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

特許第4496506号
(P4496506)

(45)発行日　平成22年7月7日(2010.7.7)　(24)登録日　平成22年4月23日(2010.4.23)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675D
H04L	9/36	(2006.01)	H04L	9/00	685
G06F	21/24	(2006.01)	G06F	12/14	530C
H04N	7/16	(2006.01)	G06F	12/14	560B
H04N	5/765	(2006.01)	G06F	12/14	540A

請求項の数 3　(全 23 頁)　最終頁に続く

(21)出願番号　特願2008-121630 (P2008-121630)
(22)出願日　平成20年5月7日 (2008.5.7)
(62)分割の表示　特願平10-4030の分割
原出願日　平成10年1月12日 (1998.1.12)
(65)公開番号　特開2008-269619 (P2008-269619A)
(43)公開日　平成20年11月6日 (2008.11.6)
審査請求日　平成20年6月2日 (2008.6.2)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100082131
弁理士　稲本　義雄
(74)代理人　100121131
弁理士　西川　孝
(72)発明者　小室　輝芳
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　大澤　義知
東京都港区港南１丁目７番１号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】暗号化コンテンツ送信装置

(57)【特許請求の範囲】
【請求項１】
暗号化コンテンツが送受信される通信システムで用いられる暗号化コンテンツ送信装置であって、
他の装置から当該他の装置を識別する装置識別情報を受信する装置識別情報受信手段と、
前記装置識別情報によって識別される装置が、前記暗号化コンテンツ毎に与えられたサービスキーに基づき生成されたライセンスキーを保持する装置であるか否かを、前記装置識別情報と自身に保持している前記サービスキーとに基づき生成される情報を用いて判定するライセンス取得装置判定手段と、
不正装置として特定された不正装置識別情報のリストを記憶する不正装置識別情報リスト記憶手段と、
前記不正装置識別情報リスト記憶手段に記憶された前記不正装置識別情報のリストに基づき、前記ライセンス取得装置判定手段で前記ライセンスキーを保持する装置と判定された装置が、不正装置であるか否かを判定する不正装置判定手段と、
前記不正装置判定手段が前記他の装置は不正装置であると判定した場合に、当該不正装置に対して、暗号化コンテンツの送信を制限する暗号化コンテンツ制限手段と、
新たな不正装置識別情報のリストを、他の装置から無線通信路を介して受信する不正装置識別情報リスト受信手段と、
前記不正装置識別情報リスト受信手段で受信した前記新たな不正装置識別情報のリスト

を、前記不正装置識別情報リスト記憶手段に書き込む書き込み手段と
を備える暗号化コンテンツ送信装置。
【請求項２】
前記不正装置判定手段が前記他の装置は不正装置であると判定した場合に、自身と通信可能な全ての装置のうち、前記他の装置を除く装置に対して、前記他の装置は不正装置であることを通知する通知手段をさらに備える
請求項１に記載の暗号化コンテンツ送信装置。
【請求項３】
前記無線通信路は、衛星を介する通信路である
請求項１に記載の暗号化コンテンツ送信装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号化コンテンツ送信装置に関し、特に、不正装置によるデータの不正コピーを防止することができるようにした、暗号化コンテンツ送信装置に関する。
【背景技術】
【０００２】
最近、ＡＶ機器やパーソナルコンピュータなどの電子機器を、例えばIEEE1394バス（以下、単に1394バスと称する）などの伝送路を介して相互に接続し、相互の間でデータを授受することができるようにするシステムが提案されている。
【０００３】
図９は、そのような情報処理システムの構成例を示している。なお、本明細書において、システムとは、複数の装置で構成される全体的な装置を示すものとする。この例においては、1394バス１１を介してDVD（Digital Video Disk）プレーヤ１、パーソナルコンピュータ２、光磁気ディスク装置３、データ放送受信装置４、モニタ５、テレビジョン受像機６が相互に接続されている。
【０００４】
図１０は、この内のDVDプレーヤ１、パーソナルコンピュータ２、および光磁気ディスク装置３の内部のより詳細な構成例を表している。DVDプレーヤ１は、1394インタフェース（Ｉ／Ｆ）２６を介して、1394バス１１に接続されている。CPU２１は、ROM２２に記憶されているプログラムに従って各種の処理を実行し、RAM２３は、CPU２１が各種の処理を実行する上において必要なデータやプログラムなどを適宜記憶する。操作部２４は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより操作されたとき、その操作に対応する信号を出力する。ドライブ２５は、図示せぬDVD（ディスク）を駆動し、そこに記録されているデータを再生するようになされている。EEPROM（electrically erasable programmable ROM）２７は、装置の電源オフ後も記憶する必要のある情報を記憶するようになされている。内部バス２８は、これらの各部を相互に接続している。
【０００５】
光磁気ディスク装置３は、CPU３１乃至内部バス３８を有している。これらは、上述したDVDプレーヤ１におけるCPU２１乃至内部バス２８と同様の機能を有するものであり、その説明は省略する。ただし、ドライブ３５は、図示せぬ光磁気ディスクを駆動し、そこにデータを記録または再生するようになされている。
【０００６】
パーソナルコンピュータ２は、1394インタフェース４９を介して1394バス１１に接続されている。CPU４１は、ROM４２に記憶されているプログラムに従って各種の処理を実行する。RAM４３には、CPU４１が各種の処理を実行する上において必要なデータやプログラムなどが適宜記憶される。入出力インタフェース４４は、キーボード４５とマウス４６が接続されており、それらから入力された信号をCPU４１に出力するようになされている。また、入出力インタフェース４４には、ハードディスク（HDD）４７が接続されており、CPU４１は、そこにデータ、プログラムなどを記録再生させることができるようになされてい

る。入出力インタフェース４４にはまた、拡張ボード４８を適宜装着し、必要な機能を付加することができるようになされている。EEPROM５０には、電源オフ後も保持する必要のある情報が記憶されるようになされている。例えば、PCI(Peripheral Component Interconnect)、ローカルバスなどにより構成される内部バス５１は、これらの各部を相互に接続するようになされている。

【０００７】

なお、この内部バス５１は、ユーザに対して解放されており、ユーザは、拡張ボード４８に所定のボードを適宜接続したり、所定のソフトウェアプログラムを作成して、CPU４１にインストールすることで、内部バス５１により伝送されるデータを適宜受信することができるようになされている。

【０００８】

これに対して、DVDプレーヤ１や光磁気ディスク装置３などのコンシューマエレクトロニクス（CE）装置においては、内部バス２８や内部バス３８は、ユーザに解放されておらず、特殊な改造などを行わない限り、そこに伝送されるデータを取得することができないようになされている。

【０００９】

以上の構成のシステムにおいて、例えば、ユーザが、DVDに記録されている映画を、モニタ５またはテレビジョン受像器６等の表示装置を用いて観賞する場合、DVDプレーヤ１は、DVD（ディスク）から読みとった映画データを、1394バス１１を介して表示装置に伝送し、表示装置は、それを受信して表示する。

【００１０】

ところで、このとき、映画データをそのままの状態で1394バス１１を介して伝送すると、不正なユーザがその映画データを受信し、それを不法コピーする可能性がある。そこで、送信側の装置（以下、このような装置をソース（source）と称する）は伝送するデータを暗号化して伝送し、受信側の装置（以下、このような装置をシンク（sink）と称する）は、それを鍵を用いて復号するようにする。その際、送信側の装置は、相手の装置が正規の装置であるか否かを判断するために、データを伝送する前に、その装置との間で認証処理を実行する。

【００１１】

以下に、ソースとシンクとの間で行われる認証処理について説明する。この認証処理は、図１１に示すように、ソースとしての、例えばDVDプレーヤ１のROM２２に予め記憶されているソフトウェアプログラムの１つとしてのファームウェア２０と、シンクとしての、例えばパーソナルコンピュータ２のROM４２に記憶されており、CPU４１が処理するソフトウェアプログラムの１つとしてのライセンスマネージャ６２との間において行われる。

【００１２】

図１２は、ソース（DVDプレーヤ１）と、シンク（パーソナルコンピュータ２）との間において行われる認証の手順を示している。DVDプレーヤ１のEEPROM２７には、サービスキー（service_key）と関数（hash）が予め記憶されている。これらはいずれも伝送するデータ（映画データ）の著作権者から、このDVDプレーヤ１のユーザに与えられたものであり、各ユーザは、EEPROM２７に、これを秘密裡に保管しておくものである。

【００１３】

サービスキーは、著作権者が提供する情報毎に与えられるものであり、この1394バス１１で構成されるシステムにおいて、共通のものである。hash関数は、任意長の入力に対して、６４ビットまたは１２８ビットなどの固定長のデータを出力する関数であり、ｙ（＝hash（ｘ））を与えられたとき、ｘを求めることが困難であり、かつ、hash（ｘ１）＝hash（ｘ２）となるｘ１と、ｘ２の組を求めることも困難となる関数である。１方向hash関数の代表的なものとして、MD５やSHAなどが知られている。この１方向hash関数については、Bruce Schneier著の「Applied Cryptography(Second Edition),Wiley」に詳しく解説されている。

【００１４】

一方、シンクとしての例えばパーソナルコンピュータ２は、著作権者から与えられた、自分自身に固有の識別番号（device_ID：以下、適宜、IDと略記する）とライセンスキー（license_key）を、EEPROM５０に秘密裡に保持している。このライセンスキーは、ｎビットのIDとｍビットのサービスキーを連結して得たｎ＋ｍビットのデータ（ID ‖ service_key）に対して、hash関数を適用して得られる値である。すなわち、ライセンスキーは次式で表される。

licence_key=hash(ID ‖ service_key)

【００１５】

IDとしては、例えば1394バス１１の規格に定められているnode_unique_IDを用いることができる。このnode_unique_IDは、図１２に示すように、８バイト（６４ビット）で構成され、最初の３バイトは、IEEEで管理され、電子機器の各メーカーにIEEEから付与される。また、下位５バイトは、各メーカーが、自分自身がユーザに提供する各装置に対して付与することができるものである。各メーカーは、例えば下位５バイトに対してシリアルに、１台に１個の番号を割り当てるようにし、５バイト分を全部使用した場合には、上位３バイトがさらに別の番号となっているnode_unique_IDの付与を受け、そして、その下位５バイトについて１台に１個の番号を割り当てるようにする。従って、このnode_unique_IDは、メーカーに拘らず、１台毎に異なるものとなり、各装置に固有のものとなる。

【００１６】

まず、ステップＳ１において、DVDプレーヤ１のファームウェア２０は、1394インタフェース２６を制御し、1394バス１１を介してパーソナルコンピュータ２に対してIDを要求する。パーソナルコンピュータ２のライセンスマネージャ６２は、ステップＳ２において、このIDの要求を受信する。すなわち、1394インタフェース４９は、1394バス１１を介してDVDプレーヤ１から伝送されてきたID要求の信号を受信すると、これをCPU４１に出力する。CPU４１のライセンスマネージャ６２は、このID要求を受けたとき、ステップＳ３においてEEPROM５０に記憶されているIDを読み出し、これを1394インタフェース４９を介して1394バス１１からDVDプレーヤ１に伝送する。

【００１７】

DVDプレーヤ１においては、ステップＳ４で、1394インタフェース２６がパーソナルコンピュータ２から伝送されたIDを受け取ると、このIDはCPU２１で動作しているファームウェア２０に供給される。

【００１８】

ファームウェア２０は、ステップＳ５において、パーソナルコンピュータ２から伝送を受けたIDと、EEPROM２７に記憶されているサービスキーを連結して、連結データ（ID ‖ service_key）を生成し、このデータに対して、次式に示すようにhash関数を適用して、キーlkを生成する。

lk＝hash（ID ‖ service_key）

【００１９】

次に、ステップＳ６において、ファームウェア２０は、暗号鍵skを生成する。この暗号鍵skは、セッションキーとしてDVDプレーヤ１とパーソナルコンピュータ２のそれぞれにおいて共通に利用される。

【００２０】

次に、ステップＳ７において、ファームウェア２０は、ステップＳ５で生成した鍵lkを鍵として用いて、ステップＳ６で生成した暗号鍵skを暗号化することにより、暗号化データ（暗号化鍵）ｅを得る。すなわち、次式を演算する。なお、Enc（Ａ，Ｂ）は、共通鍵暗号方式で、鍵Ａを用いて、データＢを暗号化することを意味する。

ｅ＝Enc（lk，sk）

【００２１】

次に、ステップＳ８で、ファームウェア２０は、ステップＳ７で生成した暗号化データｅをパーソナルコンピュータ２に伝送する。すなわち、この暗号化データｅは、DVDプレーヤ１の1394インタフェース２６から1394バス１１を介してパーソナルコンピュータ２に

伝送される。パーソナルコンピュータ２においては、ステップＳ９で、この暗号化データｅを1394インタフェース４９を介して受信する。ライセンスマネージャ６２は、このようにして受信した暗号化データｅをEEPROM５０に記憶されているライセンスキーを鍵として用いて、次式に示すように復号し、復号鍵sk'を生成する。なお、ここで、Dec（Ａ，Ｂ）は、共通鍵暗号方式で鍵Ａを用いて、データＢを復号することを意味する。

sk'＝Dec（license_key，ｅ）

【００２２】

なお、この共通鍵暗号方式における暗号化のアルゴリズムとしては、ＤＥＳ（Data Encryption Standard：米国データ暗号化規格）が知られている。共通鍵暗号化方式についても、上述した、Applied Cryptography(Second Edition)に詳しく解説されている。

【００２３】

DVDプレーヤ１において、ステップＳ５で生成するキーlkは、パーソナルコンピュータ２のEEPROM５０に記憶されている（license_key）と同一の値となる。すなわち、次式が成立する。

lk＝license_key

【００２４】

従って、パーソナルコンピュータ２において、ステップＳ１０で復号して得たキーsk'は、DVDプレーヤ１において、ステップＳ６で生成した暗号鍵skと同一の値となる。すなわち、次式が成立する。

sk'＝sk

【００２５】

このように、DVDプレーヤ１（ソース）とパーソナルコンピュータ２（シンク）の両方において、同一の鍵sk，sk'を共有することができる。そこで、この鍵skをそのまま暗号鍵として用いるか、あるいは、これを基にして、それぞれが疑似乱数を作り出し、それを暗号鍵として用いることができる。

【００２６】

ライセンスキーは、上述したように、各装置に固有のIDと、提供する情報に対応するサービスキーに基づいて生成されているので、他の装置がskまたはsk'を生成することはできない。また、著作権者から認められていない装置は、ライセンスキーを有していないので、skあるいはsk'を生成することができない。従って、その後DVDプレーヤ１が暗号鍵skを用いて再生データを暗号化してパーソナルコンピュータ２に伝送した場合、パーソナルコンピュータ２が適正にライセンスキーを得たものである場合には、暗号鍵sk'を有しているので、DVDプレーヤ１より伝送されてきた、暗号化されている再生データを復号することができる。しかしながら、パーソナルコンピュータ２が適正なものでない場合、暗号鍵sk'を有していないので、伝送されてきた暗号化されている再生データを復号することができない。換言すれば、適正な装置だけが共通の暗号鍵sk，sk'を生成することができるので、結果的に、認証が行われることになる。

【００２７】

仮に１台のパーソナルコンピュータ２のライセンスキーが盗まれたとしても、IDが１台１台異なるので、そのライセンスキーを用いて、他の装置がDVDプレーヤ１から伝送されてきた暗号化されているデータを復号することはできない。従って安全性が向上する。

【００２８】

ところで、何らかの理由により、不正なユーザが、暗号化データｅと暗号鍵skを両方とも知ってしまったような場合のことを考える。この場合、ｅは、平文skを、鍵lkで暗号化した暗号文であるので、暗号アルゴリズムが公開されている場合、不正ユーザは、鍵lkを総当たりで試すことにより、正しい鍵lkを得る可能性がある。

【００２９】

不正ユーザによるこの種の攻撃を、より困難にするために、暗号アルゴリズムの一部または全部を一般に公開せずに秘密にしておくことができる。

【００３０】

または同様に、license_keyから、service_keyを総当たりで調べる攻撃を、より困難にするために、hash関数の一部または全文を一般に公開せずに秘密にしておくようにすることもできる。

【００３１】

図１４は、ソース（DVDプレーヤ１）に対して、パーソナルコンピュータ２だけでなく、光磁気ディスク装置３もシンクとして機能する場合の処理例を表している。

【００３２】

この場合、シンク１としてのパーソナルコンピュータ２のEEPROM５０には、IDとしてID１が、また、ライセンスキーとしてlicense_key１が記憶されており、シンク２としての光磁気ディスク装置３においては、EEPROM３７に、IDとしてID２が、また、ライセンスキーとしてlicense_key２が記憶されている。

【００３３】

DVDプレーヤ１（ソース）とパーソナルコンピュータ２（シンク１）の間において行われるステップＳ１１乃至ステップＳ２０の処理は、図１２におけるステップＳ１乃至ステップＳ１０の処理と実質的に同様の処理であるので、その説明は省略する。

【００３４】

すなわち、上述したようにして、DVDプレーヤ１は、パーソナルコンピュータ２に対して認証処理を行う。そして次に、ステップＳ２１において、DVDプレーヤ１は、光磁気ディスク装置３に対して、IDを要求する。光磁気ディスク装置３においては、ステップＳ２２で1394インタフェース３６を介して、このID要求信号が受信されると、そのファームウェア３０（図１８）は、ステップＳ２３でEEPROM３７に記憶されているID（ID２）を読み出し、これを1394インタフェース３６から、1394バス１１を介してDVDプレーヤ１に伝送する。DVDプレーヤ１のファームウェア２０は、ステップＳ２４で、1394インタフェース２６を介して、このID２を受け取ると、ステップＳ２５で、次式から鍵lk２を生成する。

lk２＝hash（ID２ ‖ service_key）

【００３５】

さらに、ファームウェア２０は、ステップＳ２６で次式を演算し、ステップＳ１６で生成した鍵skを、ステップＳ２５で生成した鍵lk２を用いて暗号化し、暗号化したデータｅ２を生成する。

ｅ２＝Enc（lk２，sk）

【００３６】

そして、ステップＳ２７で、ファームウェア２０は、この暗号化データｅ２を1394インタフェース２６から1394バス１１を介して光磁気ディスク装置３に伝送する。

【００３７】

光磁気ディスク装置３においては、ステップＳ２８で、1394インタフェース３６を介してこの暗号化データｅ２を受信し、ステップＳ２９で、次式を演算して暗号鍵sk２’を生成する。

sk２’＝Dec（license_key２，ｅ２）

【００３８】

以上のようにして、パーソナルコンピュータ２と光磁気ディスク装置３のそれぞれにおいて、暗号鍵sk１’，sk２’が得られたことになる。これらの値は、DVDプレーヤ１における暗号鍵skと同一の値となっている。

【００３９】

図１４の処理例においては、DVDプレーヤ１が、パーソナルコンピュータ２と、光磁気ディスク装置３に対して、それぞれ個別にIDを要求し、処理するようにしているのであるが、同報通信によりIDを要求することができる場合は、図１４に示すような処理を行うことができる。

【００４０】

すなわち、図１５の処理例においては、ステップＳ４１で、ソースとしてのDVDプレーヤ１が、全てのシンク（この例の場合、パーソナルコンピュータ２と光磁気ディスク装置

３）に対して同報通信でIDを要求する。パーソナルコンピュータ２と光磁気ディスク装置３は、それぞれステップＳ４２とステップＳ４３で、このID転送要求の信号を受け取ると、それぞれステップＳ４４またはステップＳ４５で、EEPROM５０またはEEPROM３７に記憶されているID１またはID２を読み出し、これをDVDプレーヤ１に転送する。DVDプレーヤ１は、ステップＳ４６とステップＳ４７で、これらのIDをそれぞれ受信する。

【００４１】

DVDプレーヤ１においては、さらにステップＳ４８で、次式から暗号鍵lk１を生成する。

lk１＝hash（ID１ ‖ service_key）

【００４２】

さらに、ステップＳ４９において、次式から暗号鍵lk２が生成される。

lk２＝hash（ID２ ‖ service_key）

【００４３】

DVDプレーヤ１においては、さらにステップＳ５０で、暗号鍵skが生成され、ステップＳ５１で、次式で示すように、暗号鍵skが、鍵lk１を鍵として暗号化される。

ｅ１＝Enc（lk１，sk）

【００４４】

さらに、ステップＳ５２においては、暗号鍵skが、鍵lk２を鍵として、次式に従って暗号化される。

ｅ２＝Enc（lk２，sk）

【００４５】

さらに、ステップＳ５３においては、ID１，ｅ１，ID２，ｅ２が、それぞれ次式で示すように連結されて、暗号化データｅが生成される。

ｅ＝ID１ ‖ ｅ１ ‖ ID２ ‖ ｅ２

【００４６】

DVDプレーヤ１においては、さらにステップＳ５４で、以上のようにして生成された暗号化データｅが同報通信で、パーソナルコンピュータ２と光磁気ディスク装置３に伝送される。

【００４７】

パーソナルコンピュータ２と光磁気ディスク装置３においては、それぞれステップＳ５５またはステップＳ５６で、これらの暗号化データｅが受信される。そして、パーソナルコンピュータ２と光磁気ディスク装置３においては、それぞれステップＳ５７またはステップＳ５８において、次式で示す演算が行われ、暗号鍵sk１’，sk２’が生成される。

sk１’＝Dec（license_key１，ｅ１）

sk２’＝Dec（license_key２，ｅ２）

【００４８】

図１６は、１つのシンクが複数のサービスを受けること（複数の種類の情報の復号）ができるようになされている場合の処理例を表している。すなわち、この場合においては、例えば、シンクとしてのパーソナルコンピュータ２は、複数のライセンスキー（license_key１，license_key２，license_key３など）をEEPROM５０に記憶している。ソースとしてのDVDプレーヤ１は、そのEEPROM２７に複数のサービスキー（service_key１，service_key２，service_key３など）を記憶している。この場合、DVDプレーヤ１は、ステップＳ８１でシンクとしてのパーソナルコンピュータ２に対してIDを要求するとき、DVDプレーヤ１が、これから転送しようとする情報（サービス）を識別するservice_IDを転送する。パーソナルコンピュータ２においては、ステップＳ８２で、これを受信したとき、EEPROM５０に記憶されている複数のライセンスキーの中から、このservice_IDに対応するものを選択し、これを用いて、ステップＳ９０で復号処理を行う。その他の動作は、図１１における場合と同様である。

【００４９】

図１７は、さらに他の処理例を表している。この例においては、ソースとしてのDVDプ

レーヤ１が、そのEEPROM２７に、service_key、hash関数、および疑似乱数発生関数pRNGを記憶している。これらは、著作権者から与えられたものであり、秘密裡に保管される。また、シンクとしてのパーソナルコンピュータ２のEEPROM５０には、著作権者から与えられたID、LK, LK'、関数Ｇ、および疑似乱数数発生関数pRNGを有している。

【００５０】

LKは、著作権者が作成したユニークな乱数であり、LK'は、次式を満足するように生成されている。

LK'＝Ｇ＾－１（Ｒ）

Ｒ＝pRNG（Ｈ）　（＋）　pRNG（LK）

Ｈ＝hash（ID ‖ service_key）

【００５１】

なお、Ｇ＾－１（＾はべき乗を意味する）は、Ｇの逆関数を意味する。Ｇ＾－１は、所定の規則を知っていれば、簡単に計算することができるが、知らない場合には、計算することが難しいような特徴を有している。このような関数としては、公開鍵暗号に用いられている関数を利用することができる。

【００５２】

また、疑似乱数発生関数は、ハードウェアとして設けるようにすることも可能である。

【００５３】

DVDプレーヤ１のファームウェア２０は、最初にステップＳ１０１において、パーソナルコンピュータ２のライセンスマネージャ６２に対してIDを要求する。パーソナルコンピュータ２のライセンスマネージャ６２は、ステップＳ１０２でID要求信号を受け取ると、EEPROM５０に記憶されているIDを読み出し、ステップＳ１０３で、これをDVDプレーヤ１に伝送する。DVDプレーヤ１のファームウェア２０は、ステップＳ１０４でこのIDを受け取ると、ステップＳ１０５で次式を演算する。

Ｈ＝hash（ID ‖ service_key）

【００５４】

さらに、ファームウェア２０は、ステップＳ１０６で鍵skを生成し、ステップＳ１０７で次式を演算する。

ｅ＝sk　（＋）　pRNG（Ｈ）

【００５５】

なお、Ａ（＋）Ｂは、ＡとＢの排他的論理和の演算を意味する。

【００５６】

すなわち、疑似ランダム発生キーpRNGにステップＳ１０５で求めたＨを入力することで得られた結果、pRNG（Ｈ）と、ステップＳ１０６で生成した鍵skのビット毎の排他的論理和を演算することで、鍵SKを暗号化する。

【００５７】

次に、ステップＳ１０８で、ファームウェア２０は、ｅをパーソナルコンピュータ２に伝送する。

【００５８】

パーソナルコンピュータ２においては、ステップＳ１０９でこれを受信し、ステップＳ１１０で、次式を演算する。

sk'＝ｅ　（＋）　Ｇ（LK'）　（＋）　pRNG（LK）

【００５９】

すなわち、DVDプレーヤ１から伝送されてきたｅ、EEPROM５０に記憶されている関数Ｇに、やはりEEPROM５０に記憶されているLK'を適用して得られる値Ｇ（LK'）、並びに、EEPROM５０に記憶されているLK'を、やはりEEPROM５０に記憶されている疑似乱数発生関数pRNGに適用して得られる結果pRNG（LK）の排他的論理和を演算し、鍵sk'を得る。

【００６０】

ここで、次式に示すように、sk＝sk'となる。

sk'＝ｅ　（＋）　Ｇ（LK'）　（＋）　pRNG（LK）

＝sk （＋） pRNG（H） （＋） R （＋） pRNG（LK）
＝sk （＋） pRNG（H） （＋） pRNG（H） （＋） pRNG（LK） （＋） pRNG（LK）
＝sk

【００６１】
このようにして、ソースとしてのDVDプレーヤ１とシンクとしてのパーソナルコンピュータ２は、同一の鍵sk，sk'を共有することができる。LK，LK'を作ることができるのは、著作権者だけであるので、ソースが不正に、LK，LK'を作ろうとしても作ることができないので、より安全性を高めることができる。

【００６２】
以上においては、ソースとシンクにおいて認証を行うようにしたが、例えばパーソナルコンピュータ２には、通常、任意のアプリケーションプログラムをロードして用いることができる。そして、このアプリケーションプログラムとしては、不正に作成したものが使用される場合もある。従って、各アプリケーションプログラム毎に、著作権者から許可を得たものであるか否かを判定する必要がある。そこで、図１２に示すように、各アプリケーション部６１とライセンスマネージャ６２との間においても、上述したように、認証処理を行うようにすることができる。この場合、ライセンスマネージャ６２がソースとなり、アプリケーション部６１がシンクとなる。

【００６３】
次に、以上のようにして、認証が行われた後（暗号鍵の共有が行われた後）、暗号鍵を用いて、ソースから暗号化したデータをシンクに転送し、シンクにおいて、この暗号化したデータを復号する場合の動作について説明する。

【００６４】
図１８に示すように、DVDプレーヤ１、あるいは光磁気ディスク装置３のように、内部の機能が一般ユーザに解放されていない装置においては、1394バス１１を介して授受されるデータの暗号化と復号の処理は、それぞれ1394インタフェース２６または1394インタフェース３６で行われる。この暗号化と復号化には、セッションキーＳと時変キーｉが用いられるが、このセッションキーＳと時変キーｉ（正確には、時変キーｉを生成するためのキーｉ’）は、それぞれファームウェア２０またはファームウェア３０から、1394インタフェース２６または1394インタフェース３６に供給される。セッションキーＳは、初期値として用いられる初期値キーSsと時変キーｉを攪乱するために用いられる攪乱キーSiとにより構成されている。この初期値キーSsと攪乱キーSiは、上述した認証において生成された暗号鍵sk（＝sk'）の所定のビット数の上位ビットと下位ビットにより、それぞれ構成するようにすることができる。このセッションキーＳは、セッション毎に（例えば、１つの映画情報毎に、あるいは、１回の再生毎に）、適宜、更新される。これに対して、攪乱キーSiとキーｉ’から生成される時変キーｉは、１つのセッション内において、頻繁に更新されるキーであり、例えば、所定のタイミングにおける時刻情報などを用いることができる。

【００６５】
いま、ソースとしてのDVDプレーヤ１から再生出力した映像データを1394バス１１を介して光磁気ディスク装置３とパーソナルコンピュータ２に伝送し、それぞれにおいて復号するものとする。この場合、DVDプレーヤ１においては、1394インタフェース２６において、セッションキーＳと時変キーｉを用いて暗号化処理が行われる。光磁気ディスク装置３においては、1394インタフェース３６において、セッションキーＳと時変キーｉを用いて復号処理が行われる。

【００６６】
これに対して、パーソナルコンピュータ２においては、ライセンスマネージャ６２が、セッションキーＳのうち、初期値キーSsをアプリケーション部６１に供給し、攪乱キーSiと時変キーｉ（正確には、時変キーｉを生成するためのキーｉ’）を1394インタフェース４９（リンク部分）に供給する。そして、1394インタフェース４９において、攪乱キーSi

とキーｉ’から時変キーｉが生成され、時変キーｉを用いて復号が行われ、その復号されたデータは、アプリケーション部６１において、さらにセッションキーＳ（正確には、初期値キーSs）を用いて復号が行われる。

【００６７】

このように、パーソナルコンピュータ２においては、内部バス５１が、ユーザに解放されているので、1394インタフェース４９により第１段階の復号だけを行い、まだ暗号の状態としておく。そして、アプリケーション部６１において、さらに第２段階の復号を行い、平文にする。これにより、パーソナルコンピュータ２に対して、適宜、機能を付加して、内部バス５１において授受されるデータ（平文）をハードディスク４７や他の装置にコピーすることを禁止させる。

【発明の開示】

【発明が解決しようとする課題】

【００６８】

しかしながら、以上のような認証方法を用いても、例えば、所定の装置がリバースエンジニアリング等の何らかの処理が施され、その装置において秘密裡に保管しておくべき情報（例えば、鍵情報）が露呈した（盗まれた）場合、それらの情報を用いて、暗号化データが復号される可能性がある課題があった。

【００６９】

本発明は、このような状況に鑑みてなされたものであり、秘密裡に保管しておくべき情報が露呈した装置に対してデータの伝送を行わないようにし、より安全性を図るようにするものである。

【課題を解決するための手段】

【００７０】

本発明の一側面の暗号化コンテンツ送信装置は、暗号化コンテンツが送受信される通信システムで用いられる暗号化コンテンツ送信装置であって、他の装置から当該他の装置を識別する装置識別情報を受信する装置識別情報受信手段と、前記装置識別情報によって識別される装置が、前記暗号化コンテンツ毎に与えられたサービスキーに基づき生成されたライセンスキーを保持する装置であるか否かを、前記装置識別情報と自身に保持している前記サービスキーとに基づき生成される情報を用いて判定するライセンス取得装置判定手段と、不正装置として特定された不正装置識別情報のリストを記憶する不正装置識別情報リスト記憶手段と、前記不正装置識別情報リスト記憶手段に記憶された前記不正装置識別情報のリストに基づき、前記ライセンス取得装置判定手段で前記ライセンスキーを保持する装置と判定された装置が、不正装置であるか否かを判定する不正装置判定手段と、前記不正装置判定手段が前記他の装置は不正装置であると判定した場合に、当該不正装置に対して、暗号化コンテンツの送信を制限する暗号化コンテンツ制限手段と、新たな不正装置識別情報のリストを、他の装置から無線通信路を介して受信する不正装置識別情報リスト受信手段と、前記不正装置識別情報リスト受信手段で受信した前記新たな不正装置識別情報のリストを、前記不正装置識別情報リスト記憶手段に書き込む書き込み手段とを備える。

前記不正装置判定手段が前記他の装置は不正装置であると判定した場合に、自身と通信可能な全ての装置のうち、前記他の装置を除く装置に対して、前記他の装置は不正装置であることを通知する通知手段をさらに設けることができる。

【００７１】

前記無線通信路は、衛星を介する通信路であるようにすることができる。

【００７２】

本発明の一側面においては、他の装置から当該他の装置を識別する装置識別情報が受信され、前記装置識別情報によって識別される装置が、前記暗号化コンテンツ毎に与えられたサービスキーに基づき生成されたライセンスキーを保持する装置であるか否かが、前記装置識別情報と自身に保持している前記サービスキーとに基づき生成される情報を用いて判定され、不正装置として特定された不正装置識別情報のリストが不正装置識別情報リス

ト記憶手段に記憶され、前記不正装置識別情報リスト記憶手段に記憶された前記不正装置識別情報のリストに基づき、前記ライセンスキーを保持する装置と判定された装置が、不正装置であるか否かが判定され、前記他の装置は不正装置であると判定された場合に、当該不正装置に対して、暗号化コンテンツの送信が制限され、新たな不正装置識別情報のリストが、他の装置から無線通信路を介して受信され、受信された前記新たな不正装置識別情報のリストが、前記不正装置識別情報リスト記憶手段に書き込まれる。

【発明の効果】

【００７３】

本発明の一側面によれば、例えば、不正装置によるデータの不正コピーを防止することができる。

【発明を実施するための最良の形態】

【００７４】

以下、図面を参照して本発明を適用した実施の形態について説明する。

【００７５】

図１は、本発明を適用した情報処理システムの構成例を示す図であり、図９に示した場合と対応する部分には同一の符号を付してあり、その説明は適宜省略する。この構成例においては、管理センタ１１０は、不正装置の識別番号が記載されたリスト（revocation list：リボケーションリスト）を作成するリボケーションリスト作成部１１１と、リボケーションリスト作成部１１１により作成されたリボケーションリストをアンテナ１１３を介して送信する送信部１１２とにより構成されている。

【００７６】

リボケーションリスト作成部１１１は、所定の装置において管理されている情報の露呈が発覚した場合、その装置の識別番号（device_ID）を不正装置のdevice_IDとして記したリスト（以下、リボケーションリスト（revocation list）と称する）を作成する。また、リボケーションリスト作成部１１１は、リボケーションリストを作成したものが管理センタ１１０であることを示す署名（例えば、公開鍵暗号を用いたデジタル署名）とその作成時刻を、作成したリボケーションリストに付加する。このデジタル署名は、リボケーションリストを受け取った装置において、そのリボケーションリストが正規のものであるのか否かの検証の際に用いられる。送信部１１２は、所定のタイミングで、リボケーションリスト作成部１１１により作成されたリボケーションリストを、アンテナ１１３を介して送信する。なお、このタイミングは、例えば、１ヶ月に一度の定期的なものでもよいし、例えば、また、他の装置から要求があったときのタイミングでもよい。

【００７７】

管理センタ１１０から送信されたリボケーションリストは、例えば衛星１２０を介して、他の装置（いまの場合、データ放送受信装置１３０）に提供される。

【００７８】

データ放送受信装置１３０は、1394インタフェース１３８を介して1394バス１１に接続されている。チューナ１３２は、アンテナ１３１を介して、管理センタ１１０から衛星１２０を介して送信されるリボケーションリストを受信し、CPU１３３に出力するようになされている。CPU１３３は、ROM１３６に記憶されているプログラムに従って各種の処理を実行し、RAM１３７は、CPU１３３が各種の処理を実行する上において必要なデータやプログラム等を適宜記憶する。ハードディスク（HDD）１３５は、データまたはプログラムなどを記録または再生することができるようになされている。EEPROM１３４は、装置の電源オフ後も記憶する必要のある情報（例えば、リボケーションリスト）を記憶するようになされている。内部バス１３９は、これらの各部を相互に接続している。

【００７９】

なお、DVDプレーヤ１、パーソナルコンピュータ２、および光磁気ディスク装置３の詳細な構成は、図１０に示した場合と同様とされている。

【００８０】

ここで、1394バス１１に接続されている各装置には、それぞれに固有の識別番号である

device_ID（例えば、node_unique_ID）が与えられている。また、各装置のうち、データ放送受信装置１３０、DVDプレーヤ１、パーソナルコンピュータ２、または光磁気ディスク３等の、他の装置間でデータを送受信することができる装置（以下、特にこれらの装置を個々に区別する必要がない場合、適宜、これらの装置を総称して送受信装置と記述する）は、1394バス１１を介して自分に接続されている装置（具体的には、少なくとも一度、データの伝送を行った相手の装置）のdevice_IDが記される識別番号テーブル（connected device_ID table：以下、CDTと略記する）を、例えば、それぞれに内蔵するEEPROM内（例えば、データ放送受信装置の場合、EEPROM１３４内）の所定の領域に用意している。なお、各装置のうち、データの送信を行うことができない装置は、CDTを有する必要はない。

【００８１】

各送受信装置は、例えば、図８を参照して後述する認証処理（勿論、これ以外の認証処理でもよい）を行う際に、相手装置のdevice_IDを入手し、それをCDTに格納することができる。そして、各送受信装置は、相手側のdevice_IDを確認した後（すなわち、相手装置が正当な装置であるか否かを確認した後）、暗号化データを復号するための鍵（例えば、セッションキーまたは時変キー）を相手装置に送信するか否かを決定するようになされている。

【００８２】

データ放送受信装置１３０は、1394バス１１に接続されているこれらの全装置のdevice_IDまたは各送受信装置のCDTに格納されている情報を、所定のタイミングで適宜読み出すことができるようになされている。このタイミングは、例えば、一週間に一回のように、定期的なものであってもよいし、また、例えば、1394バス１１に新たな装置が追加または排除されたことが検出できる場合、それが検出されたタイミングで行うようにしてもよい。そして、データ放送受信装置１３０は、読みとった情報を自分自身のCDTに反映する（具体的には、新規の項目を格納する）ことができる。

【００８３】

図２は、CDTの構成例を示す図である。この例において、アドレス１乃至ｎには、1394バス１１を介して接続されている装置のdevice_IDと、不正装置のdevice_ID（リボケーションリストに記されているdevice_ID）であるか否かを示すフラグ（revocateフラグ）とが格納されるようになされている。この例においては、アドレス１乃至３のdevice_IDＡ乃至device_IDＣに、フラグ（×印）が付加されている（具体的には、フラグを示す値が、例えば１に設定されている）。すなわち、これらのdevice_IDＡ乃至device_IDＣに対応する装置は、不正な装置であるとされる。

【００８４】

データ放送受信装置１３０（または他の送受信装置）は、フラグが格納されているdevice_ID（すなわち、不正装置に対応するdevice_ID）が、常にアドレスの前段に配置されるように、CDTをソートするようになされている。例えば、図３に示すように、アドレス６に格納されているdevice_IDＦに対応する装置が不正装置であることが新たに発覚し、そのアドレス６にフラグが付加されたとき、データ放送受信装置１３０のCPU１３３は、図４に示すように、アドレス６に格納されていたdevice_IDＦを、アドレス４に移動させるとともに、アドレス４とアドレス５に格納されていたdevice_IDＥとdevice_IDＦを、それぞれアドレス５とアドレス６に移動させる。

【００８５】

なお、CDTには、ｎ個（例えば、１００個）の項目（device_IDとフラグ）を格納することができるものとする。ただし、各送受信装置のうち、管理センタ１１０から提供されるリボケーションリストを用いて、各装置のdevice_IDまたはCDTを管理する管理装置（いまの場合、データ放送受信装置１３０）のCDTには、ｎ個以上のdevice_IDとフラグを格納することができるものとする。ここで、このCDTのアドレスが全て使用されている状態において、新たにCDTに格納すべき項目が発生した場合、CDT中の、フラグが付加されていない項目のうち、一番古いものが消去され、空いたアドレスに新規の項目が格納される。

【００８６】
例えば、いま、１００個の項目を格納することができるCDTがあり、そのアドレス１乃至アドレス１０までは、フラグが付加されている項目が、古いものから順に格納されており、また、そのアドレス１１乃至アドレス１００までは、フラグが付加されていない項目が、古いものから順に格納されているものとする。例えば、このCDTを有する装置が、データの伝送を初めて行う相手装置のdevice_IDを入手し、これを新たな項目としてCDTに格納する場合、フラグが付加されていない項目のうち、一番古いものである、アドレス１１の項目を消去し、アドレス１２乃至アドレス１００に格納されていた項目を１つずつ繰り上げる（それぞれアドレス１１乃至９９に移動する）。そして、それにより空いたアドレス１００に、新たな項目が格納される。

【００８７】
また、例えば、このCDTを持つ装置が、新たなリボケーションリストを受け取り、その中のdevice_IDをCDTに格納する場合、アドレス１１の項目を消去して、そこに、リボケーションリストのdevice_IDを、フラグとともに格納する。

【００８８】
さらに、このCDTが、フラグが付加されている項目で一杯となった場合において、このCDTを有する装置は、新規に格納すべき項目が、新たに受け取ったリボケーションリストのdevice_IDであるとき、CDTの古い項目を消去して、空いたアドレスに格納し、データの伝送を初めて行った相手装置のdevice_IDであるとき、それはCDTに格納しない。

【００８９】
次に、図５のフローチャートを参照して、図１の情報処理システムの動作を説明する。ステップＳ２０１において、管理センタ１１０のリボケーション作成部１１１は、不正装置のdevice_IDを示したリボケーションリストを作成し、続いて、ステップＳ２０２において、作成したリボケーションリストに、署名と時刻を付加する。ステップＳ２０３で、送信部１１２は、所定のタイミングで、リボケーション作成部１１１により作成されたリボケーションリストを、アンテナ１１３を介して送信する。

【００９０】
そして、ステップＳ２０４において、データ放送受信装置１３０のチューナ１３２は、衛星１２０を介して提供されるリボケーションリストを、アンテナ１３１を介して受信する。CPU１３３は、ステップＳ２０５において、受信したリボケーションリストが、正当なものであるか否かを検証する。すなわち、リボケーションリストに付加されている署名が、管理センタ１１０のものであるかを検証する。なお、この検証処理においては、例えば、管理センタ１１０から発行された公開鍵を有する装置のみが署名を確認することができるものとする。

【００９１】
ステップＳ２０５において、リボケーションリストが正当なものではない（すなわち、署名が管理センタ１１０のものではない）と判定された場合、CPU１３３は、ステップＳ２０６においてリボケーションリストは不正なものとして破棄し、処理を終了する。一方、ステップＳ２０５において、リボケーションリストが正当なものである（すなわち、署名が管理センタ１１０のものである）と判定された場合、ステップＳ２０７に進み、CPU１３３は、リボケーションリスト中に記されている不正装置のdevice_IDと、CDT中のdevice_IDとを比較する。CPU１３３は、ステップＳ２０８において、CDT中に、リボケーションリストに記されているdevice_IDと合致するdevice_IDが存在するか否かを判定し、対応するdevice_IDはCDT中に存在しないと判定した場合、処理を終了する。

【００９２】
ステップＳ２０８において、リボケーションリストに記されているdevice_IDと合致するdevice_IDがCDT中に存在すると判定された場合、ステップＳ２０９に進み、CPU１３３は、CDT中の対応するdevice_IDにフラグを付加する。続いて、CPU１３３は、ステップＳ２１０において、1394インタフェース１３８を制御して、CDT中の、フラグが付加されているdevice_IDを、リボケーションリストとともに、1394バス１１を介して接続されてい

る他の送受信装置に送信する。

【００９３】

各送受信装置は、ステップＳ２１１において、データ放送受信装置１３０のフラグが付加されたdevice_IDとリボケーションリストを受信し、ステップＳ２１２において、受信したリボケーションリストが正当なものであるか否かを判定する。ステップＳ２１２において、リボケーションリストは正当なものではない（すなわち、署名が管理センタ１１０のものではない）と判定された場合、ステップＳ２１３において、そのリボケーションリストが破棄され、処理が終了される。

【００９４】

ステップＳ２１２において、リボケーションリストが正当なものであると判定された場合、ステップＳ２１４に進み、各送受信装置は、受信したリボケーションリストに対応して、それぞれのCDTの内容を更新する（対応するdevice_IDにフラグを付加する）。

【００９５】

以上の処理により、1394バス１１に接続されている全ての送受信装置のCDTが、管理センタ１１０により作成されたリボケーションリストに対応して更新された。

【００９６】

次に、以上をふまえた上で、図７を参照して、例えば、送受信装置としてのDVDプレーヤ１に対して、パーソナルコンピュータ２からデータの伝送の要求があった場合の、DVDプレーヤ１の処理を説明する。まず、ステップＳ３０１において、DVDプレーヤ１は、パーソナルコンピュータ２との間で認証処理（例えば、図８を用いて後述）を実行する。これにより、DVDプレーヤ１は、パーソナルコンピュータ２のdevice_IDを入手することになる。ステップＳ３０２において、パーソナルコンピュータ２のdevice_IDが、自分自身のCDT中でフラグが付加されているdevice_IDであるか否かが判定され、パーソナルコンピュータ２のdevice_IDが、CDT中でフラグが付加されているものであると判定された場合、ステップＳ３０３において、DVDプレーヤ１は、パーソナルコンピュータ２を不正装置であるとし、処理を終了する。

【００９７】

ステップＳ３０２において、パーソナルコンピュータ２のdevice_IDは、CDT中でフラグが付加されているものではないと判定された場合、ステップＳ３０４に進み、DVDプレーヤ１は、パーソナルコンピュータ２との間で、鍵および暗号データの伝送処理を実行する。続いて、ステップＳ３０５において、DVDプレーヤ１は、パーソナルコンピュータ２が、新規の装置であるか（すなわち、伝送処理を初めて行った装置であるか）否かを判定し、パーソナルコンピュータ２は新規の装置ではない（すなわち、伝送処理を既に行ったことがある装置である）と判定した場合、処理を終了する。

【００９８】

ステップＳ３０５において、パーソナルコンピュータ２が新規の装置である（すなわち、初めて伝送処理を行った装置である）と判定された場合、ステップＳ３０６に進み、DVDプレーヤ１は、パーソナルコンピュータ２のdevice_IDをCDTに追加する。これにより、データ放送受信装置１３０は、DVDプレーヤ１のCDTを所定のタイミングで読み出したときに、1394バス１１に新規に接続された装置（いまの場合、パーソナルコンピュータ２）のdevice_IDを入手することできるので、例えば、次に受け取ったリボケーションリストにより、このパーソナルコンピュータ２が不正装置であることが判明した場合、1394バス１１に接続されている各送受信装置（パーソナルコンピュータ２を除く）にこれを知らせることにより、パーソナルコンピュータ２を実質的に排除することが可能となる。

【００９９】

以上のようにして、各送受信装置は、管理センタ１１０から提供されたリボケーションリストに対応して、相手装置が不正な装置であるか否かを判断することができ、映画などのデータの伝送を安全に行うことができる。

【０１００】

図８は、図７のステップＳ３０１で実行される認証の処理例を示すタイミングチャート

である。この例においては、ソースとしてのDVDプレーヤ１のEEPROM２７には、サービスキー（service_key）とhash関数（Ｆ，Ｇ，Ｈ）が予め記憶されている。一方、シンクとしてのパーソナルコンピュータ２は、そのdevice_ID（ID）、ライセンスキー（license_key）、および、hash関数（Ｇ，Ｈ）を、EEPROM５０に秘密裡に保持している。まず、ステップＳ１１１において、パーソナルコンピュータ２は、乱数Ｎｂを生成する。そして、ステップＳ１１２において、1394インタフェース４９を制御して、生成した乱数Ｎｂとともに認証要求を1394バス１１を介してDVDプレーヤ１に送信する。

【０１０１】

DVDプレーヤ１は、ステップＳ１１３において、この認証要求と乱数Ｎｂを受信する。次にDVDプレーヤ１は、ステップＳ１１４において、パーソナルコンピュータ２に対してそのdevice_IDを要求する。パーソナルコンピュータ２は、ステップＳ１１５において、device_IDの要求を受信し、その対応として、ステップＳ１１６において、EEPROM５０に記録されているdevice_IDを読み出し、それをDVDプレーヤ１に送信する。これにより、DVDプレーヤ１は、パーソナルコンピュータ２のdevice_IDを入手することができる。

【０１０２】

DVDプレーヤ１は、ステップＳ１１７において、パーソナルコンピュータ２から送信されたdevice_IDを受信し、ステップＳ１１８において、次式で示すように、サービスキー（Kser）を鍵とするhash関数Ｆに、受信したIDを適用することにより、データKvを生成する。なお、keyedhashＡ１（Ａ２，Ａ３）は、Ａ２を鍵とするhash関数Ａ１に、Ａ３を適用することを示している。

Kv＝keyedhashＦ（Kser，ID）

【０１０３】

次に、DVDプレーヤ１は、ステップＳ１１９で、乱数Ｎａを生成し、ステップＳ１２０で、乱数Ｎａをパーソナルコンピュータ２に送信する。パーソナルコンピュータ２は、ステップＳ１２１で乱数Ｎａを受信し、ステップＳ１２２において、次式に示すように、ライセンスキーKlicを鍵とするhash関数Ｈに、乱数Ｎａと乱数Ｎｂを連結したデータ（Na‖Nb）を適用することにより、データＲを生成する。

Ｒ＝keyedhashＨ（Klic，Na‖Nb）

【０１０４】

そして、パーソナルコンピュータ２は、ステップＳ１２３において、生成したデータＲをDVDプレーヤ１に送信する。DVDプレーヤ１は、ステップＳ１２４で、データＲを受信し、ステップＳ１２５において、ステップＳ１１８で生成されたデータKvを鍵とするhash関数Ｈに連結データ（Na‖Nb）を適応して得られた値が、受信されたデータＲと等しいか否かを判定する。

【０１０５】

ステップ１２５において、両者が等しくないと判定された場合、受信されたデータＲは破棄され、認証処理は終了される（すなわち、パーソナルコンピュータ２は不適正なものと判定される）。一方、ステップ１２５において、両者が等しいと判定された場合、ステップＳ１２６に進み、DVDプレーヤ１は、次式に示すように、データKvを鍵とするhash関数Ｇに連結データ（Na‖Nb）を適用することにより、鍵Kabを生成する。

Kab＝keyedhashＧ（Kv，Na‖Nb）

【０１０６】

なお、この鍵Kabは、DVDプレーヤ１とパーソナルコンピュータ２の間で一時的に用いられる鍵である。例えば、ソースとしてのDVDプレーヤ１に、パーソナルコンピュータ２の他にシンクとして光磁気ディスク装置３が接続されている場合、DVDプレーヤ１と光磁気ディスク装置３との間で用いられる鍵が、さらに別途生成されることになる。

【０１０７】

次に、ステップＳ１２７において、DVDプレーヤ１は、セッション内で共通に使用する鍵Kcを生成し、ステップＳ１２８において、鍵Kabを用いて鍵Kcを暗号化して、暗号化データ（暗号化鍵）Ｘを生成する。すなわち、次式が演算される。なお、Enc（Ｂ１，Ｂ２

）は、Ｂ１を鍵として、Ｂ２を暗号化することを示している。

Ｘ＝Enc（Kab，Kc）

【０１０８】

そして、DVDプレーヤ１は、ステップＳ１２９において、暗号化データＸをパーソナルコンピュータ２に送信する。ステップＳ１３０において、パーソナルコンピュータ２は、DVDプレーヤ１から送信された暗号化データＸを受信し、ステップＳ１３１で、ライセンスキーKlicを鍵とするhash関数Ｇに、連結データ（Na‖Nb）を適用することにより、鍵K'abを生成する。すなわち、次式が演算される。

K'ab＝keyedhashＧ（Klic，Na‖Nb）

【０１０９】

そして、ステップＳ１３１において、パーソナルコンピュータ２は、次式にし示すように、鍵K'abを用いてデータＸを復号して、鍵Kcを得る。なお、Dec（Ｃ１，Ｃ２）は、Ｃ１を鍵として、Ｃ２を復号することを示している。

Kc＝Dec（K'ab，Ｘ）

【０１１０】

これにより、例えば、シンクとしての装置が複数存在する場合においても、ソースと全てのシンクとの間で、同一の鍵Kcを安全に共有することができる。

【０１１１】

そして、DVDプレーヤ１のファームウェア２０は、ステップＳ１２１において、乱数N'aを生成し、ステップＳ１３３において、乱数N'aをパーソナルコンピュータ２に送信する。パーソナルコンピュータ２のライセンスマネージャ６２は、ステップＳ１３４で、乱数N'aを受信する。そして、DVDプレーヤ１のファームウェア２０とパーソナルコンピュータ２のライセンスマネージャ６２は、それぞれ、ステップＳ１３５とステップＳ１３６において、鍵Kcと乱数N'aを用いて次式を演算することにより、ともにセッションキーskを得る。

sk＝keyedhashＨ（Kc，N'a）

【０１１２】

なお、セッションキーを変更する場合、ソースは、新たな乱数を生成して、シンクとなる全ての装置にそれを送信し、それぞれの装置において、その新たな乱数を用いてセッションキーを生成するようにする。

【０１１３】

ところで、以上の処理では、各送受信装置が、リボケーションリストの正当性を確認することができるようにするため、管理装置であるデータ放送受信装置１３０は、受信したリボケーションリストを各送受信装置に伝送するようになされているが、リボケーションリストのデータサイズが大きい場合、通信コストが高くなることが予想される。そこで、この対策として、以下の２つの方法が考えられる。

（１）　管理センタ１１０が、リボケーションリストを作成する際に、それを所定の数に分割し、分割したリストそれぞれに対して署名を付加し、それをデータ放送受信装置１３０等の管理装置に提供し、また、データ放送受信装置１３０等の管理装置は、管理センタ１１０から提供されたリボケーションリストの中から、自分自身に接続されている装置に関連するものだけを、接続されている他の送受信装置に伝送するようにする。

（２）　データ放送受信装置１３０等の管理装置は、デジタル署名を作成する機能を備えるようにし、リボケーションリストの中から自分のCDTに含まれている部分を取り出し、自分のネットワーク用のリボケーションリストを新たに作成して、それに署名を付加し、それを接続されている他の送受信装置に伝送するようにする。

【０１１４】

なお、上記の各種の指令を実行するプログラムまたはリボケーションリストは、磁気ディスク、CD-ROM等の伝送媒体を介してユーザに提供したり、ネットワーク等の伝送媒体を介してユーザに提供し、必要に応じて内蔵するRAMやハードディスク等に記憶して利用させるようにすることができる。

【図面の簡単な説明】

【０１１５】

【図１】本発明を適用した情報処理システムの構成例を示すブロック図である。

【図２】CDTの構成例を示す図である。

【図３】図２のCDTに新規のdevice_IDが追加された様子を示す図である。

【図４】CDTのアドレスをソートする処理を説明する図である。

【図５】図１の情報処理システムの処理を説明するフローチャートである。

【図６】図５に続く図である。

【図７】DVDプレーヤ１の処理を説明するフローチャートである。

【図８】図７のステップＳ３０１の認証処理を説明するタイミングチャートである。

【図９】従来の情報処理システムの構成例を示すブロック図である。

【図１０】図８のDVDプレーヤ１、パーソナルコンピュータ２、および光磁気ディスク装置３の内部の構成例を示すブロック図である。

【図１１】認証処理を説明する図である。

【図１２】認証処理を説明するタイミングチャートである。

【図１３】node_unique_IDのフォーマットを示す図である。

【図１４】他の認証処理を説明するタイミングチャートである。

【図１５】他の認証処理を説明するタイミングチャートである。

【図１６】他の認証処理を説明するタイミングチャートである。

【図１７】他の認証処理を説明するタイミングチャートである。

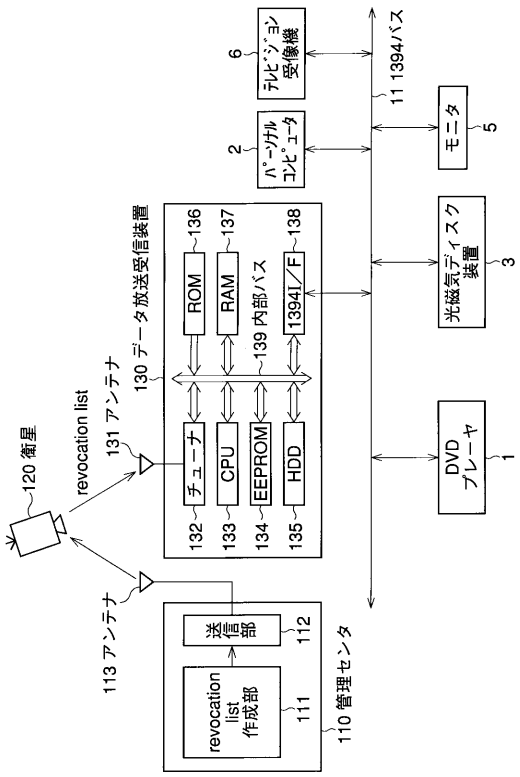
【図１８】暗号化処理を説明するブロック図である。

【符号の説明】

【０１１６】

１　DVDプレーヤ，　２　パーソナルコンピュータ，　３　光磁気ディスク装置，　１１　1394バス，　１１０　管理センタ，　１１１　リボケーションリスト作成部，　１１２　チューナ，　１１３　アンテナ，　１２０　衛星，　１３０　データ放送受信装置，　１３１　アンテナ，　１３２　チューナ，　１３３　CPU，　１３４　EEPROM，　１３５　ハードディスク，　１３６　ROM，　１３７　RAM，　１３８　1394インタフェース，　１３９　内部バス

【図１】



【図２】

アドレス	device_ID	revocate フラグ
1	A	X
2	B	X
3	C	X
4	D	
5	E	
6		
・		
・		
・		
n		

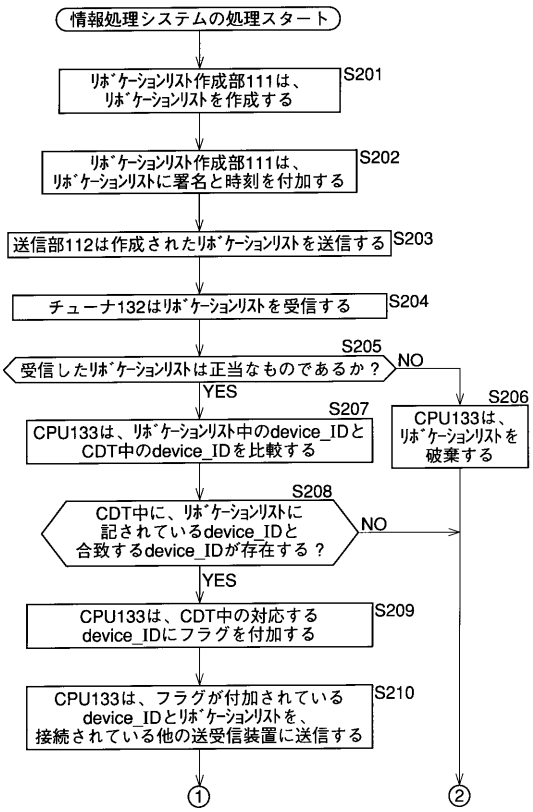
【図３】

アドレス	device_ID	revocate フラグ
1	A	X
2	B	X
3	C	X
4	D	
5	E	
6	F	X (新規)
・		
・		
・		
n		

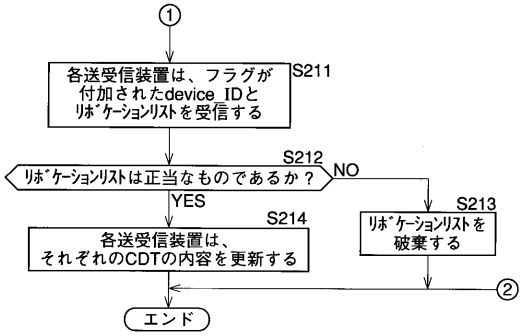
【図４】

アドレス	device_ID	revocate フラグ
1	A	X
2	B	X
3	C	X
4	F	X
5	D	
6	E	
・		
・		
・		
n		

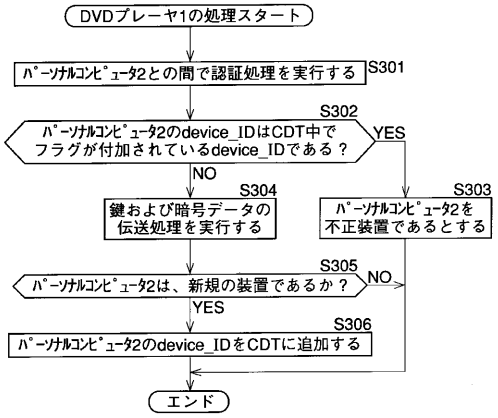
【図５】



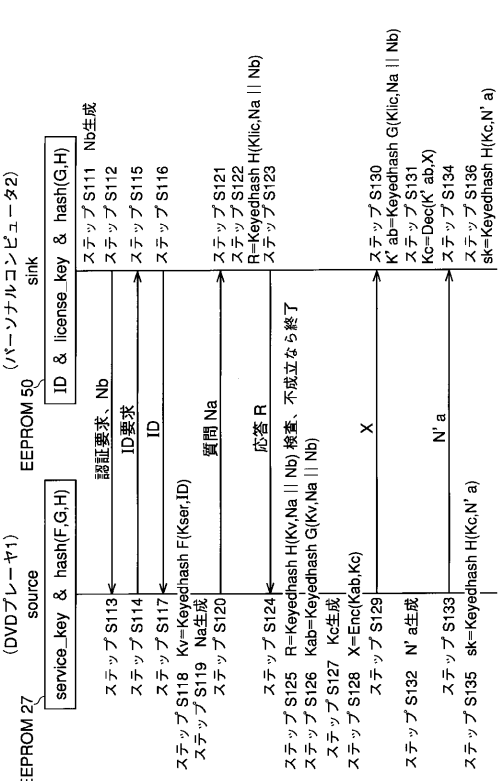
【図６】


①
各送受信装置は、フラグが付加されたdevice_IDとﾘﾎﾞｹｰｼｮﾝﾘｽﾄを受信する
S211
ﾘﾎﾞｹｰｼｮﾝﾘｽﾄは正当なものであるか？
S212
NO
YES
ﾘﾎﾞｹｰｼｮﾝﾘｽﾄを破棄する
S213
各送受信装置は、それぞれのCDTの内容を更新する
S214
②
エンド

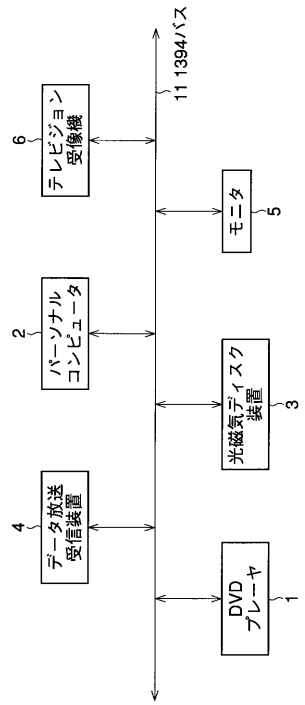
【図７】


DVDプレーヤ1の処理スタート
ﾊﾟｰｿﾅﾙｺﾝﾋﾟｭｰﾀ2との間で認証処理を実行する
S301
ﾊﾟｰｿﾅﾙｺﾝﾋﾟｭｰﾀ2のdevice_IDはCDT中でフラグが付加されているdevice_IDである？
S302
YES
NO
鍵および暗号データの伝送処理を実行する
S304
ﾊﾟｰｿﾅﾙｺﾝﾋﾟｭｰﾀ2を不正装置であるとする
S303
ﾊﾟｰｿﾅﾙｺﾝﾋﾟｭｰﾀ2は、新規の装置であるか？
S305
NO
YES
ﾊﾟｰｿﾅﾙｺﾝﾋﾟｭｰﾀ2のdevice_IDをCDTに追加する
S306
エンド

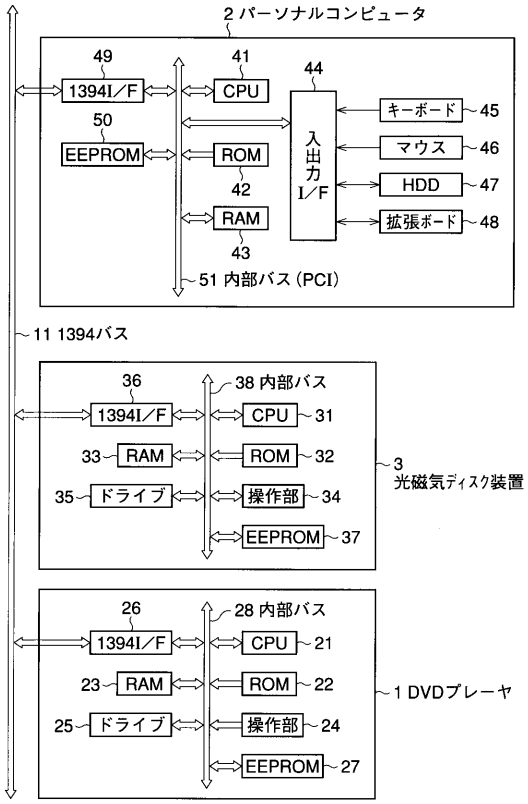
【図８】


(DVDプレーヤ1)
source
EEPROM 27
service_key & hash(F,G,H)
(パーソナルコンピュータ2)
sink
EEPROM 50
ID & license_key & hash(G,H)
ステップ S111 Nb生成
ステップ S112 認証要求、Nb
ステップ S113
ステップ S114 ID要求
ステップ S115 ID
ステップ S116
ステップ S117
ステップ S118 Kv=Keyedhash F(Kser,ID)
ステップ S119 Na生成
ステップ S120 質問 Na
ステップ S121
ステップ S122 R=Keyedhash H(Klic,Na || Nb)
ステップ S123 応答 R
ステップ S124
ステップ S125 R=Keyedhash H(Kv,Na || Nb) 検査、不成立なら終了
ステップ S126 Kab=Keyedhash G(Kv,Na || Nb)
ステップ S127 Kc生成
ステップ S128 X=Enc(Kab,Kc)
ステップ S129 X
ステップ S130
K' ab=Keyedhash G(Klic,Na || Nb)
ステップ S131
Kc=Dec(K' ab,X)
ステップ S132 N' a生成
ステップ S133 N' a
ステップ S134
ステップ S135 sk=Keyedhash H(Kc,N' a)
ステップ S136
sk=Keyedhash H(Kc,N' a)

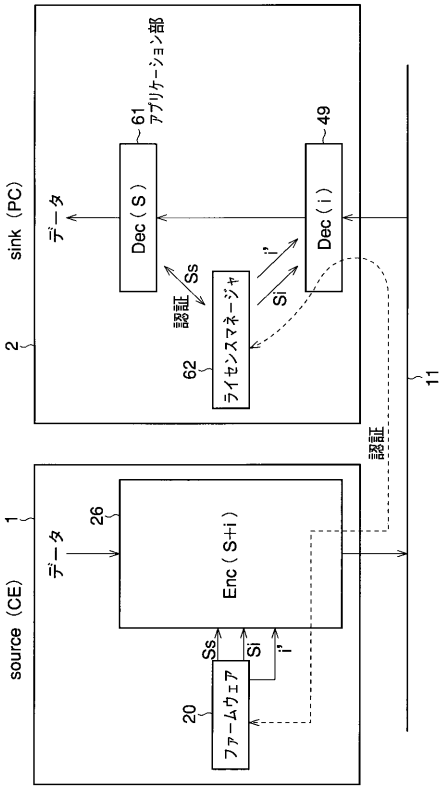
【図９】


11 1394バス
6 テレビジョン受像機
モニタ 5
2 パーソナルコンピュータ
光磁気ディスク装置 3
4 データ放送受信装置
DVDプレーヤ 1

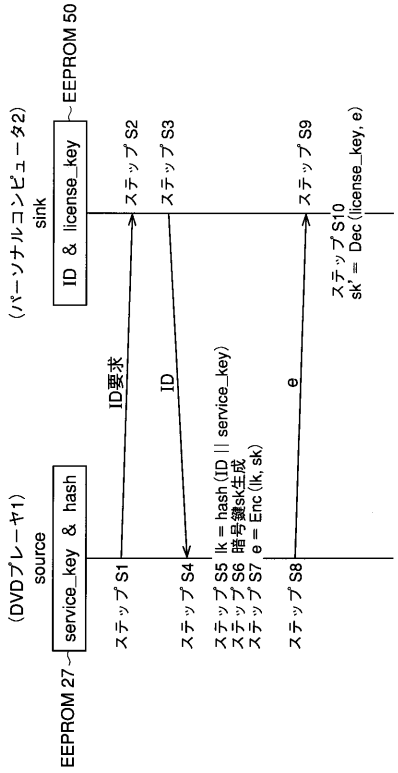
【図１０】



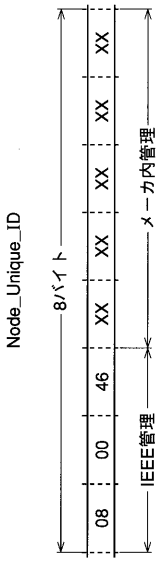
【図１１】



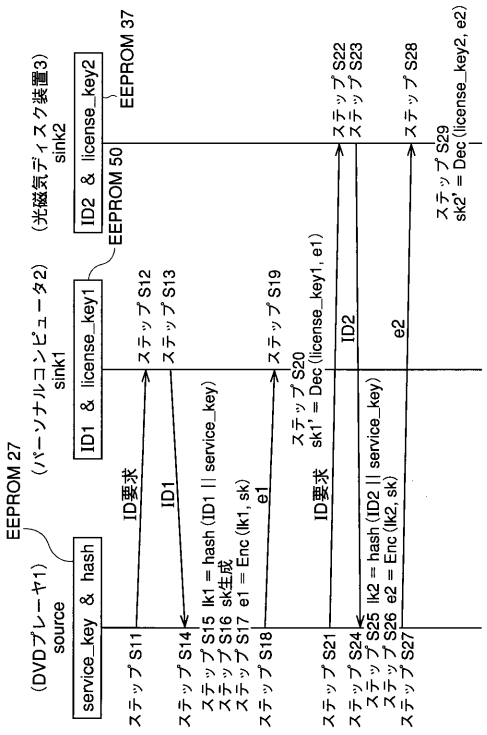
【図１２】



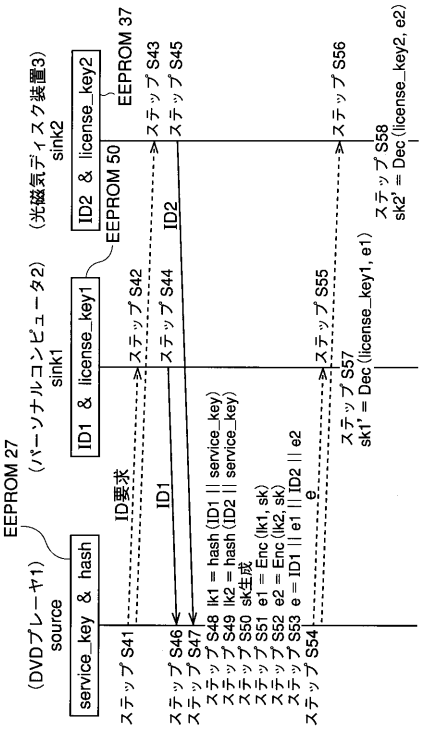
【図１３】



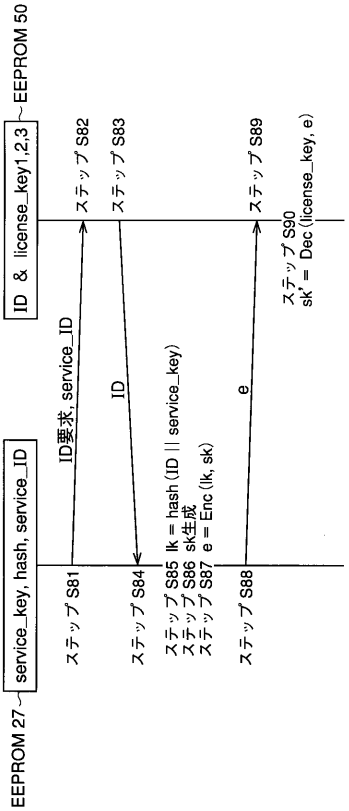
【図１４】



【図１５】

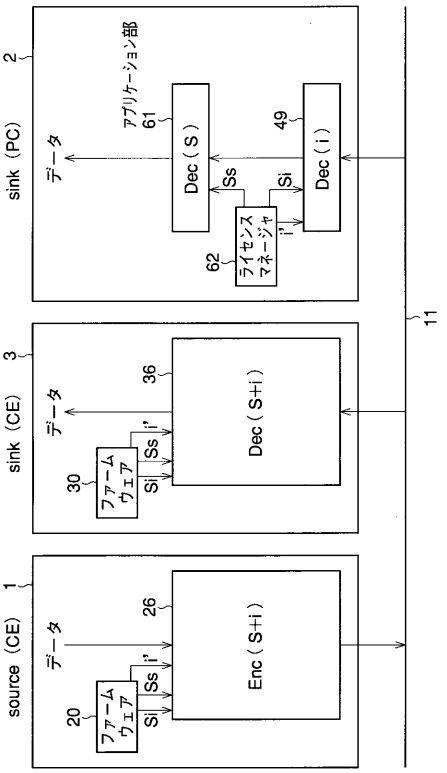


【図１６】



【図１７】

【図１８】


source (CE)
1
データ
20
フレーム
ウェア
Si
Ss
i'
26
Enc (S+i)
sink (CE)
3
データ
30
フレーム
ウェア
Si
Ss
i'
36
Dec (S+i)
sink (PC)
2
データ
アプリケーション部
61
Dec (S)
Ss
62
ライセンス
マネージャ
i'
Si
49
Dec (i)
11

フロントページの続き

(51)Int.Cl.			FI		
H04N 5/91	*(2006.01)*		H04N	7/16	Z
			H04N	5/91	L
			H04N	5/91	P

(72)発明者 浅野 智之
東京都港区港南１丁目７番１号 ソニー株式会社内

審査官 鳥居 稔

(56)参考文献 特開平０７－０８５１７２（ＪＰ，Ａ）
特開平０９－０９１１３３（ＪＰ，Ａ）
特開平０６－０９６０９８（ＪＰ，Ａ）
特開平９－１０７３５０（ＪＰ，Ａ）
特開平９－１２８３３６（ＪＰ，Ａ）
特開昭６１－１８８６６６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｈ０４Ｌ ９／３６
Ｇ０６Ｆ ２１／２４