(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5021639号
(P5021639)
(45)発行日　平成24年9月12日(2012.9.12)　(24)登録日　平成24年6月22日(2012.6.22)

(51)Int.Cl.　F I
H04N 7/173 (2011.01)　H04N 7/173 630
H04N 7/173 610Z

請求項の数 16　(全 22 頁)

(21)出願番号	特願2008-520256 (P2008-520256)
(86)(22)出願日	平成18年6月22日 (2006.6.22)
(65)公表番号	特表2009-500944 (P2009-500944A)
(43)公表日	平成21年1月8日 (2009.1.8)
(86)国際出願番号	PCT/US2006/024293
(87)国際公開番号	WO2007/008362
(87)国際公開日	平成19年1月18日 (2007.1.18)
審査請求日	平成21年6月18日 (2009.6.18)
(31)優先権主張番号	11/176,058
(32)優先日	平成17年7月7日 (2005.7.7)
(33)優先権主張国	米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　アナンド　パカ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】ストリーミング用制御プロトコルおよびトランスポートプロトコルを使用した、保護付きコンテンツの搬送

(57)【特許請求の範囲】
【請求項１】
コンピュータによって実施される方法であって、
クライアントから制御フロー要求を受信すること、
前記制御フロー要求に応答して制御フローを確立することであって、前記制御フローは、リアルタイムストリーミングプロトコル（ＲＴＳＰ）を使用して、前記クライアントと保護付きメディアコンテンツの交換を確立し、前記確立することは、
前記クライアントから、ＲＴＳＰ　ＤＥＳＣＲＩＢＥ要求の本文中でライセンス要求メッセージを受信すること、
前記クライアントへ、ライセンスを含むライセンス応答メッセージを含むＲＴＳＰ　Ｓｅｓｓｉｏｎ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｐｒｏｔｏｃｏｌ（ＳＤＰ）を使用して、記述子を送信すること
データフローを使用して、前記保護付きメディアコンテンツを前記クライアントへ通信することであって、前記データフローはトランスポートプロトコルを使用し、前記送信することはストリーミングすることを含み、前記トランスポートプロトコルは、ＲＴＰパケットにカプセル化された前記保護付きメディアコンテンツを有するリアルタイムトランスポートプロトコル（ＲＴＰ）を含み、前記ＲＴＰパケットは前記保護付きメディアコンテンツを復号するために復号プロセスで使用される暗号化パラメータを含むこと、および、
前記クライアントに、前記保護付きメディアコンテンツのストリーミング中に保護付

きメディアコンテンツポリシー、または、前記保護付きメディアコンテンツポリシー及び前記保護付きメディアコンテンツに関する保護付きメディアコンテンツフォーマットの両方を変化させるＲＴＳＰ　ＡＮＮＯＵＮＣＥ要求を送信することであって、前記ＲＴＳＰ　ＡＮＮＯＵＮＣＥ要求は、新しいライセンスを含む新しいライセンス応答メッセージを含み、前記新しいライセンスは、前記保護付きメディアコンテンツのストリーミング中に前記保護付きメディアコンテンツに適用される前記変化したメディアコンテンツポリシーを示し、前記保護付きメディアコンテンツポリシー及び前記保護付きメディアコンテンツに関する保護付きメディアコンテンツフォーマットの両方が変化する場合に、前記新しいライセンス応答メッセージが、前記ＲＴＳＰ　ＡＮＮＯＵＮＣＥ要求を介して送信された更新済みＳＤＰ記述に埋め込まれること
　を含むこと
を含むことを特徴とする方法。

【請求項２】
　コンピュータによって実施される方法であって、
　ＲＴＳＰ　ＤＥＳＣＲＩＢＥ要求の本文中でライセンス要求メッセージを送信することによって、リアルタイムストリーミングプロトコル（ＲＴＳＰ）を使用して、サーバと保護付きメディアコンテンツを交換するために、前記サーバと制御フローを確立すること、
　前記ライセンス要求メッセージに応じて、前記サーバから、ライセンスを含むライセンス応答メッセージを受信すること、
　前記サーバから、ＲＴＰパケットにカプセル化された前記保護付きメディアコンテンツを有するリアルタイムトランスポートプロトコル（ＲＴＰ）を介して、前記保護付きメディアコンテンツを受信することであって、前記ＲＴＰパケットは前記保護付きメディアコンテンツを復号するために復号プロセスで利用することのできる暗号化パラメータを含むこと、および、
　前記サーバから受信したＲＴＳＰ　ＡＮＮＯＵＮＣＥ要求で、前記保護付きメディアコンテンツの交換中に、保護付きメディアコンテンツポリシー、または、前記保護付きメディアコンテンツポリシー及び前記保護付きメディアコンテンツに関する保護付きメディアコンテンツフォーマットの両方を更新することであって、前記ＲＴＳＰ　ＡＮＮＯＵＮＣＥ要求は、新しいライセンスを含む新しいライセンス応答メッセージを含み、前記新しいライセンスは、前記保護付きメディアコンテンツの交換中に前記保護付きメディアコンテンツに適用される前記更新したメディアコンテンツポリシーを示し、前記保護付きメディアコンテンツポリシー及び前記保護付きメディアコンテンツに関する保護付きメディアコンテンツフォーマットの両方が更新される場合に、前記新しいライセンス応答メッセージが、前記ＲＴＳＰ　ＡＮＮＯＵＮＣＥ要求内の更新済みＳＤＰ記述に埋め込まれること
を含むことを特徴とする方法。

【請求項３】
　前記ＲＴＰパケットは、複数の異なる暗号化済みペイロードを含むことを特徴とする請求項２に記載の方法。

【請求項４】
　前記暗号化パラメータは、各暗号化済みペイロードにつき鍵ＩＤ拡張子および初期化ベクトルを含むことを特徴とする請求項３に記載の方法。

【請求項５】
　前記受信することは、
　前記保護付きメディアコンテンツを復号するために復号プロセスで利用される暗号化パラメータを含む、前記ＲＴＰパケット内の記述子を識別すること、および、
　前記記述子を前記保護付きメディアコンテンツに関連付けること
を含むことを特徴とする請求項２に記載の方法。

【請求項６】
　前記記述子は、前記ＲＴＰパケット内の前記保護付きメディアコンテンツの最後に付加されることを特徴とする請求項５に記載の方法。

【請求項７】
前記保護付きメディアコンテンツは、前記記述子によって参照される単一の鍵を使用して復号されることを特徴とする請求項５に記載の方法。
【請求項８】
前記ラインセンスを含む前記ライセンス応答メッセージは、ＲＴＳＰ　Ｓｅｓｓｉｏｎ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｐｒｏｔｏｃｏｌ（ＳＤＰ）に含まれることを特徴とする請求項２に記載の方法。
【請求項９】
コンピュータによって実施される方法であって、
ＲＴＳＰ　ＤＥＳＣＲＩＢＥ要求の本文中でライセンス要求メッセージを受信することに応じて、リアルタイムストリーミングプロトコル（ＲＴＳＰ）を使用して保護付きメディアコンテンツを交換するために、受信側と制御フローを確立すること、
前記ラインセンス要求メッセージに、ライセンスを含むラインセンス応答メッセージで応答すること、
データフローを使用して前記受信側に前記保護付きメディアコンテンツを送信することであって、前記データフローは、トランスポートプロトコルを使用し、前記送信することは、ストリーミングすることを含み、前記トランスポートプロトコルは、ＲＴＰパケット内にカプセル化された前記保護付きメディアコンテンツを有するリアルタイムトランスポートプロトコル（ＲＴＰ）を含み、前記ＲＴＰパケットは、前記保護付きメディアコンテンツを復号するために復号プロセスで使用される暗号化パラメータを含むこと、および、
ＲＴＳＰ　ＡＮＮＯＵＮＣＥ要求で、前記保護付きメディアコンテンツのストリーミング中に、保護付きメディアコンテンツポリシー、または、前記保護付きメディアコンテンツポリシー及び前記保護付きメディアコンテンツに関する保護付きメディアコンテンツフォーマットの両方を更新することであって、前記ＲＴＳＰ　ＡＮＮＯＵＮＣＥ要求は、新しいライセンスを含む新しいライセンス応答メッセージを含み、前記新しいライセンスは、前記保護付きメディアコンテンツのストリーミング中に前記保護付きメディアコンテンツに適用する前記保護付きメディアコンテンツポリシーを示し、前記保護付きメディアコンテンツポリシー及び前記保護付きメディアコンテンツフォーマットの両方が更新される場合に、前記新しいライセンス応答メッセージが、前記ＲＴＳＰ　ＡＮＮＯＵＮＣＥ要求を介して送信された更新済みＳＤＰ記述に埋め込まれること
を含むことを特徴とする方法。
【請求項１０】
コンピュータによって実施される方法であって、
ストリーミングのための制御プロトコルを使用して保護付きコンテンツを交換するために、制御フローを確立すること、
データフローを使用して保護付きコンテンツをストリーミングすることであって、前記データフローは、ＲＴＰパケット内にカプセル化された前記保護付きコンテンツを有するリアルタイムトランスポートプロトコル（ＲＴＰ）を含む、トランスポートプロトコルを使用し、前記ＲＴＰパケットは、前記保護付きコンテンツを復号するために復号プロセスで使用される暗号化パラメータを含むこと、
前記保護付きコンテンツのストリーミング中に、ポリシー、または、前記ポリシー及び前記保護付きコンテンツに関するフォーマット情報の両方を更新することであって、前記更新することは、ストリーミングのために前記制御プロトコルを介して更新を送信することを含み、前記制御プロトコルは、リアルタイムストリーミングプロトコル（ＲＴＳＰ）を含み、前記更新は、ＲＴＳＰ　ＡＮＮＯＵＮＣＥ要求を介して送信され、各ＲＴＳＰ　ＡＮＮＯＵＮＣＥ要求は、ライセンスを含むライセンス応答メッセージを含み、前記ライセンスは、どのポリシーを前記保護付きコンテンツのストリーミング中に前記保護付きコンテンツに適用するかを示し、前記ポリシー及び前記フォーマット情報の両方が更新される場合に、各新しいライセンス応答メッセージが、各ＲＴＳＰ　ＡＮＮＯＵＮＣＥ要求を介して送信された更新済みＳＤＰ記述に埋め込まれること

を含むことを特徴とする方法。
【請求項１１】
前記ＲＴＰパケットは、複数の異なる暗号化済みペイロードを含むことを特徴とする請求項１０に記載の方法。
【請求項１２】
前記暗号化パラメータは、各暗号化済みペイロードにつき鍵ＩＤ拡張子および初期化ベクトルを含むことを特徴とする請求項１１に記載の方法。
【請求項１３】
前記保護付きコンテンツを復号するために復号プロセスで利用される暗号化パラメータを含む、前記ＲＴＰパケット内の記述子を識別すること、および、
前記記述子を前記保護付きコンテンツに関連付けること
をさらに含むことを特徴とする請求項１０に記載の方法。
【請求項１４】
前記記述子は、前記ＲＴＰパケット内の前記保護付きコンテンツの最後に付加されることを特徴とする請求項１３に記載の方法。
【請求項１５】
前記復号プロセスは、前記記述子によって参照される単一の鍵を使用して復号される前記保護付きコンテンツを含むことを特徴とする請求項１３に記載の方法。
【請求項１６】
前記ライセンスを含む前記ライセンス応答メッセージは、ＲＴＳＰ　Ｓｅｓｓｉｏｎ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｐｒｏｔｏｃｏｌ（ＳＤＰ）に含まれることを特徴とする請求項１０に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＤＲＭなどの保護付きコンテンツを他のマシンに移して、そのマシン上でコンテンツの再生を可能にする技術に関する。
【背景技術】
【０００２】
ディジタル著作権管理（ＤＲＭ、Digital Rights Management）は、電子デバイス上でのディジタルメディアコンテンツの使用を制御または制限することなどによってコンテンツを保護するのに用いられる技法を指す。ＤＲＭの特性の１つは、メディアコンテンツを所与のマシンまたはデバイスに束縛できることである。すなわち、特定のコンテンツに属するライセンスであって、このコンテンツに関連する権利および制限を定義するライセンスは、通常、所与のマシンまたはデバイスに束縛されることになる。この結果、ユーザは通常、このコンテンツを再生するために、このコンテンツを取り込んで別のマシンに移すことはできなくなる。
【０００３】
【非特許文献１】http://www.ietf.org/rfc/rfc2326.txtで入手可能なRTSP RFC, Schulzrinne, H., Rao, A., and R. Lanphier, "Real Time Streaming Protocol (RTSP)", RFC 2326、１９９８年４月
【非特許文献２】ＲＦＣ－２３９７（http://www.ietf.org/rfc/rfc2397.txt）
【非特許文献３】http://download.microsoft.com/download/5/5/a/55a7b886-b742-4613-8ea8-d8b8b5c27bbc/RTPPayloadFormat_for_WMAandWMV_vl.doc
【発明の開示】
【発明が解決しようとする課題】
【０００４】
ＤＲＭ保護付きコンテンツを他のマシンに移してこれらのマシン上でコンテンツの再生を可能にできるようにする技術はいくつかあるが、このような技術は、コンテンツの転送と再生とを同時に行うのには適さない非リアルタイムのコンテンツ転送用プロトコルを使

用しがちな可能性がある。
【課題を解決するための手段】
【０００５】
本発明の様々な実施形態は、ディジタル著作権管理（ＤＲＭ）などのコンテンツ保護方法を利用して、ホームメディアネットワークなどのローカルネットワーク内のマシンおよびデバイス上での安全なコンテンツ再生を可能にする。少なくともいくつかの実施形態では、メッセージおよびコンテンツは、ストリーミング用制御プロトコルおよびトランスポートプロトコルをそれぞれ使用して送達される。少なくともいくつかの実施形態では、ストリーミング用制御プロトコルはリアルタイムストリーミングプロトコル（ＲＴＳＰ）であり、トランスポートプロトコルはリアルタイムトランスポートプロトコル（ＲＴＰ）である。
【発明を実施するための最良の形態】
【０００６】
（概観）
本明細書に述べる様々な実施形態は、ディジタル著作権管理（ＤＲＭ）などのコンテンツ保護方法を利用して、ホームメディアネットワークなどのローカルネットワーク内のマシンおよびデバイス上での安全なコンテンツ再生を可能にする。少なくともいくつかの実施形態では、メッセージおよびコンテンツは、ストリーミング用制御プロトコルおよびトランスポートプロトコルをそれぞれ使用して送達される。少なくともいくつかの実施形態では、ストリーミング用制御プロトコルはリアルタイムストリーミングプロトコル（ＲＴＳＰ）であり、トランスポートプロトコルはリアルタイムトランスポートプロトコル（ＲＴＰ）である。これらの実施形態では、ＲＴＳＰ／ＲＴＰによってもたらされる利点を享受するプロトコル拡張子（protocol extension）が導入され、当業者には理解されるであろうが、これらの利点には、ユーザデータグラムプロトコル（ＵＤＰ）を介したデータ送達、および、クライアントとサーバとの間の双方向通信が含まれる。
【０００７】
具体的には、少なくともいくつかの実施形態では、プロトコル拡張子は、ＲＴＳＰを使用してセッションを安全に確立し、ＲＴＰ中にカプセル化された保護付きデータを転送し、ＲＴＰペイロードフォーマットに応じてデータを暗号化および転送する方式を提供し、暗号化済みコンテンツデータと共に暗号化パラメータを転送するための様々な方法を提供する。
【０００８】
以下の説明では、「コンテンツセキュリティおよびライセンス転送プロトコル」という題名のセクションを提供し、発明的技法をその中で利用できる１つの特定のシステムについて述べる。これに続いて、「ＲＴＳＰ」という題名のセクションを提供して、ＲＴＳＰに馴染みのない読者に、ＲＴＳＰ空間で発明的技法を理解するための少なくともいくらかのコンテキストを提供する。このセクションに続いて、「ＲＴＳＰを使用した例示的な実装形態」という題名のセクションを提供し、制御フローの確立にＲＴＳＰを利用してデータフローの確立にＲＴＰを利用する様々な発明的技法について述べる。
【０００９】
（コンテンツセキュリティおよびライセンス転送プロトコル）
以下、ディジタルリンクを介して流れるコンテンツのためにセキュリティを提供し、ライセンスを転送する例示的なプロトコルに関する説明を提供する。このプロトコルは、様々な発明的技法をそれと共に利用することのできる１つの例示的なプロトコルを構成するに過ぎない。特許請求する主題の趣旨および範囲を逸脱することなく他のプロトコルを利用することもできることを認識および理解されたい。
【００１０】
本明細書では、以下の暗号表記法を使用する。
Ｋ｛ｄａｔａ｝　データは秘密鍵Ｋで暗号化されている。
Ｋ［ｄａｔａ］　データは秘密鍵Ｋで署名されている。

{ｄａｔａ}$_{Ｄｅｖｉｃｅ}$　データはデバイスの公開鍵で暗号化されている。
［ｄａｔａ］$_{Ｄｅｖｉｃｅ}$　データはデバイスの秘密鍵で署名されている。

【００１１】

この特定のプロトコルでは、５つの主要なプロシージャがある。すなわち、登録、再妥当性検査、近接検出、セッション確立、およびデータ転送である。

【００１２】

登録プロシージャでは、送信側（すなわち別のデバイスに送信されるコンテンツを有するデバイス）は、意図された受信側（すなわちコンテンツの送信先となるデバイス）を、一意かつ安全に識別することができる。この特定のプロトコルでは、送信側は、登録された受信側を含むデータベースを維持し、わずかな所定数の受信側よりも多くの受信側が同時に使用されないようにする。登録プロセスの間、送信側はまた、保護付きコンテンツが広く配信されるのを防止するために、近接検出プロシージャを利用して、受信側がネットワーク中で送信側の「近く」に位置するようにする。

【００１３】

再妥当性検査プロシージャは、受信側が送信側の「近く」にあり続けるようにするために使用される。受信側が過去の所定期間内に登録または再妥当性検査されていない限り、コンテンツは受信側に送達されない。

【００１４】

セッション確立プロシージャは、受信側が送信側にコンテンツを要求するときはいつでも使用される。送信側は、デバイスが登録され最近に妥当性検査されていなければならないことを守らせた後で、セッション確立を完了することができる。

【００１５】

セッションが確立されると、要求されたコンテンツのデータ転送を安全な方式で行うことができる。受信側は、セッションを再利用してコンテンツの特定部分を取り出すことはできるが（シーキング）、異なるコンテンツを取り出すには新しいセッションを確立しなければならない。

【００１６】

次に、図１と、登録の間に送信側と受信側との間でやり取りされる様々なメッセージを記述した以下の表と共に、登録プロシージャを考えてみる。

【００１７】

【表１】

メッセージ	値	説明
登録要求メッセージ	Ver	8ビットのプロトコルバージョン
	Cert	受信側のXMLディジタル証明書
	DId	128ビットのシリアル番号
登録応答メッセージ	Ver	8ビットのプロトコルバージョン
	{Seed}Device	コンテンツ暗号化鍵およびコンテンツインテグリティ鍵を取り出すのに使用される128ビットのシード
	SN	128ビットのシリアル番号
	Address	送信側の入来および送出近接パケットソケットのアドレス
	SId	128ビットのランダムなセッションID
近接検出アルゴリズム		近接検出アルゴリズムは帯域外で実行される

【００１８】

ここで、受信側は登録要求メッセージを送信するが、この登録要求メッセージは、情報の中でもとりわけ、受信側のディジタル証明書を含む。送信側は、登録要求メッセージを

受信するのに応答して、受信側の証明書を妥当性検査し、シードおよびランダムなセッションＩＤを生成し、これらを、上に示す形で、登録応答メッセージ中で受信側に返す。次いで受信側は、送信側の署名を妥当性検査し、セッションＩＤを入手し、図に示す他のアクションを実施する。次いで受信側および送信側は、後述する近接検出プロセスを経ることができる。

【００１９】

再妥当性検査に関しては、上に概説したのと同じプロシージャが実施されるが、相違点として、再妥当性検査の間は、受信側はすでにデータベースに登録されている。

【００２０】

近接検出に関しては、図２と共に以下を考えてみる。

【００２１】

近接検出の間、受信側は、近接検出初期化メッセージ中で示されたセッションＩＤを含むメッセージを、送信側に送信する。次いで送信側は、ナンス（Nonce）（１２８ビットのランダム値）を含むメッセージを受信側に送信し、コンテンツ暗号化鍵を使用して暗号化されたナンスで受信側が返信するのにかかる時間を測定する。最後に、送信側は、近接検出が成功したか否かを示すメッセージを受信側に送信する。

【００２２】

受信側は、近接検出が成功したという確証を有するまで、このプロセスを繰り返すことができる。この特定のプロトコルがＩＰベースのネットワークを介して使用されるときは、近接検出メッセージはＵＤＰを介して交換される。受信側は、登録応答メッセージを介して、送信側のアドレスを知る。受信側のアドレスは、近接検出初期化メッセージを搬送するＵＤＰパケットの入来ＩＰヘッダを調べることによって決定することができるので、別個に通信する必要はない。

【００２３】

以下の表に、近接検出の間に交換されるメッセージを記述する。

【００２４】

【表２】

メッセージ	値	説明
近接開始メッセージ	SId	送信側によって送信された同じ128ビットのセッションID値
近接チャレンジメッセージ	Seq	8ビットのインクリメンタルなシーケンス番号
	SId	同じ128ビットのセッションID
	Nonce	128ビットのランダム値
近接応答メッセージ	Seq	送信側によって決定された同じシーケンス番号
	SId	同じ128ビットのセッションID
	KC[Nonce]	コンテンツ暗号化鍵を使用して暗号化された128ビットのナンス
近接結果メッセージ	SId	同じ128ビットのセッションID
	Result	登録プロシージャの成功または失敗を示すステータスコード

【００２５】

セッション確立に関しては、図３と、セッション確立の間に交換されるメッセージを記述した以下の表と共に、以下を考えてみる。

【００２６】

【表３】

メッセージ	値	説明	
ライセンス要求メッセージ	Ver	8ビットのプロトコルバージョン	
	Cert	受信側のXMLディジタル証明書	
	SN	128ビットのシリアル番号	
	Action	コンテンツに対して要求される使用。例：「再生」「コピー」または「記録」	
	RId	128ビットのランダムな権利ID	
	VCRL	受信側のCRLのバージョン	
ライセンス応答メッセージ	Ver	8ビットのプロトコルバージョン	
	CRL	送信側のCRL。バージョン番号が受信側のCRLよりも大きく、受信側コンポーネントもまた送信機能を有する場合にのみ、送信される。	
	License	KC（受信側の公開鍵で暗号化済み）	128ビットのランダムなコンテンツ暗号化鍵
		KI（受信側の公開鍵で暗号化済み）	128ビットのランダムなコンテンツインテグリティ鍵
		VCRL	送信側のCRLのバージョン
		RId	受信側から送信された同じ128ビットのランダムな権利ID
		SN	128ビットのシリアル番号

【００２７】
この例では、ライセンス要求メッセージが受信側から送信側に送信され、ライセンス要求メッセージは上述の情報を含む。これに応答して、送信側は、上述の情報を含むライセンス応答メッセージを送信することができる。

【００２８】
この特定の例では、ライセンスはＸＭＲフォーマットで表され、コンテンツ暗号化鍵、コンテンツインテグリティ鍵（content integrity key）、送信側のＣＲＬのバージョン、１２８ビットの権利ＩＤ、および１２８ビットのシリアル番号を含む。ライセンスはまた、ＯＭＡＣを使用するコンテンツインテグリティ鍵を使用して計算されたＯＭＡＣも含む。

【００２９】
データ転送プロシージャに関しては、図４と共に以下を考えてみる。セッション確立が完了すると、制御プロトコル特有の方式でデータ転送が実行される。データ転送要求と応答は両方とも、制御プロトコルおよびコンテンツタイプに対して具体的に定義されなければならない。これを図４に概念的に表す。

【００３０】
発明的な実施形態をそれと共に利用することのできる例示的なプロトコルの簡単な概観をここに提供したが、次に、ＲＴＳＰに関するいくらかの背景情報を考えてみる。

【００３１】
（ＲＴＳＰ）
当業者には理解されるであろうが、リアルタイムストリーミングプロトコルすなわちＲ

ＴＳＰは、リアルタイムプロパティを有するデータの送達（すなわちストリーミング）に対する制御のための、アプリケーションレベルのプロトコルである。ＲＴＳＰは、オーディオやビデオなどのリアルタイムデータの、制御されたオンデマンドの送達を可能にするための、拡張可能フレームワークを提供する。データのソースは、ライブデータフィードと記憶済みクリップとの両方を含むことができる。このプロトコルは、複数のデータ送達セッションを制御し、ＵＤＰやマルチキャストＵＤＰやＴＣＰなどの送達チャネルを選択する手段を提供し、ＲＴＰに基づく送達機構を選択する手段を提供するように意図されている。

【００３２】

ＲＴＳＰは、オーディオやビデオなど連続的なメディアの、単一またはいくつかの時間同期ストリームを確立および制御する。連続的なメディアストリームに制御ストリームをインタリーブすることは可能だが、ＲＴＳＰは通常、連続的なストリーム自体は送達しない。言い換えれば、ＲＴＳＰは、マルチメディアサーバに対する「ネットワークリモートコントロール」としての働きをする。

【００３３】

制御されることになる１組のストリームは、プレゼンテーション記述（presentation description）によって定義される。ＲＴＳＰでは、ＲＴＳＰ接続の概念はない。そうではなく、サーバが、識別子でラベル付けされたセッションを維持する。ＲＴＳＰセッションは、ＴＣＰ接続などのトランスポートレベルの接続に結び付けられることは決してない。ＲＴＳＰセッションの間、ＲＴＳＰクライアントは、サーバへの多くの信頼できるトランスポート接続を開閉して、ＲＴＳＰ要求を発行することができる。あるいは、当業者には理解されるであろうが、ＵＤＰなどのコネクションレストランスポートプロトコルを使用することもできる。

【００３４】

ＲＴＳＰによって制御されるストリームは、ＲＴＰを使用することができるが、ＲＴＳＰの動作は、連続的なメディアを搬送するのに使用されるトランスポート機構に依存しない。

【００３５】

次に、図５と共に、クライアント／受信側５００とサーバ／送信側５０２との間の典型的なＲＴＳＰ要求／応答交換を考えてみる。

【００３６】

ＲＴＳＰ要求／応答はヘッダを有するが、話を簡単にするために、ヘッダについては述べない。ＲＴＳＰでは、クライアント／受信側５００は通常、ＤＥＳＣＲＩＢＥ要求として知られるものを発行する。これは、要求ＵＲＬで識別されるプレゼンテーションまたはメディアオブジェクトの記述をサーバ５０２から取り出すことに向けられている。サーバ５０２は、ＳＥＳＳＩＯＮ　ＤＥＳＣＲＩＰＴＩＯＮ　ＰＲＯＴＯＣＯＬ（ＳＤＰ）中で表される要求されたリソースの記述で応答する。ＤＥＳＣＲＩＢＥ応答（ＳＤＰ）は、それが記述するリソースに関するすべてのメディア初期化情報を含む。

【００３７】

次に、クライアント５００は、ストリーミングされるメディアに使用されることになるトランスポート機構を指定するＵＲＩを求めるＳＥＴＵＰ要求を送信する。図５の例では、オーディオとビデオの両方についてＳＥＴＵＰ要求が送信される。クライアント５００はまた、ＳＥＴＵＰ要求中で、利用することになるトランスポートパラメータを示す。ＳＥＴＵＰ要求中のトランスポートヘッダは、データ伝送のためにクライアントにとって許容可能なトランスポートパラメータを指定する。サーバ５０２からのＲＥＳＰＯＮＳＥは、サーバによって選択されたトランスポートパラメータを含む。サーバはまた、ＳＥＴＵＰ要求に応答して、セッション識別子も生成する。

【００３８】

この時点で、クライアントはＰＬＡＹ要求を発行することができるが、このＰＬＡＹ要求は、ＳＥＴＵＰ中で指定された機構を介してデータ送信を開始するようサーバに伝える

。ＰＬＡＹ要求の受信に応答して、サーバはコンテンツのストリーミングを開始することができ、コンテンツは、この例ではオーディオ／ビデオコンテンツである。当業者には理解されるであろうが、この例では、ストリーミングコンテンツは、ＲＴＰパケットを使用してカプセル化され、ＵＤＰを介して送信される。

【００３９】

ＲＴＳＰプロトコルは、ＰＡＵＳＥ、ＴＥＡＲＤＯＷＮ、ＧＥＴ＿ＰＡＲＡＭＥＴＥＲ、ＳＥＴ＿ＰＡＲＡＭＥＴＥＲ、ＲＥＤＩＲＥＣＴ、およびＲＥＣＯＲＤを含めて、他にも興味を引くメソッドを有する。ＲＴＳＰに関する追加の背景については、文献を参照されたい（例えば、非特許文献１参照。）。

【００４０】

（ＲＴＳＰを使用した例示的な実装形態）

以下の説明では、２つの主要なサブセクションが現れる。一方は「制御フロー」という題名であり、ＤＲＭ保護付きコンテンツのための制御フローが、ＲＴＳＰを使用してどのように確立されるかについて述べる。もう一方は「データフロー」という題名であり、ＤＲＭ保護付きコンテンツのためのデータフローが、ＲＴＰを使用してどのように確立されるかについて述べる。これらの主要なサブセクションはそれぞれ、発明的な実施形態の態様について述べるそれ自体の関連サブセクションを有する。

【００４１】

以下の説明では、前述のプロトコルのセッション確立プロシージャおよびデータ転送プロシージャが、一実施形態によりＲＴＳＰ／ＲＴＰを使用してどのように達成されるかについて述べる。より具体的には、以下の「制御フロー」セクションでは、セッション確立がＲＴＳＰを使用してどのように達成されるかについて述べる。「データフロー」セクションでは、データ転送がＲＴＰを使用してどのように達成されるかについて述べる。

【００４２】

（制御フロー）

この実施形態によれば、ＤＲＭ保護付きコンテンツ、すなわち関連するライセンスを有するコンテンツを再生したい受信側デバイスによって、セッション確立が開始される。上記のコンテンツセキュリティおよびライセンスプロトコルの説明から、クライアント／受信側はライセンス要求メッセージをサーバ／送信側に相応に送信することになり、サーバ／送信側はこれにライセンス応答メッセージで返信することになることを想起されたい。ライセンス応答メッセージは、ライセンスを搬送するが、このライセンスは、上の例では拡張可能メディア権利（eXtensible Media Rights）（ＸＭＲ）で表される。ライセンスは、要求されているコンテンツに関連するポリシーおよびコンテンツ鍵を含む。

【００４３】

（ＤＥＳＣＲＩＢＥ要求におけるライセンス要求メッセージの搬送）

次に、図６と共に、コンテンツセキュリティおよびライセンスプロトコルとＲＴＳＰとの合流を考えてみる。具体的には、図６には、一実施形態によるクライアント／受信側６００およびサーバ／送信側６０２を示す。この実施形態によれば、クライアント／受信側６００がＤＲＭ保護付きコンテンツにアクセスしたいとき、クライアントは、ＤＥＳＣＲＩＢＥ要求の本文にライセンス要求メッセージを挿入する。

【００４４】

実装例の１つに過ぎないが、一実施形態による、ライセンス要求メッセージを組み込んだ以下のＤＥＳＣＲＩＢＥ要求の抜粋を考えてみる。

【００４５】

【表４】

```
DESCRIBE rtsp://eduardo01/file.wmv RTSP/1.0
Accept: application/sdp
CSeq: 1
Supported: com.microsoft.wmdrm-nd,
      com.microsoft.wm.eosmsg, method.announce
Require: com.microsoft.wmdrm-nd
Content-Type: application/vnd.ms-wmdrm-license-request
Content-Length: 1078
License_Request_Message
```

【００４６】

この例では、サーバが特定タイプの送信側であると受信側が予想していることを示すために、「Require:com.microsoft.wmdrm-nd」が使用されている。この例では、ＤＥＳＣＲＩＢＥの本文がライセンス要求メッセージを含むことを示すために、「Content-Type:application/vnd.ms-wmdrm-license-request」が使用されている。

【００４７】

エラーがない限り、送信側は、すぐ下のセクションで述べるライセンス応答メッセージを含むＳＤＰ記述で返信すべきである。

【００４８】

（ＳＤＰ記述中へのライセンス応答メッセージの埋め込み）

ライセンス要求メッセージを本文に含むＤＥＳＣＲＩＢＥ要求を受信すると、サーバは、ライセンス応答メッセージを返すことができる。この例では、サーバは、前述の様々なパラメータを含むだけでなく、ライセンス応答メッセージをも含むＳＤＰ記述を返す。この実施形態では、ライセンス応答メッセージは、前に示したように、どのポリシーがこのコンテンツに適用されるかを指示するＸＭＲライセンスを搬送することになる。

【００４９】

実装例の１つに過ぎないが、一実施形態による、ライセンス応答メッセージを組み込んだ以下のＳＤＰの抜粋を考えてみる。

【００５０】

【表５】

```
RTSP/1.0 200 OK
Last-Modified: Thu, 19 Dec 2002 15:36:18 GMT
Content-Length: 1891
Content-Type: application/sdp
CSeq: 1
Supported: com.microsoft.wmdrm-nd,
      com.microsoft.wm.eosmsg, method.announce
SDP_Description
```

【００５１】

一実施形態によれば、送信側から返されるＳＤＰは、非特許文献２中の仕様に従ってデータＵＲＬに符号化されたライセンス応答メッセージを含む。データＵＲＬに含まれるデータは、この例では、Ｂａｓｅ６４符号化されなければならず、ＭＩＭＥタイプは「application/vnd.ms-wmdrm-license-response」に設定されなければならない。

【００５２】

この構文の一例として、以下を考えてみる。

【００５３】

【表６】

data:application/vnd.ms-wmdrm-license-response;base64,
AggAAAAAAAABOFhNUgAAAAAB+TTbzXCRw1s+/jA4fQQY0wADAAEAAAEgAAMA
AgAAADwAAQADAAAAEgBkAAAAAAAAAAAAAQAMAAAAGKRuHVtxsJ1Lk7WPrQPe
5X0AAQANAAAACgABAAMABAAAABoAAQAFAAAAEgBkAGQAZABkAGQAAwAJAAAA
pgABAAoAAACeajiAiUBMGrAGUAOIqMGBggABAAEAgC7V1QF54EzuYbTYKPbg
BEK6nDXGtbV+bJKF+Cn2yd/FUaC4vTIOxkF/eQLx+FqvLCUMtxvRSw01dns9
Ejt021se2T+IROiZA0t5pRuNl3gq7JK9JKs+ZX8hKsEJFW0V7cyp9wdaCMh2
esJ97r9agH1Sxf0mAqcQ0j1Q5dtXlWx/AAEACwAAABwAAQAQZZaX5nGEUAV8
w6p6BQr++Q==

【００５４】

データＵＲＬは、この例では、ＳＤＰ鍵管理拡張子（SDP key management extensions）の仕様（現時点では引き続き進行中の作業である）に従って、「a=key-mgmt」属性を使用してＳＤＰセッションレベルで挿入されなければならない。この構文は、以下のとおりである。

【００５５】

a=key-mgmt:wmdrm-nd URL

ＵＲＬパラメータは、上述したデータＵＲＬである。

【００５６】

（ＡＮＮＯＵＮＣＥ要求におけるライセンス応答メッセージの搬送）

次に、いくつかのメディアファイルが、異なるポリシーの施行を必要とする複数のセグメントを含むと考えてみる。ＴＶ録画のためにウィンドウズ（登録商標）メディアセンタエディション（Windows（登録商標） Media Center Edition）によって生成されたファイルの場合を例にとる。このようなファイルは、ＷＭＤＲＭによって保護され、複数のポリシーが関連する。例えば、ＴＶショーにはマクロビジョン（Macrovision）が必要とされるが、これと同じ録画内に現れるコマーシャルセグメントには必要とされない場合がある。

【００５７】

この要件の結果、ストリームの途中で更新済みポリシーを送達するための機構を定義することが必要になる。一実施形態によれば、更新済みポリシーは、ＲＴＳＰのＡＮＮＯＵＮＣＥ要求を使用してストリームの途中で送達することができる。この実施形態では、ＡＮＮＯＵＮＣＥ要求は、新しいＸＭＲライセンスを含むライセンス応答メッセージを搬送する。

【００５８】

この例では、ストリーミングメディアに関連するポリシーが変化するかもしれない２つの異なる場合がある。第１の場合では、特定のストリームに関連するポリシーのみが変化することがある。第２の場合では、ポリシーとコンテンツフォーマット自体との両方が変化する可能性がある。

【００５９】

ストリーミングメディアに関連するポリシーのみが変化する第１の場合を考えてみる。この場合の一例は、ＴＶショーのセグメントとコマーシャルとの間の切替えであろう。ここで、ＴＶセグメントでは、マクロビジョンがアナログ出力に対してイネーブルにされる必要があるが、コマーシャルではその必要はない。この例では、ポリシーのみが変化し、ビットレートやコーデックなどの符号化パラメータは同じままであることに留意されたい。

【００６０】
ポリシーとコンテンツフォーマットとの両方が変化する第２の場合を考えてみる。この場合の一例もまた、ＴＶショーのセグメントとコマーシャルとの間の切替えであろう。ここで、ポリシーについては同じタイプの変化がある。しかしこの例では、ＴＶショーとコマーシャルは、高精細度符号化から標準精細度符号化への移行など、異なる符号化パラメータを使用して符号化される。このようなシナリオは一般に「フォーマット変更」と呼ばれる。この場合の別の例は、「エントリ変更」として一般に知られるものに関係する。エントリ変更は通常、「サーバ側プレイリスト」の一部としてサーバによって送達されているメディアファイル中の切替えの結果である。これらのプレイリストは、どんな符号化パラメータやポリシーも共有するとは限らないメディアファイルの集まりで構成される場合がある。

【００６１】
第１の場合で例示したように、ポリシーは変化するがフォーマットは変化しないときはいつでも、サーバは、新しいポリシーのみをＡＮＮＯＵＮＣＥ要求の本文の一部としてクライアントに送信する。この場合、ＡＮＮＯＵＮＣＥメッセージの本文にライセンス応答メッセージが含まれる。例として図７を考えてみるが、図７には、例示的なクライアント／受信側７００およびサーバ／送信側７０２が示してあり、サーバ／送信側７０２は、新しいライセンスを更新済みポリシーと結び付けるために、ＡＮＮＯＵＮＣＥ要求をクライアント／受信側に発行している。

【００６２】
第２の場合で例示したように、ポリシーが変化してフォーマットもまた変化するときはいつでも、サーバは、更新済みＳＤＰ記述をクライアントに送達する。このＳＤＰ記述は、行われたフォーマット変更を記述するのに必要とされる。この例では、フォーマット変更の場合のＳＤＰ記述もまた、ＡＮＮＯＵＮＣＥ要求として送達される。したがって、一方がフォーマット変更を含み、もう一方がポリシー変更を含む、２つの連続したＡＮＮＯＵＮＣＥ要求を送達する代わりに、サーバは、ＳＤＰ記述を搬送する１つのＡＮＮＯＵＮＣＥ要求のみを送信すればよい。この場合、ポリシー変更は、ＳＤＰ記述に埋め込まれたライセンス応答メッセージとして通信される。再び図７を考えてみると、図７には、ライセンス応答メッセージが埋め込まれた更新済みＳＤＰを本文に含むＡＮＮＯＵＮＣＥ要求が示してある。

【００６３】
ＡＮＮＯＵＮＣＥ要求の一部であるＳＤＰ記述にライセンス応答メッセージを埋め込むためのフォーマットは、ＤＥＳＣＲＩＢＥ応答の一部であるＳＤＰ記述を埋め込むための前述のフォーマットと同じである。

【００６４】
図８は、一実施形態による方法のステップを記述した流れ図である。この方法は、任意の適切なハードウェア、ソフトウェア、ファームウェア、またはこれらの組合せと共に実施することができる。一実施形態では、この方法は、何らかのタイプのコンピュータ可読媒体上に組み入れられた１組のコンピュータ可読命令またはソフトウェアコードとして実施される。

【００６５】
ステップ８００で、ストリーミングプロトコルを介して、ＤＲＭ保護付きコンテンツのためのライセンスを求める要求を送信することによって、制御フローの確立を試みる。図示および記述する実施形態では、このステップはクライアント／受信側によって実行される。ライセンスを求める要求の具体的な一例は、前述のライセンス要求メッセージである。特許請求する主題の趣旨および範囲を逸脱することなく、他の要求タイプまたはフォーマットを利用することもできる。加えて、ストリーミングプロトコルの一例（すなわちＲＴＳＰ）も上述してある。特許請求する主題の趣旨および範囲を逸脱することなく、他のストリーミングプロトコルを使用することもできる。ＲＴＳＰ実施形態では、要求はＤＥＳＣＲＩＢＥ要求の本文に挿入される。

【００６６】
ステップ８０２で、ライセンスを求める要求を受信することによって、制御フローの確立を試みる。このステップは、この例ではサーバ／送信側によって実施される。要求を受信するのに応答して、ステップ８０４で、ストリーミングプロトコルを使用してライセンスをクライアント／受信側に送信することができる。ライセンスがクライアント／受信側に返される場合の具体的な一例は、ライセンスがライセンス応答メッセージの形でクライアント／受信側に送信される場合として上に提供してある。特許請求する主題の趣旨および範囲を逸脱することなく、他の応答タイプまたはフォーマットを利用することもできる。加えて、ストリーミングプロトコルの一例（すなわちＲＴＳＰ）も上述してある。特許請求する主題の趣旨および範囲を逸脱することなく、他のストリーミングプロトコルを使用することもできる。ＲＴＳＰ実施形態では、応答はＳＤＰで送信される。

【００６７】
ステップ８０４はまた、更新をクライアント／受信側に送信するために実施することもできることを認識および理解されたい。この場合では、かつＲＴＳＰ実施例のコンテキストでは、更新は、前述のようにＡＮＮＯＵＮＣＥ要求を使用して送達することができる。

【００６８】
ステップ８０６で、ストリーミングプロトコルを介してライセンスを受信する。図示および記述する実施形態では、このステップはクライアント／受信側によって実施される。ライセンスの受信後、クライアントは、ライセンスに定義された条件に従って、コンテンツにアクセスしてコンテンツを消費することができる。

【００６９】
ライセンス獲得プロセスに続くデータフローについて、以下に述べる。

【００７０】
（データフロー）
ＲＴＳＰをＤＲＭ保護付きコンテンツと共に利用する制御フローの例示的な実施形態について述べたが、次に、実際のＤＲＭ保護付きコンテンツの通信を含むかまたは可能にするデータフローを考えてみる。

【００７１】
以下に述べる実施形態では、ＲＴＰをデータ転送プロトコルとして使用して、ＤＲＭ保護付きコンテンツが送信側と受信側との間で通信される。すなわち、ＤＲＭ保護付きコンテンツは、送信側から通信され、受信側に通信される。

【００７２】
提供する特定の例では、２つの異なる手法について述べる。第１の手法では、利用されるＲＴＰペイロードフォーマットは拡張子をサポートし、拡張子は、暗号化済みペイロードデータが復号プロセスを経て復号されることができるように、鍵ＩＤ拡張子や初期化ベクトルなどの暗号化パラメータをＲＴＰパケットに含めることを可能にする。第２の手法では、ＲＴＰペイロードフォーマットは拡張子をサポートしない。したがってこの手法では、記述子が定義され、記述子は、暗号化済みペイロードを含むＲＴＰパケットに関連付けられる。記述子は、暗号化済みペイロードデータを復号するために復号プロセスで使用することのできる鍵ＩＤ拡張子や初期化ベクトルなどの暗号化パラメータを含む。

【００７３】
（ウィンドウズ（登録商標）メディアペイロードフォーマットを介したサンプル暗号化済みペイロードの搬送）
図９に、一実施形態によるＲＴＰパケットの例示的な各部分を、９００において一般に示す。この実施形態では、利用されるＲＴＰペイロードフォーマットは、暗号化済みペイロードコンテンツと共に鍵ＩＤ拡張子や初期化ベクトルなどの暗号化パラメータをＲＴＰパケットに含めることができるようにして、拡張子をサポートする。このようなフォーマットの一例は、ウィンドウズ（登録商標）メディアＲＴＰペイロード（Windows（登録商標） Media RTP Payload）フォーマットであり、これは非特許文献３で述べられている。しかし、特許請求する主題の趣旨および範囲を逸脱することなく、他のフォーマットを利

用することもできる。

【００７４】

パケット９００は、この例では、ＲＴＰヘッダ９０２およびペイロードフォーマットヘッダ９０４を含む。ペイロードフォーマットヘッダは、この例では、拡張子を可能にする。したがって、パケット９００はさらに、暗号化済みペイロードデータ９１０（オーディオデータまたはビデオデータ）と共に、鍵ＩＤ拡張子９０６および初期化ベクトル９０８を含み、暗号化済みペイロードデータ９１０は、鍵ＩＤ拡張子９０６および初期化ベクトル９０８に関連付けられており、これらを使用して復号することができる。さらに、ＲＴＰパケット９００は、他の複数の暗号化済みペイロードを含むこともできる。この特定の例では、パケット９００はさらに、暗号化済みペイロードデータ９１０ａ（オーディオデータまたはビデオデータ）と共に、別のペイロードフォーマットヘッダ９０４ａ、鍵ＩＤ拡張子９０６ａ、初期化ベクトル９０８ａを含み、暗号化済みペイロードデータ９１０ａは、鍵ＩＤ拡張子９０６ａおよび初期化ベクトル９０８ａに関連付けられており、これらを使用して復号することができる。

【００７５】

この特定の実施形態では、１つのＲＴＰパケットが、複数の異なる暗号化済みペイロードを含むことができる。具体的なコンテキストの１つにおける具体的な一実装例として、ウィンドウズ（登録商標）メディアオーディオビデオコンテンツ（Windows（登録商標）Media Audio and Video Content）に関して以下を考えてみる。

【００７６】

前述のようにライセンスで保護されたウィンドウズ（登録商標）メディアコンテンツを搬送するとき、ＲＴＰパケット中では、以下の値およびフィールドが設定されなければならない。

【００７７】

１．「ＭＡＵプロパティ」セクションのビットフィールド２中の「暗号化」ビット（Ｅ）は１に設定されなければならない。

【００７８】

２．拡張子フィールドがあることを示すために「ＭＡＵタイミング」セクション中の「拡張子存在」ビット（Ｘ）は１にセットされなければならない。

【００７９】

３．「暗号化済みペイロード境界」拡張子があってはならない。

【００８０】

４．「ＷＭＤＲＭ初期化ベクトル」拡張子が含まれなければならない。以下の値が設定されなければならない。

ａ．「拡張子タイプ」は２に設定されなければならない。

ｂ．「拡張子長さ」は８に設定されなければならない（６４ビットを意味する）。

ｃ．「拡張子データ」は、以下の「サンプル暗号化」という題名のセクションで定義するサンプルＩＤ値に設定されなければならない。

ｄ．この拡張子は、あらゆるＭＡＵの第１のペイロードに対して含まれなければならない。ＭＡＵが複数のペイロードに断片化されている場合、この拡張子は第１のペイロード中のみにあるべきである。

【００８１】

５．「ＷＭＤＲＭ鍵ＩＤ」拡張子が含まれなければならない。以下の値が設定されなければならない。

ａ．「拡張子タイプ」は３に設定されなければならない。

ｂ．「拡張子長さ」は１６に設定されなければならない（１２８ビットを意味する）。

ｃ．「拡張子データ」は、ＡＳＦコンテンツを搬送するときのＡＳＦコンテンツ暗号化オブジェクトからの鍵ＩＤ値に設定されなければならない。あるいは、ＤＶＲ－ＭＳなどの非ＡＳＦコンテンツを搬送するときに使用される暗号化鍵を表す鍵ＩＤ値に設定される。

ｄ．この拡張子は、パケット損失の問題に対処するために、複数ペイロードを含むＲＴＰパケットそれぞれの中の、第１のペイロードに対して含まれなければならない。

【００８２】

（サンプル暗号化）

上の項目４（ｃ）のさらなる説明として、以下を考えてみる。この実施形態では、カウンタモードのＡＥＳを使用して各サンプルを暗号化すべきである。図１０に、この技法を使用して単一のサンプルを暗号化するためのプロセスを示す。

【００８３】

この実施形態では、カウンタモードがバイトのストリームを生み出し、次いでこれらのバイトは、メディアサンプルの平文テキストバイトと排他的論理和がとられて、暗号化済みメディアサンプルが生み出される。鍵ストリームジェネレータが、ＡＥＳラウンドを使用して、一度に１６バイトブロックの鍵ストリームを生成する。ＡＥＳラウンドへの入力は、コンテンツ暗号化鍵（Ｋｃ）、および、サンプルＩＤとサンプル内のブロック番号との１２８ビット連結である。

【００８４】

鍵ストリームジェネレータの出力は、メディアサンプルの対応するブロック（ｉ）からのデータと、バイトごとに排他的論理和がとられるべきである。メディアサンプルが１６バイトで均等に分割可能でない場合は、最後のブロックからのメディアデータの有効バイトのみが、鍵ストリームと排他的論理和がとられて、暗号化済みサンプルに対して保持されるべきである。

【００８５】

ＡＳＦファイルからサンプルを暗号化するときは、サンプルＩＤは、ペイロード拡張子からのサンプルＩＤと等価である。

【００８６】

したがって、この実施形態では、データは「サンプル」境界に従って暗号化および復号され、「サンプル」境界は、所与のメディアタイプの自然な境界である。例えば、ビデオストリームの場合はビデオフレームであり、あるいはオーディオストリームの場合はオーディオサンプルのブロックである。

【００８７】

（データセグメント記述子を使用するＲＴＰペイロードフォーマットを介したリンク暗号化済みペイロードの搬送）

図１１に、別の実施形態によるパケットの態様を、１１００において一般に示す。この例では、パケット１１００は、ＩＰヘッダ１１０２、ＵＤＰヘッダ１１０４、ＲＴＰヘッダ１１０６、ペイロードフォーマットヘッダ１１０８、ペイロードデータ１１１０、および記述子１１１２を含むことができる。この特定の例では、記述子はペイロードデータの最後に付加されているが、記述子は任意の適切な位置に配置することができる。当業者には理解されるであろうが、記述子をペイロードデータの最後に配置することで、後方互換性問題を緩和することができる。

【００８８】

この実施形態では、ＲＴＰヘッダを除くＲＴＰパケットは、記述子１１１２に関連するデータセグメントとして扱われる。記述子１１１２は、ペイロードデータ１１１０の復号を可能にする復号プロセスで使用することのできる暗号化パラメータを伴う。この特定の例では、単一のポリシーおよびコンテンツ暗号化鍵が、ペイロードデータ１１１０に適用される。

【００８９】

一実施形態によれば、記述子１１１２は、以下のデータ構造を備える。

【００９０】

【表７】

セクション	フィールド
フラグ	8ビットのフラグ
拡張子	8ビットの拡張子数
	複数の可変長拡張子
長さ	データセグメント記述子の長さ

【００９１】

この例で、フラグセクションは、データの属性を示すビットフィールドである。現在、次の値が定義されている。すなわち、０×０１は、暗号化済みデータを示す。このフラグが設定されているとき、これは、データが暗号化された形であることを示す。そうでないときは、データは平文である。

【００９２】

拡張子セクションに関しては、拡張子数フィールドは、この記述子に含まれる可変長の拡張子の数を示す。可変長拡張子フィールドに関しては、各拡張子が以下のフォーマットを有する。

【００９３】

【表８】

フィールド
8ビットの拡張子タイプ
16ビットの拡張子長さ
可変長拡張子

【００９４】

一実施形態によれば、鍵ＩＤ拡張子およびデータセグメントＩＤ拡張子が、以下のように定義される。

【００９５】

（鍵ＩＤ拡張子）

拡張子タイプ：鍵ＩＤ拡張子について０×０１に設定されなければならない。

拡張子長さ：１２８ビット（１６バイト）を表す１６に設定されなければならない。

拡張子：この記述子と共に送達される暗号化済みメディアについての鍵ＩＤ値を含まなければならない。この拡張子は、暗号化済みデータフラグが設定されているときにのみ使用される。

【００９６】

（データセグメントＩＤ拡張子）

拡張子タイプ：データセグメントＩＤ拡張子について０×０２に設定されなければならない。

拡張子長さ：６４ビット（８バイト）を表す８に設定されなければならない。

拡張子：この記述子と共に送達される暗号化済みメディアについてのデータセグメントＩＤを含まなければならない。この拡張子は、暗号化済みデータフラグが設定されているときにのみ使用される。

【００９７】

長さセクションに関しては、この実施形態では、このセクションはデータセグメント記述子の長さの総計をバイトで含まなければならない。この長さは、この記述子と共に送達されるメディアデータのサイズは含まない。

【００９８】

（結び）

上述した様々な実施形態は、ディジタル著作権管理（ＤＲＭ）などのコンテンツ保護方

法を利用して、ホームメディアネットワークなどのローカルネットワーク内のマシンおよびデバイス上での安全なコンテンツ再生を可能にする。少なくともいくつかの実施形態では、メッセージおよびコンテンツはリアルタイムストリーミングプロトコル（ＲＴＳＰ）およびリアルタイムトランスポートプロトコル（ＲＴＰ）を介して送達され、また、ＲＴＳＰ／ＲＴＰによってもたらされる利点を享受するプロトコル拡張子が導入されるが、これらの利点には、ユーザデータグラムプロトコル（ＵＤＰ）を介したデータ送達、および、クライアントとサーバとの間の双方向通信が含まれる。

【００９９】

構造上の特徴および／または方法上のステップに特有の言葉で本発明を述べたが、添付の特許請求の範囲に定義する本発明は、上述した特定の特徴またはステップに必ずしも限定されないことを理解されたい。これらの特定の特徴およびステップは、特許請求する本発明を実施する好ましい形として開示する。

【図面の簡単な説明】

【０１００】

【図１】本発明の一実施形態によるプロトコルの例示的な登録プロシージャを示す図である。

【図２】本発明の一実施形態によるプロトコルの例示的な近接検出プロシージャを示す図である。

【図３】本発明の一実施形態によるプロトコルの例示的なセッション確立プロシージャを示す図である。

【図４】本発明の一実施形態によるプロトコルの例示的なデータ転送プロシージャを示す図である。

【図５】本発明の一実施形態によるストリーミングプロトコルの態様を示す図である。

【図６】本発明の一実施形態に関して利用される図５のストリーミングプロトコルを示す図である。

【図７】本発明の一実施形態に関して利用される図５のストリーミングプロトコルを示す図である。

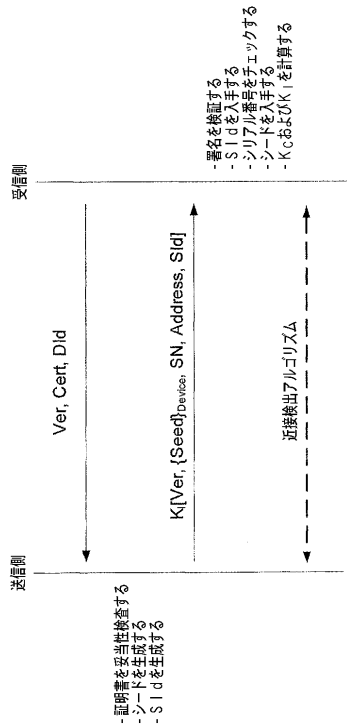
【図８】本発明の一実施形態による方法のステップを記述した流れ図である。

【図９】本発明の一実施形態によるパケットを示す図である。

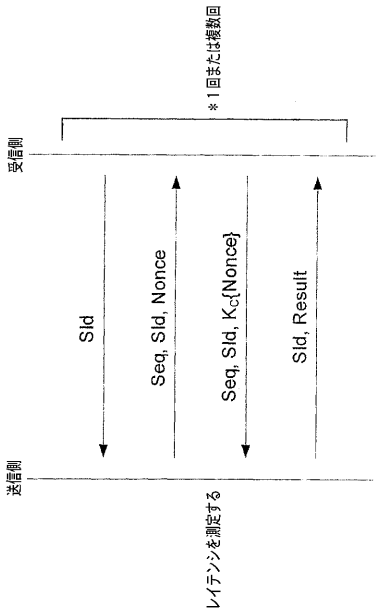
【図１０】本発明の一実施形態によるサンプル暗号化を示す図である。

【図１１】本発明の一実施形態によるパケットを示す図である。

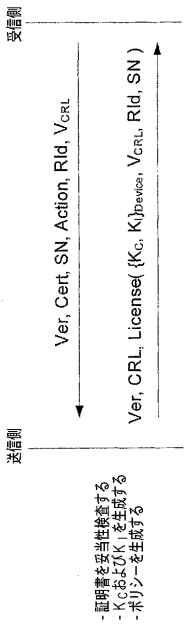
【図１】


受信側
送信側
Ver, Cert, DId
K[Ver, {Seed}Device, SN, Address, SId]
近接検出アルゴリズム
- 署名を検証する
- ＳＩｄを入手する
- シリアル番号をチェックする
- シードを入手する
- KCおよびKｉを計算する
- 証明書を妥当性検査する
- シードを生成する
- ＳＩｄを生成する

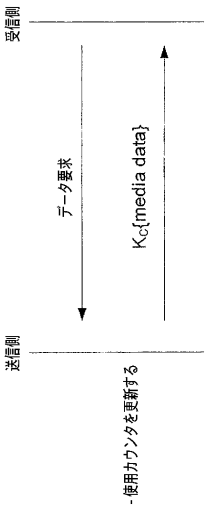
【図２】


＊1回または複数回
受信側
送信側
SId
Seq, SId, Nonce
Seq, SId, KC{Nonce}
SId, Result
- レイテンシを測定する

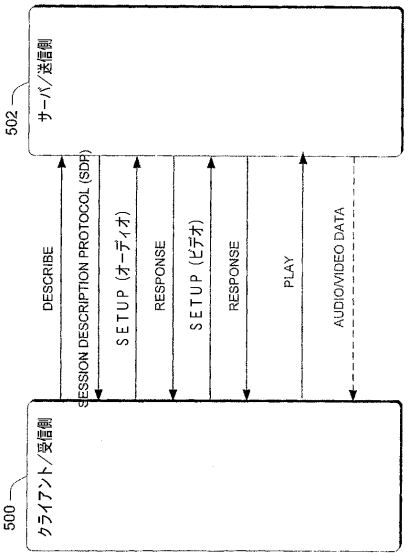
【図３】


受信側
送信側
Ver, Cert, SN, Action, RId, VCRL
Ver, CRL, License({KC, Ki}Device, VCRL, RId, SN)
- 証明書を妥当性検査する
- KCおよびKｉを生成する
- ポリシーを生成する

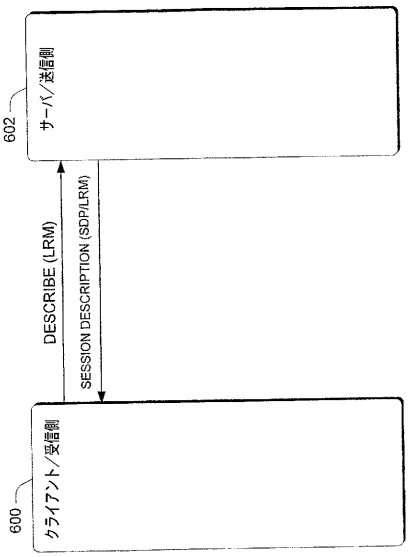
【図４】


受信側
送信側
データ要求
KC{media data}
- 使用カウンタを更新する

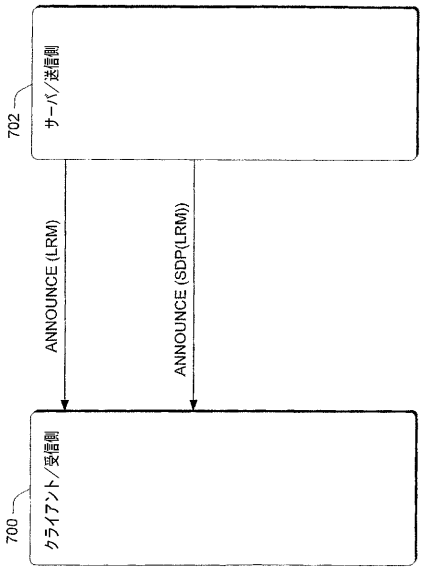
【図５】


502
サーバ／送信側
DESCRIBE
SESSION DESCRIPTION PROTOCOL (SDP)
SETUP (オーディオ)
RESPONSE
SETUP (ビデオ)
RESPONSE
PLAY
AUDIO/VIDEO DATA
500
クライアント／受信側

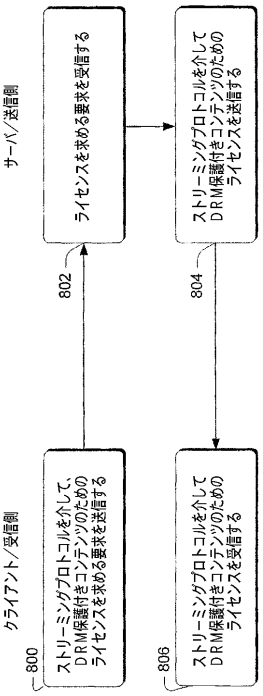
【図６】


602
サーバ／送信側
DESCRIBE (LRM)
SESSION DESCRIPTION (SDP/LRM)
600
クライアント／受信側

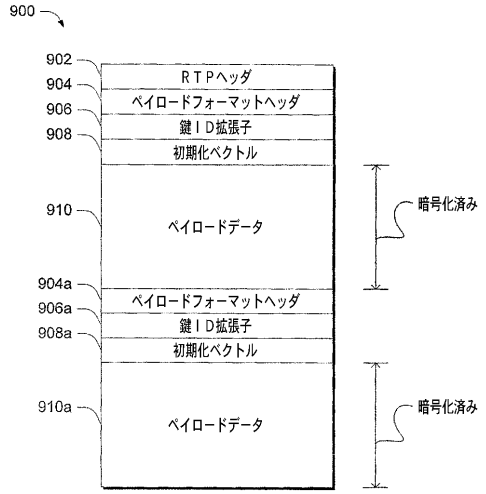
【図７】


702
サーバ／送信側
ANNOUNCE (LRM)
ANNOUNCE (SDP(LRM))
700
クライアント／受信側

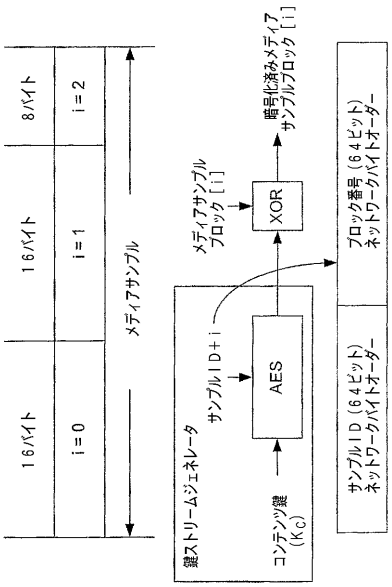
【図８】


サーバ／送信側
ライセンスを求める要求を受信する
ストリーミングプロトコルを介して
DRM保護付きコンテンツのための
ライセンスを送信する
802
804
クライアント／受信側
ストリーミングプロトコルを介して、
DRM保護付きコンテンツのための
ライセンスを求める要求を送信する
ストリーミングプロトコルを介して
DRM保護付きコンテンツのための
ライセンスを受信する
800
806

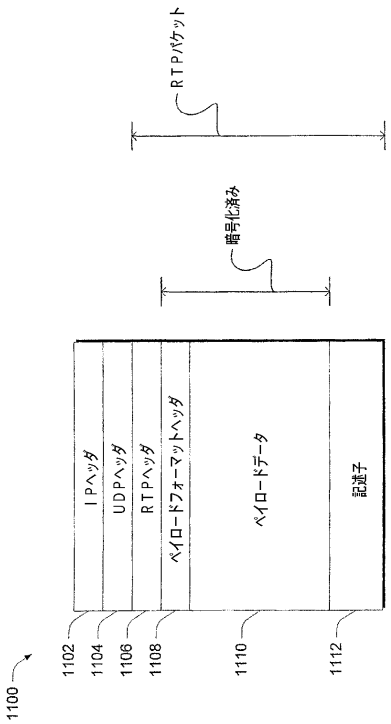
【図９】


900
902
RTPヘッダ
904
ペイロードフォーマットヘッダ
906
鍵ID拡張子
908
初期化ベクトル
910
ペイロードデータ
暗号化済み
904a
ペイロードフォーマットヘッダ
906a
鍵ID拡張子
908a
初期化ベクトル
910a
ペイロードデータ
暗号化済み

【図１０】


8バイト
i = 2
16バイト
i = 1
メディアサンプル
16バイト
i = 0
メディアサンプル ブロック [i]
暗号化済みメディア サンプルブロック [i]
XOR
鍵ストリームジェネレータ
サンプルID+i
AES
コンテンツ鍵 (K_C)
ブロック番号 (64ビット) ネットワークバイトオーダー
サンプルID (64ビット) ネットワークバイトオーダー

【図１１】


RTPパケット
暗号化済み
IPヘッダ
UDPヘッダ
RTPヘッダ
ペイロードフォーマットヘッダ
ペイロードデータ
記述子
1100
1102
1104
1106
1108
1110
1112

フロントページの続き

(72)発明者　アンダース　イー．クレメッツ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　エドアルド　ピー．オリベイラ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　サンジェイ　バット
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

審査官　矢野　光治

(56)参考文献　特開２００４－２８７９３７（ＪＰ，Ａ）
特開２００４－３２８７０６（ＪＰ，Ａ）
特開２００４－１５８９３６（ＪＰ，Ａ）
特開２００３－２２４５５６（ＪＰ，Ａ）
特開２００４－２８２７３１（ＪＰ，Ａ）
特表２００４－５３７１９１（ＪＰ，Ａ）
特表２００５－５１３６６４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04N　7/16-7/173