(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2017-184260
(P2017-184260A)
(43)公開日　平成29年10月5日(2017.10.5)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
G09C	1/00	(2006.01)	G09C	1/00	640E	

審査請求 有　請求項の数 26　ＯＬ　外国語出願　（全 35 頁）

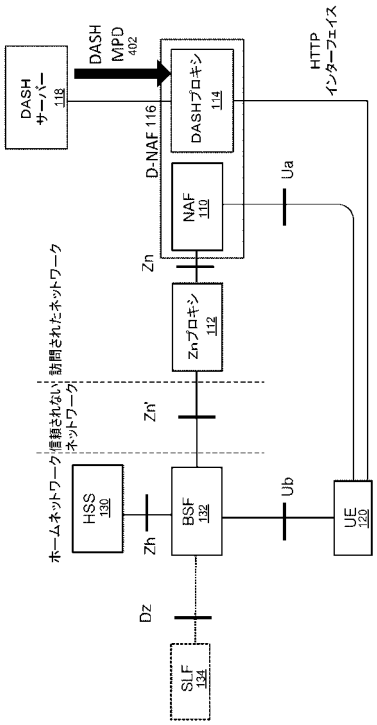
(21)出願番号	特願2017-103554 (P2017-103554)
(22)出願日	平成29年5月25日 (2017.5.25)
(62)分割の表示	特願2015-550736 (P2015-550736)の分割
原出願日	平成25年12月23日 (2013.12.23)
(31)優先権主張番号	61/753,914
(32)優先日	平成25年1月17日 (2013.1.17)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	61/821,635
(32)優先日	平成25年5月9日 (2013.5.9)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	61/824,338
(32)優先日	平成25年5月16日 (2013.5.16)
(33)優先権主張国	米国 (US)

(71)出願人　514045555
インテル　アイピー　コーポレイション
アメリカ合衆国　９５０５４　カリフォルニア州　サンタ　クララ　ミッション　カレッジ　ブールバード　２２００
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(72)発明者　オイマン，オズグル
アメリカ合衆国　９５１３４　カリフォルニア州　サンノゼ　ナヴァロ　ウェイ　４２５　ユニット　１１７

Ｆターム(参考)　5J104 AA07　KA02　KA05　PA01

(54)【発明の名称】ＤＡＳＨアウェア・ネットワークアプリケーションファンクション（Ｄ－ＮＡＦ）

(57)【要約】　（修正有）
【課題】サーバー上でのダイナミックアダプティブストリーミング・オーバー・ハイパーテキストトランスファープロトコル（ＨＴＴＰ）アウェア（ＤＡＳＨ－ａｗａｒｅ）ネットワークアプリケーションファンクション（Ｄ－ＮＡＦ）のための技術を提供する。
【解決手段】Ｄ－ＮＡＦは、クライアントを認証するためのネットワークアプリケーションファンクション（ＮＡＦ）と、クライアントに対してＤＡＳＨコンテンツおよび認証情報を配信するためのＤＡＳＨプロキシと、を含む。
【選択図】図７



【特許請求の範囲】
【請求項１】
ネットワークエレメントにおけるネットワークアプリケーションファンクション（ＮＡＦ）であって、前記ＮＡＦは、
汎用ブートストラップアーキテクチャ（ＧＢＡ）ベースの認証および承認プロシージャを使用して、クライアントを認証し、かつ、
前記ＧＢＡベースの認証および承認プロシージャを使用して、コンテンツ特定ポリシ情報の対象であるダイナミックアダプティブストリーミング・オーバーハイパーテキストトランスファープロトコル（ＨＴＴＰ）（ＤＡＳＨ）コンテンツに対するアクセスについて、前記クライアントを承認する、
ように構成されており、
前記ネットワークエレメントは、さらに、前記ＧＢＡベースの認証および承認プロシージャを使用して、前記クライアントが成功裡に認証および承認される場合に、前記クライアントに対して前記ＤＡＳＨコンテンツを配信するように構成されている、
ＮＡＦ。
【請求項２】
前記ＮＡＦは、さらに、
前記コンテンツ特定ポリシ情報を含むＤＡＳＨコンテンツ情報のためのＤＡＳＨメディア表現記述（ＭＰＤ）をパースするように構成されている、
請求項１に記載のＮＡＦ。
【請求項３】
前記ＮＡＦは、さらに、
ＤＡＳＨコンテンツ情報のユニフォームリソースロケータ（ＵＲＬ）を含むＤＡＳＨコンテンツ情報のためのＤＡＳＨメディア表現記述（ＭＰＤ）をパースするように構成されており、
前記ＤＡＳＨコンテンツ情報のＵＲＬは、ＤＡＳＨ　ＭＰＤ、期間、適合セット、または、表現レベルに対するベースＵＲＬを認証するために使用され、そうでなければ、
前記ＤＡＳＨコンテンツ情報のＵＲＬは、前記ＭＰＤのセグメントＵＲＬを認証するために使用される、
請求項１に記載のＮＡＦ。
【請求項４】
前記ＮＡＦは、さらに、
ＮＡＦ鍵マテリアル、プロフィール、ブートストラップ時間、または、鍵の有効期間を含んでいるブートストラップサーバーファンクション（ＢＳＦ）からセッション鍵を取得し、もしくは、
ＤＡＳＨコンテンツ情報に対するＮＡＦ鍵マテリアルを含んでいる前記ＢＳＦからコンテンツ鍵を取得する、
ように構成されている、請求項１に記載のＮＡＦ。
【請求項５】
前記ＮＡＦは、さらに、
ブートストラップサーバーファンクション（ＢＳＦ）またはホーム加入者サブシステム（ＨＳＳ）を介して、ＧＡＡベースの認証および承認プロシージャをオーバーライドする、
ように構成されている、請求項１に記載のＮＡＦ。
【請求項６】
前記ＮＡＦは、さらに、
ＤＡＳＨサービスプロバイダのためにオペレータネットワーク認証および承認を提供する、
ように構成されている、請求項１に記載のＮＡＦ。
【請求項７】

前記ＮＡＦは、さらに、
ＤＡＳＨメディア表現記述（ＭＰＤ）におけるＤＡＳＨサービスプロバイダの認証および承認ポリシを受け取る、
ように構成されている、請求項１に記載のＮＡＦ。
【請求項８】
前記ＮＡＦは、さらに、
前記クライアントに関するストリーミング計画の対象である前記ＤＡＳＨコンテンツに対するアクセスについて、前記クライアントを承認するように構成されており、
前記ストリーミング計画は、前記クライアントにおいて前記ＤＡＳＨコンテンツをアクセスするために許容可能なビットレートおよび解像度を記述している、
請求項１に記載のＮＡＦ。
【請求項９】
前記ＮＡＦは、さらに、
コンテンツ配信精度に係る定められたレベルを確保するために、配信されたＤＡＳＨコンテンツの整合性を検証する、
ように構成されている、請求項１に記載のＮＡＦ。
【請求項１０】
前記ＮＡＦは、さらに、
ＤＡＳＨコンテンツ情報に対するＤＡＳＨメディア表現記述（ＭＰＤ）の整合性を検証する、
ように構成されている、請求項１に記載のＮＡＦ。
【請求項１１】
前記ＮＡＦは、さらに、
前記ＤＡＳＨコンテンツおよびメディア表現記述（ＭＰＤ）におけるＤＡＳＨコンテンツ情報ロケーションについてＤＡＳＨ認証情報を受け取り、前記ＤＡＳＨ認証情報は、署名と認証鍵を含み、かつ、前記ＤＡＳＨコンテンツ情報ロケーションは、ＤＡＳＨコンテンツ情報のユニフォームリソースロケータ（ＵＲＬ）を含み、かつ、
受け取った前記ＤＡＳＨ認証情報と受け取った前記ＤＡＳＨコンテンツ情報とに基づいて、前記ＤＡＳＨコンテンツに対するアクセスについて、前記クライアントを承認する、
ように構成されている、請求項１に記載のＮＡＦ。
【請求項１２】
前記ＮＡＦは、さらに、
前記ＤＡＳＨコンテンツＵＲＬおよび前記認証鍵に基づいて、ＵＲＬ署名を計算し、かつ、
計算された前記ＵＲＬ署名が、前記ＤＡＳＨ認証情報において受け取った前記署名と一致しない場合に、計算された前記ＵＲＬ署名を拒否する、
ように構成されている、請求項１１記載のＮＡＦ。
【請求項１３】
ダイナミックアダプティブストリーミング・オーバーハイパーテキストトランスファープロトコル（ＨＴＴＰ）（ＤＡＳＨ）コンテンツを受け取るためにクライアントを認証および承認するためのインストラクションを含むコンピュータプログラムであって、一つまたはそれ以上のプロセッサによってインストラクションが実行されると、
ネットワークエレメントにおけるネットワークアプリケーションファンクション（ＮＡＦ）において、汎用ブートストラップアーキテクチャ（ＧＢＡ）ベースの認証および承認プロシージャを使用して、クライアントを認証するステップと、
前記ＮＡＦにおいて、前記ＧＢＡベースの認証および承認プロシージャを使用して、コンテンツ特定ポリシ情報の対象であるダイナミックアダプティブストリーミング・オーバーハイパーテキストトランスファープロトコル（ＨＴＴＰ）（ＤＡＳＨ）コンテンツに対するアクセスについて、前記クライアントを承認するステップと、
前記ＧＢＡベースの認証および承認プロシージャを使用して、前記クライアントが成功

裡に認証および承認される場合に、前記ＮＡＦから、前記クライアントに対して前記ＤＡＳＨコンテンツを配信するステップ、
を実施する、コンピュータプログラム。
【請求項１４】
前記一つまたはそれ以上のプロセッサによってインストラクションが実行されると、さらに、
ＤＡＳＨサービスプロバイダのためにオペレータネットワーク認証および承認を提供するステップ、
を実施する、請求項１３に記載のコンピュータプログラム。
【請求項１５】
前記一つまたはそれ以上のプロセッサによってインストラクションが実行されると、さらに、
ＤＡＳＨメディア表現記述（ＭＰＤ）におけるＤＡＳＨサービスプロバイダの認証および承認ポリシを受け取るステップ、
を実施する、請求項１３に記載のコンピュータプログラム。
【請求項１６】
前記一つまたはそれ以上のプロセッサによってインストラクションが実行されると、さらに、
前記クライアントに関するストリーミング計画の対象である前記ＤＡＳＨコンテンツに対するアクセスについて、前記クライアントを承認するステップ、を実施し、
前記ストリーミング計画は、前記クライアントにおいて前記ＤＡＳＨコンテンツをアクセスするために許容可能なビットレートおよび解像度を記述している、
請求項１３に記載のコンピュータプログラム。
【請求項１７】
前記一つまたはそれ以上のプロセッサによってインストラクションが実行されると、さらに、
コンテンツ配信精度に係る定められたレベルを確保するために、配信されたＤＡＳＨコンテンツの整合性を検証するステップ、
を実施する、請求項１３に記載のコンピュータプログラム。
【請求項１８】
前記一つまたはそれ以上のプロセッサによってインストラクションが実行されると、さらに、
ＤＡＳＨコンテンツ情報に対するＤＡＳＨメディア表現記述（ＭＰＤ）の整合性を検証するステップ、
を実施する、請求項１３に記載のコンピュータプログラム。
【請求項１９】
ネットワークアプリケーションファンクション（ＮＡＦ）を含むサーバーであって、前記サーバーは、一つまたはそれ以上のプロセッサとメモリとを含み、
前記一つまたはそれ以上のプロセッサとメモリは、
前記ＮＡＦを使用し、汎用ブートストラップアーキテクチャ（ＧＢＡ）ベースの認証および承認プロシージャを使用して、クライアントを認証し、
前記ＮＡＦを使用し、前記ＧＢＡベースの認証および承認プロシージャを使用して、コンテンツ特定ポリシ情報の対象であるダイナミックアダプティブストリーミング・オーバーハイパーテキストトランスファープロトコル（ＨＴＴＰ）（ＤＡＳＨ）コンテンツに対するアクセスについて、前記クライアントを承認する、
ように構成されており、
前記サーバーは、さらに、
前記ＧＢＡベースの認証および承認プロシージャを使用して、前記クライアントが成功裡に認証および承認される場合に、前記クライアントに対して前記ＤＡＳＨコンテンツを配信する、

ように構成されている、サーバー。
【請求項２０】
前記一つまたはそれ以上のプロセッサとメモリは、さらに、
前記ＮＡＦを使用し、前記コンテンツ特定ポリシ情報を含むＤＡＳＨコンテンツ情報のためのＤＡＳＨメディア表現記述（ＭＰＤ）をパースするように構成されている、
請求項１９に記載のサーバー。
【請求項２１】
前記一つまたはそれ以上のプロセッサとメモリは、さらに、
前記ＮＡＦを使用し、ＤＡＳＨコンテンツ情報のユニフォームリソースロケータ（ＵＲＬ）を含むＤＡＳＨコンテンツ情報のためのＤＡＳＨメディア表現記述（ＭＰＤ）をパースするように構成されており、
前記ＤＡＳＨコンテンツ情報のＵＲＬは、ＤＡＳＨ　ＭＰＤ、期間、適合セット、または、表現レベルに対するベースＵＲＬを認証するために使用され、そうでなければ、
前記ＤＡＳＨコンテンツ情報のＵＲＬは、前記ＭＰＤのセグメントＵＲＬを認証するために使用される、
請求項１９に記載のサーバー。
【請求項２２】
前記一つまたはそれ以上のプロセッサとメモリは、さらに、
前記ＮＡＦを使用して、ＮＡＦ鍵マテリアル、プロフィール、ブートストラップ時間、または、鍵の有効期間を含んでいるブートストラップサーバーファンクション（ＢＳＦ）からセッション鍵を取得し、もしくは、
前記ＮＡＦを使用して、ＤＡＳＨコンテンツ情報に対するＮＡＦ鍵マテリアルを含んでいる前記ＢＳＦからコンテンツ鍵を取得する、
ように構成されている、
請求項１９に記載のサーバー。
【請求項２３】
前記一つまたはそれ以上のプロセッサとメモリは、さらに、
前記ＮＡＦを使用し、前記クライアントに関するストリーミング計画の対象である前記ＤＡＳＨコンテンツに対するアクセスについて、前記クライアントを承認するように構成されており、
前記ストリーミング計画は、前記クライアントにおいて前記ＤＡＳＨコンテンツをアクセスするために許容可能なビットレートおよび解像度を記述している、
請求項１９に記載のサーバー。
【請求項２４】
前記一つまたはそれ以上のプロセッサとメモリは、さらに、
前記ＮＡＦを使用し、コンテンツ配信精度に係る定められたレベルを確保するために、配信されたＤＡＳＨコンテンツの整合性し、もしくは、
前記ＮＡＦを使用し、ＤＡＳＨコンテンツ情報に対するＤＡＳＨメディア表現記述（ＭＰＤ）の整合性を検証する、
ように構成されている、
請求項１９に記載のサーバー。
【請求項２５】
前記一つまたはそれ以上のプロセッサとメモリは、さらに、
前記ＤＡＳＨコンテンツおよびメディア表現記述（ＭＰＤ）におけるＤＡＳＨコンテンツ情報ロケーションについてＤＡＳＨ認証情報を受け取り、前記ＤＡＳＨ認証情報は、署名と認証鍵を含み、かつ、前記ＤＡＳＨコンテンツ情報ロケーションは、ＤＡＳＨコンテンツ情報のユニフォームリソースロケータ（ＵＲＬ）を含み、かつ、
前記ＮＡＦを使用し、受け取った前記ＤＡＳＨ認証情報と受け取った前記ＤＡＳＨコンテンツ情報とに基づいて、前記ＤＡＳＨコンテンツに対するアクセスについて、前記クライアントを承認する、

ように構成されている、
請求項１９に記載のサーバー。
【請求項２６】
請求項１３乃至１８いずれか一項に記載のコンピュータプログラムを記憶したコンピュータで読取り可能な記憶媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、Ｄ－ＮＡＦに関する。
【０００２】
本特許出願は、２０１３年1月１７日に出願された米国仮特許出願第６１／７５３９１４号、代理人整理番号Ｐ５３５０４Ｚ、に係る優先権を主張するものであり、ここにおいて参照として包含されている。本特許出願は、２０１３年5月９日に出願された米国仮特許出願第６１／８２１６３５号、代理人整理番号Ｐ５６６１８Ｚ、に係る優先権を主張するものであり、ここにおいて参照として包含されている。本特許出願は、２０１３年5月１６日に出願された米国仮特許出願第６１／８２４３３８号、代理人整理番号Ｐ５６２８２Ｚ、に係る優先権を主張するものであり、ここにおいて参照として包含されている。
【背景技術】
【０００３】
無線モバイル通信技術は、ノード（例えば、送信局）と無線機器（例えば、モバイル機器）との間でデータを送信するために、種々の規格およびプロトコルを使用する。いくつかの無線機器は、ダウンリンク（ＤＬ）送信における直交周波数分割多次元接続（ＯＦＤＭＡ）、および、アップリンク（ＵＬ）送信におけるシングルキャリア周波数分割多次元接続（ＳＣ－ＦＤＭＡ）を使用して通信する。信号送信のために直交周波数分割多次元接続（ＯＦＤＭＡ）を使用する規格およびプロトコルは、以下のものを含んでいる。第３世代パートナーシッププロジェクト（３ＧＰＰ）ロングタームエボリューション（ＬＴＥ）、米国電気電子学会（ＩＥＥＥ）８０２．１６規格（例えば、８０２．１６ｅ、８０２．１６ｍ）、つまりＷｉＭＡＸ（Ｗｏｒｌｄｗｉｄｅ ｉｎｔｅｒｏｐｅｒａｂｉｌｉｔｙ ｆｏｒ Ｍｉｃｒｏｗａｖｅ Ａｃｃｅｓｓ）として一般的に業界団体に知られているもの、および、ＩＥＥＥ８０２．１１規格、つまりＷｉＦｉとして一般的に業界団体に知られているもの、である。
【０００４】
３ＧＰＰの無線アクセスネットワーク（ＲＡＮ）ＬＴＥシステムにおいて、ノードは、エボルブド・ユニバーサル・テレストリアル・無線アクセスネットワーク（Ｅｖｏｌｖｅｄ Ｕｎｉｖｅｒｓａｌ Ｔｅｒｒｅｓｔｒｉａｌ Ｒａｄｉｏ Ａｃｃｅｓｓ Ｎｅｔｗｏｒｋ：Ｅ－ＵＴＲＡＮ）のＮｏｄｅＢ（ｅｖｏｌｖｅｄＮｏｄｅＢ、ｅｎｈａｎｃｅｄＮｏｄｅＢ、ｅＮｏｄｅＢ、またはｅＮＢとしても一般的に示されるもの）と、無線ネットワークコントローラ（Ｒａｄｉｏ Ｎｅｔｗｏｒｋ Ｃｏｎｔｒｏｌｌｅｒ：ＲＮＣ）、つまり、無線機器と通信し、ユーザ機器（ＵＥ）として知られているもの、との組合せであってよい。ダウンリンク（ＤＬ）送信は、ノード（例えば、ｅＮｏｄｅＢ）から無線機器（例えば、ＵＥ）への通信であり、かつ、アップリンク（ＵＬ）送信は、無線機器からノードへの通信であってよい。
【０００５】
無線機器は、ハイパーテキストトランスファープロトコル（ｈｙｐｅｒｔｅｘｔ ｔｒａｎｓｆｅｒ ｐｒｏｔｏｃｏｌ：ＨＴＴＰ）といった、種々のプロトコルを使用して、インターネットビデオのマルチメディア配信を受信するように使用され得る。ビデオストリーミングに係るＨＴＴＰベースの配信を提供するためのプロトコルは、ダイナミックアダプティブストリーミング・オーバーＨＴＴＰ（ｄｙｎａｍｉｃ ａｄａｐｔｉｖｅ ｓｔｒｅａｍｉｎｇ ｏｖｅｒ ＨＴＴＰ：ＤＡＳＨ）を含み得る。

【図面の簡単な説明】
【０００６】
本発明開示の特徴と利点が、以降の詳細な説明から明らかになり、添付の図面と併せて理解される。図面は、例として、本発明開示の特徴を共に説明するものである。
【図１】図１は、一つの実施例に従って、ダイナミックアダプティブストリーミング・オーバー・ハイパーテキストトランスファープロトコル（ＨＴＴＰ）（ＤＡＳＨ）のためのクライアントとサーバーにおけるブロックダイヤグラムを示している。
【図２】図２は、一つの実施例に従って、メディア表現記述（ｍｅｄｉａ　ｐｒｅｓｅｎｔａｔｉｏｎ　ｄｅｓｃｒｉｐｔｉｏｎ：ＭＰＤ）のメタデータファイルコンフィグレーションに係るブロックダイヤグラムを示している。
【図３】図３は、一つの実施例に従って、第３世代パートナーシッププロジェクト（ｔｈｉｒｄ　ｇｅｎｅｒａｔｉｏｎ　ｐａｒｔｎｅｒｓｈｉｐ　ｐｒｏｊｅｃｔ：３ＧＰＰ）の汎用認証アーキテクチャ（ｇｅｎｅｒｉｃ　ａｕｔｈｅｔｉｃａｔｉｏｎ　ａｒｃｈｉｔｅｃｔｕｒｅ：ＧＡＡ）ネットワークのエンティティとインターフェイスを示している。
【図４】図４は、一つの実施例に従って、ブートストラップ認証（ｂｏｏｔｓｔｒａｐｉｎｇ　ａｕｔｈｅｔｉｃａｔｉｏｎ）プロセスに係るメッセージフローチャートの例を示している。
【図５】図５は、一つの実施例に従って、ブートストラップ使用プロセスに係るメッセージフローチャートの例を示している。
【図６】図６は、一つの実施例に従って、汎用ブートストラップアーキテクチャベース（ＧＢＡ－ｂａｓｅｄ）の認証プロセスに係るフローチャートの例を示している。
【図７】図７は、一つの実施例に従って、第３世代パートナーシッププロジェクト（３ＧＰＰ）の汎用認証アーキテクチャ（ＧＡＡ）におけるダイナミックアダプティブストリーミング・オーバー・ハイパーテキストトランスファープロトコル（ＨＴＴＰ）アウェア（ＤＡＳＨ－ａｗａｒｅ）ネットワークアプリケーションファンクション（Ｄ－ＮＡＦ）の例を示している。
【図８】図８（つまり、テーブル２）は、一つの実施例に従って、コモングループの拡張可能マークアップ言語シンタックス（ｅｘｔｅｎｓｉｂｌｅ　ｍａｒｋｕｐ　ｌａｎｇｕａｇｅ－ｓｙｎｔａｘ：ＸＭＬ－ｓｙｎｔａｘ）、および、ＵＲＬ認証（ＵｒｌＡｕｔｈｅｎｔｉｃｉｔｙ）エレメントを含む属性とエレメントの表現、に係るテーブルを示している。
【図９】図９（つまり、テーブル４）は、一つの実施例に従って、コモングループの拡張可能マークアップ言語シンタックス（ＸＭＬ－ｓｙｎｔａｘ）、および、コンテンツ承認（ＣｏｎｔｅｎｔＡｕｔｈｏｒｉｚａｔｉｏｎ）エレメントを含む属性とエレメントの表現、に係るテーブルを示している。
【図１０】図１０は、一つの実施例に従って、ダイナミックアダプティブストリーミング・オーバー・ハイパーテキストトランスファープロトコル（ＨＴＴＰ）アウェア（ＤＡＳＨ－ａｗａｒｅ）ネットワークアプリケーションファンクション（Ｄ－ＮＡＦ）に係るコンピュータ回路の機能性を示している。
【図１１】図１１は、一つの実施例に従って、ハイパーテキストトランスファープロトコル（ＨＴＴＰ）またはダイナミックアダプティブストリーミング・オーバーＨＴＴＰ（ＤＡＳＨ）プロキシを使用した、コンテンツ特定認証を提供するための方法に係るフローチャートを示している。
【図１２】図１２は、一つの実施例に従って、ダイナミックアダプティブストリーミング・オーバー・ハイパーテキストトランスファープロトコル（ＨＴＴＰ）アウェア（ＤＡＳＨ－ａｗａｒｅ）ネットワークアプリケーションファンクション（Ｄ－ＮＡＦ）、ノード（例えば、ｅＮＢ）、および、ユーザ機器（ＵＥ）に係るダイヤグラムを示している。
【図１３】図１３は、一つの実施例に従って、無線機器（例えば、ＵＥ）のダイヤグラムを示している。

【０００７】
これから、図示された典型的な実施例が参照され、同一のものを記述するように特定の言葉がここにおいて使用される。しかしながら、それによる本発明の範囲の限定は意図されていないことが理解されよう。
【発明を実施するための形態】
【０００８】
本発明が開示され、説明される前に、本発明は、ここにおいて開示される特定の構成、プロセス段階、または、マテリアルに限定されるものではなく、当業者にとって認識されるように、その均等物まで拡張されることが理解されるべきである。ここにおいて使用される用語は、所定の実施例を説明する目的だけに使用されるものであり、限定することを意図するものではないことも理解されるべきである。異なる図面における同一の参照番号は、同一のエレメントを表している。フローチャートおよびプロセスにおいて提供される番号は、ステップおよびオペレーションを明らかにするために提供されるものであり、特定の順序またはシーケンスを必ずしも示すものではない
【０００９】
最初に本技術の実施例に係る概要が以下に提供され、次に、より詳細に所定の技術の実施例が以降に説明される。この最初の概要は、読者が本技術をより速く理解することを手助けするよう意図されたものであり、本技術の主要な特徴または根本的な特徴を特定することを意図するものではなく、また、特許請求の範囲を限定することを意図するものでもない。
【００１０】
ハイパーテキストトランスファープロトコル（ＨＴＴＰ）ストリーミングは、インターネットビデオのマルチメディア配信の形態として使用され得る。ＨＴＴＰストリーミングにおいて、マルチメディアファイルは一つまたはそれ以上のセグメントに分割され、ＨＴＴＰプロトコルを使用してクライアントに配信され得る。ＨＴＴＰベース配信は、ＨＴＴＰおよびＨＴＴＰの根底にあるプロトコル両方が広く使用されているために、信頼性と配置の簡潔性を提供し得る。プロトコルは、トランスミッションコントロールプロトコル（ｔｒａｎｓｍｉｓｓｉｏｎ ｃｏｎｔｒｏｌ ｐｒｏｔｏｃｏｌ：ＴＣＰ）／インターネットプロトコル（ｉｎｔｅｒｎｅｔ ｐｒｏｔｏｃｏｌ：ＩＰ）を含んでいる。ＨＴＴＰベースの配信により、ネットワークアドレス変換（ＮＡＴ）とファイアウォールのトラバーサル（ｔｒａｖｅｒｓａｌ）問題を回避することによって、容易かつ努力を要しないストリーミングサーバーが可能となる。ＨＴＴＰベースの配信またはストリーミングは、また、特化したストリーミングサーバーの代わりに、標準のＨＴＴＰサーバーとキャッシュを使用する可能性を提供することもできる。ＨＴＴＰベースの配信は、サーバー側における最小限または削減された状態情報のおかげで、スケーラビリティ（ｓｃａｌａｂｉｌｉｔｙ）を提供することができる。ＨＴＴＰストリーミング技術の実施例は、マイクロソフト社のＩＩＳ Ｓｍｏｏｔｈ Ｓｔｒｅａｍｉｎｇ、アップル社のＨＴＴＰ Ｌｉｖｅ Ｓｔｒｅａｍｉｎｇ、および、アドビ社のＨＴＴＰ Ｄｙｎａｍｉｃ Ｓｔｒｅａｍｉｎｇ、を含み得る。
【００１１】
ダイナミックアダプティブストリーミング・オーバーＨＴＴＰ（ＤＡＳＨ）は、標準化されたＨＴＴＰストリーミングプロトコルであってよい。ＤＡＳＨにおいて、メディア表現記述（ｍｅｄｉａ ｐｒｅｓｅｎｔａｔｉｏｎ ｄｅｓｃｒｉｐｔｉｏｎ：ＭＰＤ）メタデータファイルは、サーバーに保管されたメディアコンテンツ表現の構成および異なるバージョンに関する情報を提供することができる。異なるビットレート、フレームレート、解像度、または、コーデックタイプを含むものである。加えて、ＤＡＳＨは、セグメントフォーマットを特定することができる。ＭＰＤメタデータファイルは、メディアプレーヤのための初期化およびメディアセグメントに関する情報を含んでおり（例えば、メディアプレーヤは、コンテナ（ｃｏｎｔａｉｎｅｒ）フォーマットおよびメディアタイミング情報を決定するために初期化セグメントを観察することができる）、スイッチングおよび

他の表現と同期した表現のために、セグメントのメディア表現タイムラインへのマッピングを保証し得る。メディア表現の形成におけるセグメントの関係を記述する、このＭＰＤメタデータに基づいて、クライアント（またはクライアント機器）は、ＨＴＴＰ　ＧＥＴまたは部分的ＧＥＴ方法を使用してセグメントをリクエストすることができる。クライアントは、ストリーミングセッションを完全にコントロールすることができる。例えば、クライアントは、オンタイムリクエスト（ｏｎ－ｔｉｍｅ　ｒｅｑｕｅｓｔ）とセグメントのシーケンスに係るスムーズな演奏を管理することができ、潜在的に、ビットレートまたは他の属性を調整している（例えば、デバイス状態またはユーザープリファレンスの変更に対して反応する）。ＤＡＳＨ技術は、また、他の組織によっても標準化されてきている。Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ（ＭＰＥＧ）、Ｏｐｅｎ　ＩＰＴＶ　Ｆｏｒｕｍ（ＯＩＰＦ）、および、Ｈｙｂｒｉｄ　Ｂｒｏａｄｃａｓｔ　Ｂｒｏａｄｂａｎｄ　ＴＶ（ＨｂｂＴＶ）といったものである。

【００１２】

ＤＡＳＨクライアントは、一連のＨＴＴＰ要求－応答（ｒｅｑｕｅｓｔ－ｒｅｓｐｏｎｓｅ）トランザクションを通じてセグメントをダウンロードすることによって、マルチメディアコンテンツを受信することができる。ＤＡＳＨは、利用可能なバンド幅の変更として、メディアコンテンツに係る異なるビットレート表現の間を動的にスイッチする機能を提供する。このように、ＤＡＳＨにより、ネットワークと無線リンクの状況、ディスプレイ解像度といった、ユーザープロセッサリファレンスとデバイス能力、使用される中央処理装置（ＣＰＵ）のタイプ、または、利用可能なメモリリソース、等の変化に対して、素早い適用ができる。

【００１３】

ＤＡＳＨにおいて、メディア表現記述（ＭＰＤ）メタデータファイルは、図１に示されるように、ウェブ及び/又はメディアサーバー２１２に保管されたメディアコンテンツ表現の構成および異なるバージョンに関する情報を提供することができる。メディアコンテンツ表現の異なるバージョンは、異なるビットレート、フレームレート、解像度、コーデックタイプ、または、他の同様な情報のタイプを含み得る。加えて、ＤＡＳＨは、また、セグメントフォーマットを特定することができる。セグメントフォーマットは、メディアエンジンのための初期化およびメディアセグメントに関する情報を含んでおり、スイッチングおよび他の表現と同期した表現のために、セグメントのメディア表現タイムラインへのマッピングを保証することができる。セグメントの関係およびセグメントがどのようにメディア表現を形成するかを記述する、ＭＰＤメタデータ情報に基づいて、クライアント２２０は、ＨＴＴＰ　ＧＥＴ２４０メッセージまたは一連の部分的ＧＥＴメッセージを使用して、セグメントをリクエストすることができる。クライアントは、ストリーミングセッションをコントロールすることができる。オンタイムリクエストとセグメントのシーケンスに係るスムーズな演奏を管理すること、または、潜在的に、ビットレートまたは他の属性を調整して、デバイス状態またはユーザープリファレンスの変更に対して反応する、といったことである。

【００１４】

図１は、ＤＡＳＨベースストリーミングフレームワークを示している。ウェブ／メディアサーバー２１２におけるメディアエンコーダ２１４は、オーディオ／ビデオ入力２１０からの入力メディアをストレージまたはストリーミングのためのフォーマットへと符号化することができる。メディアセグメンタ（ｍｅｉａ　ｓｅｇｍｅｎｔｅｒ）２１６は、入力メディアを一連のフラグメント（ｆｒａｇｍｅｎｔ）またはチャンク（ｃｈｕｎｃｋ）２３２へと分割するために使用され得る。フラグメントまたはチャンクは、ウェブサーバー２１８に提供される。クライアント２２０は、ウェブサーバー（例えば、ＨＴＴＰサーバー）に対して送信されたＨＴＴＰ　ＧＥＴメッセージ２３４を使用して、チャンクにおける新たなデータをリクエストすることができる。

【００１５】

例えば、クライアント２２０のウェブブラウザ２２２は、ＨＴＴＰ　ＧＥＴメッセージ

２４０を使用して、マルチメディアコンテンツをリクエストすることができる。ＭＰＤは、関連するメタデータ情報において示されるように、それぞれのセグメントおよびセグメントに対応するロケーションを伝送するために使用され得る、２５２。２３６において示されるように、ウェブブラウザは、ＭＰＤ２４２に従ったセグメントによって、サーバーセグメントからメディアをプル（ｐｕｌｌ）することができる。例えば、ウェブブラウザは、ＨＴＴＰ　ＧＥＴ　ＵＲＬ（ｆｒａｇ　１　ｒｅｑ）２４４を使用して、第１のフラグメントをリクエストすることができる。ユニフォームリソースロケータ（ｕｎｉｆｏｒｍ　ｒｅｓｏｕｒｃｅ　ｌｏｃａｔｏｒ：ＵＲＬ）またはユニバーサルリソースロケータは、クライアントがどのセグメントをリクエストするかをウェブサーバーに知らせる（ｔｅｌｌ）ために使用され得る、２５４。ウェブサーバーは、第１のフラグメント（つまり、フラグメント１　２４６）を提供することができる。後続のフラグメントに対して、ウェブブラウザは、ＨＴＴＰ　ＧＥＴ　ＵＲＬ（ｆｒａｇ　１　ｒｅｑ）２４８を使用して、フラグメントｉをリクエストすることができる。ここで、ｉはフラグメントの整数インデックスである。フラグメントは、メディアデコーダ及び/又はプレーヤ２２４を介して、クライアントに対して表示され得る。

【００１６】

図２に示されるように、ＤＡＳＨは、サーバーに保管されたメディアコンテンツ表現の構成および異なるバージョンに関する情報を提供するメディア表現記述（ＭＰＤ）メタデータファイル４０２のための異なるフォーマットを特定することができる。セグメントフォーマット（またはフラグメントフォーマット）も同様である。ＤＡＳＨにおいて、メディア表現記述（ＭＰＤ）メタデータ４０２は、ウェブ及び/又はメディアサーバーに保管されたメディアコンテンツ表現の構成および異なるバージョンに関する情報を提供することができる。例えば、図２に示されるように、ＭＰＤメタデータは、既定の長さを有する期間４０４へと一時的に分割され得る。この実施例においては、６０秒といったものである。それぞれの期間は、複数の適合セット（ａｄａｐｔａｔｉｏｎ　ｓｅｔ）４０６を含み得る。それぞれの適合セットは、多くの符号化された選択肢（ａｌｔｅｒｎａｔｉｖｅ）を伴う一つまたはそれ以上のメディアコンポーネントに関する情報を提供することができる。例えば、この実施例における適合セット０は、種々の異なって符号化されたオーディオ選択肢を含んでよい。異なるビットレート、ステレオ、サラウンド音、等といったものである。期間ＩＤに対するマルチメディア表現のための異なる品質オーディオを提供することに加えて、適合セットは、また、異なる言語におけるオーディオを含み得る。適合セットにおいて提供される異なる選択肢は、表現（ｒｅｐｒｅｓｅｎｔａｔｉｏｎ）４０８として参照される。

【００１７】

図２において、適合セット１は、異なるビットレートにおけるビデオを提供するものとして示されている。５メガビット毎秒（Ｍｂｐｓ）、２Ｍｂｐｓ、５００キロビット毎秒（ｋｂｐｓ）、または、トリックモードといったものである。トリックモードは、検索（ｓｅｅｋｉｎｇ）、早送り（ｆａｓｔ　ｆｏｒｗａｒｄｉｎｇ）、巻戻し（ｒｅｗｉｎｄｉｎｇ）、または、マルチメディアストリーミングファイルにおけるロケーションの他の変更のために使用され得る。加えて、ビデオは、また、異なるフォーマットにおいても利用可能であり得る。２次元（２Ｄ）または３次元（３Ｄ）、もしくは、ポートレートまたは風景指向のビデオ、といったものである。それぞれの表現４０８は、セグメント情報４１０を含み得る。セグメント情報は、初期化情報４１２と実際のメディアセグメントデータ４１４を含み得る。この実施例において、ＭＰＥＧ－４（ＭＰ４）ファイルが、サーバーからモバイル機器までストリーミングされる。この実施例においてはＭＰ４が使用される一方で、幅広く種々の異なるコーデックが使用され得る。コーデックは、デジタルデータストリーミムまたは信号を符号化または復号化することができるデバイス、アプリケーション、エレメント、または、コンピュータプログラムである。

【００１８】

適合セットにおけるマルチメディアは、さらに、より小さなセグメントへと分割される

。図２の実施例においては、適合セット１の６０秒セグメントが、さらに、それぞれ１５秒の４つのサブセグメント４１４に分割される。これらの実施例は、限定を意図するものではない。適合セット及びそれぞれのメディアセグメントまたはサブセグメントの実際の長さは、メディアのタイプ、システムリクエスト、可能性のあるインターフェイスのタイプ、等に依存するものである。実際のメディアセグメントまたはサブセグメントは、１秒から数秒よりも少ない長さを有し得る。

【００１９】

ＤＡＳＨ標準は、セグメント認証フレームワークを含むことができ、オリジン（ｏｒｉｇｉｎ）およびコンテンツの信頼性を確認するために、ＤＡＳＨセグメントタイプに対するデジタル署名またはダイジェストを使用することができる。署名（またはダイジェスト）は、メディアセグメントまたはメディアサブセグメントに対して提供され得る。初期化、インデックス、および、ビットストリームスイッチングセグメントに対しても同様である。ここにおいて使用されるように、署名およびダイジェストという用語は、同一の特徴またはエレメントに対して互換的に使用され得るものである。セグメント認証フレームワークは、非暗号化セグメントの署名を計算することができ、その値を外部に保管する。ＭＰＤインターフェイスは、ＨＴＴＰまたはセキュアＨＴＴＰ（ＨＴＴＰＳ）を使用して、署名を取得するためのＵＲＬテンプレートを提供することができる。ＨＴＴＰＳは、コンピュータネットワーク上でのセキュア（ｓｅｃｕｒｅ）な通信のための通信プロトコルであり、インターネット上で特に広く展開されている。クライアントは、署名を取得して、次に、検証鍵（ｖａｌｉｄａｔｉｏｎ　ｋｅｙ）を使用して非暗号化メディアセグメントまたはサブセグメント上でローカルに署名を計算し、そして、取得した署名と計算された署名との間で不一致がある場合には、そのメディアセグメントまたはサブセグメントを拒否することができる。拒否されたメディアセグメントまたはサブセグメントは、クライアント機器において視聴または再生されない。

【００２０】

セグメント認証フレームワークは、３ＧＰＰ汎用認証アーキテクチャ（ＧＡＡ）において実施され得る。モバイル機器のオーナーは、ある種の認証（つまり、通信の秘匿性の保証、内容完全性（ｃｏｎｔｅｎｔ　ｉｎｔｅｇｒｉｔｙ）、および、クライアント及び/又はサーバーの識別確認（ｉｄｅｎｔｉｔｙ　ｖａｌｉｄａｔｉｏｎ）に対するもの）を使用して異なるサービスにアクセスすることができる。ＧＡＡは、インターネットまたは携帯電話会社ネットワーク上でクライアント（またはクライアント機器）とサービスとの間での認証および鍵共有（ｋｅｙ　ａｇｒｅｅｍｅｎｔ）を提供することができる。ＧＡＡは、携帯ネットワーク会社によって提供される認証サービスであってよく、クライアントとサービスはお互いに認証することができる。ユーザ認証は、共有秘密鍵（ｓｈａｒｅｄ　ｓｅｃｒｅｔ）によってインスタンス化され得る。共有秘密鍵は、図３に示されるように、クライアント機器（例えば、ＵＥ１２０）の内部のスマートカードの中、および、ホーム加入者サーバー（ｈｏｍｅ　ｓｕｂｓｃｒｉｂｅｒ　ｓｅｒｖｅｒ；ＨＳＳ）１３０上の両方に置かれ得るものである。ＧＡＡは、ネットワークコンポーネントをスマートカードにチャレンジ（ｃｈａｌｌｅｎｇｅ）させて、かつ、回答（ａｎｓｗｅｒ）が、ＨＳＳによって予測された回答と同様であることを検証させることによって、認証を行うことができる。ＧＡＡは、ネットワークとユーザ側の両方においてアプリケーション機能が共有鍵を確立できるようにするために活用され得る。例えば、３ＧＰＰは、アプリケーションセキュリティのブートストラップ（”ｂｏｏｔｓｔｒａｐｐｉｎｇ　ｏｆ　ａｐｐｌｉｃａｔｉｏｎ　ｓｅｃｕｒｉｔｙ”）」を提供することができ、認証と鍵生成（ａｕｔｈｅｔｉｃａｔｉｏｎ　ａｎｄ　ｋｅｙ　ａｇｒｅｅｍｅｎｔ：ＡＫＡ）プロトコルに基づいて、汎用ブートストラップアーキテクチャ（ｇｅｎｅｒｉｃ　ｂｏｏｔｓｔｒａｐｐｉｎｇ　ａｒｃｈｉｔｅｃｔｕｒｅ：ＧＢＡ）を定めることによって加入者を認証する。

【００２１】

非対称暗号（ａｓｙｍｍｅｔｒｉｃ　ｃｒｙｐｔｏｇｒａｐｈｙ）は、公開鍵（ｐｕｂｌｉｃ－ｋｅｙ）暗号としても知られているが、２つの別個のかぎを使用する暗号アルゴ

リズムを参照し得る。ここで、一つの鍵は秘密鍵（またはプライベート鍵）であり、もう一つの鍵は、公開鍵である。秘密鍵と公開鍵は異なるが、この鍵ペアの２つの部分は、数学的にリンクされ得るものである。公開鍵は、平文（ｐｌａｉｎｔｅｘｔ）を暗号化するため、または、デジタル署名を検証するために使用され得る。一方、秘密鍵は、暗号文（ｃｉｐｈｅｒｔｅｘｔ）を復号化するため、または、デジタル署名を作成するために使用され得る。用語「非対称（”ａｓｙｍｍｅｔｒｉｃ”）」は、こうした反対の機能を実行するための異なる鍵の使用を参照し得る。ここで、それぞれの機能は、他の機能の逆であってよい。対照的に、従来の、又は「対称（”ｓｙｍｍｅｔｒｉｃ”）」暗号は、暗号化と復号化の両方を実行するために同一の鍵に依存することができる。

【００２２】

ＧＡＡは、共通鍵ベースの認証を使用するクライアントとサーバーのために、フレッシュな鍵マテリアル（ｋｅｙ　ｍａｔｅｒｉａｌ）を提供することができ、かつ、ＧＡＡは、非対称認証を使用し得るそうしたアプリケーションに対する証明書に署名することができる。ＵＥ１２０は、既存の第３世代（３Ｇ）または第２世代（２Ｇ）認証プロトコルを使用して、オペレータのＧＡＡサービスに対して自分自身を認証することができ、かつ、認証のプロセスにおいて、新たな鍵を受け取ることができる。ユーザ（例えば、ＵＥ）が使用したいサービスは、また、ＧＡＡから鍵をフェッチ（ｆｅｔｃｈ）することもできる。結果として、クライアントとサーバーは、鍵（または秘密鍵）を共有することができる。他のサービスに加えて、ＧＡＡは、また、公開鍵インフラストラクチャ（ＰＫＩ）に対してクライアントを認証するためにも使用され得る。そのインフラストラクチャは、次に、クライアントの公開鍵に対する証明書に署名するように求められ得る。

【００２３】

ＧＡＡは、少なくとも２つの異なるプロセスのうち一つを使用してユーザを認証することができる。第１ＧＡＡ認証プロセスは、クライアントとサーバーとの間の共有秘密鍵に基づくものであり得る。第２ＧＡＡ認証プロセスは、公開鍵と秘密鍵のペアおよびデジタル証明書に基づくものであり得る。共有秘密鍵のプロセス（つまり、第１プロセス）において、クライアント（例えば、ＵＥ１２０）とオペレータは、最初に、３Ｇ認証と鍵生成（ＡＫＡ）を用いて相互に認証され得る。そして、クライアントとオペレータはセッション鍵が一致し得る。セッション鍵は、後に、クライアントとクライアントが使用を欲するサービス（つまり、ネットワークアプリケーションファンクション（ＮＡＦ）におけるもの）との間で使用され得るものである。第１プロセスは、ブートストラップとして参照され得る。ブートストラップ（または、ブーティング（ｂｏｏｔｉｎｇ））は、外部ヘルプなしに進行し得る自立したプロセスを参照するメタファ（ｍｅｔａｐｈｏｒ）のグループを参照することができる。ブートストラッププロシージャの後で、サービスは、オペレータからセッション鍵をフェッチすることができ、セッション鍵は、クライアントとサービスとの間のいくつかのアプリケーション特定プロトコルにおいて使用され得る。

【００２４】

第２ＧＡＡ認証プロセスにおいて、ＧＡＡは、証明書登録（ｃｅｒｔｉｆｉｃａｔｅ　ｅｎｒｏｌｌｍｅｎｔ）リクエストを認証するためクライアントによって使用され得る。最初に、ブートストラッププロシージャが、第１ＧＡＡ認証プロセスのように実行され得る。このブートストラッププロシージャの後で、クライアントは、オペレータの公開鍵インフラストラクチャ（ＰＫＩ）からの証明書をリクエストすることができる。ここでは、ブートストラッププロシージャを完遂することにより取得されたセッション鍵によって認証が実行され得る。これらの証明書および対応する鍵ペアは、次に、デジタル署名を生成するため、または、セッション鍵を使用する代わりにサーバーに対して認証するために使用され得る。ＰＫＩは、一式のハードウェア、ソフトウェア、ピープル（ｐｅｏｐｌｅ）、ポリシ、および、デジタル証明書を作成、管理、配信、使用、保管、および、リボーク（ｒｅｖｏｋｅ）するために使用されるプロシージャ、を含み得る。

【００２５】

ブートストラップサーバーファンクション（ＢＳＦ）１３２は、コンテンツに対するユ

ーザおよびユーザ資格情報（ｕｓｅｒ　ｃｒｅｄｅｎｔｉａｌｓ）へのアクセスを承認するために使用され得る。ＢＳＦは、Ｚｈインターフェイスを使用したＨＳＳとのインターフェイスを有している。ＵＥ１２０は、ＢＳＦを介してＨＳＳ１３０を用いてＡＫＡプロトコルを実行することができる。ＡＫＡプロトコルは、暗号鍵（ｃｉｐｈｅｒ　ｋｅｙ：ＣＫ）及び/又は整合性鍵（ｉｎｔｅｇｒｉｔｙ　ｋｅｙ；ＩＫ）を結果として生じ得る。結果として生じたＣＫおよびＩＫから、ＢＳＦおよびＵＥにおいてセッション鍵が引き出され得る。アプリケーションサーバー（３ＧＰＰ技術仕様書（ＴＳ）３３．２２０Ｖ１１．４．０（２０１２－０９）においてネットワークアプリケーションファンクション（ＮＡＦ）として参照されるもの）は、加入者プロフィール情報と供に、ＢＳＦから、このセッション鍵をフェッチすることができる。このようにしてアプリケーションサーバー（ＮＡＦとして動作しているもの）とＵＥは、アプリケーションセキュリティのため以後に使用され得る秘密鍵を共有する。アプリケーションセッションのスタートにおいてＵＥとＮＡＦを認証するといったものである。秘密鍵は、また、整合性及び/又は秘匿性保護のためにも使用され得る。ＧＡＡの範囲および機能性を拡張し得るものである。他のプロトコルの中で、ＨＴＴＰＳまたはＨＴＴＰオーバー・トランスポートレイヤセキュリティ（ｔｒａｎｓｐｏｒｔ　ｌａｙｅｒ　ｓｅｃｕｒｉｔｙ：ＴＬＳ）（またはＨＴＴＰ／ＴＬＳ）が、ＵＥとアプリケーションサーバーとの間のアプリケーションセッションを確保するために使用され得る。認証プロキシ（例えば、Ｚｎプロキシ１１２）は、ＧＡＡ手段を使用してＵＥを認証するためのＴＬＳエンドポイントとして働く（例えば、ＮＡＦとして動作しているプロキシを認証する）。

【００２６】

図３は、いくつかのＧＡＡネットワークエンティティおよびＧＡＡネットワークエンティティ間のインターフェイスを示している。任意的なエンティティが破線を用いて示されており、ネットワーク境界（例えば、ホームネットワーク、信頼されないネットワーク、および、訪問されたネットワーク）が一点鎖線で示されている。ＵＥ１２０とＢＳＦ１３２は、Ｕｂインターフェイス上で相互に自身を認証することができる。ＨＴＴＰダイジェストＡＫＡプロトコルの使用、および、後にＵＥとＮＡＦ１１０との間に適用され得るセッション鍵の一致によるものである。ＵＥは、また、アプリケーションサーバーを含み得る、ＮＡＦとＵａインターフェイス上で通信し、あらゆるアプリケーション特定プロトコルを使用することができる。ＢＳＦは、Ｚｈインターフェイス上でＨＳＳ１３０から加入者データを取得することができ、ｄｉａｍｅｔｅｒベースプロトコルを使用することができる。ＨＳＳは、ユーザ情報（例えば、アイデンティティ、認証鍵、加入、権利、等）とプロフィール（サービスプロフィール、等）を管理することができる。ネットワークにおいていくつかのＨＳＳが存在する場合、ＢＳＦは、使用するのに適切なＨＳＳを最初に決定してよい。この決定は、ＢＳＦリストに対する既定のＨＳＳを構成すること、または、Ｄｚインターフェイス上で加入者ロケータ機能（ｓｕｂｓｃｒｉｂｅｒ　ｌｏｃａｔｏｒ　ｆｕｎｃｔｉｏｎ：ＳＬＦ）をクエリ（ｑｕｅｒｙ）することのいずれかによって、なされ得る。ＮＡＦは、Ｚｎインターフェイス上でＢＳＦからセッション鍵を取得することができる。ｄｉａｍｅｔｅｒベースプロトコルを使用することもできる。

【００２７】

汎用ブートストラップアーキテクチャ（ＧＢＡ）は、３ＧＰＰ　ＴＳ　３３．２２０において記述され得る。ＧＢＡの使用は、少なくとも２つのプロシージャへと分割され得る。ブートストラップ認証プロシージャとブートストラップ使用プロシージャである。ブートストラップ認証プロシージャは、ホームネットワークに対してクライアントを認証すること、および、鍵マテリアルを引き出すことを含み得る。使用プロシージャにおいて、ＵＥは、どの鍵を使うかをＮＡＦに知らせることができ、そして、ＮＡＦは、次に、特定された鍵をＢＳＦからフェッチすることができる。認証プロシージャは、ＨＴＴＰダイジェストＡＫＡを使用し得る。

【００２８】

少なくとも２つの異なる認証メカニズムがＧＢＡを使用することができる。ＧＢＡ＿Ｍ

ＥおよびＧＢＡ＿Ｕプロシージャ（またはプロセス）を含むものである。ＧＢＡ＿Ｕ（ＧＢＡ　ＵＩＣＣまたはＧＢＡ　ＵＳＩＭ）プロセスは、ＳＩＭアプリケーション（例えば、ＧＢＡ＿ＭＥ）の代わりに、ユニバーサル集積回路カード（ｕｎｉｖｅｒｓａｌ　ｉｎｔｅｇｒａｔｅｄ　ｃｉｒｃｕｉｔ　ｃａｒｄ：ＵＩＣＣ）（つまり、加入者識別モジュール（ＳＩＭ）カード）に係る３Ｇユニバーサル・サブスクライバ・アイデンティティ。モジュール（ｕｎｉｖｅｒｓａｌ　ｓｕｂｓｃｒｉｂｅｒ　ｉｄｅｎｔｉｔｙ　ｍｏｄｕｌｅ：ＵＳＩＭ）アプリケーションの中に鍵を保管することができる。結果として、ＧＢＡ＿Ｕプロセスは、ＧＢＡ＿ＭＥプロセスよりもセキュアであり得る。

【００２９】

図４は、ＧＢＡ＿ＭＥ（ＧＢＡ　ｍｏｂｉｌｅ　ｅｑｕｉｐｍｅｎｔ（ＭＥ））メカニズム（またはプロセス）のためのブートストラップ認証プロシージャに係るメッセージフローチャートを示している。ＧＢＡ＿ＭＥは、３ＧＰＰ　ＴＳ　３３．２２０　Ｆｉｇｕｒｅ４．３と同様なものである。ＧＢＡ＿ＭＥ認証プロシージャは、ＵＥ１２０とＢＳＦ１３２との間に２つの要求－応答ペア（ｒｅｑｕｅｓｔ－ｒｅｓｐｏｎｓｅ　ｐａｉｒ）を含み得る。第１に、ＵＥは、ＵＥのユーザ名（またはユーザアイデンティティ）を用いてリクエストを送付することができる、３０２。ＢＳＦは、ＵＥのユーザ名を使用して、ＨＳＳ及び/又はホームロケーションレジスタ（ＨＬＲ）から、（Ｚｈインターフェイスを使用して）ユーザプロフィールを含む対応するＧＢＡユーザセキュリティ設定（ＧＵＳＳ）、および、（ＺｈまたはＺｈ’インターフェイスを使用して）認証ベクトル（ＡＶ）をフェッチすることができる、３０４。認証ベクトルは、ランダム（ＲＡＮＤ）、認証トークン（ＡＵＴＮ）、期待される応答（ＸＲＥＳ）、暗号鍵（ＣＫ）、及び/又は、整合性鍵（ＩＫ）値を含み得る。これらの値のうち、ＢＳＦは、ＵＥに対する認証チャレンジレスポンスを用いて（例えば、非承認ワールドワイドウェブ認証（ＷＷＷ－ａｕｔｈｅｔｉｃａｔｅ）信号）、ＲＡＮＤおよびＡＵＴＮを含むダイジェストを送付することができる、３０６。認証チャレンジレスポンスを伴うダイジェストは、ＵＥ認証自身をリクエストすることができる。ＵＥは、ＵＥのＳＩＭ上でＡＫＡアルゴリズムを実行し、ＡＵＴＮを検証することによってＢＳＦを認証し、かつ、レスポンス（ＲＥＳ）値とセッション鍵（つまり、ＣＫとＩＫ）を引き出すことができる。ここで、セッション鍵は、ＡＶにおいて、より早くＢＳＦに対して提供され得る。セッション鍵を生成した後で、ＵＥは、引き出されたＲＥＳ値を用いて第２のリクエストを送付することができる、３１０。次に、ＢＳＦは、ＵＥからのＲＥＳを認証ベクトル（ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｖｅｃｔｏｒ：ＡＶ）と比較することによって３１２、ユーザを認証することができる。ＲＥＳがＸＲＥＳと一致する場合、ＵＥは認証され得る。そして、ＢＳＦは、ＲＡＮＤ値とＢＦＳ名からブートストラップトランザクション識別子（Ｂ－ＴＩＤ）を作成することができる３１４。次に、Ｂ－ＴＩＤは、ＵＥに対する２００ＯＫレスポンスメッセージの中に含まれ得る、３１６。２００ＯＫレスポンスは、また、鍵マテリアルの有効期間（ｌｉｆｅｔｉｍｅ）も含み得る。ここで、ＵＥとＢＳＦの両方は、保管されたＣＫとＩＫを連結することによって、Ｋｓを作成する、３１４および３１８。しかしながら、実際の鍵マテリアルＫｓ＿ＮＡＦは、リクエストによりＫｓから計算されてよい（つまり、ＵＥがＮＡＦと通信を開始するときのＵＥにおいて、および、Ｋｓ＿ＮＡＦがＮＡＦによってクエリされるときにＢＳＦにおけるもの）。Ｋｓ＿ＮＡＦは、鍵導出機能を使用することによって作成され得る。

【００３０】

ＧＢＡ＿Ｕプロセスは、いくつかの相違を伴う、上述のＧＢＡ＿ＭＥプロセスの拡張であり得る。ＧＢＡ＿Ｕプロセスを用いて、鍵ＣＫとＩＫは、ＵＥ１２０の中にＵＩＣＣを残さない。ＧＢＡ＿Ｕブートストラッププロシージャにおいては、４０１の認証チャレンジメッセージ３０６においてＢＳＦ１３２によって送付されたＡＵＴＮが、ＧＢＡ＿ＭＥにおけるＡＵＴＮと異なり得る。ＵＥがチャレンジを受け取った場合、ＵＥのモバイル機器（ＭＥ）部分は、ＲＡＮＤとＡＵＴＮをＵＩＣＣに対して送付することができる。ＵＩＣＣは、そして、ＣＫ、ＩＫおよびＲＥＳを計算することができる。次に、ＵＩＣＣは、

ＣＫとＩＫを保管し、ＢＳＦに対して送付されるようにＭＥにＲＥＳを提供することができる。ＧＢＡ＿Ｕブートストラッププロシージャの後で、ＢＳＦとＵＩＣＣは、Ｋｓ＿ＮＡＦを作成することができる。ＧＢＡ＿ＭＥプロセスと同様なものである。

【００３１】

図５は、ブートストラップ使用プロシージャ（またはプロセス）に係るメッセージフローチャートを示している。３ＧＰＰ ＴＳ ３３．２２０ Ｆｉｇｕｒｅ４．４と同様なものである。ＵＥ１２０は、Ｂ－ＴＩＤとＫｓを含むことができ、３２０、かつ、ＢＳＦ１３２は、Ｂ－ＴＩＤとＫｓを含むことができる、３２２。ＵＥは、Ｋｓから鍵Ｋｓ＿ＮＡＦを引き出すことができる、３３２。次に、ＵＥは、Ｂ－ＴＩＤを用いてアプリケーションリクエストとメッセージ（ｍｓｇ）をＮＡＦ１１０に対して送付することができる、３３４。メッセージは、アプリケーション特定データセットを含み得る。次に、ＮＡＦは、与えられたＢ－ＴＩＤに対応する鍵マテリアルを得るために、ＢＳＦに対して認証リクエストを送付する、３３６。認証リクエストは、また、ＮＡＦ識別子（ＮＡＦ－ＩｄまたはＮＡＦ－ＩＤ）を含み得る。ＮＡＦ識別子は、ＵＥによって使用されるＮＡＦのパブリックホスト名とＵａセキュリティプロトコル識別子を含み得る。ＢＳＦは、ＮＡＦが与えられたホスト名を使用するよう認証されていることを検証することができる。ホスト名の検証が成功し、かつ、与えられたＢ－ＴＩＤを用いて鍵が見つかった場合、ＢＳＦは、Ｋ＿ＮＡＦのブートストラップ時間と鍵の有効期間を伴うＫｓ＿ＮＡＦ、および、ユーザプロフィール（Ｐｒｏｆ）をＮＡＦに対して送付することができる、３３８。Ｐｒｏｆは、ユーザプロフィールに係るアプリケーション特定の部分を含み得る。Ｋｓ＿ＮＡＦに加えて、ＮＡＦは、また、ＢＳＦから、いくつかのアプリケーション特定情報をリクエストすることができる。ＮＡＦは、Ｋ＿ＮＡＦのブートストラップ時間と鍵の有効期間を伴うＫｓ＿ＮＡＦを保管することができる。ＮＡＦは、リクエストされた情報を用いてＵＥに対してアプリケーション回答（ａｎｓｗｅｒ）を送付することができる、３４２。しかしながら、Ｂ－ＴＩＤを伴う鍵が見つからない場合、ＢＳＦは、Ｂ－ＴＩＤが見つからないことをＮＡＦに知らせることができ、ＮＡＦは、次に、ブートストラップ再ネゴシエーション（ｒｅｎｅｇｏｔｉａｔｉｏｎ）リクエストをＵＥに対して送付することができる。ＵＥは、次に、図４に示されるように、ブートストラップ認証プロシージャを再び実行し得る。

【００３２】

図６は、ＧＢＡベースの認証プロシージャに係るフローチャートを示している。ユーザ（例えば、ＵＥ１２０）は、ブラウザを使用してＮＡＦに対するアクセスをリクエストすることができる、３５２。ＵＥは、ＢＳＦ１３２を用いてＧＢＡブートストラップ認証プロシージャを実行することができる、３５４（図４を参照）。ＨＳＳ１３０を用いたＧＢＡブートストラップのクエリとレスポンス３５６を含んでいるものである。ブートストラップ認証が完遂した後で、ＵＥとＮＡＦ１０は、アプリケーション特定プロトコルを実行することができる。ここで、メッセージの認証は、ＵＥとＢＡＦとの間の相互認証の最中に生成されたセッション鍵に基づくものであり得る。例えば、ＵＥは、ＮＡＦチャレンジに対してレスポンスすることができる、３５８（例えば、Ｂ－ＴＩＤ）（図５を参照）。ＢＳＦは、ＮＡＦのために、ＵＥのＧＢＡチャレンジレスポンス検証を提供することができる、３６０。次に、ＵＥはＮＡＦへのアクセスが認められ得る、３６２。

【００３３】

図７は、ＧＡＡのためのＤＡＳＨ－ａｗａｒｅネットワークアプリケーションファンクション（Ｄ－ＮＡＦ）１１６のコンポーネントを示しており、ＤＡＳＨベースストリーミングのためのプロキシサービスとしても働き得る。Ｄ－ＮＡＦは、ＮＡＦ１１０、および、ＤＡＳＨサーバー１１８と通信することができるＤＡＳＨプロキシ１１４を含み得る。ＤＡＳＨプロキシを介したＤ－ＮＡＦは、ＤＡＳＨ ＭＰＤ４０２をパース（ｐａｒｓｅ）して、かつ、ＧＡＡベース認証プロシージャを最適化するために取得したＤＡＳＨコンテンツ情報を使用するように構成され得る。ＤＡＳＨプロキシは、ＨＴＴＰインターフェイスを介してＵＥと通信することができる。

【００３４】
Ｄ－ＮＡＦは、種々の機能を含み得る。例えば、Ｄ－ＮＡＦは、ＤＡＳＨコンテンツ依存マナー（ｃｏｎｔｅｎｔ－ｄｅｐｅｎｄｅｎｔ　ｍａｎｎｅｒ）において認証ポリシを適用することができる。異なるＤＡＳＨ表現と適合セットに対して、異なる認証ポリシを使用する（つまり、異なる認証鍵を介する）といったものである。クライアントは、Ｄ－ＮＡＦ認証に対して、異なるアクセス権またはＤＡＳＨフォーマットのストリームの異なる部分を受け取るための承認を有してよい。別の実施例において、Ｄ－ＮＡＦは、ＤＡＳＨサービスプロバイダから所定の認証ポリシを受け取り、かつ、ＤＡＳＨサービスプロバイダからのこれらのポリシをユーザ認証の中に組み入れることができる。ＤＡＳＨ特定認証ポリシがＤ－ＮＡＦによって管理される場合、オペレータネットワークは、サービスプロバイダに代わって認証を取り扱うように信頼され得る。オペレータネットワークによるＤＡＳＨ特定認証は、オペレータおよびオーバーザトップ（ＯＴＴ）サービスプロバイダのために、新たなビジネスの可能性を創出することができる。そのように、ＤＡＳＨ　ＭＰＤは、それぞれの表現（図２の４０８）または適合セット（図２の４０６）のために、この表現または適合セットと併せて使用されるべき認証ポリシに関する特定の信号を含んでよい。Ｄ－ＮＡＦは、ＤＡＳＨコンテンツに対して、よりきめの細かい認証を提供することができる。別のコンフィグレーションにおいて、Ｄ－ＮＡＦは、ユーザ認証資格情報のダウンロードまたは資格情報に対するプライオリティベースのアクセスを通じた外部エンティティを介して（つまり、ＤＡＳＨ　ＭＰＤにおいて）別個のＤＡＳＨコンテンツ認証を提供することができる。オーバーロードシナリオの最中に、ＨＳＳがネットワーク認証に集中できるようにである。例えば、ＢＳＦおよびＨＳＳを介するＧＡＡベース認証プロシージャは、ＭＰＤにおいて合図されたサービスプロバイダ自身の認証ポリシによってオーバーライド（ｏｖｅｒｒｉｄｅ）され得る。

【００３５】
別の実施例において、Ｄ－ＮＡＦは、ＤＡＳＨコンテンツのユニフォームリソースロケータ（ＵＲＬ）認証またはクライアント認証のために使用され得る。特定のリソースに対するアクセスをコントロールするため、かつ、所定のユーザグループ向けのものではないとしてコンテンツを特定するためにも使用され得るものである。コンテンツおよびサービスプロバイダは、彼らの著作権を保護し、かつ、ライセンス義務を果たすために、コンテンツに対するアクセスおよび視聴時間を制限することができる。クライアント認証は、特定のリソースに対するアクセスをコントロールするため、かつ、所定のユーザグループ向けのものではないとしてコンテンツを特定するためにも使用され得る。例えば、特定のタイプの制限されたマテリアルに対する認証鍵、著作権のあるマテリアルまたはペイパービュー（ｐａｙ－ｐｅｒ－ｖｉｅｗ）コンテンツといったものは、承認されたユーザだけに配信される。別の実施例として、レイティング情報（例えば、Ｇ、ＰＧ、ＰＧ－１３、ＴＶ－１４、または、Ｒ）が、親としてのコントロールのために提供される。そうしたセッティングにおいて、クライアント特定認証鍵が、意図されたユーザに対して配信され得る。そして、正しい認証鍵情報をもつユーザだけが、コンテンツにアクセスすることが許可される。プレーヤープログラム、アプリケーション、または、デバイスは、コンテンツに対する認証鍵によって特定されるものとしてＤＡＳＨコンテンツの再生を許可及び/又は禁止する特定のモードを用いて動作し得る。

【００３６】
Ｄ－ＮＡＦを介するＤＡＳＨコンテンツ認証は、種々のアプリケーション（またはユースケース（ｕｓｅ　ｃａｓｅ））を有し得る。５つのユースケースが、ＤＡＳＨコンテンツＵＲＬ認証の利点と利益のいくつかを説明することができる。第１ケースにおいて、アリス（Ａｌｉｃｅ）は、彼女がＤＡＳＨフォーマット（ＤＡＳＨ－ｆｏｒｍａｔｔｅｄ）のコンテンツを視聴できるようにするＤＡＳＨ可能（ＤＡＳＨ－ｃａｐａｂｌｅ）クライアントアプリケーションを有し得る。彼女は、Ｏｐｅｒａｔｏｒ　ＢｅｓｔＣｏｖｅｒａｇｅ　Ｔｅｌｅｃｏｍのモバイルストリーミングサービスに加入することができる。彼女は、映画を鑑賞することに興味がある。映画は”Ａ　Ｄａｓｈ　ｔｈｒｏｕｇｈ　ｔｈｅ

Ｃｌｏｕｄｓ”であり、ＤＡＳＨフォーマットにおいて利用可能である。オペレータは、映画に対するアクセスを承認されたユーザに限定することができ、かつ、アクセスを制限するために３ＧＰＰベース認証メカニズム（例えば、ＤＡＳＨコンテンツ認証）を使用することができる。アリスは、既にモバイルストリーミングサービスに加入しているので、彼女のクライアントアプリケーションは認証され、彼女は映画を楽しむことができる。

【００３７】

第２ユースケースにおいて、アリスとボブ（Ｂｏｂ）の両者は、彼らがＤＡＳＨフォーマットのコンテンツを視聴できるようにするＤＡＳＨ可能クライアントアプリケーションを有し得る。彼ら両者は、Ｏｐｅｒａｔｏｒ ＢｅｓｔＣｏｖｅｒａｇｅ Ｔｅｌｅｃｏｍのモバイルストリーミングサービスに加入することができる。ボブは、「プレミアムストリーミング」プランのために料金を支払い、一方、アリスは、より安価な「ベーシックストリーミング」プランの方を選ぶ（または料金を支払う）ことができる。彼ら両者は、映画”Ａ Ｄａｓｈ ｔｈｒｏｕｇｈ ｔｈｅ Ｃｌｏｕｄｓ”
を鑑賞することに興味がある。映画は、異なるビットレート及び/又は解像度で、ＤＡＳＨフォーマットにおいて利用可能である。ボブがプレミアムプランに加入しているおかげで、ボブのクライアントアプリケーションは、サービスによって提供される種々のビットレート及び/又は解像度においてストリームにアクセスして受信することができる（例えば、リンクのバンド幅とデバイス能力が与えられ、所与の時間において、最高の解像度を選択することによる）。アリスのクライアントアプリケーションは、彼女のベーシックな加入のせいで、最高のビットレート及び/又は解像度にアクセスすることが制限される。そこで、ＤＡＳＨコンテンツ認証を使用しているアリスのコンテンツアプリケーションは、利用可能なビットレート及び/又は解像度の限定されたセットからのストリームだけを受信する。

【００３８】

第３ユースケースにおいて、Ｏｐｅｒａｔｏｒ ＢｅｓｔＣｏｖｅｒａｇｅ Ｔｅｌｅｃｏｍ（オペレータ）は、最近、オペレータのインフラストラクチャに著しい投資をしており、オーバーザトップ（ｏｖｅｒ－ｔｈｅ－ｔｏｐ：ＯＴＴ）コンテンツ配信バリューチェインに集中することによってオペレータのサービス収入を増加させるための新たなビジネス機会を捜している。特に、オペレータは、彼らの情報システムとネットワーク設備（例えば、ホーム加入者サブシステム（ＨＳＳ））を活用するように望んでいる。認証鍵、ユーザアイデンティティ、および、ユーザサービスプロフィールを含む価値あるユーザ情報を含むものである。そうしたユーザ情報により、オペレータは、数多くのコントロール機能を実行することができる。機能は、ユーザ認証、サービスに対するユーザアクセス認証、および、コンテンツおよびコントロール配信ネットワーク（ＣＤＮ）プロバイダのための課金を含んでいる。オペレータは、最近、ＤＡＳＨコンテンツプロバイダであるＭｙＤＡＳＨと、セキュリティ及び/又は認証関連のサービスレベルアグリーメント（ＳＬＡ）に署名している。オペレータの３ＧＰＰ汎用認証アーキテクチャ（ＧＡＡ）上でのＭｙＤＡＳＨのためのユーザ認証および承認を遂行することによって、ＭｙＤＡＳＨのＤＡＳＨフォーマットのコンテンツを配信するためである。ＭｙＤＡＳＨは、層になった（ｔｉｅｒｅｄ）加入サービスをホストし、かつ、ＤＡＳＨコンテンツ認証を使用したクライアント認証のためのコンテンツ特定アクセス制限の実施を提供することができる。

【００３９】

第４ユースケースにおいて、Ｏｐｅｒａｔｏｒ ＢｅｓｔＣｏｖｅｒａｇｅ Ｔｅｌｅｃｏｍ（オペレータ）は、最近、ＤＡＳＨコンテンツプロバイダである、ＭｙＤＡＳＨとサービスレベルアグリーメント（ＳＬＡ）に署名している。ＭｙＤＡＳＨのＤＡＳＨフォーマットのコンテンツを配信及び/又は再販するためである。オペレータは、オペレータのクライアントに対して種々の新たなサービスを提供するために、ＭｙＤＡＳＨからのＤＡＳＨフォーマットのコンテンツを使用することを計画することができる。オペレータは、一貫性のあるユーザ経験のために、コンテンツおよび関連するメタデータの整合性を保証するようにＤＡＳＨコンテンツ認証を使用することができる。オペレータの投資は、セ

キュリティを保証するためのオペレータのインフラストラクチャに対して行われ得るが、オペレータは、また、ＭｙＤＡＳＨからのＤＡＳＨコンテンツ配信の最中での可能性のある侵入に対抗して備えるために、ここにおいて説明される技術を使用することができる。オペレータは、コンテンツ配信精度の所定のレベルまでＭｙＤＡＳＨをコミットする準備を含み得る。所定のレベルの精度が達成されない場合のペナルティ準備も同様である。これに応じて、ＭｙＤＡＳＨは、オペレータに対する認証メカニズムが、配信されたコンテンツおよびＭＰＤの整合性を有効にすることができる。

【００４０】

第５ユースケースにおいて、Ｏｐｅｒａｔｏｒ　ＢｅｓｔＣｏｖｅｒａｇｅ　Ｔｅｌｅｃｏｍ（オペレータ）は、最近、いくつかのオーバーザトップ（ＯＴＴ）ＤＡＳＨコンテンツプロバイダとサービスレベルアグリーメント（ＳＬＡ）に署名している。ＤＡＳＨコンテンツプロバイダのＤＡＳＨフォーマットのコンテンツを配信及び/又は再販するためである。オペレータは、オペレータのクライアントに対して、種々の新たなサービスを提供するために、これらのＤＡＳＨフォーマットのコンテンツを使用することができる。オペレータは、一貫性のあるユーザ経験のために、コンテンツおよび関連するメタデータの整合性を保証するようにＤＡＳＨコンテンツ認証を使用することができる。特に、オペレータは、複数のソースからのコンテンツを組み合せることによってメディア・マッシュアップ（ｍａｓｈｕｐ）を作成するために、ストリーム・スプライシング（ｓｐｌｉｃｉｎｇ）を介したサービスを使用することができる。例えば、広告差し込みは、ビデオオンデマンド（ＶｏＤ）とライブストリームの両方に対して、可能性のあるメディア・マッシュアップの例を提供する。そうしたスキーム（例えば、メディア・マッシュアップ）は、ダイナミックＭＰＤ生成または再書込みを使用することができる。しかし、これらのスキームは、ＤＡＳＨコンテンツ認証のために使用されるセグメントＵＲＬおよび他のメタデータを変更または除去しない。ＭＰＤとセグメントＵＲＬ又は他のメタデータの不適切な変更は、再生（ｐｌａｙｂａｃｋ）の中断を生じることがある。そして、再生されない広告の場合には、ＭＰＤとセグメントＵＲＬ又は他のメタデータのへ不適切な変更は、コンテンツプロバイダまたはオペレータにとって、収入の損失を結果として生じ得る。

【００４１】

メディア特定（例えば、ＭＰＤ４０２の表現４０８または適合４０６のセットレベル（図２））認証プロシージャが、説明した５つのユースケースを実現するために使用され得る。別の言葉で言えば、異なる加入ポリシ（特定の認証鍵に対応し得るもの）に対して、クライアントは、種々のＤＡＳＨコンポーネント（例えば、表現、適合セット、等）を異なって受け取るように認証され得る。そのように、ＮＡＦに対して提供された鍵（例えば、Ｋｓ＿ＮＡＦ）は、ユーザ特定であるだけでなく、アクセスされるべき種々のＤＡＳＨコンポーネント特定でもあり得る。ＤＡＳＨのためのＫｓ＿ＮＡＦコンポーネントは、ＧＡＡの使用を通じてイネーブル（ｅｎａｂｌｅ）され得る。ＨＳＳ及び/又はＨＬＲが既にメディア特定認証を保管している場合である。そうでなければ、ＤＡＳＨベース最適化も、また、外部エンティティ（ＨＳＳの代わりに）からのメディア特定認証ルールおよびＮＡＦによるユーザ証明書のダウンロードを介して可能である。メディア特定認証ルールおよびユーザ証明書のために外部エンティティ（ＨＳＳの他に）を使用することは、ＨＳＳにおけるロード（ｌｏａｄ）を低減することを手助けし得る。オーバーロードシナリオの最中にネットワーク認証プロシージャによってチャレンジされ得るものである。外部エンティティを使用することは、オーバーロードシナリオの最中にネットワーク認証プロシージャによるＨＳＳに対するチャレンジの数量を低減することができる。

【００４２】

コンテンツソースを表わす署名を通じたＵＲＬ認証のための検証鍵（ｖａｌｉｄａｔｉｏｎ　ｋｅｙ）に係る通信によって、ＤＡＳＨクライアントは、ＭＰＤ　ＵＲＬの妥当性を検査することができる。ＤＡＳＨクライアントは、また、種々のＤＡＳＨコンポーネント（例えば、ＤＡＳＨ期間４０４、適合セット４０６、または、表現４０８（図２））に対するコンテンツ特定認証鍵を受け取ることもできる。この通信または信号により、クラ

イアントはＵＲＬ署名を受け取ることができる。そして、次に、受け取ったＭＰＤおよび対応する認証鍵におけるＵＲＬに基づいてローカルにＵＲＬ署名を計算して、不一致の場合には対応するコンテンツを拒否する。そうしたコンテンツＵＲＬ検証情報（署名または認証鍵）又はそれらのロケーション（ＵＲＬ）は、ＭＰＤまたはメディアセグメントの一部分としてシグナル（ｓｉｇｎａｌ）され得る。フレームワークまたはプロセスは、セグメントＵＲＬの署名を計算することができ、かつ、その値を署名検証及び/又は認証鍵と一緒に外部に保管することができる。ＭＰＤインターフェイスは、ＨＴＴＰまたはＨＴＴＰＳを使用して、これらの署名を取得するためのＵＲＬテンプレートを提供することができる。ＤＡＳＨクライアントは、署名および認証鍵を取得することができ、次に、所与のセグメントＵＲＬ上でローカルに署名を計算して、不一致の場合にはＵＲＬを拒否することができる。

【００４３】

ＵＲＬサイン（ＵＲＬ　ｓｉｇｎｉｎｇ）（またはＵＲＬ署名）は、コンテンツに対するアクセスを制限し、かつ、ＤＡＳＨコンテンツのユーザ認証ができるようにするために使用され得る。例えば、サインおよびコンテンツＵＲＬの検証のために使用され得る。アクセスをいくらかのユーザに限定すること、及び/又は、視聴時間を制限することである。コンテンツアクセスを特定のユーザに限定するメカニズムは、コンテンツＵＲＬの中に、コンテンツアクセスが承認されるユーザのクライアントＩＰアドレスをエンベッド（ｅｍｂｅｄ）することであり得る。同様に、既定の時間の後にコンテンツが期限切れとなることを保証するために満了（ｅｘｐｉｒｙ）タイムスタンプがエンベッドされてよい。これらの値（例えば、クライアントＩＰアドレスおよび満了タイムスタンプ）は、次に、リクエストを送付している実際のクライアントおよびリクエストを放っているサービスエンジンでの現在時間に対して、検証され得る。２つの検証のうちいずれかが失敗した場合、リクエストは拒否され得る。しかしながら、ＵＲＬにおけるこれらのストリング（ｓｔｒｉｎｇ）のいずれもが、知識のあるユーザによって手動で編集されて騙され、承認されていないユーザと共有され、または、時間制限を超えてアクセスされる可能性があるので、ＵＲＬ変更に対して保護するために、生成されてＵＲＬに対して取り付けられた署名が使用され得る。ＵＲＬ署名は、キーハッシュ（ｋｅｙ　ｈａｓｈ）（例えば、署名）をＵＲＬに取付けることによって達成され得る。署名者と検証コンポーネントとの間だけで共有される秘密鍵（例えば、Ｋｓ＿ＮＡＦ）を使用するものである。一旦、ＨＴＴＰリクエストを受け取ると、コンテンツサーバーは、入力としてのリクエストＵＲＬから抽出された認証パラメータを用いて署名を検証する。計算結果（例えば、計算されたＵＲＬ署名）がリクエストＵＲＬにおけるＵＲＬ署名と一致する場合、ユーザは、コンテンツに対する正当なアクセスを有することができる。

【００４４】

図７に戻って参照すると、Ｄ－ＮＡＦ１１６は、既存のユーザ特定認証フレームワークと併せて（または、オントップで）コンテンツ特定認証をイネーブルすることができる。ＤＡＳＨレベルシグナルプロシージャは、コンテンツ特定認証鍵を使用してＤＡＳＨクライアントに対して情報を伝送するために使用され得る。Ｄ－ＮＡＦを使用するコンテンツ特定認証は、種々の利益を有し得るものである。

【００４５】

例えば、中間ネットワークエンティティ（例えば、ＤＡＳＨアウェア・ネットワークアプリケーションファンクション（Ｄ－ＮＡＦ）１１６の内側にあるＨＴＴＰプロキシまたはＤＡＳＨプロキシ１１４）は、コンテンツプロバイダによって実施されるコンテンツ特定認証ポリシの情報（例えば、ＭＰＤに係る特定のＤＡＳＨ表現または適合セットのための認証鍵）を受け取ることができる。Ｄ－ＮＡＦは、コンテンツ特定ＤＡＳＨ認証情報を受け取ることができる（例えば、ＤＡＳＨ　ＭＰＤをパースすることによる）。そして、Ｄ－ＮＡＦは、取得されたＤＡＳＨコンテンツ情報を使用することができる。ＨＳＳからのあらゆるユーザ特定認証証明書を一緒に用いて、ＧＡＡベース認証プロシージャの一部として、結合し、実施することによるものである（例えば、図４と図５）。ＮＡＦに対し

て提供された鍵（例えば、Ｋｓ＿ＮＡＦ）は、ユーザ特定であるだけでなく、アクセスされるべきＤＡＳＨコンポーネント特定でもあり得る。そのように、異なるＤＡＳＨ表現および適合セットのための異なる認証ポリシ（例えば、異なる認証鍵を介するもの）が、実施され得る。異なるＤＡＳＨ　ＭＰＤコンポーネントに対して異なる認証ポリシを使用することは、ＤＡＳＨフォーマットのストリームの異なる部分を受け取るための異なるアクセス権または承認をクライアントが有することを意味している。別の実施例において、ＢＳＦおよびＨＳＳを介する既存のＧＳＳベース認証プロシージャは、ＤＡＳＨレベルにおいてシグナルされるサービスプロバイダ自身の認証ポリシによってオーバーライドされてよい（例えば、ＭＰＤファイルにおいて）。

【００４６】

中間ネットワークエンティティ（例えば、ＨＴＴＰプロキシまたはＤＡＳＨプロキシ１１４）は、ＤＡＳＨコンテンツとメタデータの整合性の検証を許可することができる。中間ネットワークエンティティは、ＤＡＳＨコンテンツのためのオペレータネットワークへのエントリーポイントであってよい。検証情報（例えば、署名または認証鍵）又はそれらのロケーション（ＵＲＬ）に係る通信によって、Ｄ－ＮＡＦにおけるＤＡＳＨプロキシまたはＨＴＴＰプロキシは、コンテンツソースを表わす署名を通じたＵＲＬ認証によって、ＭＰＤ　ＵＲＬの妥当性を検査することができる。加えて、Ｄ－ＮＡＦにおけるＤＡＳＨプロキシまたはＨＴＴＰプロキシは、また、種々のＤＡＳＨコンポーネント（例えば、表現、適合セット、等）に対するコンテンツ特定認証鍵を受け取るためにも使用され得る。

【００４７】

いくつかの配置において、ユーザ認証およびコンテンツ認証は、異なるエンティティを使用して別個に処理されてよい。ユーザ認証とコンテンツ認証が分離される場合、既存のＧＡＡベース認証アーキテクチャが、ユーザ認証のために使用され得る。一方、ＤＡＳＨレベルシグナルフレームワークは、コンテンツ認証のために、なお使用することができる。ＮＡＦおよびサービスプロバイダまたはコンテンツ配信ネットワーク（ＣＤＮ）は、コンテンツ認証を実行し得る。

【００４８】

ＤＡＳＨレベルシグナルは、認証鍵と署名を送信するために使用され得る。ＵＲＬサインに基づくＤＡＳＨレベル認証情報シグナルは、また、ＤＡＳＨサービスの信頼性を検証するために使用され得る。

【００４９】

例えば、ＵＲＬ署名及び/又はダイジェストが、ＭＰＤファイルの中に含まれるＵＲＬのために生成される。コンフィグレーションにおいて、署名に関する情報は、ＭＰＤファイルを介して通信され得る。署名は、ＭＰＤファイルの中に含まれ得る。または、これらの署名を指し示すＵＲＬが、ＭＰＤファイルの中に含まれ得る。もしくは、これらの署名に対するＵＲＬを生成するためのリストまたはテンプレートベースのＵＲＬ構成ルールが、ＭＰＤファイルの中に含まれ得る。従って、ＭＰＤファイルは、署名、署名を指し示すＵＲＬ、署名に対するＵＲＬを生成するためのＵＲＬ構成ルールリスト、または、署名に対するＵＲＬを生成するためのテンプレートベースのＵＲＬ構成ルールを含み得る。

【００５０】

例えば、認証フレームワークを宣言し、かつ、署名ＵＲＬを通信するために、ＭＰＤにおいて、ＵＲＬ認証記述子（ｄｅｓｃｒｉｐｔｏｒ）が使用され得る。複数コンテンツ認証スキームが定義され得る。加えて、ＵＲＬダイジェストエレメントは、ＵＲＬを構成するためのテンプレートを提供する。テンプレートは、さらに、所与のＵＲＬに対する署名をダウンロードするために使用され得る。同様に、ＵＲＬ署名エレメントは、鍵獲得のためのＵＲＬおよびＵＲＬを構成するためのテンプレートを提供し、さらに、所与のＵＲＬに対する署名をダウンロードするために使用され得る。

【００５１】

ＵＲＬに係る異なるコンポーネントは、異なって認証され得る。例えば、ベースＵＲＬ認証のために、一式の署名がベースＵＲＬに含まれ得る（つまり、ＤＡＳＨ　ＭＰＤ４０

２、期間４０４、適合セット４０６、または、表現４０８レベルにおいて）。そして、次に、所定のＤＡＳＨ表現およびセグメントを指し示している残りのＵＲＬコンポーネントは、図２に示されるように、分離してサイン（または、認証）される。別の実施例において、一式の署名は、セグメントベース（ＳｅｇｍｅｎｔＢａｓｅ）エレメント（例えば、ＤＡＳＨセグメントベース）における@ｓｏｕｒｃｅＵＲＬ属性に含まれ得る。ＤＡＳＨセグメントベース認証のためのＤＡＳＨセグメントに係る絶対ＵＲＬを含み得るものである。別の実施例において、一式の署名は、ロケーション（Ｌｏｃａｔｉｏｎ）エレメントに含まれてよく、ＤＡＳＨ　ＭＰＤロケーション認証に対するＭＰＤのための絶対ＵＲＬを含んでいる。ＭＰＤロケーションとベースＵＲＬ認証、および、ＤＡＳＨクライアントへの対応する署名の通信は、コンテンツソース検証のために有益であり得る。

【００５２】

ＤＡＳＨプレイリスト（それぞれのＤＡＳＨが、ＭＰＤの中に含まれるＵＲＬに割り当てられている）に対して、ＤＡＳＨセグメントリスト認証のために、それぞれのプレイリスト特定ＵＲＬが、署名者によってサインされ、または、認証され得る（つまり、ＤＡＳＨ期間４０４、適合セット４０６、または、表現４０８レベルにおいて）。ＤＡＳＨテンプレート（それぞれのＤＡＳＨセグメントのＵＲＬが、既定のルールによりＤＡＳＨクライアントによって生成されている）に対して、ＤＡＳＨセグメントテンプレート認証のために、それぞれのテンプレート特定ＵＲＬが、署名者によってサインされ、または、認証され得る（つまり、ＤＡＳＨ期間、適合セット、または、表現レベルにおいて）。

【００５３】

別のコンフィグレーションにおいて、ＵＲＬ署名上の情報は、ＭＰＤの代わりに、ＤＡＳＨセグメントの中にキャリー（ｃａｒｒｙ）され、または、エンベッドされてよい。一つの実施例において、署名は、Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｏｒｇａｎｉｚａｔｉｏｎ　ｆｏｒ　Ｓｔａｎｄａｒｄｉｚａｔｉｏｎ－ｂａｓｅ　ｍｅｄｉａ　ｆｉｌｅ　ｆｏｒｍａｔ（ＩＳＯ－ＢＭＦＦ）ボックスの５つのレベルの中にキャリーされ得る（例えば、ＩＳＯ－ＢＭＦＦの”ｍｏｏｖ”ボックスの中といった初期化セグメントにおけるもの、または、ＩＳＯ－ＢＭＦＦの”ｍｏｏｆ”ボックスの中といったメディアセグメントにおけるもの）。別のコンフィグレーションにおいては、ＤＡＳＨセグメントの中で署名にエンベッドされた情報の存在をシグナルするために、ＭＰＤにおいて指標（ｉｎｄｉｃａｔｏｒ）が含まれてよい。ＤＡＳＨクライアントが、セグメント受け取り以前に、署名を受け取るために準備できるようにである。

【００５４】

別の実施例においては、認証タグＵＲＬが、ＭＰＤファイルを介して、セグメントＵＲＬのために提供され得る。認証フレームワークを宣言し、かつ、認証鍵と署名ＵＲＬを通信するＵＲＬ認証（ＵｒｌＡｕｔｈｅｎｔｉｃｉｔｙ）エレメントを使用するものである。ＵＲＬ認証は、サプリメンタリプロパティ（ＳｕｐｐｌｅｍｅｎｔａｒｙＰｒｏｐｅｒｔｙ）記述子と共に使用される場合に任意的であり、かつ、エッシェンシャルプロパティ（ＥｓｓｅｎｔｉａｌＰｒｏｐｅｒｔｙ）記述子と共に使用される場合には必須である。エッシェンシャルプロパティまたはサプリメンタリプロパティのいずれの場合でも、@ｓｃｈｅｍｅＩｄＵｒｉに係る値は、ＵＲＬ認証エレメント認証フレームワークが使用される場合に、”ｕｒｎ：ｍｐｅｇ：ｄａｓｈ：ｓｅａ：ｕｒｌａｕｔｈ：２０１３”であり得る。

【００５５】

別のコンフィグレーションにおいて、ＵＲＬ認証エレメントは、３ＧＰＰ技術仕様書（ＴＳ）２６．２４７Ｖ１１．０．０（２０１２－０９）に基づいてＤＡＳＨ　ＭＰＤにおいて実施され得る。もしくは、ジョイントワーキンググループであるＩｎｔｅｒｎａｔｉｏｎａｌ　Ｏｒｇａｎｉｚａｔｉｏｎ　ｆｏｒ　Ｓｔａｎｄａｒｄｉｚａｔｉｏｎ（ＩＳＯ）／Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｅｌｅｃｔｒｏｔｅｃｈｎｉｃａｌ　Ｃｏｍｍｉｓｓｉｏｎ（ＩＥＣ）２３００９－１：２０１２に基づいてエッシェンシャルプロパティまたはサプリメンタリプロパティとして定義され得る。アプリケーションに依存するもので

ある。ＵＲＬ認証エレメントは、鍵獲得のためにＵＲＬを、かつ、ＵＲＬを構成するためにテンプレートを提供することができる。さらに、所与のＭＰＤセグメントＵＲＬに対する認証タグをダウンロードするために使用され得る。例えば、ＵＲＬ認証エレメントは、ＭＰＤの中に含まれてよく、ＭＰＤは、属性とエレメントを有し得る。ＵＲＬ認証エレメントのセマンティクス（ｓｅｍａｎｔｉｃｓ）は、（表１）に示されるようなものであり得る。ＵＲＬ認証エレメントは、以下の属性を含み得る。@ａｕｔｈＳｃｈｅｍｅＩｄＵｒｉ、@ａｕｔｈＵｒｌＴｅｍｐｌａｔｅ、@ａｕｔｈＴａｇＬｅｎｇｔｈ、@ｋｅｙＵｒｉＴｅｍｐｌａｔｅ、@ｖａｌｉｄｉｔｙＥｘｐｉｒｅｓ、または、@ｉｎｂａｎｄＡｕｔｈＴａｇ、である。それぞれのエレメントまたは属性は、エレメントまたは属性の名前、使用、または、説明を有し得る。（表１）の「使用」カラムは、”Ｍ（必須）”、”Ｏ”（任意的）、”ＯＤ”（デフォルト値を用いて任意的）、または、”ＣＭ”（条件に応じて必須）を用いてマークされる属性を有し得る。

【表１】

エレメントまたは属性名	使用	説明
ＵｒｌＡｕｔｈｅｎｔｉｃｉｔｙ		セグメントＵＲＬのための認証タグを計算するために必要な情報を特定する
＠ａｕｔｈＳｃｈｅｍｅＩｄＵｒｉ	Ｍ	認証タグを計算するためのアルゴリズムを特定する
＠ａｕｔｈＵｒｌＴｅｍｐｌａｔｅ	Ｍ	認証タグ値の取得のために使用されるＵＲＬを作成するためのテンプレートを特定する。＠ｉｎｂａｎｄＡｕｔｈＴａｇが真である場合は、アブセントでよい。
＠ａｕｔｈＴａｇＬｅｎｇｔｈ	Ｏ	認証タグの長さをビットで特定する。アブセントであれば、タグ長さは、＠ａｕｔｈＳｃｈｅｍｅＩｄＵｒｉにより特定されるアルゴリズムにおけるものと同じである。
＠ｋｅｙＵｒＩＴｅｍｐｌａｔｅ	Ｏ	鍵ＵＲＩ生成のためのテンプレートを特定する。ＩＳＯ／ＩＥＣ２３００９－１：２０１２、５．３．９．４．４．において定義されるシンタックスと変数置換を使用する。
＠ｖａｌｉｄｉｔｙＥｘｐｉｒｅｓ	Ｍ	ＵＲＬ認証が期限切れとなる時間を（壁時計時間において）特定する
＠ｉｎｂａｎｄＡｕｔｈＴａｇ	ＯＤ	真である場合、認証タグが関連するセグメントの中に現れる（そうしたインバンドキャリッジが特定される場合に）。
凡例： 属性について：Ｍ＝必須、Ｏ＝任意的、ＯＤ＝デフォルト値を用いて任意的、 ＣＭ＝条件に応じて必須 エレメントについて：＜ｍｉｎＯｃｃｕｒｓ＞・・・＜ｍａｘＯｃｃｕｒｓ＞（Ｎ＝無境界） エレメントは太字、属性は太字ではなく＠で始まる		

（表1）

【００５６】

ＵＲＬ認証エレメントに対する拡張可能マークアップ言語シンタックス（ｅｘｔｅｎｓ

ｉｂｌｅ ｍａｒｋｕｐ ｌａｎｇｕａｇｅ－ｓｙｎｔａｘ：ＸＭＬ－ｓｙｎｔａｘ）の一つの実施例は、（表２）に示されるようなものであり得る。図８において説明されるものである。

【００５７】

別の実施例において、ＤＡＳＨコンテンツに係る認証およびアクセス承認リクエストは、ＭＰＤにおいてシグナルされ得る。例えば、（表３）に示されるように、共通適合セット（Ｃｏｍｍｏｎ Ａｄａｐｔｉｏｎ Ｓｅｔ）、表現とサブ表現属性（Ｒｅｐｒｅｓｅｎｔａｔｉｏｎ ａｎｄ Ｓｕｂ－Ｒｅｐｒｅｓｅｎｔａｔｉｏｎ）、および、エレメントに係るＭＰＤ階層レベルにおいて宣言されるコンテンツ承認（ＣｏｎｔｅｎｔＡｕｔｈｏｒｉｚａｔｉｏｎ）と名付けられた記述子においてである。それぞれのエレメント（例えば、コンテンツ認証エレメント）または属性は、エレメントまたは属性の名前、使用、または、説明を有し得る。（表１）における「使用」カラムは、最小の発生回数に対する＜ｍｉｎＯｃｃｕｒｓ＞および最大の発生回数に対する＜ｍａｘＯｃｃｕｒｓ＞を用いてマークされたエレメントを有し得る。ここで、Ｎは、発生に係る無境界数（ｕｎｂｏｕｎｄｅｄ ｎｕｍｂｅｒ）である。

【表２】

エレメントまたは属性名	使用	説明
共通の属性とエレメント		
ＣｏｎｔｅｎｔＡｕｔｈｏｒｉｚａｔｉｏｎ	０．．．Ｎ	関連する表現に使用されるコンテンツアクセス認証スキームに関する情報を特定する。
凡例： 属性について：Ｍ＝必須、Ｏ＝任意的、ＯＤ＝デフォルト値を用いて任意的、 ＣＭ＝条件に応じて必須 エレメントについて：＜ｍｉｎＯｃｃｕｒｓ＞・・・＜ｍａｘＯｃｃｕｒｓ＞（Ｎ＝無境界） エレメントは太字、属性は太字ではなく＠で始まる		

（表3）

【００５８】

コンテンツ承認エレメントに対する拡張可能マークアップ言語シンタックス（ＸＭＬ－ｓｙｎｔａｘ）の一つの実施例は、（表４）に示されるようなものであり得る。図９において説明されるものである。

【００５９】

コンテンツアクセス承認または信頼されるクライアント認証スキームを特定するために、コンテンツ承認エレメントに対して＠ｓｃｈｅｍｅＩｄＵｒｉが使用され得る。この＠ｓｃｈｅｍｅＩｄＵｒｉは、十分な情報を提供し得るものであり、おそらく＠ｖａｌｕｅ及び/又は拡張属性およびエレメントを伴う。認証システム、コンテンツアクセス承認ポリシ、および、使用される鍵配信スキームといったものであり、保護されたコンテンツを再生するための承認をクライアントがおそらく得られるか否かを、クライアントが判断できるようにする。ＭＰＤのフェッチの後で、それがコンテンツアクセス承認または信頼されるクライアント認証リクエストを満たさないであろうと判断するクライアントは、コン

テンツを無視することができる（保護されたコンテンツをダウンロードして、次に、クライアントが鍵を持っていないので保護されたコンテンツを解読することができないと認識するよりは、むしろそうである。鍵は、コンテンツアクセス承認または信頼されるクライアント認証プロトコルを通じて信頼されるクライアントについてアクセス可能とされている。）その間に、コンテンツアクセス承認または信頼されるクライアント認証リクエストを満たしているクライアントは、次に、対応するコンテンツアクセス承認または信頼されるクライアント認証プロトコルを始めて、コンテンツを解読しアクセスできるようにするために使用される鍵を得る。

【００６０】

コンテンツ承認（ＣｏｎｔｅｎｔＡｕｔｈｏｒｉｚａｔｉｏｎ）エレメントは、コンテンツアクセス認証スキーム（例えば、特定の鍵管理システムまたは認証方法）に特有の情報を提供するために、別個の名前空間（ｎａｍｅｓｐａｃｅ）において拡張され得る。複数のコンテンツ認証エレメントが存在する場合、それぞれのコンテンツ認証エレメントは、コンテンツアクセス認証スキーム、または、表現（Ｒｅｐｒｅｓｅｎｔａｔｉｏｎ）をアクセスし、かつ、表わすために十分な信頼されるクライアント認証スキームを記述することができる。

【００６１】

別の実施例は、図１０におけるフローチャートに示されるように、ダイナミックアダプティブストリーミング・オーバー・ハイパーテキストトランスファープロトコル（ＨＴＴＰ）アウェア（ＤＡＳＨ－ａｗａｒｅ）ネットワークアプリケーションファンクション（Ｄ－ＮＡＦ）に係るコンピュータ回路の機能性５００を提供する。機能性は方法として実施されるか、または、機能性はマシン上のインストラクションとして実行され得る。ここで、インストラクションは、少なくとも一つのコンピュータで読取り可能な媒体または固定のマシンで読取り可能な媒体上に含まれ得る。コンピュータ回路は、ブロック５１０におけるように、ＤＡＳＨコンテンツに対するユーザ認証ポリシおよびコンテンツ特定認証ポリシに基づいて、ＤＡＳＨコンテンツへのアクセスのためにクライアントを承認するように構成され得る。コンピュータ回路は、さらに、ブロック５２０におけるように、ＤＡＳＨ　ＭＰＤにおいて実施された認証ポリシを示すように構成され得る。

【００６２】

一つの実施例において、コンピュータ回路は、さらに、クライアントに対するユーザ認証ポリシを受け取り、かつ、コンテンツサービスプロバイダからＤＡＳＨコンテンツに対するコンテンツ特定認証ポリシを受け取るように、構成され得る。別のコンフィグレーションにおいて、ＤＡＳＨコンテンツへのアクセスのためにクライアントを承認するように構成されたコンピュータ回路は、さらに、コンテンツ特定認証ポリシ情報を含んでいるＤＡＳＨコンテンツ情報に対するＤＡＳＨメディア表現記述（ＭＰＤ）メタデータファイルをパースし、かつ、あらゆるネットワークベースユーザ認証ポリシを含むようＭＰＤを変更するように、構成され得る。ＤＡＳＨコンテンツ情報に係るそれぞれのコンポーネントは、ＭＰＤ期間、ＭＰＤ適合セット、ＭＰＤ表現、ＭＰＤセグメント、または、ＭＰＤサブセグメント、を含み得る。ＤＡＳＨコンテンツへのアクセスのためにクライアントを承認するように構成されたコンピュータ回路は、さらに、ＤＡＳＨコンテンツ情報に対するＤＡＳＨ認証情報およびＭＰＤメタデータファイルにおけるＤＡＳＨコンテンツ情報アドレスを受け取り、かつ、受け取った認証ポリシに基づいてＤＡＳＨコンテンツへのアクセスのためにクライアントを承認する、ように構成され得る。ＤＡＳＨ認証情報は、受け取ったユニフォームリソースロケータ（ＵＲＬ）署名とＵＲＬ認証鍵を含み、かつ、ＤＡＳＨコンテンツ情報アドレスは、ＤＡＳＨコンテンツ情報ＵＲＬを含み得る。ＤＡＳＨコンテンツへのアクセスのためにクライアントを承認するように構成されたコンピュータ回路は、さらに、ＤＡＳＨコンテンツ情報ＵＲＬと認証鍵に基づいてＵＲＬ署名を計算し、かつ、ローカルに計算されたＵＲＬ署名が受け取ったＵＲＬと一致しない場合にＤＡＳＨコンテンツを拒否するように、構成され得る。クライアントは、モバイルターミナル（ＭＴ）、ユーザ機器（ＵＥ）、または、モバイルステーション（ＭＳ）を含むクライアント機

器を含み得る。クライアント機器は、アンテナ、カメラ、タッチ感応ディスプレイスクリーン、スピーカ、マイクロフォン、グラフィックプロセッサ、アプリケーションプロセッサ、内部メモリ、または、不揮発性メモリポート、を含み得る。

【００６３】

別の実施例は、図１１におけるフローチャートに示されるように、ハイパーテキストトランスファープロトコル（ＨＴＴＰ）プロキシ、または、ダイナミックアダプティブストリーミング・オーバーＨＴＴＰ（ＤＡＳＨ）プロキシを使用して、コンテンツ特定認証を提供するために方法６００を提供する。方法はマシンまたはコンピュータ回路上のインストラクションとして実行され得る。ここで、インストラクションは、少なくとも一つのコンピュータで読取り可能な媒体または固定のマシンで読取り可能な媒体上に含まれ得る。方法は、ブロック６１０におけるように、クライアントに対するユーザ認証ポリシを受け取るオペレーションを含んでいる。ブロック６２０におけるように、ＤＡＳＨサービスプロバイダからＤＡＳＨコンテンツに対するコンテンツ特定認証ポリシを受け取るオペレーションが後に続く。方法に係る次のオペレーションは、ブロック６３０におけるように、ネットワークエレメント上のＨＴＴＰプロキシまたはＤＡＳＨプロキシでのユーザ認証ポリシとコンテンツ特定認証ポリシに基づいて、ＤＡＳＨコンテンツへのアクセスのためにクライアントを承認することであり得る。方法は、さらに、ブロック６４０におけるように、ＤＡＳＨ　ＭＰＤにおいて実施された認証ポリシを示すことを含み得る。

【００６４】

一つの実施例において、ＤＡＳＨコンテンツへのアクセスのためにクライアントを承認するオペレーションは、さらに、コンテンツ特定認証ポリシ情報を含んでいるＤＡＳＨコンテンツ情報に対するＤＡＳＨメディア表現記述（ＭＰＤ）メタデータファイルをパースすること、および、あらゆるネットワークベースユーザ認証ポリシを含むようＭＰＤを変更すること、を含み得る。別のコンフィグレーションにおいて、ＤＡＳＨコンテンツへのアクセスのためにクライアントを承認するオペレーションは、さらに、ＤＡＳＨコンテンツ情報に係るそれぞれのコンポーネントを承認すること、を含み得る。ＤＡＳＨコンテンツ情報に係るそれぞれのコンポーネントは、ＭＰＤ期間、ＭＰＤ適合セット、ＭＰＤ表現、ＭＰＤセグメント、または、ＭＰＤサブセグメント、を含み得る。別の実施例において、ＤＡＳＨコンテンツへのアクセスのためにクライアントを承認するオペレーションは、さらに、ＤＡＳＨコンテンツに対するＤＡＳＨ認証情報およびＭＰＤメタデータファイルにおけるＤＡＳＨコンテンツ情報ロケーションを受け取ること、および、受け取った認証ポリシに基づいてＤＡＳＨコンテンツへのアクセスのためにクライアントを承認すること、を含み得る。ＤＡＳＨ認証情報は、受け取ったユニフォームリソースロケータ（ＵＲＬ）署名とＵＲＬ認証鍵を含み得る。ＤＡＳＨコンテンツ情報ロケーションは、ＤＡＳＨコンテンツ情報ＵＲＬを含み得る。別のコンフィグレーションにおいて、ＤＡＳＨコンテンツへのアクセスのためにクライアントを承認するオペレーションは、さらに、ＤＡＳＨコンテンツ情報ＵＲＬと認証鍵に基づいてＵＲＬ署名をローカルに計算すること、および、ローカルに計算されたＵＲＬ署名が受け取ったＵＲＬと一致しない場合にＤＡＳＨコンテンツを破棄すること、を含み得る

【００６５】

別の実施例において、ＤＡＳＨコンテンツへのアクセスのためにクライアントを承認するオペレーションは、さらに、ＤＡＳＨコンテンツ情報に対するＮＡＦ鍵マテリアル（Ｋｓ＿ＮＡＦ）を含むブートストラップサーバーファンクション（ＢＳＦ）からコンテンツ鍵を取得すること、を含み得る。別のコンフィグレーションにおいて、ＤＡＳＨコンテンツへのアクセスのためにクライアントを承認するオペレーションは、さらに、既定の条件（例えば、ＨＳＳのオーバーロード条件）に基づいて、ユーザ認証を無効にすること、を含み得る。ユーザ認証は、ブートストラップサーバーファンクション（ＢＳＦ）またはホーム加入者サブシステム（ＨＳＳ）を介する汎用認証アーキテクチャベース（ＧＡＡ－ｂａｓｅｄ）認証プロシージャ、を含み得る。

【００６６】

図７に戻って参照すると、サーバーにおけるダイナミックアダプティブストリーミング・オーバー・ハイパーテキストトランスファープロトコル（ＨＴＴＰ）アウェア（ＤＡＳＨ－ａｗａｒｅ）ネットワークアプリケーションファンクション（Ｄ－ＮＡＦ）は、クライアントを認証するためのネットワークアプリケーションファンクション（ＮＡＦ）、および、ＤＡＳＨコンテンツおよびクライアントに対する情報を配信するためのＤＡＳＨプロキシ１１４、を含み得る。ＤＡＳＨプロキシは、さらに、コンテンツ特定認証ポリシ情報を含んでいるＤＡＳＨコンテンツ情報に対するＤＡＳＨメディア表現記述（ＭＰＤ）メタデータファイルをパースし、かつ、ＮＡＦからの認証ポリシ情報を含むようＭＰＤを変更するように、構成され得る。Ｄ－ＮＡＦは、さらに、コンテンツ特定認証ポリシを条件に、ＤＡＳＨコンテンツへのアクセスのためにクライアントを承認するように構成され得る。ＤＡＳＨコンテンツ情報は、ＤＡＳＨコンテンツ情報ユニフォームリソースロケータ（ＵＲＬ）を含み得る。ＤＡＳＨコンテンツ情報ＵＲＬは、ＤＡＳＨ　ＭＰＤ、期間、適合セット、または、表現レベルの対するベースＵＲＬを認証するために使用することができ、または、ＤＡＳＨコンテンツ情報ＵＲＬは、ＭＰＤに係るセグメントＵＲＬを認証するために使用され得る。

【００６７】

別の実施例において、ＮＡＦは、さらに、ＮＡＦ鍵マテリアル（Ｋｓ＿ＮＡＦ）、プロフィール、ブートストラップ時間、または、鍵の有効期間、を含んでいるブートストラップサーバーファンクション（ＢＳＦ）からセッション鍵を取得するように構成され得る。ＤＡＳＨプロキシは、さらに、ＤＡＳＨコンテンツ情報に対するコンテンツ鍵を取得するように構成され得る。別のコンフィグレーションにおいて、ＮＡＦまたはＤＡＳＨプロキシは、さらに、ＤＡＳＨコンテンツ情報に対するＮＡＦ鍵マテリアル（Ｋｓ＿ＮＡＦ）を含んでいるブートストラップサーバーファンクション（ＢＳＦ）からコンテンツ鍵を取得するように構成され得る。別の実施例において、Ｄ－ＮＡＦは、さらに、ＤＡＳＨコンテンツに対するＤＡＳＨサービスプロバイダからＤＡＳＨ特定認証ポリシを受け取り、かつ、ブートストラップサーバーファンクション（ＢＳＦ）またはホーム加入者サブシステム（ＨＳＳ）を介する汎用認証アーキテクチャベース（ＧＡＡ－ｂａｓｅｄ）認証プロシージャをオーバーライドするように、構成され得る。

【００６８】

別のコンフィグレーションにおいて、ＤＡＳＨプロキシまたはＮＡＦは、さらに、ＤＡＳＨコンテンツのＤＡＳＨサービスプロバイダからＤＡＳＨ特定認証ポリシを受け取り、ＤＡＳＨ特定認証ポリシをユーザ認証ポリシの中に組み入れ、ＤＡＳＨ特定認証ポリシ及びＤＡＳＨコンテンツ情報とクライアント認証のためのユーザ認証ポリシの両方を実施することによりＤＡＳＨコンテンツへのクライアントのアクセスを承認し、かつ、ＤＡＳＨ　ＭＰＤにおいて実施された認証ポリシを示す、ように構成され得る。Ｄ－ＮＡＦは、ＤＡＳＨサービスプロバイダのためのオペレータネットワーク認証を提供することができる。別の実施例において、Ｄ－ＮＡＦは、ＤＡＳＨ　ＭＰＤにおけるＤＡＳＨサービスプロバイダの認証ポリシを受け取ることができる。

【００６９】

別の実施例において、ＤＡＳＨポリシは、さらに、ＤＡＳＨコンテンツに対するＤＡＳＨ認証情報とメディア表現記述（ＭＰＤ）メタデータファイルにおけるＤＡＳＨコンテンツ情報ロケーションを受け取り、受け取った認証ポリシに基づいてＤＡＳＨコンテンツへのアクセスのためにクライアントを承認し、かつ、ＤＡＳＨ　ＭＰＤにおいて実施されたポリシを示す、ように構成され得る。ＤＡＳＨ認証情報は、署名と認証鍵を含み得る。そして、ＤＡＳＨコンテンツ情報ロケーションは、ＤＡＳＨコンテンツ情報ユニフォームリソースロケータ（ＵＲＬ）を含み得る。ＤＡＳＨプロキシは、さらに、ＤＡＳＨコンテンツ情報のそれぞれのコンポーネントを有効にするように構成され得る。ＤＡＳＨコンテンツ情報のそれぞれのコンポーネントは、ＭＰＤ期間、ＭＰＤ適合セット、ＭＰＤ表現、ＭＰＤセグメント、または、ＭＰＤサブセグメント、を含み得る。別の実施例において、ＤＡＳＨプロキシは、さらに、ＤＡＳＨコンテンツＵＲＬと認証鍵に基づいてＵＲＬ署名を

計算し、かつ、ローカルに計算されたＵＲＬ署名が受け取った署名と一致しない場合にＤＡＳＨコンテンツを拒否する、ように構成され得る。Ｄ－ＮＡＦは、ネットワークエレメント上でホストされ得る。

【００７０】

図１２は、ＤＡＳＨ、ノード７１０、および、ＤＡＳＨに対するコンテンツ認証のためのサーバー７３０上のダイナミックアダプティブストリーミング・オーバー・ハイパーテキストトランスファープロトコル（ＨＴＴＰ）アウェア（ＤＡＳＨ－ａｗａｒｅ）ネットワークアプリケーションファンクション（Ｄ－ＮＡＦ）、に対するコンテンツ認証を提供するためのクライアント機器７２０の一つの実施例を示している。Ｄ－ＮＡＦは、図１０の５００において説明したように、ＤＡＳＨコンテンツ情報を認証するように構成され得る。別のコンフィグレーションにおいて、Ｄ－ＮＡＦは、図１１の６００において説明したように、ＨＴＴＰプロキシまたはＤＡＳＨプロキシを使用するコンテンツ特定認証を提供することができる。クライアント機器７２０は、プロセッサ７２２とトランシーバ７２４を含み得る。一つの実施例において、クライアント機器は、ノードを介してＤ－ＮＡＦと通信することができる。ノード７１０は、基地局（ＢＳ）、Ｎｏｄｅ　Ｂ（ＮＢ）、ｅｖｏｌｖｅｄ　Ｎｏｄｅ　Ｂ（ｅＮＢ）、ベースバンドユニット（ＢＢＵ）、リモートラジオヘッド（ＲＲＨ）、リモートラジオ設備（ＲＲＥ）、リモートラジオユニット（ＲＲＵ）、または、中央処理モジュール（ＣＰＭ）、を含み得る。

【００７１】

図１３は、クライアント機器の実施例を提供する。モバイルターミナル（ＭＴ）、モバイルノード、ユーザ機器（ＵＥ）、モバイルステーション（ＭＳ）、モバイル無線機器、モバイル通信機器、タブレット、ハンドセット、または、他のタイプの無線機器、といったものである。無線機器は、ノード、マクロノード、低電力ノード（ＬＰＮ）、または、送信局と通信するように構成されている一つまたはそれ以上のアンテナを含み得る。送信局は、基地局（ＢＳ）、ｅｖｏｌｖｅｄ　Ｎｏｄｅ　Ｂ（ｅＮＢ）、ベースバンドユニット（ＢＢＵ）、リモートラジオヘッド（ＲＲＨ）、リモートラジオ設備（ＲＲＥ）、中継局（ＲＳ）、ラジオ設備（ＲＥ）、リモートラジオユニット（ＲＲＵ）、中央処理モジュール（ＣＰＭ）、または、他のタイプの無線ワイドエリアネットワーク（ＷＷＡＮ）アクセスポイント、といったものである。無線機器は、３ＧＰＰ　ＬＴＥ、ＷｉＭＡＸ、高速パケットアクセス（Ｈｉｇｈ　Ｓｐｅｅｄ　Ｐａｃｋｅｔ　Ａｃｃｅｓｓ：ＨＳＰＡ）、ブルートゥース（登録商標）、および、ＷｉＦｉのうち少なくとも一つを使用して通信するように構成され得る。無線機器は、それぞれの無線通信規格のための別個のアンテナ、または、複数の無線通信規格のための共有アンテナを使用して通信することができる。無線機器は、無線ローカルエリアネットワーク（ＷＬＡＮ）、無線パーソナルエリアネットワーク（ＷＰＡＮ）、及び/又は、ＷＡＮにおいて通信することができる。

【００７２】

図１３は、また、無線機器からのオーディオ入力と出力のために使用され得る一つのマイクロフォンと一つまたはそれ以上のスピーカの説明を提供する。ディスプレイスクリーンは、液晶ディスプレイ（ＬＣＤ）スクリーン、または、有機発光ダイオード（ＯＬＥＤ）ディスプレイといった他のタイプのディスプレイスクリーンであってよい。ディスプレイスクリーンは、タッチスクリーンとして構成され得る。タッチスクリーンは、容量性、抵抗性、または、他のタイプのタッチスクリーン技術を使用してよい。アプリケーションプロセッサとグラフィックプロセッサは、処理とディスプレイ機能を提供するために内部メモリに結合され得る。ユーザに対して入力／出力オプションを提供するために、不揮発性メモリポートも使用され得る。不揮発性メモリポートは、また、無線機器のメモリ機能を拡張するためにも使用されてよい。キーボードは、追加的なユーザ入力を提供するために、無線機器と統合されるか、または、無線機器に無線で接続されてよい。仮想キーボードが、タッチスクリーンを使用して提供されてもよい。

【００７３】

種々の技術、又は、その所定の態様または部分は、有形の媒体にエンベッドされたプロ

グラムコード（つまり、インストラクション）の形式であってよい。有形の媒体は、フロッピー（登録商標）ディスケット、コンパクト読出し専用メモリ（ＣＤ－ＲＯＭ）、ハードドライブ、固定のコンピュータで読取り可能な記録媒体、または、あらゆる他のマシンで読取り可能な記録媒体といったものである。マシンで読取り可能な記録媒体では、プログラムコードがロードされてマシンによって実行されると、そのマシンは、種々の技術を実施するための装置になる、回路は、ハードウェア、ファームウェア、プログラムコード、実行可能コード、コンピュータインストラクション、及び/又は、ソフトウェアを含み得る。固定のコンピュータで読取り可能な記録媒体は、信号を含まない、コンピュータで読取り可能な記録媒体であり得る。プログラム可能なコンピュータ上でのプログラムコード実行の場合、コンピューティングデバイスは、プロセッサ、プロセッサにより読取り可能な記録媒体（揮発性および不揮発性のメモリ及び/又はストレージエレメントを含んでいるもの）、少なくとも一つの入力デバイス、および、少なくとも一つの出力デバイス、を含んでよい。揮発性および不揮発性メモリ及び/又はストレージエレメントは、ランダムアクセスメモリ（ＲＡＭ）、消去可能プログラマブル読出し専用メモリ（ＥＰＲＯＭ）、フラッシュドライブ、光ドライブ、磁気ハードドライブ、半導体ドライブ、または、電子データを保管するための他の媒体であってよい。ノードと無線機器は、また、トランシーバモジュール（つまり、トランシーバ）、カウンターモジュール（つまり、カウンタ）、処理モジュール（つまり、プロセッサ）、及び/又は、クロックモジュール（つまり、クロック）またはタイマーモジュール（つまり、タイガー）を含んでよい。ここにおいて説明された種々の技術を実施または利用し得る一つまたはそれ以上のプログラムは、アプリケーションプログラミングインターフェイス（ＡＰＩ）、リユーサブルコントロール、等を使用してよい。そうしたプログラムは、コンピュータシステムと通信するために、ハイレベル手続型言語またはオブジェクト指向プログラミング言語であってよい。しかしながら、プログラムは、望むのであれば、アセンブリまたはマシン言語において実施されてよい。あらゆるケースにおいて、言語は、コンパイルまたはインタープリートされた言語であり、ハードウェアの実施と結合されてよい。

【００７４】

この明細書において説明された多くのファンクショナルユニットは、モジュールとしてラベル付けされてきたことが理解されるべきである。それらの実施の独立請求項をより特定的に強調するためである。例えば、モジュールは、カスタム超大型集積回路（ＶＬＳＩ）回路またはゲートウェイ、ロジックチップといった既製の半導体、トランジスタ、または、他の専用コンポーネントを含む、ハードウェア回路として実施され得る。モジュールは、また、プログラマブルゲートアレイ、プログラマブルアレイロジック、プログラマブルロジックデバイス、等といった、プログラマブルなハードウェアデバイスにおいても実施され得る。

【００７５】

モジュールは、また、種々のタイプのプロセッサによる実行のためにソフトウェアにおいても実施され得る。実行可能コードに係る特定されたモジュールは、例えば、オブジェクト、プロシージャ、または、ファンクションとして編成されている。それにもかかわらず、特定されたモジュールの実行可能プログラムは物理的に一緒に置かれることを要しない。しかし、異なるロケーションに保管された異なるインストラクションを含んでよく、論理的に一緒に結合された場合に、モジュールを構成し、モジュールのためにステート（ｓｔａｔｅ）された目的を達成する。

【００７６】

実際に、実行可能コードのモジュールは、単一のインストラクション、または、多くのインストラクションであってよく、かつ、いくつかの異なるコードセグメント上で、異なるプログラムの中で、そして、いくつかのメモリデバイスにわたり、配信されてもよい。同様に、オペレーションのデータは、モジュールの中で、ここにおいて特定され、かつ、示されてよく、そして、あらゆる好適な形式で具現化され、かつ、あらゆる好適なタイプのデータ構造の中で編成されてよい。オペレーションのデータは、単一のデータセットと

して収集されてよく、または、異なるストレージデバイス上を含む異なるロケーションにわたり配信されてよく、そして、少なくとも部分的に、システムまたはネットワーク上の電気的信号として単に存在してよい。モジュールは、受動的または能動的であってよく、所望のファンクションを実行するように動作可能なエージェントを含んでいる。

【００７７】

この明細書の全体にわたり「実施例（“ａｎ　ｅｘａｍｐｌｅ”）」または「典型的（”ｅｘｅｍｐｌａｒｙ“）」への言及は、実施例に関して説明された所定の特徴、構成、または、特性が、本発明の少なくとも一つの実施例に含まれていることを意味するものである。従って、この明細書の全体にわたる種々の場所において表れるフレーズ「一つの実施例において（”ｉｎ　ａｎ　ｅｘａｍｐｌｅ”）」または用語「典型的（”ｅｘｅｍｐｌａｒｙ“）」は、必ずしも全てが同一の実施例について言及するものではない。

【００７８】

ここにおいて使用されるように、複数のアイテム、構造エレメント、組成エレメント、及び/又は、マテリアルは、利便性のために共通のリストにおいて表わされてよい。しかしながら、これらのリストは、リストの各メンバーが分離した特有のメンバーとして個別に特定されるように、理解されるべきである。従って、そうしたリストに係る個々のメンバーは、反対への指示なく、単に共通のグループにおけるそれらの表現に基づいて、同一リストに係るあらゆる他のメンバーの事実上の均等物として理解されるべきではない。加えて、本発明に係る種々の実施例と例示は、それらの種々のコンポーネントに対する代替物と一緒にここにおいて参照されてよい。そうした実施例、例示、および、代替物は、お互いの事実上の均等物として理解されるべきではなく、本発明に係る分離した自律的な表現として考慮されるべきであることが、理解される。

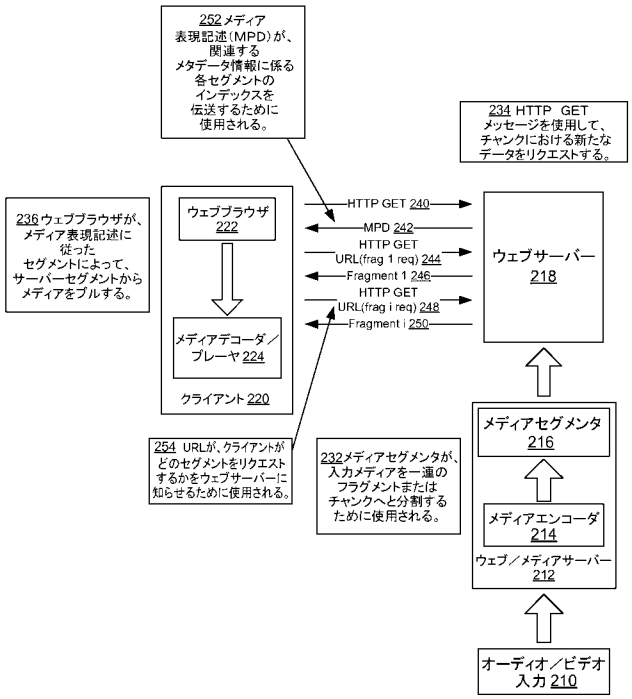
【００７９】

さらに、説明された特徴、構成、または、特性は、一つまたはそれ以上の実施例において、あらゆる好適なやり方で組み合わせることができる。以降の説明においては、本発明開示に係る実施例の完全な理解を提供するために、レイアウト、距離、ネットワーク等の実施例といった、特定の詳細が数多く提供される。当業者にとっては、しかしながら、特定の詳細の一つまたはそれ以上がなくても、または、他の方法、コンポーネント、レイアウト、等を用いても、本発明が実行され得ることが明らかである。他のインスタンスにおいて、よく知られた構造、マテリアル、または、オペレーションは、本発明の態様が不明瞭となるのを避けるために、示されないか、または、詳細には説明されない。

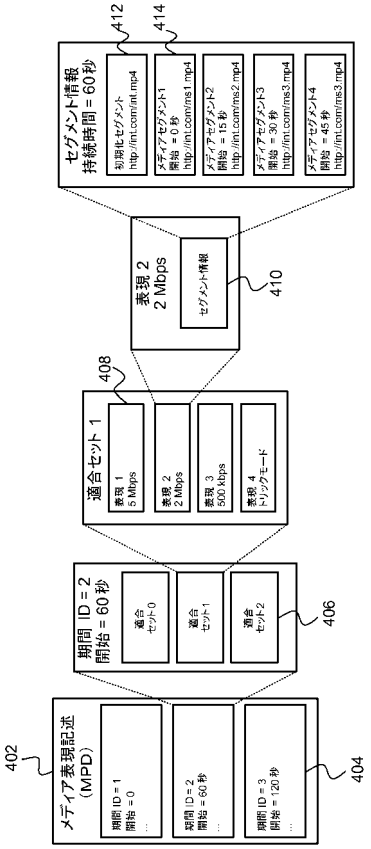
【００８０】

上記の実施例は、一つまたはそれ以上の所定のアプリケーションにおける本発明の本質を説明するものであるが、当業者にとっては、発明的才能を実行することなく、かつ、本発明の本質および概念から逸脱することなく、実施に係る形式、使用、および、詳細において数多くの変更が成され得ることが明らかであろう。従って、以降の特許請求の範囲による明示を除いて、本発明が限定されるように意図されたものではない。

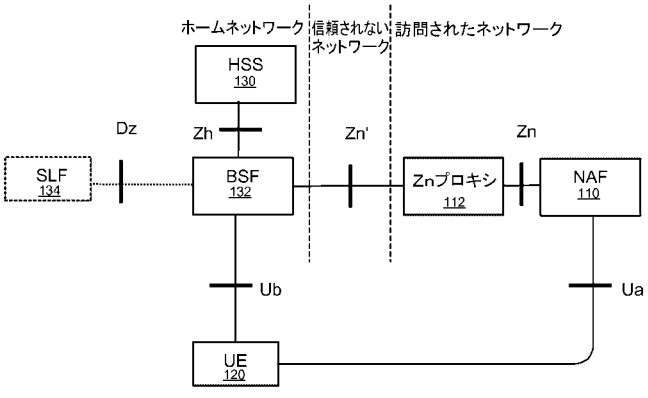
【図１】


252 メディア表現記述（MPD）が、関連するメタデータ情報に係る各セグメントのインデックスを伝送するために使用される。
234 HTTP GET メッセージを使用して、チャンクにおける新たなデータをリクエストする。
236 ウェブブラウザが、メディア表現記述に従ったセグメントによって、サーバーセグメントからメディアをプルする。
ウェブブラウザ 222
メディアデコーダ／プレーヤ 224
クライアント 220
HTTP GET 240
MPD 242
HTTP GET URL(frag 1 req) 244
Fragment 1 246
HTTP GET URL(frag i req) 248
Fragment i 250
ウェブサーバー 218
メディアセグメンタ 216
メディアエンコーダ 214
ウェブ／メディアサーバー 212
オーディオ／ビデオ入力 210
254 URLが、クライアントがどのセグメントをリクエストするかをウェブサーバーに知らせるために使用される。
232 メディアセグメンタが、入力メディアを一連のフラグメントまたはチャンクへと分割するために使用される。

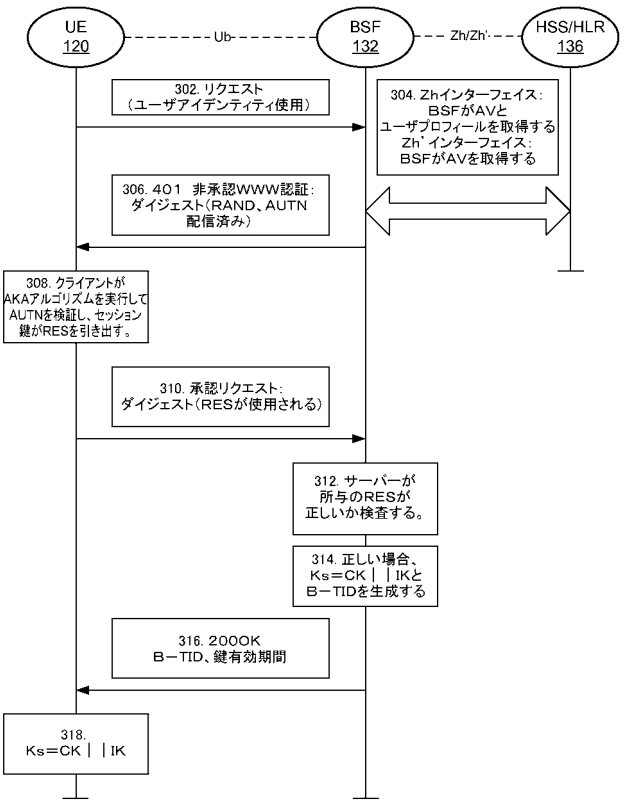
【図２】


412
414
セグメント情報 持続時間 = 60 秒
初期化セグメント http://int.com/int.mp4
メディアセグメント1 開始 = 0 秒 http://int.com/ms1.mp4
メディアセグメント2 開始 = 15 秒 http://int.com/ms2.mp4
メディアセグメント3 開始 = 30 秒 http://int.com/ms3.mp4
メディアセグメント4 開始 = 45 秒 http://int.com/ms3.mp4
表現 2 2 Mbps
セグメント情報
410
408
適合セット 1
表現 1 5 Mbps
表現 2 2 Mbps
表現 3 500 kbps
表現 4 トリックモード
期間 ID = 2 開始 = 60 秒
適合セット 0
適合セット 1
適合セット 2
406
メディア表現記述（MPD）
期間 ID = 1 開始 = 0
期間 ID = 2 開始 = 60 秒
期間 ID = 3 開始 = 120 秒
402
404

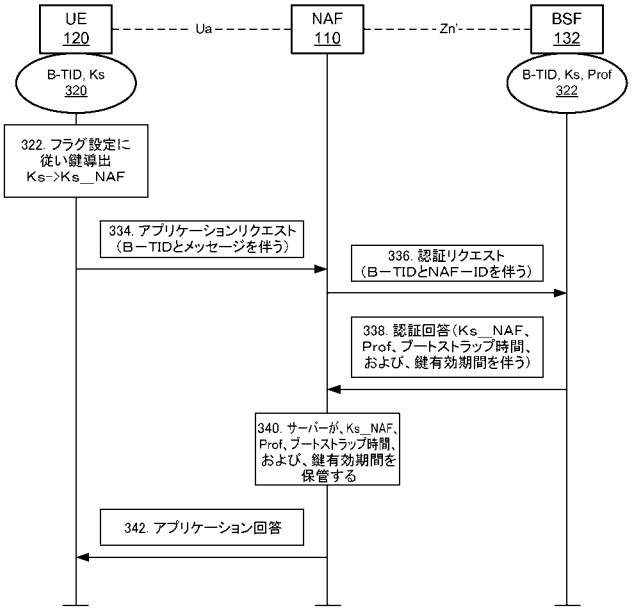
【図３】


ホームネットワーク
信頼されないネットワーク
訪問されたネットワーク
HSS 130
Dz
Zh
Zn'
Zn
SLF 134
BSF 132
Znプロキシ 112
NAF 110
Ub
Ua
UE 120

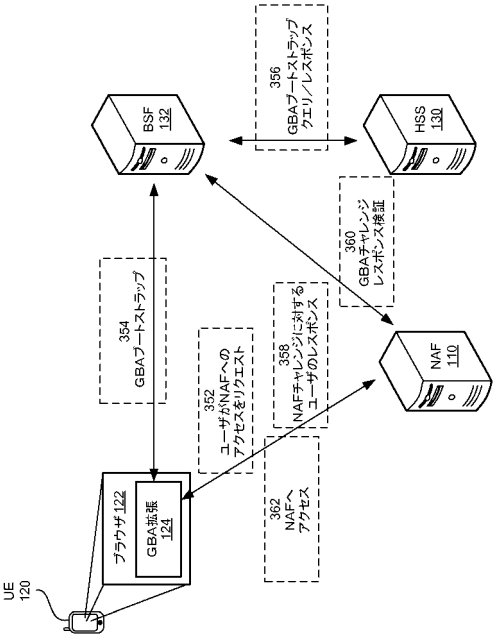
【図４】


UE 120
Ub
BSF 132
Zh/Zh'
HSS/HLR 136
302. リクエスト（ユーザアイデンティティ使用）
304. Zhインターフェイス：BSFがAVとユーザプロフィールを取得する Zh' インターフェイス：BSFがAVを取得する
306. 401 非承認WWW認証：ダイジェスト（RAND、AUTN 配信済み）
308. クライアントがAKAアルゴリズムを実行してAUTNを検証し、セッション鍵がRESを引き出す。
310. 承認リクエスト：ダイジェスト（RESが使用される）
312. サーバーが所与のRESが正しいか検査する。
314. 正しい場合、Ks＝CK｜｜IKとB－TIDを生成する
316. 200OK B－TID、鍵有効期間
318. Ks＝CK｜｜IK

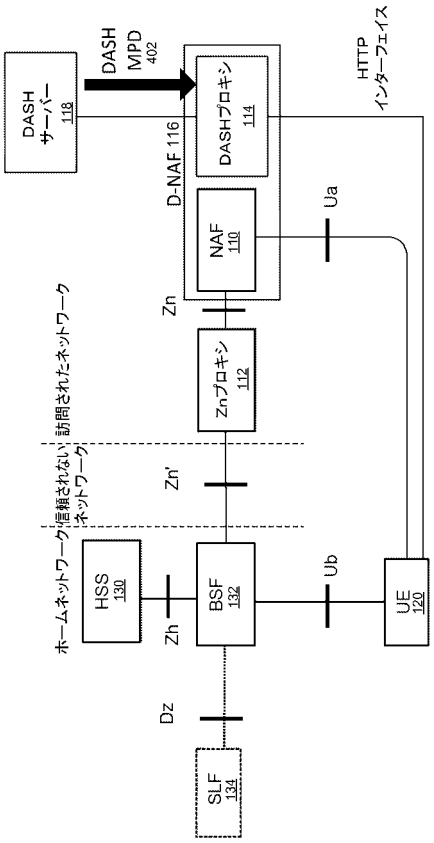
【図５】



【図６】



【図７】



【図８】

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:mpeg:dash:schema:sea:2013"
   attributeFormDefault="unqualified"
   elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns="urn:mpeg:dash:schema:sea:2013" xmlns:dash="urn:mpeg:dash:schema:mpd:2011">

   <!—URL Authenticity signaling -->

   <xs:complexType name="URLAuthenticity">
      <xs:attribute name="keyUriTemplate" type="xs:anyURI" use="required"/>
      <xs:attribute name="authSchemeIdUri" type="xs:anyURI" use="required"/>
      <xs:attribute name="authUrlTemplate" type="xs:anyURI" use="required"/>
      <xs:attribute name="authTagLength" type="xs:unsignedInt"/>
      <xs:attribute name="validityExpires" type="xs:dateTime" use="required"/>
      <xs:attribute name="inbandAuthTag" type="xs:boolean"/>
   </xs:complexType>
</xs:schema>
```

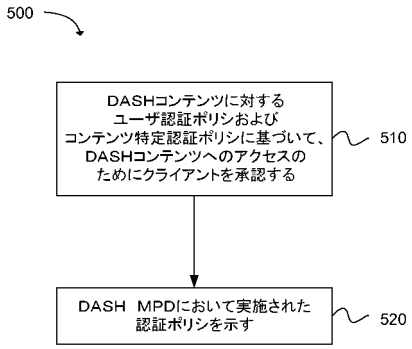
（表2）

【図９】

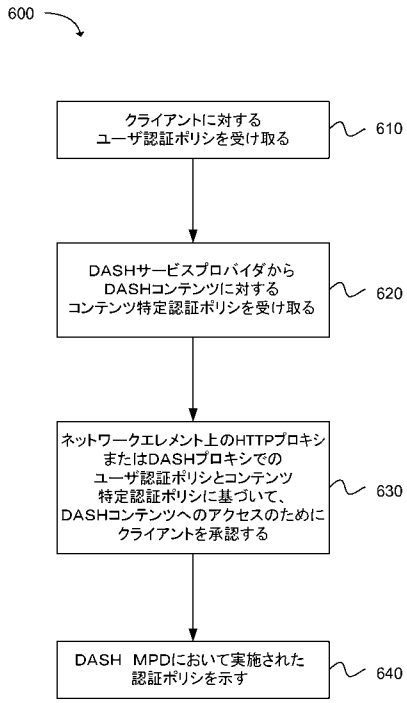
```
<!-- Representation base (common attributes and elements) -->
<xs:complexType name="RepresentationBaseType">
 <xs:sequence>
  <xs:element name="FramePacking" type="DescriptorType" minOccurs="0" maxOccurs="unbounded"/>
  <xs:element name="AudioChannelConfiguration" type="DescriptorType" minOccurs="0"
maxOccurs="unbounded"/>
  <xs:element name="ContentProtection" type="DescriptorType" minOccurs="0" maxOccurs="unbounded"/
>
  <xs:element name="ContentAuthorization" type="DescriptorType" minOccurs="0"
maxOccurs="unbounded"/>
  <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
 </xs:sequence>
 <xs:attribute name="profiles" type="xs:string"/>
 <xs:attribute name="width" type="xs:unsignedInt"/>
 <xs:attribute name="height" type="xs:unsignedInt"/>
 <xs:attribute name="sar" type="RatioType"/>
 <xs:attribute name="frameRate" type="FrameRateType"/>
 <xs:attribute name="audioSamplingRate" type="xs:string"/>
 <xs:attribute name="mimeType" type="xs:string"/>
 <xs:attribute name="segmentProfiles" type="xs:string"/>
 <xs:attribute name="codecs" type="xs:string"/>
 <xs:attribute name="maximumSAPPeriod" type="xs:double"/>
 <xs:attribute name="startWithSAP" type="SAPType"/>
 <xs:attribute name="maxPlayoutRate" type="xs:double"/>
 <xs:attribute name="codingDependency" type="xs:boolean"/>
 <xs:attribute name="scanType" type="VideoScanType"/>
 <xs:anyAttribute namespace="##other" processContents="lax"/>
</xs:complexType>

<!-- Stream Access Point type enumeration -->
<xs:simpleType name="SAPType">
 <xs:restriction base="xs:unsignedInt">
  <xs:minInclusive value="0"/>
  <xs:maxInclusive value="6"/>
 </xs:restriction>
</xs:simpleType>

<!-- Video Scan type enumeration -->
<xs:simpleType name="VideoScanType">
 <xs:restriction base="xs:string">
  <xs:enumeration value="progressive"/>
  <xs:enumeration value="interlaced"/>
  <xs:enumeration value="unknown"/>
 </xs:restriction>
</xs:simpleType>
```

（表4）

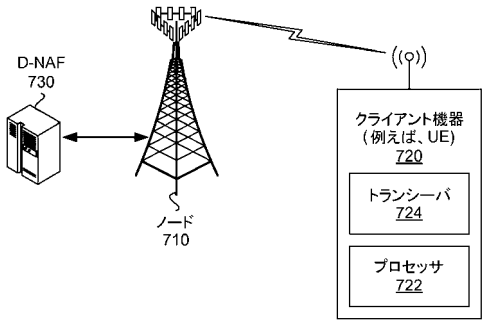
【図１０】



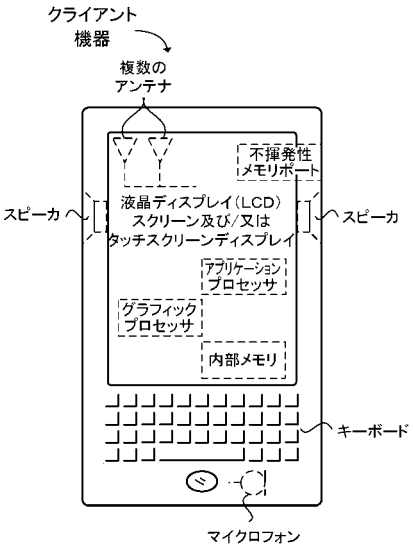
【図１１】



【図１２】



【図１３】


クライアント
機器
複数の
アンテナ
不揮発性
メモリポート
スピーカ
液晶ディスプレイ（LCD）
スクリーン及び/又は
タッチスクリーンディスプレイ
スピーカ
アプリケーション
プロセッサ
グラフィック
プロセッサ
内部メモリ
キーボード
マイクロフォン

【外国語明細書】
2017184260000001.pdf