(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4705958号
(P4705958)
(45)発行日　平成23年6月22日(2011.6.22)　(24)登録日　平成23年3月18日(2011.3.18)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
H04L 9/00 601E

請求項の数 10　(全 20 頁)

(21)出願番号	特願2007-546577 (P2007-546577)
(86)(22)出願日	平成18年1月13日 (2006.1.13)
(65)公表番号	特表2008-524914 (P2008-524914A)
(43)公表日	平成20年7月10日 (2008.7.10)
(86)国際出願番号	PCT/KR2006/000158
(87)国際公開番号	WO2006/075900
(87)国際公開日	平成18年7月20日 (2006.7.20)
審査請求日	平成19年6月15日 (2007.6.15)
(31)優先権主張番号	60/643,997
(32)優先日	平成17年1月14日 (2005.1.14)
(33)優先権主張国	米国(US)
(31)優先権主張番号	10-2005-0029717
(32)優先日	平成17年4月9日 (2005.4.9)
(33)優先権主張国	韓国(KR)

(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，ヨンドゥンポーク，ヨイド－ドン，２０
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明
(74)代理人　100113413
弁理士　森下　夏樹

最終頁に続く

(54)【発明の名称】ブロードキャスト／マルチキャストサービスにおけるデジタル著作権管理方法

(57)【特許請求の範囲】
【請求項１】
ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理方法であって、
前記方法は、端末によって実行され、
前記方法は、
ネットワークとの登録手順を実行することであって、前記端末の公開キーは、ブロードキャストチャネルまたは双方向チャネルを介して実行される前記登録手順の間に共有される、ことと、
共通ドメインキーを共有する複数のサービスを含むサービスバンドルに対応するサービスドメインに参加するための要求メッセージを前記ネットワークに送信することと、
前記サービスバンドルに対する前記共通ドメインキーを前記ネットワークから受信することであって、前記共通ドメインキーは、前記公開キーを用いることによって暗号化されている、ことと、
複数のサービス暗号化キー（ＳＥＫ）を含むサービスドメイン使用権利（ＲＯ）を前記ネットワークから受信することであって、各ＳＥＫは、前記受信された共通ドメインキーによって暗号化され、前記サービスドメインＲＯは、前記サービスドメインに参加した複数の端末に、前記双方向チャネルを介して直接伝送されるか、前記ブロードキャストチャネルを介してブロードキャストされる、ことと、
前記複数のＳＥＫのうちの１つを用いることによって暗号化されたトラヒック暗号化キ

ー（ＴＥＫ）を前記ネットワークから受信することであって、前記ＴＥＫは、前記双方向チャネルを介して直接伝送されるか、前記ブロードキャストチャネルを介してブロードキャストされる、ことと、

前記ブロードキャスト／マルチキャストサービスのサービスデータを前記ネットワークから受信することであって、前記サービスデータは、前記ＴＥＫを用いることによって暗号化される、ことと

を含む、方法。

【請求項２】

前記ＴＥＫを用いることによって前記受信されたサービスデータを復号化することをさらに含む、請求項１に記載の方法。

【請求項３】

前記共通ドメインキーおよび前記サービスドメインＲＯは、前記ネットワークの権利発行装置（ＲＩ）から受信される、請求項１に記載の方法。

【請求項４】

前記要求メッセージは、前記ＲＩからのサービスバンドルまたは特定のサービスを提供するためのサービスドメインに加入することを要求するために用いられるドメイン加入要求メッセージである、請求項３に記載の方法。

【請求項５】

前記サービスドメインへの加入を要求するときに、サービスＩＤまたはサービスバンドルＩＤ、端末ＩＤおよび端末デザイン署名のうちの少なくとも１つが前記ＲＩに送信される、請求項４に記載の方法。

【請求項６】

ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理方法であって、

前記方法は、ネットワークによって実行され、

前記方法は、

端末との登録手順を実行することであって、前記端末の公開キーは、ブロードキャストチャネルまたは双方向チャネルを介して実行される前記登録手順の間に共有される、ことと、

共通ドメインキーを共有する複数のサービスを含むサービスバンドルに対応するサービスドメインに参加するための要求メッセージを前記端末から受信することと、

前記サービスバンドルに対する前記共通ドメインキーを前記端末に送信することであって、前記共通ドメインキーは、前記公開キーを用いることによって暗号化されている、ことと、

複数のサービス暗号化キー（ＳＥＫ）を含むサービスドメイン使用権利（ＲＯ）を前記端末に送信することであって、各ＳＥＫは、前記送信された共通ドメインキーによって暗号化され、前記サービスドメインＲＯは、前記サービスドメインに参加した複数の端末に、前記双方向チャネルを介して直接伝送されるか、前記ブロードキャストチャネルを介してブロードキャストされる、ことと、

前記複数のＳＥＫのうちの１つを用いることによって暗号化されたトラヒック暗号化キー（ＴＥＫ）を前記端末に送信することであって、前記ＴＥＫは、前記双方向チャネルを介して直接伝送されるか、前記ブロードキャストチャネルを介してブロードキャストされる、ことと、

前記ブロードキャスト／マルチキャストサービスのサービスデータを前記端末に送信することであって、前記サービスデータは、前記ＴＥＫを用いることによって暗号化される、ことと

を含む、方法。

【請求項７】

前記共通ドメインキーおよび前記サービスドメインＲＯは、前記ネットワークの権利発行装置（ＲＩ）から送信される、請求項６に記載の方法。

【請求項８】
前記要求メッセージは、前記ＲＩからのサービスバンドルまたは特定のサービスを提供するためのサービスドメインに参加することを要求するために用いられるドメイン参加要求メッセージである、請求項７に記載の方法。
【請求項９】
前記サービスドメインへの参加を要求するときに、サービスＩＤまたはサービスバンドルＩＤ、端末ＩＤおよび端末デザイン署名のうちの少なくとも１つが前記ＲＩによって受信される、請求項８に記載の方法。
【請求項１０】
前記ＴＥＫは、前記ネットワークのＢＣＡＳＴサーバによって前記端末に送信される、請求項６に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、デジタル著作権管理に関し、より詳しくは、移動通信端末のブロードキャスト／マルチキャストサービスにおけるデジタル著作権管理方法に関する。
【背景技術】
【０００２】
一般に、ブロードキャスト／マルチキャストサービスは、地上波放送や付加情報を移動端末に提供するサービスである。前記ブロードキャスト／マルチキャストサービスは、プロバイダがプロバイダ自身のサービスに加入中の全てのクライアントに有用な情報を伝送するブロードキャストサービスと、特定主題又はコンテンツに予め加入した所定グループのクライアントにのみ情報を伝送するマルチキャストサービスとを含む新しいタイプのサービスである。
【０００３】
前記ブロードキャスト／マルチキャストサービスは、複数のクライアントに同時に同一の情報を提供できるため、ネットワークリソースの効率的な管理が可能であり、前記ネットワークリソースの効率的な管理により高帯域アプリケーション（High Bandwidth Application）を提供することができる。また、前記ブロードキャスト／マルチキャストサービスは、クライアントの要求に応じて多様な高速サービスを提供することにより、増加する一方のクライアントの要求事項を満たすことができる。
【０００４】
前記ブロードキャスト／マルチキャストサービスにより提供されるコンテンツに対する権利を安全に保護し体系的に管理するためには、サービス保護及びコンテンツ保護機能が必要である。最近活発に論議されているデジタル著作権管理（Digital Rights Management：ＤＲＭ）は、前記ブロードキャスト／マルチキャストサービスに適用されて前記ブロードキャスト／マルチキャストサービスにより提供されるコンテンツを保護することを可能にする。
【０００５】
前記ＤＲＭは、暗号化技術を用いてコンテンツをパッケージタイプの暗号化したデータに変換した後、認証及び権限確認の手続きを経たユーザのみにオリジナルコンテンツへのアクセスを許可することにより、前記コンテンツの未認証（不法な）使用を事前に防止できる。
【０００６】
従って、従来のブロードキャスト／マルチキャストサービスのデジタル著作権管理方法においては、前記サービスを使用する各端末は、権利発行サーバ（Rights Issuer：ＲＩ）から前記サービスを使用するための使用権利（Rights Object：ＲＯ）を受信した後、暗号化されたサービスデータ又はコンテンツを前記受信されたＲＯを利用して解読する。ここで、前記ＲＯは、各端末の公開キー（Public key：ＰＫ）を利用して暗号化される。

【０００７】
すなわち、前記ＲＩは、各端末の公開キーを利用して暗号化されたＲＯを前記ブロードキャスト／マルチキャストサービスを利用する端末に伝送しなければならない。例えば、前記ブロードキャスト／マルチキャストサービスを利用する端末の数がＫである場合、前記ＲＩは、Ｋ個の端末のそれぞれの公開キーを利用して暗号化されたそれぞれのＲＯを生成して前記全ての端末に繰り返し伝送しなければならない。
【０００８】
しかしながら、前記ブロードキャスト／マルチキャストサービスのデジタル著作権管理方法においては、前記サービスを利用する端末が多い場合、前記ＲＩは、各端末の公開キーを利用して暗号化されたＲＯを１つずつ生成／管理しなければならない。これにより、動作負荷が増加し、ネットワークの効率的な管理及び動作が困難になる。
【発明の開示】
【発明が解決しようとする課題】
【０００９】
従って、本発明の重要な点は、前述したように、従来の特定問題を本発明の発明者が認識しているということである。その結果、本発明者は、次のとおりこのような問題に対する解決策を提供している。
【００１０】
本発明の目的は、同一のサービスを利用する移動通信端末グループに対するデジタル著作権を効率的に管理できるブロードキャスト／マルチキャストサービスのデジタル著作権管理方法を提供することにある。
【００１１】
本発明の他の目的は、同一のサービスパッケージを使用する移動通信端末グループに対するデジタル著作権を効率的に管理できるブロードキャスト／マルチキャストサービスのデジタル著作権管理方法を提供することにある。
【課題を解決するための手段】
【００１２】
このような目的を達成するために、１つ以上の端末に同一のサービスデータを同時に提供するためのブロードキャスト／マルチキャストサービスにおけるデジタル著作権管理方法は、権利発行サーバ（ＲＩ）が同一のサービスを使用する端末に同一の使用権利（ＲＯ）及び前記ＲＯを解読するための暗号化キーを伝送すると、前記端末がブロードキャスト／マルチキャストサーバから受信した暗号化されたサービスデータを前記送信されたＲＯ及び前記暗号化キーを利用して解読する。
【００１３】
本発明の第１態様によると、同時に１つ以上の端末に暗号化されたサービスデータを提供するためのブロードキャスト／マルチキャストサービスにおけるデジタル著作権管理方法は、ＲＩがサービス登録を要求した特定端末から公開キーを受信する段階と、前記ＲＩが前記端末から特定ドメインに対する加入要求を受信すると、前記特定ドメインに対するドメインキーを前記端末に伝送する段階と、前記ＲＩから前記ドメインに提供されたサービスデータに対するドメイン使用権利を前記端末に伝送する段階とを含む。
【００１４】
本発明の第２態様によると、ブロードキャスト／マルチキャストサービスにおけるデジタル著作権管理方法は、ＲＩが特定端末から登録要求及び公開キーを受信する段階と、前記ＲＩが前記端末から特定サービスドメインに対する加入要求を受信した場合、前記サービスドメインに対するドメインキーを前記端末に伝送する段階と、前記ＲＩが前記ドメインキーを利用して前記サービスドメインに対するサービスドメイン使用権利を暗号化し、前記暗号化されたサービスドメイン使用権利を前記端末に伝送する段階とを含む。
【００１５】
本発明の第３態様によると、ブロードキャスト／マルチキャストサービスにおけるデジタル著作権管理方法は、ＲＩが特定端末から登録要求及び公開キーを受信する段階と、前

記ＲＩが前記特定端末から特定サービスドメインに対する加入要求を受信した場合、前記公開キーを利用して前記サービスドメインに対するドメインキーを暗号化し、前記暗号化されたドメインキーを前記端末に伝送する段階と、前記ＲＩが前記ドメインキーを利用して前記サービスドメインに対するサービスドメイン使用権利を暗号化した後、前記暗号化されたサービスドメイン使用権利を前記端末に伝送する段階と、前記ＲＩが前記サービスドメイン使用権利に含まれるキーメッセージ暗号化キーを利用してサービスデータ暗号化キーを暗号化した後、前記暗号化されたサービスデータ暗号化キーを前記端末に伝送する段階とを含む。

【００１６】

本発明の第４態様によると、ブロードキャスト／マルチキャストサービスにおけるデジタル著作権管理方法は、ＲＩが特定端末から登録要求及び公開キーを受信する段階と、前記ＲＩが前記端末から特定サービスバンドルに対する加入要求を受信した場合、前記サービスバンドルに対するドメインキーを前記端末に伝送する段階と、前記ＲＩが前記ドメインキーを前記サービスバンドルに対するサービスバンドル使用権利を暗号化した後、前記暗号化されたサービスバンドル使用権利を前記端末に伝送する段階とを含む。

【００１７】

本発明の第５態様によると、ブロードキャスト／マルチキャストサービスにおけるデジタル著作権管理方法は、ＲＩが特定端末から登録要求及び公開キーを受信する段階と、前記ＲＩが前記端末から特定サービスバンドルに対する加入要求を受信した場合、前記公開キーを利用して前記サービスバンドルに対するドメインキーを暗号化した後、前記暗号化されたドメインキーを前記端末に伝送する段階と、前記ＲＩが前記ドメインキーを利用して前記サービスバンドルに対するサービスバンドル使用権利を暗号化した後、前記暗号化されたサービスバンドル使用権利を前記端末に伝送する段階と、前記ＲＩが前記サービスバンドル使用権利内に含まれているキーメッセージ暗号化キーを利用してサービスデータ暗号化キーを暗号化した後、前記暗号化されたサービスデータ暗号化キーを前記端末に伝送する段階とを含む。

【００１８】

本発明の第６態様によると、１つ以上の端末に暗号化されたサービスデータを提供するためのブロードキャスト／マルチキャストサービスにおけるデジタル著作権管理方法は、サービス登録を要求するために端末がＲＩに端末自身の暗号化キーを伝送する段階と、前記端末が特定ドメインに加入し、前記ＲＩから前記ドメインに対するドメインキーを受信する段階と、前記端末が前記ＲＩから前記ドメインキーを利用して暗号化されたドメイン使用権利を取得する段階と、前記端末が暗号化されたサービスデータを受信した場合、前記サービスデータを解読するためのサービスデータ暗号化キーを有しているか否かを確認する段階と、前記端末が前記サービスデータ暗号化キーを有していると確認された場合、前記サービスデータ暗号化キーを検出して前記サービスデータを解読する段階とを含む。

【００１９】

本発明の前記及び他の目的、特徴、態様、及び長所は、後述する発明の詳細な説明及び添付図面によりさらに明確になるであろう。

【発明の効果】

【００２０】

本発明によるブロードキャスト／マルチキャストサービスにおけるデジタル著作権管理方法において、ＲＩがサービスに参加している端末の数と関係なく全てのサービスドメインに対して１つのドメインＲＯのみを発行することにより、ＲＩの負荷を低減できるという効果がある。

【００２１】

また、本発明によるブロードキャスト／マルチキャストサービスにおけるデジタル著作権管理方法において、ＲＯがドメインユニットにより発行され、前記サービスを利用する全ての端末が短時間で前記ＲＯを受信することによりネットワークを効率的に使用することができるという効果がある。

【発明を実施するための最良の形態】
【００２２】
以下、本発明によるブロードキャスト／マルチキャストサービスにおけるデジタル著作権管理方法の実施形態を添付図面を参照して説明する。
【００２３】
一般に、デジタル著作権管理において、コンテンツ使用権利及びコンテンツ暗号化キーを共有するために、多様な装置（端末を含む）はドメインと呼ばれる概念を利用する。
【００２４】
ドメインの使用は、一人のユーザが所有した多様な装置間でコンテンツ及びコンテンツ使用権利を共有することを可能にし、コンテンツ発行サーバ（Contents Issuer）又は権利発行サーバにアクセスできない装置は、アクセス可能装置を利用してコンテンツ及びコンテンツ使用権利を取得することができる。例えば、無線インターネット能力を有しない携帯用音楽再生機をインターネットアクセスできるパーソナルコンピュータ（ＰＣ）に接続してコンテンツ及びコンテンツ使用権利を取得することができる。従って、前記権利発行サーバは、前記ドメインに属する装置への参加要求及び脱退要求を処理するために前記ドメインを管理する。
【００２５】
本発明は、特定タイプのブロードキャストドメインを提供する。サービス又はサービスバンドルに加入した全ての端末は、共通グループキーを共有する。前記共通グループキーを利用してサービス暗号化キー（Service Encryption Keys：ＳＥＫ）又はプログラム暗号化キー（Program Encryption Keys：ＰＥＫ）を暗号化する。このようなタイプのブロードキャストドメインをサービスドメインという。すなわち、サービス又はサービスバンドルに加入して共通暗号化キー（common encrypted key）を共有する端末のセット（又は、グループ）をサービスドメインという。ここで、選択的に組み合わせられた１つ以上のサービスのセット（又は、グループ）をサービスバンドルという。
【００２６】
サービスドメイン内の端末は、コンテンツ又はサービスプロバイダにより明示された許可条件に従って、他の端末と同一のサービスドメイン内でコンテンツ及びサービスを共有できる。サービスドメインの利点は、ＳＥＫの変更の通信における帯域の消費が非常に少ないことである。
【００２７】
本発明において、ＲＩは、端末に同一のサービス又はサービスバンドルを利用する端末グループのサービスドメインに対するキーメッセージを伝送する。
【００２８】
ここで、前記キーメッセージとは、前記ＲＩから端末（装置）に伝送されたサービスドメイン（端末が参加する場合）を利用する権利に関する情報を提供する手段を意味する。１つの例としてはサービスドメイン使用権利（すなわち、ＲＯ）があるが、これに限定されるものではない。以下、本発明において、説明の便宜のために、「使用権利」と略称する。また、他の種類のキーメッセージ又は他の情報提供手段も利用できる。
【００２９】
前記ドメイン使用権利（ＲＯ）を受信した各端末は、端末自身のドメインに該当するドメインＲＯを端末自身が有するドメインキーを利用して復号化する。ここで、前記ＲＩは、前記サービス又は前記サービスバンドルを使用する端末の数とは関係なくサービスドメインの数と同一の数のＲＯを発行する。前記同一のドメインに属する端末は、同一のドメインキーを互いに共有する。
【００３０】
本発明において、ＲＩは、サービス登録を要求する端末から公開キーを受信し、端末が使用しようとするドメインに該当するドメインキーを前記公開キーを利用して暗号化した後、前記暗号化されたドメインキーを伝送する。前記ＲＩは、前記ドメインキーを利用して暗号化されたドメインＲＯを伝送する。ここで、前記ドメインＲＯは、前記ブロードキ

ャスト／マルチキャストサーバから受信された暗号化されたサービスデータを復号化するためのサービスデータ暗号化キーを含む。

【００３１】

本発明において、前記ＲＩは、サービス登録を要求する端末から公開キーを受信する。前記ＲＩは、前記公開キーを利用して前記端末が利用しようとするドメインに該当するドメインキーを暗号化した後、前記暗号化されたドメインキーを前記端末に伝送する。また、前記ＲＩは、前記ドメインキーを利用してキーメッセージ暗号化キーを含むドメインＲＯを暗号化した後、前記暗号化されたドメインＲＯを前記端末に伝送する。さらに、前記ＲＩは、前記キーメッセージ暗号化キーを利用してブロードキャスト／マルチキャストサーバから受信されたサービスデータを復号化するためのサービスデータ暗号化キーを暗号化した後、前記暗号化されたサービスデータ暗号化キーを前記端末に伝送する。

【００３２】

図１は、本発明によるブロードキャスト／マルチキャストサービスシステムの構成を示すブロック図である。前記ブロードキャスト／マルチキャストサービスシステムは、端末１０と、前記端末１０にサービスを提供するブロードキャスト／マルチキャスト（ＢＣＡＳＴ）サーバ２０と、前記端末１０がサービスを利用できるようにする使用権利（ＲＯ）を管理する権利発行サーバ（ＲＩ）３０とから構成される。

【００３３】

ここで、前記ＲＩ３０が前記ＲＯを前記端末１０に伝送するか、前記ＢＣＡＳＴサーバ２０が前記ＲＩ３０から前記ＲＯを受信した後、前記受信されたＲＯを前記端末１０に伝送する。

【００３４】

本発明は、利用されるサービス又はサービスバンドルによって前記端末を区分する。前記サービスバンドルは、互いに関連のない１つ以上のサービス（コンテンツ）を結合して１つのパッケージタイプに構成したものである。ここで、サービス又はサービスバンドルに加入して共通暗号化キーを共有する端末のセット（グループ）をサービスドメインという。また、選択的に結合された１つ以上のサービスのセット（グループ）をサービスバンドルという。ここで、１つの端末は、１つ以上のサービスドメインに属することができる。

【００３５】

図２は、サービスバンドルの概念を示す図である。

【００３６】

図２に示すように、サービスバンドル１は、サービス１とサービス２を含むパッケージであり、サービスバンドル２は、サービス１とサービス３を含むパッケージであり、サービスバンドル３は、サービス１を含み、サービスバンドル４は、サービス３とサービス４を含むパッケージであると仮定する。前記サービスバンドル１に加入している端末は、サービス１とサービス２を利用でき、前記サービスバンドル４に加入している端末は、サービス３とサービス４を利用できる。ここで、複数の端末のグループがサービスバンドル内で１つ以上のサービスを利用できる。

【００３７】

従って、ＲＩ３０は、各端末１０に対するＲＯを発行するのではなく、前記端末１０が属するサービスドメインに対するＲＯを発行する。すなわち、同一のサービスドメインに属する端末１０は、ＲＩ３０から同一のドメインＲＯを受信する。このようなドメインＲＯは、各ドメインに該当するドメインキーを利用して暗号化され、前記同一のドメインに属する端末１０がＲＯを復号化するために前記ドメインキーを利用できる。

【００３８】

図３は、本発明によるサービスドメインに基づいた動作方法を示す図である。ここで、第１端末１１及び第２端末１２は、第１サービスバンドルに加入し、第３端末１３は、第２サービスバンドルに加入している。

【００３９】

まず、前記第１端末１１及び第２端末１２は、ＲＩ（図示せず）から第１サービスドメインに対するドメインキーを受信して保有し、前記第３端末１３は、第２サービスドメインに対するドメインキーを受信して保有する。

【００４０】

ＲＩ又はブロードキャスト／マルチキャストサーバ２０は、各端末１１、１２、１３にサービスドメインＲＯを伝送する。図３は、前記ブロードキャスト／マルチキャストサーバ２０が前記ＲＩ（図示せず）から各サービスドメインに対するＲＯを受信して各端末１１、１２、１３に前記受信されたＲＯを伝送する例を示す。

【００４１】

前記ドメインＲＯを受信した各端末１１、１２、１３は、端末自分が有するドメインキーを利用して前記ドメインＲＯを復号化する。すなわち、前記第１端末１１及び第２端末１２は、前記受信された２つのドメインＲＯのうち第１サービスドメインＲＯを復号化でき、前記第３端末１３は、第２サービスドメインＲＯを復号化できる。

【００４２】

前述したように、本発明において、前記ＲＩ又はブロードキャスト／マルチキャストサーバがサービスを利用する端末の数に関係なくサービスドメインの数だけドメインＲＯを発行し、各端末は、前記ドメインＲＯのうち端末自身が保有するドメインキーを利用して復号化できるドメインＲＯのみを復号化する。従って、本発明によるサービスシステムは、サービス（コンテンツ）に対するセキュリティを維持すると同時に、前記サーバと端末間のネットワークを効率的に使用することができる。

【００４３】

図４は、本発明によるデジタル著作権管理方法に関する第１実施形態を示す信号フローチャートである。特に、図４は、端末がドメインＲＯとサービスデータを受信する過程をセキュリティキーの階層構造（layered　structure）を参照して示す。

【００４４】

図４に示すように、第１層は、端末１０とＲＩ３０間でサービス登録を実行可能にするために使用される（Ｓ１１）。ここで、このような装置登録は、オフライン又はオンライン方式で行われる。例えば、オンライン方式は、ブロードキャスト又は双方向チャネルを使用する。

【００４５】

端末１０の公開キーは、前記第１層を介してＲＩ３０に伝送され、前記端末１０とＲＩ３０間で使用されるセキュリティアルゴリズムは、ネゴシエートされる。ここで、前記端末１０にはＲＩコンテキストが生成される。前記ＲＩコンテキストは、前記端末１０が前記ＲＩ３０に登録するときにネゴシエートされた情報を含み、特に、ＲＩ　ＩＤ、ＲＩの認証書、バージョン、セキュリティアルゴリズム、及びその他の情報を含む。

【００４６】

ドメイン管理層として利用される第２層は、特定サービスドメインへの加入又はそのドメインからの脱退のために使用される。ここで、前記第２層を利用する前に、端末１０は、端末自身が使用できるブロードキャスト／マルチキャストサービスを記述するための情報（サービス情報、ドメイン情報など）が含まれるサービスガイドを受信する。

【００４７】

前記サービスガイドにより端末１０で利用可能なサービスを確認した後、ユーザが前記端末１０を利用してＲＩ３０にドメイン加入を要求すると（Ｓ１３）、ＲＩ３０は、公開キーを利用して暗号化されたドメインキーを前記端末１０に伝送する（Ｓ１５）。前記ドメイン加入を要求するとき、前記端末１０は、サービスＩＤ又はサービスバンドルＩＤ、端末ＩＤ、及び端末のデジタル署名などをパラメータタイプで伝送する。

【００４８】

前記ドメイン加入の結果として、前記端末１０にはドメインコンテキストが生成される。前記ドメインコンテキストは、ドメインキー、ドメインＩＤ、ドメイン有効期間などの情報を含む。

【００４９】
前記端末１０がＲＩ３０にドメイン脱退を要求すると、前記ＲＩ３０は、前記ドメインに属する端末のリストから該当端末１０を削除し、前記端末１０は、前記ドメインとの関係を削除（終了）する。
【００５０】
第３層は、ＲＯ管理層として利用される。前記ＲＩ３０は、前記第３層を利用して前記サービスドメインＲＯを前記端末１０に伝送する（Ｓ１７）。ここで、前記ドメインＲＯは、前記ドメインキーを利用して暗号化される１つ以上のサービスデータ暗号化キー（例えば、ＳＥＴ）を含む。
【００５１】
前記ＲＩ３０は、前記サービスドメインＲＯを前記端末１０に直接伝送するか、前記ブロードキャスト／マルチキャストサーバ２０を介して端末１０に伝送する。すなわち、前記ＲＩ３０が前記サービスドメインＲＯを前記ブロードキャスト／マルチキャストサーバ２０に伝送すると、前記ブロードキャスト／マルチキャストサーバ２０は、該当ＲＯを前記端末１０に伝送する。ここで、前記ＲＩ３０から伝送されたＲＯは、前記ブロードキャスト／マルチキャストサーバ２０を介して端末１０に伝送される。前記ＲＯを端末１０に直接伝送したり、ブロードキャスト／マルチキャストサーバ２０を介して伝送する動作は、必要に応じて選択的に行われる。ＲＩ３０が前記ブロードキャスト／マルチキャストサーバ２０により行われる必須機能を備える場合、前記ＲＩ３０は、前記ＲＯを端末１０に直接伝送できる。
【００５２】
第４層は、サービス暗号化キーとして利用される。前記ブロードキャスト／マルチキャストサーバ２０は、前記サービスデータ暗号化キーを利用して暗号化されたサービスデータを前記第４層を介して端末１０に伝送する（Ｓ１９）。前記端末１０は、特定サービスドメインに対するＲＯ及び前記特定サービスデータ暗号化キーを利用して暗号化されたサービスデータを受信し、前記ＲＯを利用して前記サービスデータを復号化する。前記端末がサービスデータを復号化する方法は後述する。
【００５３】
従って、前記サービスデータを復号化するためのサービスデータ暗号化キーを前記ドメインキーを利用して暗号化したため、同一のドメインキーを有する端末は、前記サービスデータ暗号化キーを取得して前記サービスデータを実行できる。
【００５４】
図５は、本発明によるデジタル著作権管理方法の第２実施形態を示す信号フローチャートである。端末がドメインＲＯ及びサービスデータを受信する過程をセキュリティキーの階層構造を参照して説明する。
【００５５】
特に、本発明の第２実施形態は、第１実施形態における１つ以上のサービスデータ暗号化キー（例えば、ＳＥＫ）とともに、前記サービスデータ暗号化キーを導くキーメッセージ暗号化キー（例えば、ＴＥＫ（Traffic Encryption Key））をさらに利用することにより、サービスデータの保護及びセキュリティを強化した実施形態である。
【００５６】
従って、前記装置（端末）とＲＩ間で公開キー（ＰＫ）が共有されるだけでなく、前記装置（端末）と前記ＲＩにより使用される特定セキュリティキー（すなわち、ドメインキー、ＳＥＫ、ＴＥＫ）間にも所定の関係がある。すなわち、前記ドメインキーは、１つ以上のＳＥＫを含むＲＯの暗号化及び復号化のために使用され、ＳＥＫは、ＴＥＫの暗号化及び復号化のために使用され、ＴＥＫは、コンテンツの暗号化及び復号化のために使用される。
【００５７】
図５に示すように、まず、前記端末１０が第１層で前記ＲＩ３０に登録を要求した場合（Ｓ２１）、前記端末１０とＲＩ３０間で使用されるセキュリティアルゴリズムがネゴシ

エートされる。ここで、このような装置登録は、オフライン又はオンライン方式で行われる。例えば、オンライン方式による登録は、ブロードキャスト又は双方向チャネルを使用する。

【００５８】

前記登録要求の結果、前記端末１０にはＲＩコンテキストが生成される。前記ＲＩコンテキストは、ＲＩ　ＩＤ、ＲＩの認証書、バージョン、セキュリティアルゴリズムに関する情報、及びその他の情報を含む。

【００５９】

前記第２層で動作を行う前に、端末１０は、端末自身が利用できるブロードキャスト／マルチキャストサービスに関するサービスガイドを受信する。

【００６０】

第２層において、端末１０は、ＲＩ３０に特定サービス又はサービスバンドルを提供するためのサービスドメインへの加入を要求する（Ｓ２３）。前記ＲＩ３０は、端末１０に端末１０の公開キーを利用して暗号化されるドメインキーを伝送する（Ｓ２５）。前記端末１０は、ドメイン加入を要求するとき、サービスＩＤ又はサービスバンドルＩＤ、端末ＩＤ、端末のデジタル署名などを前記ＲＩ３０に伝送する。

【００６１】

従って、ＲＩ３０からドメインキーを受信した端末１０にドメインコンテキストが生成される。前記ドメインコンテキストは、ドメインキー、ドメインＩＤ、ドメイン有効期間などの情報を含む。前記端末１０が１つ以上のサービスドメインへの加入を要求した場合、端末１０が有するドメインキー及びドメインＩＤの数はドメインの数と同一でもよい。

【００６２】

第３層は、ＲＯ管理層として利用される。ＲＩ３０は、前記第３層を介して端末１０にサービスドメインＲＯを伝送する（Ｓ２７）。ここで、前記サービスドメインＲＯは、前記ドメインキーを利用して暗号化される１つ以上のサービスデータ暗号化キー（例えば、ＳＥＫ）を含んでいるので、前記ドメインキーを有するサービスドメインに属する端末のみが前記サービスデータ暗号化キーを復号化できる。

【００６３】

第１実施形態のように、前記ＲＩ３０は、ＲＯを前記端末１０に直接伝送したり、ブロードキャスト／マルチキャストサーバ２０を介して前記端末１０に伝送する。前記ＲＩ３０が前記ブロードキャスト／マルチキャストサーバ２０の必須機能を備えている場合、前記ＲＯを前記端末１０に直接伝送する。

【００６４】

第４層は、キートランスポート層として利用される。ＲＩ３０は、前記キーメッセージ暗号化キーを利用して暗号化されたサービスデータ暗号化キー（例えば、ＴＥＫ）を前記第４層を介して前記端末１０に伝送する。これにより、前記キーメッセージ暗号化キーを有する端末のみが前記サービスデータ暗号化キーを復号化できる。

【００６５】

前記サービスデータ暗号化キーは、前記ＲＩ３０を介してだけでなく、前記ブロードキャスト／マルチキャストサーバ２０を介して前記端末１０に伝送できる。ここで、前記ＲＩ３０が前記サービスデータ暗号化キーを前記ブロードキャスト／マルチキャストサーバ２０に伝送すると、前記ブロードキャスト／マルチキャストサーバ２０が該当サービスデータ暗号化キーを前記端末１０に伝送する。ＲＩ３０が前記ブロードキャスト／マルチキャストサーバ２０の必須機能を備えている場合、前記ＴＥＫを前記端末１０に直接伝送できる。

【００６６】

第５層は、サービス暗号化キーとして利用される。前記ブロードキャスト／マルチキャストサーバ２０は、前記サービスデータ暗号化キーを利用して暗号化されたサービスデータを前記第５層を介して前記端末１０に伝送する（Ｓ３１）。

【００６７】

本発明によるセキュリティキーの階層構造は、サービスドメインとともに第１及び第２実施形態で示したものとは異なる構成を有する。

【００６８】

本発明は、本発明によるサービス保護のためのキー階層（key hierarchy）を示す図６を参照すればより一層理解できる。すなわち、図６は、本発明によるドメインに対するサービス保護のためのキー階層を示す図である。

【００６９】

レイヤ１は、装置（端末）登録を行う。前記登録過程中に取得されたキー要素（key material）及びメタデータは、前記装置がＲＯを復号化して確認し、究極的にはコンテンツに接続できるようにする。

【００７０】

図６は、前記装置が装置登録によりＲＩに装置自身の公開キーを登録し、前記ＲＩが装置公開キーを利用してＳＥＫを暗号化する状況を示す。ここで、前記装置だけでなく、他のドメインも前記ＲＩに登録できる。このために、前記ドメインは、「ドメイン内の装置の公開キー」又は「ドメインキー」を前記ＲＩに登録できる。

【００７１】

レイヤ２は、サービスグループ管理機能を行う。ＯＭＡ　ＤＲＭ参加／脱退ドメインプロトコルは、双方向チャネルに接続できる装置のために使用される。このレイヤは、ドメインキーとしてＳＥＫを伝送する。前記ＳＥＫは、新しいドメイン形成過程又はドメインアップグレード過程によりアップデートされる。

【００７２】

レイヤ３は、著作権（rights）管理機能を行う。サービスキー（例えば、ＳＥＫ）により保護できる使用権利（ＲＯ）は、（一部の）サービスの復号化のために利用されるトラヒックキー（例えば、ＴＥＫ）及び前記トラヒックキーを暗号化されたコンテンツ及びドメインにリンクできるようにする識別子を含む。前記トラヒックキーの寿命（crypto-period）（すなわち、ライフタイム）は、リアルタイム分配攻撃（real-time distribution attacks）を防止するために相対的に短い。

【００７３】

レイヤ３の裏の意図は、強化したセキュリティ、拡張性、及び豊富なユーズケース（use-case）サポートを提供することである。レイヤ３の標準は、このような要求事項を満たすことを保障しなければならない。

【００７４】

ここで、前記構成においては、キー導出（key derivation）のようなセキュリティ要素を変更するなどの解決策が排除されていないという点に注目すべきである。

【００７５】

レイヤ２の実行は、予想外の条件により妨害される可能性があるので、レイヤ３は、レイヤ２の手順が開始してから、適当な時間遅延後に行われるように実現されなければならない。

【００７６】

レイヤ４は、前記トラヒックキーを有するブロードキャストコンテンツの暗号化を実現する。前記暗号化は、ネットワーク層（すなわち、ＩＰ）、トランスポート層（例えば、ＵＤＰ）、又はセッション層（例えば、ＲＴＰ）で行われる。

【００７７】

本発明は、図７～図１０、及び以下のような説明によりさらに理解できる。

【００７８】

サービス及びコンテンツ保護機能は、モバイルブロードキャストサービス（Mobile Broadcast Services）内で伝達されたコンテンツ及びサービスを保護するＢＤＳ－不可知論方式を可能にする。図７は、サービス保護とコンテンツ保護の相違点を示す。

【００７９】

サービス保護の目的は、所定時間の間、特定視聴覚的データのセットのサービスへのア

クセスを可能にすることである。サービス保護は、ユーザ端末が解除されたコンテンツに対するいかなる責任も持たず、アクセス制御を実現するビットパイプ（bit-pipe）外部のコンテンツを保護する技術的手段を提供しないと仮定する。

【００８０】

コンテンツ保護の目的は、個別のコンテンツを保護することである。コンテンツは、コンテンツ自身に関する事後伝達使用権（post-delivery usage rights）を有することも、有しないこともある。

【００８１】

サービス保護は、コンテンツ保護とは異なり、加入管理のためのものでる。コンテンツ保護がない場合、コンテンツに対する使用権は、無料となるか、又は、適用可能な法律、ビジネスモデル、もしくはその他の要求事項に従う。しかし、このような条件は、これらの定義の範囲外である。コンテンツ保護は、許可及び制限によってコンテンツを使用する方法を指定する事後伝達使用権を扱う。

【００８２】

図８は、サービス保護及びコンテンツ保護に対するキー階層を示す。

【００８３】

レイヤ１は、認証を行う。加入者識別（subscriber identity：ＳＩ）又は装置登録手順中に取得されたキー要素及びメタデータは、前記加入者又は装置の認証、及びコンテンツへの順次アクセスを可能にし、端末又はスマートカードに安全に保存される。ここで、前記スマートカードは、ＵＳＩＭ／（Ｒ－）ＵＩＭでもよい。レイヤ１で取得されてレイヤ２で長期キー伝達（Long Term Key delivery）を保護するために使用された前記キー要素は、加入者管理キー（Subscriber Management Key）又は権利暗号化キー（Rights Encryption Key）という。

【００８４】

レイヤ２は、長期キーメッセージ（Long-Term Key Message：ＬＴＫＭ）伝達を行う。このレイヤは、サービス暗号化キー（ＳＥＫ）又はプログラム暗号化キー（ＰＥＫ）を伝達する。前記サービス又はプログラム暗号化キーは、中間キーであり、コンテンツを直接暗号化する代わりにＴＥＫの順序を保護する。サービス加入管理及び保護のために、ＳＥＫ又はＰＥＫは、普通ＴＥＫトラヒックキーより長い寿命を有するようにアップデートされる。

【００８５】

レイヤ３は、ブロードキャストチャネル又は双方向チャネルで短期（Short-Term）キーメッセージ伝達を行う。ＳＥＫもしくはＰＥＫにより暗号化されたＴＥＫ、又は前記トラヒックキーを伝達するために使用できる必要データを、前記トラヒックキーと暗号化されたコンテンツとをリンクできるようにする識別子とともに前記端末に伝送する。

【００８６】

レイヤ３の裏の意図は、強化したセキュリティ、拡張性、及び豊富なユーズケースサポートを提供することである。レイヤ３の標準は、このような意図を満たすことを保障しなければならない。

【００８７】

レイヤ４、又は保護は、短期トラヒックキー（Short-Term traffic key）を利用してブロードキャストコンテンツの暗号化を行う。このような暗号化は、サービス保護のためにネットワーク層（すなわち、ＩＰ）、トランスポート層（例えば、ＵＤＰ）、セッション層（例えば、ＲＴＰ）、又はコンテンツ層（AU encryption）で行われる。

【００８８】

図９は、サービス保護機能ブロック及びそれらの間のインタフェースを示す。図９に示す特徴は、この分野の通常的知識を有する者であれば理解できるので、詳しい説明は省略する。

【００８９】

図１０は、インタフェースを定義し、これらをＢＣＡＳＴ基準点にマッピングするテー

ブルを示す。

【００９０】

ファイルアプリケーション／ストリームアプリケーション機能（File Application/Stream Application Function：ＦＡ／ＳＡ）

ＢＳＡにおけるファイルアプリケーション／ストリームアプリケーション機能は、ファイル及びストリームをＣｏｎｔｅｎｔ Ｃｒｅａｔｉｏｎから受信し、前記ファイル及びストリームを属性情報及び付加的な情報とともにＢＣＡＳＴサービス分配／適用（Service Distribution/Adaptation）に伝送する役割を果たす。

【００９１】

ＳＰ管理機能

ＢＳＭにおけるサービス保護管理機能（Service Protection Management Function：ＳＰ－Ｍ）は、登録、及び双方向チャネルでのＬＴＫＭ伝達を担当する。前記ＳＥＫを含む長期キーメッセージは、前記ＳＰ－Ｍからサービス保護クライアント機能（Service Protection Client Function：ＳＰ－Ｃ）に伝送される。ブロードキャスト専用（broadcast-only）端末は、登録、及び長期キーメッセージ伝達の要求を開始するために帯域外チャネルを要求する。前記ブロードキャスト専用端末は、前記登録及び長期キーメッセージ伝達に対する応答をブロードキャストチャネルで受信する。

【００９２】

前記ＳＰ－Ｍは、また、ＳＴＫＭ伝達及び安全なグループ管理を担当する。前記ＳＰ－ＭからＳＰ－ＫＤに伝達されたＳＴＫＭは、前記ブロードキャストチャネルで前記ＳＰ－Ｃに分配される。前記安全なグループ管理方法は、前記長期キーメッセージの効率的なブロードキャスト及び廃止手順のために使用される。前記ＳＰ－Ｍは、ドメイン管理を担当する。前記端末は、前記ＳＰ－Ｍを利用してドメインに参加したり、ドメインから脱退できる。

【００９３】

ＳＰキー分配機能

ＢＳＤ／Ａにおけるサービス保護キー分配機能（Service Protection Key Distribution Function：ＳＰ－ＫＤ）は、ＬＴＫＭ及びＳＴＫＭのブロードキャストを担当する。前記端末は、暗号化されたサービスの復号化のためにＳＴＫＭからＴＥＫを取得できる。前記ＳＴＫＭ、ＬＴＫＭ、及び登録キー要素は、ＳＰ－ＭからＳＰ－ＫＤに伝送されて前記端末に分配される。前記ＳＰ－ＫＤは、ブロードキャスト専用端末のためにブロードキャストチャネルで前記ＳＴＫＭ、ＬＴＫＭ、及びキー要素を伝達する。

【００９４】

ＳＰ暗号化機能

前記ＢＳＤ／Ａにおけるサービス保護暗号化機能（Service Protection Encryption Function：ＳＰ－Ｅ）は、サービスを暗号化してブロードキャストチャネルで伝達するための機能を担当する。ＳＰ－Ｍから伝達されたＴＥＫは、サービスを暗号化するために使用される。前記暗号化されたサービスのフォーマットは、特定サービス保護システムに基づく。

【００９５】

ＳＰ復号化機能

端末におけるサービス保護復号化機能（Service Protection Decryption Function：ＳＰ－Ｄ）は、ＳＴＫＭから抽出されたＴＥＫを利用して前記暗号化されたサービスを復号化する機能を担当する。前記ＳＴＫＭは、ＳＰ－ＭからＳＰ－ＫＤに伝達され、前記ＳＰ－Ｃは、ブロードキャストチャネルで前記ＳＰ－ＫＤから前記ＳＴＫＭを受信する。

【００９６】

ＳＰクライアント機能

前記サービス保護クライアント機能（ＳＰ－Ｃ）は、端末にのみ存在するか、端末とスマートカードの両方に存在する。前記ＳＰ－Ｃは、登録並びにＬＴＫＭ及びＳＴＫＭの取得を担当する。前記登録の後、前記ＳＰ－Ｃは、登録の結果ＲＥＫ、ＳＭＫ、又はＧＭＫ

を取得する。前記ＬＴＫＭは、前記ＳＴＫＭを暗号化するために利用されるＳＥＫを含む。前記ＳＰ－Ｃは、また、ＳＥＫを利用してＳＴＫＭを復号化することによりＴＥＫを取得し、前記ＴＥＫは、前記暗号化されたサービスの復号化のために前記ＳＰ－Ｄに伝送される。

【００９７】

本発明は、ブロードキャスト／マルチキャストサービス方法を提供し、前記方法は、共通グループキーを有するサービスドメインに参加するための要求を端末から受信する段階と、前記共通グループキーを利用して１つ以上のサービス暗号化キーを暗号化して参加を要求した前記端末に伝送する段階と、前記サービスドメイン内で同一のコンテンツ及び同一のサービスを前記端末が１つ以上の他の装置と共有できるようにする段階とを含む。

【００９８】

前記共有できるようにする段階は、１つ以上のサービス暗号化キーを含むとともに、前記共通グループキーを利用して暗号化される使用権利を伝送する段階をさらに含む。前記サービスドメインは、少なくとも１つのサービスを含むか、又は、複数のサービスを有するサービスバンドルを含む。各サービスは、サービス暗号化キーを含む。各サービス暗号化キーは、１つ以上のトラヒック暗号化キーを暗号化するために使用される。前記トラヒック暗号化キーは、同一のコンテンツ及び同一のサービスのサービスデータを暗号化するために使用される。

【００９９】

また、本発明は、ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理方法を提供し、前記方法は、共通グループキーを共有するサービスドメインへの参加要求を端末から受信する段階と、前記端末が少なくとも１つの他の装置と前記サービスドメイン内で同一のコンテンツ及び同一のサービスを共有できるように、前記サービスドメインに参加している端末に前記共通グループキーを利用して暗号化された１つ以上のサービス暗号化キーを有するキーメッセージを伝達する段階とを含む。

【０１００】

前記キーメッセージは、使用権利であり、前記サービスドメインは、少なくとも１つのサービスを含むか、又は、複数のサービスを有するサービスバンドルを含む。各サービスは、サービス暗号化キーを含み、各サービス暗号化キーは、１つ以上のトラヒック暗号化キーを暗号化するために使用される。前記トラヒック暗号化キーは、サービスデータ又はコンテンツを暗号化するために使用される。

【０１０１】

また、本発明は、ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理方法を提供し、前記方法は、サービスドメインに参加するとき、共通グループキーを受信する段階と、１つ以上のサービス暗号化キーを含むとともに、前記共通グループキーを利用して暗号化される使用権利を受信する段階と、サービスデータを受信した後、前記受信された使用権利を利用して前記受信されたサービスデータを復号化する段階とを含む。

【０１０２】

前記サービスドメインは、少なくとも１つのサービスを含むか、又は、複数のサービスを有するサービスバンドルを含む。各サービスは、サービス暗号化キーを含み、各サービス暗号化キーは、１つ以上のトラヒック暗号化キーを暗号化するために使用される。前記トラヒック暗号化キーは、サービスデータ又はコンテンツを暗号化するために使用される。

【０１０３】

また、本発明は、ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理方法を提供し、前記方法は、装置と権利発行サーバ間で登録手順をネゴシエートする段階と、前記装置が前記サービスドメインに参加した全ての装置に関するドメインキーを共有できるようにするために、前記ネゴシエートされた登録手順に従って前記装置と権利発行サーバ間にサービスドメイン参加手順を行う段階と、前記ドメインキーを利用して暗

号化された１つ以上のサービスデータ暗号化キーを含めることにより、前記装置に前記サービスドメイン使用権利を提供する段階と、前記サービスデータ暗号化キー及び前記ドメインキーを利用した前記サービスデータの復号化を許可することにより、前記端末が前記権利発行サーバから伝送されたサービスデータのコンテンツに接続できるようにする段階とを含む。

【０１０４】

前記提供段階は、キーメッセージ暗号化キーを利用して暗号化されたサービスデータ暗号化キーを前記権利発行サーバから前記装置に伝送する段階をさらに含む。

【０１０５】

本発明は、ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理システムを提供し、前記システムは、前記ブロードキャスト／マルチキャストサービスのコンテンツを提供するためのコンテンツプロバイダサーバと、サービスドメインに参加した全ての装置に関するドメインキーを共有する前記サービスドメインに参加した後、前記ブロードキャスト／マルチキャストサービスのコンテンツを受信するための装置と、前記コンテンツプロバイダサーバ及び前記装置と連動し、前記装置が前記サービスドメインに参加して前記コンテンツプロバイダサーバから提供されたコンテンツをサービスデータ暗号化キー及びトラヒック暗号化キーを利用して適切に復号化する権利発行サーバとを含む。

【０１０６】

前記サービスデータ暗号化キーは、ブロードキャスト／マルチキャストサーバを介して前記権利発行サーバから前記装置に伝送される。

【０１０７】

本発明は、ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理方法を提供し、前記方法は、前記装置がドメインキーを共有できるように、ネゴシエートされた登録手順に基づいて装置と権利発行サーバ間のサービスドメイン参加手順を行う段階と、前記ドメインキーを利用して暗号化され、少なくとも１つのサービス暗号化キーを有する少なくとも１つの使用権利を、前記権利発行サーバから装置に伝送する段階と、前記サービス暗号化キーを利用して暗号化されたトラヒック暗号化キーを利用して復号化するとき、前記装置で前記ブロードキャスト／マルチキャストサービスのコンテンツを利用する段階とを含む。

【０１０８】

本発明は、ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理をサポートする端末を提供し、前記端末は、信号及び情報を送受信する送受信機と、前記送受信機と連動し、共通グループキーを有するサービスドメインに参加するための要求を端末から受信する段階と、前記サービスドメイン内で１つ以上の他の装置と同一のコンテンツ及び同一のサービスを共有できるように、前記共通グループキーを利用して１つ以上のサービス暗号化キーを暗号化した後、前記参加要求をした端末に伝送する段階とを行うプロセッサとを含む。

【０１０９】

本発明は、ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理をサポートする端末を提供し、前記端末は、ネットワークと信号及び情報を送受信する送受信機と、前記送受信機と連動し、共通グループキーを共有するサービスドメインに参加するための要求を前記ネットワークに伝送する段階と、前記サービスドメイン内で少なくとも１つの他の装置と同一のコンテンツ及び同一のサービスを共有できるように、前記ネットワークで前記共通グループキーを利用して暗号化された１つ以上のサービス暗号化キーを有するキーメッセージを受信する段階とを行うプロセッサとを含む。

【０１１０】

本発明は、ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理をサポートする端末を提供し、前記端末は、ネットワークと信号及び情報を送受信する送受信機と、前記送受信機と連動し、サービスドメインに参加するときに共通グループキーを受信する段階と、１つ以上のサービス暗号化キーを含むとともに、前記共通グループキー

を利用して暗号化された使用権利を受信する段階と、サービスデータを受信した後、前記受信された使用権利を使用して前記受信されたサービスデータを復号化する段階とを行うプロセッサとを含む。

【０１１１】

本発明は、ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理をサポートする端末を提供し、前記端末は、ネットワークと信号及び情報を送受信する送受信機と、前記送受信機と連動し、前記ネットワークの権利発行サーバと登録手順をネゴシエートする段階と、前記サービスドメインに参加した全ての装置に関するドメインキーを共有できるように、前記ネゴシエートされた登録手順に従って前記権利発行サーバとサービスドメイン参加手順を行う段階と、前記権利発行サーバが前記ドメインキーを利用して暗号化された１つ以上のサービスデータ暗号化キーを含む前記サービスドメインの使用権利を受信する段階と、前記サービスデータ暗号化キー及びドメインキーを利用して前記権利発行サーバが伝送したサービスデータを復号化することにより前記サービスデータのコンテンツにアクセスする段階とを行うプロセッサとを含む。

【０１１２】

本発明は、ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理をサポートする端末を提供し、前記端末は、権利発行サーバ及びコンテンツプロバイダサーバを備えたネットワークと信号及び情報を送受信する送受信機と、前記送受信機と連動し、サービスドメインに参加した全ての装置に関するドメインキーを共有する前記サービスドメインに参加した後、前記ブロードキャスト／マルチキャストサービスのコンテンツを受信する段階と、前記サービスドメインに参加できるように、前記権利発行サーバ及びコンテンツプロバイダサーバと連動する段階と、前記コンテンツプロバイダサーバから提供されたコンテンツをサービス暗号化キー及びトラヒック暗号化キーを利用して適切に復号化する段階とを行うプロセッサとを含む。

【０１１３】

本発明は、ブロードキャスト／マルチキャストサービスのためのデジタル著作権管理をサポートする端末を提供し、前記端末は、ネットワークと信号及び情報を送受信する送受信機と、前記送受信機と連動し、ドメインキーを共有できるように、ネゴシエートされた登録手順に従って権利発行サーバとサービスドメイン参加手順を行う段階と、前記権利発行サーバが前記ドメインキーを利用して暗号化された少なくとも１つのサービス暗号化キーを含む少なくとも１つの使用権利を前記権利発行サーバから受信する段階と、前記サービス暗号化キーを利用して暗号化されたトラヒック暗号化キーを利用して復号化するとき、前記ブロードキャスト／マルチキャストサービスのコンテンツを利用する段階とを行うプロセッサとを含む。

【０１１４】

前述したような多様な特性を実現するために、本発明は、多様な形態のハードウェア及び／又はソフトウェア構成要素（モジュール）を採用する。例えば、他のハードウェアモジュールは、前記方法の段階を行うために必要な多様な回路および構成要素を含む。また、プロセッサ及び他のハードウェアにより実行される他のソフトウェアモジュールは、前記方法の段階を行うために必要な多様なコード及びプロトコルを含む。

【０１１５】

本発明の思想や重要な特性から外れない限り、本発明は多様な形態で実現することができ、前述した実施形態によって限定されるものでなく、むしろ請求の範囲に記載の本発明の思想や範囲内で広く解釈されるべきであり、本発明の請求の範囲内で行われるあらゆる変更及び変形、並びに請求の範囲の均等物は本発明の請求の範囲に含まれる。

【図面の簡単な説明】

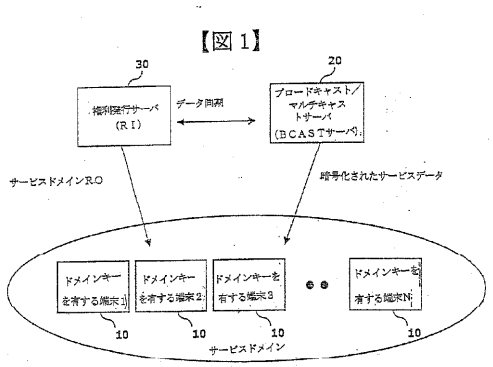
【０１１６】

発明の理解を容易にするために添付され、本明細書の一部を構成する図面は、発明の多様な実施形態を示し、明細書と共に発明の原理を説明するためのものである。

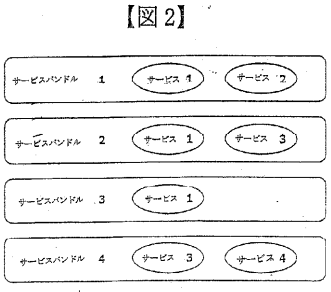
【図１】本発明によるブロードキャスト／マルチキャストサービスシステムの構成を示す

ブロック図である。
【図２】サービスバンドルの例を示す図である。
【図３】本発明によるサービスドメインに基づいた動作方式の例を示す図である。
【図４】本発明によるデジタル著作権管理方法の第１実施形態を示す信号フローチャートである。
【図５】本発明によるデジタル著作権管理方法の第２実施形態を示す信号フローチャートである。
【図６】本発明によるサービス保護のためのキー階層を示す図である。
【図７】本発明によるサービス保護とコンテンツ保護の相違点を示す図である。
【図８】本発明によるサービス保護及びコンテンツ保護に対するキー階層の例を示す図である。
【図９】本発明によるサービス保護機能ブロックとそれらの間のインタフェースを示す図である。
【図１０】本発明によるインタフェースを定義して前記インタフェースをＢＣＡＳＴ基準点にマッピングするテーブルを示す図である。

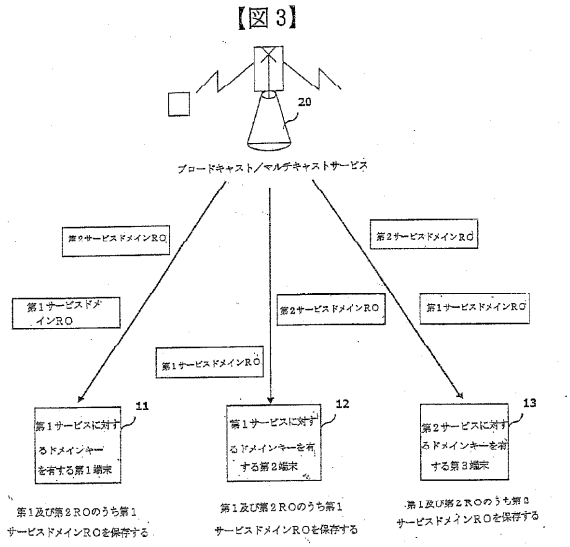
【図１】



【図２】

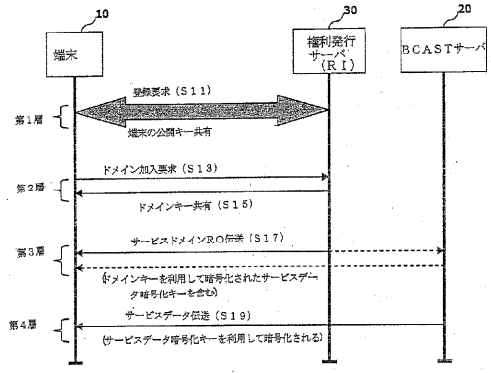


【図３】



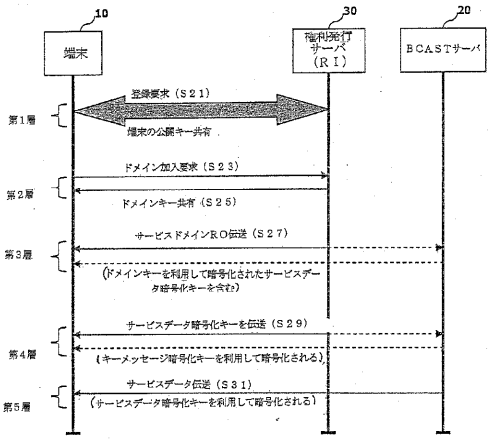
【図４】

【図4】



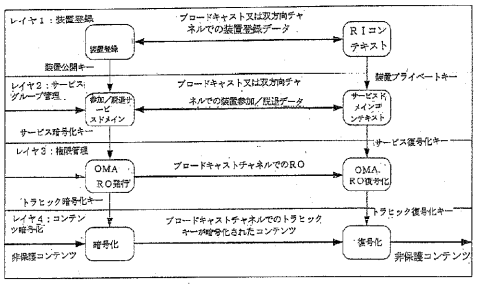
【図５】

【図5】



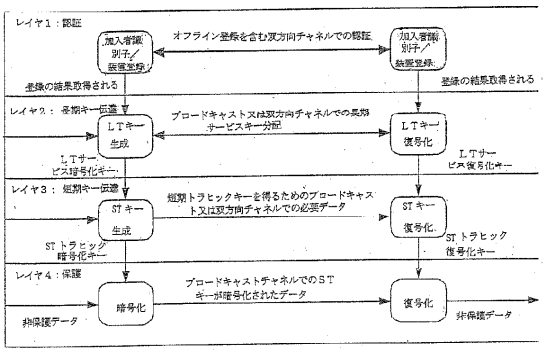
【図６】

【図6】



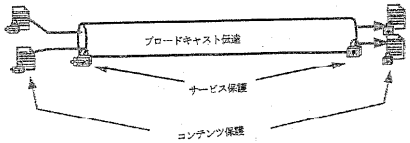
【図８】

【図8】



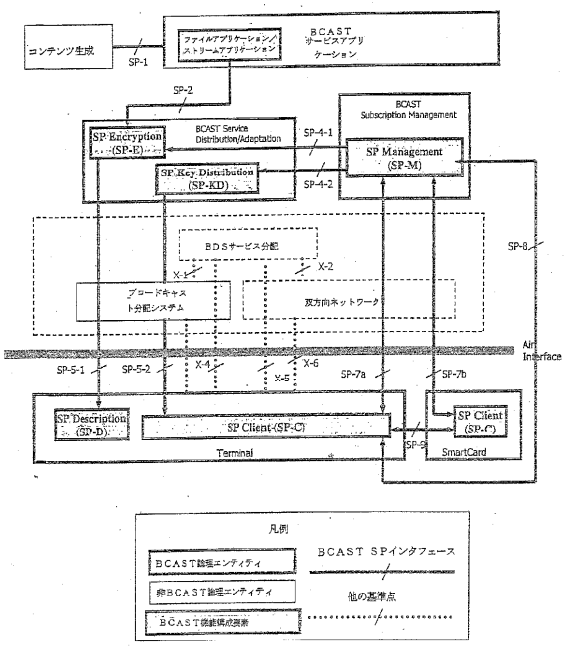
【図７】

【図7】



【図９】

【図９】



【図１０】

【図10】

インタフェース	基準点	定義
SP-1	BCAST-1	Content creation からのファイル及びストリームをＢＣＤ／Ａに伝送する。
SP-2	BCAST-2	(ファイル及び／又はストリーム分配による) ブロードキャストサービスは －端末への非同期分配のためにＢＤＳに提供できる。 －ＢＤＳのオリジナルサービス原理を利用して端末への非同期分配のためにＢＤＳに提供できる。 －端末へのOMA-同期分配のために ブロードキャストサービス分配システムに提供できる
SP-4-1	BCAST-4	このインタフェースは、サービス暗号化のためのＴＥＫをＳＰ－ＭからＳＰ－Ｅに伝送する。
SP-4-2	BCAST-4	このインタフェースは、加入のためのＳＴＫＭ及びＬＴＫＭをＳＰ－ＭからＳＰ－ＫＤに伝送する。
SP-5-1	BCAST-5	このインタフェースは、4層モデルのレイヤ4（「コンテンツ層」）を実現する。 OMA-保護サービスは、ＢＤＳを介して端末に分配される。 Ｎｏｔｅ：このインタフェースは、ＦＤ－５及びＵＳＤ－５と同一である。
SP-5-2	BCAST-5	このインタフェースは4層モデルのレイヤ３（「ＳＴＫＭ保護レイヤ」）を実現する。 トラヒックキーメッセージがＢＤＳを介して端末に分配される。 このインタフェースの他の役割は、ブロードキャストチャネルでのＬＴ キーメッセージの伝送のための４層モデルのレイヤ２（「ＬＴキー伝送レイヤ」）を実現することである。 インタフェース SP-8 に関連した他のインタフェース役割は ブロードキャストチャネルでの端末の登録のための４層モデルのレイヤ１（「登録レイヤ」）を実現する。 これは、登録が必要のために端末をキー 要素を設定するために ブロードキャストチャネルで「ブロードキャスト暗号鍵材 付加から、双方向チャネルを有しない端末」を登録するものである。また、このインタフェースを介して互いにＤＲＭセールドメインを登録する装置の登録をカバーできる。
SP-7	BCAST-7	このインタフェースは、ＬＴキーメッセージの伝送と双方向チャネルでの登録のための４層モデルのレイヤ２とレイヤ１を実現する。
SP-8	BCAST-8	このインタフェースはブロードキャストチャネルでの登録のために帯域外チャネルを提供する。
SP-9	N/A	これは、端末とスマートカード間のインタフェースである。このインタフェースは、スマートカードを有しない端末には存在しない。 Ｎｏｔｅ：インタフェースＳＰ－９に対してはより多くの理論が要求される。

フロントページの続き

(72)発明者 ソン, スンーム
大韓民国 ４６３－９２２ キョンギード, ソンナム, ブンダンーク, ジョンジャードン, ハンソルマウル ジュゴン ４－ダンジ アパートメント ４１５－１４０５
(72)発明者 シム, ドンーヘ
大韓民国 １５０－８５３ ソウル, ヨンドゥンポーク, シンギル １－ドン, ４５４－１, クムソンーリビングテル ５０３
(72)発明者 ハン, キューソン
大韓民国 １５３－８１９ ソウル, クムチョンーク, ドクサン ３－ドン, ８８９－２６, ヤンミ アパートメント エーー５０１
(72)発明者 ション, ミンーユン
大韓民国 １５２－７７０ ソウル, クローク, クロードン, ロッテ アパートメント １０２－１０１
(72)発明者 キム, テ ヒュン
大韓民国 ４３７－７７１ キョンギード, ウィワン, ポイルードン, ５１８, トンガエコービレ アパートメント １０２－１００２
(72)発明者 リー, シュン ジェ
大韓民国 ４２３－７６３ キョンギード, クァンミョン, ハン ４－ドン, ハン ジュゴン １１－ダンチ アパートメント １１０１－１４０５
(72)発明者 チュ, ヤン スン
大韓民国 ４３７－８３８ キョンギード, ウィワン, ネソンードン, ８０３－１３, ３０１

審査官 松平 英

(56)参考文献 特開昭５９－０３４７４１（ＪＰ，Ａ）
特開平０４－２１３２４２（ＪＰ，Ａ）
特開２００３－０６９５４７（ＪＰ，Ａ）
特開２００４－５２９５３８（ＪＰ，Ａ）
特開２００４－５３３７３５（ＪＰ，Ａ）
特表２００７－５２７１７８（ＪＰ，Ａ）
米国特許第０６０４９８７８（ＵＳ，Ａ）
DRM Specification V2.0 Draft Version 2.0, online, ２００４年 4月２０日, http://xml.coverpages.org/OMADRMv204-20040420.pdf
赤羽 泰彦 Yasuhiko Akahane, チャットにおける鍵配送プロトコルの一提案 A Key Distribution Protocol For Chat Program, コンピュータセキュリティシンポジウム２００２ Computer Security Symposium 2002, 日本, 社団法人情報処理学会 Information Processing Society of Japan, ２００２年１０月３０日, 第2002巻, ｐ．２６３～２６８
Chung Kei Wong et al, Secure Group Communications Using Key Graphs, IEEE/ACM TRACSACTIONS ON NETWORKING, IEEE, ２０００年 2月, VOL.8, NO.1, p.16-30

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/00
G09C 1/00
G06F 12/14
G06F 15/00
H04N 5/91
H04N 7/167