(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-253109
(P2005-253109A)
(43)公開日　平成17年9月15日(2005.9.15)

(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 有　請求項の数 1　OL　（全 59 頁）

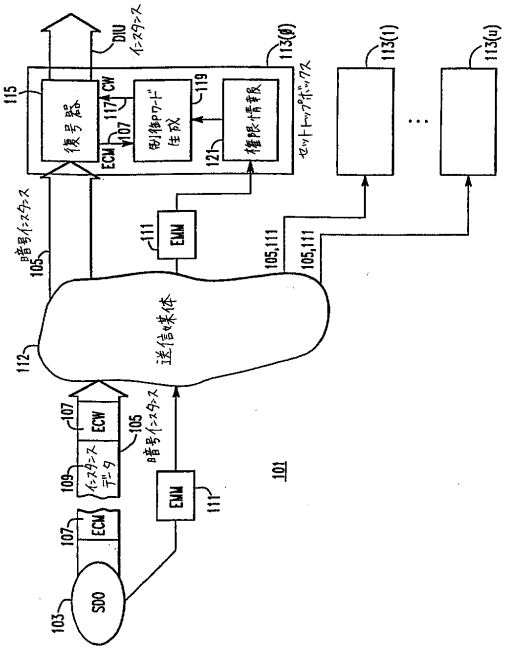
(21)出願番号	特願2005-120425 (P2005-120425)
(22)出願日	平成17年4月18日 (2005.4.18)
(62)分割の表示	特願2000-510276 (P2000-510276)の分割
原出願日	平成10年7月31日 (1998.7.31)
(31)優先権主張番号	60/054,575
(32)優先日	平成9年8月1日 (1997.8.1)
(33)優先権主張国	米国(US)
(31)優先権主張番号	09/126,921
(32)優先日	平成10年7月31日 (1998.7.31)
(33)優先権主張国	米国(US)

(71)出願人　501098050
サイエンティフィック－アトランタ，　インコーポレイテッド
アメリカ合衆国　ジョージア　３００４４，　ローレンスビル，　シュガーローフ　パークウェイ　５０３０
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明
(74)代理人　100113413
弁理士　森下　夏樹

最終頁に続く

(54)【発明の名称】条件付きアクセスシステム

(57)【要約】　（修正有）
【課題】　サービスに対する条件付きアクセスを提供する、ケーブルテレビシステム。
【解決手段】　このケーブルテレビシステムは、ここからサービス「インスタンス」またはプログラムが放送されるヘッドエンドと、これらのインスタンスを受け取り、そして、システム加入者に表示するために、このインスタンスを選択的に復号化する複数のセットトップユニットとを含む。サービスインスタンスは、サービスプロバイダまたは中央権限エージェントによって提供される公開鍵および／またはプライベート鍵を用いて暗号化される。選択的復号化のためにセットトップによって使用される鍵もまた、公開または秘密といった性質を有してもよく、これらの鍵が、異なる時点に再割り当てされることにより、侵害行為の懸念が最小にされたケーブルテレビシステムを提供する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
コンピュータを用いて、短期間鍵で暗号化されたサービスのインスタンスを復号化する方法であって、該方法は、メモリとサービス復号化器と第１のメッセージインタプリタと第２のメッセージインタプリタとを含む受信器において行われ、該メモリには公開鍵／プライベート鍵対が格納されており、
該方法は、
暗号化された第１のメッセージを該受信器において受信するステップであって、該暗号化された第１のメッセージのコンテンツは長期間鍵を含み、該コンテンツは該受信器用の該公開鍵を用いて暗号化されている、ステップと、
該第１のメッセージインタプリタを用いて、該メモリに格納されている該プライベート鍵を用いて、該暗号化された第１のメッセージの該コンテンツを復号化することにより、復号化された長期間鍵を取得するステップと、
該長期間鍵を該メモリに格納するステップと、
該サービスの該暗号化されたインスタンスとともに該受信器において第２のメッセージを受信するステップであって、該第２のメッセージは鍵導出値を含む、ステップと、
該第２のメッセージインタプリタを用いて、該鍵導出値および該メモリに格納された該長期間鍵を用いて該短期間鍵を取得するステップと、
該サービス復号化器を用いて、該短期間鍵を用いて該サービスの該暗号化されたインスタンスを復号化するステップと
を包含する、方法。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連特許出願）
本発明は、以下の米国特許出願の一部継続出願であって、以下の出願はすべて、本米国特許出願の指定代理人に受託されている。
【０００２】
１９９６年１２月１６日出願の、Ｒｏｂｅｒｔ Ｏ．ＢａｎｋｅｒおよびＧｌｅｎｄｏｎ Ｌ．Ａｋｉｎｓ ＩＩＩの米国特許出願第０８／７６７，５３５号、Ｐｒｅｖｅｎｔｉｎｇ Ｒｅｐｌａｙ Ａｔｔａｃｋｓ ｏｎ Ｄｉｇｉｔａｌ Ｉｎｆｏｒｍａｔｉｏｎ Ｄｉｓｔｒｉｂｕｔｅｄ ｂｙ Ｎｅｔｗｏｒｋ Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒｓ。
【０００３】
１９９５年４月３日出願の、Ｐｉｎｄｅｒらの米国特許第５，７４２，６７７号、Ｉｎｆｏｒｍａｔｉｏｎ Ｔｅｒｍｉｎａｌ Ｈａｖｉｎｇ Ｒｅｃｏｎｆｉｇｕｒａｂｌｅ Ｍｅｍｏｒｙ。
【０００４】
１９９５年１２月２９日出願の、Ｗａｓｉｌｅｗｓｋｉらの米国特許出願第０８／５８０，７５９号、Ｍｅｔｈｏｄ ａｎｄ Ａｐｐａｒａｔｕｓ ｆｏｒ Ｐｒｏｖｉｄｉｎｇ Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ ｉｎ Ｃｏｎｎｅｃｔｉｏｎ－Ｏｒｉｅｎｔｅｄ Ｉｎｔｅｒａｃｔｉｖｅ Ｎｅｔｗｏｒｋｓ ｗｉｔｈ ａ Ｍｕｌｔｉｐｌｉｃｉｔｙ ｏｆ Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒｓ。
【０００５】
１９９８年７月８日出願の、Ｓｅａｍａｎらの米国特許出願第０９／１１１，９５８号、Ｍｅｃｈａｎｉｓｍ ａｎｄ Ａｐｐａｒａｔｕｓ ｆｏｒ Ｅｎｃａｐｓｕｌａｔｉｏｎ ｏｆ Ｅｎｔｉｔｌｅｍｅｎｔ Ａｕｔｈｏｒｉｚａｔｉｏｎ ｉｎ Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ。
【０００６】

また、本特許出願は、１９９７年８月１日出願の、Ｗａｓｉｌｅｗｓｋｉらの米国特許出願第６０／０５４，５７５号、Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍに基づく優先権を主張する。さらに本願は同一の詳細な説明を有する７つの出願の１である。これらの出願のすべては、同一の出願日を有し、同一の指定代理人を有する。他の６つの出願の名称は以下の通りである。

【０００７】

（Ｄ－３３７３）、１９９８年７月３１日出願の、Ａｋｉｎｓらの、Ｍｅｔｈｏｄ ａｎｄ Ａｐｐａｒａｔｕｓ ｆｏｒ Ｇｅｏｇｒａｐｈｉｃａｌｌｙ Ｌｉｍｉｔｉｎｇ Ｓｅｒｖｉｃｅ ｉｎ ａ Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ。

【０００８】

（Ｄ－３４５７）、１９９８年７月３１日出願の、Ｗａｓｉｌｅｗｓｋｉらの、Ａｕｔｈｏｒｉｚａｔｉｏｎ ｏｆ Ｓｅｒｖｉｃｅｓ ｉｎ ａ Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ。

【０００９】

（Ｄ－３４７２）、１９９８年７月３１日出願の、Ａｋｉｎｓらの、Ｒｅｐｒｅｓｅｎｔｉｎｇ Ｅｎｔｉｔｌｅｍｅｎｔｓ ｔｏ Ｓｅｒｖｉｃｅ ｉｎ ａ Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ。

【００１０】

（Ｄ－３３６５）、１９９８年７月３１日出願の、Ｐｉｎｄｅｒらの、Ｅｎｃｒｙｐｔｉｏｎ Ｄｅｖｉｃｅｓ ｆｏｒ ｕｓｅ ｉｎ ａ Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ。

【００１１】

（Ｄ－２９９９）、１９９８年７月３１日出願の、Ｐｉｎｄｅｒらの、Ｖｅｒｉｆｉｃａｔｉｏｎ ｏｆ ｔｈｅ Ｓｏｕｒｃｅ ｏｆ Ｐｒｏｇｒａｍ Ｉｎｆｏｒｍａｔｉｏｎ ｉｎ ａ Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ。

【００１２】

（Ｄ－３６１４）、１９９８年７月３１日出願の、Ｐｉｎｄｅｒらの、Ｓｏｕｒｃｅ Ａｕｔｈｅｎｔｉｆｉｃａｔｉｏｎ ｏｆ Ｄｏｗｎｌｏａｄ Ｉｎｆｏｒｍａｔｉｏｎ ｉｎ ａ Ｃｏｎｄｉｔｉｏｎａｌ Ａｃｃｅｓｓ Ｓｙｓｔｅｍ。

【００１３】

（発明の分野）

本発明は、情報を保護するためのシステムに関し、より詳細には、有線または無線の媒体により送信される情報を、権限付与されないアクセスから保護するためのシステムに関する。

【背景技術】

【００１４】

（発明の背景）

情報を分配する方法の１つは、それを放送すること、即ちある媒体に情報を配して、その媒体と通じている任意の装置により受信されることである。テレビジョンおよびラジオは周知の放送媒体である。放送媒体で情報を分配して収益をあげようと欲する場合、２つの選択肢が存在する。第１は、情報を放送するのに金を支払う協賛者を見つけだすことである。第２は、代価を支払った者だけに放送情報に対するアクセスを許可することである。これは一般的に、情報をスクランブルまたは暗号化された形式で放送することで為される。媒体に接続された任意の装置がスクランブルまたは暗号化された情報を受信できるが、情報へのアクセスの代価を支払ったユーザの装置のみが情報をスクランブル解除または復号化できる。

【００１５】

例えばＣＡＴＶ会社または衛星テレビジョン会社のような、サービス分配機関は、数々のプログラムソース、即ち所定種類の情報の集合から、加入者に情報を提供する。例えば、歴史チャンネルは、歴史に関するテレビジョンプログラムを提供するプログラムソース

である。歴史チャンネルにより提供される各プログラムは、そのプログラムソースの「インスタンス」を提供する。サービス分配機関は、プログラムソースのインスタンスを放送するとき、インスタンスを暗号化またはスクランブルして、暗号インスタンスを生成する。暗号インスタンスは、インスタンスデータを含む。これはプログラムを構成する暗号情報である。

【００１６】

暗号インスタンスは、送信媒体を介して放送される。送信媒体は、無線であり得るか、「有線」、即ち電線、同軸ケーブル、または光ケーブルを介して供給される。暗号インスタンスは、多数のセットトップボックスにより受信される。セットトップボックスの機能は、暗号インスタンスが復号されるべきかどうかを決定することで、そうである場合、これを復号して、プログラムを構成する復号インスタンスを生成する。この情報は、テレビジョンセットに伝達される。公知のセットトップボックスは、暗号インスタンスを復号する復号器を含む。

【００１７】

加入者は一般的に月極でサービスを購入し（ただし、サービスが一回完結の場合もあり得る）、加入者がサービスを購入した後、サービス分配機関が、購入されたサービスのための権限情報を提供するのに必要とされる加入者メッセージに属するセットトップボックスを送る。権限情報は、インスタンスデータとともに送信され得るか、個別のチャンネル、例えば帯域外周波ＲＦリンクを介してセットトップボックスに送信され得る。権限情報を復号するために、多様な技術が利用されてきた。権限情報は、サービス分配機関のサービスのための鍵と、加入者がサービスのどのプログラムを視聴するよう登録しているかの表示を含み得る。加入者が暗号インスタンスのプログラムを視聴する登録をしていると、権限情報が表示した場合、セットトップボックスは暗号インスタンスを復号する。

【００１８】

「暗号化」と「スクランブル」とが同様のプロセスであり、「復号」と「スクランブル解除」とが同様のプロセスであることを理解されたい。相違点は、スクランブルおよびスクランブル解除は、一般的、本質的にアナログであるが、暗号化および復号プロセスは通常デジタルであることである。

【発明の開示】

【発明が解決しようとする課題】

【００１９】

アナログおよびデジタルシステムの両方において、アクセス制限が必要とされる。すべてのシステムにおいて、不断の技術的向上を駆使してアクセス制限が克服されており、より安全で柔軟なアクセス制限を必要としている。より多くのシステムがアナログ形式からデジタル形式、またはアナログおよびデジタル形式両方を含むハイブリッドシステムに切り替わるにつれ、柔軟なアクセス制限が必要とされている。

【００２０】

放送情報へのアクセスを制限することは、デジタル情報において、より重要である。この理由は、まず、デジタル情報の各複製は、オリジナル同様に質がよいからである。次に、デジタル情報は圧縮し得るので、その結果、デジタル形式では、所与の量の帯域幅が遙かに多くの情報を搬送するからである。第３に、サービス分配機関が、セットトップボックスからサービス分配機関にメッセージを送ることを可能にする返送経路を付与しているので、多様なインタラクティブサービスを許容していからである。

【００２１】

従ってサービス分配機関は、従来システムに比べて、より安全でより柔軟なアクセス制限を必要とする。

【発明を実施するための最良の形態】

【００２２】

（好適な実施形態の詳細な説明）

図中の参照符号は少なくとも３桁を有する。右２桁は、図中の参照符号である。それら

より左の数字は、その参照符号により示された部材が最初に現れた図の番号である。例えば、参照符号２０３の部材は、図２に最初に現れる。

【００２３】

以下の詳細な説明は、まず、条件付きアクセスシステムと、暗号化および復号とに対する一般的紹介を提供し、次に、サービスインスタンスの暗号化および復号が、好適な実施形態においていかに行われるかを説明し、これに基づいて、好適な実施形態のＥＣＭおよびＥＭＭを認証するための好適な実施形態に使用される技術を説明する。次に、詳細な説明は、サービスにアクセスを動的に追加および削除するために、ＥＭＭがいかに使用され得るかと、それらの動作における暗号化および認証の役割とを説明する。最後に、セットトップボックスからヘッドエンドまでのノード構造および返信経路を伴う放送データ分配において、上述の技術がいかに利用されるかと、好適な実施形態において、鍵および登録情報を保護するためにセキュリティプロセッサおよびメモリがいかに利用されるかと、好適な実施形態において所定の動作がいかに実行されるかと、を説明する。

【００２４】

（条件付きアクセスシステムの概観）

図１は、放送情報へのアクセスを制限するためのシステム１０１の概観を提供する。そのようなシステムは、「条件付きアクセスシステム」と称される。例えばＣＡＴＶ会社または衛星テレビジョン会社などのサービス分配機関１０３は、多くのサービス、即ち所定種類の情報の集合からの情報を加入者に提供する。例えば、歴史チャンネルは、歴史に関するテレビジョンプログラムを提供するサービスである。歴史チャンネルにより提供される各プログラムは、そのサービスの「インスタンス」である。サービス分配機関が、サービスのインスタンスを放送するとき、インスタンスを暗号化またはスクランブルして、暗号インスタンス１０５を生成する。暗号インスタンス１０５は、プログラムを構成する暗号情報であるインスタンスデータ１０９と、登録制御メッセージ（ＥＣＭ）１０７と、を含む。登録制御メッセージは、関連するインスタンスデータ１０９の暗号部分を復号するのに必要な情報を含む。所与の登録制御メッセージは毎秒数回送信されるので、任意の新規視聴者またはサービスに即座に利用できる。侵害者がインスタンスデータ１０９を復号するのをより困難にするために、登録制御メッセージのコンテンツは、数秒ごと、またはより頻繁に変更される。

【００２５】

暗号インスタンス１０５は、送信媒体１１２を介して放送される。媒体は無線であり得るか、「有線」、即ち電線、同軸ケーブル、または光ケーブルを介して供給される。暗号インスタンスは、多数のセットトップボックス１１３（０…ｎ）により受信され、各セットトップボックスは、テレビジョンセットに接続されている。セットトップボックス１１３の機能は、暗号インスタンス１０５が復号されるべきかどうかを決定することで、そうである場合、これを復号して、テレビジョンセットに伝達される復号インスタンス１２３を生成する。セットトップボックス１１３（０）を参照して詳細に示すように、セットトップボックス１１３は、暗号インスタンス１０５を復号するための鍵として制御ワード１１７を使用する復号器１１５を含む。制御ワード１１７は、制御ワード生成器１１９により、登録制御メッセージ１０７に含まれる情報およびセットトップボックス１１３に格納された権限情報１２１から生成される。例えば、権限情報１２１は、サービスに対する鍵と、加入者がサービスのどのプログラムを視聴するよう登録しているかの表示を含み得る。加入者が暗号インスタンス１０５のプログラムを視聴する権利を与えられていると権限情報１２１が示した場合、制御ワード生成器１１９は、ＥＣＭ１０７からの情報とともにこの鍵を使用して、制御ワード１１７を生成する。もちろん、各新規のＥＣＭ１０７に対して新規の制御ワードが生成される。

【００２６】

特定のセットトップボックス１１３（ｉ）において使用される権限情報は、セットトップボックス１１３（ｉ）にアドレスされた１つ以上の登録管理メッセージ１１１から獲得される。加入者は一般的に月極でサービスを購入し（ただし、サービスが一回完結の場合

もあり得る）、加入者がサービスを購入した後、サービス分配機関１０３が、要求に応じて加入者の登録管理メッセージ１１１に属するセットトップボックス１１３（ｉ）を送信し、購入されたサービスのために必要な権限情報１２１を提供する。登録管理メッセージ（ＥＭＭ）は、ＥＣＭ１０７と同じ様態で、インスタンスデータ１０９とインターリーブされて送信されるか、または個別のチャンネル、例えば帯域外周波ＲＦリンクを介してセットトップボックス１１３（ｉ）に送信され得、権限情報１２１内に登録管理メッセージ（ＥＭＭ）１１１からの情報を格納する。もちろん、登録管理情報を暗号化するために多様な技術が利用されてきた。

【００２７】

（一般的な暗号化および復号）

サービスインスタンスの暗号化および復号のために使用される暗号化および復号技術は、２つの一般的分類に属する。即ち、対称鍵技術および公開鍵技術である。対称鍵暗号化技術は、通信を欲する各エンティティが鍵の複製を有するものである。送信エンティティが鍵の複製を使用してメッセージを暗号化し、受信エンティティが鍵の複製を使用してメッセージを復号する。対称鍵暗号化／復号システムの例は、デジタルエンクリプションスタンダード（ＤＥＳ）システムである。公開鍵暗号化システムは、通信を欲する各エンティティが、自分の公開鍵／プライベート鍵の対を有するものである。公開鍵により暗号化されたメッセージは、プライベート鍵によってのみ復号され得るか、その逆である。従って、所与のエンティティがプライベート鍵の秘密を保持する限り、通信を欲してくる他の任意のエンティティに公開鍵を提供し得る。他のエンティティは、所与のエンティティに送信を欲するメッセージを単に所与のエンティティの公開鍵で暗号化し、所与のエンティティは、プライベート鍵を用いてこのメッセージを復号する。プライベート鍵は、デジタル署名処理にも使用でき、認証を提供する。暗号化一般と、特定の対称鍵および公開鍵暗号化に関する詳細は、ＢｒｕｃｅＳｃｈｎｅｉｅｒのＡｐｐｌｉｅｄＣｒｙｐｔｏｇｒａｐｈｙ、Ｊｏｈｎ Ｗｉｌｅｙ and Ｓｏｎｓ，Ｎｅｗ Ｙｏｒｋ，１９９４を参照されたい。

【００２８】

所与のアプリケーションのための暗号化システムの設計は、多くの考慮を必要とする。以下に示すように、放送メッセージ環境において特に重要な考慮は、以下を含む。

【００２９】

・鍵のセキュリティ：通信者によって共有される鍵に第３者がアクセスを有する場合、対称鍵システムは無用であり、所与の公開鍵の所有者以外の誰かが、対応するプライベート鍵にアクセスを有する場合、公開鍵システムも無用である。

【００３０】

・鍵の証明：受取人は、自分が受け取った鍵が、本当に自分が暗号メッセージを送りたいエンティティに属する鍵であり、メッセージを妨害しようと欲する別のエンティティに属する鍵でないことを、いかにして確証するのか。

【００３１】

・メッセージ認証：メッセージが示されたとおりの相手からのものであり、および／またはメッセージが変更されていないことを、メッセージの受取人は、いかにして確証するのか。

【００３２】

・暗号化および復号の速度：一般的に、対称鍵暗号化システムは、公開鍵暗号化システムより速く、実時間媒体での使用が好まれる。

【００３３】

・鍵のサイズ：一般的に暗号化システムに使用される鍵が長いほど、暗号を復号するのに、ひいてはメッセージにアクセスを得るのに、より多くのリソースを必要とする。

【００３４】

上述の考慮はすべて、条件付きアクセスシステムが動作する環境が、敵対的であると推測せねばならない事実による影響を受けている。放送サービスの多くの顧客は、サービス

プロバイダを欺くことを別に悪いと考えておらず、受信器に含まれる条件付きアクセスシステムの部分を物理的に改竄したり、様々な暗号攻撃を使用して鍵を盗んだり、受信者が受け取るメッセージのソースに関して受信者を欺いたりすることを何とも感じていない。さらに、サービスを実際に放送するシステムのプロバイダは、サービスコンテンツのプロバイダと同じ関心を必ずしも有している訳ではなく、従って、サービスの所与のインスタンスに誰がアクセスするかだけでなく、どのエンティティが所与の受信者にサービスを供給できるかも制御する必要がある。

【００３５】

（サービスインスタンス暗号化および復号：図２Ａおよび２Ｂ）

概して、本発明による暗号化システムは、対称鍵暗号化技術を使用して、サービスインスタンスを暗号化および復号し、公開鍵暗号化技術を使用して、サービスプロバイダの鍵の対称鍵技術において使用された鍵の１つの複製をセットトップボックスに搬送する。

【００３６】

図２Ａでは、ＭＰＥＧ－２プログラムを含むエレメンタリーデジタルビットストリームなどのクリアサービスが、プログラム暗号化機能２０１と呼ばれる第１レベルの暗号化を介して送信される。プログラム暗号化機能２０１は、好適には、周知のＤＥＳアルゴリズムなどの対称暗号である。各エレメンタリーストリームは個別に暗号化され、生成された暗号ストリームはＭＵＸ２００に送られて、他のエレメンタリーストリーム、および条件付きアクセスデータなどのプライベートデータと組み合わされる。プログラム暗号化機能２０１に使用される鍵は、制御ワード（ＣＷ）２０２と呼ばれる。ＣＷ２０２は、制御ワード生成器２０３により生成される。制御ワード生成器２０３は、物理的乱数生成器であるか、ランダムＣＷのストリームを生成するための適切なランダムアルゴリズムを備えた順次カウンタ（ｓｅｑｕｅｎｔｉａｌ　ｃｏｕｎｔｅｒ）を使用し得る。新規のＣＷは、おそらく数分に一度の割合で頻繁に生成され、同時刻スケールの各エレメンタリーストリームに付与される。各新規のＣＷは、制御ワード暗号化およびメッセージ認証機能２０４により、マルチセッション鍵（ＭＳＫ）生成器２０５により提供されるマルチセッション鍵（ＭＳＫ）２０８を使用して暗号化される。次にＣＷは、他のサービス関連情報とともにＥＣＭ１０７に組み込まれる。ＥＣＭ１０７は、制御ワード暗号化およびメッセージ認証機能２０４により認証される。制御ワード暗号化およびメッセージ認証機能２０４は、受信セットトップボックス１１３に共有され得る秘密と組み合わせたメッセージコンテンツから誘導された有鍵のハッシュ値を使用して、メッセージ認証コードを生成する。この秘密は、好適には、すべてのＭＳＫ２０８の一部である。メッセージ認証コードは、残りのＥＣＭ１０７に添付される。ＣＷ２００は、ＥＣＭの他の部分に伴ってＭＵＸ２００に送信される前に常に暗号化される。この暗号は、好適には、２つの異なる５６ビット鍵（併せてＭＳＫ２０８を構成する）を用いた三重ＤＥＳアルゴリズムなどの対称暗号である。

【００３７】

ＭＳＫ２０８は、ＣＷ２０２よりも長い寿命を有する。ＭＳＫの寿命は典型的には、数時間から数日の長さである。ＭＳＫ２０８は、ＥＭＭ１１１に封入されたＭＵＸ２００に送信される前に、ＭＳＫ暗号およびデジタル署名機能２０６により、暗号化およびデジタル署名の両方をされる。

【００３８】

ＭＳＫ２０８およびＥＭＭ１１１の他の部分とは、好適には、周知のＲＳＡアルゴリズムなどの公開鍵アルゴリズムを使用して、そのＥＭＭがアドレスされる特定のセットトップボックス１１３に関連する公開鍵とともに暗号化される。システム１０１におけるすべてのセットトップボックス１１３の公開鍵は、公開鍵データベース２０７に格納される。このデータベース内の公開鍵は、好適には、証明機関により証明される。２０６におけるデジタル署名機能は、好適には、ＲＳＡデジタル署名方法であるが、他のものも使用し得る。ＲＳＡデジタル署名の場合は、署名するのに使用されるプライベート鍵は、関連サービスの認証を司るサービス分配機関１０３内の登録エージェントに属する。

【００３９】
図２Ｂでは、対応するＤＨＣＴプライベート鍵および関連するＤＨＣＴ公開セキュリティミクロシリアル番号が、デコーダ２４０のメモリ２３２に格納される。公開セキュリティミクロシリアル番号が供給されることにより、デマルチプレクサ２３０は、トランスポートデータストリーム（ＴＤＳ）からデコーダ２４０にアドレスされた暗号マルチセッション鍵を選択し得る。暗号化マルチセッション鍵E_{Kpr}は、メモリ２３２からのＤＨＣＴプライベート鍵を使用して復号器２３４において復号され、マルチセッション鍵ＭＳＫを提供する。また、デマルチプレクサ２３０は、トランスポートデータストリームからＴＤＳ暗号化された制御ワード（ＣＷ）E_{MSK}（ＣＷ）を選択する。暗号ＣＷは、復号鍵としてマルチセッション鍵ＭＳＫを使用して復号器２３６で処理され、暗号化されていないＣＷを提供する。暗号化されていないＣＷは、好適には、速い速度、例えば数秒間に一度で変化する。デマルチプレクサ２３０は、トランスポートデータストリームからＴＤＳ暗号化されたサービスE_{CW}（ＳＥＲＶＩＣＥ）も選択する。暗号サービスは、復号鍵としてＣＷを使用して復号器２３８で処理され、暗号化されていないサービスを復元する。

【００４０】
（図２の暗号化システムの詳細な実施：図３）
図３は、図２のシステムの好適な実施をより詳細に提供する。暗号化／復号システム３０１は、２つの主要要素を有する。即ち、サービス開始要素３０５およびサービス受容要素３３３である。この２つは、送信媒体３３１により接続される。送信媒体３３１は、サービス開始要素３０５からサービス受容要素３３３へのメッセージを搬送する任意の媒体であり得る。サービス受容要素３３３は、セットトップボックスにおいて実施され、本願ではデジタルホーム通信端末（ＤＨＣＴ）と称される。しかしながら、サービス受容要素３３３は、例えば、パーソナルコンピュータ、ワークステーション、または「インテリジェント」テレビジョンセットなど、必要な演算能力を有する任意の装置において実施し得る。サービス開始要素では、少なくとも３０６と表示された部分が、ケーブルテレビジョン（ＣＡＴＶ）または衛星ＴＶシステムなどの、放送システムヘッドエンドに位置する機器において実施される。しかしながら、実施形態によっては、ヘッドエンドは、サービスの暗号化済みのインスタンスを供給され得る。残りの部分３０８もヘッドエンドに位置し得るが、ヘッドエンド３０６およびサービス受容要素３３３へのある種のアクセスを有する任意の場所に位置してもよい。後者は特に、例えばインターネットなどの広域ネットワークにより、ＥＭＭが帯域幅外で送信される場合である。また、送信媒体は格納媒体であり得、ここでは、サービス開始点が媒体の製造者であり、サービス受容要素は、格納媒体を読み出す要素であり得る。例えば、送信メディアは、ＣＤ－ＲＯＭ、ＤＶＤ、フロッピー（登録商標）ディスク、または物理的、電気的などにより転送できる他の任意の媒体であり得る。

【００４１】
まず、サービス開始部分３０５では、乱数生成器３０７を使用して、ＭＳＫ３０９が生成される。次に、ＭＳＫ３０９を含むＥＭＭ３１５および関連情報が生成される。ＥＭＭ３１５は、封印されたダイジェスト（ｓｅａｌｅｄ　ｄｉｇｅｓｔ）も含む。封印されたダイジェストは、２つの目的を有する。サービス開始３０５によりＥＭＭ３１５に配置された情報が、ＤＨＣＴ３３３に到着した情報と同一であるかを確認すること、およびその情報がサービスへアクセスする権利を与えられたエンティティから実際に到来した情報であることを確認することである。

【００４２】
封印されたダイジェストは、２つの段階において生成される。第１に、ＥＭＭのコンテンツ（ここでは、ＭＳＫ３０９および関連情報）のダイジェストがセキュリティ一方向ハッシュ関数でハッシュされることにより生成され、比較的短いビットストリングを形成する。セキュリティ一方向ハッシュ関数は３つの属性を有する。

【００４３】
・短いビットストリングを形成するためにハッシュされたコンテンツは、その短いビッ

トストリングにより規定され得ない。

【００４４】

・ハッシュされることによる任意の変更は、短いビットストリングの変更を形成する。

【００４５】

・ＥＭＭと同一の短いビットストリングを形成する異なるメッセージの構築が、計算的に実行不能である。

【００４６】

従って、ハッシュ関数の短いビットストリングの出力は、ＥＭＭのコンテンツが、それらのコンテンツを公表せずに転送において変更されたのか否かを決定するのに使用され得る。好適な実施形態は、符号ＭＤ５により示されたメッセージダイジェスト５一方向ハッシュ関数を使用する。一方向ハッシュ関数の詳細については、上述のＳｃｈｎｅｉｅｒの文献を参照されたい。ダイジェストは封印されたダイジェストである。これは、ダイジェストが、ＭＳＫを使用して鍵を生成するサービスへへのアクセスをＤＨＣＴに与える権利を有する登録エージェント（ＥＡ）に属する公開鍵ＳＰＫｒ３１０により暗号化されているためである。ＥＭＭが正しく送信されているかどうかを確認するために、封印されたダイジェストが使用される前に、ダイジェストは、登録エージェントの公開鍵を使用して復号されなければならない。従って、封印されたダイジェストは、ＥＭＭのコンテンツが正しく送信されたことと、ＥＭＭのソースが登録エージェントであることをＤＨＣＴに確信させる。

【００４７】

いったん封印されたダイジェストが生成されれば、ＥＭＭのコンテンツ（ここでは、ＭＳＫ３０９および関連情報）は、ＥＭＭ３１５がアドレスされるＤＨＣＴ３３３の公開鍵ＤＨＣＴＫｕ３１２で暗号化され、暗号コンテンツおよび封印されたダイジェストを含むＥＭＭ３１５は、送信媒体３３１を介してＤＨＣＴ３３３に送信される。以下では、プライベート鍵を示すのに符号Ｋｒが使用され、公開鍵を示すのに符号Ｋｕが使用される。符号ＲＳＡは、暗号化が周知のＲＳＡ公開鍵アルゴリズムを使用して為されることを示す。

【００４８】

ＤＨＣＴ３３３に示すように、ＥＭＭ３１５は、そのプライベート鍵３３７（ＤＨＣＴＫｒ）がＥＭＭ３１５を暗号化するのに使用される公開鍵に対応する、ＤＨＣＴ３３３によってのみ暗号化され得る。ＤＨＣＴ３３３は、ＥＭＭ３１５を復号し、封印されたダイジェストを用いてＥＭＭ３１５が正しく送信されたか否かを決定する。この決定は、登録エージェントが封印されたダイジェストを復号するための公開鍵ＳＰ　Ｋｕ３３５を使用することにより為される。次に、ＥＭＭ３１５のコンテンツは、ダイジェストを生成するのに使用されたのと同一のセキュリティ一方向ハッシュ関数を使用してハッシュされる。このハッシュの結果が復号された封印されたダイジェストと同一である場合、決定は成功する。ＤＨＣＴ３３３への送信が送信中に改竄（文字化け）された場合、ＥＭＭの暗号化に使用された公開鍵に対応するプライベート鍵をＤＨＣＴ３３３が有していない場合（即ち、ＥＭＭ３１５が意図されたＤＨＣＴ３３３でない）、または封印されたダイジェストの生成に使用されたプライベート鍵に対応する対応する公開鍵３３５（ＳＰ　Ｋｕ）をＤＨＣＴ３３３が有していない場合、封印されたダイジェストの確認は失敗する。後者は、ＤＨＣＴ３３３が登録エージェントにより提供されるサービスへのアクセスを有していない場合である。ＤＨＣＴ３３３にアドレスされたＥＭＭ３１５は、反復して送信される。その結果、問題が転送中の改竄である場合、改竄されていないＥＭＭ３１５がすぐに受信され、決定は成功する。ＤＨＣＴ３３３が、封印されたダイジェストの復号に必要なＳＰ　Ｋｕ３３５をいかにして有するようになるかは、後に詳細に説明する。

【００４９】

サービス開始３０５の次の段階は、実際にサービスインスタンス３２５を暗号化する制御ワード３１９を生成すること、およびサービスインスタンスを復号するのに必要な情報をＤＨＣＴ３３３に搬送することである。制御ワード３１９は、乱数生成器３１７により生成される。これは、真の乱数生成器であり得、その出力は、いくつかの基本的な下敷き

となるランダムな物理プロセスの結果であるか、または、例えば、ＭＳＫを鍵として用いて、（１使用ごとに１ずつ増加する）「カウンタ」と呼ばれる値を３ＤＥＳとともに暗号化した結果などの他の手段である。真の乱数の場合、暗号化された制御ワードはＥＣＭに送信される。カウンタベースの制御ワード生成の場合、「カウンタ」のクリアバージョンは、送信されたＥＣＭにおいて使用される。上述のように、制御ワードは短期間の鍵、即ち数秒以下の寿命である。ＥＣＭ３２３に含まれるのは、コンテンツのダイジェストおよび先述のＭＤ５一方向ハッシュを使用して生成されたＭＳＫである。ダイジェストの生成にＭＳＫを含むことは、登録エージェントからのサービスインスタンスを受信するよう登録されたＤＨＣＴ３３３との共有秘密を、ＥＣＭ３２３が属する登録エージェントに与え、その結果ＥＣＭ３２３の「スプーフィング（ｓｐｏｏｆｉｎｇ）」、即ち、登録エージェント以外のソースからのＥＣＭ３２３の取得を防ぐ。後に詳述して示すように、好適な実施形態は、一般的に共有秘密技術を使用して、サービスのインスタンスに関して実時間値を有するメッセージを含むメッセージを認証する。

【００５０】

ＥＣＭ３２３は、暗号コンテンツ３２９とともにＤＨＣＴ３３３に送信される。暗号コンテンツ３２９の所与の部分に対する第１のＥＣＭ３２３は、もちろん、暗号コンテンツが到着する前にＤＨＣＴ３３３に到着する。好適な実施形態では、コンテンツ３２５およびＥＣＭ３２３は、ＭＰＥＧ－２規格により符号化される。この規格は、多数の要素ストリームを含むトランスポートストリームを提供する。それらのあるものはコンテンツ３２９を搬送し、別のものはＥＣＭ３２３を搬送し、第３のものはＥＭＭ３１５を搬送する。コンテンツ３２９を搬送するストリームのみが、ＤＥＳ３２９により暗号化される。これは、ＥＣＭ３２３における制御ワードおよびＥＭＭ３１５のコンテンツは、既に暗号化されており、ＭＰＥＧ－２トランスポートストリームにより送信されるときにはさらなる暗号化を必要としないからである。ＥＭＭおよびＥＣＭがＭＰＥＧ－２トランスポートストリームにより搬送される様態は後に詳述する。

【００５１】

ＥＣＭ３２３がＤＨＣＴ３３３に受信されるとき、制御ワード３１９は、復号されるか、またはＭＳＫを使用して３４３においてカウンタ値を暗号化することにより発見される。ＥＣＭ３２３のコンテンツの完全性は、ＥＭＣ３２３に含まれるメッセージダイジェストとともに、一方向ハッシュ関数において、コンテンツと、（暗号原理に基づく）いくつかまたはすべてのＭＳＫをハッシュした結果の値と比較することにより確認される。コンテンツの中に含まれるのは、制御ワード３１９と、ＥＣＭ３２３を伴うサービスインスタンス３２５を識別する情報とである。識別情報は、ＥＭＭ３１５に受け取られた権限情報とともに使用され、ＤＨＣＴ３３３がサービスインスタンス３２５を受信するよう認証されたか否かを決定する。そうである場合、制御ワード３１９が、サービス復号器３４７により使用され、暗号コンテンツを復号してオリジナルのコンテンツ３２５を生成する。

【００５２】

システム３０１は、セキュリティに関して数々の利点を提供する。スピードが必要なところでは、対称暗号化システムのスピードの利点を採り入れ、暗号化されたコンテンツ３２９およびＥＣＭ３２３における制御ワードの復号を行う。制御ワードは、ＭＳＫを使用して暗号化されることにより保護され、ＥＣＭ３２３は、登録エージェントとＤＨＣＴ３３３との間の共有秘密として、いくつかまたはすべてのＭＳＫ３０９を使用することにより認証される。ＭＳＫ３０９は、次に、ＤＨＣＴの公開鍵を使用して暗号化されたＥＭＭにおいて送信されたという事実、およびＥＭＭが登録エージェントのプライベート鍵を使用して暗号化された封印されたダイジェストを含むという事実により保護される。さらなるセキュリティは、制御ワード３１９がサービス復号器３４７に供給される前にＥＭＭ３１５に受け取られた権限情報と、ＥＣＭ３２３からのサービス識別情報とが一致しなければならないという事実により提供される。例えば、上述したＢａｎｋｅｒおよびＡｋｉｎｓの親出願に詳細に説明されるように、ＥＣＭ３２３およびＥＭＭ３１５の情報の一度の使用が、暗号化サービスへの「リプレイアタック（ｒｅｐｌａｙ　ａｔｔａｃｋ）」と呼

ばれるものを防いでいる。安全であることに加え、システム３０１は柔軟である。ＥＭＭ３１５に含まれる権限情報と、ＥＣＭ３２３に含まれるサービス識別情報とが、ＤＨＣＴ３３３に受信されるサービスインスタンスへの広範なアクセスを可能にしている。

【００５３】

（ＤＨＣＴ３３３への多重登録エージェントの動的提供：図４）

ＥＭＭ３１５における封印されたダイジェストは、ＥＭＭ３１５においてＭＳＫにより復号されるサービスへの登録を与える権利を有する登録エージェントのための公開鍵をＤＨＣＴ３３３が有さない限り、ＤＨＣＴ３３３がＥＭＭ３１５に応答しないことを意味する。これは、ＤＨＣＴ３３３に１つ以上の登録エージェントを動的に提供し、ＤＨＣＴ３３３から提供された登録エージェントを動的に削除する、より広範な取り決め（ａｒｒａｎｇｅｍｅｎｔ）の一部である。

【００５４】

登録エージェントを提供したり削除するエンティティは、条件付きアクセスオーソリティ（ＣＡＡ）と呼ばれる。この取り決めは、ＤＨＣＴ３３３に提供された登録エージェントが、ＤＨＣＴ３３３にあるそれらの権限情報を動的に改変することを、さらに可能にする。これらの動作を実行するのに必要な情報はすべて、封印されたダイジェストとともに、ＥＭＭを介して送信される。封印されたダイジェストは、ＣＡＡのみが登録エージェントを追加または削除し得ることと、権限情報が属する登録エージェントのみが権限情報を改変し得ることとを確実にするために使用される。

【００５５】

上記の取り決めは多数の利点を有する。

【００５６】

・複数の登録エージェントを可能にする。

【００５７】

・登録エージェントの動的追加および削除を可能にする。

【００５８】

・登録エージェントが登録を許可し得るサービスに制限を設けるが、登録エージェントが自分たちの権限情報を管理することを可能にする。

【００５９】

・サービスおよびサービスインスタンスへの登録を提供するビジネスを、実際にサービスのインスタンスを提供するビジネスから分離する。その結果、ＣＡＴＶオペレータは、単に分配ユーティリティとして機能する。

【００６０】

・エンティティに登録エージェントである権利を付与するビジネスを登録エージェントであるビジネスから分離する。

【００６１】

・自分に適合するとの考えに従い、顧客が登録エージェントを変更する簡単な方法を提供する。

【００６２】

・ＤＨＣＴ３３３が返信経路により登録エージェント、条件付きアクセスオーソリティ、または、可能性としてサービスインスタンスのプロバイダと通信し得る安全な取り決めを提供する。

【００６３】

図４は、好適な実施形態において、この取り決めがいかにして実施されるかを示す。図４は、図３の延長として最もよく理解される。図４および図３は両方とも同じ主要要素を有する。即ち、サービス開始３０５、ＤＨＣＴ３３３、および両者を結合する送信媒体３３１である。さらに、暗号器３１３および復号器３３９が両図で使用されている。また、参照符号３０８により示されているように、ＥＭＭは、サービスインスタンスとともに、または別のチャンネルにより送信される。さらに、図４は、ＤＨＣＴ３３３の追加の要素、即ちＥＭＭマネジャー４０７を示す。ＥＭＭマネジャー４０７は、ＤＨＣＴ３３３内の

セキュリティプロセッサにおいて実行されるソフトウェアで実施される。ＥＭＭマネジャー４０７のタスクは、登録エージェントを追加または削除するＥＭＭと、登録エージェントに対する認証を改変するＥＭＭとに応答することである。ＥＭＭマネジャー４０７は、どのＤＨＣＴ３３３が、登録エージェントまたは条件付きアクセスオーソリティと通信し得るかによりさらにメッセージを供給する。

【００６４】

最初に、登録エージェントにより提供されるか、またはネットワークオペレータにより要求された改変情報４０３に応答して、登録エージェントの権限情報を改変するＥＭＭが生成される。３１３に示すように、改変情報は、ＤＨＣＴ３３３に対する公開鍵３１２を使用して暗号化され、登録エージェントに対するプライベート鍵３１０を使用して暗号化された封印されたダイジェストを有する。生成された権限改変ＥＭＭ４０５は、送信媒体３３１を介して、ＤＨＣＴ３３３に含まれる復号器３３９に送信される。ここで、権限改変ＥＭＭ４０５は復号され、ＭＳＫに含まれるＥＭＭ３１５に関し上述した様態で確認される。しかしながら、ＥＭＭに含まれるＥＡ改変情報４０３はＥＭＭマネジャー４０７に進み、ＥＭＭマネジャー４０７は、この情報を用いてＤＨＣＴ３３３内の登録エージェントに対する権限情報を改変する。改変の例は、登録オーソリティにより提供されたサービスの追加または取り消し、および所与のサービスのインスタンスへのアクセスが認められる条件の変更を含む。

【００６５】

上述のように、封印されたダイジェストは、登録エージェントのプライベート鍵を用いて暗号化される。その結果、ＤＨＣＴ３３３が登録エージェントの公開鍵を有している場合のみ、ＥＭＭの妥当性が決定され得る。登録エージェントに対する公開鍵は、ＥＡ割当てＥＭＭ４１３により条件付きアクセスオーソリティからＤＨＣＴ３３３に提供される。ＥＭＭ４１３は、条件付きアクセスオーソリティからの登録エージェント割当て情報４０９を含む。少なくとも、登録エージェント割当て情報４０９は、登録エージェントに対する公開鍵を含み、ＤＨＣＴ３３３内に登録エージェントが有しているメモリ量および登録エージェントが提供し得るサービスの種類に関する情報も含む。例えば、登録エージェントは、インタラクティブサービスを提供することは許可され得ない。情報４０９は、ＤＨＣＴ３３３の公開鍵３１２で暗号化され、封印されたダイジェストは、条件付きアクセスオーソリティのプライベート鍵４１１で暗号化される。

【００６６】

ＤＨＣＴ３３３では、ＤＨＣＴ３３３に属するプライベート鍵３３７を使用してＥＭＭ４１３が復号され、ＣＡＡの公開鍵４１５を使用して封印されたダイジェストが復号される。ダイジェストがＥＭＭのコンテンツの正しさを確証した場合、ＥＭＭマネジャー４０７は、公開鍵がＥＭＭ４１３に含まれる登録エージェントのための格納場所を割り当てる。これが済めば、ＥＭＭマネジャー４０７は、格納場所に登録エージェントの公開鍵を配置する。この格納場所は、登録エージェントの公開鍵、登録エージェントにより提供されたサービスおよびサービスインスタンスに対する権限情報、および登録エージェントにより提供されたＭＳＫを格納する場所を提供する。いったんＤＨＣＴ３３３が登録エージェントの公開鍵と、登録エージェントの権限情報およびＭＳＫに対する格納場所を有したら、ＥＭＭマネジャー４０７は、登録エージェントからのＥＭＭに応答できる。もちろん、封印されたダイジェストを復号するためには、ＤＨＣＴ３３３は、条件付きアクセスオーソリティに対する公開鍵４１５を有さなければならない。後により詳細に示すように、好適な実施形態では、公開鍵４１５と、ＤＨＣＴ３３３に対する公開鍵およびプライベート鍵とは、ＤＨＣＴ３３３が製造されるときにそのＤＨＣＴ３３３にインストールされる。

【００６７】

顧客がサービスを注文するとき、先述の取り決めが以下のようにインタラクトする。

１．顧客のＤＨＣＴ３３３が公開鍵を有さない登録エージェントによりサービスが提供された場合、条件付きアクセスオーソリティが、まずＤＨＣＴ３３３にＥＡ割当てＥＭＭ４１３を送信しなければならない。ＥＭＭマネジャー４０７は、登録エージェントのための

格納場所を割り当てることにより応答する。条件付きアクセスオーソリティのみがＥＡ割当てＥＭＭ４１３を送信し得、その結果、条件付きアクセスオーソリティ（ＣＡＡ）は、特定のサービス分配機関の顧客への登録エージェントによるアクセスを制御できる。
２．ＤＨＣＴ３３３が登録エージェントの公開鍵を有する場合、過去のある時点において、ステップ（１）が実行されているか、またはされたので、登録エージェントは、新規に注文されたサービスまたはサービスインスタンスとともに、改変ＥＭＭ４０５をＤＨＣＴ３３３に送信する。ＥＭＭマネジャー４０７は、権限情報を割り当てられたスペースに格納することにより、これに応答する。
３．いったんステップ（３）が完了したら、ＤＨＣＴ３３３は、登録エージェントからのサービスに対するＭＳＫとともにＥＭＭ３１５を受け取ることができる。ＥＭＭマネジャー４０７は、割当てスペース内にＭＳＫを格納する。
４．実際のサービスインスタンスが送信されるとき、現在の制御ワードを含むＥＣＭを伴う。ＥＣＭを復号するためにＭＳＫが使用され、サービスのインスタンスを復号するのに、ＥＣＭから獲得された制御ワードが使用される。

【００６８】

従って、サービスのインスタンスへのアクセスを制御するための、上述したＥＭＭおよびＥＣＭの使用は、条件付きアクセスオーソリティの許可なく登録エージェントがＤＨＣＴ３３３にアクセスできないことと、サービスに対する登録エージェントの許可がなくＤＨＣＴ３３３がサービスのインスタンスにアクセスできないこととを保証する。また、登録エージェントがサービスを完全に制御することも可能にする。サービスへのアクセスは、ＥＭＭ４０５および３１５により定義され、これらは、サービス分配機関から独立して、登録エージェントによりＤＨＣＴ３３３へ送信され得る。さらに、制御ワードを生成するのに使用されるＭＳＫを提供し、サービス分配機関およびＤＨＣＴ３３３の両方へのＥＣＭを復号するのは、登録エージェントである。実際、登録エージェントがそうしたいと欲せば、自身でサービス分配機関にサービスの暗号インスタンスを提供し得、そのような場合、サービス分配機関は、単に登録エージェントとＤＨＣＴ３３３との間の経路として機能する。

【００６９】

（返送経路を介したメッセージセキュリティ送信）

また、図４は、ＥＭＭの安全を確保する技術が、いかにしてＤＨＣＴ３３３から送信されたメッセージの安全をも確保するかを示している。図４に示す例は、転送購入メッセージである（ＦＰＭ）。転送購入メッセージは、サービスのインスタンスのインタラクティブな購入のために使用される。そのような購入の一例は、インパルス－ペイ－パー－ヴュー即ちＩＰＰＶと呼ばれるものである。そのようなシステムでは、例えば野球の試合などのイベントの始まりが一般的に放送され、顧客がすべてを観たいかどうかを決める。その場合、ＤＨＣＴ３３３にイベント全体を観たい旨を示す入力を提供しなければならない。ＥＭＭマネジャー４０７は、ＦＰＭを生成して登録エージェントに送信することにより入力に応答し、これにより、登録エージェントは、イベントに対して顧客に課金し、ＤＨＣＴ３３３がイベントを復号し続け得ることを確認するＥＭＭ３１５を送信する。登録エージェントにより必要とされる情報は、転送登録情報４１７である。顧客のプライバシーを確保するため、この情報は、３４３に示すように、３ＤＥＳアルゴリズムを使用し鍵４２０で暗号化されており、暗号化された転送登録情報４１９を提供する。鍵４２０は、２つの５６ビットＤＥＳ鍵で構成される。３ＤＥＳ暗号化処理は、３つのＤＥＳ処理のシーケンスである。即ち、第１のＤＥＳ鍵を使用した暗号化、第２のＤＥＳ鍵を使用した復号、および第１のＤＥＳ鍵を使用した暗号化である。次に、登録エージェントの公開鍵３３５を使用して鍵４２０が暗号化され、ＤＨＣＴ３３３のプライベート鍵を使用して封印されたダイジェストが生成される。これらの部分すべてが一緒になって、登録エージェントにアドレスする転送購入メッセージ４２１を構成する。

【００７０】

登録エージェントでは、登録エージェントのプライベート鍵３１０を使用して鍵４２０

が復号され、ＤＨＣＴの公開鍵３１２を使用して封印されたダイジェストが復号される。ＦＰＭ４２１に含まれる暗号化された転送登録情報（ＥＦＥＩ）４１９は、改竄されていないことを決定され、３ＤＥＳ復号４４３に渡される。３ＤＥＳ復号４４３は、鍵４２０を使用してことを復号し、転送登録情報４１７を登録エージェントに提供する。直ちに明白なように、メッセージのコンテンツの３ＤＥＳ暗号化を伴うか、または伴わずに、同一の技術が、ＤＨＣＴ３３３が公開鍵を有する任意のエンティティへメッセージを送信するのに使用され得る。少なくとも、これはＣＡＡとＤＨＣＴ３３３内に割り当てられた任意の登録エージェントとを含む。

【００７１】

（グローバル放送メッセージの認証）

グローバル放送メッセージは、任意の個別ＤＨＣＴ３３３またはＤＨＣＴ３３３の任意のグループにアドレスされないものである。好適な実施形態では、グローバル放送メッセージは、サービスのインスタンスを伴い、伴うインスタンスに相当する関連した情報を含む。その結果、グローバル放送メッセージに使用される暗号化および認証技術は、高速の復号および認証確認を可能にする。グローバル放送メッセージの一例はＥＣＭである。他の例は、様々なタイプのグローバル放送認証メッセージ、即ちＧＢＡＭである。ＥＣＭでは、グローバル放送メッセージがスプーフィングされるのを防ぐ必要があり、これはＥＣＭと同一の様態において為される。より詳細には、いくつかまたはすべてのＭＳＫをグローバル放送メッセージのコンテンツとともに使用してダイジェストが生成される。従って、ＭＳＫは、登録エージェントとＤＨＣＴ３３３との間で共有される秘密として機能する。グローバルメッセージを受信すると、ＥＭＭマネジャー４０７は、受け取ったメッセージのコンテンツおよびＭＳＫを使用してダイジェストを生成し、ダイジェストがメッセージに含まれるものと一致した場合のみ、受信されたメッセージに応答する。ＭＳＫにより生成されたダイジェストを使用してグローバル放送メッセージを認証することの利点は、ダイジェストが非常に迅速に生成かつ確認されることである。

【００７２】

（デジタル放送分配システムにおける条件付きアクセスシステムの実施）

以上、ＥＣＭ、ＥＭＭ、および他のメッセージの観点と、メッセージとそのダイジェストとが暗号化および復号される様態の観点とから、条件付きアクセスシステムを説明した。先述の条件付きアクセスシステムは、サービスのインスタンスがＥＣＭまたは他の放送メッセージとともにＤＨＣＴに伝達されることを許容し、ＤＨＣＴが条件付きアクセスオーソリティおよび１つ以上の登録エージェントからＥＭＭを受信することを許容する任意の通信取り決めにて機能する。しかしながら、条件付きアクセスシステムは、現代的デジタル広帯域幅伝達システムにおける使用に特によく適合し、以下、そのような伝達システムで条件付きアクセスシステムがいかに実施されるかを説明する。

【００７３】

（デジタル広帯域幅伝達システムの概観：図５）

図５は、デジタル広帯域幅伝達システム（ＤＢＤＳ）５０１の概観を提供する。ＤＢＤＳ５０１は、サービス基盤（ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）５０３、ヘッドエンド５１５、搬送５１７、ハブ５１９（０…ｎ）、アクセスネットワーク５２１（０…ｎ）、およびデジタルホーム通信端末（ＤＨＣＴ）３３３を含む。サービス基盤は、広帯域幅伝達システムにサービスを提供するシステムである付加価値サービスプロバイダ（ＶＡＳＰ）システム５０９、ＤＢＤＳ５０１により提供されるサービスを管理し制御するデジタルネットワークコントロールシステム（ＤＮＣＳ）５０７、ＤＢＤＳ５０１におけるサービス提供および権限情報のソースである管理ゲートウェイ（ＡＧ）５０５、システム状態および性能情報のデータベースを維持するネットワークマネジメントシステム（ＮＭＳ）５１１、および他のサービス基盤５０３の要素をヘッドエンド５１５に相互接続するコアネットワーク５１３を含む。好適な実施形態では、コアネットワーク５１３は、ＡＴＭベーススイッチングおよび送信機能を含む。ヘッドエンド５１５は、サービス基盤５０３と搬送基盤５１７との間のインターフェイスを提供する。搬送基盤５１７は、ヘッドエンド５１５

からハブ５１９（０…ｎ）までの高帯域幅相互接続を提供する。各ハブ５１９（ｉ）は、アクセスネットワーク５２１（ｉ）を提供し、アクセスネットワーク５２１（ｉ）は、同軸バスネットワークからＤＨＣＴ３３３に接続されるハイブリッドファイバ同軸（ＨＦＣ）ノード５２３を含む。従ってＤＢＤＳ５０１内の所与のＤＨＣＴ３３３（ｋ）は、アクセスネットワーク５２１（ｉ）内のＨＦＣノード５３２（ｊ）に属する。搬送基盤５１７およびアクセスネットワーク５２３は、ヘッドエンド５１５から所与のＤＨＣＴ３３３（ｋ）までの転送チャンネルのみ提供するが、好適には、転送チャンネルおよび返送経路の両方を提供し得る。ＤＢＤＳ５０１の各インスタンスは、一般的に、大都市圏でのサービスを提供する。

【００７４】

ＤＢＤＳ５０１は多様な構成で実施され得、特定のサービス環境の状況に適合する。例えば、ヘッドエンド設備がヘッドエンド５１５の中、ハブ５１９（ｉ）の中、またはＶＡＳＰシステム５０９の一部として配備され得る。ＤＮＣＳ要素５０６は、ヘッドエンド５１５の中に配備され得るか、またはハブ５１９の中に分配される。搬送基盤５１７は、ＳＯＮＥＴアド／ドロップ多重化、アナログファイバ技術、または他の搬送技術を利用し得る。

【００７５】

（条件付きアクセスシステムの概観：図６）

図６は、ＤＢＤＳ５０１における条件付きアクセスシステム６０１の好適な実施形態の要素を示す。条件付きアクセスシステム６０１は、一緒になってセキュリティおよび条件付きアクセスサービスを提供する要素ＤＮＣＳ５０７、ヘッドエンド５１５、およびＤＨＣＴ３３３の集合である。

【００７６】

条件付きアクセスシステム６０１の要素は、以下の機能を実行する。

１．サービスコンテンツの暗号化
２．サービス暗号化に使用される制御ワードの暗号化
３．暗号制御ワードに含まれるＥＣＭの認証
４．ＤＨＣＴへのＥＣＭ受け渡し
５．加入者権限データベースの管理
６．加入者登録情報を含むＥＭＭの暗号化および認証
７．ＤＨＣＴへのＥＭＭ受け渡し
８．ＥＭＭの復号およびＤＨＣＴにおけるその正当性の確認
９．ＤＨＣＴ内の権限情報を改変することによるＥＭＭへの応答
１０．ＥＣＭを認証し、制御ワードを復号し、ＤＨＣＴ３３３での登録を確認することによるＥＣＭへの応答
１１．ＥＣＭが正当であり、認証が許可された場合、サービスコンテンツの復号これらの要求は、条件付きアクセスシステム６０１下記の要素により満たされている。

【００７７】

ヘッドエンド５１５におけるストリーム暗号化およびＥＣＭストリーマモジュール６２０、

ＤＮＣＳ５０７における制御スイート（ｓｕｉｔｅ）６０７。

Ｉ．ＤＮＣＳ５０７へのセキュリティリンクを備えた、ヘッドエンド５１５におけるトランザクション暗号化装置６０５
ＩＩ．ＤＨＣＴ３３３におけるサービス復号器モジュール６２５
ＩＩＩ．ＤＨＣＴ３３３におけるセキュリティマネジャーモジュール６２６
ＩＶ．ＤＨＣＴ３３３におけるＤＨＣＴＳＥ６２７

図６は、ＤＢＤＳ５０１内でのセキュリティデジタルサービスのための、これらの要素の典型的な構成を示す。以下に、これらの要素をより詳細に説明する。

【００７８】

（サービス暗号化およびＥＣＭストリーマモジュール６２０）

サービス暗号化およびＥＣＭストリーマ（ＳＥＥＳ）モジュール６２０は、制御スイート６０７の命令下で動作するＱＡＭモジュール６１９の要素であって、サービスコンテンツ３２５を送信するための好適な実施形態に使用されるＭＰＥＧ－２トランスポートストリームパケットを暗号化する。図６に示すように、サービスコンテンツ３２５は、デジタル衛星分配システム６１３、デジタル地上波分配システム６１１、またはメディアサーバー６０９などのソースから受信され得る。メディアサーバー６０９は、高帯域幅内蔵ゲートウェイ６１５によりヘッドエンド５１５に接続され得る。ＳＥＥＳ６２０は、ＭＳＫ３０９を使用して、サービス暗号化に使用される制御ワード３１９を生成し、出力されるＭＰＥＧ－２トランスポートストリーム内の暗号サービスコンテンツ３２９とともに制御ワード３１９を搬送するためのＥＣＭ３２３を生成する。ＳＥＥＳ６２０は、ＭＳＫ３０９でＥＣＭ３２３内の制御ワードを暗号化する。ＭＳＫはＴＥＤ６０３により生成され、ＥＭＭなどのメッセージの暗号形式でＳＥＥＳ６２０に送信される。

【００７９】

（ＤＨＣＴ３３３）

ＤＨＣＴ３３３は、ＨＦＣネットワーク５２１と顧客のテレビションセットとの間に接続されている。ＤＨＣＴ３３３はＥＭＭ、ＥＣＭおよびＧＢＡＭを受信して解釈し、サービスのインスタンスを復号する。ＤＨＣＴ３３３は、ＤＢＤＳ５０１に対する顧客インターフェイスをさらに提供し、顧客から顧客入力６２８を受信する。顧客入力に応答して、ＤＨＣＴ３３３は、ＦＰＭか、またはＣＡＡまたはＥＡへの返送経路を介して伝わる他のメッセージを生成し得る。好適な実施形態では、ＤＨＣＴ３３３は、汎用プロセッサ、ＡＳＩＣ、およびセキュリティエレメント（独立して、または内蔵で実施され得る）の組み合わせを使用して実施される。本説明の目的では、ＤＨＣＴ３３３は３つの重要要素を有する。即ち、サービス復号器モジュール６２５、セキュリティマネジャー６２６、およびＤＨＣＴセキュリティエレメント（ＤＨＣＴＳＥ）６２７である。サービス復号器モジュール６２５は、好適にはＡＳＩＣにおいて実施され、セキュリティマネジャー６２６は、好適にはソフトウェアにおいて実施される。ＤＨＣＴＳＥ６２７はセキュリティエレメントであり、セキュリティおよび条件付きアクセス関連機能を実行する。

【００８０】

（サービス復号器モジュール６２５）

サービス復号器モジュール６２５は、暗号ＭＰＥＧ－２トランスポートストリームパケットを復号するＤＨＣＴ３３３の要素である。サービス復号器６２５は、サービス復号のために使用される制御ワードをＤＨＣＴＳＥ６２７から受信する。ＤＨＣＴＳＥ６２７は、認証されたサービスのための制御ワードをサービス復号器６２５に渡すことのみにより、どのトランスポートストリームパケットが復号されるのかを制御する。

【００８１】

（セキュリティマネジャー６２６）

セキュリティマネジャー６２６は、ＤＨＣＴのソフトウェアモジュールであり、条件付きアクセスシステムを使用するＤＨＣＴ３３３上で起動するアプリケーションと、ＤＨＣＴＳＥ６２７との間のインターフェイスを提供する。また、サービス復号器モジュールとＤＨＣＴＳＥ６２７との間の処理を統合する。

【００８２】

（ＤＨＣＴＳＥ６２７）

ＤＨＣＴＳＥ６２７は、鍵を格納し、ＥＭＭおよびＥＣＭを解釈し、ＦＰＭを生成する。ＥＭＭおよびＥＣＭにより、ＤＨＣＴＳＥ６２７は、解釈に必要な復号と認証とを行い、ＦＰＭにより、封印されたダイジェストを生成しＦＰＭを暗号化する。従って好適な実施形態では、ＥＭＭマネジャー４０７が、セキュリティエレメント６１７において実施される。さらに、ＤＨＣＴＳＥ６２７は、ＤＨＣＴ３３３上で実行する他のアプリケーションに対する暗号化、復号、ダイジェスト、およびデジタル署名サービスを行う。セキュリティエレメント（ＤＨＣＴＳＥ）６２７は、マイクロプロセッサと、マイクロプロセッサのみがアクセスするメモリを含む。メモリとマイクロプロセッサの両方は、改竄防止パッ

ケージに収容されている。ＥＭＭを解釈するにあたり、ＤＨＣＴＳＥ６２７は鍵および登録情報を獲得して格納し、ＥＣＭを解釈するにあたり、ＤＨＣＴＳＥ６２７は登録情報を使用して、ＥＣＭを受信するＤＨＣＴ３３３が、ＥＣＭを伴うサービスのインスタンスに対する登録を有するか否かを判定する。もしそうであれば、ＤＨＣＴＳＥ６２７はＥＣＭを処理し、サービスを復号またはスクランブル解除するのに使用し得る様態で、サービス復号器モジュール６２５へ制御ワードを供給する。さらにＤＨＣＴＳＥ６２７は、ＩＰＰＶなど衝動買い可能なサービスに対する情報の購入を記録し、転送購入メッセージを介して制御スイート６０７に首尾よくデータが転送されるまで、購入データを格納する。ＤＨＣＴＳＥ６２７は、ＥＡに対するＭＳＫと、ＤＨＣＴ３３３に対するプライベート／公開鍵の組と、条件付きアクセスオーソリティおよび登録エージェントの公開鍵を維持する。

【００８３】

（制御スイート６０７）

制御スイート６０７は、ソフトウェアのＤＮＣＳファミリーのメンバーである。制御スイート６０７は、ＤＮＣＳ放送制御スイート要素からの入力に基づいて、ＳＥＥＳモジュール６２０により実行されるサービスの暗号化を制御する。制御スイート６０７は、管理ゲートウェイ５１１から受け取るトランザクションに基づき、加入者権限のデーベースも維持する。制御スイート６０７はＥＭＭを生成し、ＤＨＣＴＳＥ６２７へ加入者権限および他の条件付きアクセスパラメータを通信する。制御スイート６０７は、登録エージェントの代わりとして働く。制御スイート６０７により生成され、ＤＨＣＴＳＥ６２７へ加入者権限および他の条件付きアクセスパラメータを通信するＥＭＭは、ＤＨＣＴ３３３の公開鍵で暗号化され、指示されてＥＡのプライベート鍵で認証される。ＥＡは、トランザクション暗号化装置（ＴＥＤ）６０３により維持される。ＤＨＣＴＳＥ６２７は、ＥＡの公開鍵を維持し、これを用いて、ＥＡに対する制御スイート６０７により生成されるＥＭＭの認証を確認する。

【００８４】

さらに制御スイート６０７は、条件付きアクセスオーソリティ（ＣＡＡ）の確立を可能にする。制御スイート６０７は、ＥＡの公開鍵をＤＨＣＴＳＥ６２７に渡すＥＡ割当てＥＭＭ４１３を生成する。これらのＥＭＭ４１３は上述のように暗号化されるが、ＴＥＤ６０３により維持されるＣＡＡのプライベート鍵で生成されたデジタル署名を使用して認証される。ＤＨＣＴＳＥ６２７は、ＣＡＡの公開鍵とともに予め提供され、これらのＥＭＭ４１３の正当性を確認する。

【００８５】

制御スイート６０７と残りの条件付きアクセスシステム６０１との間の通信は、ＬＡＮ相互接続装置６０５および６１７による。装置６０５は、制御スイート６０７を登録ゲートウェイ５０５に接続し、ここから、ＥＣＭおよびＥＭＭを生成するのに必要な情報を受け取る。装置６１７は、制御スイート６０７を、ＱＡＭ変調器内のＳＥＥＳモジュール６２０と、ＨＦＣネットワーク５２１に接続されるＱＰＳＫ変調器６２１およびＱＰＳＫ復調器６２３とに接続する。ＬＡＮ相互接続装置６１７、変調器６２１、復調器６２３、およびＨＦＣネットワーク５２１を介する制御スイート６０７とＤＨＣＴ３３３との間の接続は、ＦＰＭ４２１などのメッセージに対して必要な返信経路を実施し、ＤＨＣＴ３３３への送信チャンネルも実施する。この送信チャンネルは、サービスを提供するのに使用される送信チャンネルとは独立している。条件付きアクセスシステム６０１では、制御スイート６０７は、先述の送信チャンネルによるか、サービスのインスタンスとともに送信するかのいずれかにより、ＥＭＭまたは放送メッセージをＤＨＣＴ３３３に送信し得る。

【００８６】

（トランザクション暗号化装置６０３）

トランザクション暗号化装置（ＴＥＤ）６０３は、制御スイート６０７の周辺機器として機能する。ＴＥＤ６０３は、制御スイート６０７の命令のもと、ＥＭＭを含む様々な条件付きアクセスシステムメッセージを暗号化し封印されたダイジェストを生成する。ＴＥＤ６０３は、ＳＥＥＳ６２０によるＥＣＭの制御ワードの暗号化と、ＤＨＣＴＳＥ６２７

の制御ワードの復号とに使用される（ＭＳＫ）も生成する。さらに、ＴＥＤ６０３は、ＭＳＫを使用して条件付きアクセスシステムメッセージのグローバル放送メッセージ分類を認証する。認証は、メッセージのコンテンツをいくつかまたはすべてのＭＳＫとともにハッシュすることにより為される。ＴＥＤ６０３は、ＤＨＣＴ３３３から送信された転送購入メッセージ４２１および返送経路を使用して送信された他のメッセージを復号し、正当性を検証する。ＴＥＤ６０３はＣＡＡのプライベート鍵およびＥＡを維持し、メッセージを受信するＤＮＣＳからＤＨＣＴの公開鍵を受け取る。以下により詳細に説明するように、ＴＥＤ６０３は、各鍵の正当性を確認するソースからの公開鍵を受け取る。最後にＴＥＤ６０３は、ＣＡＡおよびＥＡのプライベート鍵を使用して、ＥＭＭに適合するように、ＥＭＭの封印されたダイジェストを生成する。

【００８７】

（ＤＨＣＴ３３３またはサービス基盤５０７において実行するサービスおよびプログラムのサポートへの条件付きアクセスシステムの使用）

条件付きアクセスシステムは、サービスの提供を確保し、ＤＨＣＴ３３３上で実行するプログラムまたは制御スイート６０７内のプログラムにセキュリティサービスを提供し得る。セキュリティサービスの提供は、サービスをサポートするＤＨＣＴプログラムが安全であることを必要としない。この理由は、ＤＨＣＴ３３３内のＤＨＣＴＳＥ６２７またはＴＥＤ６０３のみにより、以下が行われ得るからである。

【００８８】

・ＭＳＫの生成

・ＭＳＫの格納

・ＥＭＭの暗号化および／または復号と、封印されたダイジェストの確認に必要な鍵の格納

・ＥＡより受信された登録情報の格納

・ＥＭＭの暗号化および／または復号

・制御ワードの暗号化または復号

・ＳＥＥＳモジュール６０７へのＭＳＫの提供と、サービス復号器モジュール６２５への復号された制御ワードの提供

・共有された秘密でのダイジェストの生成および確認

・封印されたダイジェストの生成および確認

・ＤＨＣＴ３３３がサービスを受信するよう登録されていることの確認

ＤＨＣＴ３３３上で実行するプログラム、または制御スイート６０７内のプログラムは、ＤＨＣＴＳＥ６２７またはＴＥＤ６０３に格納された任意の情報へのアクセスを有さず、従って、ＤＨＣＴＳＥ６２７またはＴＥＤ６０３にＥＭＭおよびＥＣＭの生成または解釈を尋ねる以外は、ＥＭＭおよびＥＣＭと関係ない。例えば、ＤＨＣＴ３３３がＥＭＭを受け取るとき、ＤＨＣＴＳＥ６２７に処理のためにＥＭＭを渡すだけである。ＥＣＭを受け取るときも、同様のことを行う。ＥＣＭに含まれ、ＤＨＣＴＳＥ６２７に格納される権限情報が、ＤＨＣＴ３３３がサービスに登録していることを示す場合、ＤＨＣＴＳＥ６２７は、サービス復号モジュール６２５に復号された制御ワードを提供する。

【００８９】

条件付きアクセスシステムは、一般的にプログラムに対する安全確認も行う。例えば、サーバーアプリケーションからダウンロードされた情報を必要とするＤＨＣＴ３３３上で実行するプログラムは、情報がダウンロードされる前に封印されたダイジェストが添付されたことを予測し得、プログラムは、ＤＨＣＴＳＥ６２７を使用して封印されたダイジェストを確認し、情報が正当であるかを判定し得るが、ＤＨＣＴＳＥ６２７が情報を正当でないと示したときに、その情報をどう処理するかを決定するのはプログラム次第である。

【００９０】

（条件付きアクセスシステム６０１におけるメッセージの詳細）

条件付きアクセスシステム６０１では、ＥＣＭ、ＥＭＭ、ＦＰＭ、およびＧＢＡＭがすべて、異なるタイプの条件付きアクセスメッセージである。条件付きアクセスメッセージ

はすべて、共通の形式、即ちヘッダと、メッセージ自体と、メッセージ認証符号、即ちＭＡＣを有する。ヘッダは以下の情報を含む。

【００９１】

・メッセージのタイプ、即ち、ＥＣＭ、ＥＭＭ、ＧＢＡＭ、それ以外のいずれであるか

・メッセージの長さ

・条件付きアクセスシステムに対する識別子

・メッセージの暗号化およびコンテンツの認証を含む、メッセージに使用されるセキュリティアルゴリズムのタイプの識別子

・メッセージコンテンツの長さ

ヘッダは、暗号化されたメッセージおよびＭＡＣをその後に伴い、ＭＡＣは、メッセージのタイプにより、封印されたダイジェストか、またはメッセージに伴うＭＳＫのいくつかまたはすべてにより生成されるダイジェストであり得る。

【００９２】

デジタル広帯域幅伝達システム５０１では、ＣＡメッセージが、ＭＰＥＧ－２データストリーム内、またはＩＰパケット内のいずれかを伝わる。ＩＰパケットは、インターネットプロトコルの規則に従い生成されたパケットである。また、ＡＴＭなどの他のトランスポートプロトコルも使用し得る。好適な実施形態では、制御スイート６０７からＤＴＣＨ３３３へのメッセージは、ＭＰＥＧ－２内またはＩＰパケット内を伝わる。ＤＨＣＴ３３３から制御スイート６０７メッセージは、ＱＰＳＫ復調器６２３およびＬＡＮ相互接続装置６１７により提供される返送経路上のＩＰパケットに従って伝わる。一般的に、ＥＣＭおよびＧＢＡＭなど、サービスの特定のインスタンスに密接に関連するＤＨＣＴ３３３へのメッセージは、ＭＰＥＧ－２データストリーム内を伝わる。ＥＭＭは、ＭＰＥＧ－２トランスポートストリーム内か、またはＱＰＳＫ変調器６２１およびＬＡＮ相互接続装置６１７により提供されるＩＰパケットに従って伝わる。

【００９３】

（ＭＰＥＧ－２トランスポートストリーム内のＣＡメッセージ：図７）

図７は、ＭＰＥＧ－２トランスポートストリーム７０１の模式図である。ＭＰＥＧ－２トランスポートストリームは、１８８バイト長のトランスポートパケット７０３のシーケンスで生成される。ストリーム内のパケット７０３は、ＤＨＣＴ３３３と結合されるとき、サービスのインスタンスと、所与のＤＨＣＴ３３３からサービスへのアクセス権を決定する情報を搬送する。情報には２つの広いカテゴリが存在する。実際の映像および音声を生成するのに必要なプログラム７０９、およびプログラム特定情報（ＰＳＩ）７１１である。ＰＳＩ７１１は、トランスポートストリームがネットワークにいかに送られるべきか、プログラム７０９がいかにパケット化されるか、およびプログラム７０９へのアクセスを制限するのにどのデータが使用されるか、などの事項に関する情報である。これらの広いカテゴリのそれぞれは、複数の下位のカテゴリを有する。例えば、プログラム７０９は、ビデオ情報と、オーディオ情報のいくつかのチャンネルとを含み得る。

【００９４】

各トランスポートパケット７０３は、パケット識別子、即ちＰＩＤを有し、所与の下位のカテゴリに対する情報を搬送するパケット７０３のすべては、同一のＰＩＤを有する。従って、図７では、パケットトランスポートビデオＩはすべて、ＰＩＤ（ａ）を有し、その下位のカテゴリに属するパケットは７０５（ａ）により識別される。同様に、オーディオＩを搬送するパケットはすべて,

ＰＩＤ（ｂ）を有し、そのカテゴリに属するパケットは７０５（ｂ）により識別される。このように、情報の下位のカテゴリは、そのパケットの識別子により識別される。出力パケット７０７に示すように、ＭＵＸ７０４からの出力は、様々な下位のカテゴリからの、隣接する個々のパケットのシーケンスであるるすべてのＭＰＥＧ－２トランスポートストリーム７０１の任意の部分が暗号化され得るが、パケットヘッダおよび順応（ａｄａｐｔａｔｉｏｎ）フィールドは、決して暗号化されない。好適な実施形態では、プログラム７０９を構成するパケットの組は、制御ワードを鍵として、ＤＥＳアルゴリズムに従い暗号

化される。

【００９５】

下位のカテゴリのうち２つは特別である。ＰＩＤ０（７０５（ｅ））およびＰＩＤ１７０５（ｃ））により識別されるものは、サービスに関連する他のパケットを列挙し、任意のサービスに関連した情報をすべて発見するのに使用され得る。ＰＩＤ１　７０５（ｃ））のパケットは、そのコンテンツとして、ＥＭＭを含む他のパケットのＰＩＤを列挙する条件付きアクセステーブルを有する。そのようなパケットの一組は、ＣＡＴ７１０からパケット７０５（ｄ）への→により示されるＥＭＭパケット７０５（ｄ）として表される。パケット７０５（ｄ）内の各パケット７０３は、プライベート情報、即ち条件付きアクセスシステム６０１の秘密とされる情報を含む。以下により詳細に説明するように、本発明の目的では、プライベート情報７１３は、ＣＡメッセージのシーケンスであって、それぞれがＥＭＭを含んでおり、プライベート情報７１９は、メッセージのシーケンスであって、それぞれがＥＣＭを含んでいる。

【００９６】

ＰＩＤ（７０５（ｅ））パケットは、特定のサービスのインスタンスに関連するパケットのＰＩＤを列挙するプログラム関連テーブルを含む。そのようなパケット組の１つが、プログラムマップパケット７０５（ｆ）であり、プログラムに対するＥＣＭを含むトランスポートパケット７０３のＰＩＤをとりわけ列挙するプログラムマップテーブル７１７を含む。そのようなパケットの組の１つを、７０５（ｇ）において示す。トランスポートパケットのそれぞれがプライベート情報７１９を含み、それは、この場合、それぞれがＥＣＭを含むＣＡメッセージのシーケンスである。

【００９７】

図８は、トランスポートパケット７０３の中をＥＭＭがいかにして搬送されるかの詳細である。パケット内のペイロードスペース７１９が、ＣＡ＿ＰＲＩＶＡＴＥ＿ＳＥＣＴＩＯＮ層８０３からのデータを搬送し、続いて、ＣＡメッセージ８０５のシーケンスを含む。ＣＡメッセージ８０５のそれぞれはＥＭＭ８０７を含む。ＥＣＭを搬送するパケット７０５（ｇ）の組では、ＭＳＫを鍵として３ＤＥＳアルゴリズムを使用し、ＥＣＭ内の制御ワードが暗号化される。ＥＭＭを搬送するパケット７０５（ｄ）の組では、意図されるＤＨＣＴ３３３の公開鍵を使用してＥＭＭが暗号化される。直ちに明らかなように、上述の技術は、任意のＣＡメッセージ８０５をＭＰＥＧ－２トランスポートストリームの一部として送信するのに利用し得る。

【００９８】

（ＣＡメッセージをＩＰプロトコルパケットにマッピング：図９）

図９は、ＬＡＮデバイス６１７、ＱＰＳＫ変調器６２１および復調器６２３を介して制御スイート６０７とＤＨＣＴ３３３との間で通信するために使用されるインターネットプロトコル（ＩＰ）パケットに、ＥＭＭがどのようにマッピングされるのかを示す。ＩＰパケット９０３は、単にヘッダおよびペイロードからなる可変長パケットである。ヘッダは、パケットのためのソースおよびデスティネーションＩＰアドレスを含む。ＥＭＭの場合、ソースアドレスは、ＣＡまたはＥＡのＩＰアドレスであり、そしてデスティネーションアドレスは、ＤＨＣＴ３３３のＩＰアドレスである。好ましい実施態様において、ＤＨＣＴ３３３のＩＰアドレスは、そのシリアル番号を使用して構築される。ＤＢＤＳ５１におけるＩＰアドレスは、ＨＦＣノード５２３によって区切られる。ＩＰパケットのペイロードは、ユーザデータグラムプロトコル（ＵＤＰ）に属するパケット９０５であり、パケット９０５は、そのペイロードとしてＣＡ＿ＰＲＩＶＡＴＥ＿ＳＥＣＴＩＯＮ８０３を含み、ＣＡ＿ＰＲＩＶＡＴＥ＿ＳＥＣＴＩＯＮ８０３は、ＣＡメッセージ８０５のシーケンスを含む。ＣＡメッセージ８０５の各々は、ＥＭＭ８０７を含む。

【００９９】

（ＥＣＭ構造の詳細：図１０）

図１０は、ＥＣＭ１００８の構造の詳細を示し、そしてＥＣＭ１００８からＭＰＥＧ－２転送パケット７０３のセット７０５（ｅ）へのマッピング１００１を示す。上記のよう

に、ＣＡ＿ＰＲＩＶＡＴＥ＿ＳＥＣＴＩＯＮ８０３のデータは、同じＰＩＤを有する１組のＭＰＥＧ－２転送パケット７０３において転送される。そのデータは、秘密セクション８０３のためのヘッダ１００３およびＣＡメッセージ８０５のシーケンスである。ＣＡメッセージ８０５の各々は、ＣＡメッセージヘッダ１００５、ＣＡ ＥＣＭメッセージ１００７、およびＥＣＭ ＭＡＣ１０１３を含む。ＣＡ ＥＣＭメッセージ１００７およびＥＣＭ ＭＡＣ１０１３は一緒になってＥＣＭ１００８を構成する。

【０１００】

図１０はまた、どのように制御ワードがＥＣＭ１００８において保護されるか、およびどのようにＥＣＭ ＭＡＣ１０１３が生成されるかを示す。鍵としてＭＳＫを使用して制御ワードは、３ＤＥＳ暗号化を使用して暗号化されるか、または３ＤＥＳ暗号化を使用してカウンタ値を暗号化することによって作成されるかのいずれかであるランダムな値である。いずれの場合においても、好ましい実施態様は、２つの５６ビットＤＥＳ鍵から構成されるＭＳＫを必要とし、そして３ＤＥＳ暗号化演算は、３つのＤＥＳ演算のシーケンスである：第１ＤＥＳ鍵を使用する暗号化、第２ＤＥＳ鍵を使用する復号化、および第１ＤＥＳ鍵を使用する暗号化である。制御ワードも、偶数または奇数のパリティを有し得る。１０１３に示されるように、（適切な暗号化後の）奇数制御ワードは、ＥＣＭ＿ｅｎｔｉｔｌｅｍｅｎｔ＿ｕｎｉｔ＿ｍｅｓｓａｇｅ１０１１の一部となり、そして非暗号化の形態でいくつかまたはすべてのＭＳＫと一緒に、ＭＤ５一方向ハッシュ関数入力として使用され、ＥＣＭ ＭＡＣ１０１３を生成する。同じ手順が、偶数パリティ制御ワードを用いて使用される。ＥＣＭ＿ｅｎｔｉｔｌｅｍｅｎｔ＿ｕｎｉｔ＿ｍｅｓｓａｇｅ１０１１の制御ワード以外の内容は、以下でより詳細に検討される。

【０１０１】

（ＥＭＭ構造の詳細：図１１）

図１１は、ＥＭＭ１１１２を含むＣＡメッセージ８０５を示す。ＣＡメッセージ８０５は、ヘッダ１００３、ＣＡ ＥＭＭメッセージ１１０１、および封印ダイジェスト１１０３を有する。ＣＡ ＥＭＭメッセージ１１０１は、ＣＡ ＥＭＭメッセージヘッダ１１０５、ＥＭＭメッセージ１１０７、およびＣＲＣエラー検出コード１１０９からなる。ＥＭＭメッセージ１１０７は、ＥＭＭヘッダ１１１３およびＥＭＭ＿ｉｎｓｉｄｅ＿ｄａｔａ１１１５を含む。ＥＭＭ＿ｉｎｓｉｄｅ＿ｄａｔａ１１５は、対象となるＤＨＣＴ３３３の公開鍵を使用して暗号化される。暗号化されたデータは、ＥＭＭデータ１１２９であり、パディング１１２７と一緒にＥＭＭ＿ｉｎｓｉｄｅ＿ｈｅａｄｅｒ１１２３およびＥＭＭ ｃｏｍｍａｎｄ＿ｄａｔａ１１２５から構成される。ＥＭＭデータ１１２９はまた、ＭＤ５一方向ハッシュ関数に入力されてＥＭＭ ＭＡＣ１１１９を生成し、そして封印ダイジェスト１１０３は、ＥＭＭ＿ｓｉｇｎｉｎｇ＿ｈｅａｄｅｒ１１１７、ＥＭＭ ＭＡＣ１１１９、ＥＭＭ＿ｓｉｇｎｉｎｇ＿ｈｅａｄｅｒ１１１７、およびパディング１１２１をそれがどのようなＥＭＭであるかに依存して登録エージェントまたは条件付アクセスオーソリティのいずれかの公開鍵を用いて暗号化することによってなされる。

【０１０２】

ＥＭＭ＿ｓｉｇｎｉｎｇ＿ｈｅａｄｅｒは、ＥＭＭ＿ｉｎｓｉｄｅ＿ｈｅａｄｅｒからの情報である。この情報は、特に機密であり、そしてしたがってデジタル署名するためには、プライバシーの理由からＤＨＣＴ３３３の公開鍵、および登録エージェントまたは条件付アクセスオーソリティの公開鍵の両方によって暗号化される。受信の際、およびプライバシー復号化の後、署名検証が失敗した場合、ＥＭＭは、ＤＨＣＴ３３３によって棄却される。この情報に含まれているのは、条件付アクセスシステムのためのＩＤ、ＣＡメッセージのタイプ、ＤＨＣＴのＤＨＣＴＳＥ６２７におけるマイクロプロセッサのシリアル番号、ＥＭＭのソースであるＣＡＡまたはＥＡのための識別子、ＤＨＣＴ３３３のセキュリティエレメントにおけるＣＡＡのための３つの公開鍵のどれが封印ダイジェストを復号化するために使用されるかの表示、およびＥＭＭのフォーマットの表示である。ＥＭＭ ｃｏｍｍａｎｄ＿ｄａｔａ１１２５の内容は、ＥＭＭを使用して行われる演算の議論においてより詳細に説明される。

【０１０３】
（ＤＨＣＴＳＥ６２７の詳細：図１２～１４）
ＤＨＣＴＳＥ６２７は、条件付アクセスシステム６０１において５つの主要な機能を有する。
・ＤＨＣＴ３３３のための公開およびプライベート鍵、ＣＡＡのための公開鍵、ＥＡのための公開鍵（サービスを受信ためにＤＨＣＴ３３３がＥＡから認証される）、およびこれらのＥＡによって提供されるＭＳＫを含む鍵を安全に格納する。
・ＥＡによって送信された登録情報を安全に格納する。
・復号化し、認証し、そしてＥＭＭに応答する。
・ＥＣＭにおける制御ワードを復号化し、ＥＣＭを認証し、そしてＥＣＭが属するサービスインスタンスを受信するためにＤＨＣＴ３３３が認証された場合に、制御ワードをサービス復号化器６２５に提供する。
・暗号化、復号化、および認証サービスをＤＨＣＴ３３３上で実行するアプリケーションに提供する。
【０１０４】
ＤＨＣＴＳＥ６２７は、ＲＳＡ暗号化および復号化を行うための専用ハードウェアであるマイクロプロセッサ（ＤＥＳを行い得る）、およびセキュリティメモリエレメントを含む。ＤＨＣＴＳＥ６２７のコンポーネントのすべては、パッケージ内に含まれる情報にアクセスしようとする際にその情報が破壊されるようなパッケージなどの単一の不正改変防止パッケージ中に含まれる。ＤＨＣＴＳＥ６２７のコンポーネントだけがセキュリティメモリエレメント中に格納された情報にアクセスする。ＤＨＣＴＳＥ６２７のいずれの部分にアクセスしようとするユーザのいずれの試みもＤＨＣＴＳＥ６２７を使用不可にし、そしてその内容を読み出し不可にする。ＤＨＣＴＳＥ６２７は、ＤＨＣＴ３３３の一体部分であり得るか、または「スマートカード」などのユーザインストール可能なモジュール中に含まれ得る。ユーザは、モジュールをＤＨＣＴ３３３中にインストールすることによってＤＨＣＴ３３３を「自分用」にする。
【０１０５】
図１２は、ＤＨＣＴＳＥ６２７のコンポーネントの概略を提供する。示されるように、ＤＨＣＴＳＥ６２７のコンポーネントはすべて、バス１２０５に接続される。インターフェース１２０３に始まって、アプリケーションがＤＨＣＴ３３３において実行する汎用プロセッサへ、インターフェース１２０３は、ＤＨＣＴ３３３の残りのコンポーネントとＤＨＣＴＳＥ６２７との間のデータの転送を許可するが、ＤＨＣＴ３３３の残部におけるコンポーネントがＤＨＣＴＳＥ６２７におけるメモリ中の秘密の値を有する内容をアドレッシングおよび読み出しすることを許可しない。マイクロプロセッサ１２０１は、暗号化、復号化、および認証を行い、そしてＥＭＭおよびＥＣＭをインタープリタするためのコードを実行する；ＲＳＡハードウェア１２１７は、ＲＳＡ暗号化および復号化に関係する演算を行う専用ハードウェアである。メモリ１２０７は、マイクロプロセッサ１２０１によって実行されるコード、鍵、および登録情報を含む。好ましい実施態様において、メモリ１２０７において２種類の物理的なメモリが存在する：ＤＨＣＴＳＥ６２７が製造される時に、内容が固定される読み出し専用メモリであるＲＯＭ１２１９、および通常のランダムアクセスメモリのように読み出しおよび書き込みが可能であるが、ＤＨＣＴＳＥ６２７が電源を切られた場合でも電流値を維持する不揮発性メモリ（ＮＶＭ）１２０９。不揮発性メモリ１２０９は、１９９５年４月３日付け出願の米国特許第５，７４２，６７７号、Ｐｉｎｄｅｒら、Ｉｎｆｏｒｍａｔｉｏｎ Ｔｅｒｍｉｎａｌ Ｈａｖｉｎｇ Ｒｅｃｏｎｆｉｇｕｒａｂｌｅ Ｍｅｍｏｒｙにおいて記載されるように、１組の不揮発性格納セル（ＮＶＳＣ）１２１１（０．．ｎ）として構成される。
【０１０６】
以下により詳細に説明されるように、マイクロプロセッサ１２０１において実行するコードは、ＮＶＳＣ１２１１を登録エージェントに動的に割り当てる。好ましい実施態様において、ＮＶＭ１２０９は、ＥＭＭによって再書き込みされ得る情報の格納のために使用

され、そしてＲＯＭ１２１９は、ＤＨＣＴＳＥ６２７がつぶれるまで変化し得ないコードのために使用される。

【０１０７】

図１３は、ＤＨＣＴＳＥ６２７中のメモリ１２０７の内容の模式的概略である。メモリは、２つの主要部分に分けられる：ＥＭＭのインタープリテーションの結果で変化しないコードおよび他の情報を含む読み出し専用格納部１３０１、およびＥＭＭのインタープリテーションの結果で変化する不揮発性格納部であるＮＶＡ格納部１３０３である。ＲＯ格納部１３０１は、コード１３０５を含む。

【０１０８】

コード１３０５は、４つのカテゴリに分けられる：ＤＨＣＴＳＥ６２７によって行われる暗号化、復号化、および認証の演算のためのコード１３０７、ＥＭＭ１３１３をインタープリタするためのコード、ＥＣＭ１３２１をインタープリタするためのコード、およびＦＰＭおよびＧＢＡＭなどのほかのＣＡメッセージを取り扱うためのコードである。コード１３０７は、ＭＤ５一方向ハッシュアルゴリズムのためのコード１３０８、ＲＳＡ公開鍵アルゴリズムのためのコード１３０９、および３ＤＥＳアルゴリズムのためのコード１３１１を含む。ＥＭＭコード１３１３は、３つのクラスに分けられる：条件付アクセスオーソリティから受信されるＥＭＭをインタープリタするコード１３１５、登録エージェントがＣＡＡから受信する格納割り当てを構成するために登録エージェントによって使用されるＥＭＭをインタープリタするコード１３１７、およびＭＳＫおよび登録を含むＥＭＭをインタープリタするコード１３１９である。このようにコード１３１５、１３１７および１３１９は、好ましい実施態様において、ＥＭＭマネージャ４０７を実施する。ＥＣＭ１３２１をインタープリタするためのコードは、ＥＣＭに含まれる制御ワードを復号化し、そしてＤＨＣＴ３３３がＥＣＭのともなうサービスのインスタンスにアクセスすることが許可されるかどうかをチェックし、そうである場合、その復号化された制御ワードをサービス復号化モジュール６２５に提供する。他のＣＡメッセージ１３２３のためのコードは、ＦＰＭおよびＧＢＡＭなどのメッセージを扱う。

【０１０９】

ＮＶＡ格納部１３０３は、２つの主コンポーネントを有する：管理格納部１３３０およびＥＡ格納部１３３１である。管理格納部１３３０は、ＤＨＣＴ鍵１３２５、ＣＡＡ鍵１３２９、およびＣＡＡデータ１３３０を含む。まずＤＨＣＴ鍵１３２５の場合、各ＤＨＣＴ３３３は、２つの公開－プライベート鍵ペアを有する。ペアの１つの公開鍵は、ＤＨＣＴ３３３に送信されたＥＭＭを暗号化するために使用される公開鍵として機能し、そしてプライベート鍵は、メッセージを復号化するためにＤＨＣＴ３３３において使用される；ペアの他方のプライベート鍵は、ＤＨＣＴ３３３によって送信されたメッセージの封印ダイジェストを暗号化するために使用され、そして公開鍵は、ＤＨＣＴ３３３から受信されたメッセージの封印ダイジェストを復号化するために他のネットワークエレメントによって使用される。鍵のペアは、ＤＨＣＴＳＥ６２７が製造される時に、ＤＨＣＴＳＥ６２７中にインストールされる。

【０１１０】

好ましい実施態様において、ＤＨＣＴ３３３の製造者は、各ＤＨＣＴのシリアル番号とともにそれに属する公開鍵のペアを有する証明されたデータベースを維持する。ＣＡＡまたはＥＡが、ＥＭＭをＤＨＣＴ３３３に送信を開始することを望む場合、ＤＨＣＴのシリアル番号とともにメッセージを制御スイート６０７に送信する。制御スイート６０７は、ＤＨＣＴ３３３の製造者によって維持されるデータベースからＤＨＣＴのための公開鍵をリクエストすることによってリクエストに応答する。データベースは、ＤＨＣＴのための公開鍵の証明されたコピーを制御スイート６０７に送信することによってメッセージに応答する。このように製造者は、鍵のための証明オーソリティとして機能する。制御スイート６０７は、自分自身のデータベース中に公開鍵を格納する。鍵証明についての詳細については、Ｓｃｈｎｅｉｅｒ、上記、４２５～４２８頁を参照のこと。製造者からＤＨＣＴのための公開鍵を得ることは、２つの利点が有る：第一に、それが、鍵を証明する問題を

解決すること；第二に、公開鍵がＤＨＣＴ３３３からではなく製造者から来るので、条件付アクセスシステム６０１において、ＤＨＣＴ３３３が制御スイート６０７へのパスを有する必要がないことである。

【０１１１】

ＣＡＡ鍵１３２９は、条件付アクセスオーソリティのための公開鍵である。好ましい実施態様において、ＣＡＡ鍵１３２９は、条件付アクセスオーソリティのための３つの公開鍵を含む。これらの鍵は、ＤＨＣＴＳＥ６２７が製造される時に、初めからインストールされるが、以下により詳細に説明されるように、ＥＭＭに応答して変更され得る。ＣＡＡデータ１３３０は、ＥＡ格納部１３３１を管理するさいにＣＡＡによって使用されるパラメータ、およびマップを含む。そのマップは、特定の登録エージェントに属するＮＶＳＣを８ビットの名前にマッピングし、そしてそれによってＣＡＡおよび登録エージェントが名前によってＮＶＳＣ１２１１を操作することを可能にする。

【０１１２】

登録エージェント１３３１は、各登録エージェントごとにＥＡ情報１３３１を有し、そのＥＡ情報から、ＤＨＣＴＳＥ６２７を含むＤＨＣＴ３３３は、サービスを得ることができる。ＣＡＡは、ＥＭＭを使用して登録エージェントのためのＮＶＳＣ１２１１を割り当て、そして次にその登録エージェントは、ＥＭＭを使用してその登録エージェントの情報１３３３の内容を設定する。

【０１１３】

図１４は、好ましい実施態様においてＮＶＳＣ１２１１がどのようにＥＡ格納部１３３１に組織化されるのかを示す。２種類のＮＶＳＣ１２１１が存在する：１４０５で示されるような「細型」ＮＶＳＣ、および１４０９で示されるような「太型」ＮＶＳＣである。太型ＮＶＳＣは、多くの細型ＮＶＳＣから構成される。３つのＣＡＡ公開鍵を含む格納部１４０３はまた、２つのポインタを含む：１つは、１４０２であり、割り当てされていない細型ＮＶＳＣのフリーリスト１４０７を指し、そして他方は、１４０４であり、割り当てされた太型ＮＶＳＣ１４０９の登録エージェントリスト１４０６を指す。各登録エージェントごとにそのような太型ＮＶＳＣ１４０９（ｉ）が存在し、そこからＤＨＣＴ３３３は、サービスを受信し得る。これらのＮＳＶＣ１４０９（ｉ）の各々はまた、細型ＮＶＳＣ１４０５、太型ＮＶＳＣ１４０９、またはその両方の組み合わせであり得るＮＶＳＣのリスト１４１１を有する。所定のＮＶＳＣ１４０９（ｉ）およびその細型ＮＶＳＣリストは、ＥＡのためのＥＡ情報１３３３（ｉ）を構成する。太型ＮＶＳＣ１４０９は、ＥＡ記述子である。１３３３（ｉ）で示されるように、細型ＮＶＳＣ１４１１は、登録エージェントによって提供されるサービスのための情報を含む。その情報は、サービスのためのＭＳＫ、登録情報のビットマップ、およびＩＰＰＶなどのインタラクティブなサービスのために必要な情報などである。

（ＮＶＡ格納部１３０３の制御）

好ましい実施態様において、ＮＶＳＣ１２１１の割り当ておよび割り当て解除は、最終的にＣＡＡまたはＤＨＣＴＳＥ６２７のいずれかによって制御され得る。ＣＡＡが割り当ておよび割り当て解除を制御する場合、ＣＡＡは、通常ＤＢＤＳ５０１のオペレータの役割をするが、登録エージェントの各々と交渉し、そしてその登録エージェントのための種々のタイプのＮＶＳＣの割り当てに同意する。ＥＡ管理コード１３１７は、登録エージェントからのＥＭＭをインタープリタする際に、その登録エージェントが自分に割り当てられたＮＶＳＣよりも多くの各タイプのＮＶＳＣを使用しないことを確実にするようにチェックする。

【０１１４】

ＤＨＣＴＳＥ６２７は、ＮＶＡ格納部１３０３を制御する場合に、ＣＡＡのオペレータは、サービスプロバイダと交渉し、そして提供されるサービスのために必要な格納の割り当てに同意する。次に、ＣＡＡは、暗号化されたメッセージを登録エージェントに送信する。暗号化されたメッセージは、データタイプに基づいた割り当てを含み、そして登録エージェントは、サービスプロバイダが交渉されたものよりも多くのリソースを要求するこ

とを抑制する。にもかかわらず、ＤＨＣＴＳＥ６２７がＮＶＡ１３０３において利用可能なものを超える格納領域の要求を受信する場合、ＤＨＣＴＳＥ６２７は、ユーザインターフェースを介して、さらなる格納は利用可能でないことを示し、そしてユーザにいくつかのサービスプロバイダリソースを除去するか、またはその要求を取り消すかのいずれかをＤＨＣＴ３３３ユーザに要求する。

【０１１５】

（ＥＭＭによって規定される動作の詳細）

以下に、ＥＭＭによって規定される動作の例を与える。動作は、ＣＡＡ公開鍵の変更で始まり、ＤＨＣＴＳＥ６２７においてＥＡを確立を介し、そして放送、イベント、およびインタラクティブサービスで終了する。好ましい実施態様において、１つのＣＡＡは、ＥＡ格納部１３３１の登録エージェントへの割り当てを制御する。他の実施態様において、１つより多いＣＡＡが存在し得る。２種類の登録情報が存在する：放送サービスのためのものおよびインタラクティブサービスのためのものである。放送登録のための格納は、インタラクティブ登録のためのものよりもより恒久的である。

【０１１６】

ＤＨＣＴＳＥ６２７におけるメモリ１２０７の量には、限度がある。ＣＡＡは、この不十分なリソースを管理し、そしてそれを登録エージェントに割り当てる。ＤＨＣＴ３３３は、登録エージェントからサービスを受信する。異なるＥＡは、必要に応じて、異なる量の格納領域を割り当てられ得る。ＥＡは、一旦ＣＡＡからの割り当てを受信したら、ＣＡＡによって規定される限度内に格納領域を構成し得る。異なるＥＡは、異なる限度および異なる種類の限度を有し得る。極端な場合、ＣＡＡは、ＥＡがそのＥＡ情報１３３３において有し得るＮＶＳＣ１２１１の総数を限定するだけである。ＣＡＡは、ＮＶＳＣ１２１１のタイプおよび／または各タイプの数を制限することによってより厳しい限定を課し得る。このように、ＣＡＡは、ＥＡが特定種類のサービスを提供することを抑制し、そしてそのような提供されるサービスの量、すなわちそのようなサービスが提供される時間の量を制限し得る。

【０１１７】

ＣＡＡは、ＥＡのために太型および細型ＮＶＳＣ１２１１を割り当てる場合に、各割り当てられるＮＶＳＣ１２１１に「名前」を与える、すなわち、ＮＶＳＣ１２１１は、８ビット識別子などの識別子を有する。ＣＡＡは、ＮＶＳＣ１２１１を割り当てたＥＡとその識別子を関連づける。ＣＡＡおよびＥＡは、ＮＶＳＣ１２１１のための名前を使用して、ＮＶＳＣを操作するＥＭＭ中でそのＮＶＳＣ１２１１を参照する。ＮＶＳＣの名前は、ＮＶＭ１２０９中のその物理的位置と関係を有する必要がない。名前の空間は、８ビット幅であるので、２５６ビットマップを使用して指定される。登録エージェントは、ＮＶＳＣの名前を有する場合、ＮＶＳＣを任意のタイプのＮＶＳＣにし得るが、それはそのタイプがＥＡに対して許可されるものであり、かつＥＡに属するそのタイプのＮＶＳＣの総数が、ＥＡを認証したＣＡＡによって設定された限度を超えない場合に限られる。

【０１１８】

一旦ＣＡＡがＤＨＣＴＳＥ中にＥＡ格納領域を割り当てたら、その格納領域を構成するのは、ＥＡである。第１のステップは、ＰＩＮなどの所定のパラメータをＥＡのための記述子にロードすることである。第２のステップは、どのタイプのＮＶＳＣが、提供される保護されたサービスのために使用されるのかを決定する。次に、ＣＡＡによって割り当てられた名前は、種々のタイプのＮＶＳＣの間に配布される。最後に、各ＮＶＳＣは、適切なＥＭＭを送信することによってロードされる。

【０１１９】

（ＥＭＭのアドレッシング）

条件付アクセスレイヤーにおいて、ＥＭＭは、ＣＡＡまたはＥＡによるインデックスにしたがって、特定のＤＨＣＴＳＥ６２７にアドレッシングされる。このインデックス法は、ＥＭＭヘッダ１１１３において扱われる。ＥＭＭヘッダ１１１３は、ＥＭＭのソースであるＣＡＡまたはＥＡのための一意の識別子を含み、そしてしたがってＥＭＭの封印ダイ

ジェストを作成するために使用されるプライベート鍵と関連する。ＥＭＭヘッダはまた、ＤＨＣＴＳＥ６２７のためのシリアル番号を含む。ＤＨＣＴＳＥ６２７は、シリアル番号を含むＥＭＭのみに応答する。ＣＡＡがＥＭＭのソースである場合は、ＣＡＡ公開鍵のどれがメッセージのソースのための公開鍵であるかを示すヘッダ中にまた値がある。条件付アクセスメッセージは、他のアドレッシングメカニズムを含み得る他のデータプロトコル中に転送され得る。

【０１２０】

ＤＨＣＴＳＥ６２７は、ＤＨＣＴＳＥ６２７にとって「既知」でないＣＡＡまたはＥＡにアドレッシングされたＥＭＭを無視する（すなわち、ＣＡＡＩＤに対応するＣＡＡがないか、またはＥＡＩＤに対応するＥＡがないＥＭＭ）。以下により詳細に説明されるように、個々の登録についての情報は、登録のためのＮＶＳＣ１２１１中に含まれる。これらのＮＶＳＣの各々は、タイプを有し、そしてＥＡは、変更すべきＮＶＳＣ１２１１の名前を特定するＥＭＭを送信することによってＮＶＳＣ１２１１のタイプまたは内容を変更し得る。ＤＨＣＴＳＥ６２７は、ＥＭＭにおいて示されるように、ＮＶＳＣ１２１１を変更する。但し、登録エージェントがその名前を有するＮＶＳＣを有さない場合、またはその変更がＣＡＡによって設定された拘束条件を満たさない場合を除く。これらの場合、ＥＭＭは、ＤＨＣＴＳＥ６２７によって無視される。条件付アクセスシステム６０１は、デジタル広帯域送達システム５０１が逆向きのパスを有することを要求しないし、または逆向きパスが存在しても、逆向きパス上の任意の帯域がＥＭＭ条件付アクセス機能に対して利用可能であることを要求しない。したがって、ＤＨＣＴ３３３は、ＥＭＭに応答して、承認、確認、あるいはエラーメッセージを全く返さない。したがって、ＥＭＭのソースであるＣＡＡまたはＥＡは、ＮＶＳＣ１２１１の割り当てをトラックし、そして正しい動作を要求するＥＭＭのみを送信する。他の実施態様において、逆向きパスが必要とされ得、そしてこれらの実施態様のために、その逆向きパスが承認またはエラーメッセージのために使用され得る。

【０１２１】

（ＣＡＡの変更）

上記のように、ＣＡＡは、ＤＨＣＴＳＥ６２７においてその公開鍵によって表される。ＣＡＡのための３つの公開鍵は、ＤＨＣＴＳＥ６２７が製造される時にその中にインストールされる。ＤＨＣＴＳＥ６２７のＣＡＡを変更する必要がときおり生じることがある。そのような必要が生じ得る１つの状況は、ＣＡＡのためのプライベート鍵が侵犯された場合であり得る；別の状況は、新しいエンティティが登録エージェントを認証する機能を乗っ取る場合であり得る。このような状況が生じ得るのは、例えば、ＤＢＤＳ５０１のすべてまたは一部を販売する結果としてである。

【０１２２】

ＣＡＡのための公開鍵のいずれもが２つのＥＭＭのシーケンスによって置換され得る。その２つのＥＭＭのうちの、第１のＥＭＭは、他の２つの公開鍵の第１のＥＭＭに対応する公開鍵を用いて暗号化された封印ダイジェストを有し、そして第２のＥＭＭは、他の２つのプライベート鍵の第２のＥＭＭに対応するプライベート鍵を用いて暗号化された封印ダイジェストを有する。２つのＥＭＭの各々は、識別子、新しいＣＡＡのためのＣＡＡＩＤ、３つのＣＡＡ公開鍵のうちのどれが置換されるべきかを示す鍵選択値、および新しいＣＡＡのための公開鍵を含む。第１ＥＭＭが、第１ＣＡＡ鍵によって適用されたデジタル署名を確認することによってＤＨＣＴＳＥ６２７により首尾良く認証された後に、ＤＨＣＴＳＥ６２７は、この第１ＥＭＭ中の新しいＣＡＡ公開鍵のＭＤ５ハッシュを計算し、そしてそれを格納する。第２ＥＭＭが、第２ＣＡＡ鍵によって適用されたデジタル署名を確認することによってＤＨＣＴＳＥにより首尾良く認証された後に、ＤＨＣＴＳＥは、この第２ＥＭＭ中に含まれる新しいＣＡＡ公開鍵のＭＤ５ハッシュを計算する。この第２ハッシュは、第１ハッシュと比較される。これらのハッシュが同一である場合、新しいＣＡＡ公開鍵およびＣＡＡＩＤは、鍵選択値によって特定されたＣＡＡの公開鍵およびＣＡＡＩＤに取って代わる。１つのＣＡＡ公開鍵は、他の２つのＣＡＡ公開鍵の１つが中間で変更

されずに２度変更されてはいけない。

【０１２３】

（ＤＨＣＴＳＥ６２７中の登録エージェントの動的な追加および除去；図１５）

ＣＡＡは、ＤＨＣＴ３３３を認証して登録エージェントからサービスを受信する場合、新しい登録エージェントのための登録エージェント記述子ＥＡＤ１４０９を作成するＥＭＭのシーケンスを送信することによってそうする。図１５は、ＣＡＡ　ＥＭＭによって作成されるようなＥＡＤ１４０９（ｉ）の詳細な図を示す。ヘッダ１５０２は、すべてのＮＶＳＣ１２１１に共通である。セルステータス１５０１は、ＮＶＳＣ１２１１が割り当てられたかどうかを示す。セルタイプ１５０３は、どの種類のデータを、ＥＡＤ１４０９とともに、それが含むかを示す。セルタイプ１５０３は、セルが「太型」ＮＶＳＣであることを示す。セルの名前１５０５は、ＣＡＡがセルを割り当てる場合にＣＡＡがセルに与える８ビットの名前である。名前は、ＥＡごとである。すなわち、１つのＥＡのためのＥＡ情報１３３３は、２５５個までのＮＶＳＣを含む。ネクストエレメント１５０７は、ＮＶＳＣが属するリスト中の次のエレメントへのポインタである。したがって、ネクストエレメント１５０７は、割り当てられていないＮＶＳＣにおいては、フリーリスト１４０７中の次のＮＶＳＣへのポインタ；ＥＡＤ１４０９においては、ＥＡＤリスト１４０６中の次のエレメントへのポインタ；およびリスト１４１１の一部である細型ＮＶＳＣにおいては、そのリスト中の次の細型ＮＶＳＣである。次のエレメント１５０７は、ＥＭＭによってリストが操作される場合につねに応答して設定される。

【０１２４】

残りのフィールドは、ＥＡＤ１４０９に対して特有のものである。図１５において１５０６でラベルされたフィールドは、ＣＡＡからのＥＭＭによってすべて設定される。ＥＡＩＤ１５０９は、ＥＡＤ１４０９が属する登録エージェントのための識別子である；好ましい実施態様において、ＥＡＩＤ１５０９は、所定の登録エージェントためのＥＡＤ１４０９を配置するために使用される。ＣＡＡフラグ１５１１は、１組のフラグであり、（１）登録エージェントがアクセスを授与し得るサービスのクラス、および（２）登録エージェントのための公開鍵がＥＡＤ１４０９中にインストールされるかどうか、を示す。第１細型ＮＶＳＣ１５１３は、ＥＡＤ１４０９が属するＥＡ情報１３３３に属する細型ＮＶＳＣリスト１４１１へのポインタである。ＥＡ最大１５１５は、ＥＡ情報１３３３が属するＥＡのためのサービスの最大量を定義する。ＣＡＡによって設定される最後のフィールド１５０６は、ＥＡ情報１３３３に属するＥＡのための公開鍵であるＥＡ公開鍵１５２７である。

【０１２５】

ＥＡフィールド１５１６中のフィールドは、ＤＨＣＴ３３３が属する顧客に関連する情報を含む。そのフィールドは、ＥＡＤ１４０９が割り当てられ、そしてフィールド１５１０６が設定された後で、ＥＡから受信されたＥＭＭによって設定される。ＤＨＣＴフラグ１５１７は、この特定のＤＨＣＴ３３３が受信する権利を現在与えられているＥＡによって提供されるサービスを示すフラグを含む。格納されたクレジット限度フィールド１５１９は、インパルスサービスのインスタンス、すなわち、前もって購入される必要のないサービスのインスタンス、を用いて使用される。格納されたクレジット限度サービスフィールド１５１９は、インタラクティブ顧客がＥＡからの認証なしに使用し得るサービスの最大量を示す。以下に詳細が示されるように、認証は、ＦＰＭをＥＡに送信し、そしてＥＡから確認のＥＭＭを受信することによって得られる。Ｘ座標１５２１およびＹ座標１５２３は、登録エージェントによって確立された座標系（以下により完全に説明される）におけるＤＨＣＴ３３３の位置を定義する。座標系は、地理的であり得、そして例えば、ＤＨＣＴ３３３が、放送中にブラックアウトされるべき領域中に存在するかどうかを決定するために使用され得る。座標系はまた、ＥＡの顧客のサブセットを定義するために一般に使用される。例えば、Ｘ座標およびＹ座標は、ＧまたはＰＧ－１３以外の格付けを有する映画を受信することを望まない顧客を定義するために使用される。ＰＩＮは、ＤＨＣＴのための顧客が自分自身を登録エージェントに対して身分証明するために使用するマルチキャ

ラクターコードである。

【０１２６】

ＣＡＡがＥＡのためのＥＡ情報１３３３を設定するために送信するＥＭＭは、以下のとおりである：

・ＥＡ割り当て名前マップ設定

・ＥＡ最大割り当て設定

・登録エージェント公開鍵更新

これらのＥＭＭのすべてにおけるＥＭＭヘッダ１１１３は、ＣＡＡのためのＣＡＡＩＤを含み、そしてそのＥＭＭのすべては、ＣＡＡのプライベート鍵を用いて暗号化された封印ダイジェストを有する。ＣＡＡは、これらのＥＭＭを使用して、ＥＡ情報１３３３を設定するだけでなく、ＥＡのためのすでに既存のＥＡ情報１３３３を変更し、そしてＥＡのためのＥＡ情報１３３３を除去する。後者が行われた場合、ＤＨＣＴＳＥ６２７は、登録エージェントからのＥＭＭまたはＥＣＭにもはや応答しない。

【０１２７】

（ＥＡ割り当て名前マップ設定）

ＥＡ割り当て名前マップ設定ＥＭＭは、ＥＡ情報１３３３が作成中または変更中のＥＡを一意に識別するＥＡＩＤ、および名前マップをを含む。マップは、名前ごとに１ビットを有する；ＣＡＡがＥＡのためにＮＶＳＣを割り当てた場合、ＮＶＳＣの名前に対応するビットが設定される。ＣＡＡのＥＭＭコード１３１５は、このＥＭＭに応答する。その応答は、ＥＡ情報１３３３に必要とされるＮＶＳＣを割り当て、ＥＡＩＤのための名前をＮＶＳＣの物理的位置にマッピングし、リスト１４１１を作成し、そしてそれを指すように第１のＮＶＳＣフラグ１５１３を設定し、新しいＥＡ記述子１４０９をＥＡリスト１４０６の先頭に加え、そしてそれに応じてネクストエレメントポインタ１５０７を設定し、そしてヘッダフィールド１５０２およびＥＡＩＤフィールド１５０９を満たすことによってなされる。

【０１２８】

ＣＡＡのＥＭＭコード１３１５は、ＣＡＡデータ１３３０中のＥＡのための現在の名前マップを格納し、そしてその結果、新しく受信されたセットＥＡ割り当て名前マップＥＭＭを現在の名前マップと比較し得る。１つの名前が両方の名前マップにおいて特定される場合、ＥＡ割り当て名前マップ設定コマンドは、その名前を用いてＮＶＳＣ１２１１に影響を及ぼすことはない。ＥＭＭにおける名前マップが、現在の名前マップになかった名前を特定する場合、その名前に対応するＮＶＳＣ１２１１は、リスト１４１１に追加される。ＥＭＭ中の名前マップが前回登録エージェントに割り当てられた名前をもはや指定しない場合、その名前に対応するＮＶＳＣ１２１１は、フリーリスト１４０７に返却される。これがなされた後、ＥＭＭ中の名前マップは、現在の名前マップになる。

【０１２９】

通常、登録エージェントおよび条件付アクセスオーソリティは、リスト１４１１がどのくらいの大きさであるべきかを決定する際に協力する。例えば、登録エージェントが少ない空間しか必要としない場合、その効果に対するメッセージをＣＡＡに送信し得、そのメッセージは、登録エージェントが望む除去すべきＮＶＳＣ１２１１の名前を含み、そしてＣＡＡによって送信されたＥＭＭ中の名前マップは、登録エージェントが保持を望むＮＶＳＣ１２１１の名前だけを指定し得る。しかし、登録エージェントが協力的でないか、または条件付アクセスオーソリティが、登録エージェントからメッセージを受信する前に登録エージェントのためのリスト１４１１の大きさを低減しなければならないことが起こり得る。この場合、ＣＡＡは、名前の値によってリスト１４１１からＮＶＳＣ１２１１を除去し得る、すなわち、最高の数値を有する名前で始まり、２番目に高い数値という具合に、必要な数のＮＶＳＣ１２１１が除去されるまで続けられる。

【０１３０】

ＣＡＡはまた、セットＥＡ割り当て名前マップＥＭＭを使用して、ＥＡのためのＥＡ情報をＤＨＣＴＳＥ６２７から除去する。ＥＭＭがこのように使用される場合、名前マップ

にビットは１つも設定されない。ＣＡＡのＥＭＭコード１３１５は、ＥＭＭ中のＥＡＩＤによって識別されたＥＡのためのＥＡ情報１３３３およびＥＡ記述子１４０９（ｉ）中のＮＶＳＣのすべてをフリーリスト１４０７へ返却し、そして必要に応じてＥＡリスト１４０６を再リンクすることによって応答する。

【０１３１】

（ＥＡ最大割り当て設定）

ＥＡ最大割り当て設定は、作成または変更中の登録情報１３３３を有するＥＡのためのＥＡＩＤを含み、そしてまた、ＥＡＤ１４０９のフィールド１５１１および１５１５のための値を含む。ＣＡＡのＥＭＭコード１３１５は、このＥＭＭに応答する。この応答は、ＥＭＭ中に指定されたＥＡＩＤを用いてＥＡ記述子１４０９を見つけるまでＥＡリスト１４０６を読み進み、そしてＥＭＭ中の値を使用してＥＡＤ１４０９のフィールド１５１１および１５１５を設定することによってなされる。登録エージェントがＥＭＭを所定タイプ、例えばイベント、の登録情報を確立したＤＨＣＴＳＥ６２７に送信する場合、ＥＭＭをインタープリタするコードは、ＥＡ最大割り当てをチェックしてそのＥＡのための登録の最大数を超えたかどうかを決定する。好ましい実施態様において、登録は、ＮＶＳＣによって表される。したがって、制限されるものは、リスト１４１１中の所定タイプのＮＶＳＣの数である。

【０１３２】

（登録エージェント公開鍵更新）

登録エージェント公開鍵更新ＥＭＭは、作成または変更中の登録情報を有するＥＡのためのＥＡＩＤ、およびＥＡの公開鍵を含む。ＣＡＡのＥＭＭコード１３１５のこのＥＭＭに対する応答は、上記のようにＥＡ記述子１４０９を配置し、そしてＥＭＭ中に公開鍵からのフィールド１５２７を設定することによってなされる。ＥＡの公開鍵が適切な位置にあると、ＤＨＣＴＳＥ６２７は、ＥＭＭの署名されたダイジェストを使用してＥＭＭがＥＡからのものであることを確認し得る。この確認は可能である。なぜなら、ＥＡが更新された公開鍵に対応するプライベート鍵を使用して署名動作を行うからである。

【０１３３】

（登録情報１３３３を変更するＥＡのＥＭＭ）

登録情報を変更するＥＡのＥＭＭは、ＥＡの公開鍵を使用して暗号化される封印ダイジェストを封印した。ＥＭＭは、２つのグループに分けられる：ＥＡＤ１４０９のＥＡフィールド１５１６を変更するＥＭＭ、およびリスト１４１１を構成するＮＶＳＣの内容を変更するＥＭＭである。ＥＡＤ１４０９に関しての記載のように、各ＮＶＳＣは名前を有し、そしてリスト１４１１中の各ＮＶＳＣは、タイプを有する。ＮＶＳＣは、上記のように、ＣＡＡによって名付けられ、そしてその名前は、登録エージェントによっては変えられ得ない。しかし、登録エージェントは、ＥＡのためのＥＡＤ１４０９中に確立されたタイプのための最大値のみに依存してＮＶＳＣのタイプおよび内容を変更する。ＥＡ情報１３３３中のＮＶＳＣのタイプおよび内容を追跡するのは、登録エージェントである。

【０１３４】

ＥＡＤ１４０９のＥＡフィールド１５１６を変更するＥＭＭは、登録エージェントプロパティ更新ＥＭＭである。ＥＭＭの第２のグループは、さらにＥＭＭが提供する登録の種類にしたがって細分化される。登録の２つの広い系が存在する：非インタラクティブサービスのための放送登録、およびインタラクティブセッションのためのインタラクティブ登録である。放送登録内において、ユーザが個々に支払うイベントのためのイベント登録が存在する。このような場合として、視聴ごと有料イベント、インタラクティブペイ－パー－ビューイベント、およびニアビデオ－オン－デマンドイベントがある。非イベント放送ＥＭＭは、以下を含む：

・ＭＳＫ更新
・デジタルビットマップ更新
・デジタルリスト更新
・アナログＭＳＫアンドビットマップ更新

・アナログＭＳＫアンドリスト更新
・アナログビットマップ更新
・アナログリスト更新
である。
イベントのための放送ＥＭＭは、以下を含む：
・ニューイベント格納
・追加／除去ＰＰＶイベント
・承認ＩＰＰＶ／ＮＶＯＤイベント
である。
インタラクティブセッションのためのＥＭＭは、以下を含む：
・新規インタラクティブセッション格納
・追加インタラクティブセッション
・除去インタラクティブセッション
である。ＥＭＭの名前からわかるように、ＥＡは、ＥＡＤ１４０９において特定される最大値のみに依存して、イベントおよびインタラクティブセッションの必要に応じて、ＣＡＡによって割り当てられる、名前の付けられたＮＶＳＣのタイプを変更し得る。

【０１３５】

ＮＶＳＣを割り当て、ＮＶＳＣのタイプに制限を設定し、そして公開鍵を登録エージェントに付与するための別々のＣＡＡのＥＭＭが存在する。また、ＮＶＳＣ１２１１を書き込むためのＥＡのＥＭＭは、名前によってそれを行い、そしてＮＶＳＣ１２１１のタイプおよびその内容を変更し得る。したがって、アクセス制御システム６０１は、高度の制御性および柔軟性を有する。ＣＡＡは、必要に応じて、登録エージェントが与え得る登録の総数、登録のタイプ、および各種類の登録の総数を動的に制約する。ＣＡＡはまた、部分的にまたは全体的にその制約条件を変更し得、そして登録エージェントと協力して、または単独のいずれかでそうし得る。しかし、ＣＡＡによって課された制約条件内で、登録エージェントは、所定タイプの登録を変更するだけでなく、タイプそのものさえを変更して、自由にそれ自身の登録を動的に管理する。

【０１３６】

（登録エージェントプロパティ更新）

このＥＭＭは、ＥＡＤ１４０９のＥＡフィールド１５１６のための値を含む。ＥＡ管理ＥＭＭコード１３１７は、ＥＭＭヘッダ１１１３を読み出して、ＥＭＭの対象のＥＡのためのＥＡＩＤを取得し、そしてＥＭＭから、ＥＡのためのＥＡＤ１４０９中にフィールド１５１６を設定するだけである。

【０１３７】

（非イベント放送ＥＭＭ）

非イベント放送ＥＭＭのうち、４つのタイプをここで検討する。ＭＳＫ更新、ビットマップ更新、リスト更新、およびＭＳＫとリストまたはビットマップとの更新の組み合わせが存在する。当業者は、以下に説明される原理を、他の非イベント放送ＥＭＭの名前によって示される機能を行うＥＭＭに容易に適用し得る。例えば、デジタルＥＭＭの原理は、アナログＥＭＭに適用され得る。上記非イベント放送ＥＭＭによって提供される各情報タイプのための別々のタイプのＮＶＳＣ１４０５が存在する。図１６は、これら４つのタイプのＮＶＳＣの内容を示す。各ＮＶＳＣタイプを、それを含む情報を提供するＥＭＭとともに検討する。

【０１３８】

（ＭＳＫ更新）

ＭＳＫ更新ＥＭＭは、ＥＭＭによって特定されたＥＡによって提供される１組のサービスのために新しいＭＳＫを送信するために使用される。新しいＭＳＫおよびそのＭＳＫに関連する他の情報は、ＥＭＭによって特定されるＥＡに属するＥＡ情報１３３３のためのリスト１４１１中のＭＳＫ　ＮＶＳＣ１６０１中に格納される。ＭＳＫ　ＮＶＳＣ１６０１中に含まれるのは、ヘッダ１５０２である。ヘッダ１５０２は、ＮＶＳＣ１６０１がＭ

ＳＫ　ＮＶＳＣであることを指定し、ＮＶＳＣの名前を与え、そしてリスト１４１１中の次のエレメントへのネクストエレメントポインタ１５０７を含む。他のフィールドは、ＭＳＫについての情報を含む。好ましい実施態様において、ＭＳＫ１６０８は、２つの１２８－ビット部分を有する：偶数ＭＳＫ１６０９および奇数ＭＳＫ１６１１である。各部分は、２つの半分、すなわち、第１半分および第２半分であり、それぞれ５６鍵ビットおよび８未使用パリティビットを有する。ＭＳＫ１６０８は、ＭＳＫ１６０８のためのペア識別子１６０３、ＭＳＫ１６０８のための期限日１６０５、および期限日１６０５の値が無視されるべきかどうかを示すフラグ１６０７と関連する。期限日１６０５が無視されない場合、ＤＨＣＴＳＥ６２７は、期限日の後に制御ワードを復号化するためにＭＳＫ１６０８を使用しない。識別子１６０３は、ＥＡごとに存在し、そしてその結果、所定のＥＡは、複数の異なるＭＳＫを格納するために１つ以上のＭＳＫ　ＮＶＳＣ１６０１を任意の所定時間に有し得る。したがって、条件付アクセスシステム６０１は、各ＥＡのための別々のセキュリティパーティションを可能にするだけでなく、ＥＡ内のセキュリティパーティションを可能にする。

【０１３９】

アップデートＭＳＫ　ＥＭＭヘッダは、ＥＡのためのＥＡ情報１３３３を配置するために必要なＥＡＩＤを含む；そのメッセージは、ＭＳＫを受信するＮＶＳＣの名前、更新されるべきＭＳＫのためのＭＳＫペアＩＤを指定するＭＳＫペアセレクタ、ＥＡがＭＳＫペアＩＤ１６０３を選択的に変更することを可能にする１組のフラグ、期限日１６０５、非期限日１６０７、およびＭＳＫ１６０８の半分の片方、およびその変更を行うために必要な情報を含む。ＥＭＭは最大、ＭＳＫペアＩＤ１６０３のための値、期限日１６０５のための値、非期限日１６０７のための値、ならびに偶数ＭＳＫ１６０９および奇数ＭＳＫ１６１１のための値を含む。ＥＡのＭＳＫコード１３１９によるアップデートＭＳＫ　ＥＭＭの処理は、ＥＭＭヘッダのＥＡＩＤによって識別されたＥＡのためのＥＡ情報１３３３を配置し、セル名を使用して適切なＮＶＳＣを配置し、そのＮＶＳＣにＭＳＫタイプを与え、そして次にＥＭＭ中のフラグおよび情報によって必要とされるようにＭＳＫ　ＮＶＳＣ１６０１へ書き込むことによってなされる。この方法は、アナログおよびデジタル両方のアップデートＭＳＫ　ＥＭＭについて同じである。違いは、ＥＭＭヘッダ１１２３およびＮＶＳＣタイプ１５０３中のＥＭＭコマンドコードの点である。

【０１４０】

（登録識別子）

以下により詳細に説明されるように、ＥＣＭは、それが付随するサービスインスタンスを、（１）そのＥＣＭのソースである登録エージェントのためのＥＡＩＤ、および（２）そのインスタンスのための３２ビット登録ＩＤ、によって指定する。登録ＩＤは、ＥＡごとに存在する。登録ＩＤを３２ビット長にすることによって、各ＥＡは、ペイ－パー－ビューイベントおよびインタラクティブサービスなどの一過性のサービスに対してさえ十分な登録ＩＤを有し得る。好ましい実施態様において、ＤＨＣＴＳＥ６２７は、ＥＣＭをインタープリタする場合、ＤＨＣＴ３３３がインスタンスを復号化する権利を与えられたかどうかを、ＥＣＭ中で特定された登録ＩＤに対応する登録ＩＤを、ＥＣＭ中で特定されたＥＡのためのＥＡ情報１３３３中で探すことによってチェックする。ＥＭＭおよびＥＡ情報１３３３中の登録ＩＤは、少なくとも２つの方法で表される。１つの方法は、登録ＩＤを単にリストするだけによる。この技術の欠点は、３２ビット登録ＩＤが大きく、そしてＮＶＳＣが不十分なリソースであることである。他方の方法は、開始登録ＩＤ値およびビットマップによるものである。開始登録ＩＤ値によって特定される登録ＩＤ値の２５５内の値を有する任意の登録ＩＤは、ビットマップ中に１ビットを設定することによって特定され得る。この技術は、上記ＢａｎｋｅｒおよびＡｋｉｎｓの上記特許出願において記載される。特に、ＢａｎｋｅｒおよびＡｋｉｎｓの特許出願の図２およびその図の検討を参照のこと。開始ＩＤおよびビットマップによって登録ＩＤを特定することの以下の検討は、上記特許出願の検討を拡張するものである。

【０１４１】

（ビットマップ更新ＥＭＭ）

このＥＭＭは、１つ以上の登録ＩＤを特定するビットマップを更新する。ビットマップは、登録ビットマップＮＶＳＣ１６１３中に格納される。ＮＶＳＣ１６１３は、そのＮＶＳＣのセル番号およびタイプを有するヘッダ１５０２；ビットマップによって特定され得る第１登録ＩＤである第１登録ＩＤ１６１５；第１登録ＩＤ１６１５およびビットマップによって特定される登録ＩＤがいつ期限切れとなるのかを指定する期限日１６１７；実際に期限日が存在するのかどうかを示す非期限日フラグ１６１９；およびビットマップ１６２１を有する。アップデートビットマップＥＭＭは、設定されるべきＮＶＳＣ１６１３のためのセル名、そのＥＭＭによって設定されるＮＶＳＣ１６１３中の情報を示す１組のフラグ、および情報のための値を含む。ＥＭＭは、任意のまたはすべての第１登録ＩＤ１６１５、期限日１６１７、非期限日１６１９、およびビットマップ１６２１を設定し得る。ＥＡ管理ＥＭＭコード１３１７は、ＥＭＭ中で示されるように特定のＮＶＳＣ１６１３のフィールドを設定することによって、ＥＭＭに応答する。この手順は、デジタルビットマップ更新およびアナログビットマップ更新ＥＭＭの両方について同じである。違いは、ＥＭＭヘッダ１１２３およびＮＶＳＣタイプ１５０３中のＥＭＭコマンドコードの点にある。

【０１４２】

（リスト更新ＥＭＭ）

リスト更新ＥＭＭは、登録リストＮＶＳＣ１６２３中に含まれる登録ＩＤのリストを更新する。ＮＶＳＣ１６２３は、そのＮＶＳＣのためのセル名およびタイプを有するヘッダ１５０２を有し、そして６個までの登録ＩＤエレメント１６２５を含む。そのエレメントの各々は、登録ＩＤ１６２７、その登録ＩＤ期限日１６２９、およびその登録ＩＤが期限日を有するかどうかを示すフラグ１６３１を含む。リスト更新ＥＭＭは、ＮＶＳＣのためのセル名、フラグのための値、期限日、および６個までの登録ＩＤエレメント１６２５のための値を含む。この手順は、デジタルリスト更新およびアナログリスト更新ＥＭＭの両方について同じである。違いは、ＥＭＭヘッダ１１２３およびＮＶＳＣタイプ１５０３中のＥＭＭコマンドコードの点にある。

【０１４３】

（放送イベント）

放送イベントは、ボクシング試合のペイ－パー－ビュー放送などの１回のサービスである。好ましい実施態様において、２種類の放送イベントが存在する：顧客がイベントを見るためにあらかじめ注文しておく普通のペイ－パービュー放送イベント、および顧客が注文したいイベントが放送される時間を顧客が決定するインパルスイベントである。異なる種類のインパルスイベントが存在する：顧客がイベントの時間でそのイベントを購入することを決定し得るペイ－パー－ビューイベントであるインパルスペイ－パー－ビュー（ＩＰＰＶ）イベント、および人気のある映画を短い間隔で再放送し、そして顧客が見たいかどうかにかかわらずいつ再放送がされるかを顧客が決定し得るニアビデオオンデマンド（ＮＶＯＤ）。「イベント」の概念が、ビデオオンデマンドイベントまたは本明細書中でリストしない他の種類のイベントなどの、特定の期間の任意のサービス（放送または非放送にかかわらない）を参照し得ることは、当業者の認めるところである。

【０１４４】

ペイ－パー－ビューイベントの場合、顧客は、登録エージェントからイベントを注文し、そしてそのエージェントは、必要な登録情報を含むＥＭＭを送信することによって応答する。顧客がイベントを購入したいと放送時間で決定するイベントの場合、購入情報、すなわち、購入され得る登録についての情報、がイベントとともに配布されなければならない。これらの場合、購入情報は、グローバル放送認証済メッセージすなわちＧＢＡＭによって配布される。顧客は、購入を特定する入力６２８を提供する。ＤＨＣＴ３３３は、ＤＨＣＴＳＥ６２７中に購入の記録を格納し、そして次にイベントの復号化を始めることによって入力６２８に応答する。その後、ＤＨＣＴ３３３は、顧客によって何が購入されたかを示す転送購入メッセージ（ＦＰＭ）を登録エージェントに送信し、そして登録オーソ

リティは、ＥＭＭを用いて応答する。そのＥＭＭは、購入を確認し、そして必要な登録情報を含む。購入の記録は、購入を確認するＥＭＭがＤＨＣＴＳＥ６２７によって受信されるまで残る。

【０１４５】

（イベントＮＶＳＣ：図１７）

図１７は、イベントのための登録情報を格納するために使用されるイベントＮＶＳＣ１７０１を示す。ヘッダフィールド１５０２は、他のＮＶＳＣ１７０１についてのものと同様である。各イベントＮＶＳＣ１７０２は、３個までのイベント記述子１７０３を含み得る。各記述子１７０３は、１つのイベントを記述する。各記述子１７０３は、フラグフィールド１７０５を含む。フラグフィールド１７０５は、（１）イベントがアクティブかどうか、（２）その終了時間が延長されたかどうか、（３）登録エージェントがイベントの購入を確認したかどうか、（４）顧客が任意の時間にキャンセルし得るかどうか、（５）顧客がキャンセルウインドウにおいてキャンセルし得るかどうか、（６）顧客が購入をキャンセルしたかどうか、（７）イベントをコピーする権利が購入されたかどうか、および（８）イベントがアナログまたはデジタルサービスでどちらであるかを示すフラグを含む。購入時間１７０９は、イベントの開始時間の後、または顧客がイベントを購入した時間である。終了時間１７０９は、イベントが終了する時間である。コスト１７１１は、顧客に対するイベントのコストであり、そして登録ＩＤ１７１３は、イベントのための登録ＩＤである。

【０１４６】

（ニューイベント格納ＥＭＭ）

ＣＡＡは、登録エージェントのための登録エージェント記述子１４０９を設定する場合、登録エージェントが有し得るイベントＮＶＳＣ１７０１の数を制限するＥＡ最大１５１５中に値を含む。しかし、その値内で、登録エージェントは、登録エージェントに属するＮＶＳＣ１４０５の総数からイベントＮＶＳＣ１７０１を割り当て、そして既存のイベントＮＶＳＣ１７０１を再使用することを自由に行う。イベントＮＶＳＣを割り当てるために、ＥＡは、ニューイベント格納ＥＭＭを使用する。ニューイベント格納ＥＭＭは、割り当てられるＮＶＳＣのためのセル名を単に含む。一旦イベントＮＶＳＣ１７０１が割り当てられると、そのフィールドは、以下のように設定される。

・普通のＰＰＶの場合、フィールドは、追加／削除イベントＥＭＭによって設定される；
・ＩＰＰＶまたはＮＶＯＤイベントの場合、フィールドは、部分的にイベントのためのＧＢＡＭから、および部分的に顧客入力６２８から設定される。

【０１４７】

イベントＮＶＳＣ１７０１の内容は、イベント記録が承認イベントＥＭＭを受信することによって前回に承認された場合、追加／削除イベントＥＭＭによって、またはイベントＮＶＳＣ１７０１中の、イベント終了時間を超える時間を含むＥＣＭを受信することによって削除される。

【０１４８】

（追加／削除イベントＥＭＭ）

追加／削除イベントＥＭＭは、ＥＭＭがイベントを設定中または削除中のどちらであるかを示すフラグを含む。後者の場合、ＥＭＭの内容は、削除されるべきＮＶＳＣ１７０１の現在の内容と一致しなければならない。前者の場合、ＥＭＭの値は、時間延長が可能かどうか、およびコピーする権利が購入されたかどうかを示すフラグを含む。さらに含まれるのは、イベントの開始時間および終了時間ならびにイベントのための登録ＩＤのための、値である。追加／削除フラグが「削除」を示す場合、ＥＡ管理コードは、ＮＶＳＣ１７０１の内容を削除する。追加／削除フラグが「追加」を示す場合、コードは、ＮＶＳＣ１７０１の対応フィールドにＥＭＭ中に特定される値を設定する。ＥＡが購入を承認したかどうかを示すフラグは、そのことを示すように設定される。

【０１４９】

（グローバル放送認証済メッセージ：図１８－２０）

グローバル放送認証済メッセージ（ＧＢＡＭ）は、ＥＭＭ，ＥＣＭ、およびＥＰＭのようなＣＡメッセージである。ＧＢＡＭは、登録エージェントによってＤＨＣＴ３３３に放送される。図１８は、ＧＢＡＭ１８０１を含むＣＡメッセージ８０５を示す。メッセージ８０５は、ＣＡメッセージヘッダ１００３およびＣＡ

ＧＢＡＭメッセージ１８０３を含み、ＣＡ　ＧＢＡＭメッセージ１８０３は、ＧＢＡＭヘッダ１８０７およびグローバル放送データ１８０９から構成される。グローバル放送データ１８０９は、暗号化されないが、ＧＢＡＭ１８０１は、ＥＣＭと同じ方法で認証される：ヘッダ１８０７、グローバル放送データ１８０９、およびＧＢＡＭを送信したＥＡに属するＭＳＫ１０１５は、一方向ハッシュ関数ＭＤ５によってハッシュされＧＢＡＭ　ＭＡＣ１８０５を作成する。ＥＣＭと同様に、ＭＳＫ１０１５は、ＧＢＡＭを送信したＥＡとＥＡのためのＥＡ情報１３３３を有するＤＨＣＴ３３３との共有の秘密である。

【０１５０】

図１９は、ＧＢＡＭヘッダ１８０７を詳細に示し、さらにＧＢＡＭ１８０１を使用してＩＰＰＶまたはＮＶＯＤのための登録情報を提供する場合にグローバルデータ１８０９がとる形態を示す。ＧＢＡＭヘッダ１８０７は、ＧＢＡＭ１８０１が使用されているＣＡシステム６０１を識別する条件付アクセスシステムＩＤ１９０１、メッセージがＧＢＡＭであることを示すタグ、およびＧＢＡＭを送信する登録エージェントの識別子１９０５を有する。フィールド１９０７および１９０９は、ＭＡＣ１８０５を作成するために使用された鍵を特定する。フィールド１９０７は、ダイジェストを作成するために使用されるＭＳＫの半分のパリティを特定し、そしてＭＳＫセレクタ１９１１は、ＭＳＫそのもののための識別子である。

【０１５１】

購入可能な登録データ１９１３は、ＩＰＰＶまたはＮＶＯＤのための登録情報を提供するために使用されるグローバル放送データ１８０９の形態に関する。現在の議論に関連するフィールドのうち、登録ＩＤ１９１５は、ＧＢＡＭと関連するイベントのための登録ＩＤであり、そしてフラグ１９１７は、どのような種類のキャンセルが可能であるかおよびイベントのための時間が延長され得るかを示すフラグを含む。モード数１９１９は、イベントを購入するためにいくつの異なるモードが存在するのかを示す。イベントに対して購入者が受け取る権利、および購入者が支払わなければならない金額は、モードとともに変化する。好ましい実施態様において、イベントは、５個までの購入モードを有し得る。より多くの購入モードが必要とされる場合、さらなるＧＢＡＭが送信され得る。各モードに対する権利および金額は、配列によって示される。各配列は、モードと同じ多さの有効エレメントを有する。モードに対応するエレメントの値は、そのモードの権利または価格を示す。したがって、モードコピー権利フィールド１９２１は、ビット配列である；１モードための１ビットが設定されるならば、そのモードの購入者は、イベントをコピーする権利を有する。同様に、モード長フィールド１９２７は、そのモードにおけるイベントのための時間長を示す各モードのための値を含む。モードコストフィールド１９２９は、そのモードにおけるイベントのためのコストを示す、各モードのための値を含む。最初開始フィールド１９２３は、イベントのための登録が開始し得る最も早い時間を与え、そして最終終了フィールド１９２５は、登録が終了しなければならない最終時間を与える。

【０１５２】

ＤＨＣＴ３３３は、ＧＢＡＭ１８０１を受信する場合、グローバル放送データ１８０９を認証するためにＧＢＡＭ１８０１をＤＨＣＴＳＥ６２７に渡す。ＤＨＣＴＳＥ６２７が必要なＭＳＫを有さない場合、認証は失敗する。（１）ＤＨＣＴＳＥ６２７が必要なＭＳＫを有し、そして（２）グローバル放送データ１８０９がデータ１９１３である場合、ＤＨＣＴ３３３は、顧客がイベントを購入することを許可する。そうする際に、顧客は、ＰＩＮによってＤＨＣＴ３３３に対して自分自身を証明し、そしてそのＰＩＮは、ＧＢＡＭを送った登録エージェントのためのＥＡＤ１４０９におけるＰＩＮ１５２５に一致しなければならない。顧客はまた、購入を行う際に関連するモードを特定する。ＧＢＡＭにおけるモード情報およびコスト情報が与えられると、ＤＨＣＴ３３３は、インパルスイベント

を注文することによって、顧客がＥＡＤ１４０９における格納クレジット限度１５１９において特定された（時間、金銭などの）量を超えるかどうかを決定し得る。顧客が限度を超えなかった場合、ＧＢＡＭおよび購入者の入力からの情報は、イベントのためのイベント記述子１７０３を作成するための使用される。ＤＨＣＴ３３３は、その情報をＤＨＣＴＳＥ６２７に渡す。ＤＨＣＴＳＥ６２７は、ＤＨＣＴ３３３によって提供された値にしたがってイベント記述子１７０３におけるフィールドを設定する。購入情報が承認されたかどうかを示すフラグは、クリアされ、そしてイベントのコストは、現在のクレジットバランスに追加される。

【０１５３】

（転送購入メッセージ：図２１）

好ましい実施態様において転送購入メッセージ（ＦＰＭ）は、２つの目的を果たす：

・転送購入メッセージは、顧客がＩＰＰＶまたはＮＶＯＤイベントを購入したことを登録エージェントに通知する；および

・転送購入メッセージは、顧客が任意のイベントの購入をキャンセルしたことを登録エージェントに通知する。

【０１５４】

他の実施態様において、ＦＰＭのようなメッセージは、任意の種類の情報をＤＨＣＴ３３３からＣＡＡまたはＥＡに転送するために使用され得る。例えば、そのようなメッセージは、ＤＨＣＴ３３３からＥＡへ月々の注文情報を転送するために使用され得る。

【０１５５】

ＤＨＣＴ３３３は、購入情報を有する転送購入メッセージを、逆向きチャネルを介して、ＧＢＡＭを送信した登録エージェントに送信する。ＦＰＭは、ＥＡにアドレッシングされる逆向きチャネルデータパケット中に含まれる。図２１は、ＦＰＭ、およびその内容を保護するために使用される暗号手段の概観を提供する。ＦＰＭ２１０１は、ＣＡメッセージ８０５であり、そしてしたがって、ＣＡメッセージヘッダ１００３を用いて送信される。ＦＰＭ２１０１そのものは、ＦＰＭ暗号化エンベロップ鍵２１０３から構成される。ＦＰＭ暗号化エンベロップ鍵２１０３は、登録エージェントのためのＥＡＩＤ、およびＦＰＭ暗号化イベント２１１３中に含まれる購入情報を復号化するためのＦＰＭ鍵２１１９を含む。エンベロップ鍵２１０３の鍵および他の内容は、ＦＰＭ２１０１が対象である登録エージェントの公開鍵を使用して、プライバシーのために暗号化される。ＣＡ　ＦＰＭメッセージ２１０５は、ＣＡ　ＦＰＭヘッダ２１１を含む。ＣＡ　ＦＰＭヘッダ２１１は、対象のＥＡのためのＥＡＩＤ、およびＦＰＭ暗号化イベント２１１３を含む。後者は、エンベロップ鍵２１０３中の鍵を用いた３－ＤＥＳアルゴリズムを使用して暗号化される。ＣＡ　ＦＰＭメッセージ２１０５の部分は、ヘッダ２１３、ＦＰＭクリアイベント２１３３、およびパディング２１３５を含む。ＦＰＭクリアイベント２１３３は、購入情報を含む。ＦＰＭ２１０１の最後の部分は、ＦＰＭメッセージ２１０１を送信するＤＨＣＴ３３３のプライベート鍵を用いて暗号化されたＦＰＭ署名済認証２１０７である。

【０１５６】

暗号化材料は、ＦＰＭ署名ヘッダ２１２５、ＦＰＭ　ＭＡＣ２１２７、およびパディング２１２９を含む。ＦＰＭ　ＭＡＣ２１２７は、ＭＤ５一方向ハッシュアルゴリズムを使用してＦＰＭクリアイベント２１３３から作成される。ＦＰＭを対象とするＥＡだけが、ＦＰＭ暗号化イベント２１２３を復号化するために、エンベロップ鍵２１０３を復号化して鍵２１１９を得、そしてそのＥＡは、ＦＰＭ２１０１を送信するＤＨＣＴ３３３のための公開鍵を有する場合のみ、ＦＰＭクリアイベント２１３３の認証をチェックし得る。

【０１５７】

本明細書中でさらに興味のあるＦＰＭ２１０１の部分は、ＦＰＭクリアイベント２１３３である。ＦＰＭのその部分における情報は、そのメッセージを送ったＤＨＣＴ３３３中のＤＨＣＴＳＥ６２７のシリアル番号、デスティネーションＥＡのＥＡＩＤ、およびＦＰＭが購入情報を含むイベントの数の表示を含む。各イベントのための情報は、そのイベントのための転送イベントデータ中に含まれる。転送イベントデータは、ＧＢＡＭ１８０１

およびイベントのためのイベント記述子１７０３から取り出される。現在の文脈における対象のフィールドは、（１）イベントが延長されたかどうか、（２）ユーザがイベントをキャンセルしたかどうか、および（３）顧客がコピーする権利を購入したかどうかを示すフラグを含む。他の情報は、イベントが始まった時間または購入された時間のどちらか遅い方、イベントの終了する時間、イベントの顧客に対するコスト、およびイベントのための登録ＩＤを含む。ＤＨＣＴ３３３は、普通のペイ－パー－ビューイベントを含む任意のイベントをキャンセルするために、キャンセルを示すために設定されたイベントキャンセル済フラグ以外は同じメッセージを有するＦＰＭを送信する。ＤＨＣＴ３３３がＦＰＭキャンセルメッセージを送る条件は、以下に詳細に説明される。ＦＰＭはまた、例えば、月払い加入またはデータダウンロードなどの他のサービスタイプを購入するために使用され得る。

【０１５８】

（承認ＩＰＰＶ／ＮＶＯＤイベントＥＭＭ）

登録エージェントは、ＦＰＭを受信する場合、そのＦＰＭに含まれる情報をその顧客情報データベースに入力し、そして承認ＩＰＰＶ／ＮＶＯＤイベントＥＭＭをＤＨＣＴ３３３に返す。このＥＭＭ中のＥＭＭコマンドデータ１１２５は、ＥＭＭが承認しているＦＰＭ中の転送イベントデータの正確なコピーを含む。ＤＨＣＴＳＥ６２７は、このＥＭＭを受信する場合、それを復号化および認証し、そして次に、コピーされた転送イベントデータの各項目に対して、登録ＩＤを使用してイベントのためのイベントＮＶＳＣ１７０１を配置する。ＤＨＣＴＳＥ６２７は、イベントＮＶＳＣ１７０１を配置した場合、コピーされた転送イベントデータをイベントＮＶＳＣ１７０１の対応するフィールドと比較する。それらが同じである場合、ＤＨＣＴＳＥ６２７は、購入が確認されたことを示すフラグをフラグフィールド１７０５中に設定し、そして格納されたクレジットバランスを調整する。ＥＭＭがその「キャンセル」フラグをセットされた場合、イベントＮＶＳＣ１７０１中の「使用中」フラグは、イベントＮＶＳＣ１７０１が使用中でなく、そしてしたがって登録エージェントによって再使用に利用可能であることを示すように設定される。

【０１５９】

（ＧＢＡＭ１８０１の他の使用）

ＧＢＡＭ１８０１は、認証されたメッセージを、ＭＰＥＧ－２転送システム、または他の転送メカニズムを介してＤＨＣＴ３３３に放送するように一般に使用され得る。ＣＡシステム６０１自身は、ＧＢＡＭ１８０１を２つの他の方法で使用する：時間値をＤＨＣＴ３３３へ定期的に放送する方法、およびイベントの時間を延長する方法。前者の場合、ＧＢＡＭ１８０１は、ＧＢＡＭの認証により、安全な時間である時間値を単に搬送する。システム時間ＧＢＡＭを送る登録エージェントのためのタスクを実行するＤＨＣＴ３３３中のコードは、時間値を使用してその動作とＥＡによる動作とを協調させる。但し、この構成は、登録エージェントごとの時間スキームの使用を可能にする。それはまた、デジタル放送送達システムの各ＤＨＣＴ３３３中の１つの登録エージェントを「システム時間登録エージェント」として設定し、そしてシステム時間ＧＢＡＭをシステム時間登録エージェントにアドレッシングすることによって、デジタル放送送達システム全体を通して均一なシステム時間を確立することを可能にする。

【０１６０】

イベントの時間を延長するＧＢＡＭ１８０１は、イベントのための登録ＩＤ、およびイベントのための時間が延長される分数（ｎｕｍｂｅｒ　ｏｆ　ｍｉｎｕｔｅｓ）を搬送する。ＧＢＡＭ１８０１がＤＨＣＴＳＥ６２７に受信および提供される場合、セキュリティエレメントは、分数を終了時間１７０９に付加する。

【０１６１】

図２０は、登録エージェント２００５、および１グループのＤＨＣＴ３３３によって受信されるＭＰＥＧ－２転送システムへのアクセスを有するプロセッサ上で実行するサーバアプリケーション２００１を示す。サーバアプリケーション２００１は、ＧＢＡＭ１８０１を使用して認証されたメッセージをＤＨＣＴ３３３へ送信する。サーバアプリケーショ

ン２００１は、メッセージを登録エージェント２００５に送信する。登録エージェント２００５は、そのトランザクション暗号化デバイス６０３を使用してペイロードを含むＧＢＡＭ１８０１を作成する。次に、登録エージェント２００５は、ＧＢＡＭをサーバアプリケーション２００１に返し、サーバアプリケーション２００１は、２００７で示されるように、アプリケーションデータをＧＢＡＭとともにＤＨＣＴ３３３中のクライアントアプリケーション２００９に送信する。各クライアントアプリケーションは、ＧＢＡＭ１８０１をそれを認証するＤＨＣＴＳＥ６２７に送信する。認証が成功する場合、ＤＨＣＴＳＥ６２７は、承認をクライアントアプリケーション２００９に送信する。ここで注意すべきことは、ペイロードを認証するのは、登録エージェントであって、サーバアプリケーション２００１ではないことである。

【０１６２】

（インタラクティブセッションのためのＮＶＳＣおよびＥＭＭ）

ＤＢＤＳ５０１はまた、インタラクティブセッションのために使用され得る。そのような使用の例は、インターネットの閲覧すること、またはビデオゲームをすることである。そのようなアプリケーションにおいて、顧客に送信されるデータは、一般にＭＰＥＧ－２転送ストリームを介して転送される一方、顧客から送られるデータは、逆向きチャネルを介して転送される。そのような構成は、顧客が大量のデータ（例えば、画像を表すデータ）を受信し、短い応答を行い、そして次に別の大量のデータを受信する多くのインタラクティブアプリケーションに対して有利である。

【０１６３】

ＤＨＣＴ３３３のユーザとの現在起こっている各インタラクティブセッションは、そのインタラクティブセッションにアクセスを与える登録エージェントに属するリスト１４１１中のインタラクティブセッションＮＶＳＣ１２１１を有する。インタラクティブセッションＮＶＳＣは、インタラクティブセッションのためのセッション鍵、およびインタラクティブセッションのための登録ＩＤを含む。ＤＨＣＴＳＥ６２７は、登録エージェントからの新しいインタラクティブセッション格納ＥＭＭに応答してインタラクティブセッションＮＶＳＣを割り当てる。新しいインタラクティブセッション格納ＥＭＭは、そのインタラクティブセッションのために使用されるＮＶＳＣのセル名を単に含む。

【０１６４】

ＥＡは、一旦ＮＶＳＣを確立すると、「追加インタラクティブセッション」ＥＭＭを送信する。追加インタラクティブセッションＥＭＭは、新しく割り当てられたＮＶＳＣの名前に関し、そして登録ＩＤ、およびインタラクティブセッションのための鍵を含む。セキュリティエレメントは、ＮＶＳＣ中に登録ＩＤおよび鍵を配置する。ＥＡは、インタラクティブセッションが終了したことを決定する場合、インタラクティブセッションのための登録ＩＤを有する「除去インタラクティブセッション」ＥＭＭを送信し、そしてセキュリティエレメントは、ＮＶＳＣの内容を削除する。ＣＡＡによってＥＡに割り当てられるインタラクティブセッションＮＶＳＣのすべてがすでに使用中である時点で、登録エージェントが新しいインタラクティブ格納ＥＭＭを送信することは、当然可能である。好ましい実施態様におけるＤＨＣＴＳＥ６２７は、各インタラクティブセッションがデータを送信または受信した最後の時間を把握することによってこの状況を取り扱う。新しいインタラクティブセッションが必要とされ、そして全く利用可能でない場合、ＤＨＣＴＳＥ６２７は、最も最近にデータを送信または受信したインタラクティブセッションをシャットダウンし、そしてそのインタラクティブセッションの、新しいインタラクティブセッションのためのインタラクティブセッションＮＶＳＣを使用する。別の解決法は、ユーザに終了すべきインタラクティブセッションを選択するように要求することである。

【０１６５】

（ＥＣＭの詳細：図２２）

ＥＣＭがともなうサービスのインスタンスが所定のＤＨＣＴ３３３において復号化されるかどうかを決定するために使用されるＥＣＭ中の情報は、ＥＣＭ登録ユニットメッセージ１０１１に含まれる。図２２は、本発明の好ましい実施態様のためのＥＣＭ登録ユニッ

トメッセージ１０１１の内容の詳細を与える。まずメッセージＩＤ２２０５は、２つのフィールド２２０１および２２０３がこのメッセージをＥＣＭ登録ユニットメッセージとして識別する。ＥＡＩＤ２２０７は、ＥＣＭがともなうサービスのインスタンスにアクセスするための登録を授与する登録エージェントのための識別子である。

【０１６６】

復号化情報２２０９は、制御ワード２２３５を生成するために使用される情報である。制御ワードカウンタ値２２３５は、好ましい実施態様において３ＤＥＳアルゴリズムを使用して暗号化される。このアルゴリズムは、２つの鍵を使用し、そして好ましい実施態様においては、各鍵がＭＳＫの１／２である。また、ＭＳＫの２つのバージョンが存在する：偶数および奇数である。ＭＳＫパリティ２２１１は、どのバージョンが３ＤＥＳアルゴリズムにおいて使用されるかを特定する。ＭＳＫ　ＩＤ２２１３は、登録エージェントのどのＭＳＫが使用されるかを特定し、そしてＥＣＭがインタラクティブセッションのためのデータをともなう場合は、その鍵がそのインタラクティブセッションのためのＮＶＳＣにおいて見出されることを特定する。制御ワードパリティ２２１５は、未暗号化制御ワード２２３５のパリティを特定する。パリティカウント２２１７は、制御ワードのパリティが偶数の場合に値０、そしてそれが奇数の場合に値１を有する０－１カウンタである。

【０１６７】

フリープレビュー２２１９は、ＥＣＭが、フリープレビューであるサービスインスタンスの一部をともなっていることを示すフラグである。すなわち、顧客がサービスインスタンスのためのＭＳＫを有する限り、その顧客は、サービスのフリープレビュー部分を視聴するためのさらなる登録を全く必要としない。フリープレビューは、主にＩＰＰＶまたはＮＶＯＤサービスとともに使用される。コピー保護レベル２２２１は、インスタンスがどの程度コピーされるかを示す値である。ブラックアウト／スポットライト２２２３は、ブラックアウト／スポットライト情報２２３６がどのように使用されるかを示す値である：全く使用されないか、ブラックアウトか、またはスポットライト（すなわち、サービスが特定の領域を標的とする）かである。

【０１６８】

登録ＩＤ２２２５の番号は、このＥＣＭ中に含まれる登録ＩＤ２２４５の数を特定する。好ましい実施態様における最大値は、１つのＥＣＭにおいて６である。複数のＥＣＭが各サービスごとに送信され得る。ＩＰＰＶ可能２２２９は、サービスインスタンスが１つのＩＰＰＶまたはＮＶＯＤごとに視聴され得るかどうかを示すフラグである。キャンセルウインドウ２２３１は、顧客がイベントをキャンセルし得る期間の最後を示すために、イベントとして視聴され得るサービスインスタンス中に設定されるビットである。タイムスタンプ２２３３は、ＥＣＭが作成された時間を示すタイムスタンプである。暗号化制御ワード２２３５は、ＥＣＭ中に含まれる制御ワードである。それは、３ＤＥＳアルゴリズム、およびサービスインスタンスのためのＭＳＫを使用して暗号化される。

【０１６９】

ブラックアウト／スポットライト情報２２３６は、サービスのインスタンスによってブラックアウトされるか、またはスポットライトされる地理的領域を定義する。これは、ｘ重心２２３９およびｙ重心２２４１によって行われる。この２つの重心は、登録エージェントによって定義される地理的座標系における点、およびブラックアウト半径２２３７を定義する。ブラックアウト半径２２３７は、フィールド２２３９および２２４１によって定義される点を中心とする、そしてブラックアウト半径２２３７の値の２倍の辺を有する正方形を決定するために使用される。登録ＩＤリスト２２４３は、ＥＣＭがともなうサービスのインスタンスのための１～６登録ＩＤを含む。

【０１７０】

（ブラックアウト／スポットライト情報２２３６の詳細：図２６および２７）

好ましい実施態様において使用される座標系は、図２６において使用される。座標系２６０１は、２５６ユニット×２５６ユニットの正方形であり、その原点は左下隅にある。その座標系において、番号付けされているのは、線であり、線の間の空間ではない。座標

系２６０１が属する登録エージェントは、その座標系によって覆われる領域における各ＤＨＣＴ３３３を、ｘ軸に垂直な線とｙ軸に垂直な線との交点の座標に割り当てる。このように、ＤＨＣＴ３３３（ｋ）は、座標系２６０１における点（ｉ，ｊ）２６０３を割り当てられ得る。

【０１７１】

図２７は、領域が座標系２６０１においてどのように定義されるかを示す。領域２７０５は、その重心２７０１を座標が（５７，９０）である点に有する。その領域の半径２７０３は、３であり、そこでこの数を重心の各座標値から加算および減算して、左下隅が（５４，８７）にあり、そして右上隅が（６０，９３）にある正方形２７０５を生成する。好ましい実施態様において、左および下の線上の点は、領域中に含まれ、上および右の線上の点は、領域中に含まれない。

【０１７２】

（ＥＣＭをともなうサービスインスタンスを復号化するかどうかの決定）

概念的には、ＤＨＣＴ３３３がサービスのインスタンスをともなうＥＣＭを受信する場合に起こることは、ＤＨＣＴ３３３がそのＥＣＭをＤＨＣＴＳＥ６２７に提供し、ＤＨＣＴＳＥ６２７が、ＥＡ格納部１３３１中のＮＶＳＣを検査して、ＤＨＣＴ３３３の属する顧客がサービスのインスタンスを受信するように登録されたかどうかを見出すことである。顧客がそのように登録された場合、ＤＨＣＴＳＥ６２７は、ＥＣＭ中の制御ワードを復号化し、そしてそれをサービス復号化器６２５に提供する。サービス復号化器６２５は、それを使用してサービスのための音声および映像を含むＭＰＥＧ－２パケットを復号化する。しかし、異なる種類のサービスの数、サービスを購入され得る異なる方法の数、およびアクセスが制限され得る方法の数は、すべて一緒に機能してＤＨＣＴＳＥ６２７がＥＣＭを処理する方法をむしろ複雑にする。

【０１７３】

最も単純な場合は、標準的なＣＡＴＶチャネルなどの放送サービスのための場合である。ここで、ＤＨＣＴ３３３を有する顧客は、サービスに対する自分の月々の料金を支払って、そして登録オーソリティは、２つのＥＭＭをＤＨＣＴ３３３に送信した：サービスのための月のＭＳＫを有するＭＳＫ　ＥＭＭ、およびサービスのための登録ＩＤを特定するＥＭＭである。上記に指摘したように、後者のＥＭＭは、登録ＩＤのリスト、または第１登録ＩＤおよびビットマップのいずれかを含み得る。これらのＥＭＭのすべてはまた、期限日を含み得る：ＭＳＫ　ＥＭＭの場合、ＭＳＫの期限日が存在する；登録ＩＤリストＥＭＭの場合、リスト上の各登録ＩＤのための期限日が存在する。登録ビットマップＥＭＭの場合、全ビットマップのための期限日が存在する。

【０１７４】

少なくとも、ＥＣＭがともなっているサービスインスタンスのための登録を提供する登録エージェントのためのＥＡ情報１３３３は、ＥＡ記述子１４０９、ＭＳＫ　ＮＶＳＣ１６０１、および登録ビットマップＮＶＳＣ１６１３またはインスタンスが属するサービスのための登録リストＮＶＳＣ１６２３を含む。ＥＡ情報１３３３はまた、他のサービスまたはインスタンスのための登録情報を有するＮＶＳＣを含む。

【０１７５】

サービスインスタンスのためのＥＣＭは、少なくとも、サービスのインスタンスのための登録エージェントＩＤ２２０７、復号化情報２２０９、タイムスタンプ２２３３、暗号化制御ワード２２３５、および１つの登録２２４５を含み得る。

【０１７６】

ＤＨＣＴ３３３は、ＥＣＭを受信する場合、そのＥＣＭをＤＨＣＴＳＥ６２７に送達し、ＤＨＣＴＳＥ６２７は、そのＥＣＭ中の値ＥＡＩＤ２２０７と同じであるＥＡＩＤ１５０９中の値を有するＥＡ記述子１４０９を見つけるまでＥＡリスト１４０６を読み進む。次に、ＤＨＣＴＳＥ６２７は、第１ＮＶＳＣポインタ１５１３からリスト１４１１を進み、そしてＥＣＭ中のＭＳＫ　ＩＤフィールド２２１３と同じ値を含むＭＳＫ　ＩＤフィールド１６０３を有するＭＳＫ　ＮＶＳＣ１６０１を探す。そのようなＭＳＫ　ＮＶＳＣを

見つけた場合、ＤＨＣＴＳＥ６２７は、非期限日フラグ１６０７から、期限日フィールド１６０５が有効な時間値を有するかどうかを決定し、そして有する場合、ＤＨＣＴＳＥ６２７は、その値とＥＣＭのタイムスタンプフィールド２２３３とを比較する。タイムスタンプフィールド２２３３中の値が時間においてより最近である場合、ＤＨＣＴＳＥ６２７は、制御ワード２２３５を復号化するためにはＭＳＫ　ＮＶＳＣ１６０１からのＭＳＫ１６０８を使用しない。セキュリティエレメントは、適切なＭＳＫ　ＩＤおよび期限切れでないＭＳＫを用いてＭＳＫ　ＮＶＳＣを検索し続け、そしてそのようなＭＳＫ　ＮＶＳＣを見つけた場合、そのＭＳＫ　ＮＶＳＣを使用する；セキュリティエレメントは、そのようなＭＳＫ　ＮＶＳＣを見つけなかった場合、制御ワードを復号化しない。

【０１７７】

ＤＨＣＴＳＥ６２７は、登録ビットマップＮＶＳＣ１６１３のためのリスト１４１１、またはＥＣＭ中の登録ＩＤ２２４５の１つと同じである登録ＩＤを含む登録リストＮＶＳＣ１６２３を単に検索する。（１）ＤＨＣＴＳＥ６２７がそのような登録ＩＤを有するＮＶＳＣを見つけた場合、および（２）ＥＣＭ中のタイムスタンプ２２３３より早い登録ＩＤを特定するＮＶＳＣ中に有効な期限時間が存在しない場合、および（３）ＤＨＣＴＳＥ６２７がまた上記のように有効なＭＳＫ　ＮＶＳＣ１６０１を見つけた場合、ＤＨＣＴＳＥ６２７は、ＥＣＭ中のＭＳＫおよび復号化情報２２０９を使用して制御ワード２２３５を復号する。復号化は、制御ワードを暗号化するために使用された３ＤＥＳアルゴリズムを使用してなされる。好ましい実施態様において、ＥＣＭ中に含まれる制御ワードは、上記のようなカウンタ値であり、そしてＤＨＣＴＳＥ６２７は、ＭＳＫおよび３ＤＥＳアルゴリズムを使用して整数を再暗号化することによってサービスインスタンスを復号化するために実際に使用される制御ワードを生成する。次に、サービス復号化器によって使用可能なその制御ワードは、サービス復号化モジュール６２５に返され、サービス復号化モジュール６２５は、その制御ワードを使用してサービスインスタンスを復号化する。

【０１７８】

上記から明らかなように、ＤＨＣＴＳＥ６２７は、サービスに対する所定の登録のための登録エージェントの登録エージェント情報１３３３を検索する場合、その登録を含むＮＶＳＣを見つけたか、またはリスト１４１１の最後に達したかのいずれかまで検索を続ける。これが論理上で意味するところは、所定の登録エージェントが与え得る登録は、登録エージェント情報１３３３中に特定される論理ＯＲである。例えば、ＥＣＭと同じ登録ＩＤを含む１つの登録ビットマップＮＶＳＣが期限切れしたが、別のがまだである場合、ＤＨＣＴＳＥ６２７は、期限切れしたＮＶＳＣを除去し、そしてアクティブＮＶＳＣに基づいて、制御ワード２２３５を生成する。

【０１７９】

ここでさらに指摘すべきことは、ＥＣＭ中のタイムスタンプ２２３３およびＮＶＳＣ中の期限情報が現在の月におけるインスタンスを復号化するために前月のＭＳＫの再使用を抑制し、そしてまた、上記のＢａｎｋｅｒおよびＡｋｉｎｓの特許出願に記載の再生攻撃に対する保護を実施するために現在月における前月の登録の再使用を抑制する。

【０１８０】

さらなる制限が登録に課される場合、ＤＨＣＴＳＥ６２７は、その情報を登録エージェント情報１３３３においても同様に検索する。例えば、ＥＣＭのブラックアウト／スポットライトフィールド２２２３が、ブラックアウトがサービスに適用されることを示す場合、ＤＨＣＴＳＥ６２７は、ブラックアウト／スポットライト情報２２３６を使用してｘ座標１５２１およびｙ座標１５２３によって特定される位置がブラックアウト／スポットライト情報２２３６によって特定される正方形内にあるかどうかを決定する；そうである場合、ＤＨＣＴＳＥ６２７は、制御ワード２２３５を復号化しない。スポットライトが適用される場合、その手順は、当然反対である：ＤＨＣＴＳＥ６２７は、ｘ座標フィールド１５２１およびｙ座標フィールド１５２３が正方形内の位置を特定する場合のみ制御ワードを復号化する。

【０１８１】

上記のように、地理的領域にしたがって登録を授与するために使用される技術は、顧客の種々の部分集合に登録を授与するように一般化され得る。例えば、登録は、ベン図において概念的に表され得、ブラックアウト／スポットライト情報２２３６は、サービスを受信するために登録された顧客のセットを表すベン図における領域を特定し得、そしてｘ座標１５２１およびｙ座標１５２３は、ベン図における顧客の位置を特定する。そのような構成の１つの使用は、顧客のＤＨＣＴが好ましくない内容を有するインスタンスへのアクセスを有さないという顧客の希望にしたがってサービスのインスタンスへのアクセスを限定することである。他の実施態様において、多い座標、または集合の親子関係を表す他の方法が当然使用され得る。

【０１８２】

（イベントサービス）

ＥＣＭがイベントのある例を伴う場合、このイベントについての登録情報がイベントＮＶＳＣ１７０１内に含まれることを除いては、上述のようにＥＣＭのインタプリテーションが行われる。ＤＨＣＴＳＥ６２７は、ＥＣＭ内の登録ＩＤ２２４５の１つと同じである登録ＩＤ１７１３を有するイベント記述子１７０３を含むイベントＮＶＳＣ１７０１についてのＥＣＭであるＥＡＩＤを有する登録エージェントについて、エンタイトル情報１３３３を検索する。イベントが標準ペイパービューイベントである場合、ＤＨＣＴＳＥ６２７はフラグ１７０５を調べて、顧客がイベントをキャンセルしたかどうか、および、イベントの購入が確認されたかどうかを判定する。（標準ペイパービューで、いつも行われる。）次に、ＤＨＣＴＳＥ６２７は購入時刻１７０７および終了時刻１７０９を時刻スタンプ２２３３と比較して、時刻スタンプによって示された時刻がフィールド１７０７および１７０９に示された期間内にあるかを判定する。イベントＮＶＳＣ１７０１の調査が、顧客がイベントに対する資格を与えられていることを示すと、ＤＨＣＴＳＥ６２７は、上述のように制御ワード２２３５を復号化する。

【０１８３】

ＩＰＰＶまたはＮＶＯＤイベントで、ＥＣＭ内の許可ＩＰＰＶフラグ２２２９は、そのイベントが前もって購入する必要のないイベントであることを示す必要がある。フリープレビューフラグ２２１９はまた、ＥＣＭを伴うイベントの例の一部がフリープレビューの一部であることを示すように設定され得、かつ、キャンセルウィンドウフラグ２２３１は、そのイベントが依然キャンセルされ得ることを示すようにさらに設定され得る。フリープレビューフラグ２２１９が設定される場合、ＤＨＣＴＳＥ６２７は単に、ＥＣＭ内のＭＳＫ　ＩＤ２２１３によって指定されるＭＳＫを含むＥＡ情報１３３３内のＭＳＫ　ＮＶＳＣ１６０１を探す。

【０１８４】

フリープレビューフラグ２２１９が設定されない場合、ＤＨＣＴＳＥ６２７は、ＥＣＭフィールド２２４５内の登録ＩＤと同じである登録ＩＤ１７１３を有するイベントＮＶＳＣ１７０１へ行く。フラグ１７０５に含まれるフラグが、イベントの購入が確認され、かつ、イベントがキャンセルされていないことを示す場合、ＤＨＣＴＳＥ６２７は、制御ワード２２３５を復号化する。イベントがキャンセルされておらず、かつ、確認されていないが、時刻スタンプ２２３３が、イベント記述子１７０３に示された購入時刻１７０７の後の所定の期間内の時刻を示す場合、ＤＨＣＴＳＥ６２７はまた、制御ワード２２３５を復号化する。このようにして、サービスの例は、ＦＰＭが登録エージェントに送られる時刻と、登録エージェントがアクノリッジＩＰＰＶ／ＮＶＯＤイベントＥＭＭを戻す時刻との間に復号化され続ける。このことにより、確認フラグがフラグ１７０５内に設定される。

【０１８５】

（イベントに対する登録のキャンセル：図１７、１９，および２２）

ユーザが既に購入したＩＰＰＶ／ＮＶＯＤイベントに対する登録をユーザがキャンセルできるかどうかは、好適には、そのイベントによって決まる。これには３つの可能性がある：

・登録は購入後２分までキャンセルできる。

【０１８６】

・イベントは、「キャンセルウィンドウ」と呼ばれる期間の間、キャンセルできる。

【０１８７】

・イベントをキャンセルすることはできない。

３つの可能性のうちのいずれが所定のイベントに関連するかは、イベントに付随するＧＢＡＭ内の購入可能登録データ１９１３によって判定される。フラグ１９１７内の１つのフラグが、イベントをキャンセルできるかどうかを示し、別のフラグが、キャンセルが可能であることをキャンセルウィンドウ内に示す。いずれのフラグも設定されない場合、イベントをキャンセルすることはできない。ＤＨＣＴＳＥ６２７は、そのイベントについてのイベント記述子１７０３を形成する。ＧＢＡＭ内のフラグの値は、イベントがキャンセルされ得るかどうか、またはキャンセルウィンドウの間にのみキャンセルし得ることを示すフラグ１７０５内のフラグを設定するのに使用される。再び、いずれのフラグも設定されない場合、イベントをキャンセルすることはできない。

【０１８８】

顧客入力６２８を介してＤＨＣＴ３３３にキャンセルを要求することにより、ユーザはイベントをキャンセルする。ＤＨＣＴ３３３がその入力を受け取る場合、ＤＨＣＴ３３３は、ＥＡＩＤおよび登録ＩＤを用いて、そのイベントについてのイベント記述子１７０３を含むイベントＮＶＳＣ１７０１を配置するこの例についての、ＥＡＩＤおよび登録ＩＤを含むキャンセル要求を、ＤＨＣＴＳＥ６２７に提供する。フラグ１７０５内のフラグが、登録をキャンセルすることが登録をキャンセルできないことをユーザに示す。登録をキャンセルすることができることをフラグが示す場合、ＤＨＣＴＳＥ６２７は、単に、キャンセルされたフラグをイベント記述子１７０３にセットする。キャンセルウィンドウの間にのみ登録がキャンセルされ得、かつ、キャンセルウィンドウが終了したことを示すＥＣＭフラグが未だ受け取られていないことをフラグが示す場合、ＤＨＣＴＳＥ６２７は、キャンセルフラグをイベント記述子１７０３にセットする。そうでない場合には、登録をキャンセルすることができないことをＤＨＣＴ３３３に示し、ＤＨＣＴ３３３がユーザにその旨を知らせる。イベントがキャンセルされた場合、ＤＨＣＴＳＥ６２７は承認されたフラグをクリアし、このアクションが、新たなＦＰＭをイベントについての登録エージェントに送信させる。登録エージェントは、キャンセルによって要求されるそのビリングを調節し、新たな承認ＥＭＭを送信することにより、ＦＰＭに応答する。

【０１８９】

（インタラクティブセッション）

放送サービスとインタラクティブサービスをの間の主要な差は、インタラクティブサービスの各セッションが、そのインタラクティブセッションについてのインタラクティブセッションＮＶＳＣに含まれる、それ自体のインタラクティブセッション鍵を有する点にある。インタラクティブセッションについてのＮＶＳＣはまた、インタラクティブセッションについての登録ＩＤを含む。インタラクティブセッションについてのＭＰＥＧ－２ストリームを伴うＥＣＭにおいて、ＭＳＫ　ＩＤフィールド２２１３は、ＭＰＥＧ－２ストリームがインタラクティブセッション鍵を用いて復号化されることを示す値に設定される。ＤＨＣＴＳＥ６２７がＥＣＭ等を解釈する場合、ＤＨＣＴＳＥ６２７は登録ＩＤ２２４５を用いて、そのインタラクティブセッションについてのＮＶＳＣを見つけ、そして、ＮＶＳＣに含まれるインタラクティブセッション鍵を用いて制御ワード２２３５を復号化する。

【０１９０】

（トランザクション暗号化デバイス６０３の詳細な説明：図２４および図２５）

デジタル広帯域配信システム５０１内の登録エージェントに権限を与え得る各ＣＡＡ、および、システム５０１内の登録を許可し得る各ＥＡは、システム５０１内にトランザクション暗号化デバイスまたはＴＥＤ６０３を有する。好適には、各ＣＡＡまたはＥＡは、

システム６０１内にそれ自身の分離ＴＥＤを有する。あるいは、ＴＥＤは１つのデバイスに組み合わされ得る。ＴＥＤ６０３は、それの属するエンティティによって使用されるプライベート鍵を格納し、かつ、そのエンティティによって必要とされる暗号化、復号化、鍵生成、および認証を行うためのハードウェアおよびソフトウェアを有する。ユーザインターフェースまたはユーザＩ／Ｏデバイスなしでの ＴＥＤを実行し、不正改変不可能なコンテナ内でＴＥＤを実行し、ＴＥＤをＤＮＣＳにのみ接続し、かつ、その接続についてのセキュリティリンクを使用し、さらに、ＴＥＤをロックルーム等の物理的に安全な環境内に維持することにより、鍵は安全性を維持される。

【０１９１】

ＣＡＡについてのＴＥＤ６０３の場合、ＴＥＤ６０３は、ＤＨＣＴ３３３内のＣＡＡを表す３つの公開鍵に対応するプライベート鍵を格納し、ＣＡＡからＤＨＣＴ３３３へと、ＥＭＭの封印されたダイジェストを暗号化および提供し、そして、ＤＨＣＴ３３３からＣＡＡへとメッセージを復号化して、認証する。ＥＡについてのＴＥＤ６０３の場合、ＥＡ ＴＥＤは以下のことを行う：

（１）ＥＡについての公開鍵およびプライベート鍵、ならびにＥＡについてのＭＳＫを格納する。

【０１９２】

（２）ＥＡ公開鍵およびプライベート鍵ならびにＭＳＫを生成する。

【０１９３】

（３）ＥＡの代わりに送信されたＥＭＭについての封印されたダイジェストの暗号化および準備を行う。

【０１９４】

（４）グローバル放送メッセージに権限を与えるために使用される共有された秘密ダイジェストを準備する。

【０１９５】

（５）サービスの例を暗号化に用いるために、ＳＥＥＳモジュール６２０にＭＳＫを提供する。

【０１９６】

（６）インタラクティブセッションＥＭＭについてのインタラクティブセッション鍵（ＩＳＫ）を生成し、インタラクティブセッションを暗号化するために、それらをＳＥＥＳモジュール６２０に提供する。

【０１９７】

（７）ＤＨＣＴ３３３から登録エージェントに送信されたＦＰＭおよび他のメッセージを復号化する。

【０１９８】

（条件付けアクセスシステム６０１におけるＴＥＤ６０３：図２４）

図２４は、ＴＥＤ６０３の数と条件付きアクセスシステム６０１の残りの部分との関係を示す。条件付きアクセスシステム６０１の部分２４０１は、システム６０１内の登録エージェントに権限を与えるＣＡＡについてのＣＡＡ ＴＥＤ２４２７を含む。部分２４０１はまた、デジタル広帯域配信システム５０１におけるＤＨＣＴ３３３について現在権限が与えられている、ＣＡＡが有するｎ＋１個の登録エージェントの各々についての１つのＥＡ ＴＥＤ２４２５を含む。あるいは、全てのＥＡ ＴＥＤ２４２５機能は、単一のＴＥＤに組み合わされ得る。この単一のＴＥＤは、ＣＡＡ ＴＥＤ２４２７機能を含み得る。各ＴＥＤは、物理的に安全な領域２４２８内に維持され、かつ、ＤＮＣＳ５０７およびＴＥＤ６０３にのみ接続する安全高速リンク２４２３によってＤＮＣＳ５０７に接続される。好適な実施形態において、セキュリティリンクは、セキュリティイーサネット（登録商標）リンクである。ＤＮＣＳ５０７はＴＥＤ６０５を用いて、ＥＭＭを暗号化し、ＦＰＭを復号化し、ＥＡ公開鍵およびプライベート鍵を生成し、ＭＳＫおよびＩＳＫを生成し、そして、グローバル放送メッセージダイジェストを準備する。ＤＮＣＳ６０７は、これらの動作を実行するＴＥＤ６０３への遠隔手続き呼び出しインターフェースを有し、そし

て結果的に、ＤＮＣＳ６０７上で実行されるプログラムは、単に手続き呼び出しを行うことにより、ＴＥＤの機構を使用し得る。

【０１９９】

ＤＮＣＳ５０７は、所定のＴＥＤ６０３と条件付きアクセスシステム６０１の残りの部分との間の唯一の接続である。ＤＮＣＳ５０７は、ネットワーク２４１５によって、ＣＡＡおよびさまざまなＥＡに属するシステムに接続される。これらのエンティティの各々が、その機能に関連する情報を含むデータベースを有する。ＣＡＡ２４０５は、少なくともＣＡＡの３つの公開鍵および暗号化されたバージョンの対応する３つのプライベート鍵を含むＣＡＡデータベース２４０３、ＣＡＡが権限を与える登録エージェントについての登録エージェント識別子、ならびに、ＤＨＣＴについて権限を与えられた各登録エージェントにＣＡＡが割り当てられたＮＶＳＣの名前、タイプ、および、番号を含むｐｅｒ－ＤＨＣＴデータベースを有する。

【０２００】

各ＥＡ２４０９（ｉ）は、それ専用のＥＡデータベース２４０７（ｉ）を有する。ＥＡデータベース２４０７（ｉ）は、好適には、ＥＡについてのＥＡＩＤ、ＥＡが現在使用しているＭＳＫについてのＭＳＫ　ＩＤおよび満了日のリスト、ならびに、ＥＡが提供しているサービスおよび／またはインスタンスのデータベースを含む。このサービスのデータベースは、少なくとも、各サービスについての登録ＩＤを含む。ＥＡデータベース２４０７（ｉ）はまた、登録ＩＤのｐｅｒ－ＤＨＣＴデータベース、登録満了時刻、ならびに登録についてのＭＳＫ　ＩＤおよびＥＭＭ内でＤＨＣＴに送信されるＭＳＫを含む。ｐｅｒ－ＤＨＣＴデータベースはまた、ＦＰＭ内の購入情報を取り扱うために要求される情報等の顧客ビリング情報を含む。

【０２０１】

鍵証明機関２４１３は、ＤＮＣＳ５０７に対して、ＤＨＣＴ３３３の公開鍵を証明するエンティティである。好適な実施形態において、鍵証明機関２４１３は、ＤＨＣＴ３３３の製造者によって維持される。ＤＨＣＴ鍵データベース２４１１は、ＤＨＣＴシリアルナンバーおよびそれらの公開鍵のデータベースを含む。ＤＨＣＴ３３３のユーザがＥＡによって提供されるサービスのインスタンスを購入したいと望む場合、ユーザは購入申し込みをＤＨＣＴ３３３のシリアルナンバー（これはＩＰアドレスでもある）を有するＥＡへ送信する。ＥＡはＤＮＣＳ５０７にシリアルナンバーを提供し、これが、ＤＨＣＴ公開鍵のデータベース２４２１をシリアルナンバーにより維持する。このシリアルナンバーがデータベース内にない場合、ＤＮＣＳ５０７は、公開鍵についての要求をＫＣＡに送信する。この要求はシリアル番号を含み、鍵証明機関は、デジタル的に署名されたメッセージ２４１２をＤＮＣＳ５０７に送信することにより要求に応答する。このメッセージはＤＨＣＴ公開鍵を含む。ＤＮＣＳ５０７は、鍵証明機関についての公開鍵を有し、かつ、公開鍵およびデジタル署名を用いて、メッセージ内のＤＨＣＴ公開鍵の正当性を確認する。公開鍵が正当である場合、ＤＮＣＳ５０７は、それを公開鍵データベース２４２１内に配置する。

【０２０２】

ＤＮＣＳ５０７は、別の高速リンク２４１７を介してＳＥＥＳ６２０にさらに接続される。ＳＥＥＳ６２０は、サービスのインスタンスを暗号化するＭＳＫを備えている。さらに、ＤＮＣＳ５０７は、グローバル放送メッセージ（ＧＢＡＭ）および放送のためのＥＭＭを、トランスポートリンク５１７を介してＤＨＣＴ３３３に提供する。最後に、ＤＮＣＳ５０７は、ＬＡＮ相互接続デバイス６１７によって提供される逆パスを介してＤＨＣＴ３３３に接続され、そして、ＤＨＣＴ３３３からＦＰＭを受け取る。他の実施形態において、ＤＨＣＴ３３３はまた、この経路により、ＥＭＭをＤＨＣＴ３３３に送信し得る。

【０２０３】

部分２４０１内のデータフローは、構成要素をつなぐ矢印上のラベルにより示される。したがって、ＥＡ２４０８（ｉ）は、ＥＡ　ＥＭＭの暗号化されなかったコンテンツ２４１０およびグローバル放送メッセージをＤＮＣＳ５０７に送信し、かつ、ＥＡについての

ＦＰＭの暗号化されなかったコンテンツ２４１２をＤＮＣＳ５０７から受け取る。ＥＡ　ＥＭＭおよびグローバル放送メッセージで、ＤＮＣＳ５０７はＥＡ　ＴＥＤ２４２５（ｉ）を用いて必要な暗号化、ダイジェスト生成、および鍵生成を行い、そして、暗号化されかつ認証されたＥＭＭおよびグローバル放送メッセージ、ならびにＭＳＫを２４２６および２４１８に示すように、ＳＥＥＳ６２０に送信する。ＥＭＭの場合、ＥＭＭは延長された期間の間繰り返しＤＨＣＴに送信されるが、ＤＮＣＳ５０７は暗号化されたＥＭＭをＥＭＭデータベース２４２０に格納し、そして、それらをここからＳＥＥＳ６２０に提供する。ＦＰＭで、ＤＮＣＳ５０７は、ＦＰＭがアドレスされるＥＡ２４０９（ｊ）についてのＥＡ　ＴＥＤ２４２５（ｊ）を用いて、復号化および認証を行い、そして、復号化されたＦＰＭコンテンツ２４１２をＥＡ２４０９（ｉ）に送信する。ＤＮＣＳ５０７は、暗号化およびダイジェスト生成がＣＡＡ　ＴＥＤ２４２７を用いて行われることを除いては、ＥＡ　ＥＭＭと同じ方法でＣＡＡ　ＥＭＭを処理する。

【０２０４】

ＤＮＣＳ５０７はまた、暗号化されたエンティティ情報のデータベース２４１９を含む。これは、ＤＮＣＳ５０７に接続されたＴＥＤ６０９に格納されたプライベート鍵およびＭＳＫの暗号化されたコピーを含む。万一ＴＥＤの誤作動または物理的な崩壊が鍵情報の喪失を招く場合、この暗号化されたエンティティ情報は、ＴＥＤを再格納するために使用される。暗号化は、パス位相を用いてＴＥＤ内で行われる。情報が暗号化された場合、この暗号化された情報は、ＤＮＣＳ５０７に出力され、データベース２４１９に格納される。ＴＥＤが再格納される場合は、この情報はパス位相と共にＴＥＤに入力される。そして、このＴＥＤが鍵情報を復号化する。

【０２０５】

（ＴＥＤ２４２５（ｉ）の詳細な実行：図２５）

図２５は、ＥＡ　ＴＥＤ２４２５（ｉ）の好適な実施形態の詳細なブロック図である。好適な実施形態において、ＥＡ　ＴＥＤ２４２５（ｉ）は、標準コンピュータマザーボードおよび標準イーサネット（登録商標）ボードを有するシャーシ、ならびに、ＲＳＡ暗号化および復号化を促進するさらなる手段を用いて実行される。

【０２０６】

図２５に示すように、ＴＥＤ２４２５（ｉ）の主要な構成要素はＣＰＵ２５０１、メモリ２５０５、ハードウェア乱数生成器２５３７、イーサネット（登録商標）ボード２５４１、および複数のＲＳＡアクセラレータボード２５３９（０．．．ｎ）であり、バス２５０３によって全て相互接続されている。１つより多いＲＳＡアクセラレータボード２５３９を用いることにより、ＲＳＡ暗号化および／または復号化が並行して行われる。その結果、ＴＥＤ２４２５（ｉ）の好適な実施形態は、暗号化、ダイジェスト生成、または同様の速度での復号化を含む他の動作を行いつつ、複数のＥＭＭを極めて高速で、例えば１秒以内に、暗号化することができる。

【０２０７】

メモリ２５０５は、ＴＥＤ２４２５（ｉ）が属する登録エージェントについての公開およびプライベート鍵であるＥＡ情報２５０７と、ＥＡについてのＭＳＫと、ＣＰＵ２５０１によって実行されるコードであるコード２５２３とを含む。コード２５２３およびＥＡ情報２５０７を含むメモリ２５０５の部分は不揮発性であり、コード２５２３を含む部分は読み出し専用であり、ＥＡ情報２５０７を含む部分は読み出し可能かつ書き込み可能である。この説明で採りあげているコードは：

（１）乱数生成器２５３７によって提供される乱数からＭＳＫおよびＩＳＫを生成する、ＭＳＫ生成コード２５２５

（２）乱数から公開および秘密ＲＳＡ鍵を生成する、ＲＳＡ鍵生成器２５１７

（３）ＭＤ５一方向ハッシュアルゴリズムを実行する、ＭＤ５コード２５２９

（４）３ＤＥＳ暗号化および復号化を行う、３ＤＥＳコード２５３１

（５）グローバル放送メッセージを認証するのに使用される共有秘密ダイジェストを生成する、ＧＢＡＭ権限付与コード２５３３

（６）ＲＳＡハードウェア２５３９の援助によってＲＳＡ暗号化／復号化を実行する、ＲＳＡ暗号化／復号化コード２５３５
（７）ＤＮＣＳ５０７に格納するために、パス位相(pass phase)でＥＡ情報２５０７を暗号化する、ＥＡ情報暗号化コード２５３６
（８）暗号化されかつ認証されたＥＭＭを生成する、ＥＭＭコード２５３８
（９）ＦＰＭの復号化およびチェックを行う、ＦＰＭコード２５４０
ＥＡ情報２５０７は、ＴＥＤ２４２５（ｉ）によって表されるＥＡの代わりに送信されたＧＢＡＭおよびＥＭＭの暗号化および認証を行うのに必要な情報を含む。ＥＡ情報２５０７はまた、そのＥＡに向けられたＦＰＭの復号化および正当性チェックを行うための情報を促進し、かつ、その情報を含む。好適な実施形態において、ＥＡ情報２５０７は、少なくとも、（１）ＥＡＩＤ２４０９（ｉ）についてのＥＡＩＤであるＥＡＩＤ２５０９、それぞれＥＡ２４０９（ｉ）についての公開鍵およびプライベート鍵であるＥＡ　Ｋｕ２５１１およびＥＡ　Ｋｒ２５１３、ならびに、（２）ＴＥＤ２４２５（ｉ）が属する条件付きアクセスシステム６０１内のＥＡ２４０９（ｉ）によって使用されている各ＭＳＫについてのＭＳＫエントリ（ＭＳＫＥ）２５１５、を含む。各ＭＳＫＥ２５１５は、ＭＳＫについてのＭＳＫ識別子２５１７、もしあればＭＳＫについての満了時刻２５１９、ＭＳＫについてのＭＳＫパリティ２５２０、およびＭＳＫ２５２１自体を含む。
【０２０８】
（ＥＡ　ＴＥＤ２４２５（ｉ）によって実行される動作）
ＥＡ　ＴＥＤ２４２５（ｉ）は、初期化されると、ＴＥＤ２４２５（ｉ）によって表されるＥＡについてのＥＡＩＤを提供される。ＥＡ　ＴＥＤ２４２５（ｉ）は、ＥＡＩＤを２５０９において格納し、そして、ＲＳＡ鍵生成コード２５１７および乱数生成器２５３７からの乱数を用いて、ＥＡ公開鍵２５１１およびＥＡプライベート鍵２５１３を生成する。ＥＡ公開鍵２５１１およびＥＡプライベート鍵２５１３は、ＥＡ情報２５０７に格納される。遠隔手続き呼び出し（ＲＰＣ）は、ＤＮＣＳ５０７がＥＡ公開鍵２５１１を読むことを許可する。他のＲＰＣは、ＤＮＣＳ５０７がＴＥＤ２４２５（ｉ）のシリアルナンバーを読み、ＴＥＤ２４２５（ｉ）のシステム時間を得てセットし、そして、ＴＥＤ２４２５（ｉ）を呼び出して、それが応答しているかどうかを判定するのを許可する。ＴＥＤ２４２５（ｉ）は、それのシリアルナンバーで、この呼び出しに応答する。ＥＡ
ＴＥＤ２４２５（ｉ）はまた、複数のアラーム条件をＤＮＣＳ５０７に報告する。これらは、暗号化部分および全体失敗、乱数生成失敗、メモリ失敗、ならびにＴＥＤおよびイーサネット（登録商標）オーバーロードを含む。
【０２０９】
ＥＭＭの暗号化および認証を継続しつつ、ＤＮＣＳ５０７は２つのＲＰＣを有し、通常一方はＥＭＭについてのものであり、他方はＭＳＫ　ＥＭＭについてのものである。ＤＮＣＳ５０７がＥＡ２０４９（ｉ）についての非ＭＳＫ　ＥＭＭを生成する場合、ＤＮＣＳ５０７は、ＥＡ２０４９（ｉ）から以下のものを受け取る：
（１）ＥＭＭの送信先であるＤＨＣＴ３３３のシリアルナンバー
（２）ＥＡ２０４９（ｉ）についてのＥＡＩＤ
（３）ＥＭＭのタイプ
（４）第１の登録ＩＤ、満了期日、および非満了期日フラグと共に、その特定のタイプのＥＭＭ、例えば登録ビットマップ、に必要とされる情報
ＤＮＣＳ５０７はシリアルナンバーを用いて、公開鍵データベース２４２１内のＤＨＣＴ３３３についての公開鍵を調べ、ＥＡＩＤを用いて、いずれのＴＥＤ２４２５を使用するかを決定し、このタイプのＥＭＭに要求される情報をフォーマットし、そして、フォーマットされた情報（図１１の１１２３、１１２５、１１２７）を、ＤＨＣＴの公開鍵と共に、ＲＰＣを介してＴＥＤ２４２５（ｉ）に提供する。次に、ＥＭＭコード２５３８はＭＤ５コード２５２９を用いて、フォーマットされた情報のダイジェストを生成し、そして、ＲＳＡ　Ｅ／Ｄコード２５３５を用いて、ＤＨＣＴの公開鍵でフォーマットされた情報を暗号化し、かつ、ＥＡについてのプライベート鍵２５１３でダイジェストを暗号化する

。暗号化され、フォーマットされた情報および暗号化されたダイジェストはＤＮＣＳ５０７に提供される。ＤＮＣＳ５０７は、何か他の必要なものを加えて、ＥＭＭデータベース２４２０内にＥＭＭを配置する。

【０２１０】

ＭＳＫ　ＥＭＭについて、ＤＮＣＳ５０７は、ＥＡ２４０９（ｉ）から、ＥＡＩＤ、ＤＨＣＴシリアルナンバー、ＥＭＭタイプ、ＭＳＫパリティ、ＭＳＫＩＤ、および満了期日を受け取る。次に、ＤＮＣＳ５０７は、ＤＨＣＴシリアルナンバーを取り出し、情報をフォーマットし、そして、先ほど説明したＲＰＣ呼び出しを生成する。この場合、ＥＭＭコード２５３８は、ＥＡ情報２５０７を覗いて、ＭＳＫ　ＩＤに対応するＭＳＫを見つけ、かつ、フォーマットされた情報にＭＳＫを加える。次に、ＥＭＭコード２５３８はＲＳＡ暗号化／復号化コードを用いて、ＤＨＣＴの公開鍵でフォーマットされた情報を暗号化し、かつ、ＥＡのプライベート鍵でダイジェストを暗号化し、そして、上述のように、ＥＭＭをＤＮＣＳ５０７に戻す。

【０２１１】

グローバル放送メッセージにその認証情報を与えるインターフェースは、供給された秘密となるＭＳＫのＭＳＫＩＤ、および、グローバル放送メッセージのコンテンツを要求する。ＴＥＤ２４２５（ｉ）内のＧＢＡＭ認証コード２５３３はＭＳＫＩＤを用いて、ＭＳＫについてのＭＳＫＥ２５２５を配置し、ＭＳＫ２５２１をグローバルメッセージのコンテンツ（図１８のＧＢＡＭヘッダ１８０７およびグローバル放送データ１８０９）と組み合わせ、そして、ＭＤ５コード２５２９を用いて、ダイジェスト（ＧＢＡＭ　ＭＡＣ１８０５）を生成する。このダイジェストはＤＮＣＳ５０７に戻る。

【０２１２】

転送された購入メッセージ等の、ＤＨＣＴ３３３からＥＡに送信されたメッセージで、メッセージが送信されたＩＰパケットは、このメッセージのソースであるＤＨＴＣ３３３のＩＰアドレスを含み、そして、このＩＰアドレスは、ＤＨＣＴ３３３のシリアルナンバーを含む。ＤＮＣＳ５０７はこのシリアルナンバーを用いて、ＤＨＣＴ３３３についての公開鍵を公開鍵データベース２４２１内に配置し、そして、公開鍵を、ＦＰＭから、暗号化されたエンベロープ鍵２１０３、ＣＡ　ＦＰＭメッセージ２１０５、およびＦＰＭ署名された認証２１０７と共に、ＴＥＤ２４２５（ｉ）に提供する。次に、ＦＰＭコード２５４０は：

（１）ＥＡ公開鍵２５１１およびＲＳＡ暗号化／復号化コード２５３５を用いて、ＦＰＭ暗号化されたエンベロープ鍵２１０３を復号化する；

（２）３ＤＥＳコード２５３１および復号化されたエンベロープ鍵を用いて、ＦＰＭ暗号化されたイベント２１１３を復号化する；

（３）ＲＳＡ暗号化／復号化コード２５３５およびＤＨＣＴ３３３についての公開鍵を用いて、ＦＰＭ認証２１０７を復号化する；

（４）ＭＤ５コード２５２９を有する暗号化された後に復号化されたイベントを用いて、ＦＰＭ認証２１０７の復号化された値と比較する新たなハッシュを生成する。この比較は、ＦＰＭが正当であることを示す場合、ＴＥＤ２４２５（ｉ）は、復号化されたイベントをＤＮＣＳ５０７に戻す。ＤＮＣＳ５０７は、それらをＥＡ２４０９（ｉ）に転送する。

【０２１３】

ＭＳＫ２５１５内のＭＳＫは、ＴＥＤ２４２５（ｉ）によって生成される。ＭＳＫ生成のためのインターフェースは、単に、新たなＭＳＫについてのＭＳＫＩＤ、新たなＭＳＫについてのパリティ、および任意の満了時刻を要求する。ＭＳＫ生成コード２５２５は、乱数生成器２５３７から乱数を受け取り、そして、その乱数を用いて新たなＭＳＫを生成する。次に、新たなＭＳＫについてのＭＳＫＥ２５１５が生成されて、ＥＡ情報２５０７に加えられる。新たなＭＳＫについてのＭＳＫＩＤについてのＭＳＫＥ２５２５が既に存在する場合、新たなＭＳＫＥは、既存のＭＳＫＥに取って代わる。ＴＥＤ２４２５（ｉ）はまた、追加インタラクティブセッションＥＭＭについてのインタラクティブセッション

鍵を生成する。鍵生成は、ＭＳＫ　ＥＭＭについて説明したとおりである。一旦ＴＥＤ２４２５（ｉ）が、暗号化された鍵を有するＥＭＭコンテンツをＤＮＣＳ５０７に提供すると、ＴＥＤ２４２５（ｉ）は、メモリ２５０５内のインタラクティブセッション鍵が格納された領域に上書きする。

【０２１４】

（ＣＡＡ　ＴＥＤ）

ＣＡＡ　ＴＥＤ２４２７は、ＥＡ　ＴＥＤと同じハードウェアを有するが、好適な実施形態においては、ＤＨＣＴ３３３内に登録エージェントを確立するために使用されるＣＡＡ　ＥＭＭを暗号化するだけである。ＥＭＭ暗号化は、まさにＥＡ　ＴＥＤについて説明した通りに行われる。ＣＡＡ　ＴＥＤの暗号化および認証に要求される鍵は、ＤＨＣＴ３３３の公開鍵およびＣＡＡのプライベート鍵のみである。したがって、ＣＡＡを表す３つの公開鍵プライベート鍵対のうちの１つの対を格納することを要求されるのみである。ＣＡＡ公開プライベート鍵対は別のどこかで生成される。プライベート鍵は、その鍵対と共に、ＣＡＡ　ＴＥＤ２４０５に提供されるパス位相を用いて暗号化される。次に、ＣＡＡ　ＴＥＤは、プライベート鍵を復号化して、そして、パス位相ではなく、復号化されたプライベート鍵をメモリ２５０５に格納する。パス位相ではなく、暗号化されたプライベート鍵も、ＤＮＣＳ５０７内の暗号化されたエンティティ情報２４１９に格納される。

【０２１５】

（ＤＨＣＴ３３３上で実行されるアプリケーションのためのデータの認証：図２３）

上記は、条件付きアクセスシステム６０１が、どのように、条件付きアクセスオーソリティ、登録エージェント、ＤＨＣＴＳＥ６２７、およびトランザクション暗号化デバイス６０３を用いて、サービスのインスタンスを復号化するのに要求されるそれ自体の動作ならびに鍵および登録情報のセキュリティを提供するかを開示した。条件付きアクセスシステム６０１の別の機能は、ＤＨＣＴ３３３上で実行されるアプリケーションのための安全なデータダウンロードを確保することである。データがダウンロードされ得る２つの通路が存在する：（１）ＳＥＥＳ６１９からトランスポートネットワーク５１７を介してＨＦＣネットワーク５２１へ、そしてさらにＤＨＣＴ３３３へとつながる高帯域幅パスを介したＭＰＥＧ２ストリーム内、および（２）制御スイート６０７からＬＡＮ相互接続デバイス６１７およびＱＰＳＫ変調器６２１を介して、ＨＦＣネットワーク５２１およびＤＨＣＴ３３３へとつながる低帯域幅パスを介したＩＰパケット内。

【０２１６】

条件付きアクセスシステム６０１において使用されるデータで見られるように、問題には２つの局面、つまりセキュリティと認証、がある。安全性は、データを暗号化することにより達成される。高帯域幅通路によって配信されたデータの場合、データが所定の登録エージェントを有する全てのＤＨＣＴ３３３に向けられている場合にはＭＳＫを用いたＤＥＳによって、または、データが特定のＤＨＣＴ３３３に向けられている場合にはＤＨＣＴについての公開鍵によって、暗号化が行われ得る。低帯域幅通路によって配信されたデータの場合、データは特定のＤＨＣＴ３３３のＩＰアドレスにアドレスされ、そして、ＤＨＣＴ３３３の公開鍵で暗号化され得る。ＭＳＫで暗号化を行う場合は、ＭＳＫはトランザクション暗号化デバイス６０３によって提供され、ＤＨＣＴ３３３の公開鍵で暗号化を行う場合は、トランザクション暗号化デバイス６０３は鍵を提供し得るか、または、それ自体で暗号化を行い得る。ＤＨＣＴＳＥ６２７は、ＤＨＣＴ３３３において必要な復号化を行うのに必要とされる鍵を含む。

【０２１７】

条件付きアクセスシステム６０１における認証エンティティは、条件付きアクセスオーソリティおよび登録エージェントを含む。ダウンロードされたデータの認証は、ＥＭＭと同じ様態で、つまり、一方向ハッシュ関数を用いて、ダウンロードされたデータのダイジェストを生成し、次に、そのダイジェストを認証エンティティのプライベート鍵で暗号化して、封印されたダイジェストを生成することにより行われる。好適な実施形態において、封印されたダイジェストは、トランザクション暗号化デバイス６０３において生成され

る。ダウンロードされたデータがＤＨＣＴ３３３に到着した場合、ＤＨＣＴＳＥ６２７は、認証エンティティの公開鍵を用いて、封印されたダイジェストを復号化し、次に、一方向ハッシュ関数を用いて、ダウンロードされたデータを再びハッシュする。ダウンロードされたデータが正当であり、かつ、送信中に破壊されない場合に、封印されたダイジェストを復号化したダイジェスト、および、一方向ハッシュ関数でデータをハッシュした結果は等しい。ここで、認証は、データの作成者(originator)によってではなく、デジタルブロードバンド配信システムに知られたＣＡＡまたはＥＡによって行われるということに留意されたい。さらに、ＣＡＡまたはＥＡはＤＨＣＴ３３３に既に知られているので、認証データのＤＨＣＴ３３３へのダウンロードは、ＤＨＣＴ３３３のユーザが介入することなく起こり得る。

【０２１８】

認証を認証されているデータに関連付けるには、多くの方法がある。１つの方法は、図２０について上で説明したように、ＧＢＡＭを用いるという方法である。このような場合、ＧＢＡＭペイロード２００３は、ダウンロードされているデータについてのダイジェストであり、登録エージェント２００５は、ペイロード２００３およびＭＳＫを用いてダイジェストを生成するのに加えて、プライベート鍵でダイジェストを暗号化する。別の方法は、単にＭＰＥＧ－２トランスポートストリームを介して、または認証部分を含んだＩＰパケットを用いて、データと同様に、メッセージを送信するという方法である。

【０２１９】

上記技術を用いてダウンロードされ得るある種類のデータは、ＤＨＣＴ３３３内の汎用プロセッサによって実行されるコードである。プロセッサによって使用され得るメモリは、フラッシュメモリである部分を含む。つまり、このメモリは通常の書き込み可能メモリのように書き込み得ないが、全体としてのみ再書き込みされ得る。通常、このようなメモリは、ダウンロード可能なコードを保持するために使用される。図２３は、ダウンロード可能なコードを含むメッセージを示す。コードメッセージ２３０１は２つの部分、つまり認証部分２３０３およびコード部分２３０５、を有する。コード部分２３０５は、状況が要求すれば、暗号化されたまたは暗号化されないコードを含む。認証部分２３０３は、情報の少なくとも２つのアイテム、つまり認証識別子（ＡＩＤ）２３０７および封印されたダイジェスト２３０９、を含む。認証識別子２３０７は、条件付きアクセスオーソリティ、または認証コード２３０５である登録エージェントについての、ＣＡＡＩＤまたはＥＡＩＤである。封印されたダイジェスト２３０９は、一方向ハッシュ関数内でコード２３０５をハッシュしてダイジェストを生成し、そして、コードを認証しているＣＡＡまたはＥＡのプライベート鍵でこのダイジェストを暗号化することにより生成される。ＳＤ２３０９は、好適な環境において、トランザクション暗号化デバイス６０５によって生成される。

【０２２０】

コードメッセージ２３０１は、ＭＰＥＧ－２トランスポートストリームまたはＩＰパケットのいずれかを送信し得る。メッセージ２３０１は、認証ＣＡＡまたはＥＡを有するＤＨＣＴ３３３に放送され得るか、または、特定のＤＨＣＴ３３３に送信され得る。その場合、コードメッセージ２３０１を搬送するパケットは、ＤＨＣＴ３３３についてのアドレスを含む。好適な実施形態において、アドレスはＤＨＣＴ３３３のシリアルナンバーである。コードメッセージ２３０１がＤＨＣＴ３３３に到着した場合、プロセッサ上で実行されるコードは、コード２３０５について一方向ハッシュ関数を実行し、ＡＩＤ２３０７および封印されたダイジェスト２３０９と共に、結果をＤＨＣＴＳＥ６２７に提供する。ＤＨＣＴＳＥ６２７は、ＡＩＤ２３０７を用いてＣＡＡまたはＥＡについての公開鍵を配置して、次に、公開鍵を用いて、封印されたダイジェスト２３０９を復号化する。最後に、ＤＨＣＴＳＥ６２７が、封印されたダイジェストを復号化したダイジェスト２３０９内のハッシュ値を、プロセッサ上で実行されているコードによって提供されたハッシュ値と比較して、そして、それらが等しい場合には、ＤＨＣＴＳＥ６２７は、コードが認証された旨の信号を送る。

【０２２１】
（公開鍵ヒエラルキー（図２８））
本明細書中で説明する本システムのさまざまなエレメントは、ネットワーク内で公開鍵ヒエラルキー２８０１を集団で実行する。このようなヒエラルキーは、ＤＨＣＴ３３３とインターネット等の公開鍵型セキュリティを用いる他のネットワークとの間の、測定可能(scaleable)かつ自然発生的な商業インタラクションをサポートする「トラストチェイン(trust chain)」を確立するのに使用され得るので、有利である。ＤＢＤＳ５０１とのユーザ商業インタアクションにおいて信用を確立するために、使用され得る。
【０２２２】
図２８は、ＤＢＤＳ内の公開鍵証明書のヒエラルキーを示す。２つの独立した「トラストチェイン」を示す。左手側は「ＤＨＣＴチェイン」であり、これは、ＤＨＣＴ３３３に関連する公開鍵の有効性(validity)を確立し、ＤＨＣＴ３３３によってなされるデジタル署名の信頼された使用を可能にする。右手側は「オペレータチェイン」であり、これは、各システム内のネットワークオペレータおよび内在するＥＡに関連する公開鍵のバリディティを確立し、これらのエンティティの署名の信頼された使用を可能にする。
【０２２３】
ＤＨＣＴ署名２８０６は、本明細書中の別の箇所で説明したように、ＤＨＣＴ３３３から送信されたメッセージを認証するのに使用され得る。しかし、受取人がそのようなＤＨＣＴ署名を正当であると信頼できるには、ＤＨＣＴ３３３に関連するように請求された公開鍵が、実際にＤＨＣＴのプライベート鍵をマッチする正当の鍵であると、受取人が確信する必要がある。このことは、ＤＨＣＴ証明書２８０６をファクトリープログラマー証明機関（ＦＰＣＡ）署名で証明することにより達成される。ＦＰＣＡ証明書２８０５への参照が行われ得るので、ＦＰＣＡ署名は信頼され得る。ＤＨＣＴ証明書２８０６およびＦＰＣＡ署名は、ＦＰＣＡ証明書２８０５と同様、好適にはＤＨＣＴ３３３の生成時に安全な方法で生成される。新たなＦＰＣＡ証明書を発行し、新たなＦＰＣＡ署名を使用することはそのうち必要となり得るので、各ＦＰＣＡ証明書はまた、それ自体の証明書２８０４を有し得るＤＨＣＴルートの署名で証明される。このＤＨＣＴルート証明書２８０４は、自分自身で署名を行い得るか、または、別の機関によって証明され得る。ＤＨＣＴルート署名は、好適には、ＦＩＰＳ４０－１レベル３証明書の要件を満たすもの等の、優れた不正改変不可能なデバイスにおいて管理される。
【０２２４】
オペレーターチェインにおいて、さまざまなＥＡ証明書２８０３は、本明細書中の別の箇所で説明した様態で署名を行うために使用される。同様に、オペレーターＣＡＡ証明書２８０２を用いるオペレーターＣＡＡ署名は、本明細書中で既に説明したように、各ＥＡ署名を証明するために使用される。オペレーターＣＡＡ署名の上で、オペレーターＣＡＡ２８０２をＤＨＣＴ３３３に安全な方法で導入するために、２つのルートＣＡＡ署名が使用され得る。実際、好適には生成時に、３つのルートＣＡＡ公開鍵がＤＨＣＴ３３３の安全なＮＶＭ内に配置される。次に、第３のルートＣＡＡ公開鍵を、その鍵がオペレーターＣＡＡ証明書２８０２内で証明されるオペレーターＣＡＡの公開鍵と置き換えるために、ルートＣＡＡのいずれか２つからの正当のメッセージが使用され得る。ルートＣＡＡは、好適には、製造者によって、ＦＩＰ１４０－１レベル３証明書の要件を満たすかまたはそれを上まわる不正改変不可能なデバイス内で管理される。しかし、適切なメッセージのシーケンスを介して、全てのルートＣＡＡ公開鍵を、製造者の制御下にない他のＣＡＡの公開鍵に変えることは可能である。したがって、署名チェインから製造者を排除することができる。この場合、ルートＣＡＡは、１人より多いオペレータによって承認された他の何らかの機構であり得るか、または、オペレータによって管理され得る。
【０２２５】
図２８に示し、かつ、本明細書中の別の場所で説明するように、各オペレータは複数のＥＡを有し得る。好適な実施形態において、ある任意のオペレータのオペレーティングサイト毎に、異なるＥＡおよび関連するＥＡ証明書２８０３が存在する。このことにより、

オペレータＣＡＡ署名２８０２の知識および関与なしでは、ＤＨＣＴはオペレーショナルサイト間で移動され得ないことが確実になる。

【０２２６】

図２８に示すジオポリティカル(geo-political)ＣＡ証明書２８０７は、オペレータの通常の条件付きアクセスおよび電子活動を行うことを要求されない。しかし、オペレータは、その署名チェインをより大きなチェインにリンクさせて、オペレータのＤＢＤＳの外部のエンティティを含むトランザクションに関与するか、またはＤＨＣＴ３３３をそのトランザクションに関与させることができるようにすることを望み得る。この場合、署名チェインは、ジオポリティカルＣＡ署名によって証明されたＤＨＣＴルート署名２８０４、ルートＣＡＡ署名２８０８、またはオペレータＣＡＡ署名２８０２のうちの１つまたは全ての公開鍵を有することにより、ジオポリティカルＣＡのチェインおよびその署名２８０７に容易にリンクされ得る。このことは、署名２８０４、２８０８、および２８０２に関連する公開鍵の各々について、データベース内に配置された証明書を有することにより達成される。上記証明書は、ジオポリティカルＣＡ２８０７のプライベート鍵で署名される。

【０２２７】

図２９はＥＭＭ生成器２９０１を示す。本明細書中の別の箇所で説明するように、異なるＤＢＤＳインスタンス内の異なるオペレータによって操作されるＤＨＣＴは、そのオペレータおよびシステムに固有のオペレータのＣＡＡによって制御されるのが好ましい。生成時におけるＤＨＣＴ３３３は、任意のオペレータＣＡＡによって制御されるように構成されておらず、その代わり、製造の間にセキュリティプロセッサのメモリ内に配置される３つのルートＣＡＡ公開鍵によって制御されるので、ＤＨＣＴ３３３は、異なるオペレータによって制御されるように再構成される必要がある。これは、安全に行われる必要がある。本明細書中の別の箇所で説明するように、ルートＣＡＡのうちの２つのルートＣＡＡのデジタル署名を有するメッセージは、第３のＣＡＡについてのターミナルを再構成するために使用され得る。ＥＭＭ生成器２９０１は、証明された方法で新たなオペレータＣＡＡ公開鍵をＤＨＣＴ３３３に導入するために必要とされる２つのメッセージのうちの一方を生成するために使用される。ＤＨＣＴ公開鍵証明書２９０２はＥＭＭ生成器に入力され、それについてＤＨＣＴメッセージが生成されることを知り得る。特定のオペレータによって制御されるＤＨＣＴは、入力デバイスの別個のファイル内に配置され得るか、または、当業者に明らかな他の方法でオペレータに関連付けられ得る。

【０２２８】

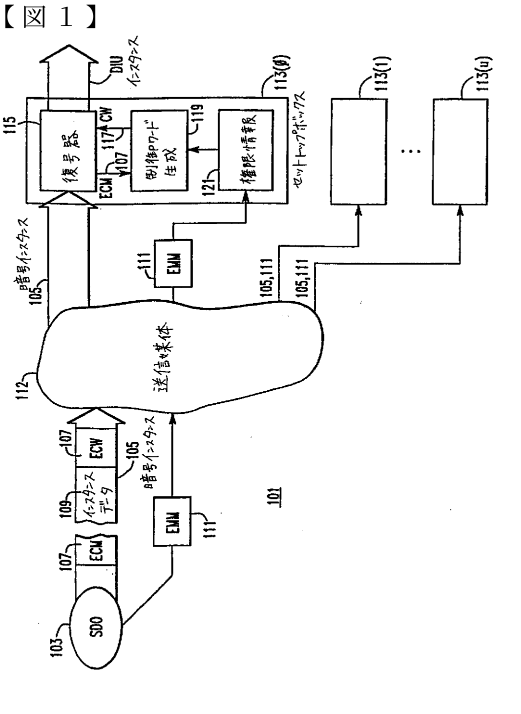
導入的なＥＭＭ２９０３を生成するのに先立って、ＥＭＭ生成器２９０１によって提供される、さまざまなオペレータの証明された公開鍵は、ＥＭＭ生成器２９０１の公開鍵メモリ２９０４にロードされる。したがって、ＥＭＭ生成器２９０１がオペレータＡに導入されることが必要なＤＨＣＴの入力を読む場合、ＥＭＭ生成器は、メモリ２９０４から読み出されたオペレータＡの公開鍵を用いて、オペレータＡの公開鍵を含むＥＭＭを生成する。同様に、導入的なＥＭＭ２９０３を生成するのに先立って、ルートＣＡＡのプライベート鍵は、ＥＭＭ生成器２９０１のプライベート鍵メモリ２９０５にロードされる必要がある。上記ＥＭＭは、メモリ２９０５内に含まれるルートＣＡＡのプライベート鍵を用いて、ＥＭＭ生成器２９０１によってデジタル署名される。秘密署名鍵はＥＭＭ生成器２９０１のメモリ２９０５内に含まれるので、ＥＭＭ生成器２９０１は、メモリ２９０５に格納されたルートＣＡＡプライベート鍵の値が発見されるのを防ぐ安全な様態で実行される必要がある。したがって、ＥＭＭ生成器２９０１は、ＦＩＰＳ４０－１レベル３証明書の要件を満たすか、または、それよりも高度な不正改変不可能なデバイス内で実行される。

【０２２９】

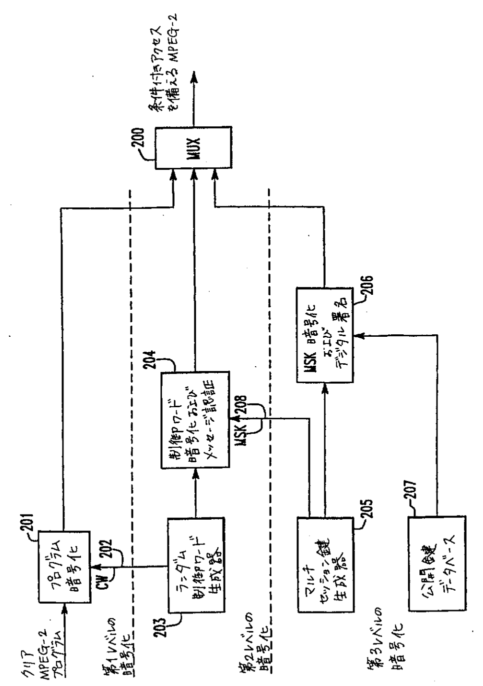
個々のＣＡＡ導入ＥＭＭ２９０３を署名するために２つのルートＣＡＡプライベート鍵を用いる必要があるので、好適には、２つのＥＭＭ生成器２９０１が設けられ、それぞれが、２つのルートＣＡＡプライベート鍵の各々に対応する。ＥＭＭ生成器２９０１は個々の物理的設備において動作されるのが好適である。

【０２３０】
上に説明した好適な実施形態の詳細な説明は、例示的であり、かつ、限定的なものではないとみなされる。そして本明細書中で開示した本発明の範囲は、特許法により許可される最大の範囲で解釈される特許請求の範囲から判断される。
【図面の簡単な説明】
【０２３１】
【図１】条件付きアクセスシステムのブロック図である。
【図２Ａ】本願に開示するサービスインスタンス暗号化技術のブロック図である。
【図２Ｂ】本願に開示するサービスインスタンス復号技術のブロック図である。
【図３】本願に開示するサービスインスタンス暗号化および復号技術のより詳細なブロック図である。
【図４】ＤＨＣＴに対して動的に登録を提供するために使用される技術のブロック図である。
【図５】条件付きアクセスシステムが実施されるデジタル広帯域伝達システムのブロック図である。
【図６】図５のデジタル広帯域伝達システムにおける条件付きアクセスシステムのブロック図である。
【図７】ＭＰＥＧ－２トランスポートシステムの図である。
【図８】ＥＭＭをＭＰＥＧ－２トランスポートシステムにマッピングする方法の図である。
【図９】ＥＭＭをＩＰパケットにマッピングする方法の図である。
【図１０】ＥＣＭをＭＰＥＧ－２トランスポートシステムにマッピングする方法の図である。
【図１１】ＥＭＭの詳細な図である。
【図１２】ＤＨＣＴＳＥ６２７の好適な実施形態の図である。
【図１３】ＤＨＣＴＳＥ６２７のメモリコンテンツの図である。
【図１４】好適な実施形態においてＮＶＳＣを登録エージェントに割り当てる方法の図である。
【図１５】ＥＡＤ　ＮＶＳＣの図である。
【図１６】別種のＮＶＳＣの図である。
【図１７】イベントＮＶＳＣの図である。
【図１８】グローバル放送認証メッセージ（ＧＢＡＭ）の図である。
【図１９】ＧＢＡＭの一種の図である。
【図２０】ＧＢＡＭを用いて一般的にクライアントアプリケーションにデータを提供する方法を示す図である。
【図２１】送信された購入メッセージの図である。
【図２２】ＥＣＭにおける登録ユニットメッセージの図である。
【図２３】コードメッセージの図である。
【図２４】ＴＥＤと条件付きアクセスシステム６０１の残りとの関係を示す図である。
【図２５】ＴＥＤの詳細な図である。
【図２６】スポットライトおよびブラックアウトに使用される座標系の図である。
【図２７】図２６の座標系において領域を計算する方法を示す図である。
【図２８】公開鍵階層の図である。
【図２９】本発明によるＥＭＭ生成器の図である。

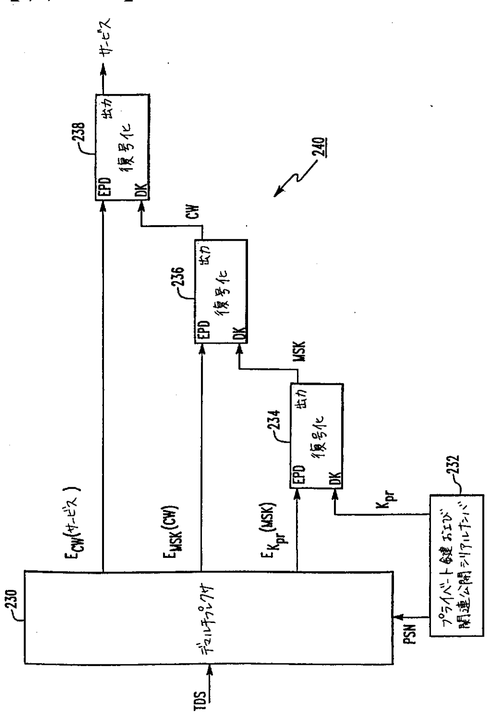
【図１】


103
SDO
107
ECM
109
インスタンスデータ
ECW
105
暗号インスタンス
EMM
111
101
112
送信媒体
105,111
115
復号器
117
CW
ECM
107
制御ワード生成
119
121
権限情報
セットトップボックス
113(0)
113(1)
113(n)
DIU
インスタンス

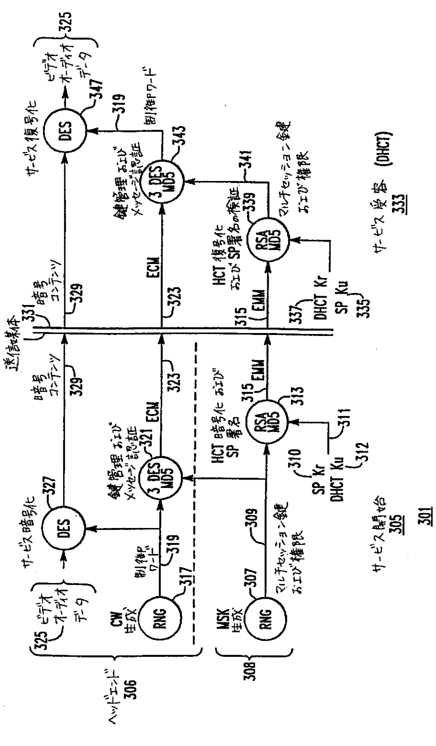
【図２Ａ】


クリア MPEG-2 プログラム
201
プログラム暗号化
CW
202
203
ランダム制御ワード生成器
204
制御ワード暗号化および メッセージ認証
MSK
208
205
マルチセッション鍵生成器
206
MSK暗号化および デジタル署名
207
公開鍵データベース
200
MUX
条件付きアクセスを備える MPEG-2
第１レベルの暗号化
第２レベルの暗号化
第３レベルの暗号化

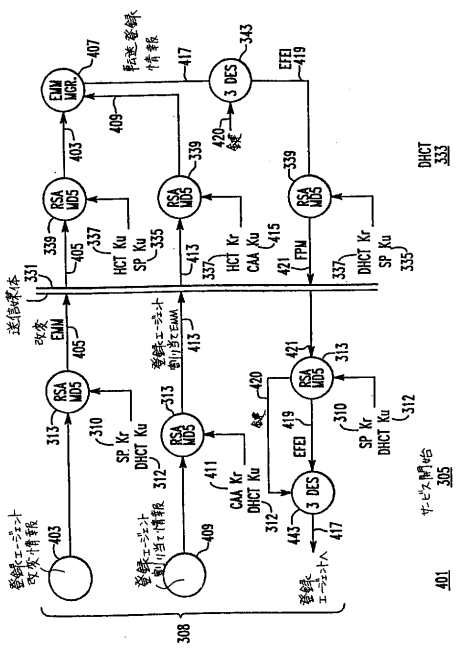
【図２Ｂ】


TDS
230
デマルチプレクサ
PSN
232
プライベート鍵および関連公開シリアルナンバ
K_pr
234
EPD
DK
復号化
出力
MSK
236
238
CW
サービス
240

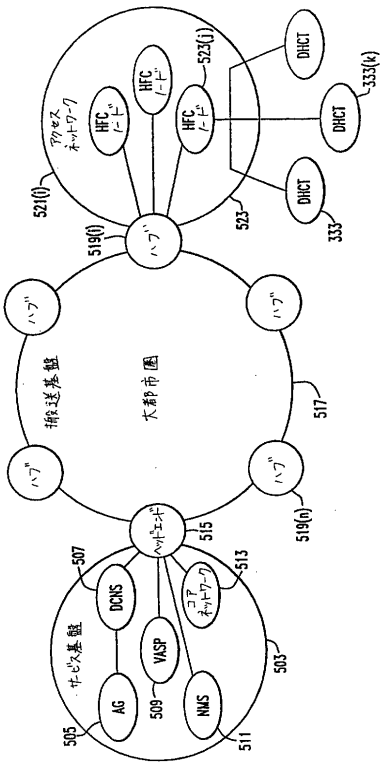
【図３】


325
ビデオ オーディオ データ
CW 生成
RNG
317
319
制御ワード
DES
327
サービス暗号化
3 DES MD5
321
鍵管理および メッセージ認証
ECM
323
MSK 生成
RNG
307
309
マルチセッション鍵 および権限
HCT暗号化 SP署名
RSA MD5
313
315
EMM
310
SP Kr
DHCT Ku
311
312
サービス開始台
305
301
ヘッドエンド
306
308
送信媒体
331
暗号コンテンツ
329
DHCT Kr
SP Ku
335
337
RSA MD5
339
HCT復号化 SP署名の検証
341
マルチセッション鍵 および権限
3 DES MD5
343
鍵管理および メッセージ認証
制御ワード
DES
347
サービス復号化
サービス受容 (DHCT)
333

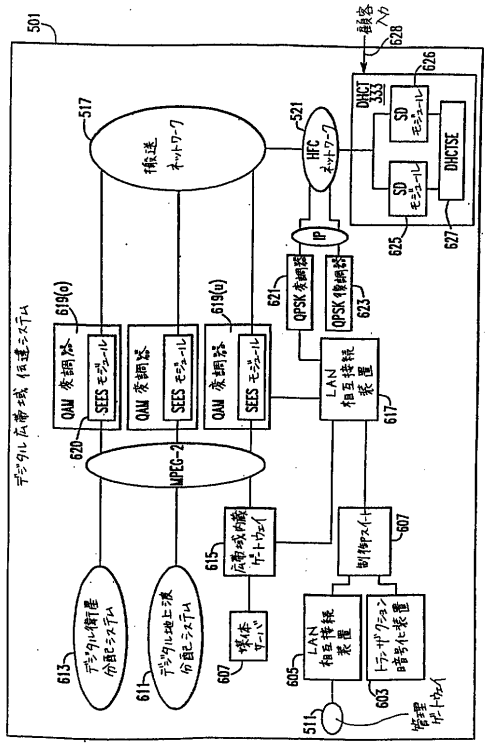
【図４】



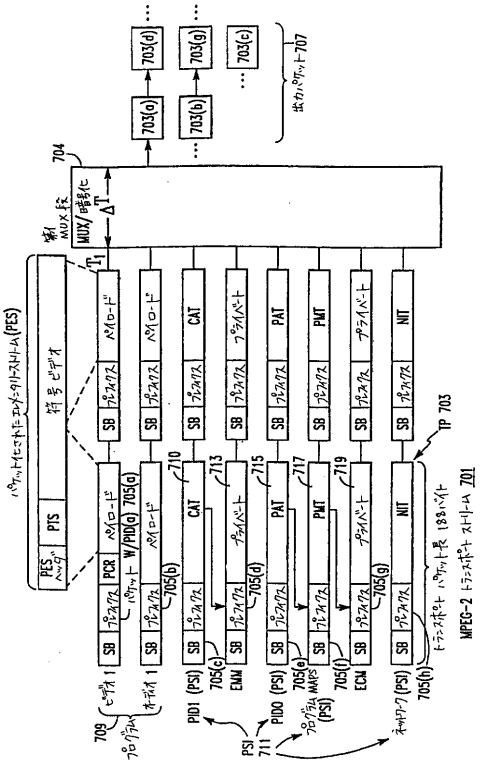
【図５】



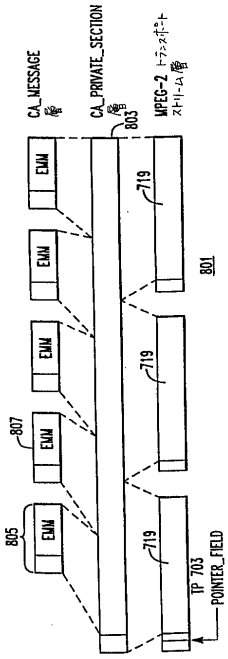
【図６】



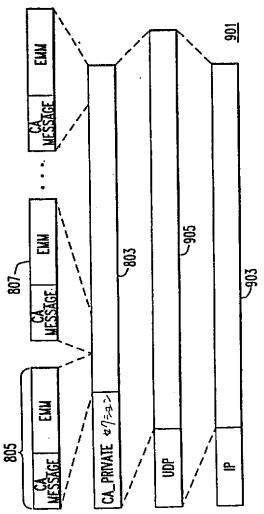
【図７】



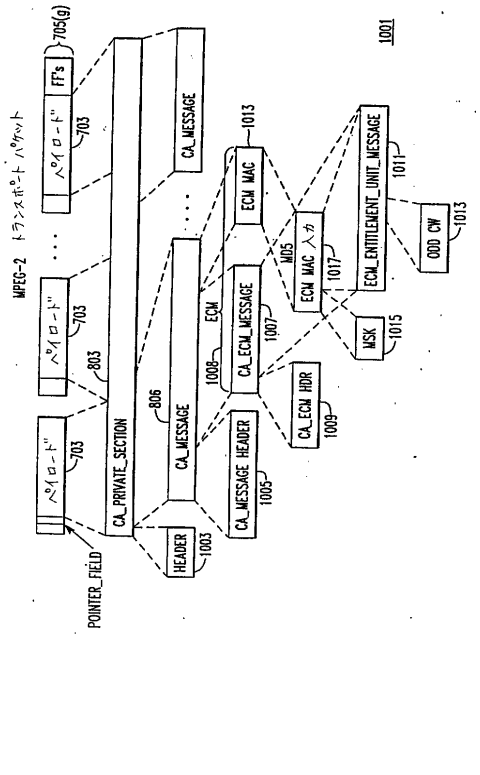
【図８】


CA_MESSAGE 層
CA_PRIVATE_SECTION 層
803
MPEG-2 トランスポート ストリーム層
EMM
807
805
719
801
TP 703
POINTER_FIELD

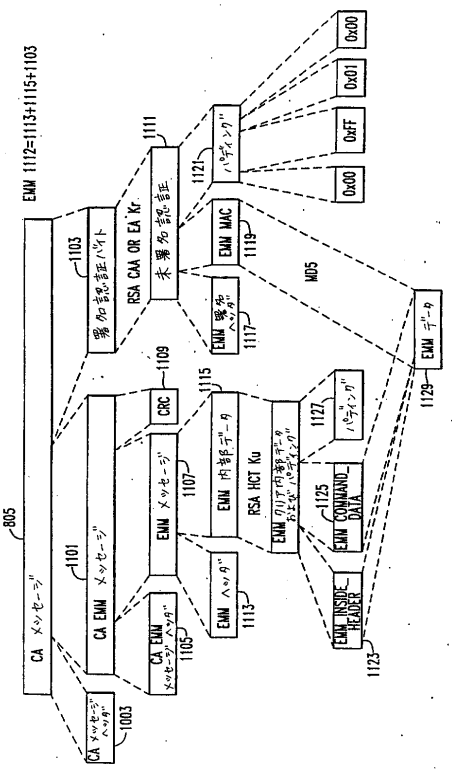
【図９】


CA MESSAGE
EMM
807
805
803
CA_PRIVATE セクション
905
UDP
903
IP
901

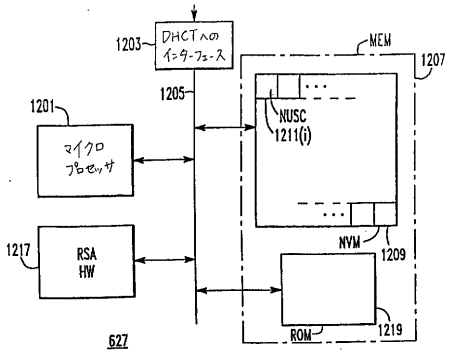
【図１０】


MPEG-2 トランスポート パケット
705(g)
ペイロード
FFs
703
803
CA_PRIVATE_SECTION
CA_MESSAGE
806
HEADER
1003
CA_MESSAGE HEADER
1005
ECM
1008
CA_ECM_MESSAGE
1007
CA_ECM HDR
1009
MD5
ECM MAC
1013
ECM MAC 入力
1017
WSK
1015
ECM_ENTITLEMENT_UNIT_MESSAGE
1011
1001
ODD CW
1013
POINTER_FIELD

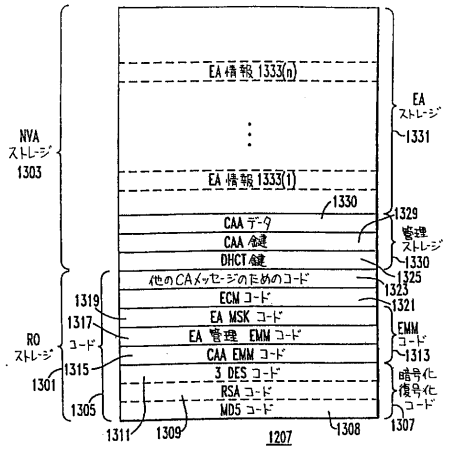
【図１１】


EMM 1112=1113+1115+1103
805
CA メッセージ
1101
CA EMM メッセージ
CA EMM メッセージ ヘッダ
1105
CA メッセージ ヘッダ
1003
EMM メッセージ
1107
EMM ヘッダ
1113
CRC
1109
EMM 内部データ
1115
RSA HCT Ku
EMM INSIDE HEADER
1123
EMM COMMAND DATA
1125
パディング
1127
EMM データ
1129
RSA CAA OR EA Kr
1111
署名認証バイト
未署名認証
EMM 署名 ヘッダ
1117
EMM MAC
1119
MD5
パディング
1121
0x00
0xFF
0x01
0x00

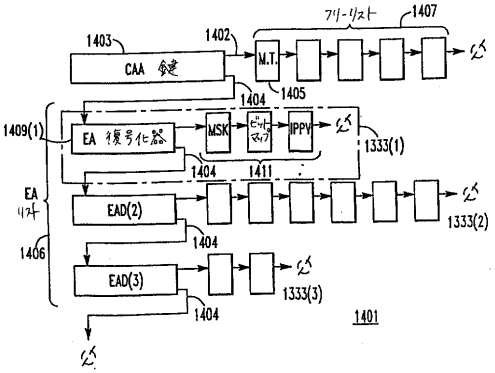
【図１２】



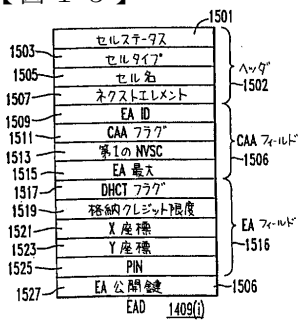
【図１３】



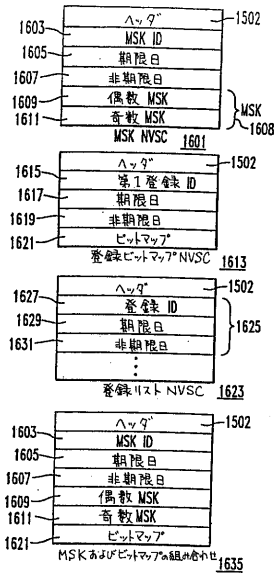
【図１４】



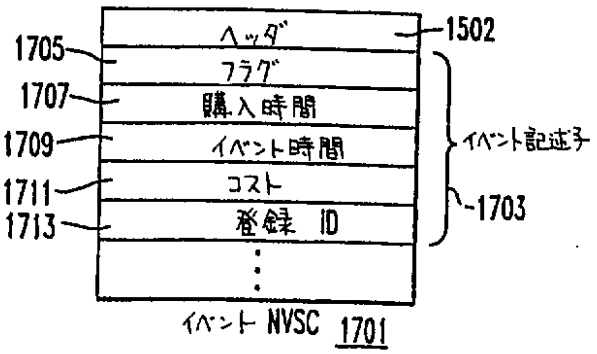
【図１５】



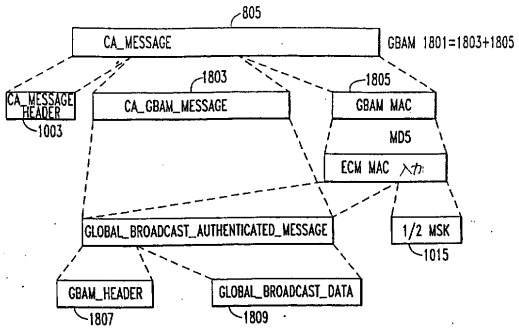
【図１６】



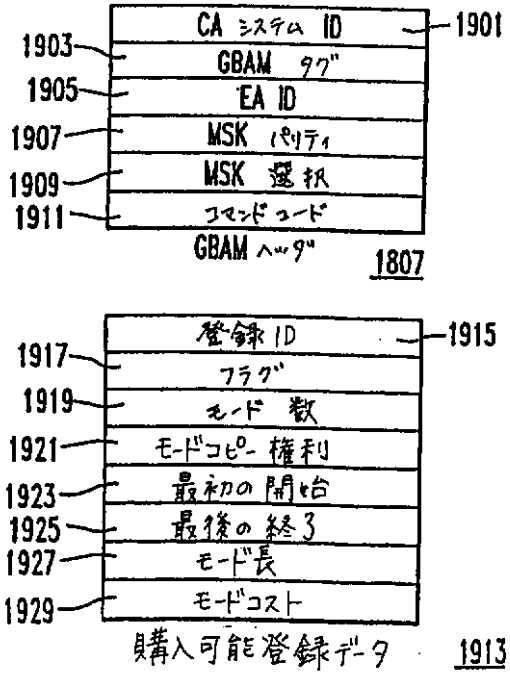
【図１７】



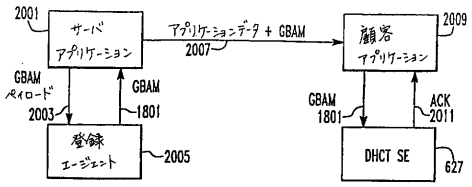
【図１８】



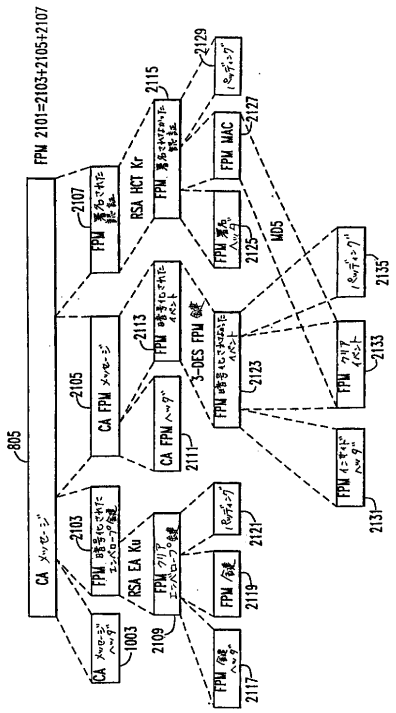
【図１９】



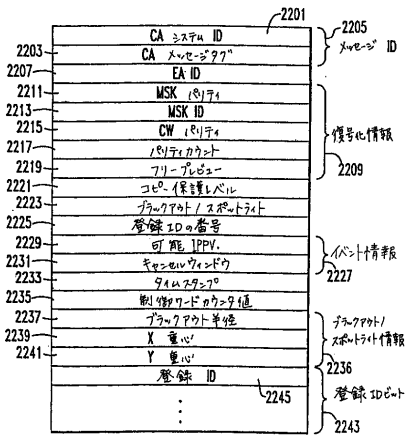
【図２０】



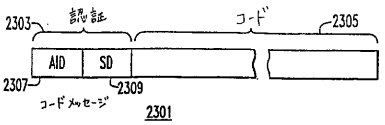
【図２１】



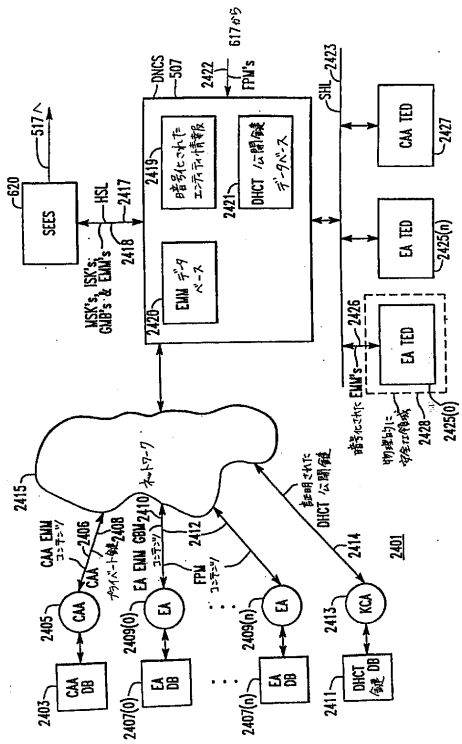
【図２２】



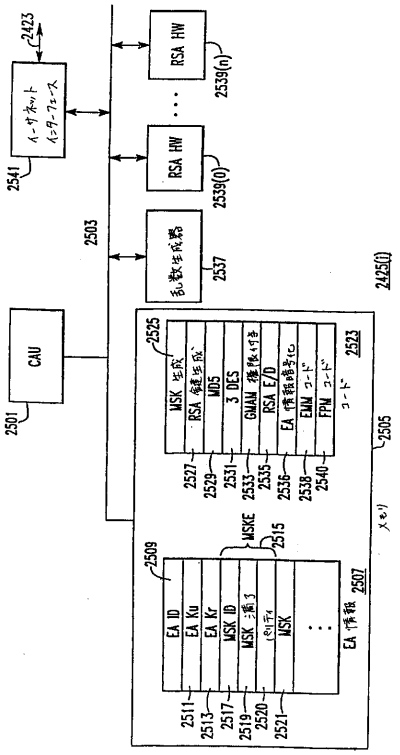
【図２３】



【図２４】



【図２５】



【図２６】

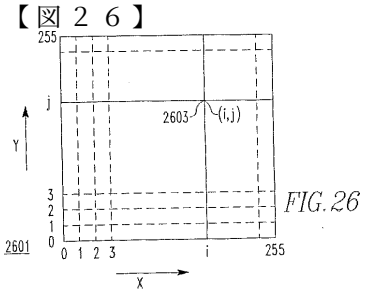


FIG. 26

【図２７】

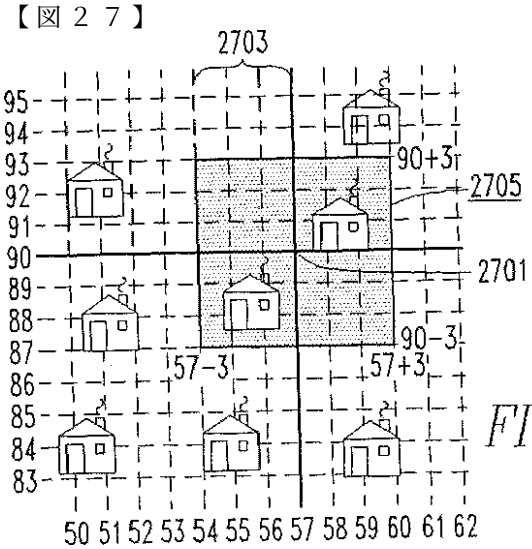
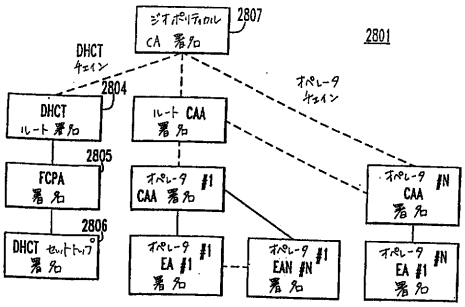
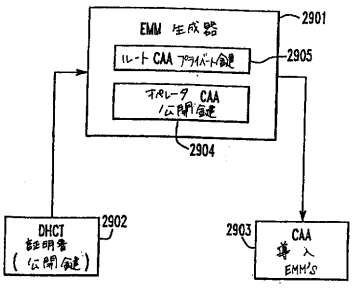


FIG. 27

【図２８】



【図２９】



フロントページの続き

(72)発明者 グレンドン エル. エイキンズ ザ サード
アメリカ合衆国 ジョージア ３０５０１, ゲイネスビル, ウィンドワード レーン エヌ. イー. ２５１０
(72)発明者 マイケル エス. パルゴン
アメリカ合衆国 ジョージア ３０３０６, アトランタ, ポプラー グローブ ドライブ １１９６
(72)発明者 ハワード ジー. ピンダー
アメリカ合衆国 ジョージア ３００９２, ノークロス, スティルソン サークル ４３１７
(72)発明者 アンソニー ジェイ. ワシルースキー
アメリカ合衆国 ジョージア ３００２２, アルファレッタ, レン リッジ ロード １０６８０

Ｆターム(参考) 5J104 EA17 EA18 PA05 PA06