(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2009-545229
(P2009-545229A)
(43)公表日　平成21年12月17日(2009.12.17)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/08	(2006.01)	H04L	9/00	601B	5B017
H04L	9/14	(2006.01)	H04L	9/00	641	5C164
G09C	5/00	(2006.01)	G09C	5/00		5J104
G06F	21/24	(2006.01)	G06F	12/14	520D	
H04N	7/167	(2006.01)	G06F	12/14	540P	

審査請求 未請求　予備審査請求 未請求　（全 16 頁）　最終頁に続く

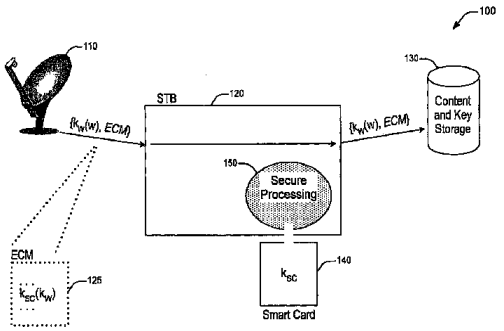
(21)出願番号　特願2009-521733 (P2009-521733)
(86)(22)出願日　平成18年12月13日 (2006.12.13)
(85)翻訳文提出日　平成21年3月23日 (2009.3.23)
(86)国際出願番号　PCT/US2006/047634
(87)国際公開番号　WO2008/013562
(87)国際公開日　平成20年1月31日 (2008.1.31)
(31)優先権主張番号　60/832,830
(32)優先日　平成18年7月24日 (2006.7.24)
(33)優先権主張国　米国 (US)

(71)出願人　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　エフ－９２１００　ブローニュ　ビヤンクール，　ケ　アルフォンス　ル　ガロ，　４６番地
４６　Ｑｕａｉ　Ａ．　Ｌｅ　Ｇａｌｌｏ，　Ｆ－９２１００　Ｂｏｕｌｏｇｎｅ－Ｂｉｌｌａｎｃｏｕｒｔ，　Ｆｒａｎｃｅ
(74)代理人　100115864
弁理士　木越　力
(74)代理人　100121175
弁理士　石井　たかし

最終頁に続く

(54)【発明の名称】コンテンツを安全に配信する方法、装置およびシステム

(57)【要約】
本発明の種々の実施態様は、ユーザがコンテンツを悪用するのを防止し、且つ海賊版のデータをその不正利用が行われた最初の位置までさかのぼって追跡する機構を提供するように、音声映像コンテンツなどのコンテンツを安全に配信する方法、装置およびシステムを提供する。本発明の一実施態様によるセキュリティ装置は、同報通信される暗号化鍵を確実に安全に保つための暗号化方法をその内部に実装している。本発明の一実施態様によるマーク付け装置は、例えば、セット・トップ・ボックス（ＳＴＢ）および／またはスマート・カードなどの不正利用が行われた起源の位置を識別するための情報をコンテンツに付加する電子透かし方法をその内部に実装している。



【特許請求の範囲】
【請求項１】
コンテンツを安全に配信する方法であって、
第１の鍵を用いて前記コンテンツを暗号化するステップと、
第２の鍵を用いて前記第１の鍵を暗号化するステップと、
前記暗号化されたコンテンツおよび前記暗号化された第１の鍵を配信するステップと、を含み、
前記第２の鍵のローカルに記憶されたコピーを用いて前記第１の鍵を復号化し、かつ前記復号化された第１の鍵を用いて前記コンテンツを復号化することによって前記コンテンツを復号化する、前記方法。
【請求項２】
前記復号化されたコンテンツを、安全なチャネルを介して取得される第３の鍵を用いて暗号化するステップと、
前記第３の鍵を用いて暗号化された前記コンテンツを前記第３の鍵のソースに通信するステップと、をさらに含み、
前記第３の鍵を用いて暗号化された前記コンテンツを、前記第３の鍵のローカル・コピーを用いて復号化する、請求項１に記載の方法。
【請求項３】
前記第３の鍵を用いて前記コンテンツを暗号化する前に、前記復号化されたコンテンツに識別のためにマーク付けを行うステップをさらに含む、請求項２に記載の方法。
【請求項４】
前記復号化されたコンテンツに識別のためにマーク付けを行うステップと、
前記マーク付けが行われたコンテンツを前記第１の鍵を用いて再暗号化するステップと、をさらに含む、請求項１に記載の方法。
【請求項５】
前記マーク付けが行われて再暗号化されたコンテンツを記憶するステップをさらに含む、請求項４に記載の方法。
【請求項６】
前記マークが電子透かしを含む、請求項４に記載の方法。
【請求項７】
前記配信されたコンテンツおよび前記第１の鍵を、復号化する前に記憶するステップをさらに含む、請求項１に記載の方法。
【請求項８】
前記第１の鍵がワーク鍵を含む、請求項１に記載の方法。
【請求項９】
前記第２の鍵がスマート・カード鍵を含む、請求項１に記載の方法。
【請求項１０】
前記第３の鍵がセッション鍵を含む、請求項２に記載の方法。
【請求項１１】
前記コンテンツが音声映像コンテンツを含む、請求項１に記載の方法。
【請求項１２】
コンテンツを安全に配信する装置であって、
コンテンツの暗号化および復号化を行うセキュア処理モジュールと、
暗号化鍵をローカルに記憶して復号化するスマート・カードと、を含み、
第１の鍵で暗号化されたコンテンツを受信し、第２の鍵で暗号化された前記第１の鍵を受信すると、前記装置の前記スマート・カードが、前記第２の鍵のローカルに記憶されたコピーを用いて前記第１の鍵を復号化し、前記セキュア処理モジュールが、前記受信された暗号化されたコンテンツを前記復号化された第１の鍵を用いて復号化する、前記装置。
【請求項１３】
前記復号化されたコンテンツにマーク付けを行うマーク付けモジュールをさらに含む、

請求項１２に記載の装置。
【請求項１４】
前記セキュア処理モジュールは、前記マーク付けされたコンテンツを前記第１の鍵を用いて再暗号化する、請求項１３に記載の装置。
【請求項１５】
前記装置が、安全なチャネルを介してコンテンツ・プレーヤから第３の鍵を受信し、前記セキュア処理モジュールが、前記復号化されたコンテンツを前記第３の鍵を用いて暗号化し、前記装置が、前記第３の鍵を用いて暗号化された前記コンテンツを前記コンテンツ・プレーヤに通信する、請求項１２に記載の装置。
【請求項１６】
前記コンテンツ・プレーヤが、前記第３の鍵で暗号化された前記コンテンツを、前記第３の鍵のローカルに記憶されたコピーを用いて復号化する、請求項１５に記載の装置。
【請求項１７】
前記復号化されたコンテンツを前記第３の鍵を用いて暗号化する前に、前記復号化されたコンテンツにマーク付けを行うマーク付けモジュールをさらに含む、請求項１５に記載の装置。
【請求項１８】
コンテンツを安全に配信するシステムであって、
コンテンツを配信するコンテンツ・ソースと、
前記配信されたコンテンツを第１の鍵を用いて暗号化し、前記第１の鍵を第２の鍵を用いて暗号化する電子対策装置と、
第１の鍵で暗号化された前記コンテンツと第２の鍵で暗号化された前記第１の鍵とを受信する装置であって、コンテンツの暗号化および復号化を行うセキュア処理モジュールと、暗号化鍵をローカルに記憶して復号化するスマート・カードとを含む前記装置と、
前記受信された暗号化されたコンテンツおよび前記第１の鍵を記憶する記憶装置と、を含み、
前記第１の鍵で暗号化されたコンテンツを受信し、前記第２の鍵で暗号化された前記第１の鍵を受信すると、前記装置の前記スマート・カードが、前記第２の鍵のローカルに記憶されたコピーを用いて前記第１の鍵を復号化し、前記セキュア処理が、前記受信された暗号化されたコンテンツを前記復号化された第１の鍵を用いて復号化する、前記システム。
【請求項１９】
前記装置が、前記復号化されたコンテンツにマーク付けを行うマーク付けモジュールをさらに含む、請求項１８に記載のシステム。
【請求項２０】
前記装置の前記セキュア処理モジュールが、前記マーク付けされたコンテンツを前記第１の鍵を用いて再暗号化する、請求項１９に記載のシステム。
【請求項２１】
前記マーク付けされて再暗号化されたコンテンツが、前記記憶装置に記憶される、請求項２０に記載のシステム。
【請求項２２】
第３の鍵を安全なチャネルを介して前記装置に通信するコンテンツ・プレーヤをさらに含み、
前記装置が、前記復号化されたコンテンツを前記第３の鍵を用いて暗号化し、前記第３の鍵を用いて暗号化された前記コンテンツを前記コンテンツ・プレーヤに通信し、前記コンテンツ・プレーヤが、前記第３の鍵で暗号化された前記コンテンツを、前記第３の鍵のローカルに記憶したコピーを用いて復号化する、請求項１８に記載のシステム。
【請求項２３】
前記装置が、前記復号化したコンテンツを前記第３の鍵を用いて暗号化する前に、前記復号化したコンテンツにマーク付けを行うマーク付けモジュールをさらに含む、請求項２

２に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概ねコンテンツの配信に関し、さらに詳細には、音声映像コンテンツなどのコンテンツを安全に通信する方法、装置およびシステムに関する。
【背景技術】
【０００２】
セット・トップ・ボックス（ＳＴＢ）などのコンテンツ装置に安全に記憶された音声映像コンテンツなどのコンテンツは、しばしば、安全でないチャネル（例えばホーム・ネットワーク）を介して例えばパーソナル・コンピュータ（ＰＣ）などで動作するソフトウェア・プレーヤに転送される。ＳＴＢでは、高機能な限定受信（ＣＡ）機構を使用してコンテンツの不正使用を防止しているが、安全でないチャネルでは著作権侵害行為が容易に行われうる。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
従って、音声映像コンテンツを安全に配信する方法、装置およびシステムが必要とされている。
【課題を解決するための手段】
【０００４】
本発明の種々の態様は、音声映像コンテンツなどのコンテンツを安全に配信する方法、装置およびシステムを提供することによって、従来技術の上記及びその他の欠点に対処するものである。
【０００５】
本発明の一態様では、コンテンツを安全に配信する方法は、第１の鍵を用いてコンテンツを暗号化するステップと、第２の鍵を用いて第１の鍵を暗号化するステップと、暗号化されたコンテンツおよび暗号化された第１の鍵を配信するステップとを含む。本発明のこのような態様では、ローカルに記憶された第２の鍵のコピーを用いて第１の鍵を復号化し、復号化された第１の鍵を用いてコンテンツを復号化することによって、配信されたコンテンツが復号化される。この方法は、不正利用されたコンテンツの本来のユーザを識別するための識別情報を含めることをさらに含むことができる。すなわち、この方法は、復号化されたコンテンツに識別のためにマーク付けを行うステップと、マーク付けが行われたコンテンツを再暗号化するステップとをさらに含むことができる。さらに、この方法は、安全なチャネルを介して取得される第３の鍵を用いてコンテンツを暗号化するステップと、第３の鍵を用いて暗号化されたコンテンツを第３の鍵のソースに通信するステップとをさらに含むことができ、第３の鍵を用いて暗号化されたコンテンツは、第３の鍵のローカル・コピーを用いて復号化される。
【０００６】
本発明の他の態様では、コンテンツを安全に配信する装置は、コンテンツの暗号化および復号化を行うセキュア処理モジュールと、暗号化鍵をローカルに記憶して復号化するスマート・カードとを含む。この装置では、第１の鍵で暗号化されたコンテンツを受信し、第２の鍵で暗号化された第１の鍵を受信すると、該装置のスマート・カードが、第２の鍵のローカルに記憶されたコピーを用いて第１の鍵を復号化し、セキュア処理モジュールが、受信された暗号化されたコンテンツを復号化された第１の鍵を用いて復号化する。本発明のこの装置は、復号化されたコンテンツにマーク付けを行うマーク付けモジュールをさらに含むこともできる。
【０００７】
本発明の他の態様では、コンテンツを安全に配信するシステムは、コンテンツを配信するコンテンツ・ソースと、配信されたコンテンツを第１の鍵を用いて暗号化し、第１の鍵

を第２の鍵を用いて暗号化する電子逆探装置と、第１の鍵で暗号化されたコンテンツおよび第２の鍵で暗号化された第１の鍵を受信する装置と、受信された暗号化されたコンテンツおよび第１の鍵を記憶する記憶装置とを含む。このシステムの上記装置は、コンテンツの暗号化および復号化を行うセキュア処理モジュールと、暗号化鍵をローカルに記憶して復号化するスマート・カードとを含むことができる。本発明のこのシステムでは、第１の鍵で暗号化されたコンテンツを受信し、第２の鍵で暗号化された第１の鍵を受信すると、該装置のスマート・カードが、第２の鍵のローカルに記憶されたコピーを用いて第１の鍵を復号化し、セキュア処理が、受信された暗号化されたコンテンツを、復号化された第１の鍵を用いて復号化する。本発明のシステムの上記装置は、復号化されたコンテンツにマーク付けを行うマーク付けモジュールをさらに含むことができる。さらに、本発明のシステムは、第３の鍵を安全なチャネルを介して上記装置に通信するコンテンツ・プレーヤをさらに含むことができ、上記装置は、復号化されたコンテンツを第３の鍵を用いて暗号化し、第３の鍵を用いて暗号化されたコンテンツをコンテンツ・プレーヤに通信し、コンテンツ・プレーヤは、第３の鍵で暗号化されたコンテンツを、第３の鍵のローカルに記憶したコピーを用いて復号化する。

【０００８】

以下の詳細な説明を添付の図面と併せて考慮すれば、本発明の教示を容易に理解することができる。

【０００９】

添付の図面は、本発明の概念を例示するためのものであり、本発明を示す唯一の可能な構成であるとは限らないことを理解されたい。理解を容易にするために、全図面に共通して示される同じ要素は、可能な限り同じ参照番号を用いて示してある。

【図面の簡単な説明】

【００１０】

【図１】本発明の一実施形態による、セキュリティ暗号化をコンテンツに付加するシステムのハイレベル・ブロック図である。

【図２】本発明の一実施形態による、図１に示すセット・トップ・ボックスおよび図１の暗号化されたコンテンツの受信及び再生を行うソフトウェア・プレーヤを含むシステムのハイレベル・ブロック図である。

【図３】本発明の一実施形態によるコンテンツ配信システムのハイレベル・ブロック図である。

【図４】本発明の一実施形態による、コンテンツ配信および電子透かし入れシステムのハイレベル・ブロック図である。

【図５】本発明の他の実施形態による、他の電子透かし方法を含む、暗号化されたコンテンツの受信及び再生を行うシステムのハイレベル・ブロック図である。

【発明を実施するための形態】

【００１１】

本発明は、音声映像コンテンツなどのコンテンツを、例えばホーム・ネットワーク環境などで安全に通信する方法、装置およびシステムを提供するのに有利である。主にソフトウェア・プレーヤを含むホーム・ネットワーク環境における音声映像コンテンツに関連して本発明を説明するが、以下に具体的に示す本発明の実施形態は本発明の範囲を限定するものではない。本発明の教示を得た当業者なら、本発明の概念は、実質的に任意のコンテンツ・プレーヤで再生される任意のコンテンツ（例えば映像、音声、音声映像など）を安全に転送する実質的に任意のネットワークに有利に適用されることを理解するであろう。

【００１２】

図１は、本発明の一実施形態による、音声映像コンテンツなどのコンテンツにセキュリティ暗号化を付加するシステムのハイレベル・ブロック図を示している。例示として、図１のシステム１００は、音声映像コンテンツ伝送装置（例えばパラボラ・アンテナ）１１０、セット・トップ・ボックス１２０、電子対策（ＥＣＭ：Ｅｌｅｃｔｒｉｃ Ｃｏｕｎｔｅｒ－Ｍｅａｓｕｒｅ）装置１２５、およびコンテンツ／鍵記憶装置１３０を含んでい

る。図１のシステム１００では、セット・トップ・ボックス１２０は、スマート・カード１４０、およびセキュア処理／記憶モジュール１５０を含んでいる。図１のシステム１００では、セット・トップ・ボックスのモジュール１５０は、スマート・カード１４０との安全な通信リンクを備えている。さらに、スマート・カード１４０は、セキュア処理／記憶機能を備えている。

【００１３】

図１のシステム１００では、電子対策（ＥＣＭ）装置１２５からのＥＣＭメッセージは、音声映像コンテンツとともにＳＴＢ１２０に通信される。ＥＣＭメッセージは、特に、暗号化鍵すなわちワーク鍵k_wを含む。傍受を防止するために、ワーク鍵k_wは、スマート・カード１４０で使用される鍵で暗号化される。本明細書では、この鍵をスマート・カード鍵k_{sc}と呼び、暗号化されたワーク鍵をk_{sc}（k_w）と呼ぶ。スマート・カード鍵は、スマート・カード１４０に安全に記憶されており、音声映像コンテンツを傍受またはコピーしようとする第三者が復元することはできない。図１の実施形態では、スマート・カード鍵は対称鍵暗号の鍵である。ＥＣＭメッセージの暗号化は、本明細書で述べる本発明の実施形態の理解に不可欠なものではないので、本明細書では詳細には説明しない。本発明の一実施形態では、ＥＣＭメッセージの暗号化は公開鍵暗号でもよいが、任意の既知の暗号化方法を適用することができる。

【００１４】

上述のように、ＥＣＭメッセージは、暗号化された音声映像コンテンツとともに、例えばコンテンツ／鍵記憶装置１３０に記憶される。音声映像コンテンツが再生されると、ＥＣＭが記憶装置１５０から呼び出され、暗号化されたワーク鍵がスマート・カード１４０に通信される。スマート・カード１４０は、k_{sc}のローカル・コピーを使用してk_wを復号化し、ＳＴＢ１２０のセキュア処理モジュール１５０に戻す。こうして、ＳＴＢ１２０は、記憶した音声映像コンテンツの復号化に必要な鍵を取得する。この復号化は、セキュア処理モジュール１５０で実施することができる。図１に示すシステムの実施形態では、音声映像コンテンツおよびＥＣＭを単一のＳＴＢ１２０に通信するものとして示しているが、本発明の他の実施形態では、音声映像コンテンツおよびＥＣＭを複数のセット・トップ・ボックスまたはその他の受信装置に同報通信して、上述のように暗号化および処理を行ってもよい。例えば、同報通信された各々の音声映像コンテンツを、対称鍵暗号を用いて暗号化することもできる。上述のように、本明細書では、暗号化鍵すなわち音声映像ワーク鍵をk_wと呼び、暗号化された音声映像コンテンツをk_w（Ｗ）と呼ぶ。暗号化された音声映像コンテンツは、各ＳＴＢが受信し、後の使用に備えて記憶する。

【００１５】

図２は、本発明の一実施形態による、図１に示すセット・トップ・ボックス１２０と、図１の暗号化された音声映像コンテンツの受信及び再生を行うソフトウェア・プレーヤとを示すハイレベル・ブロック図である。図２において、ソフトウェア・プレーヤは例示としてパーソナル・コンピュータ（ＰＣ）２１０を含んでいる。コンテンツ配信システムでは、上述した図１のＳＴＢ１２０及び／又はコンテンツ／鍵記憶装置１３０に記憶された音声映像コンテンツなどの、記憶されたコンテンツは、パーソナル・コンピュータに転送して表示することができることが望ましい。図２では、ソフトウェア・プレーヤ２１０は、固有の秘密鍵／公開鍵の対およびＳＴＢ１２０の公開鍵を備えている。ソフトウェア・プレーヤ２１０は、それ自身の公開鍵をＳＴＢ公開鍵で暗号化して、この情報をＳＴＢに通信する。ＳＴＢは、自身の秘密鍵を用いてこのメッセージを復号化することができる。こうして、これら２つの装置は互いの公開鍵を知り、安全な通信チャネルを確立することができる。このチャネルを介して、これら２つの装置は、セッション鍵を作成して交換し、その後、この安全なチャネルを終了する。セッション鍵は、ＳＴＢからソフトウェア・プレーヤにコンテンツを安全に転送するために使用されることになる。

【００１６】

さらに詳しくは、本発明の一実施形態では、記憶された音声映像コンテンツは、ＳＴＢの記憶装置からＰＣ２１０に直接通信される。従って、鍵k_wは、音声映像コンテンツと

ともにＰＣ２１０に通信する必要がある。図２のシステムでは、ＰＣ２１０は、安全でないプラットフォームであると考えられ、ＰＣ２１０に通信するまでは非常に安全だった鍵k_wのセキュリティが危険にさらされることになる。

【００１７】

k_wのセキュリティを維持するために、リンク暗号化が実施される。さらに詳しくは、ＰＣ２１０およびＳＴＢ１２０が、公開鍵暗号を使用して、安全な通信チャネル（例えばＴＬＳ）を確立する。ただし、公開鍵暗号は計算コストが高く、従ってデータ・ペイロードが大きい場合にはあまり使用されない。代わりに、このＴＬＳチャネルを使用して、対称鍵暗号のセッション鍵k_sを確立し、交換する。この場合には、ＳＴＢは、ワーク鍵k_wを用いて音声映像コンテンツを復号化し、その後直ちにセッション鍵k_sを用いてそれを暗号化することになる。この再暗号化された音声映像コンテンツは、例えばホーム・ネットワークなどの安全でないチャネルを介してＰＣ２１０に安全に通信し、そこで復号化して表示することができる。

【００１８】

例えば、図３は、本発明の一実施形態による音声映像コンテンツ配信システムを示すハイレベル・ブロック図を示している。図３の音声映像コンテンツ配信システム３００は、例示として、図１に示すコンテンツ／鍵記憶装置１３０およびセット・トップ・ボックス（ＳＴＢ）１２０と、図２に示すソフトウェア・プレーヤ２１０とを含んでいる。図３のシステムでは、セッション鍵k_sが一度確立されると、ＳＴＢ１２０内のセキュア処理装置１５０が、対称暗号セッション鍵k_sを使用して作品（ワーク）を復号化し、それを再暗号化することに用いられる。その後、暗号化されたコンテンツを、ホーム・ネットワークなどの安全でないチャネルでＰＣ２１０に通信することができる。プレーヤは、セッション鍵k_sのコピーを用いてコンテンツを復号化することができる。

【００１９】

公開鍵暗号を使用するためには、ＳＴＢ１２０と、ＰＣ２１０で動作するソフトウェアとが、それぞれ公開鍵／秘密鍵の対を有していなければならない。本発明の一実施形態では、ＳＴＢ１２０の秘密鍵

【００２０】

【数１】

$$k_{stb}^{pv}$$

は、製造中にセキュア処理モジュール１５０に埋め込まれ、公開鍵

【００２１】

【数２】

$$k_{stb}^{pu}$$

は、その後の配信に備えて安全なデータベースに記憶される。ソフトウェア・プレーヤ２１０は、ＳＴＢの所有者／管理者からその顧客に要求に応じて割り当てられる独自のプレーヤを含むことができる。ソフトウェア・プレーヤ２１０の各コピーは、固有の秘密鍵／公開鍵の対

【００２２】

【数３】

$$\left(k_{pc}^{pv}, k_{pc}^{pu}\right)$$

を含むことになる。音声映像コンテンツを求める顧客の要求は、接続の要求元であるＳＴＢの固有の識別を含むことになる。当該ＳＴＢの公開鍵は、各々のソフトウェア・プレーヤに埋め込まれて、そのソフトウェア・プレーヤが当該ＳＴＢでしか動作できないようにする。これにより、ＳＴＢの管理者にも、どのＳＴＢがどのＰＣとの通信を可能にされているかを示す記録が与えられる。

【００２３】
従って、本発明によれば、ＳＴＢ１２０は秘密鍵を有し、ソフトウェア・プレーヤ２１０は対応する公開鍵およびそれ自身の秘密鍵／公開鍵の対を有することになる。ソフトウェア・プレーヤ２１０は、例えばホーム・ネットワークなどの安全でないチャネルを介してＳＴＢ１２０との接続を開始し、その公開鍵に関する情報をＳＴＢ１２０に通信することができる。このようにして、ＳＴＢ１２０およびソフトウェア・プレーヤ２１０は、図２を参照して上述したように、それらが対称暗号セッション鍵を確立して交換することができる安全なチャネルを確立することができる。

【００２４】
安全なチャネルを確立するための多くのプロトコルは、全ての通信装置が、信頼できるソールからのディジタル認証に署名していることを必要とする。提案したアーキテクチャが独自のものであることを考慮すると、これらの認証は、例えばＳＴＢの管理者（信頼できるソース）が生成し、ＳＴＢ１２０およびソフトウェア・プレーヤ２１０の両方に提供することができる。これにより、ＳＴＢ１２０は、ＳＴＢの管理者が許可したソフトウェア・プレーヤとの安全なリンクのみを確立することが保証される。上述の本発明の概念は、配信された音声映像コンテンツの著作権侵害からの保護に役立つ。本発明の様々な実施形態では、高度なソフトウェア・セキュリティ技術を実施して、ソフトウェア秘密鍵および得られたセッション鍵を発見されないように保護する。しかし、残念ながら、知識の豊富な著作権侵害者たちは、まず間違いなくこれらの鍵の発見に成功するだろう。一度発見されてしまえば、そのセッション鍵を使用して音声映像コンテンツを復号化することができる。しかし、本発明の一実施形態によれば、異なる音声映像コンテンツは異なるセッション鍵で暗号化されることになる。従って、発見された鍵は、それに対応するＳＴＢ上の、それに対応する保護された音声映像コンテンツを復号化するには有効だが、別のＳＴＢを有する他の者にとっては無価値であり、その他の配信された音声映像コンテンツの復号化にも役に立たない。それを行うためには、別のセッション鍵を発見する必要がある。

【００２５】
さらに、ソフトウェア秘密鍵が発見され、それを使用してＴＬＳセッションを監視することによって、セッションを確立するたびにそのセッション鍵が知られてしまうおそれもある。例えば、このような不正コピーを行う可能性がある者は２つのグループに分けられる。自分自身と友人のためのコピーを作成する顧客と、プロフェッショナルの窃盗犯である。これら２つのグループの違いの１つは、顧客が不正を行う場合は、コンテンツ配信サービスで得をしようとするのが第１であり、複製によって利益を得るのは二の次だという点である。プロフェッショナルの窃盗犯は、海賊版のコンテンツを作成するためにコンテンツ配信サービスを利用する。

【００２６】
電子透かしは、ある種の識別可能なメタデータを音声映像コンテンツに付加するためにディジタル画像を改変する技術である。メタデータは、電子透かし入りのコンテンツが再圧縮されている場合またはアナログ・フォーマットに変換されている場合でも、そのコンテンツのコピーから復元可能である。コンテンツ内の電子透かしは、捕捉可能なクリア・テキスト・コンテンツがアナログだけとなるように、単一の安全なシリコン・チップで実行できるコンテンツの解読、復号およびディジタル－アナログ変換が行われても、失われないようになっている。このようなプロセスは、一般に「アナログ・ホール」と呼ばれている。

【００２７】
本発明の様々な実施形態では、電子透かしは、本発明によって安全になった音声映像コンテンツにオプションで適用することができる。例えば、第１の手法では、受信した音声映像コンテンツをセット・トップ・ボックス（ＳＴＢ）に直接記憶することはしない。その代わりに、コンテンツを復号化し、電子透かしを入れ、再暗号化した後で記憶する。電子透かしは、ＳＴＢとそれに関連するスマート・カードとを固有に識別する情報を含み、受信時刻および記録時刻を示すタイムスタンプを含む。

【００２８】
図４は、本発明の一実施形態による、音声映像コンテンツ配信および電子透かし入れシステムのハイレベル・ブロック図を示している。図４のシステム４００は、例示として、図１に示すコンテンツ伝送装置（例えばパラボラ・アンテナ）１１０、コンテンツ／鍵記憶装置１３０およびセット・トップ・ボックス（ＳＴＢ）１２０を含んでいる。ただし、図４のシステムでは、ＳＴＢ１２０は、コンテンツ伝送装置１１０から受け取ったコンテンツに対して、コンテンツ／鍵記憶装置１３０に記憶する前に電子透かしを入れる、電子透かし入れモジュール１７５をさらに含んでいる。
【００２９】
図４のシステム４００では、ＳＴＢ１２０のセキュリティが損なわれ、コンテンツがＳＴＢ１２０から取得され、著作権侵害が行われた場合に、電子透かし入れモジュール１７５によって入れられた電子透かしによって、その犯罪を行ったＳＴＢの顧客が識別されることになる。ただし、本発明の電子透かし入れでは、更なる復号化／暗号化サイクルがプロセス中で行われることになり、このサイクルと電子透かし入れとによって、ＳＴＢでリアルタイム処理を行う場合には計算コストが高くなる可能性がある。
【００３０】
従って、本発明の他の実施形態では、記憶する間にコンテンツに電子透かしを入れるのではなく、ソフトウェア・プレーヤに転送する際にコンテンツに電子透かしを入れる。例えば、図５は、本発明の他の実施形態による他の電子透かし入れ手段を含む、暗号化された音声映像コンテンツの受信及び再生を行うシステムのハイレベル・ブロック図を示している。図５のシステム５００は、例示として、図１に示すコンテンツ／鍵記憶装置１３０およびセット・トップ・ボックス（ＳＴＢ）１２０と、図２に示すソフトウェア・プレーヤ２１０とを含んでいる。図１に示す実施形態と同様に、受信されたコンテンツは、暗号化された形態で直接記憶される。要求に応じて、コンテンツは復号化され、前述の場合と同様にセッション鍵を用いて再暗号化されるが、図５の実施形態では、電子透かし入れモジュール１７５によってコンテンツに電子透かしが付加される。前述したように、この透かしは、第１の透かし手法の場合と同様に、少なくともダウンロードの時刻と、（ＳＴＢの記憶装置から入手可能な場合には）最初に記憶した時刻とを識別するタイムスタンプを含むことができる。さらに、ソフトウェア・プレーヤ２１０の固有のＩＤは電子透かし入れの時点では既知であるので（なぜならディジタル署名であるため）、特定のソフトウェア・プレーヤ２１０を識別する情報を電子透かし情報に含ませることができる。
【００３１】
本発明の一実施形態では、電子透かしは、ＭＰＥＧ－２ビットストリーム内に直接付加される。電子透かし入れのプロセスは、図４を参照して説明した第１の透かし入れの実施形態ではリアルタイムに行うことができ、図５を参照して説明した第２の透かし入れの実施形態ではリアルタイムより速く行うことができる。一実施形態では、電子透かし入れのプロセスにおいて、その存在をユーザに知らせることになる可視または可聴のアーチファクトが使用されない。さらに、電子透かしデータは、さらに小さいサイズへのサイズ変更、トランスコーディング、およびインタレース解除、ノイズ低減、色調整などを含むその他のいくつかの標準的なテレビジョン・ピクチャ・プロセスの後で復元できるようにすることができる。電子透かし検出器（不図示）は、埋め込みプロセスに含まれるいかなる情報も有していない。すなわち、埋め込み器（不図示）および検出器は秘密を共有することができるが、検出器はどの埋め込み装置が使用されたかをアプリオリに知ることはない。検出は犯罪捜査として行われる操作であり、リアルタイムより遅くてもよい。
【００３２】
上述の両方の電子透かし手法はいずれも、視聴用であって配信用はでないコンテンツに顧客識別情報を埋め込む。ソフトウェア・プレーヤの鍵を発見する海賊版ソフトウェアをユーザが入手し、そのユーザがその海賊版ソフトウェアを使用して、ＳＴＢに記憶された作品の不正コピーを作成した場合、それらのコピーは、その海賊版コンテンツの出所の位置を識別する識別情報を備えた電子透かしを含むことになる。これらのコピーの何れかが

配信された場合（すなわち、例えばＰ２Ｐネットワークまたはウェブ・サイト上で配信された場合）には、全ての不正コピーはそれぞれ、当該コンテンツの本来の受信者を識別するのに必要な犯罪捜査情報（例えば電子透かし及び識別情報）を含むことになる。これらの発見後、ＳＴＢの管理者は、警告書を発送する、サービスを取り止める、法的制裁を行うなどを含む（ただしこれらに限定されない）、適当と考えられる任意の救済措置をとることができる。

【００３３】

本発明の様々な実施形態によれば、ＳＴＢは、秘密鍵／公開鍵の対を含む。秘密鍵はＳＴＢに埋め込まれ、公開鍵はＳＴＢの管理者によって安全なデータベースに記憶される。ＳＴＢは、ＳＴＢの管理者から供給されるディジタル認証を含むこともできる。その結果、顧客は、ＳＴＢの管理者に連絡を取り、所望のコンテンツを見るためのソフトウェア・プレーヤを要求することができる。この要求は、ＳＴＢ識別子によって実現される（この要求はＳＴＢを介して容易に行うことができる）。ＳＴＢの管理者は、データベースからＳＴＢ公開鍵を復元し、ソフトウェア・プレーヤ用のディジタル認証を作成し、この情報を顧客に通信する。さらに、上述のように、ソフトウェア・プレーヤは、それ自身の秘密鍵／公開鍵の対を有する。

【００３４】

上述のように、第１の手法では、ＳＴＢにローカルに記憶するコンテンツを最初に復号化し、電子透かしを入れ、次いで再暗号化する。ソフトウェア・プレーヤは、ＳＴＢとのセッションを開始し、その公開鍵を提供する。ソフトウェア・プレーヤおよびＳＴＢは、それらのディジタル認証を用いて安全なチャネルを取り決め、セッション鍵を確立する。第１の手法では、記憶した電子透かし入りコンテンツを、ＳＴＢ上で復号化し、セッション鍵を用いて再暗号化した後で、ソフトウェア・プレーヤに転送する。

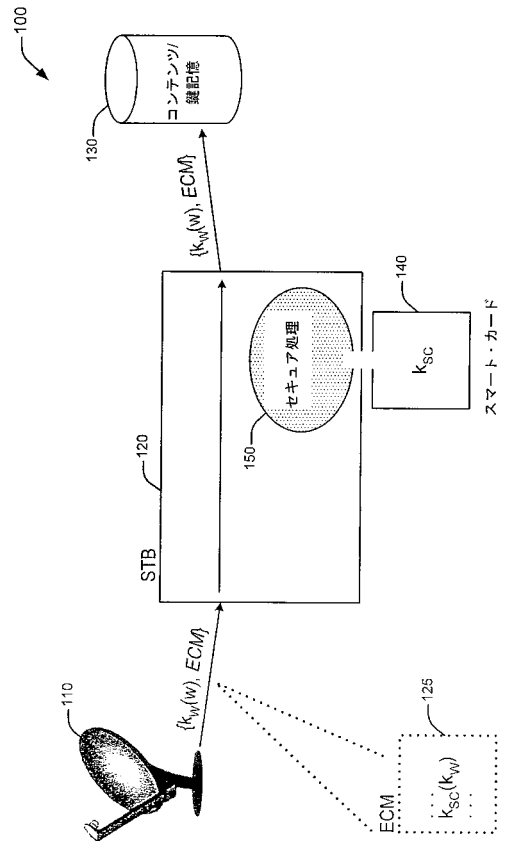
【００３５】

第２の手法では、記憶したコンテンツを、ＳＴＢ上で復号化し、電子透かしを入れ、次いでセッション鍵を用いて再暗号化した後で、ソフトウェア・プレーヤに通信する。ソフトウェア・プレーヤは、セッション鍵を用いてコンテンツを復号化し、そのコンテンツを再生する。

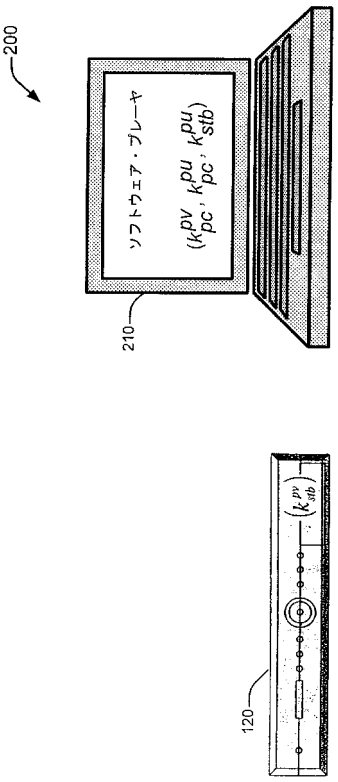
【００３６】

コンテンツを安全に配信する方法、装置およびシステムの（限定的なものではなく例示を目的とした）様々な実施形態について説明したが、当業者であれば上記の教示に照らして様々な変更および変形を行うことができることに留意されたい。従って、添付の特許請求の範囲に外延が記載された本発明の範囲および趣旨の範囲内で、開示した本発明の具体的な実施形態に様々な変更を加えることができることを理解されたい。前述の説明は、本発明の様々な実施形態を対象としたものであるが、本発明の基本的な範囲を逸脱することなく、本発明の他のあるいは更なる実施形態を考案することができる。

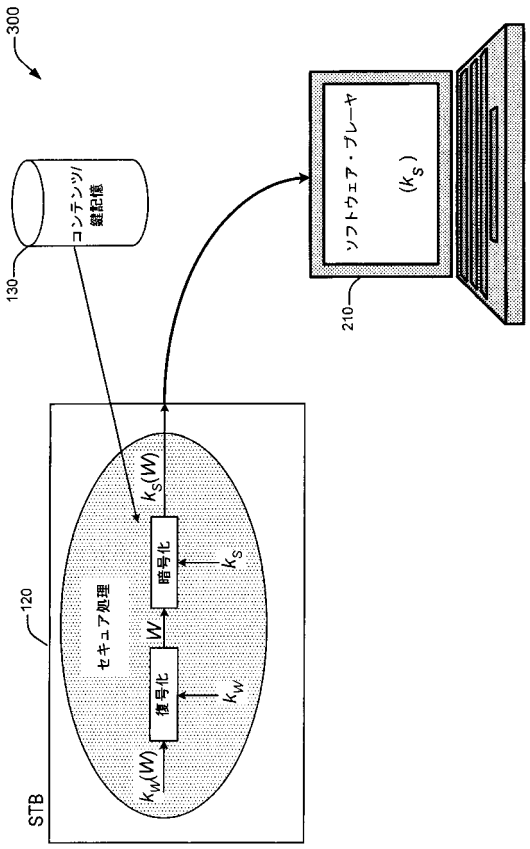
【図１】


100
コンテンツ/鍵記憶
130
{kW(W), ECM}
140
kSC
スマート・カード
セキュア処理
150
120
STB
{kW(W), ECM}
110
125
ECM
kSC(kW)

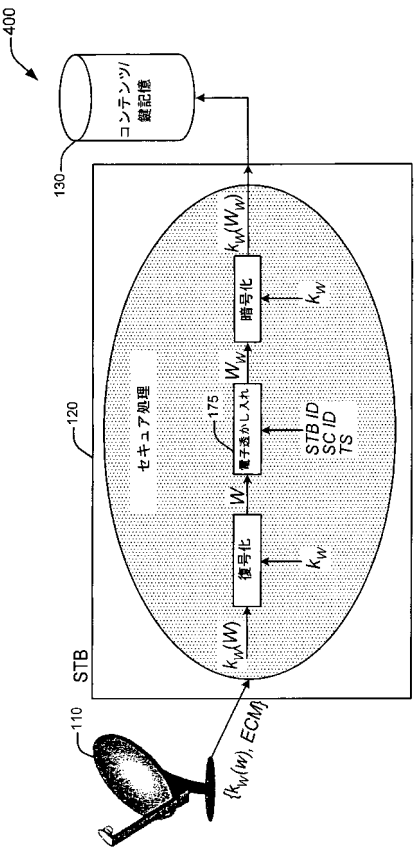
【図２】


200
ソフトウェア・プレーヤ
210
120

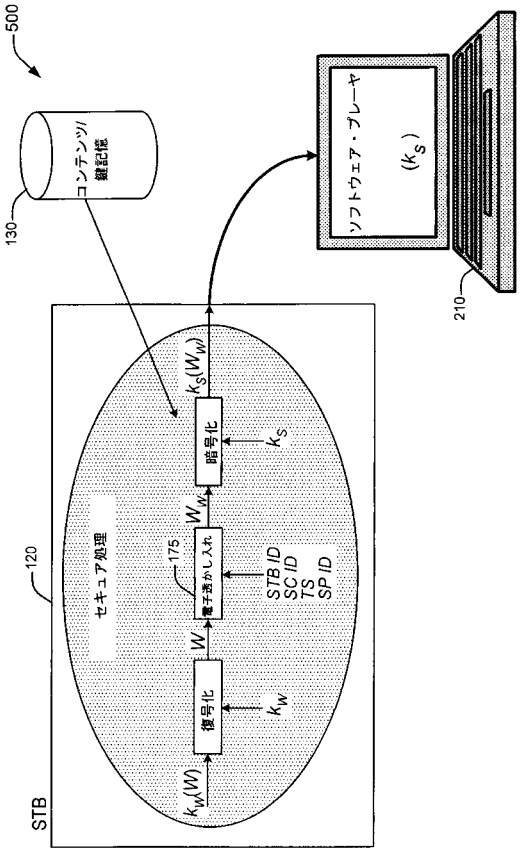
【図３】


300
コンテンツ/鍵記憶
130
ソフトウェア・プレーヤ
210
セキュア処理
復号化
暗号化
120
STB

【図４】


400
コンテンツ/鍵記憶
130
セキュア処理
復号化
暗号化
電子透かし入れ
175
STB ID
SC ID
TS
120
STB
110

【図５】


500
コンテンツ/鍵記憶
130
ソフトウェア・プレーヤ
(k_S)
210
120
セキュア処理
STB
$k_S(W_W)$
暗号化
k_S
W_W
175
電子透かし入れ
STB ID
SC ID
TS
SP ID
W
復号化
k_W
$k_W(W)$

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/047634

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04N5/00 H04N7/16 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, no. 266, 21 December 1995 (1995-12-21), pages 64-77, XP000559450 ISSN: 0251-0936	1,2, 8-12,18
Y	page 67, left-hand column, paragraph 3 - page 69, right-hand column, last line ; figures 4,5	3-7, 13-17, 19-23
	-/--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance
'E' earlier document but published on or after the international filing date
'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
'O' document referring to an oral disclosure, use, exhibition or other means
'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 June 2007	29/06/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schoeyer, Marnix

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/047634

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GUILLOU L C ET AL: "ENCIPHERMENT AND CONDITIONAL ACCESS" SMPTE JOURNAL, SMPTE INC. SCARSDALE, N.Y, US, vol. 103, no. 6, 1 June 1994 (1994-06-01), pages 398-406, XP000457575 ISSN: 0036-1682	1,2, 8-12,18
Y	page 402	3-7, 13-17, 19-23
Y	WO 03/058618 A (LANG JUERGEN K [DE]; BING URSULA MARIA [DE]) 17 July 2003 (2003-07-17) abstract	3-7, 13-17, 19-23
Y	JUDGE P ET AL: "WHIM: watermarking multicast video with a hierarchy of intermediaries" COMPUTER NETWORKS, ELSEVIER SCIENCE PUBLISHERS B.V., AMSTERDAM, NL, vol. 39, no. 6, 21 August 2002 (2002-08-21), pages 699-712, XP004371479 ISSN: 1389-1286 page 699	3-7, 13-17, 19-23

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2006/047634

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 03058618 A	17-07-2003	AU 2002358425 A1	24-07-2003
		DE 10164131 A1	17-07-2003
		EP 1472690 A1	03-11-2004
		US 2005010790 A1	13-01-2005

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
	H04N 7/167 Z	

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 ブルーム，ジエフリー，アダム
アメリカ合衆国 ニユージヤージ州 ウエスト・ウインザー バリントン・ドライブ １４
(72)発明者 ラマズワミイ，クマー
アメリカ合衆国 ニユージヤージ州 プリンストン セイヤー・ドライブ ７１

Ｆターム(参考) 5B017 AA03 AA07 BA07 CA16
5C164 MB35S PA24 PA26 SB03P SC02P UA03S UA12S UB03S UB06P UC22P
5J104 AA14 AA16 AA32 EA01 EA04 EA08 EA18 JA03 NA02 NA24
NA33 NA37 PA05