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

特許第4259764号
(P4259764)

(45)発行日　平成21年4月30日(2009.4.30)　(24)登録日　平成21年2月20日(2009.2.20)

(51)Int.Cl.		F I		
H04N 7/173	(2006.01)	H04N	7/173	630
H04N 7/16	(2006.01)	H04N	7/16	Z
G06F 21/24	(2006.01)	G06F	12/14	550Z
G06F 21/22	(2006.01)	G06F	9/06	660G

請求項の数 35　(全 20 頁)

(21)出願番号	特願2000-552850 (P2000-552850)
(86)(22)出願日	平成11年5月25日 (1999.5.25)
(65)公表番号	特表2002-517960 (P2002-517960A)
(43)公表日	平成14年6月18日 (2002.6.18)
(86)国際出願番号	PCT/US1999/011537
(87)国際公開番号	WO1999/063757
(87)国際公開日	平成11年12月9日 (1999.12.9)
審査請求日	平成18年5月24日 (2006.5.24)
(31)優先権主張番号	09/087,386
(32)優先日	平成10年5月29日 (1998.5.29)
(33)優先権主張国	米国(US)
(31)優先権主張番号	09/196,964
(32)優先日	平成10年11月20日 (1998.11.20)
(33)優先権主張国	米国(US)

(73)特許権者　500200845
オープンティブイ・インコーポレーテッド
アメリカ合衆国・９４１１１・カリフォルニア州・サンフランシスコ・サクラメント　ストリート・２７５
(74)代理人　100078282
弁理士　山本　秀策
(72)発明者　シャリ，　スレッシュ　エヌ．
アメリカ合衆国　ニューヨーク　１０５２３，　エルムスフォード，　リッジビュー　テラス　１９
(72)発明者　ジマンスキ，　スティーブン
アメリカ合衆国　カリフォルニア　９５７１７，　サン　ノゼ，　スペノ　ドライブ　３４７５

最終頁に続く

(54)【発明の名称】インタラクティブテレビアプリケーションのためのセキュリティモデル

(57)【特許請求の範囲】

【請求項１】

インタラクティブテレビシステムにおいて受信された第１のインタラクティブテレビアプリケーションの機能を制御する方法であって、

特定の機能を実行するために、前記第１のアプリケーションの特権を識別するように構成された信用証明を受信することであって、前記信用証明は、前記受信された第１のアプリケーションを識別し、前記第１のアプリケーションによって実行され得る１つ以上の制限された機能に対応する権利を識別し、前記１つ以上の制限された機能が指示されるエンティティを識別するための情報を含む、ことと、

前記第１のアプリケーションが、前記１つ以上の制限された機能のうちの第１の機能を実行することを試みることと、

前記第１のアプリケーションが前記第１の機能を実行することを認証されているか否かを決定することであって、前記決定することは、前記第１の機能を実行するために十分な権利を前記第１のアプリケーションが有することを前記情報が示しているか否かを決定することを含む、ことと、

前記第１のアプリケーションが前記第１の機能を実行することを認証されていることを検出したことに応答して、前記第１のアプリケーションが前記第１の機能を実行することを可能にすることと

を包含する、方法。

【請求項２】

前記信用証明は、
前記エンティティを一意的に識別する譲渡人情報と、
前記第１のアプリケーションを一意的に識別する譲受人情報と
をさらに含む、請求項１に記載の方法。
【請求項３】
前記譲渡人情報は、譲渡人の作成者ＩＤと譲渡人のアプリケーションＩＤとを含み、前記譲受人情報は、譲受人の作成者ＩＤと譲受人のアプリケーションＩＤとを含む、請求項２に記載の方法。
【請求項４】
前記信用証明は、
前記エンティティおよびその他のエンティティを一意的に識別する譲渡人情報と、
前記第１のアプリケーションおよびその他のアプリケーションを一意的に識別する譲受人情報と
をさらに含む、請求項１に記載の方法。
【請求項５】
前記譲渡人情報は、譲渡人の作成者ＩＤと複数の譲渡人のアプリケーションＩＤとを含み、前記譲受人情報は、複数の譲受人の作成者ＩＤと対応する複数の譲受人のアプリケーションＩＤとを含む、請求項４に記載の方法。
【請求項６】
前記信用証明は、満了日をさらに含み、前記満了日を過ぎると、前記信用証明はもはや有効ではなくなる、請求項４に記載の方法。
【請求項７】
前記エンティティは、第２のアプリケーションに対応するモジュールのカルーセルを含み、前記信用証明は、前記カルーセルの一部として受信され、前記第１の機能は、前記第１のアプリケーションが前記第２のアプリケーションの実行を開始することを含む、請求項１に記載の方法。
【請求項８】
前記信用証明は、前記信用証明の認証を可能にするように構成されている追加の情報をさらに含む、請求項１に記載の方法。
【請求項９】
前記追加の情報は、作成者の認可を含み、前記作成者の認可は、信頼される関係者により署名される公開暗号鍵を含む、請求項８に記載の方法。
【請求項１０】
前記信用証明は、前記信用証明の完全性の検証を可能にするために、秘密暗号鍵を用いてさらに署名される、請求項９に記載の方法。
【請求項１１】
前記譲渡人のアプリケーションＩＤ、前記譲受人の作成者ＩＤ、前記譲受人のアプリケーションＩＤのうちの１つ以上は、ワイルドカードであり、前記ワイルドカードは、全てのＩＤと、それらと比較されるものとが一致しているとして考えられる、請求項５に記載の方法。
【請求項１２】
前記第１のアプリケーションは、複数のモジュールを含み、前記信用証明は、前記第１のアプリケーションの特定のモジュールをさらに識別し、前記第１の機能は、前記特定のモジュールの機能に対応する、請求項１に記載の方法。
【請求項１３】
前記エンティティは、第２のアプリケーションに対応する受信されたモジュールのカルーセルを含み、前記第１の機能は、前記複数のモジュールのうちの１つのモジュールにアクセスすることを含む、請求項１に記載の方法。
【請求項１４】
前記第１のアプリケーションのモジュールと、前記エンティティのモジュールとは、暗

号化されていない状態で受信される、請求項１２に記載の方法。
【請求項１５】
前記エンティティは、第２のアプリケーションを含み、前記第１の機能は、前記第２のアプリケーションの実行を終了すること、または、前記第２のアプリケーションの実行を開始することのいずれか一方を含む、請求項１に記載の方法。
【請求項１６】
前記インタラクティブテレビシステムは、放送局と受信局とを含み、前記放送局は、前記放送局から前記受信局に前記第１のアプリケーションを送信するように構成されている、請求項１に記載の方法。
【請求項１７】
インタラクティブテレビシステムにおいて受信された第１のインタラクティブテレビアプリケーションによって試みられる機能を制御する、インタラクティブテレビシステムにおけるデバイスであって、
前記デバイスは、
受信器と、
前記第１のアプリケーションを格納するデータ格納デバイスと、
制御ユニットと
を含み、
前記受信器は、
前記第１のアプリケーションを含む放送インタラクティブテレビ信号を受信することと、
特定の機能を実行するために、前記第１のアプリケーションの特権を識別するように構成された信用証明を受信することであって、前記信用証明は、前記受信された第１のアプリケーションを識別し、前記第１のアプリケーションによって実行され得る１つ以上の制限された機能に対応する権利を識別し、前記１つ以上の制限された機能が指示されるエンティティを識別するための情報を含む、ことと
を行うように構成されており、
前記制御ユニットは、
前記１つ以上の制限された機能のうちの第１の機能を実行することを前記第１のアプリケーションが試みることを検出することと、
前記第１のアプリケーションが前記第１の機能を実行することを認証されているか否かを決定することであって、前記決定することは、前記第１の機能を実行するために十分な権利を前記第１のアプリケーションが有することを前記情報が示しているか否かを決定することを含む、ことと、
前記第１のアプリケーションが前記第１の機能を実行することを認証されていることを検出したことに応答して、前記第１のアプリケーションが前記第１の機能を実行することを可能にすることと
を行うように構成されている、デバイス。
【請求項１８】
前記信用証明は、
前記エンティティを一意的に識別する譲渡人情報と、
前記第１のアプリケーションを一意的に識別する譲受人情報と
をさらに含む、請求項１７に記載のデバイス。
【請求項１９】
前記譲渡人情報は、譲渡人の作成者ＩＤと譲渡人のアプリケーションＩＤとを含み、前記譲受人情報は、譲受人の作成者ＩＤと譲受人のアプリケーションＩＤとを含む、請求項１８に記載のデバイス。
【請求項２０】
前記信用証明は、
前記エンティティおよびその他のエンティティを一意的に識別する譲渡人情報と、

前記第１のアプリケーションおよびその他のアプリケーションを一意的に識別する譲受人情報と
をさらに含む、請求項１７に記載のデバイス。
【請求項２１】
前記譲渡人情報は、譲渡人の作成者ＩＤと複数の譲渡人のアプリケーションＩＤとを含み、前記譲受人情報は、複数の譲受人の作成者ＩＤと対応する複数の譲受人のアプリケーションＩＤとを含む、請求項２０に記載のデバイス。
【請求項２２】
前記信用証明は、満了日をさらに含み、前記満了日を過ぎると、前記信用証明はもはや有効ではなくなる、請求項１９に記載のデバイス。
【請求項２３】
前記エンティティは、第２のアプリケーションに対応するモジュールのカルーセルを含み、前記信用証明は、前記カルーセルの一部として受信され、前記第１の機能は、前記第１のアプリケーションが前記第２のアプリケーションの実行を開始することを含む、請求項１７に記載のデバイス。
【請求項２４】
前記信用証明は、前記信用証明の認証を可能にするように構成されている追加の情報をさらに含む、請求項１７に記載のデバイス。
【請求項２５】
前記追加の情報は、作成者の認可を含み、前記作成者の認可は、信頼される関係者により署名される公開暗号鍵を含む、請求項２４に記載のデバイス。
【請求項２６】
前記信用証明は、前記信用証明の完全性の検証を可能にするために、秘密暗号鍵を用いてさらに署名される、請求項２５に記載のデバイス。
【請求項２７】
前記譲渡人のアプリケーションＩＤ、前記譲受人の作成者ＩＤ、前記譲受人のアプリケーションＩＤのうちの１つ以上は、ワイルドカードであり、前記ワイルドカードは、全てのＩＤと、それらと比較されるものとが一致しているとして考えられる、請求項２１に記載のデバイス。
【請求項２８】
前記第１のアプリケーションは、複数のモジュールを含み、前記信用証明は、前記第１のアプリケーションの特定のモジュールをさらに識別し、前記第１の機能は、前記特定のモジュールの機能に対応する、請求項１７に記載のデバイス。
【請求項２９】
前記エンティティは、第２のアプリケーションに対応する受信されたモジュールのカルーセルを含み、前記第１の機能は、前記複数のモジュールのうちの１つのモジュールにアクセスすることを含む、請求項１７に記載のデバイス。
【請求項３０】
前記第１のアプリケーションのモジュールと、前記エンティティのモジュールとは、暗号化されていない状態で受信される、請求項２８に記載のデバイス。
【請求項３１】
前記エンティティは、第２のアプリケーションを含み、前記第１の機能は、前記第２のアプリケーションの実行を終了すること、または、前記第２のアプリケーションの実行を開始することのいずれか一方を含む、請求項１７に記載のデバイス。
【請求項３２】
前記インタラクティブテレビシステムは、放送局と受信局とを含み、前記放送局は、前記放送局から前記受信局に前記第１のアプリケーションを送信するように構成されている、請求項１７に記載のデバイス。
【請求項３３】
セットトップボックスを含む、請求項１７に記載のデバイス。

【請求項３４】
前記信用証明は、前記第１のアプリケーションとは無関係に前記受信器に送られる、請求項１７に記載のデバイス。
【請求項３５】
実行可能なインタラクティブテレビアプリケーションによって実行されるアクションを制御するように構成されたインタラクティブテレビシステムであって、
前記システムは、放送局と受信器とを含み、
前記放送局は、第１のインタラクティブテレビアプリケーションを含む放送信号を送信するように構成されており、
前記受信器は、
前記第１のインタラクティブアプリケーションを含む前記放送インタラクティブテレビ信号を受信することと、
特定の機能を実行するために、前記第１のアプリケーションの特権を識別するように構成された信用証明を受信することであって、前記信用証明は、前記受信された第１のアプリケーションを識別し、前記第１のアプリケーションによって実行され得る１つ以上の制限された機能に対応する権利を識別し、前記１つ以上の制限された機能が指示されるエンティティを識別する情報を含む、ことと、
前記１つ以上の制限された機能のうちの第１の機能を実行することを前記第１のアプリケーションが試みることを検出することと、
前記第１のアプリケーションが前記第１の機能を実行することを認証されているか否かを決定することであって、前記決定することは、前記第１の機能を実行するために十分な権利を前記第１のアプリケーションが有することを前記情報が示しているか否かを決定することを含む、ことと、
前記第１のアプリケーションが前記第１の機能を実行することを認証されていることを検出したことに応答して、前記第１のアプリケーションが前記第１の機能を実行することを可能にすることと
を行うように構成されている、インタラクティブテレビシステム。
【発明の詳細な説明】
【０００１】
（発明の背景）
（発明の分野）
本発明は、インタラクティブテレビシステムに関し、さらに詳細には、他のモジュールにアクセスするか、または制限されているなんらかのアクションを取り得る、インタラクティブテレビアプリケーションに関するセキュリティを実行するための手段に関する。
【０００２】
（関連技術の説明）
インタラクティブテレビシステムは、視聴者にサービスを提供するための各種の新しい手段を提供するために、テレビセットを用いることを可能にする。インタラクティブテレビシステムは、通常の映像番組ストリームに加えて、テキストおよびグラフィックイメージを表示することができる。インタラクティブテレビシステムはまた、視聴者のアクションまたは応答を登録することも可能である。インタラクティブテレビの提案されている特徴としては、宣伝された商品またはサービスをオーダーしたり、ゲームショーでの出場者と競ったり、または特定の番組に関する専門的な情報をリクエストすることにより、ユーザが放映された番組とインタラクトすることができるような、各種のマーケティング、エンターテイメント、および教育能力が含まれる。
【０００３】
概して、放送サービス提供者は、視聴者のテレビへ伝送するためのインタラクティブテレビ信号を生成する。インタラクティブテレビ信号は、テレビ番組からなる音声映像部分はもちろん、アプリケーションコード、または制御情報からなるインタラクティブ部分を含む。本明細書中において用いられるとおり、「アプリケーション」なる用語は、コンピュ

ータソフトウェアアプリケーションに含まれるような、タスクに関連づけられたコードまたはデータの集合を一般に示す。放送サービス提供者は、音声映像およびインタラクティブ部分を組合せて、ユーザのテレビと接続された受信器への伝送のために、単一の信号にする。この信号は、一般に、伝送の前に圧縮され、ケーブルテレビ（ＣＡＴＶ）線、または直接衛星伝送システム等の通常の放送チャネルを介して伝送される。

【０００４】

テレビのインタラクティブ機能性は、テレビと接続されたセットトップボックスにより制御される。セットトップボックスは、放送サービス提供者により伝送された信号を受信し、インタラクティブ部分と音声映像部分を分離し、且つ信号のそれぞれの部分を展開する。セットトップボックスは、例えば、音声映像情報がテレビへ伝送される一方で、アプリケーションを実行するために、インタラクティブ情報を用いる。セットトップボックスは、音声映像情報を、テレビへとその情報を伝送するよりも前に、インタラクティブアプリケーションにより生成されたインタラクティブグラフィックスまたは音声と組み合わせ得る。インタラクティブグラフィックスおよび音声は、視聴者へさらなる情報を提供するか、または視聴者に入力を促し得る。セットトップボックスは、視聴者の入力または他の情報を、モデム接続を介して放送サービス提供者へと提供し得る。

インタラクティブテレビアプリケーションは、テレビシステムで用いられるインタラクティブコンテンツを含むアプリケーションである。

インタラクティブテレビアプリケーションは、１以上の番組モジュールから成る。

モジュールは、概して、完全なアプリケーションまたは番組を形成するように他のモジュールと組み合され得るアプリケーションコードの１単位である。

【０００５】

アプリケーションが複数のモジュールを有している場合、そのアプリケーションを形成しているモジュールのセットは、概して、自蔵式である。すなわち、アプリケーションが必要とするコードの全てが、そのモジュールのセットの中にある。第１のモジュールは、アプリケーションの一部であるモジュールの全てを識別するデイレクトリモジュールである。ディレクトリモジュール内に列挙されるモジュールのセット全体が、放送チャネルを介してセットトップボックスへと伝送され、アプリケーションが実行される。（このモジュールのセットは、下記の説明のとおり、カルーセル（ｃａｒｏｕｓｅｌ）と呼ばれ得る。）第１のインタラクティブテレビアプリケーションが、実行を完了し、第２のインタラクティブテレビアプリケーションが次に実行されると、その第２のインタラクティブテレビアプリケーションのディレクトリおよび他のモジュールが、セットトップボックスへと伝送され、第２のアプリケーションが実行される。第２のアプリケーションにより用いられるモジュールセットの全体が伝送されるが、そのモジュールのいくつかは、第１のアプリケーションにより用いられたモジュールと同一であってよい。

【０００６】

モジュールがアプリケーション間で共有され得るように、モジュール方式でソフトウェアアプリケーションを設計することは、有利であり得る。モジュール方式の利点は、インタラクティブアプリケーションに用いることができるセットトップボックス内の限られたメモリ量を維持すること、放送局からセットトップボックスへとアプリケーションをダウンロードするために必要な時間を低減すること、またはモジュールを共有可能にすることにより必ず書きこまれるアプリケーションコードの量を低減することを含み得る。アプリケーションのコンポーネントは、異なるカルーセル内に常駐し得るので、個々のモジュールのセキュリティを確実にし、且つ、従って、認定されたモジュールへのアクセスを制限することが望ましい。

【０００７】

アプリケーションが、モジュールを共有していない場合でも、制御された方法で相互にインタラクトすることを可能にするメカニズムを提供することも有効である。例えば、あるアプリケーションが、別のアプリケーションへと制御を転送し、その第２のアプリケーションがストール（ｓｔａｌｌ）する場合、第１のアプリケーションは制御を取り戻すため

に第２のアプリケーションを終了する必要があり得る。それゆえ、第１のアプリケーションのアクセス権を検証し、且つ第１のアプリケーションがそのようなアクションを取ることを可能とするかどうかを判定するシステムを提供することは望ましい。さらに、システムと関連づけられたオーバーヘッドを最小化する方法でこれらの特徴を実現することが望ましい。

ＷＯ　９８　１００９７２は、加入者情報リクエストを情報サービス提供者へと伝送するためのシステムを提案するが、インタラクティブテレビアプリケーションが、信用証明検証の際に許可を有するときに、機能を実行することは許可しない。

【０００８】

本発明は、インタラクティブテレビアプリケーションのアクセス権を制限または制御するためのシステムおよび方法を包含する。（「アクセス権」は、本明細書中において、番組モジュールを共有するための、他のアプリケーションを制御するための、システムリソースを用いるための、または他のアクションを取るための、アプリケーションの権利を示すために用いられる。）本発明の１つの実行形態は、インタラクティブテレビシステム内に、他のアプリケーションに影響を及ぼし得るアクションを取ろうと試みる、あるアプリケーションの信用証明（ｃｒｅｄｅｎｔｉａｌｓ）を検証するための手段を提供する。

本明細書中において用いられるとおり、「信用証明」なる用語は、アプリケーションモジュールがある機能を実行するための権限を識別する、特定のアプリケーションまたはモジュールと関連づけられた一片の情報である。

システムは、ある動作に関連して、個々のアプリケーションのセキュリティ、安全性、および権限を保証するために実現される。システムは、アプリケーション、個々の特権、権利、および制限を識別するための、各種の情報の断片からなる信用証明を利用する。

【０００９】

１つの実施形態において、この信用証明は、作成者識別番号（ＩＤ）、およびアプリケーション、有効期間満了日、権利のリスト、作成者の認可および署名のためのアプリケーションＩＤを含む。作成者およびアプリケーションＩＤは、アプリケーションを唯一的に識別する。権利のリストは、別のアプリケーションモジュールへアクセスすること、または他のアプリケーションの実行を終了すること等の、制限された権利を実行するため、アプリケーションの能力を識別する。この制限された権利は、システム内のアプリケーションにより実行されるいずれの動作にも関係し得る。有効期間満了日は、それを過ぎると、その信用証明が有効でなくなる期限を設定する。信用証明は、セキュリティのために公開鍵暗号化（下記に詳述する）を利用する。作成者証明は、その作成者の公開鍵である。信用証明全体が、信用証明の完全性が検証されることができるように、作成者の個人鍵を用いて署名される。

上述の暗号化セキュリティ手段および有効期間満了日を利用することで、信用証明が本物であるかどうか、および、もしそうであれば、まだ有効であるかどうかが判定され得る。

【００１０】

１つの実施形態において、信用証明は、第１のアプリケーションが、第２のアプリケーションが第１のアプリケーションのコードを共有するか、または第１のアプリケーションに関するアクションを取ることを許可し得るメカニズムを提供するために用いられ得る。第１のアプリケーションの所有者は、信用証明内に、所有者であることを識別するためのＩＤを有する。同様に、第２のアプリケーションは、許可されたアプリケーションとして、信用証明内に列挙されたＩＤを有する。第１および第２のアプリケーション両方の所有者は、アプリケーションに特定のＩＤを割り当てるので、各ＩＤは、その所有者のアプリケーション中では唯一的である。所有者はまた、所有者（作成者）中において唯一的である自身のＩＤを有する。いずれの所与のアプリケーションは、それゆえ、その所有者およびアプリケーションＩＤにより識別されることができる。よって、いずれの所与のアプリケーションも、特定の所有者により所有される、特定のアプリケーションに対して、特定の許可を認めることができる。アプリケーションの作成者、およびアプリケーションＩＤは、単一のアプリケーションが、あるグループの所有者またはアプリケーションに、許可を

認め得るように、ワイルドカードと置きかえられ得る。

【００１１】

１つの実施形態において、信用証明は、他のアプリケーションに影響を及ぼさない第１のアプリケーションのアクションを制御するために用いられ得る。例えば、アプリケーションは、セットトップボックス内に格納された、個人的で、制限されたデータにアクセスを試み得る。セットトップボックスは、そのデータにアクセスする権利を表わす有効な信用証明が提供されたときのみ、その制限されたデータに対応するメモリ内の位置へのアクセスを認めるように構成され得る。別の実施形態において、システムは、放送局へのリターンパス（ｒｅｔｕｒｎ　ｐａｔｈ）等の他のシステムリソースへのアクセスを制限するように構成され得る。このシステムは、実行をする前、またはリターンパスへのアクセスがリクエストされるときに、アプリケーションの信用証明をチェックし得る。有効な信用証明がリターンパスの使用許可を表わすのであれば、アクセスは許可される。信用証明は、アプリケーションの任意の数の機能を制御するために用いられ得、その信用証明を有効にするために用いられるメカニズムの実現においては、多くの変形例があり得る。

【００１２】

本発明の他の目的および利点は、以下の詳細な説明および添付の図面を参照することにより、明らかになる。

【００１３】

本発明は、各種の修正および改変可能であるが、その特定の実施形態が、図面の例を用いて示され、且つ本明細書中において詳述される。しかしながら、図面およびその詳細な説明は、本発明を、開示された特定の形式に限定するためのものではなく、反対に、本発明は、添付の請求の範囲により定義されるような、本発明の精神および範囲に該当する、修正、同様のもの、および変形の全てを含む。

【００１４】

（好適な実施形態の詳細な説明）

本発明の１つの実施形態を下記に説明する。本実施形態において、インタラクティブテレビ受信器は、直接衛星伝送等の放送チャネルを介して、音声映像インタラクティブ信号を受け入れる。本明細書中において用いられる「直接」衛星伝送は、インタラクティブテレビ受信器、より詳細には、アンテナにより、衛星から直接受信される伝送体（ｔｒａｎｓｍｉｓｓｉｏｎ）を意図する。音声映像インタラクティブ信号は、制御信号またはインタラクティブアプリケーション等のインタラクティブコンテンツはもちろん、テレビ番組、または同様の音声映像コンテンツを含む。「放送」という用語は、本明細書中において、全ての加入受信器への単一の信号の伝送を示すために用いられる。インタラクティブテレビ受信器はまた、モデム等の放送チャネルでないものを介して、音声映像インタラクティブ信号を受信するように構成される。インタラクティブテレビ受信器は、音声映像コンテンツを、音声映像インタラクティブ信号のインタラクティブコンテンツから分離するよう構成される。音声映像コンテンツは、テレビ番組として表示するために処理される一方で、インタラクティブコンテンツは、受信器による実行のために処理される。インタラクティブコンテンツは、表示のためにテレビ番組と組み合わせられる音声またはグラフィックスを生成することを含む、各種の機能を受信器が実行することを可能にし得る。インタラクティブコンテンツがアプリケーションを含むのであれば、そのアプリケーションは、いくつかのサブコンポーネントまたはモジュールから成り得る。モジュールは、アプリケーションコード、生データ、またはグラフィックス情報等の任意のタイプのデータを含むことができる。

【００１５】

インタラクティブアプリケーションを形成するモジュールは、概して、カルーセルと呼ばれるモジュールの単一の集合に属する。カルーセルは、一般に、同じ作成者により所有され、且つ相互にアクセスする権利を有するモジュールの集合として定義することができる。これらのモジュールは、概して、周期的方式でインタラクティブテレビ受信器へと伝送されるので、カルーセルと呼ばれる。アプリケーションは、「トップレベル」の番組を含

むカルーセルである。

【００１６】

アプリケーションが（データの共有、アプリケーションの制御の伝送、または他の目的のために）別のカルーセルのモジュールにアクセスすることを可能とすることが望ましくあり得る。１つのカルーセルのアプリケーションまたはモジュールは、「信用証明」を用いることにより、別のカルーセルのモジュール、またはインタラクティブテレビシステムとインタラクトできる。信用証明は、特定のモジュールの特権および制限を識別かつ検証するために用いることができるデータの集合である。この特権および制限は、モジュールが他のモジュールとインタラクトするか、またはメモリの制限された領域へのアクセス等のその他の制限されたアクションを取る権限を与えられているかどうかに関連し得る。この信用証明は、ワイルドカードを用いて、全ての関係するモジュールのリストを維持することを必要とせずに、多数のモジュールへの特権を承諾し得る。

１つの実施形態において、アプリケーションまたはモジュールに関する信用証明を検証するという行為は、インタラクティブテレビシステムの制御ユニットへ信用証明情報を伝達するアプリケーションまたはモジュールを必要とし得、そのインタラクティブテレビシステムの制御ユニットは、その搬送された情報のコンテンツと、予期されるコンテンツとを比較するように構成され得る。搬送されたコンテンツが、予期または必要とされたものと一致すれのであれば、その信用証明は、「検証」され、アプリケーションまたはモジュールは、信用証明情報に対応するなんらかのアクションまたは機能の実行を許可される。このような場合、この資格情報は、対応するアクションを実行する許可を示す。あるいは、信用証明を検証するという行為は、アプリケーションまたはモジュールが必要とされる情報の断片を所有するかどうかチェックすることを必要とし得る。アプリケーションまたはモジュールが必要とされる情報の断片を所有するのであれば、アプリケーションは、その情報の断片に対応するアクションを取ることが可能となる。

【００１７】

図１を参照して、ソースから一連の視聴者までの、インタラクティブテレビアプリケーションおよびテレビ番組の配信を説明するブロック図が示されている。放送局１０は、いくつかの番組ソース１１を有する。これらのソースは、離れた放送ネットワークフィード、ビデオレコーダ、コンピュータ、データ記憶装置等を備え得る。ソース１１は、インタラクティブテレビ信号に含まれることになる、インタラクティブまたは制御情報、音声情報、および／または映像情報を提供し得る。ソース１１により提供される情報は、概して、バンド幅の節約のために、圧縮ユニット１２により圧縮され得る。Ｍｏｔｉｏｎ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔ　Ｇｒｏｕｐ（ＭＰＥＧ）の圧縮基準の内の１つのような、多数の圧縮アルゴリズムの内のいずれかが用いられ得る。適切な圧縮アルゴリズムの選択は、中でも、圧縮される情報および伝送媒体のタイプに依存する。例えば、同調関連づけ音声および映像信号（ｓｙｎｃｈｒｏｎｉｚｅ　ａｓｓｏｃｉａｔｅｄ　ａｕｄｉｏ　ａｎｄ　ｖｉｄｅｏ　ｓｉｇｎａｌｓ）に、タイムスタンプが加えられもし得る。ある情報は、容易に、または効果的に圧縮され得ないので、その情報を圧縮せずに、情報の内のいくつかが、ソースからパケット化ユニット（ｐａｃｋｅｔｉｚａｔｉｏｎ　ｕｎｉｔ）１３まで直接送信され得る。パケット化ユニット１３は、圧縮された（または圧縮されていない）情報を受け取り、且つそれを放送チャネル上の伝送のためにパケットにフォーマットする。情報のパケット化は、下記において詳述する。パケットは、伝送の前にそのパケットを点在させる、多重化ユニット１４へと供給される。この点在されたパケットは、次に受信局２０へと送信される。（図面には、１つの受信局のみが示されているが、音声映像インタラクティブ信号は、加入受信局のグループへと送信されることが意図される。）この図面では、音声映像インタラクティブ信号は、アンテナ１５による衛星放送を介して伝送されているように図示されている。

【００１８】

放送信号は、通信衛星１８により中継され、且つ受信局２０により受信される。図面は、衛星伝送を図示しているが、いずれの放送媒体（例えば、ＣＡＴＶ、または直接衛星伝送

）が用いられ得ることが考えられる。（本発明の別の実施形態は、ポイントツーポイント、または他のタイプのデータ配信システムを用いて実行され得ることに留意されたい。）受信局２０は、放送局１０を運営している放送サービス提供者の加入者である多数の局の内の１つであると考えられる。放送信号は、受信アンテナ２１により集められ、本実施形態においては、セットトップボックスである、受信器２２へと供給される。セットトップボックス２２は、信号に組み込まれたテレビ番組およびインタラクティブアプリケーションを復元するために、パケット化された信号を処理する。この復元されたアプリケーションは、セットトップボックス内で実行される一方で、復元されたテレビ番組が、それらが表示されるテレビへと送信される。インタラクティブアプリケーションは、表示される以前にテレビ番組と組み合わせられるグラフィックスまたは音声を生成し得る。

【００１９】

放送局と、受信局との間の放送チャネルに加えて、（ｈｔｔｐ、またはハイパーテキスト転送プロトコル、チャネルとも呼ばれ得る）モデムチャネル等の他のチャネルが存在し得る。これらのタイプのチャネルは、システム内で２つの機能の役割を果たす。１つは、セットトップボックスが、放送局へフィードバックを提供することを可能にすることであり、もう１つは、送信されるソース１２から受信局２０までの、番組およびアプリケーションのための別の経路を提供することである。

【００２０】

図２を参照して、セットトップボックス２２のブロック図が示されている。放送信号が受信され、チューナー３１へと供給される。チューナー３１は、放送音声映像インタラクティブ信号が伝送されるチャネルを選択し、且つその信号を処理ユニット３２へと渡す。（チューナー３１は、各種の信号ソースから信号を受信するための他の手段、本明細書中において、入力ポートとまとめて呼ばれるもの全てのもの、と置き換えられ得る。）処理ユニット３２は、必要であれば、放送信号からパケットを分離し、且つ信号に組み込まれたテレビ番組および／またはインタラクティブアプリケーションを復元する。次いでその番組およびアプリケーションは、展開ユニット３３によって展開される。信号に組み込まれたテレビ番組と関連づけられた音声および映像情報が、次に、ＮＴＳＣまたはＨＤＴＶ音声／映像等の適切なテレビ方式への情報のさらなる変換および処理を実行し得るディスプレイユニット３４へと搬送される。放送信号から復元されたアプリケーションは、ランダムアクセスメモリ（ＲＡＭ）３７へと送られ、且つ制御ユニット３５により実行される。

【００２１】

制御ユニット３５は、マイクロプロセッサ、マイクロコントローラ、デジタルシグナルプロセッサ（ＤＳＰ）、または他のタイプのソフトウェア命令処理装置を備え得る。ＲＡＭ３７は、セットトップボックスの機能をサポートするために必要とされる、静的（例えば、ＳＲＡＭ）、動的（例えば、ＤＲＡＭ）、揮発性または不揮発性（例えば、ＦＬＡＳＨ）であるメモリユニットを備え得る。セットトップボックスに電力が与えられるときに、制御ユニット３５は、ＲＯＭ３６内に格納されたオペレーティングシステムコードを実行する。通常のパーソナルコンピュータ（ＰＣ）のオペレーティングシステムコードと同様に、セットトップボックスが駆動される間、オペレーティングシステムコードは、連続して実行し、且つセットトップボックスを制御情報に従って作用させ、且つインタラクティブおよび他のアプリケーションを実行させる。セットトップボックスはまた、モデム３８を備える。モデム３８は、視聴者データがそれにより放送局へと伝送されるリターンパス、および放送局がそれによりデータをセットトップボックスへ伝送できる別の経路の両方を提供する。

【００２２】

「セットトップボックス」なる用語が、本明細書中において用いられるが、この用語が、伝送された信号を受信および処理し、且つその処理した信号をテレビまたは他のモニタへと伝達するための、いずれの受信器または処理ユニットを示すことを理解されたい。セットトップボックスは、テレビの上に物理的に置かれるハウジング内に存在し得るが、テレビ外部の他の場所にも（例えば、テレビの横または裏側、またはテレビから離れて）存在

し得、また、テレビ自体にも組み込まれ得る。セットトップボックス２２は、放送局１０から受信した信号を復調し、且つ異なるテレビ番組およびインタラクティブアプリケーション等の信号のコンポーネントを分離する役割をする。同様に、テレビ２３は、いずれの適切なテレビ方式（例えば、ＮＴＳＣまたはＨＤＴＶ）を用いるテレビ、または映像モニタであり得、またはビデオレコーダ等の他のデバイスに置きかえられ得る。

【００２３】

受信局は、放送チャネルにより放送局と効果的に接続される。この放送チャネルは、各種の伝送媒体を利用することが可能であり、且つ（例えば、直接衛星伝送のために用いられるような）同軸ケーブルおよびフリースペース等の媒体を含むと見なされる。放送チャネルは、放送局と、受信局との間に伝送経路を形成する。放送局および受信局はまた、リターンパスにより接続される。リターンパスは、概して一方が受信局にあり、且つもう一方が放送局にある１対のモデムからなり、それぞれが標準的な電話回線に接続される。リターンパスを確立するための他の手段、例えば、伝送経路のバンド幅の一部を用いること、も考えられる。

【００２４】

図３を参照して、アプリケーションまたはカルーセルは、一連のモジュールから成り、そのモジュールの内の１つはディレクトリモジュールである。ディレクトリモジュールは、唯一的な識別子を有するので、さらなる情報なしで、伝送中に識別することができる。ディレクトリモジュールは、アプリケーション内のモジュールのそれぞれに対する入力を備え、ディレクトリモジュール内の対応する入力を有しないいずれのモジュールも、アプリケーションによっては認識されない。ディレクトリモジュールは、インタラクティブテレビ受信器が、番組の実行に必要であり得るアプリケーションの全ての部分（すなわち、モジュール）にアクセスすることを可能にするために十分な情報を含む。ディレクトリモジュールは、残りのモジュールが適切に解釈されることができるように、アプリケーションの他のモジュールの前にアクセスされなければならない。ディレクトリモジュールは、アプリケーションのモジュールが伝送されるサイクルの間、他のモジュールへの実質的なランダムアクセスに利用できることを確実にするために、数回伝送され得る。

【００２５】

全てのアプリケーションのディレクトリモジュールは、共通のフォーマットを有する。このフォーマットは、長さが固定されたコンポーネントを有する部分、長さが変化するコンポーネントを包含する部分、および認可情報を有する部分の３つの部分から成る。この長さが固定された部分は、アプリケーションおよびアプリケーション内の各モジュールに関するデータを含む。長さが変化する部分は、モジュール名およびモジュールのハッシュに関するストリングデータを含む。認可部分は、作成者認可およびディレクトリ署名を含む。

【００２６】

１つの実施形態において、アプリケーションは、自動的にダウンロードされ、且つ実行される、少なくとも１つのモジュールを備える。データまたはさらなるコードを含む他のモジュールは、すぐには必要とはされ得ないので、アプリケーションが実行が開始された後にダウンロードされ得る。これらのモジュールのダウンロードは、タイミングの制約を受けやすいが、インタラクティブテレビシステムは、これらの制約を考慮に入れ、且つ時宜にかなった方法でモジュールを搬送するように構成され得る。必要であれば、これらのモジュールの内の１つが、必要に応じて受信されたかを検証するために、他のモジュールまたはデータと多重化され得る。

【００２７】

図４を参照して、モジュール５１のそれぞれは、データセグメント５２、およびＣＲＣセグメント５３を有する。ディレクトリモジュールのデータセグメント５２は、上述されている。残りのモジュールのデータセグメント５２は、アプリケーションコードまたは生データ等のいずれのタイプのデータを含むことが可能である。各モジュールのＣＲＣセグメント５３は、エラー制御のために用いられ、且つモジュール５１全体について計算される

。モジュール５１のそれぞれは、唯一的な識別子を有する。

【００２８】

モジュール５１が伝送される前に、伝送ユニット５４へとフォーマットされる。説明の都合上、番号は同じであるが文字が異なる参照符号が付けられた項目（例えば、５４ａ、５４ｂ、５４ｃ）は、番号のみで（例えば、５４）ひとまとめにして示される。伝送ユニット５４のそれぞれは、伝送ユニットのストリーム内で、伝送ユニット５４を唯一的に識別するヘッダ情報５５、および伝送されるモジュールの一部を備えるデータ５６を含む。ヘッダ５５は、伝送ユニット５４が、完全なモジュール５１へと復元することを可能にする、モジュールＩＤ、モジュールオフセット（ｍｏｄｕｌｅ　ｏｆｆｓｅｔ）、およびサイズ等の情報を含む。特定のモジュール５１を備える伝送ユニット５４は、伝送ストリーム内の他の伝送ユニット５４とインターリーブされ得る。モジュール５１の最後の伝送ユニット５４は、ＣＲＣ５３を伝達する。

【００２９】

伝送ユニット５４の方式は、伝送媒体に依存するが、概して一連の固定された長さ（最後のパケットは適切な長さにするために引き延ばされ得る。）のパケットを用いる。一連のパケットにおける第１のパケット５８は、伝送ユニット５４のヘッダ情報を伝達する。このヘッダパケット５８は、ＣＰＵ内の割り込みを生成することが可能であり、且つＣＰＵがモジュール５１にデコードされるべきかどうか、およびどこでメモリにロードするべきかを判定することが可能な情報を含む特別なパケットである。直接衛星伝送におけるヘッダパケット５８は、割り込みを生成することが可能な、補助的なパケットを利用する。直接衛星伝送における残りのパケット５８は、単に伝送ユニットデータを伝達する、基本型のパケットを利用する。

【００３０】

放送局からインタラクティブテレビ受信器への音声映像インタラクティブ伝送は、一連の伝送ユニットを備える。所与のモジュールを形成する伝送ユニットは、概して、他の情報と時間多重化（ｔｉｍｅ　ｍｕｌｔｉｐｌｅ）される。この情報は、別のモジュール、または圧縮された音声もしくは映像の伝送ユニットからなり得る。インタラクティブテレビ受信器により受信される伝達ユニットは、個々のアプリケーションモジュールへと復元される。

【００３１】

図５を参照して、放送局１０から受信局２０へと伝送される信号の概略図が示される。いくつかの番組ソースのパケットは、必要であれば、単一の伝送ストリームへと多重化され得る。これらのパケットは、各種アプリケーションまたはテレビ番組ごとのデータを含み得る。図示された伝送ストリームは、２つのインタラクティブアプリケーションモジュール（Ｍ１、Ｍ２）のパケットはもちろん、テレビ番組の音声（Ａ）および映像（Ｖ）パケットを含む。パケットは、上記で説明したように、パケットを個々の番組およびモジュールへと復元できるようにフォーマットされる。いくつかのモジュールは、伝送信号内にそれらのパケットを組み込むことにより、同時に伝送することができることに留意すべきである。この図は、モジュールおよびテレビ番組のパケットの時間多重化を図示している。そのモジュールは、一緒に伝送される、同じカルーセルに属する必要はない。概して、伝送されなければならない映像データの量がより多い結果、概して、特定のテレビ番組のための映像データのパケットは、その番組のための音声データのパケットよりも多いことは、図面から読み取ることが可能である。

【００３２】

放送信号は、セットトップボックス２２により受信される。セットトップボックス２２はまた、ｈｔｔｐ信号を受信するためのモデム接続を有し得る。セットトップボックス２２は、インタラクティブテレビアプリケーションの実行のために必要とされるモジュールに対応するパケットを検出するように構成されている、モジュール管理ユニットを含むと考えられる。モジュールが、個々のアプリケーションの実行を開始する必要は必ずしもないが、アプリケーションが実行を開始した後に、そのアプリケーションによりリクエストさ

れ得る。

【００３３】

セットトップボックス２２は、パケットを分離する、つまり、モジュールデータを含むパケットを、テレビ番組のための音声および映像を含むパケットから分離する。モジュール管理ユニットは、モジュールパケットを検知し、且つこれらのパケットが実行アプリケーションによって必要とされるモジュールに対応するかどうかを判定する。セットトップボックスは、次に、その対応するパケットからモジュールを復元し、且つ関連づけられた音声および映像データを含むパケットからテレビ番組を復元する。上記の説明のとおり、モジュールは、制御ユニット３５内で実行しているアプリケーションにより使用可能である、ＲＡＭ３７内に格納される。

【００３４】

所与のカルーセル内のモジュールは、一般に、複数のモジュールが相互にアクセスするように意図する、単一の作成者により作成される。それらのモジュールの内の１つが別のモジュールに対して何らかのアクションをとる必要があれば、第１のモジュールは、適切な許可を有すると推測される。第１のモジュールのアクションに制限があれば、その制限を守らせることはプログラマーの責任である。それゆえ、概して、セキュリティメカニズムがこれらのモジュール間のアクセスを制限する必要がない。上記で指摘したとおり、しかしながら、アプリケーションは、他のカルーセルに属するモジュールと相互作用するように設計され得るか、または全てのモジュールによって許可されていないなんらかのアクションを取るように設計され得る。それゆえ、システムおよびアプリケーションの安全等の目的のために、１つのカルーセル内のモジュールが、制限された動作を実行することを許可されるかどうかを制御するセキュリティデバイスを実現することが望ましい。（モジュールは、制限された動作を実際に実行し得るが、アクセス権は、一般にカルーセルごとに、これを基礎として認められるので、以下の説明は、カルーセルへの権利の認可に関する。）

モジュールは、信用証明を用いて制限された動作を実行する許可を獲得し得る。信用証明は、概して、カルーセルを識別する情報のセットであり、且つその制限された動作を実行するモジュールの権限の証拠として得ることが可能である。制限された動作は、インタラクティブテレビシステム内でのアプリケーションにより実行される動作の内のいずれか１つであり得る。例えば、その動作は、アプリケーションが、別のアプリケーションの実行を一時停止するまたは再開するか、他のアプリケーションにより生成された表示を隠するかまたは示すか、あるいは他のアプリケーションへとメッセージを送信するか、のうちの１つあり得る。これらの例は、許可されることが可能な権利のいくつかを例示するためだけのものであり、網羅的なリストを意図するものではない。

【００３５】

１つの実施形態において、カルーセルの作成者は、選択されたアプリケーションが、カルーセル内に格納されたアプリケーションの実行を開始または終了させるように意図された信用証明を作成し得る。例えば、カルーセルは、インタラクティブテレビユーザがクレジットカード取引を介して買い物をすることを可能にする、電子商取引アプリケーションを含み得る。あるオンラインショッピングアプリケーションは、買い物をするために、クレジットカード取引アプリケーションを開始するための権限を与えられ得る。これらの同じアプリケーションは、または異なるアプリケーションのセットであり得るが、取引を停止または完了することができなければ、そのクレジットカードアプリケーションを終了する権限を与えられ得る。クレジットカードアプリケーションを開始したアプリケーションは、よって、クレジットカード取引を完了することができないにも関わらず、制御を回復し、且つ実行を再開することができる。

【００３６】

この例において、クレジットカードアプリケーションの作成者は、信用証明を作成し、且つその信用証明を、クレジットカードアプリケーションにアクセスしたい人（例えば、そのアプリケーションの使用を許可された人）である、他の作成者へその信用証明を配信す

る。この信用証明は、安全な手段により作成されることが可能であるので、その信用証明が実際にそのクレジットカードアプリケーションの作成者（「譲渡人カルーセル（ｇｒａｎｔｏｒ　ｃａｒｏｕｓｅｌ）」と呼ばれ得る）により作成されたかどうかを、ランタイム時に判定することが可能である。例えば、その信用証明は、信用証明の権限を認める認可を組み込むことが可能である。その信用証明が配信される作成者は、その信用証明を、クレジットカードアプリケーションを開始／終了することを必要とし得る、自身のカルーセル（「譲受人カルーセル（ｇｒａｎｔｅｅ　ｃａｒｏｕｓｅｌ）」と呼ばれ得る）に組み込むことが可能である。信用証明は、システム内に格納され得るので、そこに組み込まれた情報はアプリケーションの受信または実行時に利用できる。

【００３７】

信用証明は、概して単にアプリケーション自身の有効性を認可するため、およびアプリケーションの作成者を識別するためにに用いられる、認可とは性質が異なることに留意されたい。システムは、アプリケーションの作成者と関連づけられたある権利および／または制限（例えば、ある作成者のみが、モデムを使用するアプリケーションを作成することが許可され得る）を意味し得る。

【００３８】

１つの実施形態において、あるアプリケーションが、同時に実行することが許可され得る一方で、他のアプリケーションが、そのように実行することを禁じられる。信用証明は、アプリケーションの同時実行を制御するために用いられれ得る。信用証明は、第１のアプリケーションと同時に実行を許可される、１以上のアプリケーションを示すデータを含み得る。第１のアプリケーションが実行していれば、第２のアプリケーションを実行する試みは、システムに第２のアプリケーションが同時に実行を認められるかどうかを判定する適切な信用証明をチェックさせる。信用証明は、第２のアプリケーションが同時に実行することが認められることを示せば、その第２のアプリケーションが開始される。そうでない場合、第２のアプリケーションは開始されない。別の実施形態において、信用証明は、第１のアプリケーションと同時の実行を許可しない、１以上のアプリケーションを示すデータを含み得る。この例では、第２のアプリケーションを実行する試みは、システムに、第２のアプリケーションが同時に実行することを禁じるかどうか判定するために適切な信用証明をチェックさせる。第２のアプリケーションの開始は、次に、信用証明に含まれるデータに基づいて、認められるか、または禁止される。

【００３９】

１つの実施形態において、信用証明は、クレジットカードアプリケーションを開始／終了することを許可されることを検証するように、インタラクティブテレビシステムに譲受人カルーセルにより提供される。システムは、アプリケーションを開始／終了するために、信用証明および対応する権利の検証をする際に、このアクションを取ることを可能にする。インタラクティブテレビシステムは、信用証明に特定された作成者およびアプリケーションＩＤを、クレジットカードおよび譲受人カルーセルと比較することによって、信用証明を検証する。システムはまた、信用証明の有効期間満了日により判定されるとおり、信用証明が期限切れでないことを検証する。信用証明の検証は、他のカルーセルへのアクセスをリクエストするアプリケーションの実行前または後のどちらかに実行され得る。他の実施形態において、信用証明は、アプリケーションとは別に、システムへと伝送され得る。例えば、セットトップボックスは、セットトップボックスで実行されるアプリケーション全てに対する制限されたアクセスおよび動作を制御する、信用証明の集合を定期的にロードされ得る。

【００４０】

別の実施形態において、制限されたアクションは、別のカルーセルまたはアプリケーションとの相互作用を必要とはし得ない。制限されたアクションは、その代わりに、システムリソースの使用等の機能を必要とし得る。例えば、あるアプリケーションは、セットトップボックス内のメモリの制限された部分へのアクセスを許可するか、またはリターンパスを介した放送局へのデータ伝送を許可され得る。この場合、信用証明は、放送サービス提

供者、またはインタラクティブテレビシステムの所有者により作成され得る。信用証明は、制限されたシステムリソースへのアクセスが認められた、アプリケーションの作成者へと配信され得る。実行時に、信用証明は、インタラクティブテレビシステムへ提供され、適切なリソースへのアクセスが許可される。

【００４１】

信用証明の構造を説明する前に、「公開鍵」暗号化を用いる、さまざまなセキュリティシステムが存在することに留意されたい。公開鍵暗号化システムが、各種の暗号アルゴリズムを用い得る。１つの実施形態は、ＲＳＡ（Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ　＆　Ａｄｌｅｍａｎ）およびＤＥＳ（データ暗号規格）アルゴリズムを用いる。公開鍵暗号化は、一方は、個人鍵と呼ばれ、もう一方は、公開鍵と呼ばれる、１対の暗号鍵を利用する。この個人鍵は、その所有者により秘密にされる一方で、公開鍵は，自由に利用できる。個人鍵を用いて暗号化された１つのメッセージまたは他のファイルは、その個人鍵のみで解読されることができる。同様に、個人鍵で暗号化されたファイルは、公開鍵を用いてのみ解読可能である。あるメッセージが、それらの鍵の内の１つを用いて暗号化されているときに、見掛け上ランダムな文字の集合に変換される。よって、公開鍵を用いて暗号化されたメッセージが、個人鍵の所有者へ送信されるときに、送信者は、たとえそのメッセージが傍受できるとしても、意図された受信者（個人鍵を持っている）のみがそれを解読し、そのメッセージを読むことができることを確信することができる。暗号化ではなく、メッセージが署名されているときに、そのメッセージは、判読できる形式のままであるが、暗号化された署名はそのメッセージに添付される。そのメッセージを目にする人は誰でも、それを読むことができる一方で、その署名は、そのメッセージが、個人鍵の所有者から発信されたことを検証するために用いることが可能である。さらに、その署名を暗号化するアルゴリズムは、署名に優先するメッセージにある程度依存するので、そのメッセージへのいかなる変更も、署名を検証できないものにする。署名は、それゆえ、メッセージが改変されないことを確実にするために用いることを可能にする。

【００４２】

図６ａを参照して、単純な信用証明データ構造６０を説明する図が示される。この信用証明および図６ｂに示す信用証明は、他の制限されたアクセスと同様に、カルーセル間のアクセスのために用いられ得る。下記の説明は、カルーセル間のアクセスに集中しているが、これらの信用証明は、いずれのタイプの制限またはその組み合わせたものを識別するために用いることができ、その例は、限定ではなく、例示的であることに留意されたい。

【００４３】

信用証明６０は、譲渡人カルーセル情報、譲受人カルーセル情報、有効期間満了日、および作成者認可を含む。信用証明は、その権限の検証を可能にするために署名される。譲渡人カルーセル情報は、譲渡人カルーセルの作成者ＩＤ６１、およびカルーセルＩＤ６２を含む。同様に、譲受人情報は、譲受人カルーセルの作成者ＩＤ６３、およびカルーセルＩＤ６４を含む。有効期間満了日６５は、信用証明が有効である期間を制限するために、信用証明内に含むことができる。例示された信用証明はまた、許可データ６８を含む。このデータは、譲受人カルーセルが、制限されたリソースにアクセスするか、または他の制限された動作を実行することに対する許可を識別する。許可データ６８は、カルーセルの許可を識別するために適したいずれのタイプのデータから成り得る。１つの実施形態において、許可データ６８は、ビットの所定の位置に対応する、特定の許可を肯定または否定する個々のビットを含む一方で、別の実施形態においては、特定の許可をはっきりと識別する複数のバイトを含み得る。このデータは、カルーセルと関連づけられた任意の権利または制限を識別するために用いられ得、リソースアクセス制限に限定されないことに留意されたい。

【００４４】

信用証明は、作成者認可６６を含む。作成者認可６６は、信用証明に権限を持たせ、且つその作成者により作成されたものであることを保証するために用いられる。作成者認可６６は、信頼されたある関係者により署名された、作成者の公開鍵を含む。（信頼された関

係者は、鍵の権限を保証することができる人である。信頼される関係者の署名は、暗号化され、鍵に組み込まれる。）信頼された関係者の鍵は、周知のものである。すなわち、システム内に格納され、常にシステムで利用可能である。信用証明６０の全体は、次に、作成者の個人鍵で署名６７され、信用証明６０内のデータのいずれも修正することができないことを確実にする。同様のタイプの信用証明は、受信局が放送サービス提供者により届けられるモジュールの機能を制御するために、放送サービス提供者により用いられ得る。

【００４５】

カルーセルへのアクセスを必要とするアプリケーションの各インスタンスの単一の信用証明の使用が、結果的に、譲受人カルーセルにより維持される必要があり得る非常に多くの信用証明を生じることを可能にする。あるカルーセルが、他の作成者による他の多くのカルーセルへのアクセスを必要とし得るのであれば、１つの信用証明は、それらのカルーセルのそれぞれに対して必要とされる。そのような多くの数の信用証明を作成し、且つ維持することは、作成者間で多くの調整を要し得る。信用証明システムは、それゆえ、そのシステムが提供するセキュリティのを恩恵より重要であり得る、実質的なオーバーヘッドを作成することが可能である。

【００４６】

１つの実施形態において、この問題は、信用証明に多くの譲受人アプリケーション（作成者ＩＤおよびアプリケーションＩＤによって）、および１以上の譲渡人アプリケーションを列挙させることにより、アドレス可能である。例えば、図６ｂに示されるとおり、信用証明は、単一の譲渡人作成者ＩＤ７１、有効期間満了日７２、および許可データ７８を含み得る。信用証明は、次に、それぞれが、譲渡人ＩＤ７４、譲受人作成者ＩＤ７５、および譲受人アプリケーションＩＤ７６を有する、いくつかの連続したＩＤ７３ａ～７３ｃを列挙し得る。その情報のそれぞれは、よって、譲渡人作成者により所有される１つの譲渡人アプリケーション／カルーセル、および識別された譲渡人アプリケーションにアクセスする権限を与えられている１つのアプリケーションを識別する。譲受人アプリケーションは、上述のとおり、譲受人作成者ＩＤ７５および譲受人アプリケーションＩＤ７６により識別される。信用証明は、認証ののための、署名された作成者認可７７を含み、信用証明全体は、先に説明した信用証明と同様の方法で、署名７９される。

【００４７】

１つの実施形態は、所与のカルーセルのために維持されなければならない信用証明の潜在的な数をさらに低減するようにワイルドカードを用いる。譲受人の作成またはアプリケーションＩＤ、または譲渡人のカルーセルのアプリケーションＩＤは、ワイルドカードに置きかえられ得る。このワイルドカードは、ワイルドカードとしてあらかじめ定義された、特定のＩＤである。例えば、全てが０、または全てが１を有するＩＤは、ワイルドカードであるように定義され得る。信用証明が、検証のためにシステムに提供されるとき、ワイルドカードが、比較される全てのＩＤと等しく一致するものと考えられる。本実施形態において、システムｈａ、譲渡人が実際に信用証明の作成者であることを検証することが可能でなければならないので、譲渡人の作成者ＩＤはワイルドカードにすることはできない。譲渡人アプリケーションＩＤがワイルドカードであれば、特定された譲受人は譲渡人の作成者カルーセルの全てにアクセスし得る。その譲受人アプリケーションＩＤがワイルドカードであれば、特定された譲受人（作成者）は、特定の譲渡人カルーセルにアクセスし得る。譲受人の作成者ＩＤおよび譲受人アプリケーションＩＤが、ともにワイルドカードであるならば、いずれのカルーセルも、特定された譲渡人カルーセルにアクセスすることができる。ワイルドカードは、上述の信用証明のいずれか（すなわち、単一の譲渡人、単一の譲受人信用証明、または複数の譲渡人／譲受人信用証明）とともに用いられることが可能である。

【００４８】

上記の実施形態が、カルーセルレベルで信用証明を利用する一方で、別の実施形態は，モジュールレベルで信用証明または他のセキュリティ手段を実現し得ることが考えられる。別のセキュリティ手段は、モジュールを暗号化すること、モジュールに対するハッシュ機

能の実行すること、および対応するディレクトリモジュール等のハッシュ値を含むことを含み得る。ディレクトリモジュールでの信用証明化または他のセキュリティは、概して、例えば、ディレクトリモジュール内の他のモジュールのハッシュ値の挿入の後に実現される。

【００４９】

カルーセル間のアクセスのための、上述のものと同様の暗号化システムは、カルーセル、またはセットトップボックスにより受信されたカルーセルまたはモジュールの認証を検証する目的のためにも用いられ得る。カルーセル（さらに詳細には、そのディレクトリモジュール）は、作成者の個人鍵で暗号化された認可を含み得る。セットトップボックスは、作成者の公開鍵のコピーを有しているが、その個人鍵を用いて認可を解読することにより、カルーセルがその作成者から来たことを検証かることができる。上記のとおり、ハッシュ機能の使用は、ディレクトリモジュールでないものの認証を確実にするためにも用いられ得る。

【００５０】

さらに、上記の信用証明システムは、インタラクティブテレビ以外の環境でのアプリケーションの実行にも拡張することができる。例えば、システムは、汎用デスクトップコンピュータにおいて、そのコンピュータ上のアプリケーションの実行を制御するように実現され得る。このような別の実施形態は、上述の方法で作動することが可能であるが、アプリケーションおよび信用証明をシステムへ搬送するための手段が、その特定の環境に提供するように適合され、そのアプリケーションの出力は、テレビ上の表示内容とインタラクティブまたは適していないかもしれない。

【００５１】

上述の特定の実施形態の詳細は、添付の請求の範囲により定義される、本発明の精神および範囲から逸脱することなく修正され得る。上述の実施形態は、従って、限定ではなく、例示的なものとして意図する。各書修正および別の実施形態が、当業者には明白であるものと考えられる。

【図面の簡単な説明】

【図１】　図１は、ソースから一連の視聴者までの、インタラクティブテレビアプリケーションおよびテレビ番組の配信を説明するブロック図である。

【図２】　図２は、本発明の１つの実施形態において用いられるセットトップボックスのブロック図である。。

【図３】　図３は、本発明の１つの実施形態におけるカルーセルのコンポーネントモジュールおよびモジュールの伝送順序の説明である。

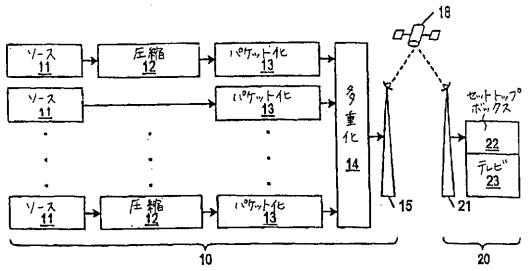
【図４】　図４は、本発明の１つの実施形態において、モジュールを含むデータがパケット化されている方式を説明するブロック図である。

【図５】　図５は、本発明の１つの実施形態において、放送局から受信局まで伝送される信号の概略図である。

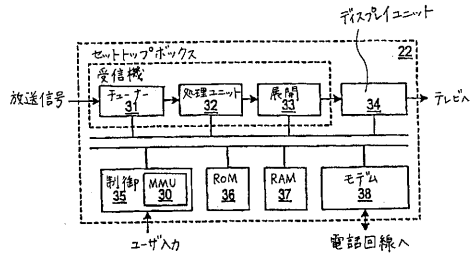
【図６ａ】　図６ａは、本発明の１つの実施形態において用いられる信用証明のデータ構造を説明するブロック図である。

【図６ｂ】　図６ｂは、本発明の別の実施形態において用いられる信用証明のデータ構造を説明するブロック図である。

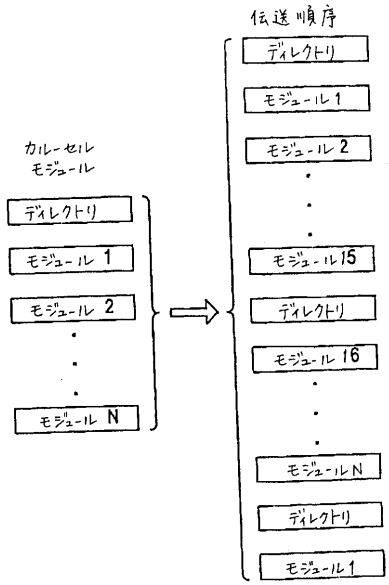
【図１】



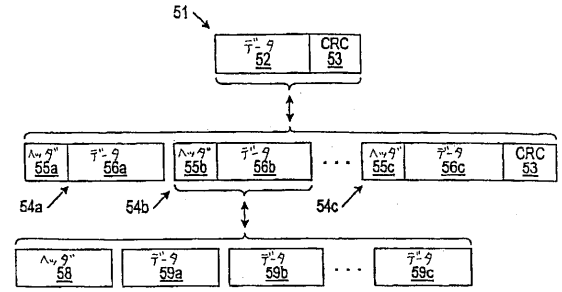
【図２】



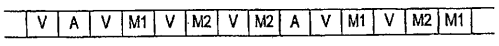
【図３】



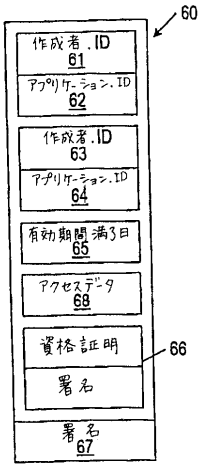
【図４】



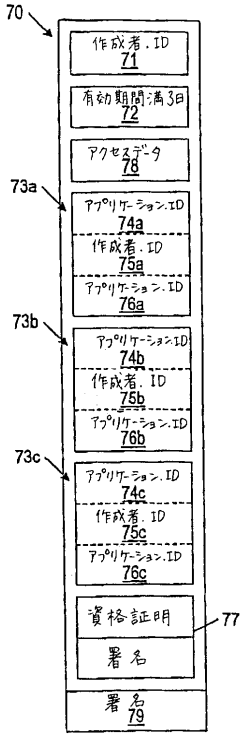
【図５】



【図６ａ】



【図６ｂ】


70
作成者.ID
71
有効期間満了日
72
アクセスデータ
78
73a
アプリケーション.ID
74a
作成者.ID
75a
アプリケーション.ID
76a
73b
アプリケーション.ID
74b
作成者.ID
75b
アプリケーション.ID
76b
73c
アプリケーション.ID
74c
作成者.ID
75c
アプリケーション.ID
76c
資格証明
77
署名
署名
79

フロントページの続き

(72)発明者 メナンド, ジーン レーヌ
アメリカ合衆国 カリフォルニア ９４３０３, パロ アルト, エンバラカデロ ロード １１０２
(72)発明者 ドゥレウ, ビンセント
アメリカ合衆国 カリフォルニア ９４３０６, パロ アルト, サウス コート ３５１９

審査官 川崎 優

(56)参考文献 特開平０９－１２１３４０（ＪＰ, Ａ）
国際公開第９８／４３４３１（WO, Ａ１）
国際公開第９９／１８７２４（WO, Ａ１）
国際公開第９９／２２５１６（WO, Ａ１）
Macq,B.M and Quisquater J-J., Cryptology for Digital TV Broadcasting, Proceedings of IEEE, １９９５年 ６月 １日, P.944-957

(58)調査した分野(Int.Cl., ＤＢ名)
H04N 7/16-173
H04L 9/08
H04H 20/00-60/98
G06F 9/445,21/22-24