(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2005-514877
(P2005-514877A)
(43)公表日　平成17年5月19日(2005.5.19)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601B	5J104
	H04L	9/00	601E	

審査請求 未請求　予備審査請求 未請求　（全 13 頁）

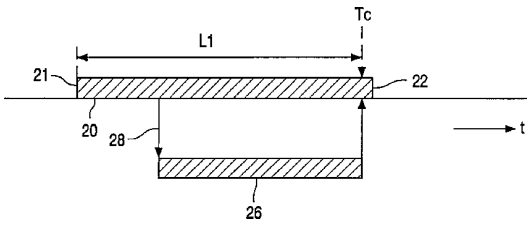
(21)出願番号	特願2003-559144 (P2003-559144)
(86)(22)出願日	平成14年12月9日 (2002.12.9)
(85)翻訳文提出日	平成16年5月25日 (2004.5.25)
(86)国際出願番号	PCT/IB2002/005272
(87)国際公開番号	WO2003/058956
(87)国際公開日	平成15年7月17日 (2003.7.17)
(31)優先権主張番号	02075144.2
(32)優先日	平成14年1月14日 (2002.1.14)
(33)優先権主張国	欧州特許庁 (EP)

(71)出願人　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
Ｋｏｎｉｎｋｌｉｊｋｅ　Ｐｈｉｌｉｐｓ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｎ．Ｖ．
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　１
Ｇｒｏｅｎｅｗｏｕｄｓｅｗｅｇ　１，５６２１　ＢＡ　Ｅｉｎｄｈｏｖｅｎ，Ｔｈｅ　Ｎｅｔｈｅｒｌａｎｄｓ
(74)代理人　100087789
弁理士　津軽　進
(74)代理人　100114753
弁理士　宮崎　昭彦

最終頁に続く

(54)【発明の名称】暗号化された情報の配信

(57)【要約】
選択的に情報のユニットの解読を可能にすることが出来るセキュアデバイスが、暗号化された情報のユニットのストリームに対するアクセスを供給するために用いられる。各ユニットはタイムスタンプと関連付けられる。権利付与管理メッセージは、指定された範囲内の値を持つタイムスタンプと関連付けられている情報のユニットの解読を可能にする権利を前記セキュアデバイスに付与する。前記範囲は、前記権利付与メッセージと同時に配信される前記タイムスタンプの現在の時間値より実質的に前に開始点を持つ。実施例においては、前記ストリームは、各々が自身のセキュアデバイスを持つ複数の受信契約者に配信される。各受信契約者のための前記現在の時間値までの前記開始点の距離は、該受信契約者のための受信契約情報に依存して選択される。



【特許請求の範囲】
【請求項１】
暗号化された情報のユニットを配信し、選択的に前記ユニットの解読を可能にすることが出来るセキュアデバイスを用いて該ユニットに対する条件付きアクセスを供給する方法であり、
－各々が各々のタイムスタンプと関連付けられる前記情報のユニットを連続的に有するストリームを配信するステップと、
－権利付与管理メッセージを前記セキュアデバイスに送るステップとを有し、前記権利付与メッセージが、タイムスタンプ値の範囲の指定を含み、その範囲内の値を持つタイムスタンプと関連付けられている情報のユニットの解読を可能にする権利を前記セキュアデバイスに付与する方法であって、前記範囲が、前記権利付与メッセージと同時に配信される前記タイムスタンプの時間値より実質的に前の開始点を持つ方法。
【請求項２】
前記ストリームが、各々が自身のセキュアデバイスを持つ複数の受信契約者に送信され、前記権利付与管理メッセージが、各々が前記受信契約者の関連する１人の前記セキュアデバイスにとって受信可能なように送られる複数の関連する権利付与管理メッセージのうちの１つであり、各権利付与管理メッセージが、関連するタイムスタンプ値の範囲の指定を含む請求項１に記載の方法であって、
－受信契約者依存受信契約情報を受信するステップと、
－関連する距離値に基づいて前記関連する範囲の各々における前記時間値に対する前記開始点の距離を設定し、前記受信契約者のセキュアデバイスのための前記権利付与管理メッセージが受信可能である該受信契約者のための前記受信契約情報に依存して、２つ以上の距離値のセットから各関連する距離値を選択するステップとを有することを特徴とする方法。
【請求項３】
前記権利付与管理メッセージが、前記開始点が実質的に前記時間値に対して時間非依存距離を持つように前記範囲が時間と共にスライドするように各々がそれ自身の範囲を指定する一連の連続的な権利付与管理メッセージの１つであることを特徴とする請求項１に記載の方法。
【請求項４】
前記セキュアデバイスが、前記タイムスタンプが時間の関数として配信されるように該タイムスタンプの前記時間値に対応して現在の時間値の維持及び更新をし、前記セキュアデバイスが、前記現在の時間値より時間非依存距離前に前記開始点を合わせ、前記セキュアデバイスが、少なくとも一連の連続的な現在の時間値のために前記権利付与管理メッセージのうちの前記１つから前記時間非依存距離を得ることを特徴とする請求項１に記載の方法。
【請求項５】
前記範囲が、前記権利付与メッセージのうちの前記１つと同時に配信される前記タイムスタンプの前記時間値より実質的に前に終了することを特徴とする請求項１に記載の方法。
【請求項６】
前記受信契約者のうちの１人のための前記受信契約情報が、当該選択を受信する時間に配信される前記タイムスタンプの前記時間値より実質的に前に終了する他の範囲の選択を有する請求項２に記載の方法であって、前記権利付与メッセージに加えて他の権利付与管理メッセージを送るステップを有し、前記他の権利付与管理メッセージが、前記他の範囲を指定し、その他の範囲内の値を持つタイムスタンプと関連付けられている情報のユニットの解読を可能にする権利を前記セキュアデバイスに付与することを特徴とする方法。
【請求項７】
暗号化された情報のユニットに対する条件付きアクセスを供給する情報配信システムであって、

－各々が各々のタイムスタンプと関連付けられる連続的な暗号化された情報のユニットのストリームを配信するよう構成される情報配信装置と、
－前記ストリームを受信するよう構成される少なくとも１つの情報受信装置と、
－前記少なくとも１つの情報受信装置に結合されるセキュアデバイスであって、タイムスタンプ値の範囲の指定を含み、その範囲内の値を持つタイムスタンプと関連付けられている情報のユニットの解読を可能にする権利を前記セキュアデバイスに付与する権利付与管理メッセージの制御のもとで選択的に前記ユニットの解読を可能にするためのセキュアデバイスとを有し、
－前記情報配信装置が、前記範囲が前記権利付与メッセージと同時に配信される前記タイムスタンプの時間値より実質的に前の開始点を持つように該権利付与メッセージを送るよう構成される情報配信システム。

【請求項８】
各々が各々の受信契約者のためのものである複数のセキュアデバイスを有し、前記権利付与管理メッセージが、各々が前記セキュアデバイスの関連する１つにとって受信可能なように送られる複数の関連する権利付与管理メッセージのうちの１つであり、前記権利付与管理メッセージの各々が、関連するタイムスタンプ値の範囲の指定を含み、前記情報配信装置が、
－受信契約者依存受信契約情報を受信する入力部と、
－関連する距離値に基づいて前記関連する範囲の各々における前記時間値に対する前記開始点の距離を設定する手段とを持ち、前記手段が、前記受信契約者のセキュアデバイスのための前記権利付与管理メッセージが受信可能である該受信契約者のための前記受信契約情報に依存して、２つ以上の距離値のセットから各関連する距離値を選択することを特徴とする請求項７に記載のシステム。

【請求項９】
情報配信システム用のセキュアデバイスであり、タイムスタンプと関連付けられている情報ユニットのストリームに対する条件付きアクセスを供給するセキュアデバイスであり、
－権利付与管理メッセージを受信する入力部と、
－現在の時間カウントを維持するメモリと、
－前記権利付与管理メッセージの制御のもとで選択的に前記情報ユニットの解読を可能にする管理ユニットとを有し、前記管理ユニットが、前記セキュアデバイスが解読を可能にしなければならない情報のユニットと関連付けられるタイムスタンプ値の範囲の指定を含む前記権利付与管理メッセージの１つを実施するよう構成されるセキュアデバイスであって、前記範囲が、前記現在の時間カウントより実質的に前に延在するセキュアデバイス。

【請求項１０】
各ユニットが各々のタイムスタンプと関連付けられる連続的な暗号化された情報のユニットのストリームをセキュアデバイスに配信するよう構成される情報配信装置であって、タイムスタンプ値の範囲の指定を含み、その範囲内の値を持つタイムスタンプと関連付けられている情報のユニットの解読を可能にする権利を前記セキュアデバイスに付与する権利付与管理メッセージを、前記範囲が前記権利付与メッセージと同時に配信される前記タイムスタンプの時間値より実質的に前の開始点を持つように送信する送信ユニットを持つ情報配信装置。

【請求項１１】
各々が各々のセキュアデバイスを持つ複数の受信契約者に前記ストリームを配信するよう構成され、前記権利付与管理メッセージが、前記セキュアデバイスの関連する１つによって受信されるための複数の権利付与管理メッセージの１つであり、各権利付与管理メッセージが、関連するタイムスタンプ値の範囲を指定する請求項１０に記載の情報配信装置であって、
－受信契約者依存受信契約情報を受信する入力部と、
－関連する距離値に基づいて前記関連する範囲の各々における前記時間値に対する前記開

始点の距離を設定する手段とを持ち、前記手段が、前記受信契約者のセキュアデバイスのための前記権利付与管理メッセージが受信可能である該受信契約者のための前記受信契約情報に依存して、２つ以上の距離値のセットから各関連する距離値を選択することを特徴とする情報配信装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、暗号化された情報を配信し、その情報に対する条件付きアクセスを供給する方法と、暗号化された情報を配信するシステムと、このようなシステム用のセキュアデバイス(secure device)とに関する。

【背景技術】

【０００２】

国際特許出願公開番号第WO98/27732号から、セキュアデバイスに情報を解読する権限が与えられる時間間隔を制御するためにタイムスタンプを用いる条件付きアクセスシステムは既知である。このシステムは、暗号化された情報と権利付与制御メッセージ(entitlement control message)(ECM)とを含むデータストリームをブロードキャストする。情報を解読するのに必要とされる解読鍵は時間とともに変わる。新しい解読鍵が必要になるたびに、この鍵はECMにおいてブロードキャストされる。解読鍵自体がECMから解読される必要がある。これは、ECMから鍵を解読するために必要な解読鍵を含むスマートカードにおいて（又はより広くはセキュアデバイスで）行なわれる。スマートカードは、データストリームから情報を解読する復号装置に解読された鍵を供給する。

【０００３】

このような条件付きアクセスシステムは、従来、受信契約者(subscriber)が情報にアクセスする権利に対して代金を支払う状況下で用いられる。これの主な例は、受信契約者が或るチャンネルを見る権利に対して代金を支払うケーブルTVシステムなどのビデオ信号配信システムである。代金を支払っている受信契約者のスマートカードには、復号装置に解読された鍵を供給する権限が与えられる。条件付きアクセスを制御するために、スマートカードは権利付与情報を含み、権利付与情報は、スマートカードが鍵を解読し、それらを復号装置に供給すべき状況を指定する。権利付与情報は、データストリームと共に権利付与管理メッセージ（entitlement management message）(EMM)においてスマートカードに供給される。

【０００４】

条件付きアクセスシステムの１つの重要な必要条件は、条件付きアクセスシステムが、不正なアクセス権を得るための不正変更に対して耐性があることである。例えば、情報の解読は、通常、当該期間に対して受信料が支払われている期間に限定される。不正変更の１つの形態は所謂リプレイ攻撃(replay attack)であり、リプレイ攻撃においては、データストリームの一部が、しばらくの間媒体に記憶され、遅延を伴ってスマートカード及び復号装置に供給される。斯くして、スマートカードが復号装置に鍵を供給する権利を有する期間外に受信されるデータストリームの一部が復号され得る。

【０００５】

国際特許出願公開番号第WO98/27732号のシステムは、このような不正変更に対処せんとする機構を記載している。このシステムは、受信契約期間(subscription period)の開始時に、受信契約期間の最初及び最後、即ち、スマートカードが鍵を供給すべき期間、逆に言えば、その期間外にはスマートカードは復号装置に鍵を供給すべきでない期間を指定するEMMを送る。タイムスタンプはECMに付加される。タイムスタンプは、各ECMがブロードキャストされた時間を特定する。ECMが受信される場合に、スマートカードは、該ECMのタイムスタンプがEMMによって指定された受信契約期間内であるか否かを調べ、前記受信契約期間内である場合にのみ解読された鍵を供給する。斯くして、受信契約期間外に受信された記録情報であって、受信契約期間中にセキュアデバイスに供給される記録情報は、解読され得ない。EMMの後の受信契約期間中にブロードキャストされる情報しか解読され得

ない。
【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明の目的は、とりわけ、条件付きアクセスを備える情報配信システムの受信契約者に他の種類の選択的なアクセス又はより多様なタイプの選択的なアクセスを供給することにある。
【課題を解決するための手段】
【０００７】
本発明による方法は請求項１に記載されている。本発明によれば、受信契約者が過去にブロードキャストされた記憶情報を見る機会を得ることが出来るタイプの契約が可能にされる。
【０００８】
本発明によれば、権利付与管理メッセージは、データストリームの一部の解読が可能にされる時間値の範囲を指定する。前記範囲は、実質的に、現在の時間から（例えば少なくとも１つのテレビ番組又はこのような番組の意味のある部分を収録するのに十分に遠い過去、例えば少なくとも１時間以上、１日以上又は１週間以上前を実質的に意味する）過去に及び、配信後に記憶されている情報であって、故に、前記情報と関連付けられたタイムスタンプが（伝送遅延を考慮しても）実質的に現在の時間に対応しない情報の解読を可能にする。本明細書で使用されているような前記現在の時間は、日付及び時刻を含み得る。前記現在は、情報ユニットが配信される場合に前記情報ユニットと関連付けられるタイムスタンプの時間値に対応する。
【０００９】
このため、前記権利付与管理メッセージは、その期間前に送信された前記データストリームの一部の解読を可能にする。即ち、セキュアデバイスには、現在の日付及び時間より指定された期間を超えないだけ前に受信された記憶情報のための解読鍵を供給する権限が与えられる。斯くして、受信契約者には、タイムシフトがあまり大き過ぎない場合にのみ、タイムシフトされた情報を見る権限が与えられる。
【００１０】
これは、サービスプロバイダが、より長い又はより短いスライディングウィンドウを持つ様々なサービスレベルを備えるサービスを売ることを可能にする。例えば、一実施例においては、個々の受信契約者が、ますますより高い受信料ではますますより遠い過去に及ぶ時間範囲を持つ様々なサービスレベルを選択し得る。又は逆に、例えばスポーツの試合の場合は、前記スライディングウィンドウが終了するのがより遠い過去であるほど受信料はより低くなり得る。このため、ユーザの契約に基づいて異なる遅延を伴って前記試合を見ることを許される様々なユーザによって該試合の単一のブロードキャストが記憶され得る。従って、各ユーザグループに対して前記試合をブロードキャストし直す必要がない。前記権利付与は、前記時間範囲中にブロードキャストされる全ての情報に及んでもよく、又は他の例においては、前記ストリームの様々な部分のための（例えば様々なテレビ番組のための）様々な範囲に対する様々な権利付与が送られてもよく、又は過去の前記ストリームの幾つかの部分のみのための権利付与が送られてもよい。
【００１１】
他の実施例においては、前記時間範囲が現在の時間と共にスライドする、即ち、前記時間範囲の最初が、現在の時間より所定の距離前に保たれ、現在の時間と共に進む。これは、例えば、前記範囲を更新するように前記セキュアデバイスに定期的に最新情報を送ることによって、又は前記セキュアデバイスにおいて進む現在の時間値を維持し、その現在の時間値を基準としてタイムスタンプの値を調べることによって達成され得る。
【００１２】
好ましくは、前記スライディングウィンドウはまた、該ウィンドウがスライドすることが出来る最大時間値を規定するために或る絶対値と関連付けられる。これは、例えば、前

記スライディングウィンドウにおいて解読を可能にする権利をセキュアデバイスに付与する権利付与管理メッセージ中にこのような最大時間値を組み込むことによって達成され得る。この場合には、前記セキュアデバイスは、解読を可能にする前に、前記ウィンドウの境界とだけでなく、前記最大時間値ともデータストリームからのタイムスタンプを比較し、且つ／又は現在の日付及び時間と前記最大時間値を比較する。別の例においては、これは、他の権利付与情報の更新（例えば、次の受信契約期間の間に情報を見るための権利付与）を、受信契約者が前記スライディングウィンドウに対して代金を支払っていない場合に該スライディングウィンドウを無効にするための命令と関連付けることによって達成され得る。

【００１３】

別の実施例においては、本発明は、受信契約者が、その権利を購入するより実質的に前の時間に終了する（現在の時間と共にスライドしない）一定期間の間に受信された情報を解読する権利を遡及的に購入することが出来る契約を可能にする。契約に対するこのような付加に応じて、前記受信契約者が前記一定期間中に媒体に記憶した前記データストリームの一部からの情報を見る権限を該受信契約者に与えるための付加的な権利付与管理メッセージが送られる。前記期間は、過去の所定の時間に始まり、好ましくは、過去の所定の時間に終わる。

【００１４】

このようにして、例えば、受信契約者は、休暇後に、該休暇中にブロードキャストされたテレビ番組又は映画などの任意のコンテンツを見る権利を購入することが出来る。前記受信契約者がこのような権利を購入する場合に、前記権利は記憶情報を用いる権限を前記受信契約者に与えることから、前記番組はブロードキャストし直される必要がない。

【００１５】

本発明による方法及びシステムのこれら及び他の目的及び有利な面を以下の図を用いてより詳細に記載する。

【発明を実施するための最良の形態】

【００１６】

図１は、情報配信システムを示している。このシステムは、暗号化されたメディアストリームの供給源１０と、受信契約管理ユニット１１と、条件付きアクセス装置１２と、記憶装置１６（例えば磁気若しくは光ディスク又はテープのレコーダ）と、他の受信システム１９とを含む。受信契約管理ユニット１１は、供給源１０に結合される出力部を持つ。供給源１０は、条件付きアクセス装置１２と、記憶装置１６と、他の受信システムとに結合される出力部を持つ。記憶装置１６は、条件付きアクセス装置１２に結合される出力部を持つ。他の受信システム１９は、条件付きアクセス装置１２及び記憶装置の組み合わせと同様の構成を任意の個数含み得る。

【００１７】

条件付きアクセス装置１２は、受信部１２０と、コンテンツ復号器１２２と、レンダリング装置１８と、セキュアデバイス１４（例えばスマートカード）とを含む。受信部１２０は、供給源１０及び記憶装置１６からの入力を受信し、コンテンツ復号器１２２に結合される暗号化されたコンテンツのための出力部と、セキュアデバイス１４に結合される暗号化制御メッセージ(ECM)及び暗号化管理メッセージ(EMM)のための出力部とを持つ（別々に示されているが、後者の出力部は実際には組み合わされて単一の出力部にされ得る）。セキュアデバイス１４は、復号器１２２の鍵入力部に結合される出力部を持つ。復号器１２２は、レンダリング装置１８に結合される解読されたコンテンツのための出力部を持つ。

【００１８】

セキュアデバイス１４は、解読ユニット１４０及び管理ユニット１４２を含み、随意に時間値記憶装置１４４を含む。解読ユニット１４０は、受信部のECMのための出力部に結合される入力部と、復号器１２２の鍵入力部に結合される出力部とを持つ。解読ユニット１４０はまた、管理ユニット１４２に結合されるタイムスタンプのための出力部も持つ。

管理ユニット１４２は、受信部１２０のEMMのための出力部に結合される入力部を持つ。更に、管理ユニット１４２は、随意の時間値記憶装置１４４に結合される入力部及び出力部を持つ。EMM及びECMのための別々の入力部が示されているが、当然、これらは、単一の入力部を介して供給され、セキュアデバイス１４において別々に処理されてもよい。

【００１９】

動作中、供給源１０は、暗号化されたメディア情報（例えば、ビデオ情報及び／又はオーディオ情報）の１つ以上のストリームを送信する。各ストリームは、暗号化されたコンテンツと、暗号化制御メッセージ(ECM)と、暗号化管理メッセージ(EMM)とを含む。これらの要素に対する帯域幅の必要量は大幅に異なる。即ち、コンテンツは、毎秒数メガビットの固定帯域幅を必要とし得るのに対して、ECMは、１キロビット未満しか必要としないかもしれず、例えば、毎分１回しか送信されない。EMMは、更に少ない頻度で、例えば毎時間１回送信される。暗号化制御メッセージは暗号化されたコンテンツを解読するための鍵を含む。これらの鍵自体もまた暗号化される。暗号化制御メッセージは、好ましくは、タイムスタンプも含む。これらのタイムスタンプは暗号化され得るが、これは必要ではない。これらのタイムスタンプは、正当と認められれば十分である、即ち、当然ながら供給源のみがタイムスタンプを供給しており、ECMが特定のタイムスタンプと関連付けられていることが確認され得るように符号化されれば十分である。

【００２０】

条件付きアクセス装置１２は、前記ストリームの少なくとも１つを受信する。受信部１２０は、このストリームからの暗号化されたコンテンツを復号器１２２に渡す。受信部１２０は、このストリームからのECM及びEMMをセキュアデバイス１４に渡す。セキュアデバイス１４は、ECMから鍵を解読し、条件付きで該鍵を復号器１２２に供給する。復号器１２２は、鍵を用いてコンテンツを解読し、解読されたコンテンツをレンダリング装置１８に供給する。レンダリング装置１８は、例えば、表示画面及び／又はスピーカを含み、コンテンツがシステムのユーザによって知覚され得るようにコンテンツをレンダリングする。

【００２１】

随意に、時間値記憶装置１４４が日付及び時刻を示す時間値を維持する。時間値記憶装置１４４における時間値は定期的に更新される。これは、セキュアデバイス１４中のクロック回路（図示せず）によって行なわれてもよく、又は例えばECMが受信されるたびに（又は所定の数のECMが受信されるたびに）管理ユニット１４２によって行なわれてもよい。

【００２２】

他の受信システム１９中に含まれるような条件付きアクセス装置１２などの任意の個数の条件付きアクセス装置は前記ストリームを受信し得る。

【００２３】

供給源１０は、セキュアデバイスがどの鍵をいつ復号器に供給してもよいのか指定するためにセキュアデバイス１４にEMMを送信する。例えばセキュアデバイス１４に固有のものである識別子をEMM中に組み込み、セキュアデバイス１４に対応する識別子を持つEMMしか処理しないようセキュアデバイスを構成することによって、EMMの各々は、原則的に、１つのセキュアデバイス１４にしか向けられない。（EMMは暗号化されたコンテンツのために鍵を供給する必要がないことから）EMMはより少ない頻度で送信される点、及びEMMは、例えばセキュアデバイス１４に鍵を供給する権利が付与されるタイプ及び時間のコンテンツを設定するための管理情報を含む点でEMMはECMと区別される。従って、EMMは、アクセスの条件を制御するのには必要であるが、アクセスを供給するのには直接的には必要ない。

【００２４】

セキュアデバイス１４は、該セキュアデバイス１４が復号器１２２に鍵を供給する権利を有するか否かをチェックする。鍵の少なくとも幾つかのための権利は時間に依存する。これ実施するために、管理ユニット１４２は、供給源１０から受信される権利付与情報を

利用し得る。単純な形態の時間依存権利付与においては、例えば、管理ユニット１４２は、EMMにおいて指定された時間値の範囲とタイムスタンプからの時間値を比較する。このようにして、例えば、鍵は、ユーザが当該期間に対して代金を支払っている期間中にのみ供給され得る。

【００２５】

図２は、本発明による権利付与時間範囲を示している。（一緒に「時刻」又は「t」と呼ばれる）日付及び時刻は水平方向にプロットされている。矢印は、現在の時刻Tc、即ち、供給源１０によってその時間にブロードキャストされるタイムスタンプの時間値を示している。開始時間２１と終了時間２２とを備える時間値の範囲２０であって、鍵を供給する権利がセキュアデバイス１４に付与される時間値の範囲２０が示されている。

【００２６】

図３は、前記時間範囲が現在の時刻Tcより前に終了する同様の権利付与範囲を示している。

【００２７】

一例として、図２はまた、記憶時間２８から始まり、現在の時刻Tcまで続く記憶時間間隔２６も示している。供給源１０から受信される情報が、記憶時間２８に記憶装置１６に記憶され、現在の時刻Tcにセキュアデバイス１４に対して再生される場合に、再生される情報中のECMからのタイムスタンプは、記憶時間２８に対応し、現在の時刻Tcには対応しない。それでも、タイムスタンプが、T1、T2によって指定されるTcを基準とする前記時間間隔内の時間値に対応する限り、管理ユニット１４２は、解読ユニット１４０がECMからの鍵を復号器１２２に供給することを可能にするであろう。

【００２８】

供給源１０は、過去に遡る権利付与時間範囲２０が使用されるためのものであることを示すコードを備えるEMMをセキュアデバイス１４に送ることによって範囲２０を指定する。それに応じて、管理ユニット１４２は、（例えば特定の開始時間及び終了時間の形態で、又は間接的に例えば時間範囲２０の継続期間及び開始点若しくは開始点だけという形で、又は管理ユニット１４２に記憶された所定の継続期間及び／若しくは期間を参照するコードを用いて）このEMMからの情報を記憶する。次いで、管理ユニット１４２がECMからのタイムスタンプを受信する場合に、管理ユニット１４２は、指定された範囲とこのタイムスタンプを比較する。タイムスタンプがこの範囲内である場合には、管理ユニット１４２は、解読ユニット１４０が解読された鍵を復号器１２２に供給することを可能にする。

【００２９】

実施例においては、前記範囲は、時間値記憶装置１４４において維持される現在の時刻Tcを基準として規定され得る。この場合には、前記範囲は、第１時間間隔の長さL1（例えば１日）だけ現在の時刻Tcに先立つ時間Tc-L1における開始点２１から、第２時刻の長さ（図２の例においては、L2は零よりわずかに大きい）だけ現在の時刻Tcに先立つ又は後続する時間Tc-L2における終了時間２２まで続く。この場合には、管理ユニット１４２は、例えば、タイムスタンプと現在の時刻との間の差がL1とL2との間であるか否かを計算して、タイムスタンプが現在の時刻Tcを基準とする指定範囲内であるか否かを決定する。タイムスタンプが前記範囲内である場合には、管理ユニット１４２は、解読ユニット１４０が解読された鍵を復号器１２２に供給することを可能にする。

【００３０】

このようにして、解読が可能にされるタイムスタンプのためのスライディングウィンドウが実現される。他の例においては、このようなスライディングウィンドウは、単一の受信契約の間時間が経過しただけセキュアデバイス１４において固定ウィンドウを更新するように定期的に新しいEMMを送信することによって実現され得る。

【００３１】

受信契約管理ユニット１１は、特定のタイプの時間間隔に対する受信料の支払いについての情報の受信に依存してEMMによって指定される時間範囲を選択する。受信契約管理ユニット１１は、例えば、支払い情報によって更新され、後に、EMMのコンテンツを制御す

るために照会される受信契約者情報のデータベースを備える適当にプログラムされた従来のコンピュータとして実施される。受信契約者が或る期間L1過去に遡る時間範囲に対して料金を支払っているという情報を受信契約管理ユニット１１が受信した場合には、受信契約管理ユニット１１は、或る期間記憶されている情報を復号するための鍵を復号器１２２に供給する権利をその受信契約者のセキュアデバイス１４に付与するEMMを供給源１０に送信させる。時間範囲の長さ及び該時間範囲のうちの過去に遡る範囲は両方とも支払われる料金に依存し得る。

【００３２】

受信契約管理ユニット１１は、複数の受信契約者の受信契約情報を管理する。解読が可能にされ得る時間値の範囲のうちの過去に遡る範囲は、各受信契約者に権利が付与される契約のタイプに依存して、様々な受信契約者に対して個々に設定され得る。このようにして、（例えば、EMMにおいて異なるIDを指定して、各EMMがIDに対応するセキュアデバイスによってしか処理されないようにすることによって）様々な受信契約者に向けられるEMMは、契約に依存して様々な過去に遡る範囲を指定し得る。

【００３３】

他の実施例においては、時間範囲２０が、現在の時刻Tcと無関係に、所定の開始時間２１に開始し、所定の終了時間２２に終了するよう選択され得る。受信契約管理ユニット１１が、受信契約者がこのような権利付与に対して代金を支払っていることを示す信号を受信する場合に、受信契約管理ユニット１１は、関連する受信契約者のセキュアデバイス１４にこの趣旨のEMMを送る。

【００３４】

このようにして、記憶装置１６に記憶された過去の情報を見たい受信契約者であって、そのための権利を持たない受信契約者は、情報が送信された時間（即ち、情報と関連付けられているECM中のタイムスタンプ）に基づいて記憶された情報を見る権利が受信契約者に付与されるよう指定するEMMを受信し得る。これは、EMMにおいて明確にその情報を特定することによって情報の或る部分を解読する権利を受信契約者に付与するのとは異なるであろう。このようにして、例えば、しばらくの間休暇中であったTV受信契約者に、個々の番組を指定する必要なしに休暇期間のTV番組を見るための権利が与えられ得る。

【００３５】

本発明が、情報ユニットのストリームを配信し、時間依存ベースでアクセスを供給するあらゆるシステムに適用されることは了解されるであろう。例えば、本発明は、図１に示されているような同じ接続部を介して暗号化された情報及び権利付与メッセージを送信するシステムに限定されない。同様に、ほんの一例としてECM及びEMMを用いる機構が示されているが、解読鍵を供給する他の方法も用いられ得る。

【図面の簡単な説明】

【００３６】

【図１】情報配信システムを示す。

【図２】権利付与時間範囲を示す。

【図３】他の権利付与時間範囲を示す。

【図１】

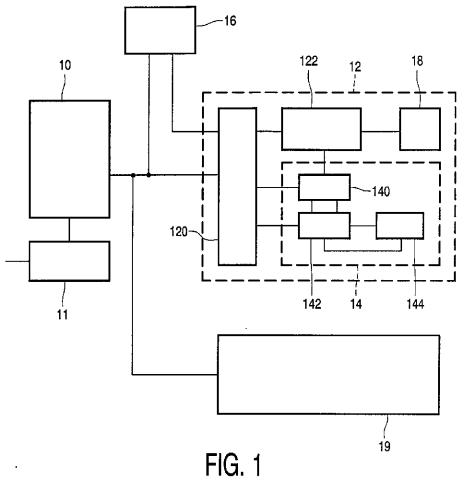


FIG. 1

【図２】

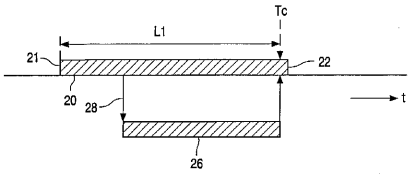


FIG. 2

【図３】

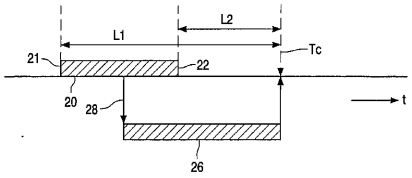


FIG. 3

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 02/05272

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N5/913 H04N7/16

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)
IPC 7 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.
A	WO 98 27732 A (SCIENTIFIC ATLANTA) 25 June 1998 (1998-06-25) cited in the application abstract	1,7,9,10
A	US 6 222 924 B1 (SALOM AUML KI ARI) 24 April 2001 (2001-04-24) column 2, line 44 -column 4, line 6	1,7,9,10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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
9 May 2003	16/05/2003

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	Dockhorn, H

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 02/05272

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9827732 A	25-06-1998	US 6005938 A	21-12-1999
		DE 69719803 D1	17-04-2003
		EP 0950319 A1	20-10-1999
		WO 9827732 A1	25-06-1998
		US 6105134 A	15-08-2000
		US 6157719 A	05-12-2000
		US 2003074565 A1	17-04-2003
		US 6424717 B1	23-07-2002
		US 6246767 B1	12-06-2001
		US 6252964 B1	26-06-2001
		US 2001001014 A1	10-05-2001
		US 2001046299 A1	29-11-2001
		US 2002044658 A1	18-04-2002
		US 2001053226 A1	20-12-2001
US 6222924 B1	24-04-2001	FI 960418 A	31-07-1997
		AU 1548297 A	22-08-1997
		DE 69720421 D1	08-05-2003
		EP 0878096 A1	18-11-1998
		WO 9728649 A1	07-08-1997
		JP 2000504169 T	04-04-2000

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,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,IE,IT,LU,MC,NL,PT,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,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(74)代理人 100122769
弁理士 笛田 秀仙
(72)発明者 レイクカエルト アルベルト エム エイ
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン ６
(72)発明者 ファン レインソエヴェル バルソロメウス ジェイ
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン ６

Ｆターム(参考) 5J104 AA01 AA16 EA01 EA04 EA15 EA16 EA22 JA03 MA05 NA02
NA35 NA37 NA40 PA05