前に、チケット検証器４４からのメッセージが到着できるようにしばらくの間待つべきであるのが好ましい。例えばそのようなログ記録により、チケットオブジェクト２２が繰り返し使用可能なチケットである場合等に引換え／使用回数データが引き換えられたチケットオブジェクト２２に対して記録されるようになる。

【００６２】

チケット検証器４４がオペレータである場合、他の引換え処理の変形例が使用される。例えば、図８の処理フローに示される検証データ及び反検証データは、電子デバイス１０のユーザインタフェース４８に入力を提供し且つユーザインタフェース４８から出力を受信するオペレータに基づいて、少なくともある程度繰り返されてもよい。例えばオペレータは、キーボードを介して電子デバイス１０と対話してもよく、ディスプレイ出力及び／又はスピーカ出力を介して電子デバイス１０から出力を受信してもよい。

【００６３】

オペレータは、特に本明細書においてユーザ可読であるべき所定のチケットオブジェクト２２のチケットＩＤ５０を何らかの方法で安全に受信しており、且つ所定のチケットオブジェクト２２の引換えに関係しているＴＫ２６の各々、すなわち対応するＴＫＩＤ７６により示されるそのようなＴＫ２６の各々に対してＲＮ及びＥ［ＴＫ］（ＲＮ）に対する値の対を更に受信していると仮定する。ＤＴＰ７２のレンダリングが知覚される方法に関してオペレータに更に通知する。当然、チケットエージェント４２及びＤＲＭエージェント１２は、関連する権利オブジェクト３０と共に、引き換えられる所定のチケットオブジェクト２２をダウンロードし且つ登録していると仮定する。尚、デバイス１０のオペレータ及びチケット検出者は、手動認証の少なくともある態様を処理する役割を更に担ってもよい。

【００６４】

オペレータを介してチケット引換えのために引換えプロトコルパラメータを提示することと関連付けられた更なる詳細を以下に示す。尚、そのような所定のパラメータは、ベース６４エンコーディングを使用すること等を介してユーザ可読形式で提示される。引換えの第１のステップとして、オペレータは、チケットＩＤ５０を電子デバイス１０に入力する。例えばこの入力は、キーパッドを介するものであってもよく、あるいはフォッブ（fob）を通して読むことによるものであってもよい。尚、更にデバイスの所有者は、入力がチケットＩＤ５０として理解されるように電子デバイス１０上でチケット引換え処理を既に開始しているか、あるいは検証を担うオペレータは、電子デバイス１０上でそのような処理を開始している。

【００６５】

チケットエージェント４２は、電子形式でチケットＩＤ５０を受信し、引換えを対象にしたチケットオブジェクト２２を識別するためにそれを使用する。チケットエージェント４２は、ＤＲＭエージェント１２が対象のチケットオブジェクト２２に対してレンダリングセッションを開くことを要求する。ＤＲＭエージェント１２は、チケットオブジェクト２２からのＣＩＤ６０を分析し、データベースで一致するＣＩＤを探索する。引換えが許可されないことを対象のチケットオブジェクト２２に対応する権利オブジェクト３０が示す場合、ＤＲＭエージェント１２は、ＮＵＬＬ（又は他の何らかの使用されない値）に送出されるチケットエージェント４２にチケットハンドルを返送する。逆に、引換えが権利オブジェクト３０により課された使用制約内で許可できる場合、チケットハンドルは有効なハンドル値に送出される。引換えが許可されることをチケットハンドルが示すと仮定すると、チケットエージェント４２は、全てのチケットデータ（すなわち、ＭＩＭＥ７０、Ａｌｇｏ７４、ＴＫＩＤ７６、ＴＫ２６、ＩＶ７８及びＥ［ＴＫ］（ＤＴＰ））を取り出す。チケットエージェント４２は、Ｅ［ＴＫ］（ＤＴＰ）を復号化し且つＤＴＰ７２を取得するためにＡｌｇｏ７４、ＴＫ２６及びＩＶ７８を使用する。更にチケットエージェント４２は、ＭＩＭＥ７０を解析し、ＤＴＰ７２がオペレータにより検証のためにレンダリングされる方法を判定する。例えば、ＭＩＭＥ７０により指示されたようなレンダリング情報は、電子デバイス１０のユーザインタフェース４８の表示画面上で静止画像又は動画像（写真又は映像）の出力を特定してもよい。更に又はあるいは、レンダリング情報は、電子デバイス１０のユーザインタフェース４８に含まれたスピーカを介して特定の音声又は音色、例えばサウンドクリップの出力を特定してもよい。

【００６６】

いずれの場合も、チケットエージェント４２は、ＭＩＭＥ７０でレンダリング情報により指示されたようなＤＴＰ７２を提示し、表示される引換え画像／パターン上のオーバーレイとしてＴＫＩＤを提示すること等により、電子デバイスのディスプレイ上にＴＫＩＤ７６を更に表示してもよい。

【００６７】

それに対応して、オペレータは、ＤＴＰの電子デバイスのレンダリングを検証する。その検証が成功する場合、すなわち例えば適切な画像／パターンが表示された場合、オペレータは、電子デバイスのディスプレイ上に提示されたＴＫＩＤ７６に対して乱数の（秘密の）表及び対応する暗号化されたＥ［ＴＫ］（ＲＮ）値を調べてもよい。表形式で印刷されるかあるいは「計算尺」型プリントアウトで提供されてもよいそのようなデータから、オペレータは、適当なＲＮ２及び鍵を選択し、その値を電子デバイス１０に通して読むかあるいは入力する。

【００６８】

それに応答して、チケットエージェント４２は、ＲＮ２を暗号化し、暗号化された値を例えばベース６４エンコードされた値としてユーザ可読形式で電子デバイスのディスプレイ上に提示する。次にオペレータは、自身の印刷された情報でこの暗号化された結果を対応する値と比較する。暗号化された結果が適切である場合、オペレータは、引換えが成功したと考え、それに対応して電子デバイス１０のユーザへのアクセスを許可する。

【００６９】

また、アクセスが許可されると仮定すると、オペレータは、電子デバイス１０のディスプレイ上でキーを押下するか、あるいはチケットオブジェクト引換え成功の表示を電子デバイス１０に入力する。成功したチケット引換えの表示を受信することに応答して、チケットエージェント４２は、ログ要求をＤＲＭエージェント１２に送出し、成功したチケット引換えを示す。それに応答して、ＤＲＭエージェント１２は、データベースでライセンスロギングデータを更新する。

【００７０】

一方、チケット引換えが成功しなかった場合、オペレータは、その失敗の表示を電子デバイス１０に入力する。その表示に応答して、チケットエージェント４２は、引換えロギング要求なしで所定のチケットオブジェクト２２に対してＤＲＭエージェントの引換えセ

ッションを直接又は間接的に閉じる。

【００７１】

また、この更なる詳細な例は、チケット検証器４４がオペレータであっても電子検証システムであっても当てはまり、ＤＲＭエージェント１２及びチケットエージェント４２は、異なるデバイス／エンティティに分割されてもよい。例えば、チケットエージェント４２は電子デバイス１０に配置され、ＤＲＭエージェント１２は、デバイス所有者のＰＣ又はホームネットワークゲートウェイデバイスに配置される。この場合、分割されたＤＲＭエージェント１２及びチケットエージェント４２は、それらの間でデータをやり取りする安全なプロトコルを実現するように構成されるのが好ましい。有利な一実施形態において、安全なプロトコルは、ＤＲＭエージェント１２及びチケットエージェント４２をそれぞれ保持する２つのデバイスで共有のシークレット又は非対称鍵対を提供することに基づく。

【００７２】

２つのデバイスが一般的な提案として同一のユーザにより所有されるかあるいは制御されるとすると、共有のシークレット／鍵対を便利にオフラインで提供することは、キーボード／キーパッドエントリ等によりユーザにより実行されてもよい。当然、ＰＫＩに基づくプライベート／パブリック鍵暗号法が代わりに使用されてもよく、一般にＰＫＩに基づくセキュリティは、共有のシークレット／鍵対プロトコルと比較してデバイスにより重い計算の負担を課す。

【００７３】

当然、本発明は、上述の説明又は添付の図面により限定されない。実際には、本発明は、以下の添付の請求の範囲及びその法的等価物によってのみ限定される。

【図１】

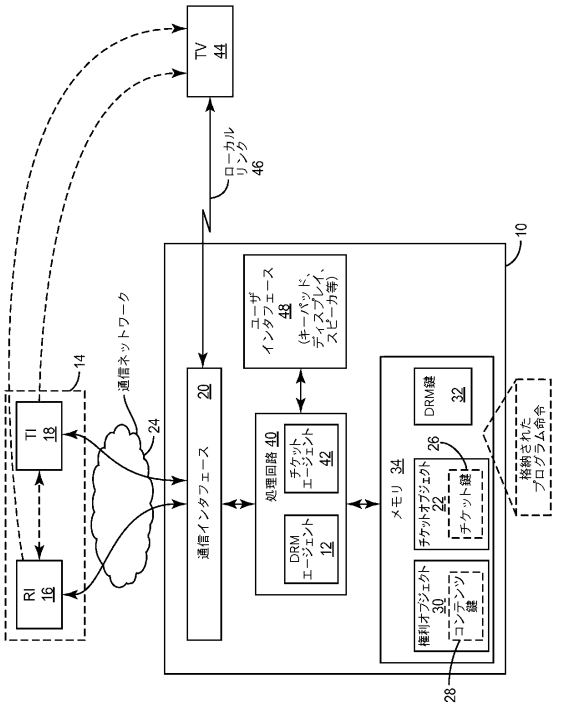

FIG. 1

【図２】

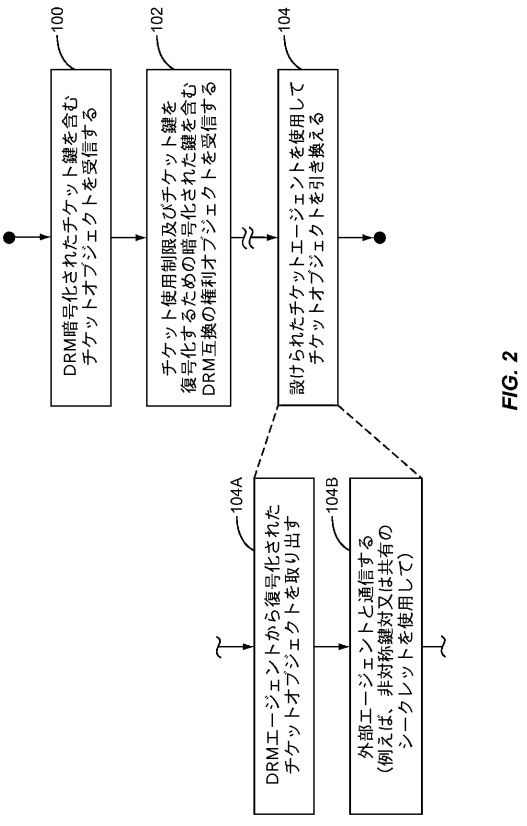

FIG. 2

【図３】

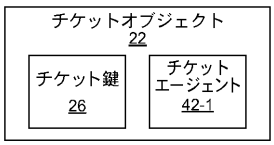

FIG. 3

【図４】

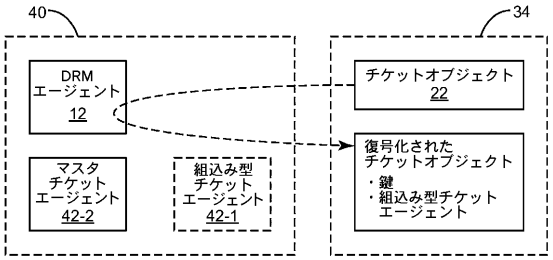

FIG. 4

【図５】

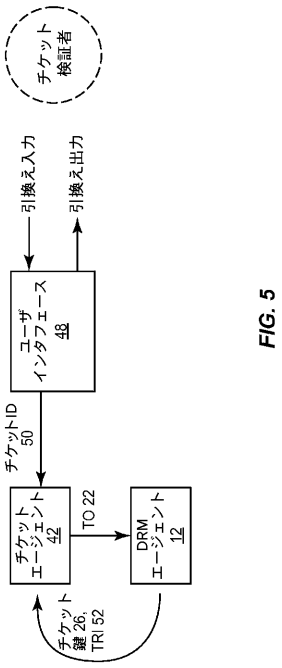

FIG. 5

【図６】

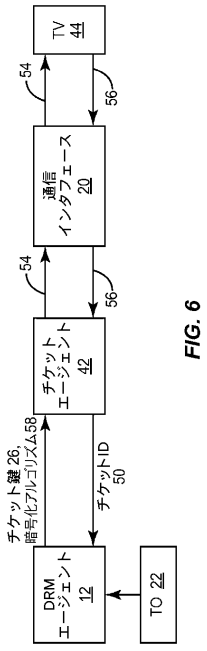

FIG. 6

【図７】

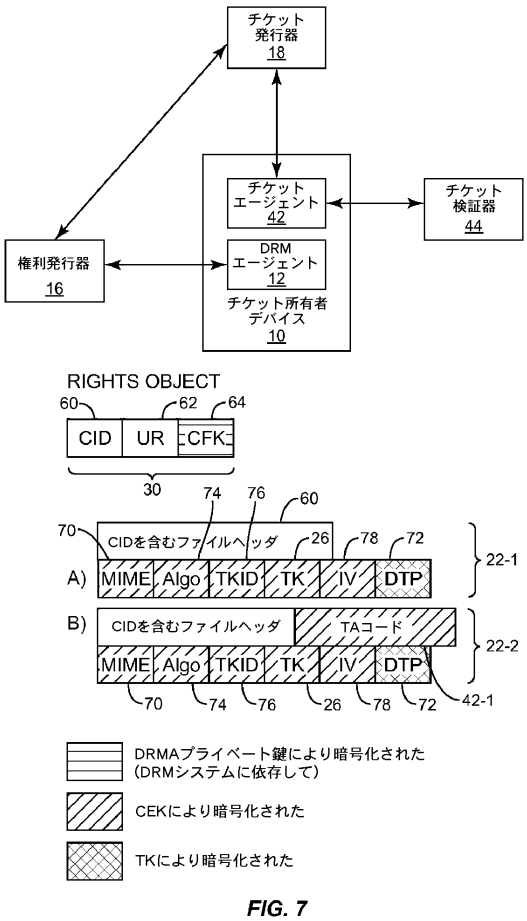

FIG. 7

【図８】

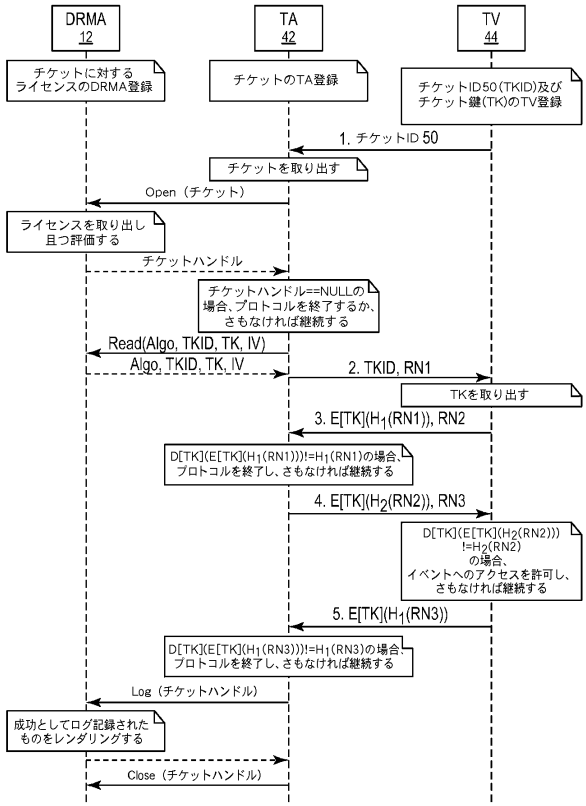
DRMA
12
TA
42
TV
44
チケットに対する
ライセンスのDRMA登録
チケットのTA登録
チケットID50(TKID)及び
チケット鍵(TK)のTV登録
1. チケットID 50
チケットを取り出す
Open（チケット）
ライセンスを取り出し
且つ評価する
チケットハンドル
チケットハンドル==NULLの
場合、プロトコルを終了するか、
さもなければ継続する
Read(Algo, TKID, TK, IV)
Algo, TKID, TK, IV
2. TKID, RN1
TKを取り出す
3. E[TK](H1(RN1)), RN2
D[TK](E[TK](H1(RN1)))!=H1(RN1)の場合、
プロトコルを終了し、さもなければ継続する
4. E[TK](H2(RN2)), RN3
D[TK](E[TK](H2(RN2)))
!=H2(RN2)
の場合、
イベントへのアクセスを許可し、
さもなければ継続する
5. E[TK](H1(RN3))
D[TK](E[TK](H1(RN3)))!=H1(RN3)の場合、
プロトコルを終了し、さもなければ継続する
Log（チケットハンドル）
成功としてログ記録された
ものをレンダリングする
Close（チケットハンドル）

FIG. 8

フロントページの続き

(72)発明者　ルース，　ヨハン
スウェーデン国　ルンド　エス－２２７　６０，　タルマンスガタン　１８
(72)発明者　イェルケングレン，　ウルフ
スウェーデン国　ビェレッド　エス－２３７　３４，　ネクテルガルスヴェーゲン　２６
(72)発明者　カトレイン，　ダニエル
ドイツ国　ヴュルゼレン　５２１４６，　キエフェルンシュトラーセ　９

審査官　山内　裕史

(56)参考文献　特開２００３－２７１８８３（ＪＰ，Ａ）
特表２００５－５２８６８５（ＪＰ，Ａ）
特表２００５－５０９２３１（ＪＰ，Ａ）
特開２００７－２２６７８５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　５０／１０
Ｇ０６Ｆ　２１／６２
Ｈ０４Ｌ　９／０８