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

特許第5496917号
(P5496917)

(45)発行日　平成26年5月21日(2014.5.21)　(24)登録日　平成26年3月14日(2014.3.14)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
H04N 21/266 (2011.01)　H04L 9/00 601E
H04N 21/2362 (2011.01)　H04N 21/266
H04N 21/2362

請求項の数 25　(全 29 頁)

(21)出願番号　特願2010-546910 (P2010-546910)
(86)(22)出願日　平成21年2月13日 (2009.2.13)
(65)公表番号　特表2011-514747 (P2011-514747A)
(43)公表日　平成23年5月6日 (2011.5.6)
(86)国際出願番号　PCT/US2009/034010
(87)国際公開番号　WO2009/102923
(87)国際公開日　平成21年8月20日 (2009.8.20)
審査請求日　平成22年10月18日 (2010.10.18)
(31)優先権主張番号　61/029,278
(32)優先日　平成20年2月15日 (2008.2.15)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/029,277
(32)優先日　平成20年2月15日 (2008.2.15)
(33)優先権主張国　米国 (US)

(73)特許権者　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100103034
弁理士　野河　信久
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】分配システム中の非リアルタイムコンテンツの条件付きアクセスのための方法および装置

(57)【特許請求の範囲】
【請求項１】
分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを分配するための機械により実現される方法において、
プロセッサにより、制御ワードで前記ＮＲＴコンテンツを暗号化して、暗号化ＮＲＴコンテンツを発生させることと、
１つ以上の受給権制御メッセージ（ＥＣＭ）発生器に前記制御ワードを提供することと、
前記１つ以上のＥＣＭ発生器から１つ以上のＥＣＭをそれぞれ受け取ることと、
前記分配ネットワークを通した送信のために、前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとをファイルフォーマットにエンコードすることとを含み、
前記１つ以上のＥＣＭ発生器は、第１のロングタームキーを使用して前記制御ワードを暗号化して第１のＥＣＭを発生させ、第１の条件付きアクセスシステムに関係付けられている第１のＥＣＭ発生器と、第２のロングタームキーを使用して前記制御ワードを暗号化して第２のＥＣＭを発生させ、前記第１の条件付きアクセスシステムとは異なる第２の条件付きアクセスシステムに関係付けられている第２のＥＣＭ発生器とを含み、前記第１のロングタームキーと前記第２のロングタームキーは異なっており、
前記第１のロングタームキーまたは前記第２のロングタームキーへのアクセスを有するユーザが前記制御ワードを解読できるように、各ＥＣＭは、前記制御ワードの一意的な暗号化を含み、

前記ファイルフォーマットは、前記第１のＥＣＭを発生させた前記第１の条件付きアクセスシステムと、前記第２のＥＣＭを発生させた前記第２の条件付きアクセスシステムとを識別するクリップ定義記録を含む機械により実現される方法。

【請求項２】

制御ワード発生器から前記制御ワードを受け取ることをさらに含む請求項１記載の機械により実現される方法。

【請求項３】

前記ファイルフォーマットは前記第１のＥＣＭおよび前記第２のＥＣＭをさらに含む請求項１記載の機械により実現される方法。

【請求項４】

前記クリップ定義記録は、前記暗号化ＮＲＴコンテンツをさらに識別する請求項３記載の機械により実現される方法。

【請求項５】

装置において、

分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを分配するように構成されているプロセッサを具備し、

前記プロセッサは、

複数の受給権制御メッセージ（ＥＣＭ）発生器に制御ワードを提供して、前記複数のＥＣＭ発生器のそれぞれから１つ以上のＥＣＭをそれぞれ受け取るように構成され、少なくとも部分的にハードウェア中で実現される同期器と、

前記制御ワードで前記ＮＲＴコンテンツを暗号化し、暗号化ＮＲＴコンテンツを発生させて、前記分配ネットワークを通した送信のために、前記暗号化ＮＲＴコンテンツとＥＣＭとを提供するように構成されている管理モジュールとを備え、

前記複数のＥＣＭ発生器のそれぞれは異なる条件付きアクセスシステムに関係付けられており、

各条件付きアクセスシステムは、異なるロングタームキーを使用して前記制御ワードを暗号化して前記１つ以上のＥＣＭを発生させ、

前記ロングタームキーのいずれかへのアクセスを有するユーザが前記制御ワードを解読できるように、各ＥＣＭは、前記制御ワードに対する別個の条件付きアクセスを提供するための、前記制御ワードの一意的な暗号化を含み、

前記管理モジュールは、前記暗号化ＮＲＴコンテンツと前記ＥＣＭとをファイルフォーマットにエンコードするように構成されており、

前記ファイルフォーマットは、前記ＥＣＭを発生させた前記複数のＥＣＭ発生器のそれぞれに関係付けられている、前記異なる条件付きアクセスシステムを識別するクリップ定義記録を含む装置。

【請求項６】

前記同期器は制御ワード発生器から前記制御ワードを取得するように構成されている請求項５記載の装置。

【請求項７】

前記クリップ定義記録は、前記暗号化ＮＲＴコンテンツを識別し、前記ＥＣＭを含む請求項５記載の装置。

【請求項８】

分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを分配するように構成されている装置において、

前記装置は、少なくとも１つのプロセッサを具備し、

前記少なくとも１つのプロセッサは、１つ以上のモジュールを備え、

前記１つ以上のモジュールは、

制御ワードで前記ＮＲＴコンテンツを暗号化して、暗号化ＮＲＴコンテンツを発生させる手段と、

複数の受給権制御メッセージ（ＥＣＭ）発生器に前記制御ワードを提供する手段と、

１つ以上のＥＣＭ発生器から１つ以上のＥＣＭをそれぞれ受け取る手段と、
前記分配ネットワークを通した送信のために、前記暗号化ＮＲＴコンテンツとＥＣＭとを提供する手段と、
前記暗号化ＮＲＴコンテンツと前記ＥＣＭとをファイルフォーマットにエンコードする手段とを含み、
前記複数のＥＣＭ発生器のそれぞれは異なる条件付きアクセスシステムに関係付けられており、各条件付きアクセスシステムは異なるロングタームキーを使用して前記制御ワードを暗号化して１つ以上のＥＣＭを発生させ、
前記ロングタームキーのいずれかへのアクセスを有するユーザが前記制御ワードを解読できるように、各ＥＣＭは、前記制御ワードの一意的な暗号化を含み、
前記ファイルフォーマットは、前記ＥＣＭを発生させた前記複数のＥＣＭ発生器のそれぞれに関係付けられている、前記異なる条件付きアクセスシステムを識別するクリップ定義記録を含む装置。
【請求項９】
制御ワード発生器から前記制御ワードを受け取る手段をさらに含む請求項８記載の装置。
【請求項１０】
前記クリップ定義記録は、前記暗号化ＮＲＴコンテンツを識別し、前記ＥＣＭを含む請求項８記載の装置。
【請求項１１】
プロセッサにより実行されるときに、分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを分配するための方法を前記プロセッサが実行できるようにする命令を具現化する機械読取可能記憶媒体において、
前記方法は、
１つ以上の受給権制御メッセージ（ＥＣＭ）発生器に制御ワードを提供することと、
前記１つ以上のＥＣＭ発生器から１つ以上のＥＣＭをそれぞれ受け取ることと、
前記制御ワードで前記ＮＲＴコンテンツを暗号化して、暗号化ＮＲＴコンテンツを発生させることと、
前記分配ネットワークを通した送信のために、前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとをファイルフォーマットにエンコードすることと、
前記分配ネットワークを通した送信のために、前記ファイルを提供することとを含み、
前記１つ以上のＥＣＭ発生器は、第１のロングタームキーを使用して前記制御ワードを暗号化して第１のＥＣＭを発生させ、第１の条件付きアクセスシステムに関係付けられている第１のＥＣＭ発生器と、第２のロングタームキーを使用して前記制御ワードを暗号化して第２のＥＣＭを発生させ、前記第１の条件付きアクセスシステムとは異なる第２の条件付きアクセスシステムに関係付けられている第２のＥＣＭ発生器とを含み、前記第１のロングタームキーと前記第２のロングタームキーは異なっており、
前記第１のロングタームキーまたは前記第２のロングタームキーへのアクセスを有するユーザが前記制御ワードを解読できるように、各ＥＣＭは、前記制御ワードの一意的な暗号化を含み、
前記ファイルフォーマットは、前記第１のＥＣＭを発生させた前記第１の条件付きアクセスシステムと、前記第２のＥＣＭを発生させた前記第２の条件付きアクセスシステムとを識別するクリップ定義記録を含む機械読取可能記憶媒体。
【請求項１２】
分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを分配するように構成されているサーバにおいて、
ネットワークインターフェースと、
前記ネットワークインターフェースと通信するように構成されているプロセッサとを具備し、
前記プロセッサは、

複数の受給権制御メッセージ（ＥＣＭ）発生器に制御ワードを提供して、前記複数のＥＣＭ発生器のそれぞれから１つ以上のＥＣＭをそれぞれ受け取るように構成され、少なくとも部分的にハードウェア中で実現される同期器と、

前記制御ワードで前記ＮＲＴコンテンツを暗号化し、暗号化ＮＲＴコンテンツを発生させて、前記分配ネットワークを通した送信のために、前記ネットワークインターフェースを通して、前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとを提供するように構成されている管理モジュールとを備え、

前記複数のＥＣＭ発生器のそれぞれは異なる条件付きアクセスシステムに関係付けられており、

各条件付きアクセスシステムは、異なるロングタームキーを使用して前記制御ワードを暗号化して１つ以上のＥＣＭを発生させ、

前記ロングタームキーのいずれかへのアクセスを有するユーザが前記制御ワードを解読できるように、各ＥＣＭは、前記制御ワードの一意的な暗号化を含み、

前記管理モジュールは、前記暗号化ＮＲＴコンテンツとＥＣＭとをファイルフォーマットにエンコードするように構成されており、

前記ファイルフォーマットは、前記ＥＣＭを発生させた前記複数のＥＣＭ発生器のそれぞれに関係付けられている、前記異なる条件付きアクセスシステムを識別するクリップ定義記録を含むサーバ。

【請求項１３】

分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを受信するための機械により実現される方法において、

ファイル中の、制御ワードで暗号化されている暗号化ＮＲＴコンテンツと１つ以上の受給権制御メッセージ（ＥＣＭ）とを受信することと、

プロセッサにより、第１のロングタームキーまたは第２のロングタームキーを使用して、選択されたＥＣＭを解読して、前記制御ワードを取得することと、

前記暗号化ＮＲＴコンテンツを解読して、解読ＮＲＴコンテンツを取得することとを含み、

前記１つ以上のＥＣＭは、第１の条件付きアクセスシステムにより前記第１のロングタームキーを使用して暗号化された前記制御ワードを有する第１のＥＣＭと、前記第１の条件付きアクセスシステムとは異なる第２の条件付きアクセスシステムにより前記第２のロングタームキーを使用して暗号化された前記制御ワードを有する第２のＥＣＭとを含み、前記第１のロングタームキーと前記第２のロングタームキーは異なっており、

前記ファイルのファイルフォーマットは、前記第１のＥＣＭを発生させた前記第１の条件付きアクセスシステムと、前記第２のＥＣＭを発生させた前記第２の条件付きアクセスシステムとを識別するクリップ定義記録を含む機械により実現される方法。

【請求項１４】

前記第１のロングタームキーまたは第２のロングタームキーを含む受給権管理メッセージ（ＥＭＭ）を受信することをさらに含む請求項１３記載の機械により実現される方法。

【請求項１５】

前記ファイルの前記ファイルフォーマットは前記第１のＥＣＭおよび前記第２のＥＣＭをさらに含む請求項１３記載の機械により実現される方法。

【請求項１６】

前記クリップ定義記録は、前記暗号化ＮＲＴコンテンツをさらに識別する請求項１５記載の機械により実現される方法。

【請求項１７】

装置において、

分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを受信するプロセッサを具備し、

前記プロセッサは、

制御ワードで暗号化されている暗号化ＮＲＴコンテンツを受信し、複数の受給権制御メ

ッセージ（ＥＣＭ）を受信するように構成され、少なくとも部分的にハードウェア中で実現される処理論理と、
異なるロングタームキーのうちの１つを使用して、前記複数のＥＣＭのうちの選択されたＥＣＭを解読して、前記制御ワードを取得するように構成されているキー獲得論理と、
前記暗号化ＮＲＴコンテンツを解読して、解読ＮＲＴコンテンツを取得するように構成されている解読論理とを備え、
前記複数のＥＣＭのそれぞれは異なる条件付きアクセスシステムにより前記異なるロングタームキーを使用して暗号化された前記制御ワードを有し、
前記処理論理は、ファイル中の、前記暗号化ＮＲＴコンテンツと前記複数のＥＣＭとを受信するように構成されており、
前記ファイルのファイルフォーマットは、前記複数のＥＣＭのそれぞれに関係付けられている前記異なる条件付きアクセスシステムを識別するクリップ定義記録を含む装置。
【請求項１８】
前記処理論理は、前記ロングタームキーのうちの１つを含む受給権管理メッセージ（ＥＭＭ）を受信するように構成されている請求項１７記載の装置。
【請求項１９】
前記クリップ定義記録は、前記暗号化ＮＲＴコンテンツを識別し、前記複数のＥＣＭを含む請求項１７記載の装置。
【請求項２０】
分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを受信する装置において、
前記装置は、少なくとも１つのプロセッサを具備し、
前記少なくとも１つのプロセッサは、１つ以上のモジュールを備え、
前記１つ以上のモジュールは、
ファイル中の、制御ワードで暗号化されている暗号化ＮＲＴコンテンツと１つ以上の受給権制御メッセージ（ＥＣＭ）とを受信する手段と、
第１のロングタームキーまたは第２のロングタームキーを使用して、選択されたＥＣＭを解読して、前記制御ワードを取得する手段と、
前記暗号化ＮＲＴコンテンツを解読して、解読ＮＲＴコンテンツを取得する手段とを含み、
前記１つ以上のＥＣＭは、第１の条件付きアクセスシステムにより前記第１のロングタームキーを使用して暗号化された前記制御ワードを有する第１のＥＣＭと、前記第１の条件付きアクセスシステムとは異なる第２の条件付きアクセスシステムにより前記第２のロングタームキーを使用して暗号化された前記制御ワードを有する第２のＥＣＭとを含み、
前記第１のロングタームキーと前記第２のロングタームキーは異なっており、
前記ファイルのファイルフォーマットは、前記第１のＥＣＭに関係付けられている前記第１の条件付きアクセスシステムと、前記第２のＥＣＭに関係付けられている前記第２の条件付きアクセスシステムとを識別するクリップ定義記録を含む装置。
【請求項２１】
前記第１のロングタームキーまたは第２のロングタームキーを含む受給権管理メッセージ（ＥＭＭ）を受信する手段をさらに含む請求項２０記載の装置。
【請求項２２】
前記ファイルの前記ファイルフォーマットは前記第１のＥＣＭおよび前記第２のＥＣＭをさらに含む請求項２０記載の装置。
【請求項２３】
前記クリップ定義記録は、前記暗号化ＮＲＴコンテンツをさらに識別する請求項２２記載の装置。
【請求項２４】
プロセッサにより実行されるときに、分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを受信するための方法を前記プロセッサが実行できるようにする命令を

具現化する機械読取可能記憶媒体において、
前記方法は、
制御ワードで暗号化されている暗号化ＮＲＴコンテンツを受信することと、
複数の受給権制御メッセージ（ＥＣＭ）を受信することと、
異なるロングタームキーのうちの１つを使用して、前記複数のＥＣＭのうちの選択されたＥＣＭを解読して、前記制御ワードを取得することと、
前記暗号化ＮＲＴコンテンツを解読して、解読ＮＲＴコンテンツを取得することとを含み、
前記複数のＥＣＭのそれぞれは、異なる条件付きアクセスシステムにより前記異なるロングタームキーを使用して暗号化された前記制御ワードを有し、
前記暗号化ＮＲＴコンテンツと前記複数のＥＣＭとがファイル中で受信され、
前記ファイルのファイルフォーマットは、前記複数のＥＣＭのそれぞれに関係付けられている、前記異なる条件付きアクセスシステムを識別するクリップ定義記録を含む機械読取可能記憶媒体。
【請求項２５】
分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを受信するように構成されているデバイスにおいて、
アンテナと、
前記アンテナを使用して、ファイル中の、制御ワードで暗号化されている暗号化ＮＲＴコンテンツと１つ以上の受給権制御メッセージ（ＥＣＭ）とを受信するように構成されている処理論理と、
第１のロングタームキーまたは第２のロングタームキーを使用して、選択されたＥＣＭを解読して、前記制御ワードを取得するように構成されているキー獲得論理と、
前記暗号化ＮＲＴコンテンツを解読して、解読ＮＲＴコンテンツを取得するように構成されている解読論理とを具備し、
前記１つ以上のＥＣＭは、第１の条件付きアクセスシステムにより前記第１のロングタームキーを使用して暗号化された前記制御ワードを有する第１のＥＣＭと、前記第１の条件付きアクセスシステムとは異なる第２の条件付きアクセスシステムにより前記第２のロングタームキーを使用して暗号化された前記制御ワードを有する第２のＥＣＭとを含み、
前記第１のロングタームキーと前記第２のロングタームキーは異なっており、
前記ファイルのファイルフォーマットは、前記第１のＥＣＭに関係付けられている前記第１の条件付きアクセスシステムと、前記第２のＥＣＭに関係付けられている前記第２の条件付きアクセスシステムとを識別するクリップ定義記録を含むデバイス。
【発明の詳細な説明】
【米国特許法第１１９条の優先権主張】
【０００１】
本特許出願は、“フォワードリンク専用フレームワークのための方法および装置”と題する２００８年２月１５日に出願され、本発明の譲受人に譲渡され、ここでの参照によりここに明確に組み込まれている仮出願第６１／０２９，２７８号に対して優先権を主張する。
【０００２】
本特許出願は、“フォワードリンク専用非リアルタイムファイルフォーマットのための方法および装置”と題する２００８年２月１５日に出願され、本発明の譲受人に譲渡され、ここでの参照によりここに明確に組み込まれている仮出願第６１／０２９，２７７号に対して優先権を主張する。
【背景】
【０００３】
ワイヤレス通信ネットワークのようなデータネットワークは、単一端末に対してカスタマイズされたサービスと、非常に多くの端末に対して提供されるサービスとの間でトレードオフしなければならない。例えば、非常に多くのリソース制限ポータブルデバイス（申

込者）に対する非リアルタイム（ＮＲＴ）コンテンツの分配は、複雑な問題である。それゆえ、早く効率的なやり方で、ならびに、帯域幅利用および端末電力効率を増加させるような方法で、ＮＲＴコンテンツおよび／または他のネットワークサービスを分配するための方法を有することが、ネットワーク管理者や、コンテンツ小売業者や、サービスプロバイダにとって非常に重要である。

【０００４】

現在のコンテンツ配信／分配システムにおいて、フォワグランドおよびバックグランドサービスは、送信フレーム中にパックされて、ネットワーク上のデバイスに配信される。例えば、通信ネットワークは直交周波数分割多重（ＯＦＤＭ）を利用して、ネットワークサーバから１つ以上の移動体デバイスにリアルタイムサービスをブロードキャストしてもよい。例えば、フォワグランドサービスは、一般的に受信したときに処理する必要があるリアルタイムストリーミングのビデオおよび／またはオーディオを含む。バックグランドサービスは、非リアルタイム広告や、プレゼンテーションや、ファイルや、他のデータを含む。

【０００５】

現在のワイヤレス分配システムでは、コンテンツに対する条件付きアクセス（ＣＡ）を提供することが可能であることがますます重要になってきている。条件付きアクセスとは、（第三者コンテンツベンダーのような）１つ以上のネットワークエンティティが、選択されたコンテンツに対するユーザアクセスを制御して、認証されていない使用を防ぐことが可能であることを意味する。例えば、旧来システムは現在、ニュースや、天気や、スポーツなどのような、リアルタイムコンテンツに対する条件付きアクセスを提供するように動作する。しかしながら、ＮＲＴコンテンツに対するアクセスを制御するための条件付きアクセスシステムは利用可能ではない。

【０００６】

それゆえ、分配ネットワークを通して、ＮＲＴコンテンツに対する条件付きアクセスを提供するように動作するシステムを有することが望ましい。

【図面の簡単な説明】

【０００７】

ここで説明した上述の側面は、添付している図面に関連して説明がなされるとき、下記の説明への参照により、さらに容易に明白になるだろう。

【図１】図１は、ＮＲＴコンテンツ分配システムの側面を図示している通信システムを示している。

【図２】図２は、従来のリアルタイム条件付きアクセスコンテンツ分配システムを示している。

【図３】図３は、例示的なＮＲＴコンテンツ分配システムを示している。

【図４】図４は、別の例示的なＮＲＴコンテンツ分配システムを示している。

【図５】図５は、さらに別の例示的なＮＲＴコンテンツ分配システムを示している。

【図６】図６は、ＮＲＴコンテンツ分配システムの側面における使用のための例示的なプロトコルスタックを示している。

【図７】図７は、ＮＲＴコンテンツ分配システムの側面における使用のための一般的なＮＲＴファイルフォーマットを図示している。

【図８】図８は、ＮＲＴコンテンツ分配システムの側面における使用のための例示的なクリップ定義記録を示している。

【図９Ａ】図９Ａは、ＮＲＴコンテンツ分配システムの側面における使用のための、図８のクリップ定義記録の一部である、例示的な条件付きアクセスパラメータを示している。

【図９Ｂ】図９Ｂは、ＮＲＴコンテンツ分配システムの側面における使用のための、図８のクリップ定義記録の一部である、コンテンツ情報パラメータを示している。

【図１０】図１０は、ＮＲＴコンテンツ分配システムの側面における使用のための、ＮＲＴコンテンツの条件付きアクセスを提供する例示的な方法を示している。

【図１１】図１１は、ＮＲＴコンテンツ分配システムの側面における使用のための、ＮＲ

Ｔコンテンツの条件付きアクセスを提供する別の例示的な方法を示している。
【図１２】図１２は、ＮＲＴコンテンツ分配システムの側面における使用のための例示的なＮＲＴコンテンツ受信モジュールを示している。
【図１３】図１３は、ＮＲＴコンテンツ分配システムの側面における使用のための、ＮＲＴコンテンツを受信するための例示的な方法を示している。
【図１４】図１４は、ＮＲＴコンテンツ分配システムの側面における使用のための例示的なＮＲＴコンテンツ配信コンポーネントを示している。
【図１５】図１５は、ＮＲＴコンテンツ分配システムの側面における使用のための、例示的なＮＲＴコンテンツ受信モジュールを示している。
【説明】
【０００８】
１つ以上の側面において、分配ネットワークを通して送信される非リアルタイムコンテンツの効率的な条件付きアクセスを提供するように動作する（方法および装置を具備している）ＮＲＴコンテンツ分配システムを説明する。１つの側面では、システムは１つ以上の第三者条件付きアクセスシステムにインターフェースし、これらのアクセスシステムがＮＲＴコンテンツに対するユーザアクセスを制御できるようにする。
【０００９】
システムは、ワイヤレスネットワーク環境における使用に適しているが、任意のタイプのネットワーク環境で使用されてもよい。任意のタイプのネットワーク環境は、これらには制限されないが、通信ネットワークや、インターネットのような公共ネットワークや、バーチャルプライベートネットワーク（ＶＰＮ）のようなプライベートネットワークや、ローカルエリアネットワークや、ワイドエリアネットワークや、長距離ネットワークや、他の任意のタイプのデータネットワークを含む。
【００１０】
図１は、ＮＲＴコンテンツ分配システムの側面を図示している通信システム１００を示している。通信システム１００は、サーバ１０２と、分配ネットワーク１０４と、デバイス１０６とを具備している。１つの側面では、分配ネットワーク１０４と通信しているデバイスに配信されるＮＲＴコンテンツに対する条件付きアクセスをサーバ１０２が提供できるように、ＮＲＴコンテンツ分配システムは動作する。ＮＲＴコンテンツは、媒体クリップ、プレゼンテーション、データ、メタデータ、アプリケーション、または、他の任意のタイプの非リアルタイムコンテンツを含んでいる。
【００１１】
サーバ１０２は、任意のタイプの通信リンク１１６を使用してネットワーク１０４と通信するように動作する。ネットワーク１０４は、フォワードリンク専用ブロードキャストネットワークのような、任意のタイプのワイヤードおよび／またはワイヤレス分配ネットワークであってもよい。１つの側面では、ネットワーク１０４は、デバイス１０６が動作しているローカルエリアにサービスを提供する。例えば、ネットワーク１０４は、ローカル領域またはローカル地域、都市、あるいは国に情報を分配するように動作してもよい。ほんのいくつかのデバイス１０６のみが示されているが、システムは、任意の数および／またはタイプのデバイスとの使用に適していることに留意すべきである。
【００１２】
サーバ１０２はＮＲＴ配信コンポーネント１０８を備え、ＮＲＴ配信コンポーネント１０８は、ネットワーク１０４を通しての分配のために、ＮＲＴコンテンツを受け取るように動作するＮＲＴコンテンツ配信モジュール１１２を備えている。ＮＲＴコンテンツ配信モジュール１１２は、第三者条件付きアクセスシステム１１４にインターフェースし、１つ以上の第三者条件付きアクセスシステムによりＮＲＴコンテンツに対するアクセスが制御できるようにする。例えば、ＮＲＴコンテンツは制御ワードで暗号化されていて、各条件付きアクセスシステム１１４は、特定の条件付きアクセスシステムに関係するロングタームキーで制御ワードを暗号化するように動作する。これにより、暗号化制御ワードを含む受給権制御メッセージ（ＥＣＭ）を発生させる。各条件付きアクセスシステムは受給権

管理メッセージ（ＥＭＭ）も発生させる。受給権管理メッセージ（ＥＭＭ）は、ロングタームキーを含んでいて、認証されたユーザ（すなわち、各ユーザがＮＲＴコンテンツを受信する申し込みをするとき）に分配される。したがって、各条件付きアクセスシステムは、その申込者に対するＮＲＴコンテンツのアクセスを制限することが可能である。

【００１３】

１つ以上の側面では、ＮＲＴ配信コンポーネント１０８は、下記の動作のうちの１つ以上のものを実行するように動作する。

１．分配すべき非リアルタイムコンテンツを取得

２．ＮＲＴコンテンツを暗号化するための制御ワードを取得

３．制御ワードを使用してＮＲＴコンテンツを暗号化して、暗号化ＮＲＴコンテンツを発生

４．１つ以上の第三者条件付きアクセスシステムにインターフェースして、ＥＣＭおよびＥＭＭを取得し、ＥＣＭおよびＥＭＭは、各条件付きアクセスシステムが暗号化コンテンツに対するアクセスを制御できるようにする

５．分配ネットワークを通して、暗号化コンテンツと、ＥＣＭと、ＥＭＭとを送信

【００１４】

送信された暗号化ＮＲＴコンテンツと、ＥＣＭと、ＥＭＭは、デバイス１０６により受信可能である。本説明の目的のために、デバイスの動作をデバイス１１０を参照して説明する。

【００１５】

デバイス１１０は、ＮＲＴコンテンツ受信モジュール１１６を備える。このモジュールは、暗号化コンテンツと、ＥＣＭと、ＥＭＭとを受信するように動作する。デバイス１１０が特定のＮＲＴコンテンツにアクセスすることについて認証されている場合、デバイス１１０は、受信したＥＭＭを使用してロングタームキーを取得し、このロングタームキーにより、ＮＲＴコンテンツに関係する適切なＥＣＭを解読する。ＥＣＭは制御ワードを含み、制御ワードは、記憶および／またはレンダリングのために、暗号化ＮＲＴコンテンツを解読するのに使用できる。

【００１６】

それゆえ、ＮＲＴコンテンツ分配システムの側面は、分配ネットワークを通して送信されたＮＲＴコンテンツに対する効率的な条件付きアクセスを提供するように動作する。通信システム１００はただ１つだけのインプリメンテーションを図示していて、側面の範囲内で、他のインプリメンテーションも可能であることに留意すべきである。

【００１７】

図２は、従来のリアルタイム条件付きアクセスコンテンツ分配システム２００を示している。システム２００は、リアルタイムコンテンツ準備モジュール２０２と、ｓｉｍｕｌ－ｃｒｙｐｔ同期器（ＳＣＳ）２０４と、１つ以上の第三者条件付きアクセスモジュール２０６とを具備している。例えば、システム２００は、分配ネットワークを通してリアルタイムコンテンツをスケジューリングおよび配信するように動作可能である。

【００１８】

リアルタイムコンテンツ準備モジュール２０２は、第三者モジュール２０６における準備論理（ＰＬ）２０８と通信して、リアルタイムコンテンツの配信を準備およびスケジューリングするように動作する。いったんコンテンツ準備が完了すると、リアルタイムコンテンツ準備モジュール２０２はｓｉｍｕｌ－ｃｒｙｐｔ同期器２０４と通信し、リアルタイムコンテンツを暗号化するための制御ワード（ショートタームキー）を取得する。ｓｉｍｕｌ－ｃｒｙｐｔ同期器２０４は、制御ワードを発生させるように動作する制御ワード発生器（ＣＷＧ）２１０を備えている。制御ワードは第三者モジュール２０６のＥＣＭ発生器２１２に渡される。応答として、ＥＣＭ発生器２１２は、それぞれの第三者モジュール２０６により提供されたロングタームキーにより暗号化されている、制御ワードを含むＥＣＭを発生させる。ｓｉｍｕｌ－ｃｒｙｐｔ同期器２０４は、その後、制御ワードと、対応するＥＣＭとを、分配のためにリアルタイム転送システム（ＲＴＳ）に渡す。

【００１９】
加えて、第三者モジュール２０６はＥＭＭ発生器２１４を備えている。ＥＭＭ発生器２１４は、対応するＥＣＭを解読して制御ワードを取得するために使用できるロングタームキーを含むＥＭＭを発生させる。ＥＭＭはまた、分配のためにＲＴＳに渡される。
【００２０】
動作の間に、ＲＴＳは、制御ワードでリアルタイムコンテンツを暗号化し、暗号化コンテンツおよびＥＣＭを、分配ネットワークの特定のフローおよびチャネルを通して送信するように動作する。ＥＭＭは、分配ネットワークを通して、異なるフローまたはチャネル上で送信される。
【００２１】
認証されていないアクセスを防ぐために、制御ワードは定期的にｓｉｍｕｌ－ｃｒｙｐｔ同期器２０４により変更される。例えば、制御ワードは１０秒毎に変更されてもよく、それにより、現在の制御ワードが危険にさらされた場合、コンテンツの１０秒分のみが、認証されていないユーザによりアクセスできる。
【００２２】
時間ライン２１６は、ｓｉｍｕｌ－ｃｒｙｐｔ同期器２０４によりどのように制御ワードを定期的に変更するかを図示している。暗号化期間２１８は、認証されていないユーザによるコンテンツアクセスを制限するように、どのくらい頻繁に制御ワードを変更するかを決定するために使用する。各暗号化期間２１８の終わりにおいて、ｓｉｍｕｌ－ｃｒｙｐｔ同期器２０４はＣＷＧ２１０を制御して、新たな制御ワードを発生させる。新たな制御ワードは、第三者条件付きアクセスモジュール２０６に渡される。新たなＥＣＭおよびＥＭＭが発生されて、リアルタイム転送システムに渡される。
【００２３】
図３は、例示的なＮＲＴコンテンツ分配システム３００を示している。例えば、システム３００は、図１中に示されているＮＲＴコンテンツ配信コンポーネント１０８としての使用に適している。
【００２４】
システム３００は、ＮＲＴコンテンツプロバイダ３０２と、ＮＲＴ暗号化モジュール３０４と、１つ以上の第三者ＥＣＭ発生器３０６と、ネットワークサービングノード３０８と、ＣＷＧモジュール３１０とを具備している。図３はまた、ＮＲＴコンテンツ分配システム３００のさまざまなコンポーネント間に存在するインターフェースを示している。各インターフェースを丸数字により識別している。
【００２５】
ＮＲＴコンテンツプロバイダ３０２は、インターフェース１を使用して、ＮＲＴコンテンツをＮＲＴ暗号化モジュール３０４に提供するように動作する。インターフェース１は、コンテンツ獲得インターフェースであり、ＮＲＴ暗号化モジュール３０４が、分配ネットワークを通しての分配のために、ＮＲＴコンテンツを獲得できるようにする。
【００２６】
ＮＲＴ暗号化モジュール３０４は、インターフェース２を使用してＣＷＧモジュール３１０と通信するように動作する。ＣＷＧモジュール３１０は、ＮＲＴコンテンツを暗号化するために使用される制御ワードを発生させるように動作する。インターフェース２は、制御ワード獲得インターフェースであり、制御ワード獲得インターフェースは、ＮＲＴ暗号化モジュール３０４が、発生された制御ワードを獲得できるようにする。
【００２７】
ＮＲＴ暗号化モジュール３０４は、インターフェース３を使用して第三者ＥＣＭ発生器３０６と通信するように動作する。第三者ＥＣＭ発生器３０６は、ＮＲＴ暗号化モジュール３０４から制御ワードを受け取って、制御ワードをロングタームキーで暗号化し、暗号化制御ワードを含むＥＣＭをそれぞれ発生させるように動作する。インターフェース３は、暗号化からＥＣＭ発生器へのインターフェースであり、暗号化からＥＣＭ発生器へのインターフェースは、ＮＲＴ暗号化モジュール３０４が１つ以上の第三者ベンダーに関係す

るＥＣＭを獲得できるようにする。
【００２８】
ＮＲＴ暗号化モジュール３０４はまた、制御ワードでＮＲＴコンテンツを暗号化して、暗号化ＮＲＴコンテンツを発生させるように動作する。暗号化ＮＲＴコンテンツおよび関係するＥＣＭは、インターフェース４を使用して、ネットワークサービングノード３０８に渡される。ネットワークサービングノード３０８は分配ネットワークへのアクセスを提供し、それにより、ＮＲＴ暗号化コンテンツを、分配ネットワークと通信しているデバイスに分配できる。インターフェース４は、暗号化コンテンツ配信インターフェースであり、暗号化コンテンツ配信インターフェースは、暗号化モジュール３０４が、暗号化ＮＲＴコンテンツおよびＥＣＭをネットワークサービングノード３０８に配信できるようにする。
【００２９】
したがって、動作の間に、ＮＲＴコンテンツ分配システム３００は下記の機能のうちの１つ以上のものを提供するように動作する。
１．分配ネットワークを通しての分配のために、ＮＲＴコンテンツを獲得
２．コンテンツを暗号化するために使用される制御ワードを獲得
３．制御ワードでＮＲＴコンテンツを暗号化
４．１つ以上の第三者ＥＣＭ発生器に関係するＥＣＭを獲得
５．分配ネットワークを通しての分配のために、暗号化ＮＲＴコンテンツとＥＣＭとをネットワークサービングノードに配信
【００３０】
図４は、別の例示的なＮＲＴコンテンツ分配システム４００を示している。例えば、システム４００は、図１中に示しているＮＲＴコンテンツ配信コンポーネント１０８としての使用に適している。
【００３１】
システム４００は、ＮＲＴコンテンツプロバイダ４０２と、ＮＲＴ処理モジュール４０４と、準備モジュール４０６と、ｓｉｍｕｌ－ｃｒｙｐｔ同期器４０８と、１つ以上の第三者ＥＣＭ発生器４１０と、ネットワークサービングノード４１２とを具備している。図４はまた、ＮＲＴコンテンツ分配システム４００のさまざまなコンポーネントの間に存在するインターフェースを示している。各インターフェースを丸数字により識別している。
【００３２】
ＮＲＴコンテンツプロバイダ４０２は、インターフェース１を使用して、ＮＲＴコンテンツをＮＲＴ処理モジュール４０４に提供するように動作する。インターフェース１は、コンテンツ獲得インターフェースであり、ＮＲＴ処理モジュール４０４が、分配ネットワークを通しての分配のために、ＮＲＴコンテンツを獲得できるようにする。
【００３３】
ＮＲＴ処理モジュール４０４は、インターフェース２を使用して準備モジュール４０６と通信するように動作する。準備モジュール４０６は、分配ネットワークを通したＮＲＴコンテンツの分配を準備およびスケジュールするように動作する。インターフェース２は、ＮＲＴコンテンツ通知インターフェースであり、ＮＲＴコンテンツ通知インターフェースは、分配ネットワークを通しての分配のためにＮＲＴコンテンツが利用可能であることを準備モジュール４０６に示す。
【００３４】
準備モジュール４０６は、インターフェース３を使用してｓｉｍｕｌ－ｃｒｙｐｔ同期器４０８と通信するように動作する。インターフェース３は、準備から暗号化へのインターフェースを備え、準備から暗号化へのインターフェースは、準備モジュール４０６が、準備や、スケジューリングや、さまざまなアクセス基準をｓｉｍｕｌ－ｃｒｙｐｔ同期器４０８に提供できるようにする。例えば、アクセス基準はＮＲＴコンテンツを識別して、分配ネットワーク上のＮＲＴコンテンツの利用可能性についての情報を提供する。
【００３５】

ｓｉｍｕｌ－ｃｒｙｐｔ同期器４０８は、準備モジュール４０６からアクセス基準を受け取り、制御ワード発生器４１４を制御して、ＮＲＴコンテンツを暗号化する制御ワードを発生させるように動作する。ｓｉｍｕｌ－ｃｒｙｐｔ同期器４０８は、その後、インターフェース４を使用して、発生させた制御ワードを第三者ＥＣＭ発生器４１０に渡す。インターフェース４は、ＳＣＳからＥＣＭ発生器へのインターフェースを構成し、ＳＣＳからＥＣＭ発生器へのインターフェースは、制御ワードをＥＣＭ発生器４１０に渡し、発生させたＥＣＭをＳＣＳ４０８に送り返せるようにする。ＳＣＳ４０８は、その後、制御ワードおよびＥＣＭをＮＲＴ処理モジュール４０４に渡す。

【００３６】

第三者ＥＣＭ発生器４１０は、制御ワードを受け取って、制御ワードをＥＣＭ中に暗号化するように動作する。各ＥＣＭ発生器は、異なるロングタームキーを使用して制御ワードを暗号化してもよい。したがって、ＥＣＭ発生器はＮＲＴコンテンツに対するアクセスを制御でき、これにより、適切なロングタームキーに対するアクセスを有するユーザのみが制御ワードを解読できる。

【００３７】

ＳＣＳ４０８はまた、インターフェース５を使用して、制御ワードおよびＥＣＭをＮＲＴ処理モジュール４０４に渡すように動作する。インターフェース５は、制御ワードおよびＥＣＭ配信インターフェースを構成し、制御ワードおよびＥＣＭ配信インターフェースは、ＮＲＴ処理モジュール４０４が制御ワードおよびＥＣＭを取得できるようにする。ＮＲＴ処理モジュール４０４は、その後、ＮＲＴコンテンツを制御ワードで暗号化して、暗号化ＮＲＴコンテンツを発生させるように動作する。暗号化ＮＲＴコンテンツおよび関係するＥＣＭは、暗号化コンテンツ配信インターフェースを構成するインターフェース６を使用して、サービングノード４１２に渡される。

【００３８】

サービングノード４１２は分配ネットワークに対するアクセスを提供し、これにより、暗号化ＮＲＴコンテンツおよびＥＣＭを、分配ネットワークと通信しているデバイスに分配できる。

【００３９】

したがって、動作の間に、ＮＲＴコンテンツ分配システム４００は、下記の機能のうちの１つ以上のものを提供するように動作する。

１．　分配ネットワークを通しての分配のために、ＮＲＴコンテンツを獲得

２．　ＮＲＴコンテンツに関係する、準備およびスケジューリングを行って、アクセス基準を決定

３．　ＮＲＴコンテンツを暗号化するのに使用される制御ワードを発生

４．　アクセス基準に基づいて、ロングタームキーで制御ワードを暗号化して、ＥＣＭを発生

５．　ＮＲＴコンテンツを制御ワードで暗号化して、暗号化ＮＲＴコンテンツを発生

６．　分配ネットワークを通しての分配のために、暗号化ＮＲＴコンテンツとＥＣＭとをネットワークサービングノードに配信

【００４０】

図５は、別の例示的なＮＲＴコンテンツ分配システム５００を示している。例えば、システム５００は、図１中に示しているＮＲＴコンテンツ配信コンポーネント１０８としての使用に適している。

【００４１】

システム５００は、ＮＲＴコンテンツモジュール５０２と、ＮＲＴファイル管理モジュール５０４と、ＳＣＳ５０６と、１つ以上の第三者ＣＡモジュール５０８と、ネットワークサービングモジュール５１０とを具備している。システム５００はただ１つのインプリメンテーションを図示しており、さまざまな側面の範囲内で、他のインプリメンテーションも可能であることに留意すべきである。

【００４２】

ＮＲＴコンテンツモジュール５０２は、非リアルタイムコンテンツを取得して、このコンテンツをＮＲＴファイル管理モジュール５０４に提供するように動作する、ハードウェア、および／または、ソフトウェアを実行するハードウェアを備えている。ＮＲＴコンテンツモジュール５０２はまた、アクセス制御（ＡＣ）パラメータ（またはアクセス基準）をＮＲＴファイル管理モジュール５０４に提供する。アクセス制御パラメータは、ＮＲＴコンテンツに関係付けられており、下記において論じるように、ＮＲＴコンテンツに対するアクセスを制御するために、第三者ＣＡモジュール５０８により利用される。１つの側面では、ＡＣパラメータはＣＡプロバイダにより使用され、そして、ＥＣＭを発生させるためにＥＣＭ発生器により消費される。１つの例では、ＡＣパラメータは、ＮＲＴコンテンツを識別するか、または、ＮＲＴコンテンツの権利に関係付けられていてもよい。

【００４３】

ＮＲＴファイル管理モジュール５０４は、ＮＲＴコンテンツとＡＣパラメータとを取得するように動作する、ハードウェア、および／または、ソフトウェアを実行するハードウェアを備えている。ＮＲＴファイル管理モジュール５０４はＡＣパラメータをＳＣＳ５０６に渡す。

【００４４】

ＳＣＳ５０６は、ＮＲＴコンテンツを暗号化するために使用される制御ワードを発生させるように動作する、ハードウェア、および／または、ソフトウェアを実行するハードウェアを備えている。例えば、ＳＣＳ５０６は、制御ワードを発生させるように動作する制御ワード発生器５１６を備えている。ＳＣＳ５０６は、発生させた制御ワードと受け取ったＡＣパラメータとを第三者ＣＡモジュール５０８に渡す。各第三者ＣＡモジュール５０８におけるＥＣＭ発生器５１８は、制御ワードおよびＡＣパラメータを受け取り、ＥＣＭメッセージを発生させる。各モジュール５０８からのＥＣＭメッセージはＳＣＳ５０６に送り返される。ＳＣＳ５０６は、制御ワードと受け取ったＥＣＭメッセージとをＮＲＴファイル管理モジュール５０４に渡すように動作する。

【００４５】

各第三者ＣＡモジュール５０８は、ＥＭＭ発生器５２０をさらに備えている。ＥＭＭ発生器５２０は、関係するＥＣＭメッセージを解読するために使用できるロングタームキーを含むＥＭＭを発生させる。発生させたＥＭＭメッセージは、分配ネットワークを通した配信のためにネットワークサービングモジュール５１０に渡される。例えば、ＥＭＭメッセージは、ＩＰデータキャストで分配ネットワークを通して配信されてもよい。１つの側面では、１つのＥＭＭを使用して、多くのユーザをカバーし、帯域幅要件を減少させるグループ化動作が実行される。

【００４６】

ＮＲＴファイル管理モジュール５０４は、発生された制御ワードでＮＲＴコンテンツを暗号化するように動作する。暗号化ＮＲＴコンテンツと、発生されたＥＣＭメッセージは、ネットワークサービングモジュール５１０に出力される。１つの側面では、ＮＲＴファイル管理モジュール５０４は、デジタル著作権管理（ＤＲＭ）モジュール５１２から情報を受け取るように動作する。この情報は、デジタル著作権管理を暗号化ＮＲＴコンテンツに関係付けるためにＮＲＴファイル管理モジュール５０４により使用される。例えば、ＤＲＭモジュール５１２は、優れた粒度制御を提供して、何回プレゼンテーションを見ることができるかを決定する。

【００４７】

加えて、ＮＲＴファイル管理モジュール５０４はフォワードエラー訂正モジュール５１４から情報を受け取るように動作する。この情報は、ＮＲＴコンテンツに対するフォワードエラー訂正を提供するために、ＮＲＴファイル管理モジュール５０４により使用される。ＦＥＣはシステム性能を調整するために使用される。

【００４８】

ネットワークサービングモジュール５１０は、ＣＰＵと、プロセッサと、ゲートアレイと、ハードウェア論理と、メモリエレメントと、仮想機械、および／または、ソフトウェ

アを実行するハードウェアのうちの少なくとも１つを備えている。ネットワークサービングモジュール５１０は、暗号化ＮＲＴコンテンツと、発生されたＥＣＭと、発生されたＥＭＭとを出力するように動作する。

【００４９】

動作の間に、選択された制御ワードでＮＲＴコンテンツを暗号化し、１つ以上の条件付きアクセスベンダーに関係している１つ以上のロングタームキーを使用して制御ワードを暗号化することにより、システムは、ＮＲＴコンテンツの条件付きアクセスを提供する。加えて、ＡＣパラメータはＮＲＴコンテンツに関係付けられて、条件付きアクセスベンダーがＮＲＴコンテンツに対するアクセスをさらに制御できるようにする。ファイル管理モジュールは、発生された制御ワードでＮＲＴコンテンツを暗号化するように動作する。暗号化ＮＲＴコンテンツと、ＥＣＭと、ＥＭＭは、その後分配ネットワークを通して分配される。

【００５０】

それゆえ、ＮＲＴコンテンツ分配システム５００は、さまざまな側面で、下記の機能のうちの１つ以上のものを実行するように動作する。

１．分配ネットワークを通しての分配のために、ＮＲＴコンテンツを獲得

２．ＮＲＴコンテンツを暗号化する制御ワードを発生

３．アクセス基準に基づいて、ロングタームキーで制御ワードを暗号化して、１つ以上のＥＣＭを発生

４．各条件付きアクセスシステムに関係しているロングタームキーを含むＥＭＭを発生

５．制御ワードでＮＲＴコンテンツを暗号化して、暗号化ＮＲＴコンテンツを発生

６．分配ネットワークを通しての分配のために、暗号化ＮＲＴコンテンツと、ＥＣＭと、ＥＭＭとを、ネットワークサービングノードに配信

【００５１】

１つの側面では、ＮＲＴコンテンツ分配システムは、機械読取可能媒体上に記憶または具現化される、１つ以上のプログラム命令（“命令”）またはコードの組（“コード”）を具備している。コードが、少なくとも１つのプロセッサにより実行されるとき、例えば、ＮＲＴファイル管理モジュール５０４におけるプロセッサにより実行されるとき、ここで述べた機能を提供する。例えば、ＮＲＴファイル管理モジュール５０４にインターフェースする、フロッピー（登録商標）ディスクや、ＣＤＲＯＭや、メモリカードや、フラッシュメモリデバイスや、ＲＡＭや、ＲＯＭや、他の何らかのタイプのメモリデバイスまたは機械読取可能媒体のような、機械読取可能媒体から、コードはＮＲＴファイル管理モジュール５０４中にロードされてもよい。別の側面では、コードは、外部のデバイスまたはネットワークリソースから、ＮＲＴファイル管理モジュール５０４中にダウンロードされてもよい。コードは、実行されるとき、ここに説明したようなＮＲＴコンテンツ分配システムの側面を提供する。

【００５２】

図６は、ＮＲＴコンテンツ分配システムの側面における使用のための例示的なプロトコルスタック６００を示している。例えば、プロトコルスタック６００は、ＮＲＴファイル管理モジュール５０４により実現されてもよい。

【００５３】

プロトコルスタック６００は、ファイルベースのアプリケーション６０２と、非リアルタイムサービス６０４と、ファイル配信レイヤ６０６と、伝送レイヤ６０８と、エアインターフェースレイヤ６１０とを具備している。

【００５４】

ファイル配信レイヤ６０６は、ＮＲＴファイルをデバイスに配信するように動作する。ファイル配信レイヤ６０６は伝送レイヤ６０８のサービスを使用する。ファイルは、これらが効率的かつ信頼性高くネットワークからデバイスに確実に配信されるようにメッセージコーディングを受ける。ファイル配信レイヤ６０６に属する、プロトコルおよびメッセ

ージのさらに詳細な説明を下記において提供する。

【００５５】

〔非リアルタイムファイルフォーマット〕

さまざまな側面では、ＮＲＴコンテンツ分配システムは、デバイスによるその後の消費のためにマルチキャストファイル配信を提供するように動作する。１つのインプリメンテーションでは、ファイル配信レイヤ６０６はＮＲＴファイル伝送メカニズムを提供するように動作する。このメカニズムは任意のフォーマットのファイルを伝送するために使用できる。

【００５６】

ＮＲＴファイル伝送メカニズムは下記の機能を提供するように動作する。

１．１つ以上のプレゼンテーションをカプセル化

２．ネットワークシステム情報（ＳＩ）構造を強化し、それによって豊富な機能サポートを可能にする

３．メタデータは、拡張性のためにＸＭＬベースである

４．条件付きアクセスに対するサポート

【００５７】

図７は、ＮＲＴコンテンツ分配システムの側面における使用のための一般的なＮＲＴファイルフォーマット７００を図示している。ＮＲＴファイルフォーマット７００のコンポーネントを下記の表１中にさらに規定している。暗号化ＮＲＴコンテンツと１つ以上のＥＣＭとをＮＲＴファイルフォーマット７００にエンコードしてもよい。

【表１】

表1

フィールド名	フィールドタイプ
NRT_FILE_DATA	変数
META_DATA_TYPE	UINT(8)
META_DATA_VALUE	変数
TOTAL_META_DATA_LENGTH	UINT(16)
CRC	UINT(16)

【００５８】

ＮＲＴ＿ＦＩＬＥ＿ＤＡＴＡ（７０２）

非リアルタイムファイルデータ（ＮＲＴ＿ＦＩＬＥ＿ＤＡＴＡ）は、カプセル化されたファイルを含んでいる。

【００５９】

ＭＥＴＡ＿ＤＡＴＡ＿ＴＹＰＥ（７０４）

メタデータタイプ（ＭＥＴＡ＿ＤＡＴＡ＿ＴＹＰＥ）は、メタデータのタイプを識別し、値“１”は“クリップ定義記録”ＸＭＬメタデータを示す。

【００６０】

ＭＥＴＡ＿ＤＡＴＡ＿ＶＡＬＵＥ（７０６）

メタデータ値（ＭＥＴＡ＿ＤＡＴＡ＿ＶＡＬＵＥ）は、メタデータを含み、メタデータは、この例では、下記でさらに論じるクリップ定義記録を含んでいる。

【００６１】

ＴＯＴＡＬ＿ＭＥＴＡ＿ＤＡＴＡ＿ＬＥＮＧＴＨ（７０８）

総メタデータ長（ＴＯＴＡＬ＿ＭＥＴＡ＿ＤＡＴＡ＿ＬＥＮＧＴＨ）は、タイプフィー

ルドと値フィールドとのトータルの長さを含んでいる。

【００６２】

ＣＲＣ（７１０）

ＣＲＣは、ＣＲＣフィールドを除く、データ部とメタデータ部とを含むＮＲＴ＿ＦＩＬＥ全体にわたって計算された、１６ビットＣＲＣである。１つの側面では、ＣＲＣは、標準ＣＲＣ－１６－ＣＣＩＴＴ生成多項式を使用して計算される。

【００６３】

図８は、ＮＲＴコンテンツ分配システムの側面における使用のための例示的なクリップ定義記録８００を図示している。例えば、クリップ定義記録８００は、上記で述べたメタデータ値７０６としての使用に適している。

【００６４】

クリップ定義記録８００は、記録タイプインジケータ８０２と、ＮＲＴプレゼンテーションインジケータ８０４と、属性８０６と、条件付きアクセス仕様８０８と、暗号化情報８１０と、コンテンツ情報８１２と、プレゼンテーション言語情報８１４と、レーティングインジケータ８１６と、ジャンルインジケータ８１８とを含んでいる。

【００６５】

図９Ａ－Ｂは、ＮＲＴコンテンツ分配システムの側面における使用のための、図８のクリップ定義記録の一部である、例示的な条件付きアクセスパラメータ９００およびコンテンツ情報パラメータ９０２を示している。

【００６６】

条件付きアクセスパラメータ９００は、１つ以上の条件付きアクセス仕様を識別する条件付きアクセス仕様インジケータ９０４と、１つ以上のＣＡベンダーまたは第三者を識別する条件付きアクセスシステム識別子９０６と、オペレーター識別子９０８と、それぞれの識別されたＣＡシステム識別子９０６に関係しているＥＭＣを含むプライベートデータ９１０とを含んでいる。コンテンツ情報パラメータ９０２は属性９１２を含んでいる。

【００６７】

図１０は、ＮＲＴコンテンツ分配システムの側面における使用のための例示的な方法１０００を示している。明確にするために、図３中に示しているＮＲＴコンテンツ分配システム３００を参照して、方法１０００をここで説明している。例えば、１つの側面では、ＮＲＴコンテンツ分配システム３００を制御して、下記に説明する動作を実行させるために、ＮＲＴ暗号化モジュール３０４は１つ以上の組のコードを実行する。

【００６８】

ブロック１００２において、分配ネットワーク上のデバイスへの分配のためにＮＲＴコンテンツが獲得される。例えば、ＮＲＴコンテンツは、クリップや、プレゼンテーションや、データや、他のタイプのＮＲＴコンテンツを含んでいてもよい。１つの側面では、ＮＲＴコンテンツはＮＲＴ暗号化モジュール３０４により獲得される。

【００６９】

ブロック１００４において、ＮＲＴコンテンツを暗号化するために使用される制御ワードが獲得される。１つの側面では、ＮＲＴ暗号化モジュール３０４は、ＣＷＧモジュール３１０から制御ワードを獲得する。

【００７０】

ブロック１００６において、ＮＲＴコンテンツが制御ワードで暗号化されて、暗号化ＮＲＴコンテンツが発生される。１つの側面では、暗号化モジュール３０４は、制御ワードを使用してＮＲＴコンテンツを暗号化するように動作する。

【００７１】

ブロック１００８において、１つ以上のＥＣＭ発生器に関係しているＥＣＭが獲得される。１つの側面では、ＮＲＴ暗号化モジュール３０４は制御ワードをＥＣＭ発生器３０６に渡し、各発生器は応答してＥＣＭを発生させる。

【００７２】

ブロック１０１０において、暗号化ＮＲＴコンテンツおよびＥＣＭは、分配ネットワー

クを通してデバイスに配信される。１つの側面では、ネットワークサービングノード３０８は、分配ネットワークを通して、暗号化ＮＲＴコンテンツおよびＥＣＭを送信するように動作する。

【００７３】

したがって、方法１０００は、ＮＲＴコンテンツ分配システムの側面を提供するように動作する。方法１０００はただ１つだけのインプリメンテーションを表していて、側面の範囲内で、他のインプリメンテーションも可能であることに留意されたい。

【００７４】

図１１は、ＮＲＴコンテンツ分配システムの側面における使用のための例示的な方法１１００を示している。明確にするために、図５中に示しているＮＲＴコンテンツ分配システム５００を参照して、方法１０１０をここで説明している。例えば、１つの側面では、ＮＲＴコンテンツ分配システム５００を制御して、下記に説明する動作を実行させるために、ＮＲＴファイル管理モジュール５０４は１つ以上の組のコードを実行する。

【００７５】

ブロック１１０２において、分配ネットワーク上のデバイスへの分配のためにＮＲＴコンテンツが獲得される。例えば、ＮＲＴコンテンツは、クリップや、プレゼンテーションや、データや、他のタイプのＮＲＴコンテンツを含んでいてもよい。１つの側面では、ＮＲＴコンテンツはＮＲＴファイル管理モジュール５０４により獲得される。

【００７６】

ブロック１１０４において、ＮＲＴコンテンツを暗号化するために使用される制御ワードが獲得される。１つの側面では、ＮＲＴファイル管理モジュール５０４は、ＳＣＳ５０６から制御ワードを獲得する。

【００７７】

ブロック１１０６において、１つ以上のＥＣＭが発生される。１つの側面では、各ＥＣＭ発生器５１８は、ロングタームキーを使用して制御ワードを暗号化し、ＥＣＭを発生させる。

【００７８】

ブロック１１０８において、１つ以上のＥＭＭが発生される。１つの側面では、各ＥＭＭ発生器５２０は、ロングタームキーを含むＥＭＭを発生させる。

【００７９】

ブロック１１１０において、ＮＲＴコンテンツを制御ワードで暗号化して、暗号化ＮＲＴコンテンツを発生させる。１つの側面では、ＮＲＴファイル管理モジュール５０４は、制御ワードを使用してＮＲＴコンテンツを暗号化するように動作する。

【００８０】

ブロック１１１２において、暗号化ＮＲＴコンテンツと、ＥＣＭと、ＥＭＭは、分配ネットワークを通してデバイスに配信される。１つの側面では、ＮＲＴファイル管理モジュール５０４は、暗号化ＮＲＴコンテンツおよびＥＣＭをネットワークサービングノード５１０に配信し、ネットワークサービングノード５１０は、分配ネットワークを通して、暗号化ＮＲＴコンテンツおよびＥＣＭを送信する。さらに、ＥＭＭ発生器５２０は、ＩＰデータキャストで分配ネットワークを通して送信するために、ＥＭＭをネットワークサービングノード５１０に配信するように動作する。

【００８１】

したがって、方法１１００は、ＮＲＴコンテンツ分配システムの側面を提供するように動作する。方法１１００はただ１つのインプリメンテーションを表していて、側面の範囲内で、他のインプリメンテーションも可能であることに留意すべきである。

【００８２】

図１２は、ＮＲＴコンテンツ分配システムの側面における使用のための例示的なＮＲＴコンテンツ受信モジュール１２００を示している。例えば、ＮＲＴコンテンツ受信モジュール１２００は、図１中に示しているＮＲＴコンテンツ受信モジュール１１６としての使用に適している。ＮＲＴコンテンツ受信モジュール１２００は、処理論理１２０２と、キ

ー獲得論理１２０４と、レンダリング論理インターフェース（Ｉ／Ｆ）１２０６と、解読論理１２０８と、プロトコルスタックインターフェース１２１０と、ユーザインターフェース１２１２とを具備していて、すべてはデータバス１２１４に結合されている。

【００８３】

１つの側面では、処理論理１２０２は、ＣＰＵ、プロセッサ、ゲートアレイ、ハードウェア論理、メモリエレメント、仮想機械、ソフトウェア、および／または、ソフトウェアを実行するハードウェアのうちの少なくとも１つを備えている。したがって、機械読取可能命令を実行し、データバス１２１４を使用して、ＮＲＴコンテンツ受信モジュール１２００の他の１つ以上の機能エレメントを制御するように構成されている論理を、処理論理１２０２は一般的に備えている。

【００８４】

ユーザインターフェース１２１２は、ＮＲＴコンテンツ受信モジュール１２００が、ユーザ命令を受け取るためにデバイスユーザと対話できるように動作する、ハードウェア、および／または、ソフトウェアを実行するハードウェアを備えている。例えば、ユーザは、レンダリングのために特定のＮＲＴコンテンツが獲得されるように要求してもよい。１つの側面では、ユーザインターフェース１２１２は処理論理１２０２により制御される。

【００８５】

レンダリング論理１２０６は、ＮＲＴコンテンツ受信モジュール１２００が受信したＮＲＴコンテンツをデバイス上でレンダリングできるように動作する、ハードウェア、および／または、ソフトウェアを実行するハードウェアを備えている。例えば、レンダリング論理１２０６は視覚ディスプレイまたは他のデバイスと通信し、選択したＮＲＴコンテンツをユーザが見ることができるようにする。１つの側面では、レンダリング論理１２０６はまた、後のプレゼンテーションのために、ＮＲＴコンテンツを記憶するのに使用できるメモリを備えている。

【００８６】

プロトコルスタックインターフェース１２１０は、ＮＲＴコンテンツ受信モジュール１２００がデバイスプロトコルスタックから暗号化ＮＲＴコンテンツと、ＥＣＭと、ＥＭＭとを取得できるように動作する、ハードウェア、および／または、ソフトウェアを実行するハードウェアを備えている。１つの側面では、処理論理１２０２は、プロトコルスタックインターフェース１２１０を制御して、プロトコルスタックから情報を取得するように動作する。

【００８７】

キー獲得論理１２０４は、ＮＲＴコンテンツ受信モジュール１２００がＥＭＭおよびＥＣＭを処理して、暗号化ＮＲＴコンテンツを解読するために使用することができる制御ワードを取得できるように動作する、ハードウェア、および／または、ソフトウェアを実行するハードウェアを備えている。例えば、キー獲得論理１２０４は、ＥＭＭを処理して、特定のＥＣＭを暗号化するために使用されたロングタームキーを取得する。ロングタームキーはその後、ＥＣＭを解読して制御ワードを取得するために使用される。制御ワードはその後、解読論理１２０８に渡される。

【００８８】

解読論理１２０８は、ＮＲＴコンテンツ受信モジュール１２００が暗号化ＮＲＴコンテンツを解読できるように動作する、ハードウェア、および／または、ソフトウェアを実行するハードウェアを備えている。例えば、プロトコルスタックインターフェース１２１０は、デバイスプロトコルスタックから暗号化ＮＲＴコンテンツを獲得するように動作する。暗号化コンテンツは、ＮＲＴコンテンツを解読するために制御ワードを使用する解読論理１２０８に渡される。ＮＲＴコンテンツはその後、レンダリング論理１２０６に渡され、ここで、デバイス上でレンダリングするために処理され、その後の処理のために、メモリ中に記憶される。

【００８９】

１つの側面では、ＮＲＴコンテンツ分配システムは、機械読取可能媒体上に記憶または

具現化される、１つ以上のプログラム命令（“命令”）またはコードの組（“コード”）を具備している。コードが、少なくとも１つのプロセッサにより実行されるとき、例えば、処理論理１２０２におけるプロセッサにより実行されるとき、ここで述べた機能を提供する。例えば、ファイル受信機１２００にインターフェースする、フロッピーディスクや、ＣＤＲＯＭや、メモリカードや、フラッシュメモリデバイスや、ＲＡＭや、ＲＯＭや、他の何らかのタイプのメモリデバイス、または機械読取可能媒体のような、機械読取可能媒体から、コードは処理論理１２０２中にロードされてもよい。別の側面では、コードは、外部のデバイスまたはネットワークリソースから、ファイル受信機１２００中にダウンロードされてもよい。コードは、実行されるとき、ここに説明したようなＮＲＴコンテンツ分配システムの側面を提供する。

【００９０】

図１３は、ＮＲＴコンテンツ分配システムの側面における使用のための例示的な方法１３００を示している。明確にするために、図１２中に示しているＮＲＴコンテンツ受信モジュール１２００を参照して、方法１３００をここで説明している。例えば、１つの側面では、ＮＲＴコンテンツ受信モジュール１２００を制御して、下記で説明している動作を実行するために、処理論理１２０２は１つ以上の組のコードを実行する。

【００９１】

ブロック１３０２において、ＮＲＴコンテンツが申し込まれる。１つの側面では、処理論理１２０２は選択されたＮＲＴコンテンツを１つ以上のコンテンツベンダーから受信する申し込みをするように動作する。

【００９２】

ブロック１３０４において、ＮＲＴコンテンツに対して申し込みがされたことに関係するＥＭＭが受信される。例えば、申し込みプロセスの一部として、処理論理１２０２は適切なコンテンツベンダーからＥＭＭを取得する。１つの側面では、ＥＭＭはプロトコルスタックインターフェース１２１０により取得され、キー獲得論理１２０４に渡される。

【００９３】

ブロック１３０６において、暗号化ＮＲＴコンテンツと関係するＥＣＭとが取得される。１つの側面では、処理論理１２０２は、プロトコルスタックインターフェース１２１０を制御して、暗号化ＮＲＴおよびＥＣＭを取得するように動作する。

【００９４】

ブロック１３０８において、受信されたＥＣＭはキー獲得論理１２０４に渡される。ここで、ＥＭＭ中で提供されたキーは、ＥＣＭを解読して、暗号化ＮＲＴコンテンツを暗号化するために使用された制御ワードを取得するのに使用される。

【００９５】

ブロック１３１０において、受信された暗号化ＮＲＴコンテンツが制御ワードで解読される。１つの側面では、解読論理１２０８は、制御ワードを使用して暗号化ＮＲＴコンテンツを解読するように動作する。

【００９６】

ブロック１３１２において、解読ＮＲＴコンテンツはレンダリング論理インターフェース１２０６に渡される。ここで、解読ＮＲＴコンテンツはレンダリングされるか、または、後のプレゼンテーションのために記憶される。

【００９７】

したがって、方法１３００は、ＮＲＴコンテンツ分配システムの側面を提供するように動作する。方法１３００はただ１つのインプリメンテーションを表しているが、側面の範囲内で、他のインプリメンテーションも可能であることに留意すべきである。

【００９８】

図１４は、ＮＲＴコンテンツ分配システムの側面における使用のためのＮＲＴコンテンツ配信モジュール１４００を示している。例えば、ＮＲＴコンテンツ配信モジュール１４００は、図１中に示しているＮＲＴコンテンツ配信モジュール１１２としての使用に適している。１つの側面では、ここに説明したようなＮＲＴコンテンツ分配システムの側面を

提供するように構成されている１つ以上のモジュールを備える、少なくとも１つのプロセッサにより、ＮＲＴコンテンツ配信モジュール１４００は実現される。例えば、各モジュールはハードウェア、および／または、ソフトウェアを実行するハードウェアを備えている。

【００９９】

ＮＲＴコンテンツ配信モジュール１４００は、制御ワードでＮＲＴコンテンツを暗号化して、暗号化ＮＲＴコンテンツを発生させる手段（１４０２）を備える第１のモジュールを具備している。第１のモジュールは、１つの側面では、ファイル管理モジュール５０４を含む。ＮＲＴコンテンツ配信モジュール１４００はまた、制御ワードを１つ以上の受給権制御メッセージ（ＥＣＭ）発生器に提供する手段（１４０４）を備える第２のモジュールを具備している。第２のモジュールは、１つの側面では、ＳＣＳ５０６を含む。ＮＲＴコンテンツ配信モジュール１４００はまた、１つ以上のＥＣＭ発生器から１つ以上のＥＣＭをそれぞれ受け取る手段（１４０６）を備える第３のモジュールを具備している。各ＥＣＭは、制御ワードに対する条件付きアクセスを提供するための、制御ワードの一意的な暗号化を含む。第３のモジュールは、１つの側面では、ＳＣＳ５０６を含む。ＮＲＴコンテンツ配信モジュール１４００はまた、分配ネットワークを通しての送信のために、暗号化ＮＲＴコンテンツと１つ以上のＥＣＭとを提供する手段（１４０８）を備える第４のモジュールを具備している。第４のモジュールは、１つの側面では、ファイル管理モジュール５０４を含む。

【０１００】

図１５は、ＮＲＴコンテンツ分配システムの側面における使用のための、ＮＲＴコンテンツ受信モジュール１５００を示している。例えば、ＮＲＴコンテンツ受信モジュール１５００は、図１に示しているＮＲＴコンテンツ受信モジュール１１６としての使用に適している。１つの側面では、ＮＲＴコンテンツ受信モジュール１５００は、ここで説明したようなＮＲＴコンテンツ分配システムの側面を提供するように構成されている１つ以上のモジュールを備える、少なくとも１つのプロセッサにより実現される。例えば、各モジュールはハードウェア、および／または、ソフトウェアを実行するハードウェアを備えている。

【０１０１】

ＮＲＴコンテンツ受信モジュール１５００は、制御ワードで暗号化されている暗号化ＮＲＴコンテンツを受信する手段（１５０２）を備える第１のモジュールを具備している。第１のモジュールは、１つの側面では、処理論理１２０２を備える。ＮＲＴコンテンツ受信モジュール１５００はまた、１つ以上の受給権制御メッセージ（ＥＣＭ）を受信する手段（１５０４）を備える第２のモジュールを具備している。第２のモジュールは、１つの側面では、処理論理１２０２を備える。ＮＲＴコンテンツ受信モジュール１５００はまた、選択されたＥＣＭをロングタームキーで解読して、制御ワードを取得する手段（１５０６）を備える第３のモジュールを具備している。第３のモジュールは、１つの側面では、キー獲得論理１２０４を備える。ＮＲＴコンテンツ受信モジュール１５００はまた、暗号化ＮＲＴコンテンツを解読して、解読ＮＲＴコンテンツを取得する手段（１５０８）を備える第４のモジュールを具備している。第４のモジュールは、１つの側面では、解読論理１２０８を備える。

【０１０２】

ここで開示した側面に関連して述べたさまざまな例示的な論理、論理ブロック、モジュールおよび回路は、汎用プロセッサ、デジタル信号プロセッサ（ＤＳＰ）、特定用途向け集積回路（ＡＳＩＣ）、現場プログラム可能ゲートアレイ（ＦＰＧＡ）または他のプログラム可能論理デバイス、ディスクリートゲートまたはトランジスタ論理、ディスクリートハードウェアコンポーネント、あるいは、ここに開示した機能を実行するように設計されているこれらの任意の組み合わせたものにより、実現または実行されてもよい。汎用プロセッサはマイクロプロセッサであってもよいが、代替実施形態では、プロセッサは、任意の従来のプロセッサ、制御装置、マイクロ制御装置または状態機械であってもよい。プロ

セッサはまた、コンピューティングデバイスを組み合わせたものとして、例えば、ＤＳＰとマイクロプロセッサの組み合わせとして、複数のマイクロプロセッサとして、ＤＳＰコアに関連した１つ以上のマイクロプロセッサとして、あるいは、このような構成の他の何らかのものとして、実現されてもよい。

【０１０３】

ここで開示した側面に関連して記述した方法またはアルゴリズムのステップは、ハードウェアで、プロセッサにより実行されるソフトウェアモジュールで、あるいは、双方を組み合わせたもので直接的に具現化してもよい。ソフトウェアモジュールは、ＲＡＭメモリ、フラッシュメモリ、ＲＯＭメモリ、ＥＰＲＯＭメモリ、ＥＥＰＲＯＭメモリ、レジスタ、ハードディスク、リムーバルディスク、ＣＤ－ＲＯＭ、または技術的に知られている何らかの形態の記憶媒体に存在していてもよい。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるようにプロセッサに結合されていてもよい。代替実施形態では、記憶媒体はプロセッサと一体化されてもよい。プロセッサおよび記憶媒体は、ＡＳＩＣに存在していてもよい。ＡＳＩＣは、ユーザ端末に存在していてもよい。代替実施形態では、プロセッサおよび記憶媒体は、ディスクリートコンポーネントとしてユーザ端末に存在していてもよい。

【０１０４】

開示した側面の記述は、当業者が本発明を製作または使用できるように提供した。これらの側面に対するさまざま改良は当業者に容易に明らかとなり、ここに定義された一般的な原理は、本発明の精神または範囲を逸脱することなく、例えば、インスタントメッセージングサービスや、任意の一般的なワイヤレスデータ通信アプリケーションである、他の側面に適用してもよい。したがって、本発明はここに示された側面に限定されることを意図しているものではなく、ここで開示されている原理および新しい特徴と一致した最も広い範囲に一致させるべきである。用語“例示的な”は、ここに限り、“例として、インスタンスとして、あるいは例証として機能すること”を意味するように使用する。ここで“例示的な”として記述した任意の側面は、必ずしも、他の側面より好ましい、または、効果的であるとして解釈すべきではない。

【０１０５】

このように、ＮＲＴコンテンツ分配システムの側面がここに図示および記述されているが、これらの精神または不可欠な特性から逸脱することなく、さまざまな変更が側面に行われてもよいことを正しく理解するだろう。それゆえ、ここでの本開示および記述は、限定してはいないが、本発明の範囲の例証となることを意図しており、下記の特許請求の範囲中でも述べられている。

以下に、本願出願時の特許請求の範囲に記載された発明を付記する。

[１]分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを分配するための方法において、

制御ワードで前記ＮＲＴコンテンツを暗号化して、暗号化ＮＲＴコンテンツを発生させることと、

１つ以上の受給権制御メッセージ（ＥＣＭ）発生器に前記制御ワードを提供することと、

前記１つ以上のＥＣＭ発生器から１つ以上のＥＣＭをそれぞれ受け取ること、

前記分配ネットワークを通した送信のために、前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとを提供することとを含み、

各ＥＣＭは、前記制御ワードに対する条件付きアクセスを提供するための、前記制御ワードの一意的な暗号化を含む方法。

[２]制御ワード発生器から前記制御ワードを受け取ることをさらに含む上記[１]記載の方法。

[３]前記ＮＲＴコンテンツに関係付けるべき１つ以上のアクセス基準（ＡＣ）パラメータを取得することと、

前記１つ以上のＡＣパラメータを前記１つ以上のＥＣＭ発生器にそれぞれ提供すること

をさらに含む上記[１]記載の方法。
[４]前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとをＮＲＴファイルフォーマットにエンコードすることをさらに含む上記[１]記載の方法。
[５]前記ＮＲＴファイルフォーマットはクリップ定義記録を含む上記[４]記載の方法。
[６]前記クリップ定義記録は、前記暗号化ＮＲＴコンテンツを識別し、前記１つ以上のＥＣＭを含む上記[５]記載の方法。
[７]分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを分配するように構成されている装置において、
１つ以上の受給権制御メッセージ（ＥＣＭ）発生器に制御ワードを提供して、前記１つ以上のＥＣＭ発生器から１つ以上のＥＣＭをそれぞれ受け取るように構成されている同期器と、
前記制御ワードで前記ＮＲＴコンテンツを暗号化し、暗号化ＮＲＴコンテンツを発生させて、前記分配ネットワークを通した送信のために、前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとを提供するように構成されている管理モジュールとを具備し、
各ＥＣＭは、前記制御ワードに対する条件付きアクセスを提供するための、前記制御ワードの一意的な暗号化を含む装置。
[８]前記同期器は制御ワード発生器から前記制御ワードを取得するように構成されている上記[７]記載の装置。
[９]前記同期器は、
前記ＮＲＴコンテンツに関係付けるべき１つ以上のアクセス基準（ＡＣ）パラメータを取得して、
前記１つ以上のＡＣパラメータを前記１つ以上のＥＣＭ発生器にそれぞれ提供するように構成されている上記[７]記載の装置。
[１０]前記管理モジュールは、前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとをＮＲＴファイルフォーマットにエンコードするように構成されている上記[７]記載の装置。
[１１]前記ＮＲＴファイルフォーマットはクリップ定義記録を含む上記[１０]記載の装置。
[１２]前記クリップ定義記録は、前記暗号化ＮＲＴコンテンツを識別し、前記１つ以上のＥＣＭを含む上記[１１]記載の装置。
[１３]分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを分配するように構成されている装置において、
制御ワードで前記ＮＲＴコンテンツを暗号化して、暗号化ＮＲＴコンテンツを発生させる手段と、
１つ以上の受給権制御メッセージ（ＥＣＭ）発生器に前記制御ワードを提供する手段と、
前記１つ以上のＥＣＭ発生器から１つ以上のＥＣＭをそれぞれ受け取る手段と、
前記分配ネットワークを通した送信のために、前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとを提供する手段とを具備し、
各ＥＣＭは、前記制御ワードに対する条件付きアクセスを提供するための、前記制御ワードの一意的な暗号化を含む装置。
[１４]制御ワード発生器から前記制御ワードを受け取る手段をさらに具備する上記[１３]記載の装置。
[１５]前記ＮＲＴコンテンツに関係付けるべき１つ以上のアクセス基準（ＡＣ）パラメータを取得する手段と、
前記１つ以上のＡＣパラメータを前記１つ以上のＥＣＭ発生器にそれぞれ提供する手段とをさらに具備する上記[１３]記載の装置。
[１６]前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとをＮＲＴファイルフォーマットにエンコードする手段をさらに具備する上記[１３]記載の装置。
[１７]前記ＮＲＴファイルフォーマットはクリップ定義記録を含む上記[１６]記載の装

置。
[１８]前記クリップ定義記録は、前記暗号化ＮＲＴコンテンツを識別し、前記１つ以上のＥＣＭを含む上記[１７]記載の装置。
[１９]分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを分配するためのコンピュータプログラムプロダクトにおいて、前記コンピュータプログラムプロダクトは、
１つ以上の受給権制御メッセージ（ＥＣＭ）発生器に制御ワードを提供するために実行可能なコードと、
前記１つ以上のＥＣＭ発生器から１つ以上のＥＣＭをそれぞれ受け取るために実行可能なコードと、
前記制御ワードで前記ＮＲＴコンテンツを暗号化して、暗号化ＮＲＴコンテンツを発生させるために実行可能なコードと、
前記分配ネットワークを通した送信のために、前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとを提供するために実行可能なコードとでエンコードされているコンピュータ読取可能媒体を具備し、
各ＥＣＭは、前記制御ワードに対する条件付きアクセスを提供するための、前記制御ワードの一意的な暗号化を含むコンピュータプログラムプロダクト。
[２０]分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを分配するように構成されているサーバにおいて、
ネットワークインターフェースと、
１つ以上の受給権制御メッセージ（ＥＣＭ）発生器に制御ワードを提供して、前記１つ以上のＥＣＭ発生器から１つ以上のＥＣＭをそれぞれ受け取るように構成されている同期器と、
前記制御ワードで前記ＮＲＴコンテンツを暗号化し、暗号化ＮＲＴコンテンツを発生させて、前記分配ネットワークを通した送信のために、前記ネットワークインターフェースを通して、前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとを提供するように構成されている管理モジュールとを具備し、
各ＥＣＭは、前記制御ワードに対する条件付きアクセスを提供するための、前記制御ワードの一意的な暗号化を含むサーバ。
[２１]分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを受信するための方法において、
制御ワードで暗号化されている暗号化ＮＲＴコンテンツを受信することと、
１つ以上の受給権制御メッセージ（ＥＣＭ）を受信することと、
ロングタームキーで、選択されたＥＣＭを解読して、前記制御ワードを取得することと、
前記暗号化ＮＲＴコンテンツを解読して、解読ＮＲＴコンテンツを取得することとを含む方法。
[２２]前記ロングタームキーを含む受給権管理メッセージ（ＥＭＭ）を受信することをさらに含む上記[２１]記載の方法。
[２３]ＮＲＴファイルフォーマットの、前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとを受信することをさらに含む上記[２１]記載の方法。
[２４]前記ＮＲＴファイルフォーマットはクリップ定義記録を含む上記[２３]記載の方法。
[２５]前記クリップ定義記録は、前記暗号化ＮＲＴコンテンツを識別し、前記１つ以上のＥＣＭを含む上記[２４]記載の方法。
[２６]分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを受信する装置において、
制御ワードで暗号化されている暗号化ＮＲＴコンテンツを受信し、１つ以上の受給権制御メッセージ（ＥＣＭ）を受信するように構成されている処理論理と、
ロングタームキーで、選択されたＥＣＭを解読して、前記制御ワードを取得するように

構成されているキー獲得論理と、
前記暗号化ＮＲＴコンテンツを解読して、解読ＮＲＴコンテンツを取得するように構成されている解読論理とを具備する装置。
[２７]前記処理論理は、前記ロングタームキーを含む受給権管理メッセージ（ＥＭＭ）を受信するように構成されている上記[２６]記載の装置。
[２８]前記処理論理は、ＮＲＴファイルフォーマットの、前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとを受信するように構成されている上記[２６]記載の装置。
[２９]前記ＮＲＴファイルフォーマットはクリップ定義記録を含む上記[２８]記載の装置。
[３０]前記クリップ定義記録は、前記暗号化ＮＲＴコンテンツを識別し、前記１つ以上のＥＣＭを含む上記[２９]記載の装置。
[３１]分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを受信する装置において、
制御ワードで暗号化されている暗号化ＮＲＴコンテンツを受信する手段と、
１つ以上の受給権制御メッセージ（ＥＣＭ）を受信する手段と、
ロングタームキーで、選択されたＥＣＭを解読して、前記制御ワードを取得する手段と、
前記暗号化ＮＲＴコンテンツを解読して、解読ＮＲＴコンテンツを取得する手段とを具備する装置。
[３２]前記ロングタームキーを含む受給権管理メッセージ（ＥＭＭ）を受信する手段をさらに具備する上記[３１]記載の装置。
[３３]ＮＲＴファイルフォーマットの、前記暗号化ＮＲＴコンテンツと前記１つ以上のＥＣＭとを受信する手段をさらに具備する上記[３１]記載の装置。
[３４]前記ＮＲＴファイルフォーマットはクリップ定義記録を含む上記[３３]記載の装置。
[３５]前記クリップ定義記録は、前記暗号化ＮＲＴコンテンツを識別し、前記１つ以上のＥＣＭを含む上記[３４]記載の装置。
[３６]分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを受信するためのコンピュータプログラムプロダクトにおいて、前記コンピュータプログラムプロダクトは、
制御ワードで暗号化されている暗号化ＮＲＴコンテンツを受信するために実行可能なコードと、
１つ以上の受給権制御メッセージ（ＥＣＭ）を受信するために実行可能なコードと、
ロングタームキーで、選択されたＥＣＭを解読して、前記制御ワードを取得するために実行可能なコードと、
前記暗号化ＮＲＴコンテンツを解読して、解読ＮＲＴコンテンツを取得するために実行可能なコードとでエンコードされているコンピュータ読取可能媒体を具備するコンピュータプログラムプロダクト。
[３７]分配ネットワークを通して、非リアルタイム（ＮＲＴ）コンテンツを分配するように構成されているデバイスにおいて、
アンテナと、
前記アンテナを使用して、制御ワードで暗号化されている暗号化ＮＲＴコンテンツを受信し、１つ以上の受給権制御メッセージ（ＥＣＭ）を受信するように構成されている処理論理と、
ロングタームキーで、選択されたＥＣＭを解読して、前記制御ワードを取得するように構成されているキー獲得論理と、
前記暗号化ＮＲＴコンテンツを解読して、解読ＮＲＴコンテンツを取得するように構成されている解読論理とを具備するデバイス。

【図１】

図１

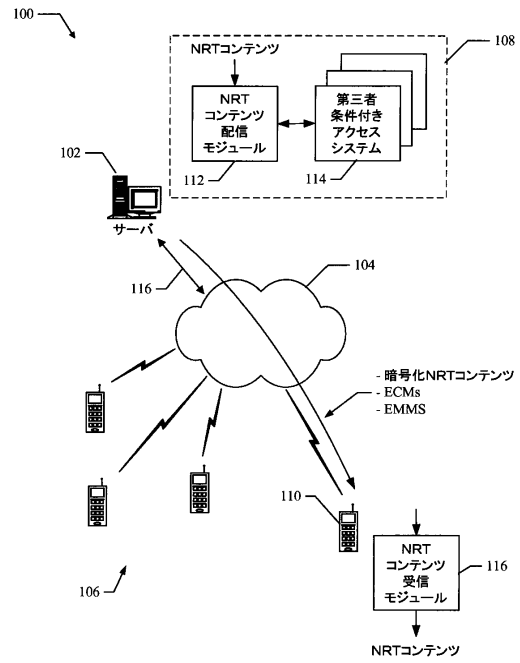

FIG. 1

【図２】

図２

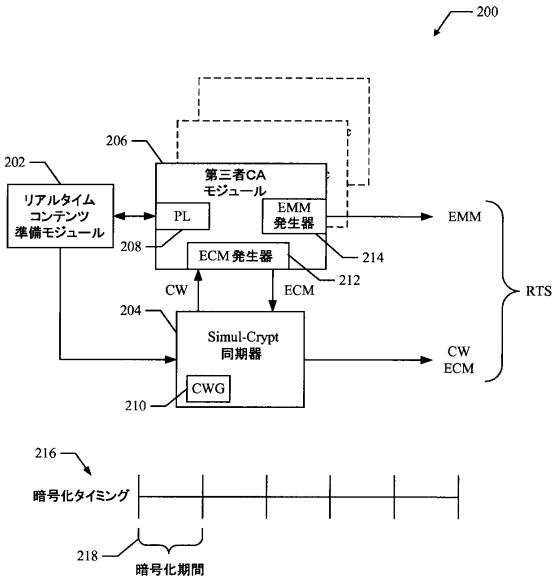

FIG. 2

先行技術

【図３】

図３

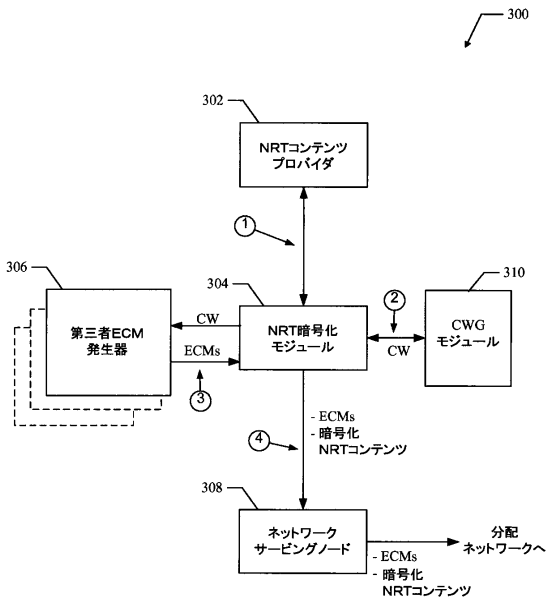

FIG. 3

【図４】

図４

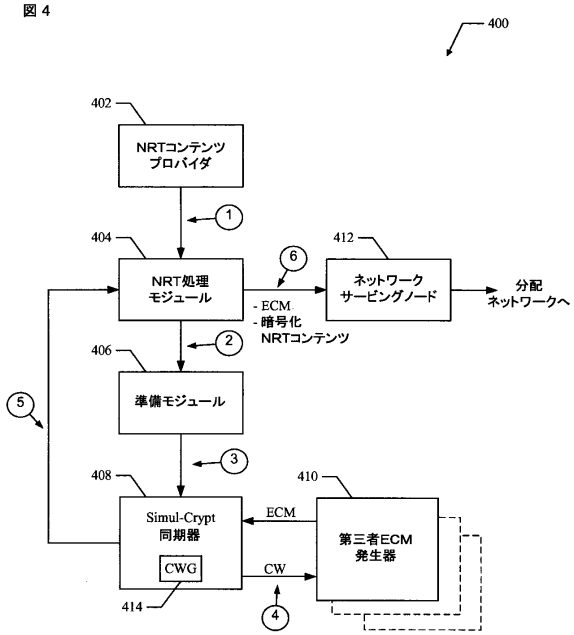

FIG. 4

【図５】

図５

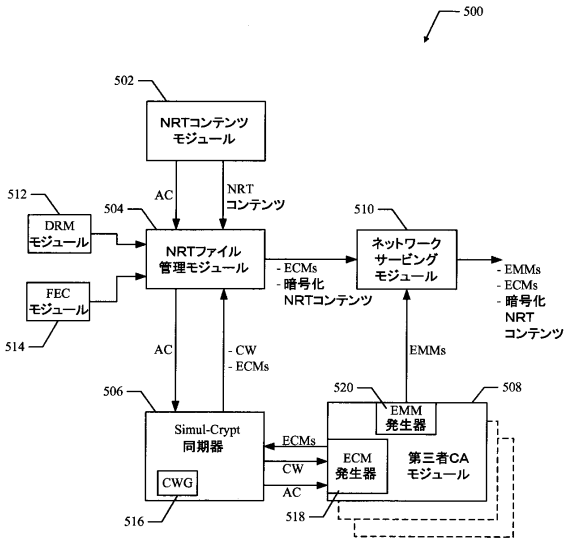

FIG. 5

【図６】

図６

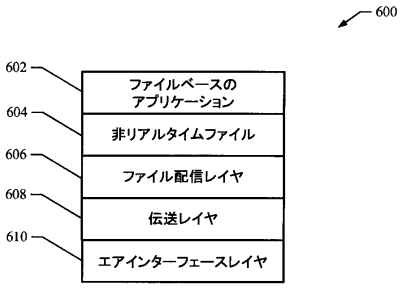

FIG. 6

【図７】

図７

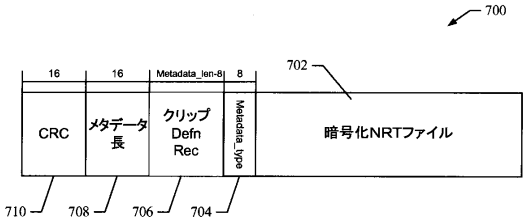

FIG. 7

【図８】

図８

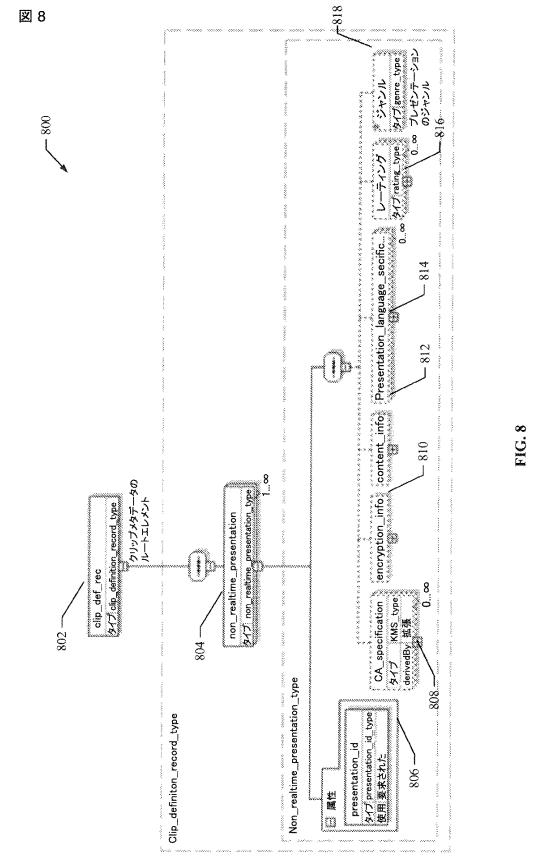

FIG. 8

【図９Ａ】

図９Ａ

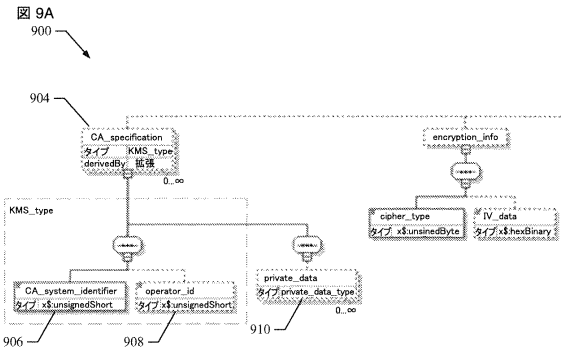

FIG. 9A

【図９Ｂ】

図９Ｂ

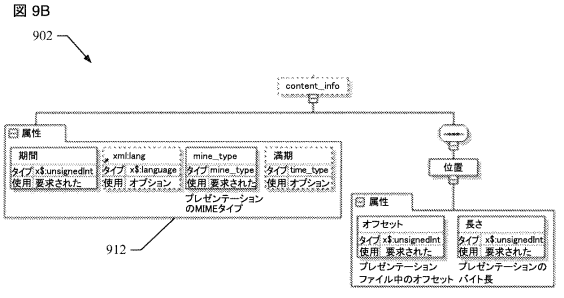

FIG. 9B

【図１０】

図 10

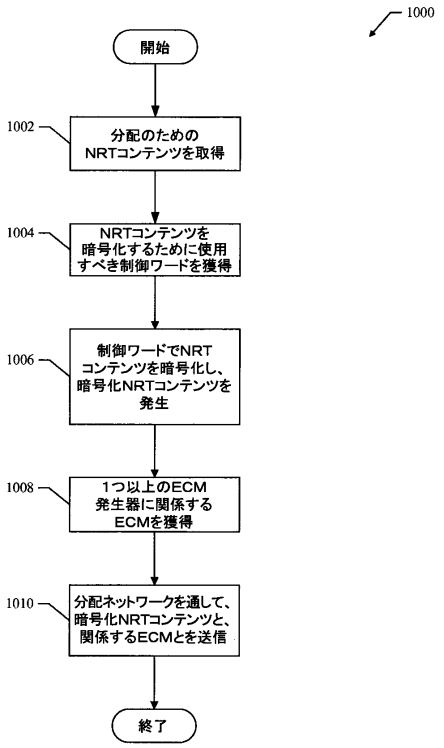

FIG. 10

【図１１】

図 11

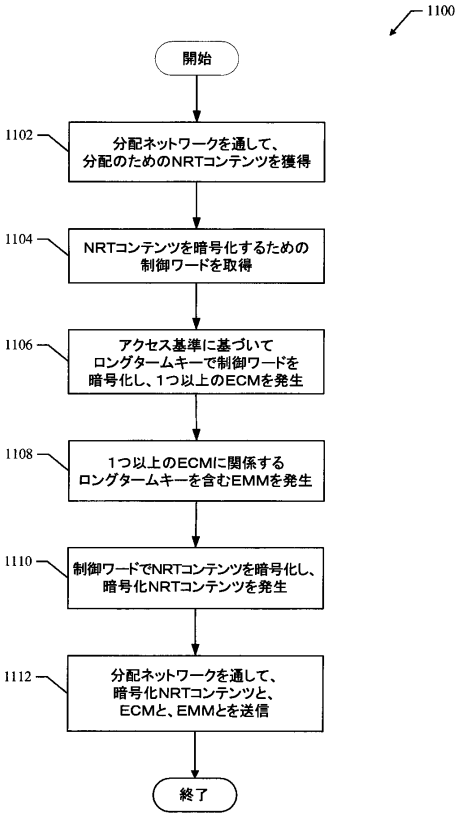

FIG. 11

【図１２】

図 12

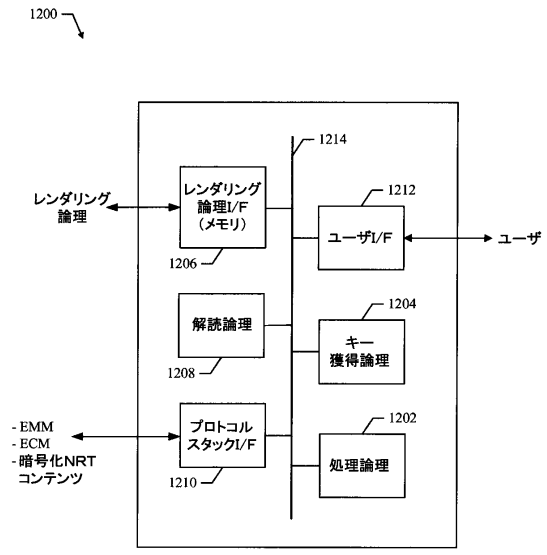

FIG. 12

【図１３】

図 13

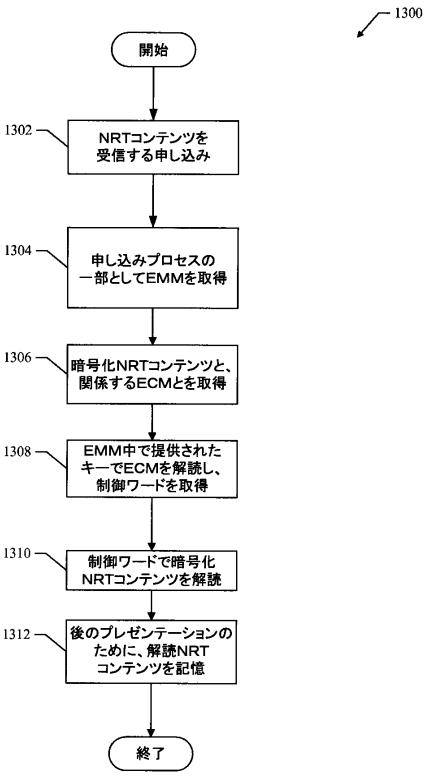

FIG. 13

【図１４】

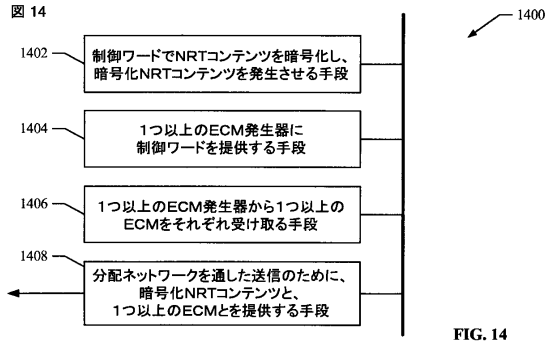

FIG. 14

【図１５】

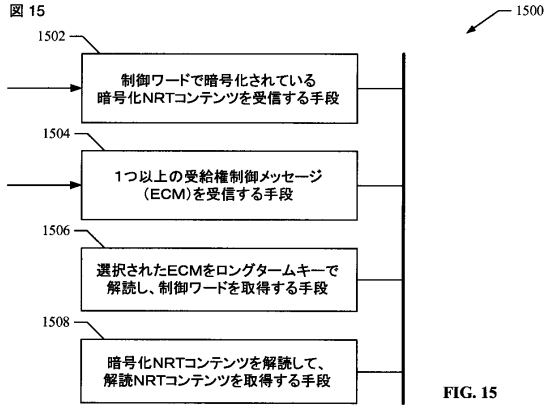

FIG. 15

フロントページの続き

(31)優先権主張番号　12/370,478
(32)優先日　平成21年2月12日(2009.2.12)
(33)優先権主張国　米国(US)

前置審査

(74)代理人　100153051
弁理士　河野　直樹
(74)代理人　100140176
弁理士　砂川　克
(74)代理人　100158805
弁理士　井関　守三
(74)代理人　100179062
弁理士　井上　正
(74)代理人　100124394
弁理士　佐藤　立志
(74)代理人　100112807
弁理士　岡田　貴志
(74)代理人　100111073
弁理士　堀内　美保子
(72)発明者　カンナン、プラサンナ
アメリカ合衆国、カリフォルニア州　９２１２１、サン・ディエゴ、モアハウス・ドライブ　５７７５
(72)発明者　チェン、アン・メイ
アメリカ合衆国、カリフォルニア州　９２１２１、サン・ディエゴ、モアハウス・ドライブ　５７７５
(72)発明者　ナガラジ、サディ・エム.
アメリカ合衆国、カリフォルニア州　９２１２１、サン・ディエゴ、モアハウス・ドライブ　５７７５

審査官　川崎　優

(56)参考文献　特開２００７－０６０１６７（ＪＰ，Ａ）
特表２００７－５２３５３６（ＪＰ，Ａ）
国際公開第２００６／６２６２５（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／００－３６
Ｈ０４Ｎ　２１／００－８５８
Ｈ０４Ｈ　２０／００－６０／９８
Ｈ０４Ｗ　　４／００－９９／００
Ｈ０４Ｂ　　７／２４－２６