

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第3962082号

(P3962082)

(45) 発行日 平成19年8月22日(2007.8.22)

(24) 登録日 平成19年5月25日(2007.5.25)

(51) Int. Cl.		F I			
HO 4 L	9/32	(2006.01)	HO 4 L	9/00	6 7 5 B
HO 4 L	9/16	(2006.01)	HO 4 L	9/00	6 4 3
HO 4 N	7/16	(2006.01)	HO 4 N	7/16	Z

請求項の数 9 (全 33 頁)

(21) 出願番号	特願2006-216465 (P2006-216465)	(73) 特許権者	502303843
(22) 出願日	平成18年8月9日(2006.8.9)		カナル プラス テクノロジーズ ソシエ
(62) 分割の表示	特願2001-573687 (P2001-573687)		テ アノニム
原出願日	平成13年1月11日(2001.1.11)		フランス国 エフ-75906 パリ セ
(65) 公開番号	特開2006-311620 (P2006-311620A)		デックス 15 プレイス ラオール ダ
(43) 公開日	平成18年11月9日(2006.11.9)	(74) 代理人	ウトリー 34
審査請求日	平成18年8月9日(2006.8.9)		100115864
(31) 優先権主張番号	00400912.2		弁理士 木越 力
(32) 優先日	平成12年4月3日(2000.4.3)	(74) 代理人	100118496
(33) 優先権主張国	欧州特許庁 (EP)		弁理士 青山 耕三
早期審査対象出願		(74) 代理人	100121175
			弁理士 石井 たかし
		(74) 代理人	100071755
			弁理士 斉藤 武彦

最終頁に続く

(54) 【発明の名称】 デジタル伝送システムで伝送されるデータの証明の方法及びその認証方法

(57) 【特許請求の範囲】

【請求項 1】

デジタル伝送システムで伝送されるデータを検証する方法であって、前記方法は、
デコーダが、前記データおよび前記データの少なくともいくつかに対して決定された複数の暗号化値を受信するステップであって、各々の暗号化値が、それぞれの暗号化アルゴリズムの鍵を使用して、同じデータに対して決定される様に構成された受信ステップと、
前記デコーダが、受信した暗号化値の数が、該デコーダに記憶された暗号化値の数を示す数値よりも小さくないことを検証するステップと、
前記デコーダが、それぞれの暗号化アルゴリズムの記憶鍵を使用して、各々の暗号化値を処理するステップと、
前記デコーダが、各々のその後に生じる値と前記データの少なくともいくつかと比較し、前記データの少なくともいくつかを検証するステップと、
を含む、前記方法。

【請求項 2】

前記受信したデータは、更に後続するデータの伝送に於ける暗号化値の数を示す数値を含む、請求項 1 に記載の方法。

【請求項 3】

前記方法は、更に、若し前記暗号化値の数が記憶された暗号化値の数を示す数値よりも小さい場合には、前記デコーダが前記データを拒否する工程をさらに含む、請求項 1 に記載の方法。

【請求項 4】

デコーダであって、

複数の鍵を記憶する様に構成された手段と、

データと、該データの少なくともいくつかに対して決定される複数の暗号化値とを含むデータファイルを受信する手段であって、各々の暗号化値が、それぞれの暗号化アルゴリズムの鍵を使用して、同一のデータに対して決定される様に構成されている、前記受信手段と、

前記データと共に送信される暗号化値の数を示す数値を記憶する手段と、

前記暗号化値の数が前記暗号化値の数を示す数値よりも小さくないことを検証する手段と、

10

前記それぞれの暗号化アルゴリズムについて記憶された鍵を使用して各々の暗号化値を処理する手段と、

各々のその後に生じる値を前記データの少なくともいくつかと比較し、前記データの少なくともいくつかを検証する手段と、

を備える、前記デコーダ。

【請求項 5】

前記受信手段は、後続して伝送されるデータにおいて暗号化値の数を示す数値を受信するように、更に構成される、請求項 4 に記載のデコーダ。

【請求項 6】

当該デコーダは、前記暗号化値の数が、記憶された暗号化値の数を示す数値よりも小さい場合には前記データを拒否する手段を更に含む、請求項 4 に記載のデコーダ。

20

【請求項 7】

デジタル伝送システムで伝送されるデータを認証する方法であって、当該方法は、伝送より前に、

データ認証装置が、前記データの少なくともいくつかに対する複数の暗号化値を決定するステップであって、各暗号化値がそれぞれの暗号化アルゴリズムの鍵を使用して同じデータに対して決定されるステップと、

前記データ認証装置が、後続するデータと共に伝送される暗号化値の数を示す数値を決定するステップと、

前記データ認証装置が、前記複数の暗号化値と、後続するデータと共に伝送される暗号化値の数を示す数値とを前記データと共に出力するステップと、

30

を備える、前記方法。

【請求項 8】

デジタル伝送システムで伝送されるデータを認証する装置であって、

前記データの少なくともいくつかに対する複数の暗号化値を決定する手段であって、各暗号化値が、それぞれの暗号化アルゴリズムの鍵を使用して同じデータに対して決定される、前記手段と、

後続するデータと共に伝送される暗号化値の数を示す数値を決定する手段と、

前記複数の暗号化値と、後続するデータと共に伝送される暗号化値の数を示す数値とを前記データと共に出力する手段と、

40

を含む、前記装置。

【請求項 9】

デコーダであって、

複数の鍵を格納する様に構成されている第 1 の記憶空間と、

データと、該データの少なくともいくつかに対して決定される複数の暗号化値であって、各々の暗号化値が、それぞれの暗号化アルゴリズムの鍵を使用して、少なくとも同一のデータに対して決定される様に構成されている暗号化値と、を含むデータファイルを受信する受信手段と、

データと共に伝送される暗号化値の数を表す数値を格納する様に構成されている第 2 の記憶空間と、

50

プロセッサであって、

前記暗号化値の数が、暗号化値の数を示す数値よりも小さくないことを検証する工程と

、
それぞれの暗号化アルゴリズムについての記憶された鍵を使用して、それぞれの暗号化
値を処理する工程と、

各々のその後に生じる値と前記データの少なくともいくつかと比較し、前記データの少
なくともいくつかを検証する工程と、

を実行する様に構成された、前記プロセッサと、

を備える、前記デコーダ。

【発明の詳細な説明】

10

【技術分野】

【0001】

本発明は、デジタル伝送システムで伝送されるデータの証明の方法及びその認証方法に関するものである。

【背景技術】

【0002】

デジタルデータの同報伝送は、スクランブルオーディオビジュアル情報が、通常衛星あるいは衛星／ケーブルリンクによって各々がその後見るための伝送番組を暗号解読できるデコーダを所有する多数の加入者に送信されるpay TVシステムの分野で周知である。地上デジタル放送システムも公知である。最近のシステムは、視聴覚データに加えてあるいは視聴覚データと同様に、デコーダあるいは接続PCのためのコンピュータプログラムあるいは対話型アプリケーションのような他のデータを伝送する放送リンクも使用した。

20

【0003】

アプリケーションの伝送に関する特定の問題は、いかなるこのようなデータの一貫性および発生源も検証する必要性にある。この種のデータは、いかなる対話型アプリケーション数も実行するのと同様にデコーダを再構成するために使用されてもよいので、受信データは完全であり、かつ公知の発生源から発生するものとして識別されることの両方であることが重要である。特に、不完全なデータのダウンロードに関係付けられる操作上の問題が、デコーダが第三者等による攻撃を受けやすくなる危険と同様に生じ得る。

【0004】

30

このようなデータの一貫性を検証することは、デコーダによって直接受信されたデータのパケットストリームの検証によって行われてもよい。伝送より前に、パケットは、一般的にはハッシングアルゴリズムをパケットのデータの少なくともいくつかに用いることによって署名される。生じるハッシュ値はパケットに記憶される。データパケットの受信の際に、デコーダは、同じハッシングアルゴリズムをデータに用い、受信データの一貫性を検証するためにデコーダによって計算されたハッシュ値を受信パケットに記憶されたハッシュ値と比較する。例えば、伝送の故障あるいは遮断の場合、計算ハッシュ値は、受信ハッシュ値と同じでない。次に、デコーダは、ダウンロードデータパケットの可能なエラーの存在のために変更され、間違ったデータパケットを再ロードする。

【0005】

40

メッセージダイジェストアルゴリズムMD5のような周知のハッシングアルゴリズムの使用に関連した問題は、ハッシュ値の計算が公に公知の一連の計算ステップに従って実行されるということであり、その結果、誰でもデータパケットのハッシュ値を計算できる。

【0006】

従って、デコーダによって受信されたデータパケットの発生源を検証できる。受信データがデコーダの演算データファイルを修正する場合、このことは特に重要であり得る。

【発明の開示】

【発明が解決しようとする課題】

【0007】

この問題を解決するために、データの少なくともいくつかに対するハッシュ値を計算す

50

るハッシングアルゴリズムを使用する代わりに、データパケットのシグネチャ値は、放送者にだけ公知である秘密鍵値を使用して計算されてもよい。この鍵は、データ暗号化規格、すなわちDESのアルゴリズムのような対称性鍵アルゴリズムを等価鍵を記憶するデコーダとともに使用して得ることができる。しかしながら、より便利なのは、公開鍵および私用鍵が数式の補数部を形成する、リベスト(Rivest)、シャミール(Shamir)およびアデルマン(Adleman)、あるいはRSAのアルゴリズムのような非対称性公開／私用鍵アルゴリズムを使用することによってもたすことができることである。

【0008】

データパケットを生成する責任のある放送者は、私用鍵を記憶し、私用鍵を使用してシグネチャ値を計算する。この公開鍵は、製造中公開鍵をデコーダメモリへハードコーディングすることによってデータを受信すべきであるデコーダに記憶される。データパケットの受信の際に、デコーダは、受信データを公開鍵アルゴリズムを受信シグネチャ値に用いる結果と比較することによって記憶された公開鍵を使用してシグネチャ値を検証する。

10

【0009】

このような安全システムにおいてさえ、私用鍵の値は、例えば不法に公然と配信することによって危険にさらされ得る。このような場合、放送者は、データパケットの無許可受信を防止するために等しい公開鍵の使用を迅速に取り消すことが必要になる。さらに、新しい公開／私用鍵対が使用されることも必要になる。したがって、放送会社は、合法ユーザのデコーダに記憶された公開鍵を新しい公開鍵と交換する必要がある。公開鍵の感度に 20
応じて、このことは、放送者がこれらのデコーダのメモリへの新しい公開鍵のハードコーディングするために製造者へのこれらのデコーダの高価で、煩わしい返却を計画することを必要とし得る。

【課題を解決するための手段】

【0010】

本発明の目的は、これらの問題および他の問題を解決しようとするものである。

本発明の第1の態様は、デジタル伝送システムで伝送されるデータを認証する方法を提供し、前記方法は、伝送より前に、データの少なくともいくつかに対する少なくとも2つの暗号化値を決定するステップであって、各暗号化値がそれぞれの暗号化アルゴリズムの鍵を使用して同じデータに対して決定されることと、前記少なくとも2つの暗号化値を前記データとともに出力するステップとを含む。

30

【0011】

本発明は、データが「出されるように」受信されることを保証するために新しい暗号化アルゴリズムで使用される鍵のような影響されやすいデータを安全に更新することが望ましい状態に特に応用できるが、これに限定されない。このようなセキュリティを行うために、データの少なくともいくつか、好ましくは多数、より好ましくは全てに対する少なくとも2つの暗号化値が決定される。各々の暗号化値は、それぞれの暗号化アルゴリズムの鍵を使用して決定される。鍵の1つが危険にさらされるようになった場合、「ハッカー」は、データを遮断し、データおよび危険にさらされた鍵を使用して計算された暗号化値の内容を変更でき得る。暗号化値を計算するために使用される鍵と等しい鍵を使用する暗号化値の検証の際に、データが破損されるようになったことを示す、等価鍵を使用する2つの値は同じでない。

40

【0012】

データおよび暗号化値は、好ましくは受信機／デコーダに伝送するために出力される。好ましくは、前記データおよび前記暗号化値は、受信機／デコーダによって受信され、この受信機／デコーダで、各暗号化値は、前記それぞれの暗号化アルゴリズムの鍵を使用して処理され、各々のその後生じる値は、データの前記少なくともいくつかと比較され、データの前記少なくともいくつかを認証する。このデータが破損されるようになった場合、受信機／デコーダは、データを無視するように選択できるので、危険にさらされるかあるいは破損された新しい鍵は、デコーダのメモリに記憶されない。好ましくは、その後に 50

生じる値の少なくとも1つがデータの前記少なくともいくつかとは異なる場合、前記受信データは、受信機／デコーダによって拒否される。

【発明を実施するための最良の形態】

【0013】

したがって、本発明は、デジタル伝送システムで伝送されるデータを認証する方法に及び、前記方法は、前記データおよびデータの少なくともいくつかに対して決定された少なくとも2つの暗号化値を受信するステップであって、各々の暗号化値がそれぞれの暗号化アルゴリズムの鍵を使用して決定されることと、複数の鍵を記憶するステップと、それぞれの暗号化アルゴリズムの記憶された鍵を使用して各々の暗号化値を処理するステップと、各々のその後に生じる値をデータの前記少なくともいくつかと比較し、データの前記少なくともいくつかを認証するステップとを含む。

10

【0014】

好ましくは、各アルゴリズムは非対称である。好ましい実施形態では各々の暗号化値は暗号化アルゴリズムの私用鍵で計算されたデジタルシグネチャにそれぞれ対応し、各シグネチャは前記暗号化アルゴリズムの公開鍵を使用し処理する。

【0015】

好ましくは、この方法は、各々のシグネチャとともに、このシグネチャを処理するために使用される公開鍵の識別子を出力するステップを含む。これによって、受信機／デコーダは、このシグネチャを検証するために使用される鍵を容易に識別することを可能にできる。

20

【0016】

好ましくは、このデータは鍵を含む。好ましい実施形態では、データは、データを処理するための暗号化アルゴリズムの公開鍵を含む少なくとも1つのデジタル認証、好ましくは少なくとも1つのデジタルルート認証を含む。この少なくとも1つのデジタル認証は、この認証に含まれる公開鍵の暗号化アルゴリズムの私用鍵を使用して計算されたデジタルシグネチャを含んでもよい。したがって、デジタル認証は、デコーダのメモリの新しい認証のハードコーディングのために製造者に戻されねばならないデコーダなしにデコーダに安全に伝送できる。

【0017】

好ましくは、前記データは、取り消された公開鍵の識別子を含む。この識別子は、前記取り消された公開鍵を含む、デジタル認証、好ましくはデジタルルート認証の識別子を含んでもよい。このデータは、複数の前記識別子を含んでもよく、各々の識別子は、それぞれの取り消された公開鍵を識別する。したがって、取り消された鍵の識別子のリストは、デコーダに安全に伝送できる。

30

【0018】

前記の方法によって、危険にさらされた鍵の数がデータとともに記憶される暗号化値の数よりも小さいとすれば、データは安全に更新できる。したがって、前記データおよび前記少なくとも2つの暗号化値は、その後に生成されたデータファイルに記憶される暗号化値の最小数の指示を含んでもよいデータファイルに構成されてもよい。鍵が危険にさらされたようになるべきであるので、暗号化値の最小数が危険にさらされた鍵の数よりも大きいままである場合、これによって、暗号化値の最小数は、変更でき、例えば増加できる。

40

【0019】

好ましくは、前記データファイルに記憶された暗号化値の数を前記最小数と比較し、前記データファイルに記憶された暗号化値の数が前記最小数よりも小さい場合、前記データファイルを拒否する受信機／デコーダによって受信される。

【0020】

このデータファイルはデータモジュールに伝送されてもよい。前記モジュールのデータの少なくともいくつかに対するモジュール暗号化値は、送信機暗号化アルゴリズムの鍵を使用して計算し、前記データモジュールに記憶できる。このデータモジュールは、送信機暗号化アルゴリズムの鍵を使用して前記モジュール暗号化値を処理し、その後に生じる値

50

を前記モジュールのデータの前記少なくともいくつかと比較し、前記モジュールのデータの前記少なくともいくつかを認証する受信機／デコーダによって受信されてもよい。

【0021】

前記モジュールのデータの少なくともいくつかに対する暗号化値は、送信機暗号化アルゴリズムの私用鍵を使用して計算され、前記送信機暗号化アルゴリズムの公開鍵を使用して処理可能であるデジタルシグネチャに対応し得る。

【0022】

デジタル伝送システムは、テレビあるいはオーディオシステムのようなデジタル放送システムであってもよい。

本発明は、デジタル伝送システムで伝送されるデータを認証する装置も提供し、前記装置は、データの少なくともいくつかに対する少なくとも2つの暗号化値を決定する手段であって、各々の暗号化値がそれぞれの暗号化アルゴリズムの鍵を使用して同じデータに決定されることと、前記データとともに前記少なくとも2つの暗号化値を出力する手段とを備えている。

10

【0023】

本発明は、デジタル伝送システムで伝送されるデータを認証するシステムも提供し、前記システムは前述されるような装置を含む。このシステムは、好ましくは、前記データおよび前記暗号化値を受信する手段と、前記それぞれの暗号化アルゴリズムの鍵を使用して各々の暗号化値を処理する手段と、各々のその後に生じる値をデータの前記少なくともいくつかと比較し、データの前記少なくともいくつかを認証する手段とを含む受信機／デコーダをさらに含む。

20

【0024】

本発明は、データおよびデータの少なくともいくつかに対して決定される少なくとも2つの暗号化値を含むデータファイルを受信する手段であって、各々の暗号化値が、それぞれの暗号化アルゴリズムの鍵を使用して決定されることと、複数の鍵を記憶する手段と、前記それぞれの暗号化アルゴリズムの記憶された鍵を使用して各々の暗号化値を処理する手段と、各々のその後に生じる値をデータの前記少なくともいくつかと比較し、データの前記少なくともいくつかを認証する手段とを含む受信機／デコーダに及ぶ。

【0025】

本発明は、デジタル伝送システムで伝送されるデータを認証するシステムにも及び、前記システムは、前述されたような装置および前述されたような受信機／デコーダを含む。

30

【0026】

本発明は、さらにデータおよびデータの少なくともいくつかに対して決定された少なくとも2つの暗号化値を含む信号に及び、各々の暗号化値は、それぞれの暗号化アルゴリズムの鍵を使用して決定される。

【0027】

本発明は、さらに実質的に添付図面を参照してここに説明されるようなデータを認証する方法、あるいは装置、受信機／デコーダ、あるいは信号に及ぶ。

ここで使用される用語「受信機／デコーダ」あるいは「デコーダ」は、いくつかの他の手段によって放送されてもよいしあるいは伝送されてもよい、符号化信号あるいは非符号化信号のいずれか、例えばテレビおよび／またはラジオ信号を受信する受信機を意味してもよい。この用語は、受信信号を復号化するデコーダも意味してもよい。このような受信機／デコーダの実施形態は、例えば、物理的に別個の受信機との組み合わせで機能を果たすデコーダ、あるいはウェブブラウザのようなあるいはビデオレコーダあるいはテレビのような他の装置と一体化された付加機能を含むデコーダのような「セットトップボックス」で受信信号を復号化する受信機と一体であるデコーダを含んでもよい。

40

【0028】

ここで使用されるように、用語「デジタル伝送システム」は、例えば、主に視聴覚データあるいはマルチメディアデータを伝送あるいは放送するいかなる伝送システムも含む。

【0029】

50

本発明は、放送デジタルテレビシステムに特に用いることができるが、本発明は、マルチメディアインターネット用途のための固定電気通信網、閉回路テレビ等にも応用できてよい。

【0030】

ここで使用されるように、用語「デジタルテレビシステム」は、例えば、任意の衛星システム、地上システム、ケーブルシステムおよび他のシステムを含む。

本発明で使用し、私用／公開鍵を生成するための適当なアルゴリズムは、RSA、フィアット-シャミール、あるいはディフィー-ヘルマンを含んでもよく、適当な対称鍵アルゴリズムは、例えばDES形アルゴリズムを含んでもよい。しかしながら、前後関係を考慮して不可欠でない限りあるいは別段の指定がない限り、対称アルゴリズムに関連した鍵と公開／私用アルゴリズムに関連した鍵との間の一般的な区別は全然行われな

10

【0031】

用語「スクランブル」および「暗号化」および「制御ワード」および「鍵」は、用語を明瞭にするためにテキストのいろいろな部分で使用された。しかしながら、「スクランブルデータ」と「暗号化データ」、「制御ワード」と「鍵」との基本的区別は、全然行われるべきでないことが分かる。

【0032】

さらに、用語「暗号化」および「署名」や「暗号解読」および「検証」は、用語を明瞭にするためにテキストのいろいろな部分で使用された。しかしながら、「暗号化データ」と「署名データ」および「暗号解読データ」および「検証データ」との基本的区別は、全

20

【0033】

同様に、用語「等価鍵」は、第1の記載された鍵によって暗号化されたデータを暗号解読、あるいはその逆をするために構成された鍵を示すために使用される。

本発明の方法態様に関連する前述の機能は、装置態様にも応用でき、あるいはその逆でも用いることができる。

【0034】

次に、添付図面を参照して本発明の好ましい実施形態だけが例として説明される。

本発明によるデジタルテレビシステム1の概略1は、図1に示される。本発明は、圧縮デジタル信号を伝送するために公知のMP EG-2圧縮システムを使用する多くの従来のデジタルテレビシステム2を含む。より詳細には、放送局のMP EG-2圧縮器3は、デジタル信号ストリーム（一般的には、ビデオ信号のストリーム）を受信する。この圧縮器3は、リンク装置5によってマルチプレクサおよびスクランブラ4に接続される。

30

【0035】

マルチプレクサ4は、複数の他の入力信号を受信し、トランスポートストリームを組み立て、もちろん通信リンクを含むいろいろの形をとることができるリンク結合装置7を介して圧縮デジタル信号を放送局の送信機6に送信する。送信機6は、アップリンク8を介して電磁信号を電子的に処理される衛星トランスポンダ9の方へ送信し、概念上のダウンリンク10を介して従来はエンドユーザによって所有されるかあるいは賃貸される皿の形の地上受信機12に放送する。受信機12によって受信された信号は、ユーザエンドによって所有されるかあるいは賃貸され、エンドユーザのテレビ受像機14に接続された統合受信機／デコーダ13に送信される。この受信機／デコーダ13は、圧縮MP EG-2信号をテレビ受像機14のためのテレビ信号に復号化する。

40

【0036】

地上放送、ケーブル伝送、結合衛星／ケーブルリンク、電話網等のようなデータの伝送のための他のトランスポートチャネルは、もちろん可能である。

マルチチャネルシステムでは、マルチプレクサ4は、多数の並列発生源から受信されたオーディオおよびビデオ情報を処理し、送信機6と対話し、対応するチャネル数に沿って情報を放送する。オーディオビジュアル情報に加えて、デジタルデータのメッセージあるいはアプリケーションもしくはは任意の他の種類のデジタルデータは、送信されたデジタル

50

オーディオおよびビデオ情報とインタレースされたこれらのチャンネルのいくつかあるいは全部に導入される。このような場合、例えば、D S M - C C (デジタル記憶メディアコマンドおよびコントロール) フォーマットソフトウェアファイルおよびメッセージの形のデジタルデータのストリームは、圧縮器 3 によって M P E G フォーマットに圧縮され、パケット化される。ソフトウェアモジュールのダウンロードは、下記により詳細に説明される。

【0037】

条件付アクセスシステム 15 は、マルチプレクサ 4 および受信機／デコーダ 13 に接続され、一部が放送局にあり、一部がデコーダにある。このシステムによって、エンドユーザは、1 つあるいはそれ以上の放送供給者からデジタルテレビ放送にアクセスできる。市販の売り物 (すなわち、放送供給者によって宣伝された 1 つあるいはいくつかのテレビ番組) に関するメッセージを解読できるスマートカードは、受信機／デコーダ 13 に挿入できる。デコーダ 13 およびスマートカードを使用すると、エンドユーザは、加入モードあるいはペイ・パー・ビューモードのいずれかで市販の売り物を購入できる。実際には、デコーダは、例えば同時暗号あるいは複数暗号設計の多重アクセス制御システムを処理するように構成されてもよい。

10

【0038】

前述されたように、システムによって放送された番組は、マルチプレクサ 4 でスクランブルされ、所与の伝送に加えられる条件および暗号化鍵は、アクセス制御システム 15 によって決定される。このようにスクランブルされたデータの伝送は、ペイ T V システムの分野で周知である。一般的には、スクランブルデータは、データを暗号解読する制御ワードとともに伝送され、制御ワードそのものは、いわゆる利用鍵によって暗号化され、暗号化形式で伝送される。

20

【0039】

スクランブルデータおよび暗号化制御ワードは、次にデコーダに挿入されたスマートカードに記憶された利用鍵の均等物へのアクセス権を有するデコーダ 13 によって受信され、暗号化制御ワードを暗号解読し、その後、伝送データを暗号解読する。支払った加入者は、例えば、伝送を見ることができるよう暗号化制御ワードを暗号解読するのに必要な利用鍵を放送月 E M M (資格管理メッセージ) で受信する。視聴覚テレビ番組を暗号解読する際のその使用に加えて、同じ利用鍵が、前述されるようなソフトウェアモジュールのような他のデータの検証で使用するために生成され、送信されてもよい。

30

【0040】

マルチプレクサ 4 および受信機／デコーダ 13 にも接続され、さらに一部が放送局にあり、一部がデコーダにある対話システム 16 によって、エンドユーザは、モデム逆方向チャンネル 17 を介していろいろなアプリケーションと対話できる。このモデム逆方向チャンネルも、条件付アクセスシステム 15 で使用される通信のために使用されてもよい。対話システムは、例えば、視聴者は、直ちに放送局と通信し、特定の試合を見て、アプリケーション等をダウンロードするための許可を要求することができる。

【0041】

(受信機／デコーダの物理的要素)

40

図 2 を参照すると、本発明で使用されるように構成される受信機／デコーダ 13 あるいはセットトップボックスの物理的要素は、次に簡単に説明される。この図に示された要素は、機能ブロックによって説明される。

【0042】

デコーダ 13 は、関連メモリ要素を含み、かつ直列インタフェース 21、並列インタフェース 22、および (図 1 のモデム逆方向チャンネル 17 に接続される) モデムから入力データを受信するように構成される中央プロセッサ 20 を含む。

【0043】

デコーダは、さらに制御装置 26 を介して赤外線遠隔制御装置 25 からおよびデコーダの正面パネル上のスイッチコンタクト 24 から入力を受信するように構成される。このデ

50

コーダは、銀行スマートカードおよび加入スマートカード 29、30 のそれぞれを読み取るように構成される 2 つのスマートカード読み取り器 27、28 も持つ。入力も、赤外線キーボード（図示せず）を介して受信されてもよい。加入スマートカード読み取り器 28 は、挿入加入カード 30 および条件付アクセス装置 29 と係合し、必要な制御ワードを多重分離装置／暗号解読器 30 に供給し、暗号化放送信号は暗号解読できる。デコーダは、装置 30 によってフィルタリングされ、多重分離される前に衛星伝送を受信し、復調する従来のチューナ 31 および復調器 32 も含む。

【0044】

デコーダ内のデータの処理は、通常、中央プロセッサ 20 によって処理される。中央プロセッサのソフトウェアアーキテクチャは、デコーダのハードウェア構成要素で実行される下部レベルオペレーティングシステムと対話する仮想機械に対応する。

10

【0045】

（伝送データの packets 構造）

次に、図 3 および 4 を参照して、送信機からデコーダに送信される放送 MPEG トランスポートストリーム内のデータの packets 構造が説明される。理解されるように、この説明は MPEG 規格で使用される作表フォーマットに集中するが、同じ原理は、同様に他の packets 化データストリームフォーマットに用いる。

【0046】

特に、図 3 を参照すると、MPEG ビットストリームは、0 の packets 識別 (PID) を有する番組アクセステーブル (PAT) 40 を含む。PAT は、多数の番組の番組マップテーブル (PMT) 41 の PID の関連を含む。各 PMT は、この番組のためのオーディオ MPEG テーブル 42 およびビデオ MPEG テーブル 43 のストリームの PPID の関連を含む。ゼロの PID を有する packets、すなわち、番組アクセステーブル 40 は、全 MPEG アクセスのためのエン트리ポイントを与える。

20

【0047】

アプリケーションおよびそのためのデータをダウンロードするために、2 つの新しいストリーム形式が規定され、関連する PMT は、アプリケーション MPEG テーブル 44（あるいはこれらの一部）およびデータ MPEG テーブル 45（あるいはこれらの一部）のストリームの PID の関連も含む。実際は、実行可能なアプリケーションソフトウェアおよびこのようなソフトウェアによって処理するためのデータのための別個のストリーム形式を規定することはいくつかの場合便利であり得るが、これは重要でない。他の実現では、データおよび実行可能なコードは、記載されるような PMT を介してアクセスされる単一ストリームに組み立てできる。

30

【0048】

図 4 を参照すると、例えばストリーム 44 内のアプリケーションをダウンロードするために、アプリケーション 46 は、各々が MPEG テーブルによって形成されるモジュール 47 に分割される。これらのテーブルのいくつかは単一部分を含むが、他のものは複数の部分 48 によって構成されてもよい。典型的なセクション 48 は、1 バイトのテーブル ID (「TID」) 50、テーブルのこのセクションのセクション番号 51、このテーブルの全セクション数 52 および 2 バイトの TID 拡張関連 53 を含むヘッダを有する。各セクションは、データ部 54 および CRC 55 も有する。特定のテーブル 47 の場合、このテーブル 47 を構成するセクション 48 の全ては、同じ TID 50 および同じ TID 拡張部 53 を有する。特定のアプリケーション 46 の場合、このアプリケーション 46 を構成するテーブルの全ては、同じ TID 50 であるが、異なるそれぞれの TID 拡張部を有する。

40

【0049】

各々のアプリケーション 46 の場合、単一 MPEG テーブルは、ディレトリテーブル 56 として使用される。このディレトリテーブル 56 は、そのヘッダにおいて、アプリケーションを構成する他のテーブル 47 と同じ TID を有する。しかしながら、ディレトリテーブルは、ID 目的のためにゼロの所定の TID 拡張部を有し、この事実のために

50

単一テーブルだけはディレクトリの情報に対して必要である。他のテーブル47の全ては、通常非ゼロT I D拡張部を有し、多数の関連セクション48で構成される。ディレクトリテーブルのヘッダは、ダウンロードされるアプリケーションのバージョン番号も含む。

【0050】

戻って図3を参照すると、PAT40、PMT41、およびアプリケーション・データストリーム成分44、45は、周期的に伝送される。伝送される各アプリケーションは、それぞれの所定のT I Dを有する。アプリケーションをダウンロードするために、適切なT I DおよびゼロのT I D拡張部を有するMP EGテーブルは、受信機／デコーダにダウンロードされる。これは、必要とされるアプリケーションのためのディレクトリテーブルである。このディレクトリのデータは、次にデコーダによって処理され、必要とされるアプリケーションを構成するテーブルのT I D拡張部を決定する。その後、ディレクトリテーブルと同じT I Dおよびディレクトリから決定されるT I D拡張部を有するいかなる必要とされるテーブルもダウンロードできる。

10

【0051】

このデコーダは、そのいかなる更新のためのディレクトリテーブルも検査するように構成される。これは、例えば、30秒あるいは1分あるいは5分毎に周期的に再度ディレクトリをダウンロードし、予めダウンロードされるディレクトリテーブルのバージョン番号を比較することによって行われてもよい。新しくダウンロードされたバージョン番号が後のバージョン番号である場合、前のディレクトリテーブルに関連したテーブルは削除され、新しいバージョンに関連したテーブルは、ダウンロードされ、集められる。

20

【0052】

代替の装置では、入ってくるビットストリームは、アプリケーションのT I D、ゼロのT I D拡張部および目下ダウンロードされたディレクトリのバージョン番号よりも1つ大きいバージョン番号のためにセットされる値とともにT I D、T I D拡張部およびバージョン番号に対応するマスクを使用してフィルタリングされる。したがって、バージョン番号の増加が検出され、一旦検出されると、前述されるように、ディレクトリはダウンロードされ、アプリケーションは更新される。アプリケーションが終了されるべきである場合、次のバージョン番号を有する空のディレクトリは、ディレクトリに列挙された少しのモジュールもないことを除いて伝送される。このような空のディレクトリの受信に応じて、デコーダ2020は、アプリケーションを削除するようにプログラムされる。

30

【0053】

実際には、デコーダでアプリケーションを実行するソフトウェアおよびコンピュータプログラムは、特に前述されるような衛星リンクを介して受信されるデータストリームに、デコーダの一部のいずれかを介してであるが、直列ポート、スマートカードリンク等も介して導入されてもよい。このようなソフトウェアは、ネットブラウザ、クイズアプリケーション、番組案内等のようなデコーダ内の対話型アプリケーションを実行するために使用される高レベルアプリケーションを含んでもよい。ソフトウェアも、例えば「パッチ」等によってデコーダソフトウェアの作動構成を変えるようにダウンロードされてもよい。

【0054】

アプリケーションも、デコーダを介してダウンロードされ、デコーダに接続されたPC等に送信されてもよい。このような場合、デコーダは、最終的には接続装置で実行されるソフトウェアのための通信ルータの役目を果たす。このルーティング機能に加えて、デコーダも、PCに経路指定する前にMP EGパケット化データを例えばDSM-CCプロトコル（下記を参照）に従って構成されたコンピュータファイルソフトウェアに変換する機能を果たしてもよい。

40

【0055】

（データファイルのデータの構成）

図5は、DSM-CC U-U（ユーザ対ユーザ）データファイル60のセット、集められたアプリケーション46に構成され、一連のMP EGテーブル47内にカプセル化されるようなデータ間の関係を示す。この関係は国際特許出願番号第99/49614に記

50

載されており、その内容は下記に参照される。

【0056】

伝送より前に、データファイルは、アプリケーション46に集められ、その後、MP EG圧縮器によって、前述されるようにMP EGパケットストリームに固有なヘッダ49を含み、かつテーブルID、バージョン番号等を含むMP EGテーブルあるいはモジュール47にパケット化される。理解されるように、データファイル61に構成されるデータと最終的なMP EGテーブル47との間に一定の関係が全然ない。デコーダによる受信およびフィルタリング後、パケットヘッダ49は、廃棄され、アプリケーション46は、テーブル47のペイロードから再構成される。

【0057】

データファイルのためのDSM-CCフォーマットは、特にマルチメディアネットワークで使用するために適合され、図6に示されるように、クライアントユーザ70、サーバユーザ71とネットワーク資源マネージャ72との間の通信のための一連のメッセージフォーマットおよびセッションコマンドを規定する規格である。ネットワーク資源マネージャ72は、ネットワーク内の資源の属性を管理するように作動する論理エンティティとみなされてもよい。

【0058】

クライアントとサーバとの間の通信は、一連のセッションによって作動可能な状態にされ、第1の一連のメッセージは、通信のためのクライアントおよび／またはサーバを構成するためにユーザ（クライアント70あるいはサーバ71）とネットワークマネージャ72との間で交換される。このようなメッセージは、いわゆるDSM-CC U-N（ユーザ対ネットワーク）に従ってフォーマット化される。このプロトコルのサブセットは、特にデータを放送ダウンロードするために規定された。

【0059】

一旦通信リンクが確立されると、メッセージは、DSM-CC U-Uプロトコルに従ってクライアント70とサーバ71との間でその後交換される。この種の一連のメッセージは、図5のデータファイル60に対応する。DSM-CC U-Uメッセージの場合、データは、BIOP（Broadcast InterOrb Protocol）に従ってグループ化される。

【0060】

各メッセージあるいはオブジェクト61は、ヘッダ62と、サブヘッダ63と、データそのものを含むペイロード64とを含む。BIOPプロトコルに従って、ヘッダ62は、とりわけ、メッセージおよびBIOPバージョンの形式の指示を含むが、サブヘッダは、システム設計者によって規定されるオブジェクトおよび他の情報の形式を示す。

【0061】

DSM-CC U-Uファイルのペイロード内のデータオブジェクト64は、通常3つの形式、すなわちディレクトリオブジェクト、ファイルオブジェクトおよびストリームオブジェクト、の中の1つとして規定できる。ディレクトリオブジェクトは、実際のアプリケーションデータを含む一連の関連ファイルオブジェクトを関連付けるために使用されるルートディレクトリあるいはサブディレクトリを規定する。

【0062】

ストリームオブジェクトは、一時の関係がデータファイルに含まれるデータとMP EGパケットストリームそのものとの間に確立できるために使用されてもよい。これは、例えば、データファイルに含まれ、かつデコーダによって受信され、処理される基本ビデオあるいはオーディオストリームと同期されるように設計される対話形アプリケーションの場合、使用されてもよい。前述されるように、特にMP EGパケット化データとデータファイルとの間に全然直接の相関が有り得ない。

【0063】

MP EGテーブルと違って、単一ディレクトリがテーブルのセットを単一レベルの階層のみと関連付ける場合、データファイル60は、かなりより複雑な階層のように構成され

10

20

30

40

50

てもよい。P Cあるいはサーバに記憶されるファイルのように、主ディレクトリあるいはルートディレクトリは、順に第2のレベルのデータファイルを参照する1つあるいはそれ以上のサブディレクトリを参照してもよい。（データファイルのセットのためのファイル構造）

【0064】

図7を参照すると、データファイルのセットのためのファイル構造の例が示されている。75に示されるルートディレクトリDIRA0は、サブディレクトリA1のグループをオブジェクトファイル77に関連付ける。明瞭にするために、サブディレクトリA4と関連するオブジェクトファイルF1、F2等の単一グループだけが示されている。実際には、多数のオブジェクトファイルのグループは、サブディレクトリA1からA4の各々によ

10

【0065】

各々のディレクトリおよびサブディレクトリ内で、認証ステップのセットは、このディレクトリに結合されるファイルのために導入される。ルートディレクトリ75を参照すると、サブヘッダ63は、ハッシュアルゴリズムを76と示されたサブディレクトリファイルA1からA4に記憶されたデータのいくつかあるいは全てに用いることによって得られたハッシュ値を含む。使用されるハッシングは、例えば、メッセージダイジェストアルゴリズムMD5のような任意の公知の形式のものであってもよい。

【0066】

1つの実現では、このアルゴリズムは、各々の関連ファイルあるいはサブディレクトリに個別に適用され、各サブディレクトリ76のためのハッシュ値のリストは、伝送より前にルートディレクトリ75に記憶されてもよい。しかしながら、このような解決策は、各々のサブディレクトリを検証することに関する分解能をチェックする度合いの増加を可能にするが、この解決策は、対応するシグネチャを計算するためにデコーダのために必要である処理時間に関してかなり役に立たないことが有り得る。したがって、ディレクトリ79のサブヘッダ63は、好ましくは、MD5ハッシングアルゴリズムを結合されたサブヘッダおよびサブディレクトリ76のペイロード部63、64に用いることによって計算され、すなわちヘッダ62がない累積ハッシュ値79を含む。特に、サブディレクトリ76内に含まれ、ファイルオブジェクト77の層を示すハッシュ値82は、このハッシング計算に含まれる。

20

30

【0067】

図7に示されたサブディレクトリA4の場合、このサブディレクトリそれ自体は、77に示されるオブジェクトF1～Fnのセットを示す。この場合、累積ハッシュ値82は、オブジェクトファイル77の結合内容のために生成される。この値は、ハッシュ値79を生じるハッシング処理に含まれる。したがって、順にディレクトリ75のハッシュ値79を変えるサブディレクトリ76のハッシュ値82を変えないでオブジェクトファイル77のいずれかを変えることができない。

【0068】

この場合、結合されたハッシュ値は、ディレクトリに示されたサブディレクトリの全てに対して計算される。このハッシュ値は、そこからデータがとられるサブディレクトリのグループの識別子とともに記憶される。他の実施形態では、一連の結合されるかあるいは個別のハッシュ値および対応する識別子は、ディレクトリのサブヘッダに記憶されてもよい。

40

【0069】

例えば、ルートディレクトリとも関連するが、異なるデータのセットあるいは実行可能なコードに関する第2のサブディレクトリのセットも、一緒にグループ化され、累積ハッシュ値は、計算され、サブヘッダルートディレクトリに記憶されたこれらのサブディレクトリのために計算されてもよい。単一ディレクトリに関連した単一ハッシュ値は、同様にルートディレクトリのサブヘッダに記憶されてもよい。

グループあるいは個別のデータファイルの認証は、もちろん、ルートディレクトリ（あ

50

るいは、実際に任意の他のファイル)が無効あるいは未ハッシュのデータファイルも示すことを防止しなくて、このようなファイルの確認がないことは、このファイルとの任意の動作を考慮する必要がある。この点では、例えば、システムオブジェクトを認証することは必要であり得ない。

【0070】

この場合のハッシング関数の使用によって、主にデコーダは、ダウンロードデータファイルの一貫性あるいはダウンロードデータファイルを完備していることを検証できる。例えば、伝送における故障あるいは遮断の場合、受信された従属ファイルの累積ハッシングアルゴリズムの演算は、ルートディレクトリに記憶されたこれらのファイルに対するハッシュ値と同じ結果を得られる。次に、デコーダは、ダウンロードデータの可能なエラーがあることに変更され、誤ったデータファイルを再ロードする。

10

【0071】

(ルートディレクトリのためのシグネチャ値)

高められたセキュリティの場合、ルートディレクトリ75のためのシグネチャ値が計算される。本実施形態では、リベスト(Rivest)、シャミール(Shamir)およびアデルマン(Adleman)あるいはRSAアルゴリズムが使用され、データファイルを生成する責任を負うべき放送会社は、私用鍵値を所有し、公開鍵は、デコーダによって保持される。一方、秘密鍵は、データ暗号規格あるいはDESアルゴリズムのような対称性鍵アルゴリズムによって得られる鍵に対応し得る。

【0072】

20

図7に示されるように、ルートディレクトリ75は、放送会社の私用鍵を使用して生成される計算されたシグネチャ値81とともに検証工程で使用される公開鍵をデコーダのために識別する放送会社識別子80を含む。この場合、シグネチャ値81は、放送会社によって保持される私用鍵を好ましくはペイロードデータ64および/または累積ハッシュ値79を含むディレクトリ75内のデータのいくつかあるいは全てに用いることによって生成される。次に、このデコーダは、放送会社識別子80によって識別される対応する公開鍵を使用してこのシグネチャ値81を検証できる。

【0073】

本例では、ディレクトリ75のデータは、暗号化されなくて、この私用鍵は、公開鍵によって検証できるシグネチャ値を生じるために単に使用できる。代替実施形態では、ディレクトリの内容のいくつかあるいは全ては、私用鍵によって暗号化され、その後、対応する鍵によって暗号解読されてもよい。

30

【0074】

どちらかの場合でも、秘密鍵の使用による暗号化コードのシグネチャ値あるいはブロックの生成によって、デコーダは、ディレクトリ75の一貫性および発生源、および密接な関係によってこのルートディレクトリによって参照されるファイルの一貫性および発生源を検証できる。参照ファイルのための累積ハッシュ値は、シグネチャ81の計算に含まれるので、これが検証工程で検出されない限りこれらの値を変更できない。各ハッシュ値は通常所与のデータのセットに固有であるので、したがってその固有のハッシュ値、それによってディレクトリの生じるシグネチャ値を変えないで従属ハッシュファイルのいずれかの内容を変えることができない。

40

【0075】

理解されるように、多数の変更は、特に各工程でハッシュされるかあるいは署名されるデータ量を減らすことを可能にし得る。特に、下部レベルデータファイルを検証するために使用されるディレクトリあるいはサブディレクトリのシグネチャあるいはハッシュ値の場合、ディレクトリシグネチャあるいはハッシュ値は、下部レベルハッシュ値だけを使用し、他のデータだけを使用しないで生成されてもよい。

【0076】

例えば、A0ディレクトリ75の結合ハッシュ値79は、76に示されるA1-A4サブディレクトリの各々の結合ハッシュ値82、83を使用して生成されてもよい。これら

50

の値は、丁度サブディレクトリのペイロードのデータと同様に独自であるので、結合ハッシュ値 79 は、なお当のサブディレクトリに固有である。さらに、ハッシュ値 82 はなお計算で使用されるので、オブジェクトファイルおよびディレクトリファイル 77、78 の下部レベルの一貫性がなお推測される。

【0077】

(放送会社デジタル認証)

図 8 を参照すると、公開鍵 91 および放送会社識別子 80 は、好ましくは、製造中デコーダのメモリにハードコード化される周知の国際標準化機構 (ISO) X.509 の形のデジタル認証でデコーダのユーザに供給される。このような認証は、通常認証局 (CA) と呼ばれる信用された第三者によってデコーダの製造者に配信される。このような認証の使用は、ワールドワイドウェブ (WWW) を介するクレジットカードトランザクションを保護するネットスケープ通信によって開発され、標準化された安全ソケットレイヤー (SSL) 安全トランスポートプロトコルにより主により広く受け入れるようになる。

【0078】

公開鍵 91 および放送会社識別子 80 と同様に、放送会社に関連したデジタル認証、すなわち、放送会社認証 90 は、以下を含む。

放送会社認証 90 のバージョン番号 92 ;

放送会社認証 90 の連続番号 93 ;

放送会社認証 90 を配信した CA の CA 識別子 94 ;

認証が使用されることを意図されている時間の開始および終了を示す放送会社認証 90 の有効期間 95 ;

放送会社認証 90 のシグネチャ値 96。

【0079】

前述から分かるように、放送会社認証は、2つの異なる識別子、すなわち認証の分配者の ID 94 に対応する第 1 の「発行者名」識別子および公開鍵 91 を識別する識別子 80 に対応する第 2 の「主題名」識別子を含む。

【0080】

CA は、CA の私用鍵、すなわち CA 私用鍵を放送会社認証内のデータの少なくともいくつかあるいは全てに用いることによって放送会社認証 90 のシグネチャ値 96 を計算する。次に、デコーダは、CA 識別子 94 によって識別される対応する CA 公開鍵 101 を使用してシグネチャを処理することによってこのシグネチャ値 96 を検証し、認証の内容が CA によってシグネチャに続いて修正されなかったことを判定する。

デコーダは、異なるそれぞれの放送会社に対する複数のこのような認証を記憶してもよい。

【0081】

(認証局デジタル認証)

さらに図 8 を参照すると、対応する CA 公開鍵 101 および CA 識別子 94 は、製造中デコーダでもハードコード化される CA 認証 100 のデコーダのユーザに供給される。CA 認証 100 は、以下を含む。

CA 認証 100 のバージョン番号 102 ;

CA 認証 100 の連続番号 103 ;

CA 認証 100 を配信した欧州電気通信標準化機構 (ETSI) のようなルート認証局 (RCA) の RCA 識別子 104 ;

CA 認証 100 の妥当性期間 105 ;

CA 認証 100 のシグネチャ値 106。

【0083】

前述から分かるように、CA 認証は、2つの異なる識別子、すなわち認証の分配者の識別子 104 に対応する第 1 の「発行者名」識別子および公開鍵 101 を識別する識別子 94 に対応する第 2 の「主題名」識別子を含む。

【0084】

10

20

30

40

50

RCAは、RCAの私用鍵、すなわちRCA私用鍵をCA認証内のデータの少なくともいくつかあるいは全てに用いることによってCA認証100のシグネチャ値106を計算する。次に、デコーダは、RCA識別子104によって識別される対応するRCA公開鍵111を使用して認証を処理することによってこのシグネチャ値96を検証し、認証の内容がRCAによってシグネチャに続いて修正されなかったことを判定する。

【0085】

デコーダは、異なるそれぞれのCAに対する複数のこのような認証を記憶してもよい。

【0086】

(RCAデジタル認証)

対応するRCA公開鍵111およびRCA識別子104は、製造中にデコーダのメモリでもハードコード化され、RCA、すなわちルート認証110のデコーダのユーザに供給される。各デコーダは、一般的には2つあるいはそれ以上のルート認証（root certificate）のセットを含む。各ルート認証110は、以下も含む。

ルート認証110のバージョン番号112；

ルート認証110の連続番号113；

ルート認証110の妥当性期間114；

ルート認証110のシグネチャ値115。

前述から分かるように、ルート認証は、単一の識別子、すなわち認証の配信者の識別子104だけを含む。この識別子104は公開鍵111も含む。したがって、ルート認証は、発行者名が主題名と同じである認証として規定されてもよい。

【0087】

ルート認証は、放送会社認証90-C A認証100-ルート認証110の連鎖の最終認証であるので、ルート認証は、自動署名され、すなわち、シグネチャ値は、公開鍵111と等価の私用鍵を使用して計算される。したがって、ルート認証の内容が公に利用できるようにならないことに関心がある。

【0088】

もちろん、RCAは、放送会社認証をデコーダの製造者に直接供給することができ、その場合、放送会社認証は、RCA識別子111を含み、RCA私用鍵を使用して署名される。

【0089】

(認証取り消しリスト)

放送会社認証90およびCAのいずれかは、例えば認証に記憶された公開鍵に対応する私用鍵が危険にさらされるようになる場合、それで指定された妥当性期間の満了より前に例えば削除によって取り消されてもよい。このような取り消しは、取り消される認証の連続番号92、102のリストを含む認証取り消しリスト（CRL）のデコーダへの伝送によって行うことができる。取り消しの際に、認証は、好ましくは、デコーダのメモリからの認証の削除によって実行できないようになり、それによって危険にさらされた私用鍵を使用して署名される任意の不許可の可能性のある悪意のあるデータパケットのダウンロードを防止する。

【0090】

CRLは、CAあるいはRCAのいずれかによって放送会社に配信される。そして放送会社はCRLをデコーダに伝送するが、モデム逆方向チャンネル17、あるいはMP EGトランスポートストリームにCRLを含めて放送することのいずれかによってCRLを伝送する。放送会社が、送信機からデコーダに送信されるトランスポートストリームの全てにCRLを挿入することは重要でない。デコーダによって同調される可能性が非常に高いトランスポートストリームに放送会社がCRLを挿入すれば十分である。CRLは、例えば、データファイルとして送信機からデコーダへ放送されるデータファイルのセットのルートディレクトリ75あるいはサブディレクトリ76に挿入されてもよい。

【0091】

図9を参照すると、CRL120は、一般的には、以下を含む。

C R L 1 2 0 を配信した C A あるいは R C A の 識別子 9 4 あるいは 1 0 4 ;
C R L 1 2 0 が発行された日付 1 2 2 ;
次の C R L の発行が予想される日付 1 2 4 ;
各々の取り消された認証に対して、この認証の取り消しの時間および日付を含む、取り消された認証の連続番号のリスト 1 2 5 ;
C R L 1 2 0 を配信した C A あるいは R C A の私用鍵を使用して計算された C R L の シグネチャ値 1 2 6。

【 0 0 9 2 】

C R L の受信の際に、デコーダは、その C R L 1 2 0 が発行された日付 1 2 2 を、予め受信した C R L によって通知された C R L 1 2 0 の発行が予想される日付 1 2 4 と比較する。新しく受信された C R L の日付 1 2 2 が C R L の 発行が予想される日付 1 2 4 よりも後でない場合、新しく受信された C R L は無視される。

10

【 0 0 9 3 】

新しく受信された C R L の日付 1 2 2 が、C R L の発行が予想される日付 1 2 4 よりも後である場合、C R L のシグネチャは、C R L に含まれる識別子 9 4 あるいは 1 0 4 を使用して識別されるように、C A の発行者の公開鍵を使用して検証される。

【 0 0 9 4 】

C R L の一貫性がそのように検証される場合、C R L は、次の C R L が出されることが予想される日付 1 2 4 を固定メモリに記憶し、取り消された認証の連続番号のリスト 1 2 5 を記憶するように日付 1 2 4 を加えるために処理される。取り消された認証の受信リスト 1 2 5 は、デコーダの固定メモリにも記憶される。性能の理由のために、C R L 1 2 0 がデコーダのメモリにキャッシュされるのが好ましい。デコーダのキャッシュメモリが C R L 1 2 0 を樹枝状に記憶することも好ましく、R C A の C R L は、「ツリー」の上部およびこの R C A がツリーの底部にある認証を配信する C A の C R L にある。

20

【 0 0 9 5 】

放送会社認証 9 0 の取り消しの場合、例えば、放送会社の私用鍵が危険にさらされるようになる場合、この放送会社に対する認証局は、放送会社認証 9 0 の連続番号 9 3 をその C R L 1 2 0 に加える。認証局は、その後、新しい C R L 1 2 0 を放送会社に配信する。その配信先は、放送のために放送会社認証 9 0 を配信するすべての放送会社である。デコーダが新しい C R L 1 2 0 をダウンロードするや否や、例えば、放送会社のチャンネルで早送りする際に、C R L キャッシュは、更新され、C R L 1 2 0 のリスト 1 2 5 でそのように識別されたいかなる認証の取り消しも行われる。

30

【 0 0 9 6 】

交換される放送会社認証 9 0 は、認証局によって生成され、ファイルのディレクトリ 7 5 あるいは 7 6 のユーザに放送する。交換放送会社認証は、とりわけ、新しい公開鍵 9 1 と、更新バージョン番号 9 2 と、更新妥当性期間 9 5 と、C A の私用鍵を使用して計算された新しいシグネチャ値 9 6 とを含む。放送会社識別子 8 0 および C A 識別子 9 4 は変更されないままである。交換される放送会社認証 9 0 の受信の際に、デコーダは、C A 識別子 9 4 によって識別された C A 認証に含まれる対応する C A 公開鍵を使用して、交換される放送会社認証 9 0 を処理することによって、その認証を検証する。

40

【 0 0 9 7 】

C A 認証 1 0 0 の取り消しの際に、この C A の C R L は、デコーダのメモリから取り除かれる。したがって、例えば、この C A の C R L のサイズがデコーダのキャッシュメモリに記憶するためにあまりに大きくなる場合、C A 認証 1 0 0 を任意に取り消すことは望ましいことで有り得る。この場合、C A 認証 1 0 0 をこの C A に配信する R C A は、この C A 認証 1 0 0 の連続番号をその C R L に追加する。ルート認証局は、その後、R C A が C A 認証を配信する C A が放送するための放送会社認証を順に配信する放送会社の全てに新しい C R L を配信する。デコーダが新しい C R L をダウンロードするや否や、例えば、放送会社のチャンネルで早送りする際に、C R L キャッシュは更新され、C R L 1 2 0 のリスト 1 2 5 にそのように識別された C A 認証の取り消しが行われる。

50

【0098】

認証局のCA認証100の取り消しの際に、この認証局のための新しいCA認証をデコーダに記憶させ、その上、この認証局が認証を配信する放送会社の全てに対して放送会社認証90を交換する必要がある。それは、この認証局のための私用鍵対はもはや有効でないで、認証局の、異なるか更新された私用鍵を使用して署名された新しい放送会社認証90が必要とされるからである。交換されるCA認証100は、ルート認証局110によって生成され、ファイルのディレクトリ75あるいは76のユーザに放送される。交換される放送会社認証と同様に、交換されるCA認証は、とりわけ、新しいCA公開鍵101と、更新バージョン番号102と、更新妥当性期間105と、RCAの私用鍵を使用して計算された新しいシグネチャ値106とを含む。CA識別子94およびRCA識別子104は変更されないままである。交換されるCA認証100の受信の際に、デコーダは、RCA識別子104によって識別されたRCA認証100に含まれる対応するRCA公開鍵を使用してCA認証100を処理することによって認証を検証する。

10

【0099】

(ルート認証管理メッセージ)

ルート認証局のRCA認証110の取り消しの際に、取り消されたRCA認証を新しいRCAと交換する必要がある。前述されるように、RCA認証は自動署名されるので、CRLへRCA認証を含めることは、ハッカーがCRLを署名するために使用される私用鍵を知っている場合、ハッカーは認証を持つことができるので望ましくない。したがって、例えば、RCA認証が旧式になったかあるいは取り消されるようになった場合、これまで

20

【0100】

この問題を解決するために、ルート認証管理メッセージ(RCMM)は、放送会社によってデコーダに放送するためにルート認証局によって生成される。下記により詳細に説明されるように、CRLと同様に、RCMMは、旧式になったかあるいはリスト125に識別されたこれらの認証のための1つあるいはそれ以上の交換ルート認証とともに、各々の取り消されたルート認証に対してこの認証の取り消しのための時間および日付を含む、取り消されるルート認証の連続番号のリスト125を含む。

【0101】

理解されるように、RCMMの秘密にかかわる内容(新しいルート認証)に関して、放送会社に「出されるような」デコーダによって受信されることを保証すること、すなわちRCMMの内容が配信と受信との間で交換されないことを保証することは、重要である。RCMMが、RCMMがアドレスされる誰かにデコーダによってだけアクセスできることを保証することも重要である。

30

【0102】

セキュリティを高めるために、CRLと違って、RCMMは、その中に含まれるデータの少なくともいくつか、好ましくは全てに対する少なくとも2つのシグネチャ値を含む。各々のシグネチャ値は、公開鍵/私用鍵対の私用鍵のようなそれぞれの暗号化アルゴリズムの鍵を使用して計算される。

【0103】

RCMMがルート認証局(RCA)によって出され、新しいルート認証110を含む場合、RCMMは、少なくとも2つのシグネチャ値を含む。各々のシグネチャ値は、例えば、RCAが認証を供給する認証局のそれぞれの私用鍵を使用して計算される(ただし、デコーダが等しい鍵を記憶するいかなる鍵も選択されてもよい)。これらの認証局の中の1つに未知であり、その私用鍵が危険にさらされるようになる場合、「ハッカー」は放送会社の放送を遮断することが可能であり得る、ハッカーが放送会社および認証局の両方の私用鍵を知っている場合、ハッカーは、RCMMの内容および認証局の私用鍵を使用して計算されたRCMMのシグネチャ値を変える。しかしながら、この鍵は危険にさらされているようにならないために、ハッカーは、他の認証局の私用鍵を使用して計算されたシグネチャ値を変えることができない。したがって、2つの認証局の公開鍵を使用してデコーダ

40

50

によるシグネチャの検証の際に、それぞれの公開鍵を使用してデコーダによって計算された2つの値は同じでない。したがって、デコーダは、RCMMの内容の一貫性の欠如のために変えられ、RCMMの処理を拒否し、またはその他RCMMの処理を続けない。

【0104】

したがって、もし危険にさらされた認証数がRCMMに含まれたシグネチャ数よりも小さいとすれば、ルート認証は安全に更新できる。したがって、RCMMのシグネチャ数は、RCMMを配信するルート認証局によって決定された変数である。

【0105】

次に、RCMMのフォーマットは、図を参照してより詳細に示されている。

RCMM130は、RCMM130を配信したRCAの一貫性132；

10

RCMM130が発行した日付134；

その後のRCMMが含むシグネチャ値の数136；

1つあるいはそれ以上の更新されるかあるいはデコーダに記憶される交換ルート認証を含むフィールド138；

【0106】

各々の取り消されたルート認証に対してこの認証の取り消しの時間および日付を含む、取り消されたルート認証の連続番号のリスト140；および各々が、このシグネチャフィールドに含まれたシグネチャ値を検証するために使用される公開鍵を含む、デコーダに記憶された認証の識別子144；および識別子144によって識別される認証に含まれる公開鍵に等しい私用鍵を使用して計算されたRCMMのシグネチャ値146を含む少なくとも2つのシグネチャフィールド142を含む。

20

【0107】

シグネチャフィールド数142は、予め受信されたRCMMに通知されるようなシグネチャフィールド数136に等しいかあるいはそれよりも大となるべきである。

モデム逆方向チャンネルは容易に切り離してもよいしあるいは単に存在しなくてもよいので、RCMMはMP EGトランスポートストリームを介して伝送されることが好ましい。RCMMが、デコーダによってダウンロードされることを保証するために放送会社によってデータファイルとしてルートディレクトリ75に挿入されることも好ましい。

【0108】

(ルート認証管理メッセージの処理および生成)

30

次に、デコーダによるRCMMの受信および処理は、図11を参照して説明される。

RCMMの受信の際に、ステップ200では、デコーダは、予めRCMMが出されたRCMM130が出された日付134を比較する。新しい受信されたRCMMの日付134が前のRCMMが出された日付よりも後でない場合、RCMMは拒否される。

【0109】

新しく受信されたRCMMの日付134が前のRCMMの受信の日付よりも後である場合、予め受信されたRCMMによって通知されるように、新しく受信されたRCMMが含むべきであるシグネチャ値の数136は、ステップ202で新しく受信されたRCMMで実際に含まれたシグネチャ値の数と比較される。新しく受信されたRCMMに含まれたシグネチャの数が予想よりも低い場合、RCMMが拒否される。これは、RCMMが危険にさらされていない私用鍵／公開鍵対に関連したシグネチャを取り除くハッカーの結果として特に処理されることを防止する。

40

【0110】

新しく受信されたRCMMに含まれたシグネチャの数が予想されたシグネチャの数に等しいかあるいはそれよりも大きい場合、ステップ204で、RCMMに含まれた各々のシグネチャ値146は、このシグネチャ値と同じシグネチャフィールド142に含まれる識別子144によって識別された公開鍵を使用して検証される。ステップ206では、デコーダは、公開鍵を使用して計算された値の少なくとも1つが異なる公開鍵を使用して計算された他の値のいずれかと異なるかどうかを決定する。少なくとも1つの計算された値が他の計算された値の少なくとも1つと異なる場合、RCMMは拒否される。

50

【0111】

R C M Mの一貫性がステップ206で証明される場合、R C M Mは、ステップ208で処理され、デコーダの固定メモリに取り消されたルート認証の連続番号のリスト140を記憶するので、これらの認証は、ステップ212で、デコーダのメモリから削除され、フィールド138に含まれたルート認証あるいは各ルート認証をデコーダの固定メモリに記憶し、ステップ212でR C M Mの日付134を固定メモリに記憶してもよい。ルート認証局の認証が削除される場合、この局によって出される任意のC R Lも削除される。

【0112】

R C M Mに含まれたデータの固定メモリの一貫性が、デコーダがR C M Mメッセージの処理中スイッチオフされる場合、保持されることが好ましい。したがって、電力が実際にR C M M処理中スイッチオフされる場合、デコーダに記憶される予め処理されたR C M Mに関連したリスト140は、あたかも新しく受信されたR C M Mメッセージが全然処理されなかったかのように保持される。

【0113】

前述されるように、ルート認証局(R C A)は、一般的には各デコーダに記憶された少なくとも2つのR C A認証、すなわちR C 0およびR C 1を有する。これらの認証の1つ、例えばR C 0が危険にさらされるようになる場合、R C 0に記憶された公開鍵の等価私用鍵を使用して署名されたデコーダに記憶された全C A認証を交換し、新しいR C A認証R C 2を生成し、R C 0を交換する必要がある。

【0114】

図12を参照すると、これらのC A認証を交換するために、最初にステップ300では取り消されるC A認証の連続番号を識別する適切なC R LメッセージがR C Aによって出される。第二に、ステップ302では、危険にさらされていない認証R C 1の私用鍵を使用して署名され交換C A認証は、デコーダに放送するために放送会社に出される。

【0115】

次に、交換C A認証は、危険にさらされたR C A認証R C 0を削除し、この認証を新しいR C A認証R C 2と交換するまでである。ステップ304では、R C Aは、新しい公開鍵／私用鍵対を生成し、認証R C 2に新しい公開鍵を挿入し、新しい私用鍵を使用して認証を署名する。

【0116】

ステップ306では、R C Aは、フィールド138では、認証R C 2およびリスト140ではR C 0の連続番号を含むR C M Mを生成する。このR C M Mは、ステップ308では、デコーダに伝送するために放送会社に配信され、危険にさらされた認証R C 0を削除し、これを新しい認証R C 2と交換する。

【0117】

R C A認証R C 1およびR C 2は、その後新しいデコーダのメモリにハードコーディングするためにデコーダ製造者に供給される。

本発明は例として単に前述去れ、詳細の修正は本発明の範囲内に行うことができることが分かる。

【0118】

例えば、R C M Mは、新しいR C A認証110に加えて、新しいC A認証100および／または新しい放送会社認証90を含んでもよく、リスト140は、C A認証および／または取り消されるべきである放送会社認証の識別子を含んでもよい。これは、R C Aによる別個のC R Lメッセージの生成が不要にされることを可能にすることができる。

説明で開示された各々の特徴、および（適切である場合）特許請求の範囲および図面は、独立してあるいは任意の適切な組み合わせで提供されてもよい。

【図面の簡単な説明】

【0119】

【図1】図1は本発明と併用するためのデジタルテレビシステムの概略図を示す。

【図2】図2は図1のシステムのデコーダの構成を示す。

10

20

30

40

50

【図 3】図 3 は M P E G 放送トランスポートシステム内の多数の構成要素の構成を示す。

【図 4】図 4 は多数の M P E G テーブルへのソフトウェアアプリケーションの分割を示す。

。

【図 5】図 5 は D E S - C C データファイルと最終的に発生された M P E G テーブルとの関係を示す。

【図 6】図 6 は D E S - C C の前後関係で規定されるようなクライアント、サーバ、ネットワークマネージャ関係を示す。

【図 7】図 7 は認証ディレクトリ、サブディレクトリおよびファイルオブジェクトを示す。

。

【図 8】図 8 は放送認証、認証局認証およびルート認証局認証のフォーマットを示す。

10

【図 9】図 9 は認証取消リストのフォーマットを示す。

【図 10】図 10 はルート認証管理メッセージ (R C M M) のフォーマットを示す。

【図 11】図 11 はデコーダによる受信の際に R C M M の処理に含まれるステップを示す。

。

【図 12】図 12 は本発明の動作を説明するフローチャートである。

【符号の説明】

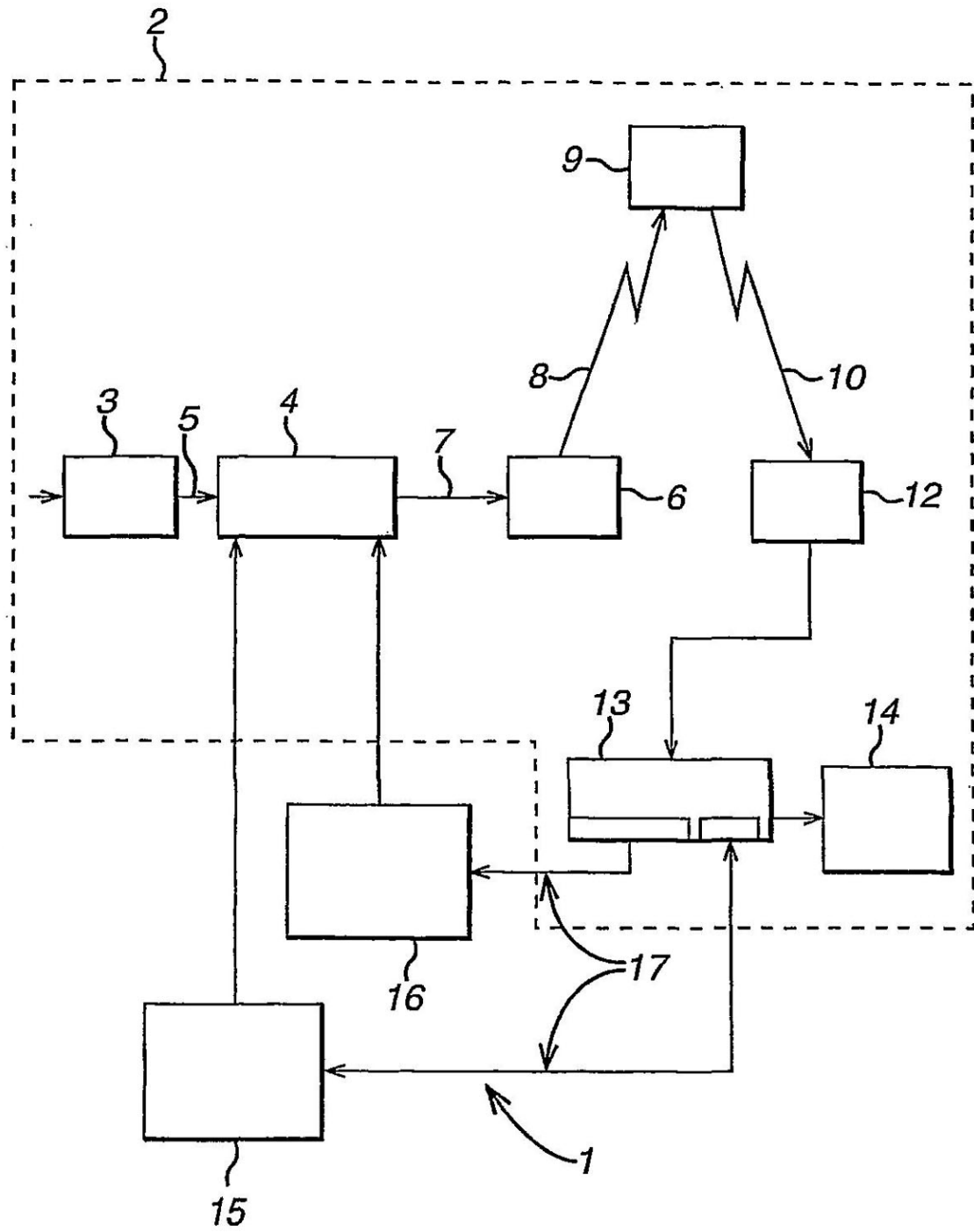
【 0 1 2 0 】

- 1 デジタルテレビシステム
- 2 従来のデジタルテレビシステム
- 3 圧縮器
- 4 スクランブラ、マルチプレクサ
- 5 リンク装置
- 6 送信機
- 7 リンク結合装置
- 8 アップリンク
- 9 衛星トランスポンダ
- 10 ダウンリンク
- 12 受信機
- 13 統合受信機／デコーダ
- 14 テレビ受像機
- 15 条件付きアクセスシステム
- 16 対話システム
- 17 モデム逆方向チャネル

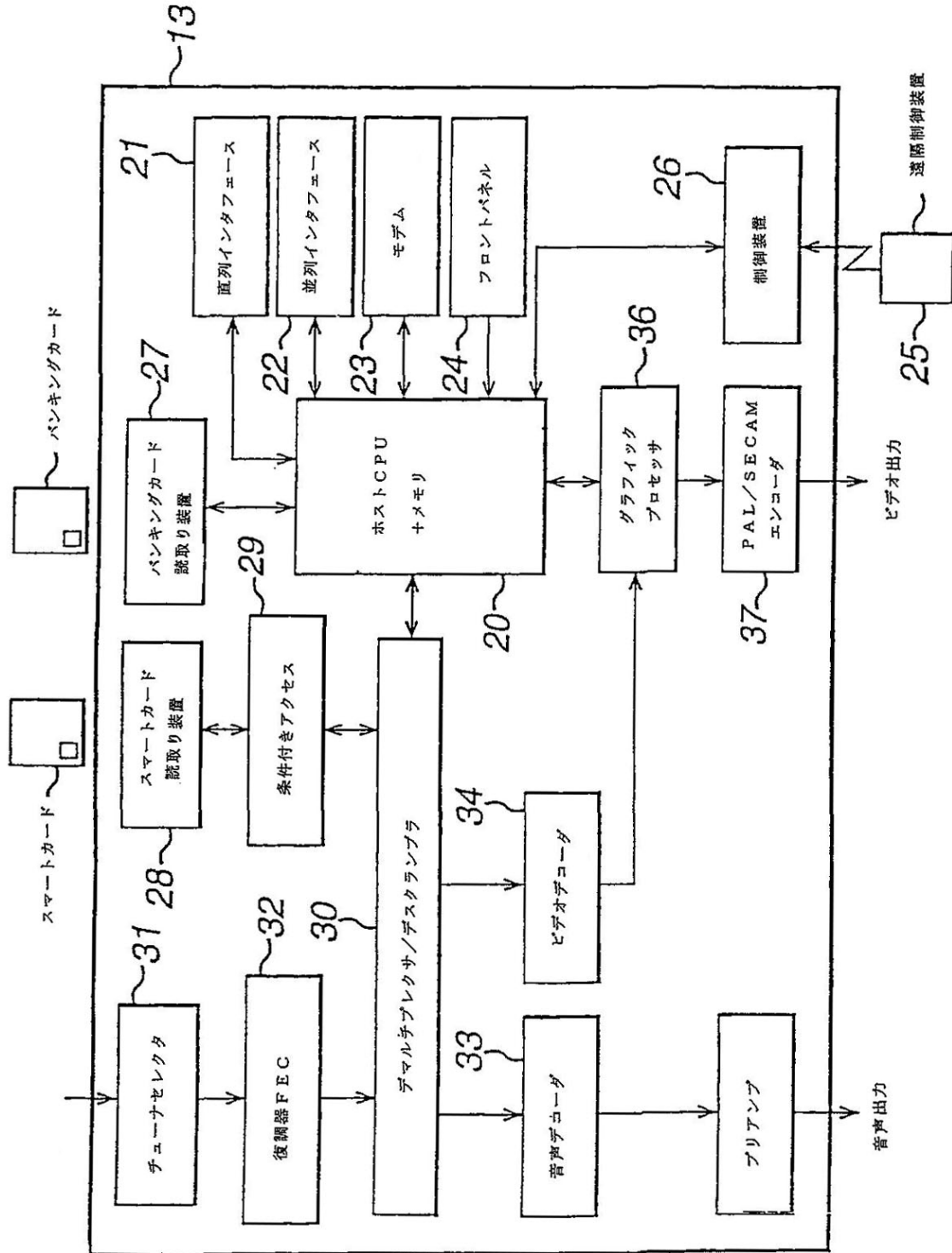
20

30

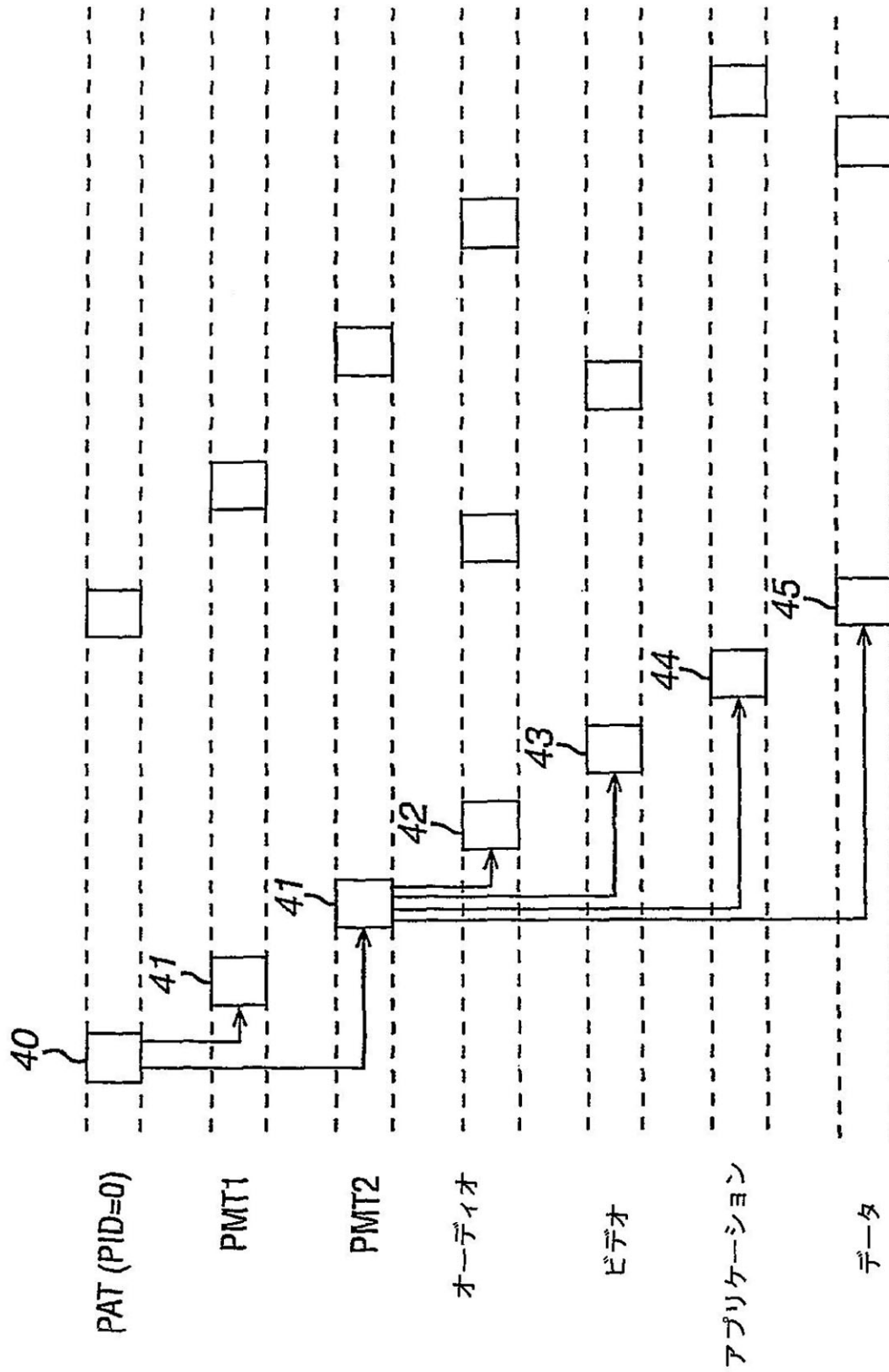
【図 1】



【 図 2 】



【図 3】

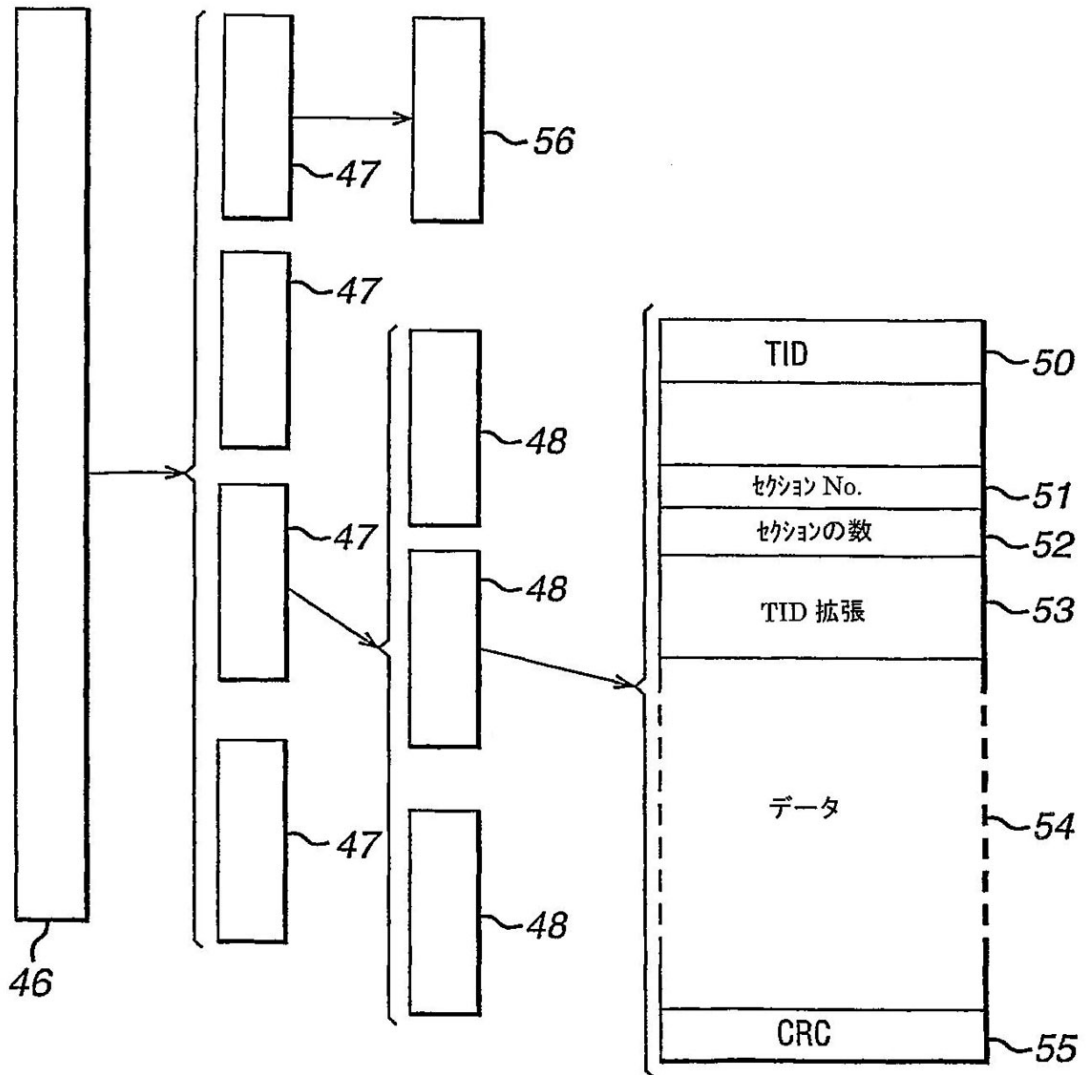


【図 4】

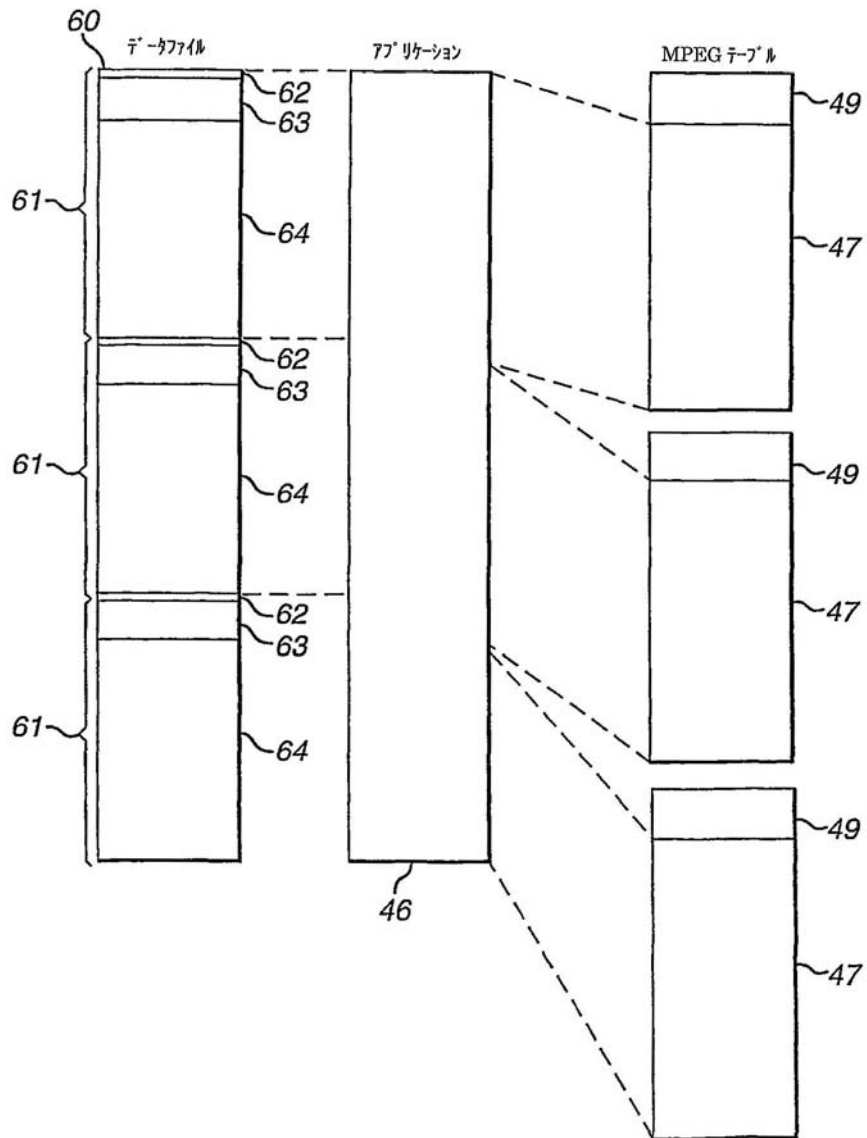
アプリケーション

モジュール
テーブル

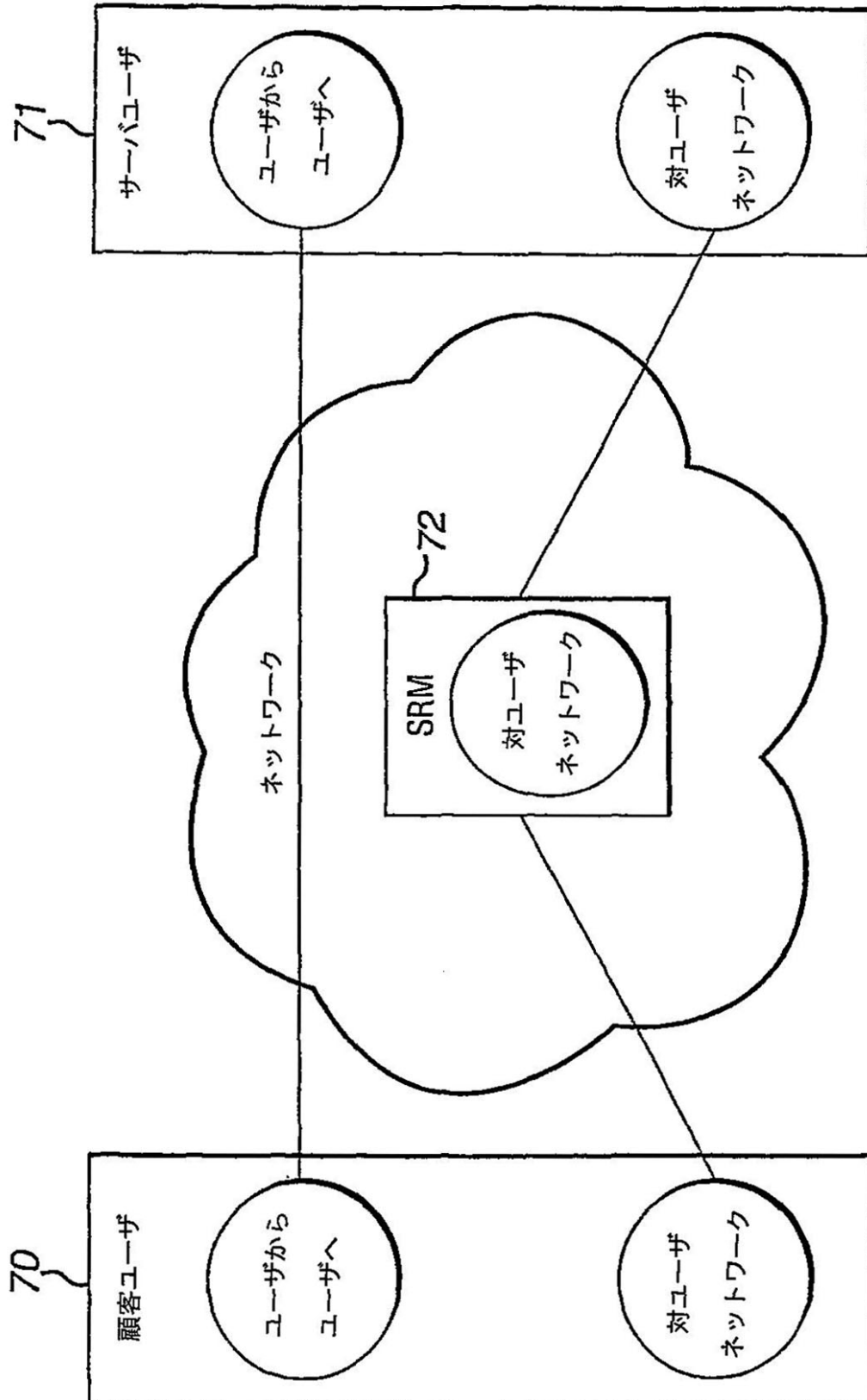
セクション



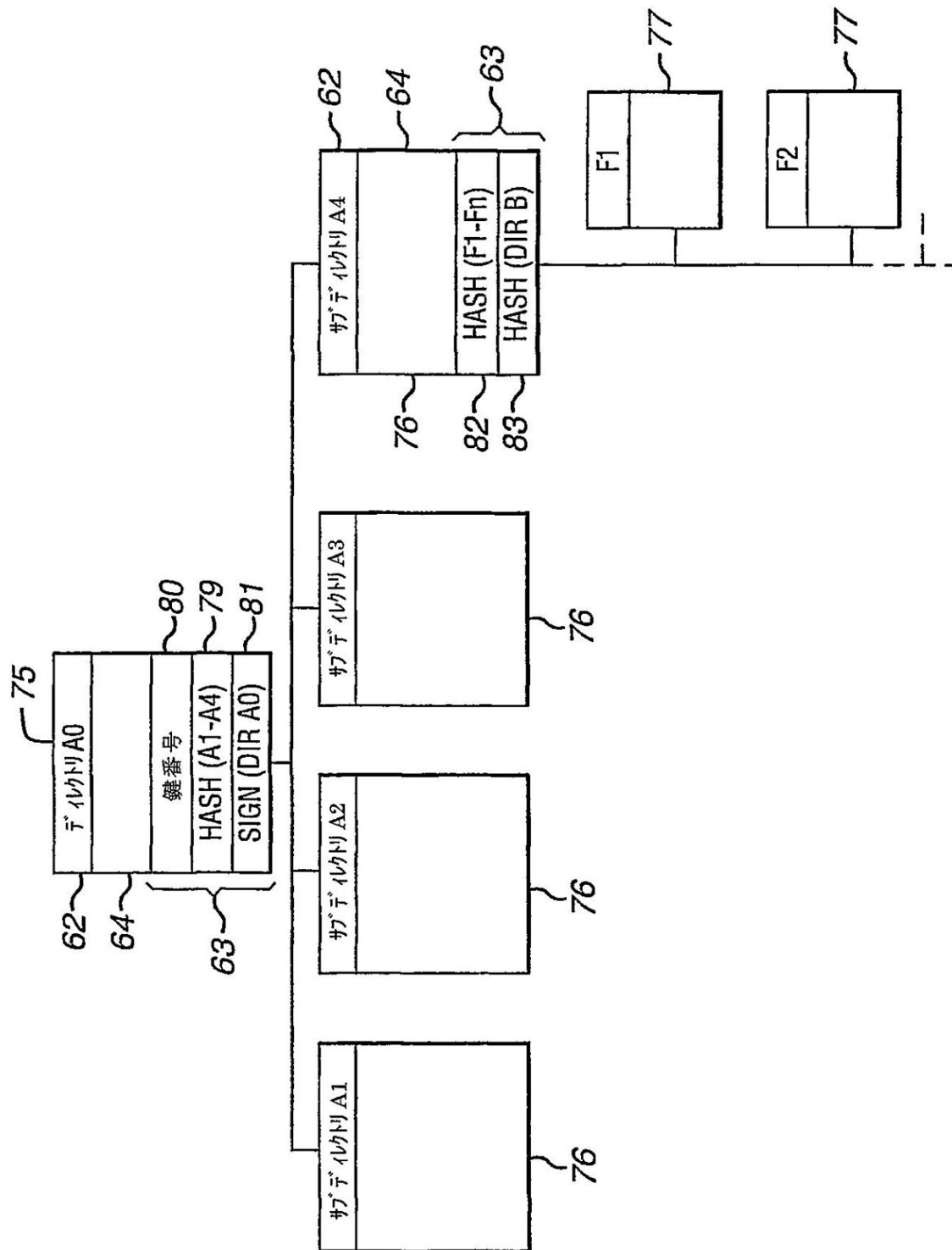
【図5】

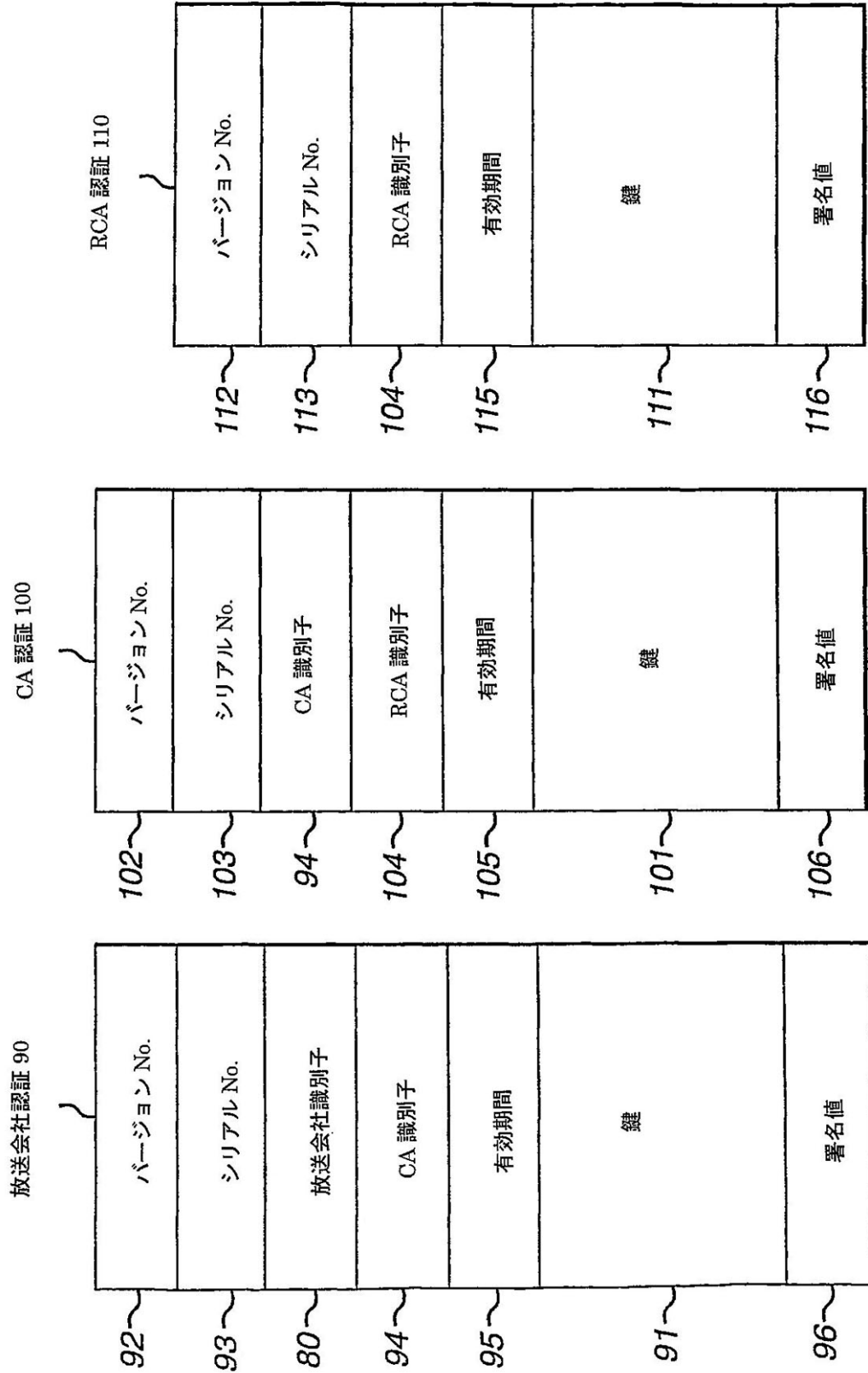


【図 6】

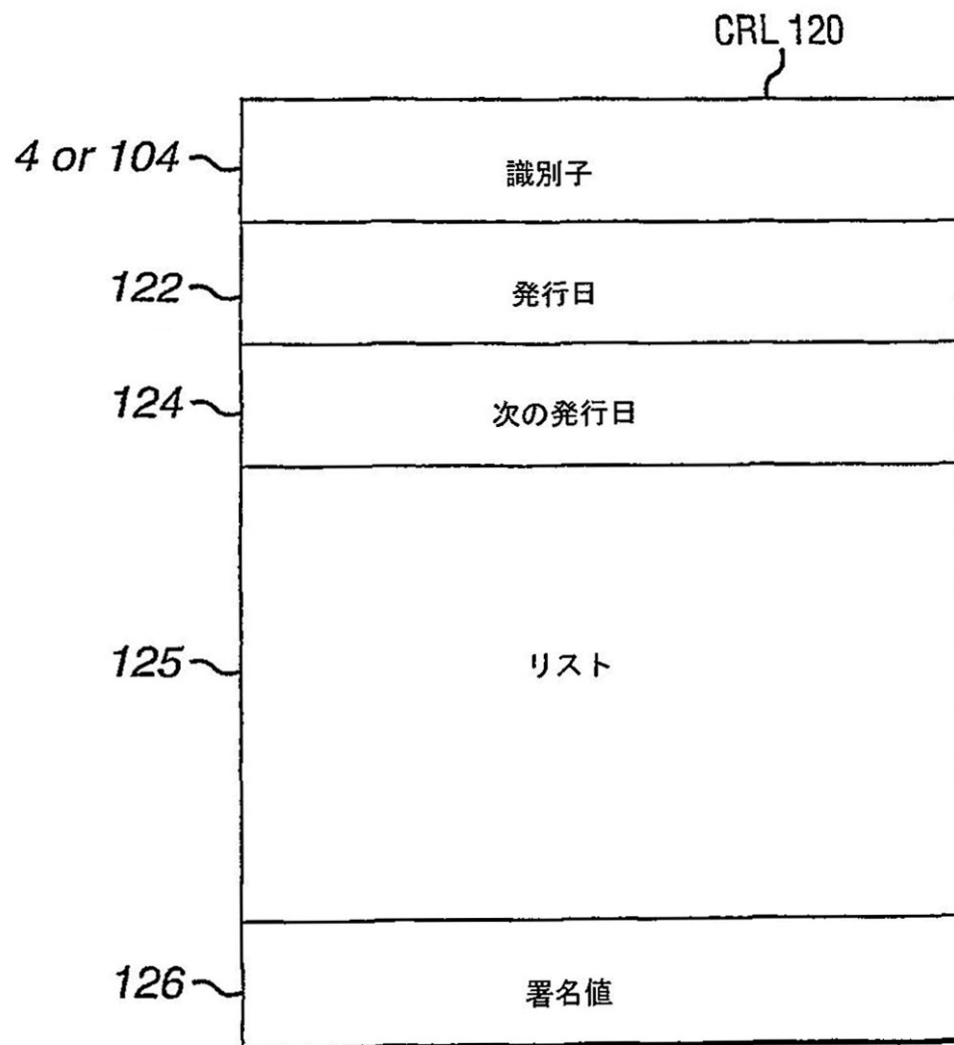


【図 7】

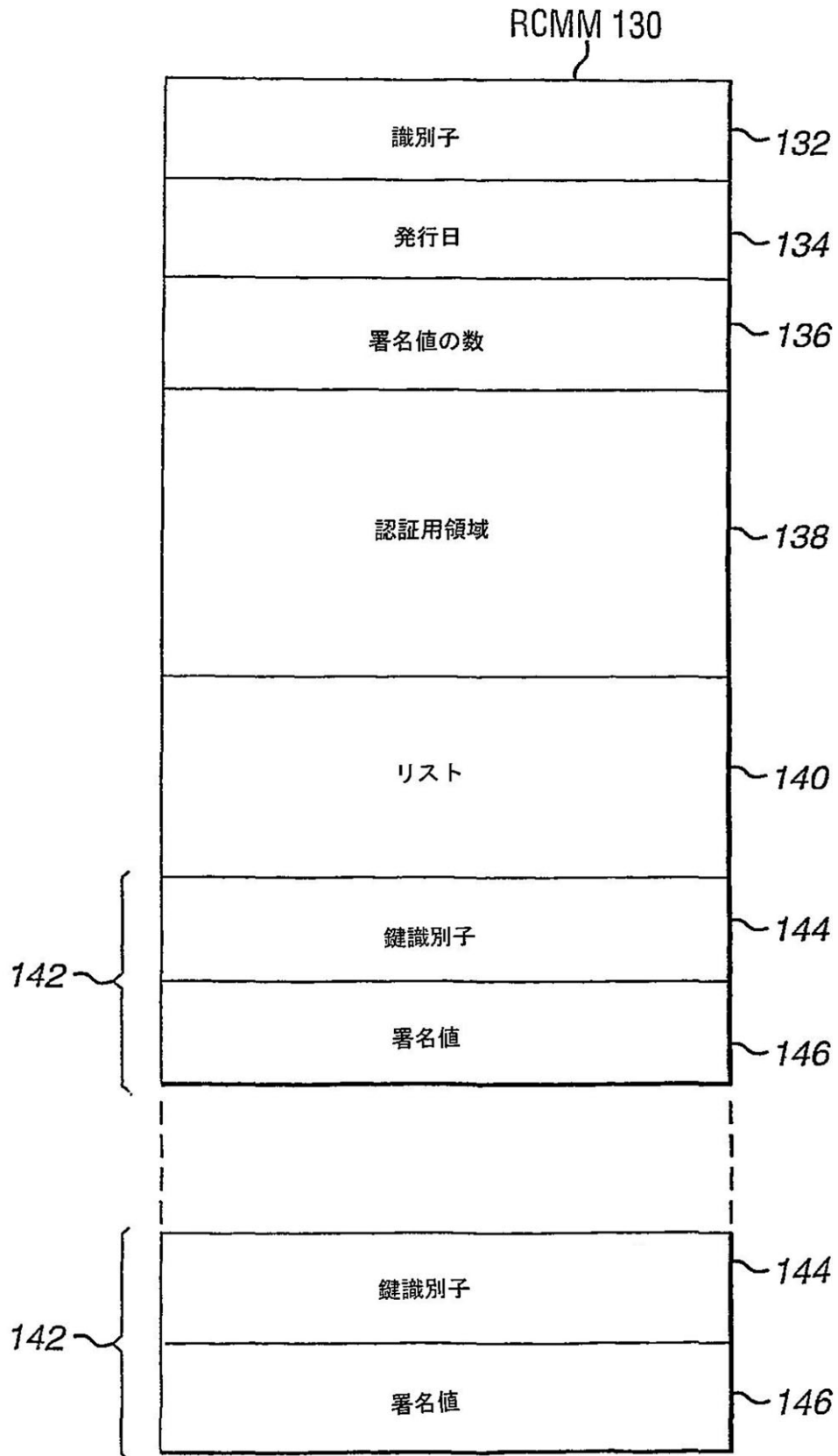




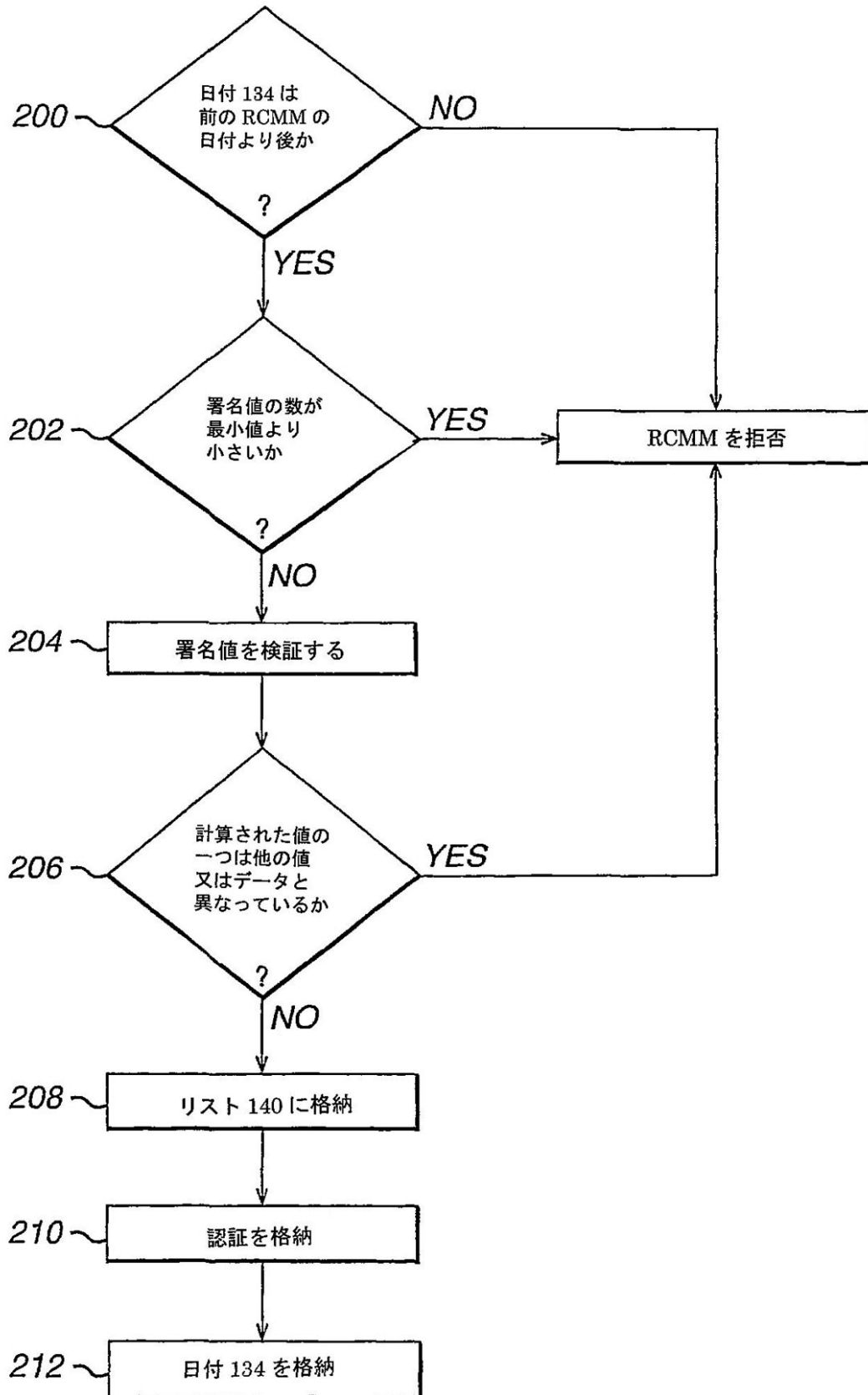
【図 9】



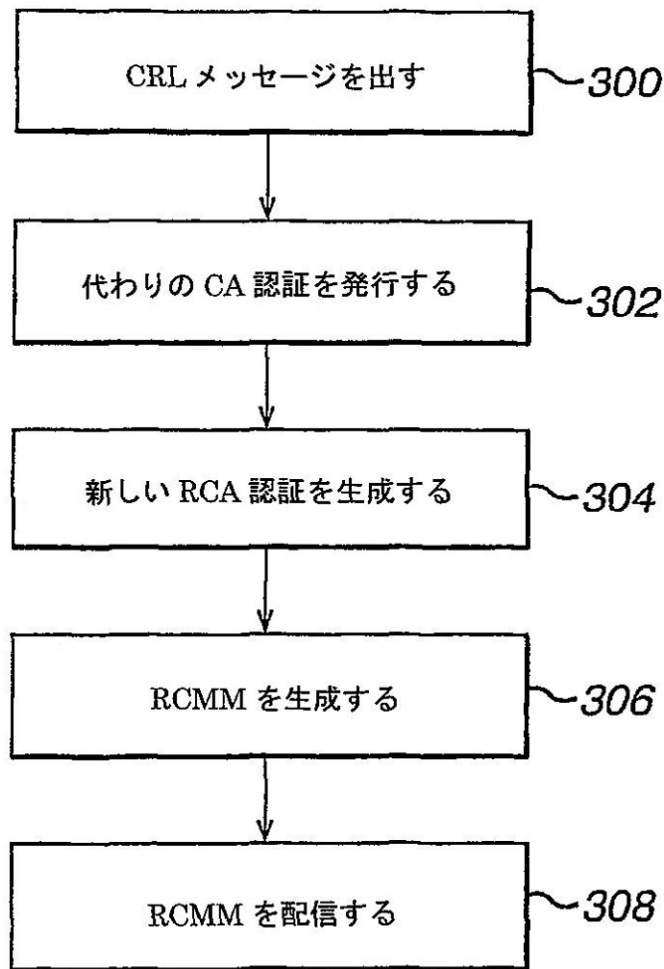
【図 10】



【図 1 1】



【図 1 2】



フロントページの続き

(74)代理人 100070530

弁理士 畑 泰之

(72)発明者 ブークエ, ジャンーベルナード ジェラルド モーリス

フランス国 エフー９２２７０ ボイスーコロンベス リュ ビクター フーゴ １３２

(72)発明者 ポーレイン, フィリップ

フランス国 エフー７５０１５ パリ リュ アライン チャーター ２３

審査官 中里 裕正

(56)参考文献 オープンネットワークにおける安全な暗号方式の更新に関する考察, 2000年暗号と情報セキュリティシンポジウム講演論文集, 2000年 1月28日, SCIS2000-C46

PGP 暗号メールと電子署名, 株式会社オライリー・ジャパン, 1996年 4月15日, p. 265-266

デジタル署名と暗号技術, 株式会社プレンティスホール出版, 1997年12月24日, 初版, p.189-196

(58)調査した分野(Int.Cl., DB名)

H04L 9/32

H04L 9/16

H04N 7/16