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

特許第5149385号
(P5149385)

(45)発行日　平成25年2月20日(2013.2.20)　(24)登録日　平成24年12月7日(2012.12.7)

(51)Int.Cl.			F I		
H04N	7/173	(2011.01)	H04N	7/173	630
G06F	13/00	(2006.01)	G06F	13/00	358A
H04L	12/46	(2006.01)	H04L	12/46	100Z

請求項の数 10　(全 23 頁)

(21)出願番号	特願2010-520933 (P2010-520933)
(86)(22)出願日	平成20年8月4日 (2008.8.4)
(65)公表番号	特表2010-536302 (P2010-536302A)
(43)公表日	平成22年11月25日 (2010.11.25)
(86)国際出願番号	PCT/KR2008/004503
(87)国際公開番号	WO2009/022802
(87)国際公開日	平成21年2月19日 (2009.2.19)
審査請求日	平成22年2月10日 (2010.2.10)
(31)優先権主張番号	60/955,125
(32)優先日	平成19年8月10日 (2007.8.10)
(33)優先権主張国	米国(US)
(31)優先権主張番号	60/957,708
(32)優先日	平成19年8月23日 (2007.8.23)
(33)優先権主張国	米国(US)

(73)特許権者　502032105
エルジー　エレクトロニクス　インコーポレイティド
大韓民国，ソウル　１５０－７２１，ヨンドゥンポ－ク，ヨイド－ドン，２０
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100114018
弁理士　南山　知広
(74)代理人　100151459
弁理士　中村　健一

最終頁に続く

(54)【発明の名称】コンテンツ共有方法

(57)【特許請求の範囲】

【請求項１】

受信デバイスを用いたコンテンツ共有方法において、

サービスプロバイダからコンテンツを受信する段階と、

ターゲットデバイスで支援されるコンテンツ保護ソリューションを検出する段階と、

前記検出されたコンテンツ保護ソリューションに基づいて前記コンテンツを、前記ターゲットデバイスおよび前記受信デバイスのうちいずれか一つで支援されるコンテンツ保護ソリューションに適するように変換する段階と、を含み、

前記受信デバイスは、前記受信デバイスの認証書中に前記受信デバイスのセキュリティ特性を表すセキュリティソリューションレベルを含み、

前記セキュリティソリューションレベルは、

非セキュリティ実行環境でセキュリティソリューション認証プロセスの認証および完全性チェックを実行しないセキュリティレベルを表すレベル０と、

非セキュリティ実行環境でデバイスのソフトウェアエレメントを使用してセキュリティソリューション認証プロセスの認証および完全性チェックを検証するセキュリティレベルを表すレベル１と、

非セキュリティ実行環境でデバイスのハードウェアエレメントを使用して直接的にセキュリティソリューション認証プロセスの認証および完全性チェックを検証するセキュリティレベルを表すレベル２と、

セキュリティ実行環境でデバイスのソフトウェアエレメントを使用してセキュリティソ

リューション認証プロセスの認証および完全性チェックを検証するセキュリティレベルを表すレベル３と、

セキュリティ実行環境でデバイスのハードウェアエレメントを使用して直接的にセキュリティソリューション認証プロセスの認証および完全性チェックを検証するセキュリティレベルを表すレベル４と、のうちいずれか一つであることを特徴とするコンテンツ共有方法。

【請求項２】

前記セキュリティソリューションレベルは、前記受信デバイスのセキュリティソリューション認証プロセスのセキュリティ特性情報によって分類されることを特徴とする請求項１に記載のコンテンツ共有方法。

【請求項３】

前記セキュリティソリューションレベルは、前記セキュリティソリューション認証プロセス実行環境、或いは、ソフトウェアまたはハードウェアのエレメントを使用した認証および完全性チェックに基づいて複数のレベルに分類されることを特徴とする請求項２に記載のコンテンツ共有方法。

【請求項４】

前記セキュリティソリューション認証プロセスのセキュリティ性が高いほど、前記セキュリティソリューションレベルは、高いレベルに指定されることを特徴とする請求項２に記載のコンテンツ共有方法。

【請求項５】

前記変換する段階は、

前記ターゲットデバイスで支援されるターゲットコンテンツ保護ソリューションが前記受信デバイスで支援されるコンテンツ保護ソリューションと同一である場合、前記コンテンツを前記受信デバイスで支援されるコンテンツ保護ソリューションに適するように変換する段階と、

前記ターゲットデバイスで支援されるターゲットコンテンツ保護ソリューションが前記受信デバイスで支援されるコンテンツ保護ソリューションと異なる場合、前記コンテンツを前記ターゲットコンテンツ保護ソリューションに適するように変換する段階と、

を含むことを特徴とする請求項１に記載のコンテンツ共有方法。

【請求項６】

前記サービスプロバイダからコンテンツを受信する段階は、

前記サービスプロバイダから伝送されるコンテンツを、サービス保護ソリューションおよび前記コンテンツ保護ソリューションのうちいずれか一つを使用して受信する段階を含むことを特徴とする請求項１に記載のコンテンツ共有方法。

【請求項７】

前記変換されたコンテンツを前記ターゲットデバイスに再配信する段階をさらに含むことを特徴とする請求項１に記載のコンテンツ共有方法。

【請求項８】

ホームデバイスは、前記ホームデバイスの認証書中に前記ホームデバイスのセキュリティ特性を表すセキュリティソリューションレベルを含むことを特徴とする請求項１に記載のコンテンツ共有方法。

【請求項９】

前記受信デバイスのセキュリティソリューションレベルまたは前記ホームデバイスのセキュリティソリューションレベルに基づいて前記ホームデバイスへのコンテンツ伝送が制限されることを特徴とする請求項８に記載のコンテンツ共有方法。

【請求項１０】

前記検出されたコンテンツ保護ソリューションに適するように前記コンテンツの使用に必要な情報を変換する段階と、

前記変換された情報をホームデバイスに伝送する段階と、をさらに含むことを特徴とする請求項１に記載のコンテンツ共有方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンテンツ共有方法に関し、より詳しくは、ＩＰＴＶ受信デバイスを用いてサービスプロバイダから提供されるコンテンツをホームデバイスに再配信することによってコンテンツを共有することができるコンテンツ共有技術に関する。
【背景技術】
【０００２】
最近、有線または無線ネットワークを用いたデジタルＴＶサービスが一般化されている。デジタルＴＶサービスは、既存のアナログ放送サービスでは提供できなかった多様なサービスを提供することができる。例えば、デジタルＴＶサービスの一種であるインターネットプロトコルテレビ（Internet Protocol Television；ＩＰＴＶ）サービスの場合、使用者が、視聴プログラムの種類、視聴時間などを能動的に選択することができる双方向性を提供する。ＩＰＴＶサービスは、この双方向性に基づいて多様な付加サービス、例えば、インターネット検索、ホームショッピング、オンラインゲームなどを提供することもできる。
【０００３】
このＩＰＴＶサービスのため、使用者側は、ＩＰＴＶセットボックスが提供されなければならない。ＩＰＴＶセットボックスは、双方向サービスを支援するソフトウェアがインストールされ、該ソフトウェアに基づいてサービスクライアントとしての機能を遂行することができる。例えば、ＩＰＴＶセットボックスは、ＩＰネットワークを介してサービスプロバイダと情報を送受信しながら、サービスプロバイダに放送コンテンツの伝送を要求し、サービスプロバイダから受信される放送信号を標準ＴＶ信号に変換してＴＶ受像機に送信することができる。
【０００４】
一方、最近ではＩＰＴＶサービスを家庭内のホームネットワーク環境と連係させてＩＰＴＶコンテンツの提供領域を拡張しようとする努力が試みられている。その例として、コンテンツ共有サービスがある。コンテンツ共有サービスは、ＩＰＴＶ互換端末機であるＩＰＴＶセットボックスをホームネットワークに接続されたデバイスと連動させた後、ＩＰＴＶセットボックスに格納されたコンテンツを連動させたデバイスに再配信する。従って、コンテンツ共有サービスは、ＩＰＴＶコンテンツをユーザの望む多様なデバイスで再生できるようにする。
【０００５】
このコンテンツ共有サービスのためのシステムの具現において、最も重要な点の一つは、コンテンツの格納または再配信時に発生することがある不法行為、例えば、コンテンツの不法な流出や複写などからコンテンツを安全に保護することである。従って、コンテンツの共有サービスではコンテンツの保護のためのセキュリティ手段及び手順などが不可欠に要求され、これらの要求に従って関連技術の開発が緊急に必要とされている。
【発明の概要】
【発明が解決しようとする課題】
【０００６】
本発明が解決しようとする技術的課題は、デバイスにセキュリティソリューションレベルを関連付け、デバイスのセキュリティ情報に基づいてコンテンツを再配信することができるコンテンツ共有方法を提供することである。
【課題を解決するための手段】
【０００７】
これらの技術的課題を解決するために、本発明は、一側面（Aspect）において、コンテンツ共有方法を提供する。前記コンテンツ共有方法は、受信デバイスを用いたコンテンツ共有方法において、サービスプロバイダからコンテンツを受信する段階と、ターゲットデバイスで支援されるコンテンツ保護ソリューションを検出する段階と、前記検出されたコ

ンテンツ保護ソリューションに基づいて前記コンテンツを、前記ターゲットデバイスおよび前記受信デバイスのうちいずれか一つで支援されるコンテンツ保護ソリューションに適するように変換する段階と、を含む。前記受信デバイスは、前記受信デバイスの認証書に前記受信デバイスのセキュリティ特性を表すセキュリティソリューションレベルを含む。

【０００８】

前記セキュリティソリューションレベルは、前記受信デバイスのセキュリティソリューション認証プロセスのセキュリティ特性情報によって分類（Classify）される。前記セキュリティソリューションレベルは、前記セキュリティソリューション認証プロセスの実行環境、ソフトウェアまたはハードウェアエレメントを使用した認証および完全性チェックに従って多数のレベルに分類される。前記セキュリティソリューション認証プロセスのセキュリティ性が高いほど、前記セキュリティソリューションレベルは、高いレベルに指定される。

【０００９】

前記変換段階は、前記検出されたコンテンツ保護ソリューションが前記受信デバイスで支援されるコンテンツ保護ソリューションと同一である場合、前記コンテンツを前記受信デバイスで支援されるコンテンツ保護ソリューションに適するように変換する段階と、前記検出されたコンテンツ保護ソリューションが前記受信デバイスで支援されるコンテンツ保護ソリューションと異なる場合、前記コンテンツを前記検出されたコンテンツ保護ソリューションに適するように変換する段階と、を含む。

【００１０】

前記サービスプロバイダからコンテンツを受信する段階は、前記サービスプロバイダから伝送されるコンテンツを、サービス保護ソリューションおよびコンテンツ保護ソリューションのうちいずれか一つを使用して受信する段階を含む。前記コンテンツ共有方法は、前記変換されたコンテンツを前記ターゲットデバイスに再配信する段階をさらに含む。また、前記コンテンツ共有方法は、前記検出されたコンテンツ保護ソリューションに適するように前記コンテンツの使用に必要な情報を変換する段階と、前記変換された情報を前記ホームデバイスに伝送する段階と、をさらに含む。

【００１１】

前記ホームデバイスは、前記ホームデバイスの認証書に前記ホームデバイスのセキュリティ特性を表すセキュリティソリューションレベルを含む。前記受信デバイスセキュリティソリューションレベルまたは前記ホームデバイスのセキュリティソリューションレベルに基づいて前記ホームデバイスへのコンテンツ伝送が制限される。

【発明の効果】

【００１２】

以上、説明した通り、本発明によると、受信デバイスを用いてサービスプロバイダから送信されるコンテンツをホームデバイスのセキュリティソリューションに適するように再配信することによってコンテンツを効率的に共有することができる。また、デバイス、例えば、受信デバイスまたはホームデバイスに該当デバイスのセキュリティ特性を表すセキュリティソリューションレベルを関連付け、これに基づいてコンテンツの伝送を制御することもできる。

【図面の簡単な説明】

【００１３】

【図１】本発明の望ましい実施例に係るコンテンツ共有方法のためのドメインシステムの構成を示すブロック図である。

【図２】コンテンツ共有方法を実現するためのシステム全体の構成を示す概略ブロック図である。

【図３】図２に示されているＩＰＴＶ受信デバイスの構成を示すブロック図である。

【図４】デバイスのセキュリティソリューションレベルを指定する基準になるセキュリティソリューションレベルテーブルを例示する図である。

【図５】本発明の望ましい実施例に係るコンテンツ格納方法の手順を例示するための図で

ある。
【図６】本発明の望ましい実施例に係るコンテンツ共有方法を実現するためのシステム構成を示すブロック図である。
【図７】本発明の望ましい実施例に係るコンテンツ共有方法を説明するためのフローチャートである。
【図８】本発明の望ましい他の実施例に係るコンテンツ共有方法を実現するためのシステム構成を示すブロック図である。
【図９】本発明の望ましい他の実施例に係るコンテンツ共有方法を説明するためのフローチャートである。
【図１０】サービスプロバイダ間のコンテンツ連動サービスの概念を例示するための図である。
【図１１】サービスプロバイダ間のコンテンツ連動サービスのためのシステム構造を例示する図である。
【図１２】サービスプロバイダ間のコンテンツ連動サービスの手順を例示するための図である。
【発明を実施するための形態】
【００１４】
以下、本発明が属する分野に通常の知識を有する者が、本発明を容易に実施することができるように、本発明の望ましい実施例を添付図面を参照して詳細に説明する。以下に説明する本発明の望ましい実施例では内容の明瞭性のために、特定の技術用語を使用する。然しながら、本発明は、その選択された特定用語に限定することではなく、各々の特定用語が類似目的を達成するために類似の方式に動作する全ての技術同義語を含むことを予め明らかにする。
【００１５】
図１は、本発明の望ましい実施例に係るコンテンツ共有方法のためのドメインシステムの構成を示すブロック図である。
【００１６】
図１に示されているように、ドメインシステム（１０）は、ドメイン（７）を構成する。ドメイン（７）とは、許可された（Authorized）デバイスであるドメインデバイス（５）の集合であり、ドメインサービスが適用される範囲を意味してもよい。ドメイン（７）内に含まれたドメインデバイス（５）間では、許可された権限に従ってコンテンツを共有して使用することができる。
【００１７】
ドメイン（７）は、デバイスの物理的な位置を考慮して構成することができる。即ち、特定の物理的領域内に存在するデバイスでドメイン（７）を構成することがある。このドメイン（７）を構成するためにはローカル環境が必要である。この場合、ローカル環境とは、特定のローカル領域内に属するデバイスが相互に連動することができる物理的ネットワークが備えられ、この物理的ネットワークが外部のネットワークとも連動できる環境を意味してもよい。
【００１８】
このようなローカル環境を提供することができる例として、ホームネットワークシステムを挙げることができる。ホームネットワークシステムは、有線または無線ローカルネットワークを介して家庭内の家電機器、各種センサ、セキュリティ機器などの相互連動が可能であり、ホームゲートウェイなどの通信ノードを介してインターネットなどの外部ネットワークとも連動することができる。前記ローカル環境は、このようなホームネットワークシステムだけでなく、相互連動可能な２個以上のネットワークデバイスが存在する場合に構成可能である。
【００１９】
以下、このようなローカル環境が備えられた領域をドメイン領域と呼ぶ。ドメイン領域内には多数のデバイスが存在してもよい。使用者は、これらのデバイスを用いてドメイン

（７）を構成し、ドメインデバイス（５）間でコンテンツを共有して使用することができる。ドメイン（７）への登録のために、デバイスは、ドメインアドミニストレータ（１）にドメイン登録要求を送信し、これを受信したドメインアドミニストレータ（１）は、前記ドメイン登録要求が正当な要求かどうかなどを判断した後、デバイスをドメイン（７）に登録する。ドメイン（７）に登録されたドメインデバイス（５）間では、許可された条件に従ってコンテンツを共有して使用することができる。一方、場合によっては、ドメイン領域の外のデバイス、例えば、インターネットなどを介して接続する外部領域のデバイスなどもリモート状態でドメインに登録されてもよい。

【００２０】

一方、ドメイン（７）は、ドメイン代表デバイス（３）を含んでもよい。ドメイン代表デバイス（３）は、ドメイン内でドメイン管理のためのマスタの役割を遂行するデバイスを意味してもよい。例えば、ドメイン代表デバイス（３）は、ドメインアドミニストレータ（１）を補助してドメイン管理機能、ドメインデバイス管理機能、ドメインデバイス認証機能などを遂行することもできる。また、前記ドメイン代表デバイスは、ドメイン領域内のデバイスの近接度（Proximity）測定を遂行し、該当デバイスがドメイン領域内に含まれるかどうかを検証することもできる。即ち、ドメイン代表デバイス（３）は、ドメイン（７）の物理的（例えば、ホップ数、反応時間、ＴＴＬ等）範囲を決定する機能を遂行することができる。前記近接度測定情報は、ドメインデバイス（５）をドメインに登録する時、ドメインアドミニストレータ（１）において該当ドメインデバイス（５）の認証が可能か否かを判断することができる情報として使われることもあり、ドメインデバイス（５）がローカルアクセス状態（即ち、ドメイン領域内でドメインにアクセスする状態）か、または、リモートアクセス状態（即ち、ドメイン領域の外でドメインにアクセスする状態）かを管理するための情報として使われることもある。

【００２１】

このドメイン代表デバイス（３）は、特定の時点（例えば、ドメインの初期構成、使用者からの要求、既存のドメイン代表デバイスにエラーが発生した場合等）にドメインデバイスから選出されてもよい。例えば、ドメインデバイス間でデバイス性能（Capability）情報を送受信しながら、デバイス性能をお互いに比較し、デバイス性能の高いデバイスは勝ち残り、デバイス性能の低いデバイスは負け落ちる選出競争（Election Competition）を遂行し、最もデバイス性能の高いドメインデバイス（例えば、最終的に選出競争で勝ち残ったデバイス）がドメイン代表デバイス（３）として選出されてもよく、または、各ドメインデバイスがドメインアドミニストレータ（１）または特定デバイスにデバイス性能情報を送信し、これを受信したドメインアドミニストレータ（１）または特定デバイスがデバイス性能の高いドメインデバイスをドメイン代表デバイス（３）として選出してもよい。

【００２２】

前記デバイス性能とは、該当デバイスが有するハードウェアまたはソフトウェアの性能（例えば、バッテリ容量、ハードウェア仕様、ソフトウェアの種類、特定ソフトウェアが搭載されているか否か等）を意味してもよい。一方、選出されたドメインデバイスは、ドメイン代表デバイス（３）として指定されて前記言及された機能を遂行するようになる。

【００２３】

以上、ドメインシステムの構成を説明した。このようなドメインの概念をＩＰＴＶサービスシステムに導入すれば、ＩＰＴＶサービスコンテンツを多数のデバイスで共有して使用することができるコンテンツ共有システムを構成することができる。

【００２４】

図２は、コンテンツ共有方法を実現するためのシステム全体の構成を示す概略ブロック図である。

【００２５】

図２に示されているように、ＩＰＴＶ受信デバイス（４０）は、ＩＰネットワークを介してサービスプロバイダ（２０）と連動することができる。このとき、前記ＩＰＴＶ受信

デバイス（４０）は、ＩＰＴＶサービス機能を備える端末機、例えば、ＩＰＴＶセットボックスなどを意味してもよい。ＩＰＴＶ受信デバイス（４０）は、ドメイン代表デバイスであることもある。また、このＩＰＴＶ受信デバイス（４０）は、ホームデバイス（５０）と連動することもできる。このとき、ホームデバイス（５０）は、有線または無線ネットワーク機能を備える固定またはポータブル端末機、例えば、家電機器、携帯電話、パーソナルコンピュータ（Personal Computer；ＰＣ）、ノートブック（Notebook）、携帯情報端末（Personal Digital Assistance；ＰＤＡ）、ポータブルマルチメディアプレーヤ（Portable Multimedia Player；ＰＭＰ）、リモコンなどである。

【００２６】

ＩＰＴＶ受信デバイス（４０）およびホームデバイス（５０）は、コンテンツの共有のためにドメイン（３０）に加入（join）することができる。即ち、ＩＰＴＶ受信デバイス（４０）およびホームデバイス（５０）は、ドメインデバイスとなることがある。ドメインに加入するために、ＩＰＴＶ受信デバイス（４０）およびホームデバイス（５０）は、各々サービスプロバイダ（２０）にドメイン（３０）への加入を要求し、サービスプロバイダ（２０）は、該当デバイス（４０、５０）を認証した後、そのデバイスに認証書（certificate）を発行してデバイス（４０、５０）をドメイン（３０）に登録することができる。

【００２７】

前記ドメイン（３０）への登録要求の際、ＩＰＴＶ受信デバイス（４０）またはホームデバイス（５０）は、各々自体のセキュリティ性能情報をサービスプロバイダ（２０）に提供することができる。このとき、セキュリティ性能情報は、該当デバイスに適用されているセキュリティソリューション（例えば、コンディショナルアクセスシステム（Conditional Access System；ＣＡＳ）モジュール、デジタル著作権管理（Digital Rights Management；ＤＲＭ）モジュール等）の情報、セキュリティソリューションレベルなどを含むことがある。前記セキュリティソリューションレベルは、デバイスに適用されたセキュリティソリューション認証プロセスのセキュリティレベルを表すセキュリティソリューションプロファイル情報を意味してもよい。望ましくは、セキュリティソリューションレベルは、セキュリティソリューション認証プロセスのセキュリティレベルを、決められたテーブルに基づいて分類（Classify）した情報を意味してもよい。このセキュリティソリューションレベルに関しては以後詳細に説明する。

【００２８】

サービスプロバイダ（２０）は、ＩＰＴＶ受信デバイス（４０）またはホームデバイス（５０）から受信されたセキュリティ性能情報を格納することもでき、セキュリティ性能情報（例えば、セキュリティソリューションの情報、セキュリティソリューションレベル等）のうち少なくともいずれか一つをデバイス（４０、５０）の認証書に挿入してデバイス（４０、５０）に発行することもできる。

【００２９】

一方、ＩＰＴＶ受信デバイス（４０）は、サービスプロバイダ（２０）にコンテンツ案内情報を要求してこのコンテンツ案内情報をサービスプロバイダ（２０）から受信することができる。このとき、コンテンツ案内情報は、サービスコンテンツの日程、目録、付加情報などを案内する情報であり、例えば、電子番組ガイド（Electronic Program Guide；ＥＰＧ）、コンテンツプログラムガイド（Content Program Guide；ＣＰＧ）、ＶｏＤコンテンツガイド、インタラクティブプログラムガイド（Interactive Program Guide；ＩＰＧ）などである。

【００３０】

ＩＰＴＶ受信デバイス（４０）は、サービスプロバイダ（２０）から受信したコンテンツ案内情報を使用者インターフェースに適するように加工して表示することができる。使用者は、表示されたコンテンツ案内情報から所望のサービスコンテンツを選択することができる。すると、ＩＰＴＶ受信デバイス（４０）は、選択されたコンテンツをサービスプロバイダ（２０）に要求することができる。

【００３１】
ＩＰＴＶ受信デバイス（４０）からの要求に応じて、サービスプロバイダ（２０）は、該当コンテンツをＩＰＴＶ受信デバイス（４０）に伝送する。このとき、サービスプロバイダ（２０）は、前記コンテンツとともに前記コンテンツの使用のために必要なコンテンツ関連情報、例えば、セキュリティ情報（Security Information）、使用権限情報（Usage Rights Information）、リボケーションリスト情報（Revocation List Information）などをＩＰＴＶ受信デバイス（４０）に伝送することもできる。前記セキュリティ情報は、コンテンツの使用または共有が可能なセキュリティレベル、コンテンツの使用に必要なセキュリティソリューション情報などを含んでもよい。前記使用権限情報は、コンテンツを使用するための権限情報、例えば、コンテンツのライセンスなどを含んでもよい。リボケーションリスト情報は、コンテンツの使用が禁止されるデバイスのリストであるリボケーションリストまたはそのリボケーションリストを識別できる情報を含んでもよい。
【００３２】
ＩＰＴＶ受信デバイス（４０）は、サービスプロバイダ（２０）から伝送されるコンテンツを受信し、格納および再生でき、ドメイン（３０）に登録されたホームデバイス（５０）に伝送することもできる。コンテンツの格納、再生または伝送などを遂行するためには、サービスプロバイダ（２０）から伝達されたコンテンツと関連する情報、例えば、セキュリティ情報、使用権限情報、リボケーションリスト情報などを考慮することができ、これらに基づいてコンテンツの格納、再生または伝送を制限することもできる。
【００３３】
図３は、図２に示されているＩＰＴＶ受信デバイス（４０）の構成を示すブロック図である。
【００３４】
図３に示されているように、ＩＰＴＶ受信デバイス（４０）は、ＩＰＴＶ受信モジュール（４１）、セキュリティコントローラ（４２）、セキュリティソリューション（４３）、コンテンツ再生機（４７）、 ストレージ（４８）および出力ポート（４６）などを含んでもよい。図示されていないが、ＩＰＴＶ受信デバイス（４０）は、通常のＩＰＴＶ端末機が備える機能モジュール、例えば、情報入力モジュール、ディスプレイモジュール、電源モジュールなども具備可能であることは当然であり、これらは本発明の要旨と直接的に関連のない要素であるため、別途の図示および説明は省略する。
【００３５】
ＩＰＴＶ受信モジュール（４１）は、サービスプロバイダ（２０）とデータを送受信するインターフェース機能を遂行することができる。例えば、ＩＰＴＶ受信モジュール（４１）は、サービスプロバイダ（２０）からコンテンツおよびコンテンツの使用に必要な情報、例えば、セキュリティ情報、使用権限情報、リボケーションリスト情報などを受信することができる。前記コンテンツは、特定の保護技術、例えば、コンディショナルアクセスシステム（Conditional Access System；ＣＡＳ）またはデジタル著作権管理（Digital Rights Management；ＤＲＭ）などのサービス保護技術またはコンテンツ保護技術が適用されてスクランブル（Scrambling）または暗号化（Encryption）されてもよい。一方、ＩＰＴＶ受信モジュール（４１）は、サービスプロバイダ（２０）または特定サーバからセキュリティソリューション（４３）と関連するデータ、例えば、ＤＲＭコード、セキュリティメッセージ、アプリケーションなどを受信することもできる。ＩＰＴＶ受信デバイスは、これらのデータをトランスポートストリーム（Transport Stream；ＴＳ）またはセキュリティダウンロード（Secure Download）の形式で受信することができる。
【００３６】
セキュリティコントローラ（４２）は、コンテンツおよびデバイスセキュリティのためのセキュリティ制御機能を遂行することができる。例えば、セキュリティコントローラ（４２）は、サービスプロバイダ（２０）にＩＰＴＶ受信デバイス（４０）をドメインに登録するように要求し、ドメインに登録されたことを証明する認証書を受信して格納することができる。ドメイン登録要求の際、セキュリティコントローラ（４２）は、ＩＰＴＶ受

信デバイス（４０）が備えるセキュリティソリューション（４３）をチェックしてＩＰＴＶ受信デバイス（４０）に適用されているセキュリティソリューション（例えば、ＣＡＳモジュール、ＤＲＭモジュール等）の情報をサービスプロバイダ（２０）に提供することができ、ＩＰＴＶ受信デバイス（４０）のセキュリティソリューションレベルをサービスプロバイダ（２０）に提供することもできる。

【００３７】

セキュリティコントローラ（４２）は、サービスプロバイダ（２０）から伝送されるコンテンツおよびそのコンテンツの使用に必要なコンテンツ関連情報をＩＰＴＶ受信モジュール（４１）を制御して受信し、セキュリティソリューション（４３）、例えば、サービス保護ソリューション（４４）を制御して、スクランブルされているコンテンツをクリーンタイプのコンテンツに変換することができる。また、セキュリティコントローラ（４２）は、セキュリティソリューション（４３）、例えば、コンテンツ保護ソリューション（４５）を制御して、クリーンタイプに変換されたコンテンツおよびそのコンテンツの使用権限情報をコンテンツ再生機（４７）で支援可能なタイプに変換して、ストレージ（４８）に格納したり、或いはコンテンツ再生機（４７）で再生したりするように制御する。

【００３８】

また、セキュリティコントローラ（４２）は、使用者からホームデバイス（５０）へのコンテンツ共有要求があった場合、ホームデバイス（５０）にどのコンテンツ保護ソリューションが適用されているかを検出し、該当コンテンツ保護ソリューションが支援する形式にコンテンツを変換した後、変換したコンテンツを出力ポート（４６）を介してホームデバイス（５０）に伝送することができる。このとき、もし、検出されたホームデバイス（５０）のコンテンツ保護ソリューション（図示せず）とＩＰＴＶ受信デバイス（４０）のコンテンツ保護ソリューション（４５）とが同一である場合、セキュリティコントローラ（４２）は、別途の変換無しに前記ＩＰＴＶ受信デバイス（４０）のコンテンツ保護ソリューション（４５）で支援可能なタイプに変換したコンテンツをホームデバイス（５０）に伝送することができる。

【００３９】

一方、セキュリティコントローラ（４２）は、ＩＰＴＶ受信デバイス（４０）のセキュリティソリューションレベルまたはホームデバイス（５０）のセキュリティソリューションレベルに基づいてコンテンツの共有を制限することもできる。例えば、セキュリティコントローラ（４２）は、コンテンツと関連付けられているセキュリティ情報を確認してコンテンツの伝送に必要なセキュリティレベルを抽出し、ＩＰＴＶ受信デバイス（４０）またはホームデバイス（５０）のセキュリティソリューションレベルでＩＰＴＶ受信デバイス（４０）またはホームデバイス（５０）のセキュリティレベルを確認した後、コンテンツの使用に必要なセキュリティレベルをＩＰＴＶ受信デバイス（４０）またはホームデバイス（５０）のセキュリティレベルが満たさない場合、コンテンツの使用または伝送を制限することができる。

【００４０】

セキュリティソリューション（４３）は、セキュリティコントローラ（４２）の制御に従ってコンテンツを保護するための機能を遂行することができる。セキュリティソリューション（４３）は、サービス保護ソリューション（４４）、コンテンツ保護ソリューション（４５）などを含んでもよい。

【００４１】

サービス保護ソリューション（４４）は、コンテンツにサービス保護技術を適用したり、或いは適用を解除したりする機能を遂行するモジュールを意味してもよい。サービス保護ソリューション（４４）は、ＣＡＳソリューションなどでもよい。サービス保護モジュール（４４）は、セキュリティコントローラ（４２）の制御に従ってサービスプロバイダ（２０）から伝送されるコンテンツを受信して処理する。例えば、サービス保護ソリューション（４４）は、サービスプロバイダ（２０）から受信されるＴＳからデスクランブル（Descrambling）鍵を抽出し、そのデスクランブル鍵を用いてスクランブルされている受

信コンテンツをデスクランブルして、デスクランブルしたコンテンツをクリーンタイプのコンテンツに変換することができる。

【００４２】

コンテンツ保護ソリューション（４５）は、コンテンツにコンテンツ保護技術を適用したり、或いは適用を解除したりする機能を遂行するモジュールを意味してもよい。コンテンツ保護モジュール（４５）は、ＤＲＭモジュール、コピー保護（Copy Protection）モジュール、許可サービスドメイン（Authorized Service Domain；ＡＳＤ）モジュールなどでもよい。コンテンツ保護ソリューション（４５）は、セキュリティコントローラ（４２）の制御に従ってコンテンツの変換を遂行することができる。例えば、コンテンツ保護ソリューション（４５）は、コンテンツを格納したりまたはホームデバイス（５０）に再配信したりするために、コンテンツをＤＲＭ技術に従って暗号化したり、或いは、再生などのために暗号化されたコンテンツを復号化したりすることができる。一方、サービスプロバイダ（２０）は、コンテンツにコンテンツ保護技術を適用してＩＰＴＶ受信デバイス（４０）に伝送することもでき、この場合、コンテンツ保護ソリューション（４５）は、前述したサービス保護ソリューション（４４）の機能などの概念に従って、コンテンツを受信したり、格納したり、或いは処理したりすることができる。

【００４３】

コンテンツ再生機（４７）は、コンテンツ、例えば、マルチメディアなどを再生する機能を遂行することができる。例えば、コンテンツ再生機（４７）は、使用者の要求に従って、セキュリティソリューション（４３）によって変換されたコンテンツを受信して再生する機能を遂行することができる。例えば、コンテンツ再生機（４７）は、コンテンツ保護ソリューション（４５）と連動して、コンテンツ保護ソリューション（４５）によって変換されたコンテンツを再生することができる。ストレージ（４８）は、セキュリティソリューション（４３）によって処理されたコンテンツを格納することができる。出力ポート（４６）は、ホームデバイス（５０）と連動する機能を遂行する。例えば、出力ポート（４６）は、セキュリティコントローラ（４２）の制御に従ってコンテンツをホームデバイス（５０）に伝送する機能を遂行することができる。

【００４４】

以上、ＩＰＴＶ受信デバイス（４０）の構成を記述した。一方、図示されていないが、ホームデバイス（５０）の場合、サービスプロバイダ（２０）と直接連動するのに必要な構成、例えば、ＩＰＴＶ受信モジュール（４１）またはサービス保護ソリューション（４４）などを有する必要がないという点以外は、前述したＩＰＴＶ受信デバイス（４０）とほぼ同じ構成を有してもよい。然しながら、これは制限事項ではなく、ホームデバイス（５０）がサービスプロバイダ（２０）と直接連動することもできる。このホームデバイス（５０）は、他のホームデバイスにコンテンツを伝送することもできる。

【００４５】

一方、デバイス、例えば、ＩＰＴＶ受信デバイス（４０）またはホームデバイス（５０）は、サービスプロバイダ（２０）または特定サーバからセキュリティソリューションのためのＤＲＭコード、セキュリティメッセージ、アプリケーションなどをダウンロードまたは受信するとき、これを認証するためのセキュリティソリューション認証プロセスを遂行することができる。セキュリティソリューション認証プロセスは、セキュリティソリューションのセキュリティ機能遂行の際、信頼性に影響を及ぼす。即ち、セキュリティソリューション認証プロセスが厳格であるほどセキュリティソリューションの信頼性は高まる。このセキュリティソリューション認証プロセスのセキュリティレベルを表す情報としてセキュリティソリューションレベルの概念を導入することができる。

【００４６】

セキュリティソリューションレベルは、デバイスのセキュリティ特性を予め決められた基準に従って等級化した（Classified）情報を意味してもよい。前記セキュリティソリューションレベルは、デバイスのセキュリティソリューションプロファイルでもよい。デバイスは、そのデバイスのセキュリティソリューション認証プロセスのセキュリティレベル

に従って指定されるセキュリティソリューションレベルと関連付けられてもよい。前記予め決められた基準とは、セキュリティソリューションレベルテーブルでもよい。

【００４７】

図４は、デバイスのセキュリティソリューションレベルを指定する基準になるセキュリティソリューションレベルテーブルを例示する図である。

【００４８】

図４に示されているように、セキュリティソリューションレベルテーブル（SSLT）は、例えば、５個の等級のセキュリティソリューションレベルを定義することができる。

【００４９】

レベル０は、非セキュリティ実行環境（Non-Secured Execution Environment）でセキュリティソリューション認証プロセスの認証（Authentication）および完全性（Integrity）のチェックを遂行しないセキュリティレベルを意味してもよい。セキュリティソリューションレベルがレベル０であるデバイスは、セキュリティソリューション認証プロセスを認証せず、セキュリティソリューション認証プロセスを開始（initiate）する。従って、デバイスのセキュリティソリューションレベルがレベル０であれば、そのデバイスはセキュリティが相当脆弱なデバイスということができる。レベル０は、定義されたセキュリティソリューションレベルのうち最も信頼度が低いレベルである。

【００５０】

レベル１は、非セキュリティ実行環境でデバイスのソフトウェアエレメント（element）を使用してセキュリティソリューション認証プロセスの認証および完全性のチェックを検証するレベルのセキュリティソリューションレベルを意味してもよい。レベル１におけるセキュリティソリューション認証プロセスは、デバイスのソフトウェアエレメントによって認証された後、開始されてもよい。このレベル１は前述したレベル０よりはセキュリティ性が高いといえる。

【００５１】

レベル２は、非セキュリティ実行環境でデバイスのハードウェアエレメントを使用して直接セキュリティソリューション認証プロセスの認証および完全性チェックを検証するレベルを意味してもよい。レベル２におけるセキュリティソリューション認証プロセスは、デバイスのハードウェアエレメントによって認証された後、開始されてもよい。このレベル２は前述したレベル１よりはセキュリティ性が高いといえる。

【００５２】

レベル３は、セキュリティ実行環境（Secured Execution Environment）でデバイスのソフトウェアエレメントを使用してセキュリティソリューション認証プロセスの認証および完全性チェックを検証するセキュリティソリューションレベルを意味してもよい。レベル３におけるセキュリティソリューション認証プロセスは、セキュリティ実行環境下でデバイスのソフトウェアエレメントによって認証された後、開始されてもよい。このレベル３は前述したレベル２よりセキュリティ性が高いといえる。

【００５３】

レベル４は、セキュリティ実行環境でデバイスのハードウェアエレメントを使用して直接セキュリティソリューション認証プロセスの認証および完全性チェックを検証するセキュリティソリューションレベルを意味してもよい。レベル４におけるセキュリティソリューション認証プロセスは、セキュリティ実行環境下でデバイスのハードウェアエレメントによって認証された後、開始されてもよい。このレベル４は、前述したレベル３よりセキュリティ性が高く、定義されたセキュリティソリューションレベルのうち最も信頼度が高いといえる。

【００５４】

デバイス、例えば、ＩＰＴＶ受信デバイス（４０）またはホームデバイス（５０）は、該当デバイスのセキュリティレベルに従って前述した基準に該当するセキュリティソリューションレベルを有してもよい。これらのセキュリティソリューションレベルは、デバイスの認証書内の特定フィールドに挿入することによって、該当デバイスと関連付けること

ができる。即ち、デバイスの認証書は、そのデバイスのセキュリティソリューションレベルを含んでもよい。

【００５５】

デバイスは、自体またはコンテンツを共有しようとするデバイス（即ち、ターゲットデバイス）のセキュリティソリューションレベルに基づいてコンテンツの使用または伝送を制限することもできる。例えば、コンテンツの使用または共有時に要求されるセキュリティレベルを自体またはターゲットデバイスのセキュリティレベル（即ち、該当デバイスのセキュリティソリューションレベル）を満たさない場合、コンテンツの使用または共有を制限することもできる。コンテンツで要求されるセキュリティレベルと関連する情報は、コンテンツと関連付けられたセキュリティ情報に含まれてもよい。前記コンテンツと関連付けられたセキュリティ情報は、該当コンテンツの使用または共有時に要求されるセキュリティソリューションレベルを表す情報を含んでもよい。

【００５６】

図５は、本発明の望ましい実施例に係るコンテンツ格納方法の手順を例示するための図であり、ＩＰＴＶ受信デバイス（４０）がサービスプロバイダ（２０）からコンテンツを受信して格納する手順を示す。

【００５７】

図５に示されているように、ＩＰＴＶ受信デバイス（４０）は、サービス保護ソリューション（４４）およびコンテンツ保護ソリューション（４５）を備える。まず、使用者は、コンテンツを視聴するために、ＩＰＴＶ受信デバイス（４０）にコンテンツのダウンロードおよび格納を要求することができる。ＩＰＴＶ受信デバイス（４０）は、これに応答してサービスプロバイダ（２０）に該当コンテンツを伝送するように要求する（段階：Ｓ１）。一方、使用者は、他のデバイス（例えば、ホームデバイス、または第３の端末機）を介してＩＰＴＶ受信デバイス（４０）へのコンテンツ伝送を要求することもできる。

【００５８】

サービスプロバイダ（２０）は、サービスプロバイダ（２０）のサービス保護ソリューションを使用してコンテンツを保護し、ＩＰＴＶ受信デバイス（４０）にその保護されたコンテンツを伝送する。例えば、サービスプロバイダ（２０）は、コンテンツを前記サービス保護ソリューションを使用してスクランブルし、スクランブルされたコンテンツおよびそのコンテンツと関連付けられた使用権限情報などをＩＰＴＶ受信デバイス（４０）に伝送することができる。

【００５９】

ＩＰＴＶ受信デバイス（４０）は、ＩＰＴＶ受信デバイス（４０）に備えられたサービス保護ソリューション（４４）を用いてサービスプロバイダ（２０）から伝送されるコンテンツをダウンロードする（段階：Ｓ２）。ダウンロードの際、ＩＰＴＶ受信デバイス（４０）のサービス保護ソリューション（４４）は、サービスプロバイダ（２０）から受信されるスクランブルされたコンテンツを内部で処理できる形式のコンテンツ、例えば、クリーンタイプのコンテンツに変換することができる。

【００６０】

次に、ＩＰＴＶ受信デバイス（４０）のコンテンツ保護ソリューション（４５）は、ダウンロードされたコンテンツを、コンテンツ再生機を支援するコンテンツ保護ソリューション（４５）に適するように変換し、変換したコンテンツをストレージに格納することができる（段階：Ｓ３）。また、前記ＩＰＴＶ受信デバイス（４０）のコンテンツ保護ソリューション（４５）は、前記コンテンツと関連付けられた使用権限情報などを前記コンテンツ保護ソリューション（４５）に適する形式に変換して格納することができる。一方、コンテンツの使用時には、ＩＰＴＶ受信デバイス（４０）のセキュリティソリューションレベルに従ってコンテンツの使用が制限されてもよい。

【００６１】

以上、説明した通り、ＩＰＴＶ受信デバイス（４０）は、ＩＰＴＶ受信デバイス（４０）が備えるサービス保護ソリューション（４４）を用いてサービスプロバイダ（２０）か

ら伝送されるコンテンツをダウンロードし、コンテンツ保護ソリューション（４５）を用いてコンテンツをＩＰＴＶ受信デバイス（４０）でセキュリティ保護されて再生可能な形式に変換することができる。

【００６２】

一方、図示されていないが、コンテンツ格納方法の他の実施例として、サービスプロバイダ（２０）は、ＩＰＴＶ受信デバイス（４０）が備えるコンテンツ保護ソリューション（４５）に適するようにコンテンツを保護してＩＰＴＶ受信デバイス（４０）にコンテンツを伝送することもできる。例えば、ＩＰＴＶ受信デバイス（４０）がコンテンツの伝送を要求する場合、サービスプロバイダ（２０）は、コンテンツがＩＰＴＶ受信デバイス（４０）で支援されるコンテンツ保護ソリューション（４５）に適する（compatible with（と互換性がある））ようにコンテンツ保護技術を使用してコンテンツを保護し、この保護されたコンテンツをＩＰＴＶ受信デバイス（４０）に伝送する。すると、ＩＰＴＶ受信デバイス（４０）のコンテンツ保護ソリューション（４５）は、このコンテンツを受信して格納することができる。

【００６３】

サービスプロバイダ（２０）は、ＩＰＴＶ受信デバイス（４０）をドメインに登録する時、またはサービスプロバイダ（２０）の要求に従ってＩＰＴＶ受信デバイス（４０）からＩＰＴＶ受信デバイス（４０）のセキュリティ性能情報を受信して格納および管理することによって、ＩＰＴＶ受信デバイス（４０）のコンテンツ保護ソリューション（４５）を把握することができる。前記セキュリティ性能情報は前述したように、ＩＰＴＶ受信デバイス（４０）が備えるセキュリティソリューションの情報、セキュリティソリューションレベルなどを含んでもよい。前記セキュリティソリューションの情報、セキュリティソリューションレベルなどはＩＰＴＶ受信デバイス（４０）の認証書に含まれてもよい。

【００６４】

図６は、本発明の望ましい実施例に係るコンテンツ共有方法を実現するためのシステム構成を示すブロック図である。また、図７は、本発明の望ましい実施例に係るコンテンツ共有方法を説明するためのフローチャートであり、サービスプロバイダ（２０）からダウンロードしたコンテンツをホームデバイス（５０）に再配信することによってコンテンツを共有する手順を示す。

【００６５】

図６に示されているように、サービスプロバイダ（２０）は、サービス保護技術を使用してコンテンツを伝送し、ＩＰＴＶ受信デバイス（４０）は、サービス保護ソリューション（４４）およびコンテンツ保護ソリューション‘Ａ’（４５ａ）を備える。また、ＩＰＴＶ受信デバイス（４０）とコンテンツを共有するホームデバイス（５０）は、ＩＰＴＶ受信デバイス（４０）のコンテンツ保護ソリューション（４５ａ）と同じコンテンツ保護ソリューション‘Ａ’（５５ａ）を備える。即ち、ホームデバイス（５０）は、ＩＰＴＶ受信デバイス（４０）と同じコンテンツ保護ソリューションを支援する。

【００６６】

図６および図７を参照すると、まず、使用者は、所望のコンテンツをホームデバイス（５０）にダウンロードして視聴するために、ホームデバイス（５０）またはディスカバリプロセスを介してホームデバイス（５０）を見つけ出す（Discover）ことができるＩＰＴＶ受信デバイス（４０）または第３のデバイスを用いてコンテンツをホームデバイス（５０）にダウンロードすることを要求することができる。すると、該当デバイスは、サービスプロバイダ（２０）に使用者によって要求されたコンテンツを伝送するように要求する（段階：Ｓ１１）。

【００６７】

サービスプロバイダ（２０）は、前記要求に応じてサービスプロバイダ（２０）のサービス保護ソリューションを使用して前記コンテンツをスクランブルし、スクランブルしたコンテンツおよびそのコンテンツの使用に必要な情報、例えば、使用権限情報、セキュリティ情報、リボケーションリスト情報などをＩＰＴＶ受信デバイス（４０）に伝送する。

これに伴い、サービス保護技術によって保護されたコンテンツがＩＰＴＶ受信デバイス（４０）に伝送される。

【００６８】

ＩＰＴＶ受信デバイス（４０）は、ＩＰＴＶ受信デバイス（４０）に備えられたサービス保護ソリューション（４４）を用いてサービスプロバイダ（２０）からコンテンツを受信して処理することができる（段階：Ｓ１２）。例えば、サービス保護ソリューション（４４）は、受信したスクランブルされたコンテンツをサービス保護技術に従ってクリーンタイプのコンテンツに変換することができる。また、コンテンツの使用に必要な情報をＩＰＴＶ受信デバイス（４０）の内部で使用可能な形式に変換することもできる。

【００６９】

次に、ＩＰＴＶ受信デバイス（４０）は、コンテンツを伝送しようとするホームデバイス（５０）が備えるコンテンツ保護ソリューションを検出（detecting）する（段階：Ｓ１３）。このとき、ホームデバイス（５０）で支援されるコンテンツ保護ソリューションとＩＰＴＶ受信デバイス（４０）のコンテンツ保護ソリューションとが同一である場合（本実施例ではホームデバイス（５０）およびＩＰＴＶ受信デバイス（４０）が同じコンテンツ保護技術を支援するコンテンツ保護ソリューション‘Ａ’（４４ａおよび５５ａ）を各々備える）、ＩＰＴＶ受信デバイス（４０）のコンテンツ保護ソリューション‘Ａ’（４５ａ）は、前記コンテンツをコンテンツ保護ソリューション‘Ａ’（４５ａ）に適応した形式に変換（convert）する（段階：Ｓ１４）。例えば、コンテンツ保護ソリューション‘Ａ’（４５ａ）は、コンテンツを約束された形式で暗号化し、コンテンツの使用権限などをコンテンツ保護ソリューション‘Ａ’（４５ａ）に適合した形式に翻訳（translates）する。

【００７０】

次に、ＩＰＴＶ受信デバイス（４０）は、変換されたコンテンツおよびそのコンテンツの使用に必要な情報をコンテンツ保護ソリューション‘Ａ’（４５ａ）で支援される技術を使用してホームデバイス（５０）に伝送することによってコンテンツを再配信する（段階：Ｓ１５）。このとき、ＩＰＴＶ受信デバイス（４０）は、コンテンツの使用権限によってコンテンツの伝送を制限することができる。即ち、コンテンツの共有は、該当コンテンツと関連付けられた使用権限で許容される範囲内で遂行することができる。

【００７１】

また、ＩＰＴＶ受信デバイス（４０）は、ホームデバイス（５０）またはＩＰＴＶ受信デバイス（４０）のセキュリティソリューションレベルに基づいてコンテンツの共有を制限することもできる。例えば、ＩＰＴＶ受信デバイス（４０）は、コンテンツの共有時に要求されるセキュリティレベルをＩＰＴＶ受信デバイス（４０）またはホームデバイス（５０）のセキュリティレベル（即ち、該当デバイスのセキュリティソリューションレベル）を満たさない場合、コンテンツの共有を制限することもできる。このとき、ＩＰＴＶ受信デバイス（４０）のセキュリティソリューションレベルおよびホームデバイス（５０）のセキュリティソリューションレベルは、各々ＩＰＴＶ受信デバイス（４０）の認証書およびホームデバイス（５０）の認証書内に含まれ、コンテンツの共有時に要求されるセキュリティレベルは、コンテンツと関連するセキュリティ情報に含まれてもよい。ＩＰＴＶ受信デバイス（４０）は、自体のセキュリティソリューションレベルを確認するために自体の認証書をチェックすることができ、ホームデバイス（５０）のセキュリティソリューションレベルを確認するためにホームデバイス（５０）に認証書を要求したり、或いは別途にセキュリティソリューションレベルの情報を要求したりすることもできる。

【００７２】

一方、ＩＰＴＶ受信デバイス（４０）は、前記ホームデバイス（５０）との相互認証を遂行し、前記ホームデバイス（５０）がＩＰＴＶ受信デバイス（４０）と同じドメインに登録されたドメインデバイスかどうかを確認することもできる。もし、ホームデバイス（５０）がＩＰＴＶ受信デバイス（４０）と同じドメインに属さなければ、ＩＰＴＶ受信デバイス（４０）は、ホームデバイス（５０）へのコンテンツ共有を制限することもできる

。
【００７３】
ＩＰＴＶ受信デバイス（４０）からホームデバイス（５０）に、コンテンツおよびそのコンテンツの使用に必要な情報が伝送された場合、ホームデバイス（５０）のコンテンツ保護ソリューション‘Ａ’（５５ａ）はこれを受信し、格納して再生することができる。再生の際、ホームデバイス（５０）のコンテンツ保護ソリューション‘Ａ’（５５ａ）は、コンテンツの使用権限情報で許容される範囲内で、コンテンツが再生できるように暗号化されたコンテンツを復号して、復号したコンテンツをコンテンツ再生機（図示せず）に提供することができる。
【００７４】
一方、図６に点線で示された通り、サービスプロバイダ（２０）とコンテンツ保護ソリューション‘Ａ’（４５ａ）が直接連動することもできる。例えば、サービスプロバイダ（２０）は、ＩＰＴＶ受信デバイス（４０）が備えるコンテンツ保護ソリューション‘Ａ’（４５ａ）に適するコンテンツ保護技術を使用してコンテンツを保護し、これをＩＰＴＶ受信デバイス（４０）に伝送することができる。この場合、ＩＰＴＶ受信デバイス（４０）は、別途のサービス保護ソリューション（４４）の処理を遂行せずに、サービスプロバイダ（２０）からコンテンツ保護ソリューション‘Ａ’（４５ａ）によって保護されたコンテンツをダウンロードしてホームデバイス（５０）に再配信することもできる。
【００７５】
図８は、本発明の望ましい他の実施例に係るコンテンツ共有方法を実現するためのシステム構成を示すブロック図である。また、図９は、本発明の望ましい他の実施例に係るコンテンツ共有方法を説明するためのフローチャートであり、サービスプロバイダ（６０）からダウンロードしたコンテンツをホームデバイス（８０）に再配信することによってコンテンツを共有する手順を示す。
【００７６】
図８に示されているように、サービスプロバイダ（６０）は、コンテンツ保護技術に従ってコンテンツを伝送し、ＩＰＴＶ受信デバイス（７０）は、コンテンツ保護ソリューション‘Ａ’（７５ａ）を備える。また、ＩＰＴＶ受信デバイス（７０）とコンテンツを共有するホームデバイス（８０）は、ＩＰＴＶ受信デバイス（７０）のコンテンツ保護ソリューション‘Ａ’（７５ａ）とは異なる種類のコンテンツ保護技術を支援するコンテンツ保護ソリューション‘Ｂ’（８５ｂ）を備える。
【００７７】
図８および図９を参照すると、まず、使用者は、所望のコンテンツをホームデバイス（８０）にダウンロードして視聴するために、ホームデバイス（８０）またはディスカバリプロセスを介してホームデバイス（８０）を見つけ出す（discover）ことができるＩＰＴＶ受信デバイス（７０）または第３のデバイスを用いてコンテンツをホームデバイス（８０）にダウンロードすることを要求することができる。すると、該当デバイスは、サービスプロバイダ（６０）に使用者によって要求されたコンテンツを伝送するように要求する（段階：Ｓ２１）。
【００７８】
サービスプロバイダ（６０）は、前記要求に応じてサービスプロバイダ（６０）のコンテンツ保護ソリューション‘Ａ’を使用して前記コンテンツを暗号化し、暗号化されたコンテンツおよびそのコンテンツの使用に必要な情報、例えば、使用権限情報、セキュリティ情報、リボケーションリスト情報などをＩＰＴＶ受信デバイス（７０）に伝送する。これに伴い、コンテンツ保護技術によって保護されたコンテンツがＩＰＴＶ受信デバイス（７０）に伝送される。
【００７９】
ＩＰＴＶ受信デバイス（７０）は、コンテンツ保護ソリューション‘Ａ’（７５ａ）を用いてサービスプロバイダ（６０）からコンテンツを受信することができる（段階：Ｓ２２）。また、コンテンツ保護ソリューション‘Ａ’（７５ａ）は、受信した暗号化された

コンテンツを他のコンテンツ保護ソリューションに変換できるようにするために、クリーンタイプのコンテンツに変換することもできる。また、コンテンツの使用に必要な情報をＩＰＴＶ受信デバイス（７０）の内部で使用可能な形式に変換することもできる。

【００８０】

次に、ＩＰＴＶ受信デバイス（７０）は、コンテンツを伝送しようとするホームデバイス（８０）が備えるコンテンツ保護ソリューションを検出（detect）する（段階：Ｓ２３）。このとき、ホームデバイス（８０）で支援するコンテンツ保護ソリューションとＩＰＴＶ受信デバイス（７０）のコンテンツ保護ソリューションが異なる場合（本実施例ではホームデバイス（８０）とＩＰＴＶ受信デバイス（７０）が、相異なるコンテンツ保護技術を支援する例を挙げる）、ＩＰＴＶ受信デバイス（７０）は、前記コンテンツをコンテンツ保護ソリューション‘Ｂ’（８５ｂ）に適応した形式に変換（convert）する（段階：Ｓ２４）。例えば、ＩＰＴＶ受信デバイス（７０）は、コンテンツを約束された形式で暗号化し、コンテンツの使用権限などをコンテンツ保護ソリューション‘Ｂ’（８５ｂ）に適合した形式に翻訳（translates）する。

【００８１】

この処理のために、ＩＰＴＶ受信デバイス（７０）は、ＤＲＭ相互互換ソリューションを具備したり、或いはコンテンツ保護ソリューション‘Ｂ’を具備したりしてもよい。もし、前記ソリューションを具備しない場合、ＩＰＴＶ受信デバイス（７０）は、サービスプロバイダ（６０）、ＤＲＭサーバ、ホームデバイス（８０）などに要求して該当ソリューションをダウンロードすることができる。

【００８２】

次に、ＩＰＴＶ受信デバイス（７０）は、変換されたコンテンツおよびそのコンテンツの使用に必要な情報を相互互換再配信（Interoperable Redistribution）技術またはサービス保護ソリューション‘Ｂ’で支援される技術を使用してホームデバイス（８０）に伝送することによってコンテンツを再配信する（段階：Ｓ２５）。このとき、ＩＰＴＶ受信デバイス（７０）は、コンテンツの使用権限によってホームデバイス（８０）へのコンテンツ伝送を制限することができる。即ち、コンテンツの共有は、該当コンテンツと関連付けられた使用権限で許容される範囲内で遂行することができる。

【００８３】

また、ＩＰＴＶ受信デバイス（７０）は、ホームデバイス（８０）またはＩＰＴＶ受信デバイス（７０）のセキュリティソリューションレベルに基づいてコンテンツの共有を制限することもできる。例えば、ＩＰＴＶ受信デバイス（７０）は、コンテンツの共有時に要求されるセキュリティレベルをＩＰＴＶ受信デバイス（７０）またはホームデバイス（８０）のセキュリティレベル（即ち、該当デバイスのセキュリティソリューションレベル）を満たさない場合、コンテンツの共有を制限することもできる。

【００８４】

このとき、ＩＰＴＶ受信デバイス（７０）のセキュリティソリューションレベルおよびホームデバイス（８０）のセキュリティソリューションレベルは、各々ＩＰＴＶ受信デバイス（７０）の認証書およびホームデバイス（８０）の認証書内に含まれ、コンテンツの共有時に要求されるセキュリティレベルは、コンテンツと関連付けられたセキュリティ情報に含まれてもよい。ＩＰＴＶ受信デバイス（７０）は、ＩＰＴＶ受信デバイス（７０）のセキュリティソリューションレベルを確認するために自体の認証書をチェックすることができ、ホームデバイス（８０）のセキュリティソリューションレベルを確認するためにホームデバイス（８０）に認証書を要求したり、或いは別途にセキュリティソリューションレベルの情報を要求したりすることもできる。

【００８５】

また、ＩＰＴＶ受信デバイス（７０）は、前記ホームデバイス（８０）との相互認証を遂行し、前記ホームデバイス（８０）がＩＰＴＶ受信デバイス（７０）と同じドメインに登録されたドメインデバイスかどうかを確認することもできる。もし、ホームデバイス（８０）がＩＰＴＶ受信デバイス（７０）と同じドメインに属さなければ、ＩＰＴＶ受信デ

バイス（７０）は、ホームデバイス（８０）へのコンテンツ共有を制限することもできる。

【００８６】

ＩＰＴＶ受信デバイス（７０）からホームデバイス（８０）に、コンテンツおよびそのコンテンツの使用に必要な情報（例えば、権限情報等）が伝送された場合、ホームデバイス（８０）のコンテンツ保護ソリューション‘Ｂ’（８５ｂ）は、これを受信し、格納して再生することができる。再生の際、ホームデバイス（８０）のコンテンツ保護ソリューション‘Ｂ’は、コンテンツの使用権限情報で許容される範囲内において、コンテンツが再生できるように暗号化されたコンテンツを復号して、復号したコンテンツをコンテンツ再生機に提供することができる。

【００８７】

一方、図８に点線で示された通り、コンテンツの権限情報を提供するためにサービスプロバイダ（６０）とホームデバイス（８０）とが直接連動することもできる。例えば、ＩＰＴＶ受信デバイス（７０）は、コンテンツをホームデバイス（８０）に伝送し、そのコンテンツの使用に必要な権限情報は、ホームデバイス（８０）が直接サービスプロバイダ（６０）から受信することもできる。

【００８８】

以下、サービスプロバイダ間のコンテンツ連動セキュリティサービスモデルを説明する。サービスプロバイダ間のコンテンツ連動サービスとは、使用者が、一回の課金を介して２個以上のサービスプロバイダが提供するコンテンツを使用することができるサービスを意味してもよい。以下の開示内容によって、このサービスの安定性を保証および提供する構造を提供することができる。

【００８９】

図１０は、サービスプロバイダ間のコンテンツ連動サービスの概念を例示するための図である。

【００９０】

図１０に示されているように、サービスプロバイダ１はサービスＡおよびサービスＢを提供し、サービスプロバイダ２はサービスＣおよびサービスＤを提供すると仮定すれば、従来の場合、使用者はサービスプロバイダ１およびサービスプロバイダ２が各々提供するサービスＡおよびサービスＣ形態のサービスを各サービスプロバイダを介して課金して用いることができる。然しながら、本発明では一回の課金によって‘サービスＡ－サービスＣ’を自由に利用できる新しい概念のサービスを提供することができる。

【００９１】

図１１は、サービスプロバイダ間のコンテンツ連動サービスのためのシステム構造を例示する図である。また、図１２は、サービスプロバイダ間のコンテンツ連動サービスの手順を例示するための図である。

【００９２】

図１１ないし図１２を参照すると、サービスプロバイダ１とサービスプロバイダ２は、各々のサービスのためのドメインを形成することができる。この場合、サービスプロバイダ間のコンテンツ連動サービスのために、コンテンツＤＲＭ相互互換マネージャ（Content DRM Interoperability Manager）、ドメインマネージャ（Domain Manager）および認証書許可サーバ（Certificate Authority）などを備えてもよい。

【００９３】

コンテンツＤＲＭ相互互換マネージャは、サービスプロバイダ間で異なるＤＲＭによって保護されているコンテンツを互換性があるようにするために情報を提供するサーバを意味してもよい。ドメインマネージャは、使用者が提供を受けることを所望するサービスプロバイダ間の異なるサービスを結合することによってサービス統合ドメインを提供するサービスドメイン機能および使用者が保有する端末がサービスドメインに属するサービスを利用できるようにこれらのサービスを結合する使用者／デバイスドメイン機能を提供することができる。認証書許可サーバは、コンテンツ連動サービスと関連するサーバ、使用者

、使用者装置の認証書を管理するサーバを意味してもよい。

【００９４】

図１２に示されているように、サービスプロバイダ間のコンテンツ連動サービスは、まず、認証書発行段階（段階：Ｓ３１）を経る。認証書許可サーバの認証書発行段階（段階：Ｓ３１）では、標準化（例えば、Ｘ．５０９　ｖ３等）された認証書許可サーバが、サービスのための認証書Ａ（Certificate a）を発行してドメインマネージャ、サービスプロバイダ、デバイスＡ（Device a）に伝達することができる。

【００９５】

コンテンツ連動サービス加入段階（段階：Ｓ３２）は、使用者がデバイスＡを介してコンテンツ連動サービスの提供を受けるために、デバイスＡがドメインマネージャにサービス加入を要求する段階を意味してもよい。

【００９６】

デバイスＡから要求メッセージを受信するドメインマネージャ内のサービスドメインコンストラクタは、使用者が要求するサービスを一つの仮想ドメインに結合し、該当仮想ドメインに属するコンテンツを保護するためのドメイン鍵Ａ（Domain key a）を生成することができる。また、ドメインマネージャの使用者ドメインコンストラクタは、使用者が保有するデバイス（例えば、デバイスＡを含む多数の使用者デバイス）を他の仮想ドメインに結合してサービス仮想ドメインに属するコンテンツが利用できる環境を構成することができる。

【００９７】

次に、ドメイン情報提供段階（段階：Ｓ３３）が遂行されてもよい。ドメイン情報提供段階（段階：Ｓ３３）では、前記のコンテンツ連動サービス加入段階（段階：Ｓ３２）を介して生成されたドメイン鍵Ａ（Domain key a）、サービスドメイン情報および使用者ドメイン情報を提供し、ドメイン鍵Ａ（Domain key a）の生成情報は、サービスドメインに属するサービスプロバイダと共有される。

【００９８】

コンテンツダウンロード段階（段階：Ｓ３４）では、サービス加入後、使用者は、使用者ドメインに属するデバイスＡにサービスドメインに属するサービスプロバイダからコンテンツをダウンロードする。ダウンロードされるコンテンツは、基本的に各サービスプロバイダで決められたＤＲＭによって保護されており、ＤＲＭによって保護されたコンテンツは、ドメイン鍵Ａ（Domain key a）によって再度保護されて使用者装置に伝達される。

【００９９】

使用者が生成したサービスドメインに属するコンテンツは、サービスプロバイダが異なっても、同じドメイン鍵Ａ（Domain key a）によって保護されることがある。保護される形態は、ＤＲＭで使われるコンテンツ暗号鍵（Content Encryption Key；ＣＥＫ）をドメイン鍵Ａ（Domain Key a）で暗号化して各ＤＲＭのライセンス（License）ファイルに格納する形態と、各ＤＲＭのライセンスファイルをドメイン鍵Ａ（Domain key a）で暗号化して使用者に伝達する方法がありうる。

【０１００】

次に、コンテンツ実行および変換段階（段階：Ｓ３５）が遂行されてもよい。コンテンツ実行および変換段階（段階：Ｓ３５）は、実際に使用者が所有するデバイスにおいて、前記コンテンツダウンロード段階（段階：Ｓ３４）でダウンロードされたコンテンツを実行する段階であり、デバイスＡが前記コンテンツ連動サービス加入段階（段階：Ｓ３２）で取得したドメイン鍵Ａ（Domain key a）とダウンロードされたコンテンツを保護するＤＲＭのアンパッキングエージェント（Unpacking Agent）とを保有する場合、コンテンツを実行することができる。

【０１０１】

もし、デバイスＡが前記ＤＲＭアンパッキングエージェントを保有していない場合、ＤＲＭコンバータ（Converter）を介してＤＲＭ変換を遂行することによってコンテンツの使用を可能にすることができる。然しながら、このとき、変換が正常に遂行されてもドメ

イン鍵Ａ（Domain key a）がない場合、コンテンツの使用は不可能である。

【０１０２】

以上、本発明についてその望ましい実施例を図面を参照して説明したが、該当技術分野の熟練された当業者は、特許請求の範囲に記載された本発明の技術的思想および領域から外れない範囲内で本発明を多様に修正および変更させて実施できることを理解することができる。従って、本発明の今後の実施例の変更は本発明の技術を外れることはない。

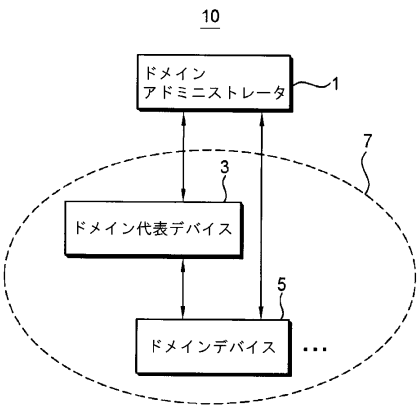
【符号の説明】

【０１０３】

２０　サービスプロバイダ
４０　ＩＰＴＶ受信デバイス
４４　コンテンツ保護ソリューション
４５ａ　ＩＰＴＶ受信デバイスのコンテンツ保護ソリューション‘Ａ’
５０　ホームデバイス
５５ａ　ホームデバイスのコンテンツ保護ソリューション‘Ａ’

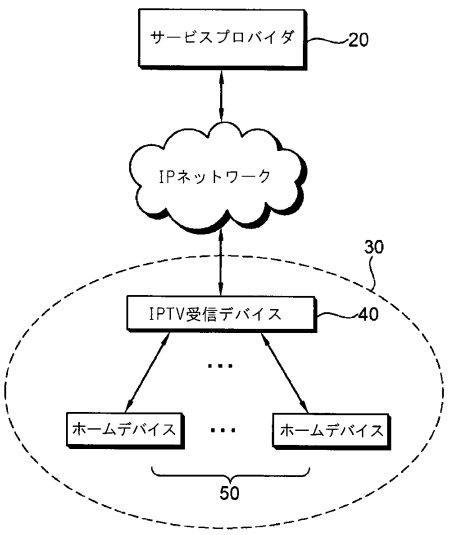
【図１】

[Fig. 1]



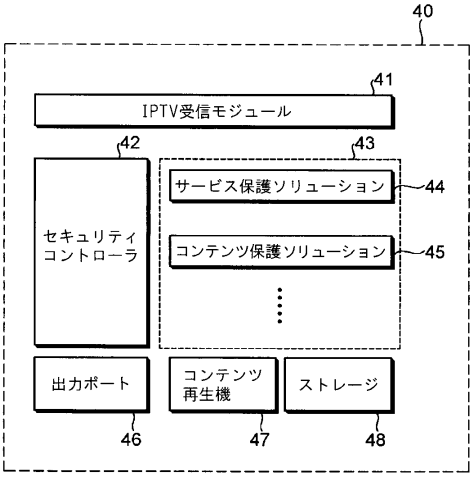
【図２】

[Fig. 2]



【図３】

[Fig. 3]



【図４】

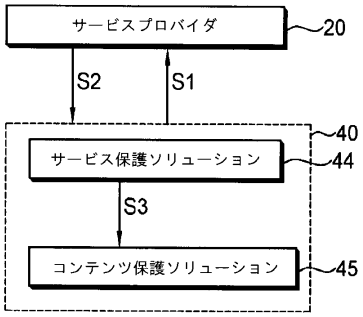
[Fig. 4]

SSLT

SSL	実行環境	定義
0	Non-Secured	認証および完全性をチェックしない
1	Non-Secured	認証および完全性をソフトウェアで検証する
2	Non-Secured	認証および完全性をハードウェアで検証する
3	Secured	認証および完全性をソフトウェアで検証する
4	Secured	認証および完全性をハードウェアで検証する

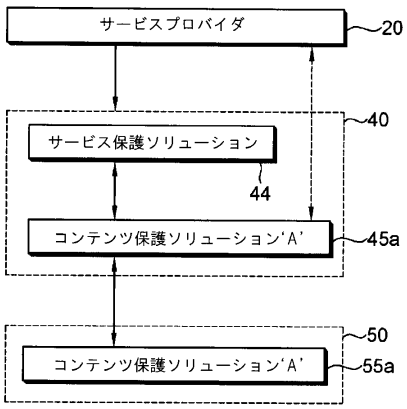
【図５】

[Fig. 5]



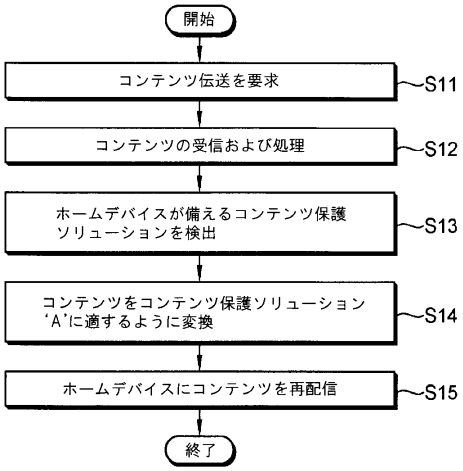
【図６】

[Fig. 6]



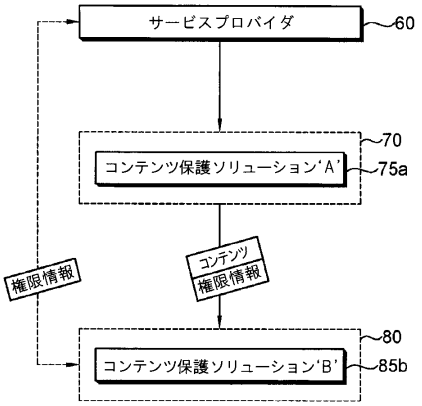
【図７】

[Fig. 7]



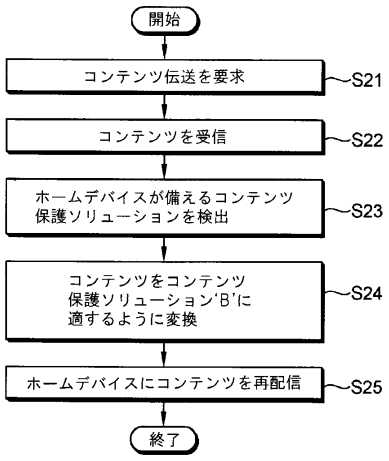
【図８】

[Fig. 8]



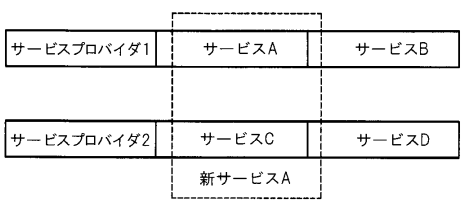
【図９】

[Fig. 9]



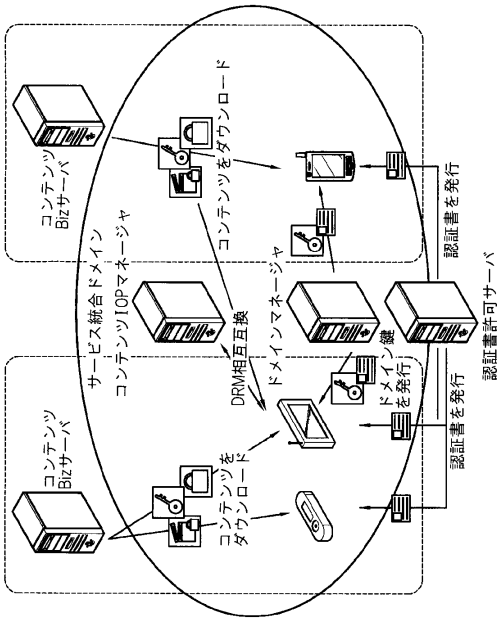
【図１０】

[Fig. 10]



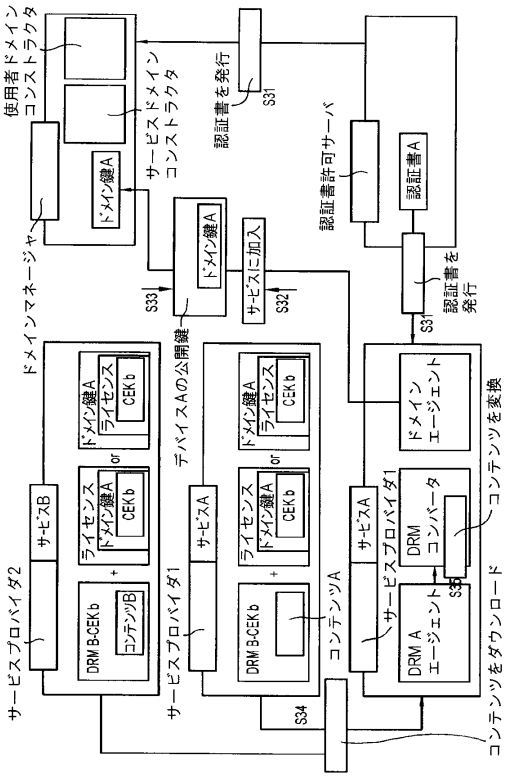
【図１１】

[Fig. 11]



【図１２】

[Fig. 12]


使用者ドメイン
コンストラクタ
ドメインマネージャ
ドメイン鍵A
サービスドメイン
コンストラクタ
認証書を発行
S31
認証書許可サーバ
認証書A
S33
ドメイン鍵A
サービスに加入
S32
認証書を
発行
S31
デバイスAの公開鍵
ドメイン鍵A
ライセンス
CEK b
or
ライセンス
ドメイン鍵A
CEK b
サービスB
DRM B-CEK b
コンテンツB
サービスプロバイダ2
サービスA
ドメイン鍵A
ライセンス
CEK b
or
ライセンス
ドメイン鍵A
CEK b
サービスプロバイダ1
DRM B-CEK b
コンテンツA
S34
サービスA
ドメイン
エージェント
サービスプロバイダ1
DRM
コンバータ
コンテンツを変換
DRM A
エージェント
S35
コンテンツをダウンロード

フロントページの続き

(31)優先権主張番号 60/971,548
(32)優先日 平成19年9月11日(2007.9.11)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/981,815
(32)優先日 平成19年10月22日(2007.10.22)
(33)優先権主張国 米国(US)
(31)優先権主張番号 60/981,816
(32)優先日 平成19年10月22日(2007.10.22)
(33)優先権主張国 米国(US)

(72)発明者 パク，クー ヨン
大韓民国，ソウル １３７－７２４，ソチョーク，ウーミョン－ドン，＃１６，エルジー アール アンド ディー キャンパス，ディーエム ラボラトリー，エヌエーエス グループ
(72)発明者 チョ，スン ヒュン
大韓民国，ソウル １３７－７２４，ソチョーク，ウーミョン－ドン，＃１６，エルジー アール アンド ディー キャンパス，ディーエム ラボラトリー，エヌエーエス グループ
(72)発明者 パク，イル ゴン
大韓民国，ソウル １３７－７２４，ソチョーク，ウーミョン－ドン，＃１６，エルジー アール アンド ディー キャンパス，ディーエム ラボラトリー，エヌエーエス グループ
(72)発明者 ジョン，マン スー
大韓民国，ソウル １３７－７２４，ソチョーク，ウーミョン－ドン，＃１６，エルジー アール アンド ディー キャンパス，ディーエム ラボラトリー，エヌエーエス グループ
(72)発明者 キラン，クマール ケー.
大韓民国，ソウル １３７－７２４，ソチョーク，ウーミョン－ドン，＃１６，エルジー アール アンド ディー キャンパス，ディーエム ラボラトリー，エヌエーエス グループ
(72)発明者 キム，スー ジュン
大韓民国，ソウル １３７－７２４，ソチョーク，ウーミョン－ドン，＃１６，エルジー アール アンド ディー キャンパス，ディーエム ラボラトリー，エヌエーエス グループ
(72)発明者 チュン，ミン ギュ
大韓民国，ソウル １３７－７２４，ソチョーク，ウーミョン－ドン，＃１６，エルジー アール アンド ディー キャンパス，ディーエム ラボラトリー，エヌエーエス グループ

審査官 松永 隆志

(56)参考文献 再公表特許第２００３／０８１４９９（ＪＰ，Ａ１）
特開２００２－１６３３９６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04N 7/173