

(19) 日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2016-512356

(P2016-512356A)

(43) 公表日 平成28年4月25日 (2016. 4. 25)

(51) Int. Cl.		F I		テーマコード (参考)
G06F 13/00	(2006.01)	G06F 13/00	540P	5B084
G06Q 30/02	(2012.01)	G06Q 30/02	150	5L049

審査請求 未請求 予備審査請求 有 (全 22 頁)

(21) 出願番号	特願2016-500336 (P2016-500336)	(71) 出願人	507364838
(86) (22) 出願日	平成26年2月21日 (2014. 2. 21)		クアルコム, インコーポレイテッド
(85) 翻訳文提出日	平成27年9月10日 (2015. 9. 10)		アメリカ合衆国 カリフォルニア 921
(86) 国際出願番号	PCT/US2014/017749		21 サン ディエゴ モアハウス ドラ
(87) 国際公開番号	W02014/149371		イブ 5775
(87) 国際公開日	平成26年9月25日 (2014. 9. 25)	(74) 代理人	100108453
(31) 優先権主張番号	61/792, 454		弁理士 村山 靖彦
(32) 優先日	平成25年3月15日 (2013. 3. 15)	(74) 代理人	100163522
(33) 優先権主張国	米国 (US)		弁理士 黒田 晋平
(31) 優先権主張番号	14/050, 055	(72) 発明者	イニアン・マオ
(32) 優先日	平成25年10月9日 (2013. 10. 9)		アメリカ合衆国・カリフォルニア・921
(33) 優先権主張国	米国 (US)		21-1714・サン・ディエゴ・モアハ
			ウス・ドライブ・5775

最終頁に続く

(54) 【発明の名称】 広告ダウンロードの検証

(57) 【要約】

広告コンテンツがクライアントによってダウンロードされたことを検証するための方法およびシステムについて説明する。ストリーミングクライアントが広告コンテンツを広告サーバに要求したとき、ストリーミングクライアントは1つまたは複数のベリファイアを広告サーバから受け取る。ストリーミングクライアントは、ベリファイアに関連する情報をメディアサーバに送る。メディアサーバは、ベリファイアに関連する情報に基づいてストリーミングクライアントへの広告コンテンツのストリーミングを妥当性検査するように構成される。

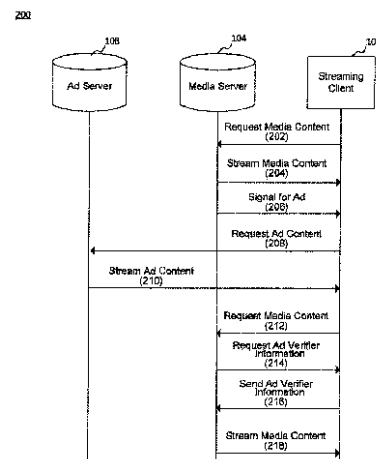


Figure 2

【特許請求の範囲】**【請求項 1】**

ストリーミングクライアントによって広告コンテンツを広告サーバに要求するステップと、

1つまたは複数のベリファイアを前記広告サーバから受け取るステップと、

前記ベリファイアに関連する情報をメディアサーバに送るステップであって、前記メディアサーバが、前記ベリファイアに関連する前記情報に基づいて前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査するように構成されたステップとを含むプロセッサ実装方法。

【請求項 2】

10

ベリファイアが、共有秘密暗号鍵に基づくデジタル署名を含み、前記共有秘密暗号鍵が前記広告サーバおよび前記メディアサーバによって記憶され、

前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査することが、前記共有秘密暗号鍵にさらに基づく、請求項1に記載の方法。

【請求項 3】

ベリファイアが、公開-秘密暗号鍵ペアに基づくデジタル署名を含み、

前記公開-秘密暗号鍵ペアの秘密暗号鍵が前記広告サーバによって記憶され、

前記公開-秘密暗号鍵ペアの公開暗号鍵が前記メディアサーバによって記憶され、

前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査することが、前記公開暗号鍵にさらに基づく、請求項1に記載の方法。

20

【請求項 4】

前記ベリファイアが、セッション識別子、本体指定子、およびデジタル署名、のうちの少なくとも1つを含む、請求項1に記載の方法。

【請求項 5】

セッション識別子が、タイムスタンプ、ノンス、およびクライアント識別子、のうちの少なくとも1つを含む、請求項4に記載の方法。

【請求項 6】

本体指定子がバイト範囲を含み、前記クライアントが、前記バイト範囲に対応するデータのハッシュを生成する、請求項4に記載の方法。

【請求項 7】

30

ベリファイアが、ISOベースメディアファイルフォーマットに従ってフォーマットされたメディアファイルの自由空間ボックスに含まれる、請求項1に記載の方法。

【請求項 8】

前記ベリファイアが広告ストリーム内のランダムな場所に位置する、請求項1に記載の方法。

【請求項 9】

ベリファイアがブラウザクッキー中で前記広告サーバから受け取られる、請求項1に記載の方法。

【請求項 10】

40

ベリファイアがローカリーストアドオブジェクト中で前記広告サーバから受け取られる、請求項1に記載の方法。

【請求項 11】

ストリーミングクライアントのプロセッサによって実行可能なプログラムコードを記憶するためのコンピュータ可読記憶媒体であって、前記プログラムコードが、

広告コンテンツを広告サーバに要求するためのプログラムコードと、

1つまたは複数のベリファイアを前記広告サーバから受け取るためのプログラムコードと、

前記ベリファイアに関連する情報をメディアサーバに送るためのプログラムコードとを含み、前記メディアサーバが、前記ベリファイアに関連する前記情報に基づいて前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査するよう

50

に構成された、コンピュータ可読記憶媒体。

【請求項 1 2】

前記ベリファイアが、セッション識別子、本体指定子、およびデジタル署名、のうちの少なくとも1つを含む、請求項11に記載のコンピュータ可読記憶媒体。

【請求項 1 3】

セッション識別子が、タイムスタンプ、ノンス、およびクライアント識別子、のうちの少なくとも1つを含む、請求項12に記載のコンピュータ可読記憶媒体。

【請求項 1 4】

本体指定子がバイト範囲を含み、前記バイト範囲に対応するデータのハッシュを生成するためのプログラムコードをさらに含む、請求項12に記載のコンピュータ可読記憶媒体。

【請求項 1 5】

メモリと、

前記メモリに結合されたプロセッサとを備えるクライアントデバイスであって、前記プロセッサが、

広告コンテンツを広告サーバに要求するステップと、

1つまたは複数のベリファイアを前記広告サーバから受け取るステップと、

前記ベリファイアに関連する情報をメディアサーバに送るステップであって、前記メディアサーバが、前記ベリファイアに関連する前記情報に基づいて前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査するように構成されたステップとを含む方法を実施するためのプロセッサ実行可能命令で構成された、クライアントデバイス。

【請求項 1 6】

前記ベリファイアが、セッション識別子、本体指定子、およびデジタル署名、のうちの少なくとも1つを含む、請求項15に記載のクライアントデバイス。

【請求項 1 7】

セッション識別子が、タイムスタンプ、ノンス、およびクライアント識別子、のうちの少なくとも1つを含む、請求項16に記載のクライアントデバイス。

【請求項 1 8】

本体指定子がバイト範囲を含み、前記バイト範囲に対応するデータのハッシュを生成するためのプログラムコードをさらに含む、請求項16に記載のクライアントデバイス。

【請求項 1 9】

メディアサーバによってストリーミングメディアをストリーミングクライアントに送るステップと、

1つまたは複数のベリファイアに関連する情報を前記ストリーミングクライアントから受け取るステップであって、前記ベリファイアが広告コンテンツに関連するものであるステップと、

前記ベリファイアに関連する前記情報に基づいて前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査するステップであって、前記妥当性検査が不成功である場合に、前記ストリーミングメディアを送る前記ステップが停止されるステップとを含むプロセッサ実装方法。

【請求項 2 0】

ベリファイアが、共有秘密暗号鍵に基づくデジタル署名を含み、前記共有秘密暗号鍵が、前記メディアサーバと、前記広告コンテンツを提供する広告サーバとによって記憶され、

前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査するステップが、前記共有秘密暗号鍵にさらに基づく、請求項19に記載の方法。

【請求項 2 1】

ベリファイアが、公開-秘密暗号鍵ペアの秘密暗号鍵を使用して生成されたデジタル署名を含み、

前記公開-秘密暗号鍵ペアの前記秘密暗号鍵が、前記広告コンテンツを提供する広告サ

10

20

30

40

50

ーバによって記憶され、

前記公開-秘密暗号鍵ペアの公開暗号鍵が前記メディアサーバによって記憶され、

前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査するステップが、前記公開暗号鍵にさらに基づく、請求項19に記載の方法。

【請求項22】

前記ベリファイアに関連する前記情報が、署名と、前記広告コンテンツに対応するデータの少なくとも一部のハッシュとを含み、前記広告コンテンツのストリーミングを妥当性検査するステップが、前記公開暗号鍵を前記ハッシュに適用して結果値を得て、前記結果値を前記署名と比較するステップを含む、請求項19に記載の方法。

【請求項23】

前記広告コンテンツのストリーミングを妥当性検査するステップが、ブラウザクッキー内に含まれるデジタル署名を妥当性検査するステップを含む、請求項19に記載の方法。

【請求項24】

前記広告コンテンツのストリーミングを妥当性検査するステップが、ローカリーストアドオブジェクト内に含まれるデジタル署名を妥当性検査するステップを含む、請求項19に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

本出願は、2013年3月15日に提出されたADVERTISING DOWNLOAD VERIFICATIONという名称の米国仮特許出願第61/792,454号に対する優先権およびこの仮出願の利益を主張するものであり、この仮出願の全体は参照により本明細書に組み込まれる。

【背景技術】

【0002】

音楽やビデオなどのメディアは、メディアコンテンツを記憶するサーバから、パーソナルコンピュータやモバイルデバイスなどのユーザデバイス上で稼働するクライアントソフトウェアに、ネットワークを介してストリーミングされることがある。多くのメディアプロバイダは、広告によってサポートされるビジネスモデルを使用する。広告主は、メディアコンテンツの再生前にストリーミングされるかまたは再生中に間欠的にストリーミングされる広告など、メディアとともに提供される広告コンテンツに対して、メディアプロバイダに代金を支払うことができる。広告コンテンツにより、メディアプロバイダは、メディアコンテンツをユーザに無料でまたは割引価格で提供することができる。

【0003】

ユーザの中には、要求したメディアコンテンツとともに広告コンテンツが提供されるのを回避しながら、広告によってサポートされるメディアを得るための対策を講じる者もいる。ブラウザにまたはメディア再生アプリケーションに適用されるソフトウェアが、メディアコンテンツの送達時に広告がダウンロードされるのをブロックすることができる。たとえば、ブラウザプラグインを使用して、ブラウザ内メディア再生アプリケーションに送達される広告コンテンツがブロックされる。

【0004】

広告コンテンツをブロックするか、広告コンテンツを修正するか、または広告コンテンツを代替コンテンツで置き換えるためのソフトウェアが広く使用されることは、メディアコンテンツの開発および提供を継続するコンテンツプロバイダの能力を脅かす可能性がある。

【発明の概要】

【発明が解決しようとする課題】

【0005】

広告コンテンツがクライアントによってダウンロードされたことを検証するための方法およびシステムについて説明する。

10

20

30

40

50

【課題を解決するための手段】

【0006】

一実施形態では、方法について説明するが、この方法では、ストリーミングクライアントが、広告コンテンツを広告サーバに要求する。ストリーミングクライアントは、1つまたは複数のベリファイア(verifier)を広告サーバから受け取る。ストリーミングクライアントは、ベリファイアに関連する情報をメディアサーバに送る。メディアサーバは、ベリファイアに関連する情報に基づいてストリーミングクライアントへの広告コンテンツのストリーミングを妥当性検査するように構成される。

【0007】

別の実施形態では、クライアントのプロセッサによって実行可能なプログラムコードを記憶するための非一時的コンピュータ可読媒体について説明する。非一時的コンピュータ可読媒体は、広告コンテンツを広告サーバに要求するためのプログラムコードを含む。非一時的コンピュータ可読媒体はさらに、1つまたは複数のベリファイアを広告サーバから受け取るためのプログラムコードを含む。非一時的コンピュータ可読媒体は追加で、ベリファイアに関連する情報をメディアサーバに送るためのプログラムコードを含む。メディアサーバは、ベリファイアに関連する情報に基づいてストリーミングクライアントへの広告コンテンツのストリーミングを妥当性検査するように構成される。

【0008】

さらに他の実施形態では、メモリと、メモリに結合されたプロセッサとを有するクライアントデバイスについて説明する。プロセッサは、広告コンテンツを広告サーバに要求するステップと、1つまたは複数のベリファイアを広告サーバから受け取るステップと、ベリファイアに関連する情報をメディアサーバに送るステップとを含む方法を実施するためのプロセッサ実行可能命令で構成され、メディアサーバは、ベリファイアに関連する情報に基づいてストリーミングクライアントへの広告コンテンツのストリーミングを妥当性検査するように構成される。

【0009】

さらに他の実施形態では、方法について説明するが、この方法では、ストリーミングメディアがメディアサーバによってストリーミングクライアントに送られる。1つまたは複数のベリファイアに関連する情報が、ストリーミングクライアントから受け取られる。ベリファイアは、広告コンテンツに関連する。ベリファイアに関連する情報に基づいて、ストリーミングクライアントへの広告コンテンツのストリーミングが妥当性検査される。妥当性検査が不成功である場合、ストリーミングメディアを送ることは停止される。

【図面の簡単な説明】

【0010】

【図1】メディアダウンロード検証が行われ得るシステムに関する例示的なシステム図である。

【図2】一実施形態による、アドサーバとメディアサーバとストリーミングクライアントとの間の通信を示す例示的なシーケンス図である。

【図3】アドベリファイアに含まれ得る例示的なコンポーネントを示す図である。

【図4】一実施形態による、アドコンテンツがストリーミングクライアントによってダウンロードされたことを検証するための例示的な流れ図である。

【図5】アドベリファイア中でバイト範囲が指定されているときに、アドコンテンツがストリーミングクライアントによってダウンロードされたことを検証するための例示的な流れ図である。

【図6】ブラウザベースのメディアプレーヤによってアドコンテンツがストリーミングクライアントにダウンロードされたことを検証するための例示的な流れ図である。

【図7】コンピュータシステムの例示的なブロック図である。

【発明を実施するための形態】

【0011】

メディアコンテンツをメディアサーバから受け取るストリーミングクライアントは、メ

10

20

30

40

50

ディアコンテンツに関連する広告コンテンツがダウンロードされないようにするためのソフトウェアによって修正されることがある。たとえば、ストリーミングクライアントは、広告コンテンツを指定の広告サーバからダウンロードする代わりに、短い継続時間のメディアを非広告サーバからダウンロードするように、修正されることがある。広告コンテンツのダウンロードを回避するように修正されたストリーミングクライアントにメディアコンテンツが送達されるのを防止するために、1つまたは複数の広告ベリファイアが広告サーバによって生成されてよく、広告ベリファイアは、広告コンテンツがストリーミングクライアントに送られるときに、ストリーミングクライアントに送られてよい。ストリーミングクライアントは、広告ベリファイアに関連する情報をメディアサーバに送ることができる。メディアサーバは、ストリーミングクライアントから受け取った情報を使用して、ストリーミングクライアントが広告コンテンツをアドサーバからダウンロードしたことを検証することができる。ストリーミングクライアントが広告コンテンツをアドサーバからダウンロードしたことをメディアサーバが検証できない場合は、メディアサーバは、ストリーミングクライアントへのメディアコンテンツの後続のストリーミングを防止することができる。本明細書において、「ダウンロード」(ストリーミングクライアントによる広告コンテンツのダウンロードなど)という用語は、ストリーミング(アドサーバからストリーミングクライアントへの広告コンテンツのストリーミングなど)を示すことがある。いくつかの事例では、「広告コンテンツ」または「コンテンツ」は、実行中に他の方法で解釈される実行可能コードまたは命令を含むことがある。

10

20

30

40

50

【0012】

図1に、例示的なシステム図100を示す。メディアコンテンツが、メディアサーバ104からストリーミングクライアント102に提供されてよい。「クライアント」と「ストリーミングクライアント」という用語は、本明細書では交換可能に使用される。

【0013】

メディアコンテンツは、メディアコンテンツデータベース106に記憶されていてよい。メディアコンテンツデータベース106は、メディアサーバ104上に記憶されていてもよく、または、メディアサーバ104に通信可能に結合された1つもしくは複数のサーバ上に記憶されていてもよい。メディアコンテンツは、ライブウェブキャストコンテンツや記憶済みメディアコンテンツなど、ある時間期間にわたりストリーミングクライアント102によって受け取られることが可能な、ビデオ、オーディオ、ストリーミングテキスト、および他の任意のコンテンツを含む可能性がある。「メディアコンテンツ」と「メディア」という用語は、本明細書では交換可能に使用される。

【0014】

広告コンテンツが、アドサーバ108からストリーミングクライアント102に提供されてよい。広告コンテンツは、アドコンテンツデータベース110に記憶されていてよい。アドコンテンツデータベース110は、アドサーバ108上に記憶されていてもよく、または、アドサーバ108に通信可能に結合された1つもしくは複数のサーバ上に記憶されていてもよい。広告コンテンツは、メディアコンテンツの上に重ねられるビデオ、オーディオ、広告画像および/もしくはテキスト、または他のコンテンツを含む場合がある。広告コンテンツは、メディアコンテンツの前に、メディアコンテンツの後に、メディアコンテンツと同時に、またはメディアコンテンツ内で所々に挿入されて、示される場合がある。通常、メディアコンテンツは、ストリーミングクライアント102のユーザインターフェースをたとえば使用して、ユーザによって要求されるコンテンツである。広告コンテンツは、ユーザによって要求されるメディアコンテンツに関連してストリーミングクライアント102に提供される、ユーザによって要求されないコンテンツとすることができる。「広告」と「アド」という用語は、本明細書では交換可能に使用される。

【0015】

ストリーミングクライアント102は、メディア再生機能を提供するように構成されたデバイスとすることができる。たとえば、ストリーミングクライアント102は、パーソナルコンピュータ、または、セルラーホンやメディアプレーヤやタブレットやラップトップコ

ンピュータなどのモバイルデバイス、または、ストリーミングメディアを再生できる他のデバイスとすることができる。ストリーミングクライアント102は、スタンドアロンのメディア再生アプリケーション112や、インターネットブラウザ116中で稼働するように構成されたブラウザベースのメディアプレーヤ114など、メディアを再生するためのコードを実行することができる。

【0016】

ストリーミングクライアント102、メディアサーバ104、アドサーバ108、メディアコンテンツデータベース106、アドコンテンツデータベース110のうちの1つまたは複数は、サーバコンピュータなど、同じデバイス上に位置することができる。いくつかの実施形態では、ストリーミングクライアント102は、ネットワーク118などのネットワークを介して、メディアコンテンツおよび広告コンテンツを受け取る。ネットワーク118は、ワイドエリアネットワーク(WAN)、ローカルエリアネットワーク(LAN)、インターネット、セルラーネットワーク、1つもしくは複数の他のネットワーク、またはこれらの組合せとすることができる。

10

【0017】

1つまたは複数の暗号鍵(たとえば、共有秘密鍵、または公開-秘密鍵ペア)が、アドサーバ108とメディアサーバ104との間で確立されてよい。一実施形態では、アドサーバ108は、署名鍵(すなわち、公開-秘密鍵ペアの秘密鍵)を保持することになり、メディアサーバ104は、検証鍵(すなわち、公開-秘密鍵ペアの公開鍵)を保持することになる。たとえば、アドサーバ108は、共有秘密鍵または公開-秘密鍵ペアを生成し、共有秘密鍵または公開鍵をメディアサーバ104に送ることができる。アドサーバ108は、各ストリーミングセッションの前に(たとえば、ストリーミングセッションが開始されるたびにアドサーバ108によってメディアサーバ104から受け取られる、鍵を求める要求に回答して)鍵をメディアサーバ104に送ることができ、または、アドサーバ108が広告コンテンツをストリーミングクライアント102に送るたびにその前に鍵をメディアサーバ104に送ることができ、または、広告コンテンツをストリーミングクライアント102に送る前の別の時点で鍵をメディアサーバ104に送ることができる。一実施形態では、アドサーバ108は、セキュアプロトコルを使用して鍵を送ることができ、たとえば、鍵を認証するのに使用できる証明書とともに鍵を送ることができる。

20

【0018】

ストリーミングクライアント102が広告コンテンツをアドサーバ108から受け取るとき、ストリーミングクライアント102はまた、1つまたは複数のアドベリファイア(ad verifier)もアドサーバ108から受け取ることができる。アドベリファイアは、アドコンテンツの前に、アドコンテンツの後に、またはアドコンテンツの一部として、ストリーミングクライアント102によって受け取られてよい。アドベリファイアは、特定のストリーミングセッションについての識別子、タイムスタンプ、特定のストリーミングクライアントの識別子、アドストリームのバイト範囲を示す情報、および、アドサーバ108によって記憶された鍵を使用して生成されたデジタル署名、のうちの1つまたは複数を含めた情報を含んでよい。「アドベリファイア」と「ベリファイア」という用語は、本明細書では交換可能に使用される。

30

40

【0019】

ストリーミングクライアント102は、アドベリファイアに関連する情報をメディアサーバ104に送信することができる。メディアサーバ104は、アドサーバ108からストリーミングされたアドコンテンツをストリーミングクライアント102が受け取ったことを検証するために、ストリーミングクライアント102から受け取った情報に共有秘密鍵または公開鍵を適用することができる。

【0020】

図2に、一実施形態による、アドサーバとメディアサーバとストリーミングクライアントとの間の通信を示す例示的なシーケンス図200を示す。202に示されるように、ストリーミングクライアント102が、メディアコンテンツをメディアサーバ104に要求することがで

50

きる。204に示されるように、メディアサーバ104は、要求に回答して、メディアコンテンツをストリーミングクライアント102にストリーミングすることができる。206に示されるように、メディアサーバ104は、ストリーミングクライアントが広告コンテンツをダウンロードすることが必要になることを、ストリーミングクライアント102にシグナリングすることができる。いくつかの実施形態では、広告に関するシグナリング206は、メディアコンテンツの要求202およびメディアコンテンツのストリーミング204の前に発生してもよい。広告に関するシグナリング206は、定期的に発生するか、またはメディアコンテンツストリーミング204の間に事前定義済みの間隔で発生する。様々な実施形態で、広告に関するシグナリング206は、メディアコンテンツ204に含まれる情報、メディアコンテンツから独立してメディアサーバ104からストリーミングクライアント102に送られる情報、または、ストリーミングクライアント102によって実行されるアプリケーション(メディア再生アプリケーション112もしくはブラウザベースのメディアプレーヤ114など)のコマンド、のうちの1つまたは複数に基づく場合がある。一実施形態では、メディアサーバ104は、JavaScript(登録商標)ルーチンなど、広告コンテンツを得るためにストリーミングクライアント102によって実行されることになるコードを送ることができる。

10

【0021】

208に示されるように、ストリーミングクライアント102は、広告に関するシグナル206に回答して、広告コンテンツを求める要求をアドサーバ108に送ることができる。210に示されるように、アドサーバ108は、アドコンテンツを求める要求208に回答して、アドコンテンツをストリーミングクライアント102にストリーミングすることができる。アドコンテンツストリームには、1つまたは複数のアドベリファイアが含まれてよい。別法として、アドベリファイアは、アドコンテンツの送信前または後に、アドサーバ108からストリーミングクライアント102に提供されてもよい。アドブロッキング修正がなされたストリーミングクライアントは、208を迂回して、アドコンテンツを要求しない可能性があり、または、広告に関するシグナル206に回答して、広告サーバでないサーバに代用コンテンツを要求する可能性がある。

20

【0022】

いくつかの実施形態では、212に示されるように、ストリーミングクライアント102は、アドコンテンツをアドサーバ108から受け取った後でメディアコンテンツを要求することができる。214に示されるように、メディアサーバ104は、ストリーミングクライアント102がアドサーバ108から受け取った1つまたは複数のアドベリファイアに関連する情報を要求することができる。216に示されるように、ストリーミングクライアント102は、要求214に回答して、1つまたは複数のアドベリファイアに関連する情報をメディアサーバ104に送ることができる。1つまたは複数のアドベリファイアに関連する情報は、署名、210で提供された広告ストリームの一部もしくは全部のハッシュ、セッション識別子、ストリーミングクライアント識別子、タイムスタンプ、暗号ノンス、またはこれらの組合せ(タイムスタンプとノンスとストリーミングクライアント識別子との連結など)、のうちの1つまたは複数を含んでよい。

30

【0023】

アドベリファイアに関連する情報をメディアサーバ104が受け取ると、メディアサーバ104は、アドベリファイアに関連する情報を使用して、上記の210で示された、ストリーミングクライアント102への広告コンテンツのストリーミングを妥当性検査することができる。広告コンテンツがストリーミングクライアント102によってダウンロードされたらメディアサーバ104が判定した場合は、218に示されるように、メディアサーバ104は、メディアコンテンツをストリーミングクライアント102にストリーミングすることができる。広告コンテンツがストリーミングクライアント102によってダウンロードされなかったらメディアサーバ104が判定した場合は、メディアサーバ104は、ストリーミングクライアント102へのメディアコンテンツのストリーミングを停止することができる。

40

【0024】

図3に、アドベリファイア300に含まれ得る例示的なコンポーネントを示す。アドベリフ

50

ファイア300は、セッション識別子302、本体指定子304、およびデジタル署名306、のうちの1つまたは複数を含んでよい。アドベリファイア300は、アドサーバ108によって生成されてよい。アドベリファイア300は、ISO/IEC14496-12に記載の国際標準化機構(ISO)ベースメディアファイルフォーマット(BMFF)または派生仕様(3GPP技術仕様書26.244に記載の3GPファイルフォーマットなど)を有するマルチメディアファイルなどの、ファイルに含まれてよい。ISO BMFFは、メディアファイルの構造を定義する。ISO BMFFを使用してフォーマットされたメディアファイルは、1つまたは複数の自由空間ボックスを含むことができる。自由空間ボックスは、メディア再生に関係のない情報を含むことができる。1つまたは複数のアドベリファイアが、自由空間ボックスに記憶されてよい。一実施形態では、広告コンテンツは、ISO BMFFによって定義されるようにフォーマットされたファイル中で送られてよく、ファイル中の1つまたは複数の自由空間ボックスには、1つまたは複数のアドベリファイアが記憶されてよい。

10

【0025】

アドベリファイア300は、広告ストリームの最初に、広告ストリームの最後に、および/または広告ストリーム内に挿入されてよい。アドベリファイア300は、アドコンテンツ内で、定期的にまたはランダムもしくは不規則な間隔で位置することができる。いくつかの実施形態では、広告ストリームに関連するアドベリファイアは、広告ストリームとは別個に送られてもよい。アドベリファイアは、ブラウザなど、プラットフォームベースの通信チャネルを介して送信されてよい。たとえば、アドベリファイアは、ブラウザクッキーを使用して、ストリーミングクライアント102に送られてメディアサーバ104によって取り出されてよい。別の例では、Adobe Flashメディアプレーヤプラットフォームにおいて定義されるローカリーストアドオブジェクト(locally stored object)(LSO)を使用して、アドベリファイアをアドサーバ108とストリーミングクライアント102とメディアサーバ104との間で通信することができる。アドベリファイア300をアドサーバ108からストリーミングクライアント102に送るために、他のファイルフォーマットおよび/または通信アプローチが使用されてもよいことは認識されるであろう。ストリーミングクライアント102は、ストリーミングクライアント102が広告コンテンツをアドサーバ108からダウンロードしたことをメディアサーバ104が検証できるように、アドベリファイア300に関連する情報をメディアサーバ104に送ることができる。アドベリファイア300に関連する情報は、本明細書では「検証情報」とも呼ばれる。

20

30

【0026】

セッション識別子302は、タイムスタンプ308、ノンス310、およびストリーミングクライアント識別子312、のうちの1つまたは複数を含んでよい。いくつかの実施形態では、メディアサーバ104は、ストリーミングクライアント102から受け取った、アドベリファイア300に関連する情報を妥当性検査するために、タイムスタンプ308を使用することができる。たとえば、メディアサーバ104は、アドベリファイアに関連する情報が、タイムスタンプ値からの事前定義済み時間ウィンドウ(120秒など)内に含まれるタイムスタンプを含むことを必要とする場合がある。他の時間ウィンドウ定義を使用して、秒、分、時間などにわたる時間期間が定義されてもよいことは認識されるであろう。ストリーミングクライアント102によってメディアサーバ104に提供されたタイムスタンプが時間ウィンドウ内に含まれない場合、メディアサーバ104は、ストリーミングクライアント102から受け取った検証情報が有効でないと判定することができ、ストリーミングクライアント102へのメディアコンテンツのストリーミングを停止することができる。たとえば、アドベリファイア300が「2012年8月1日13:30:05」のタイムスタンプ308を有し、有効時間ウィンドウが120秒である場合は、「2012年8月1日13:30:05」と「2012年8月1日13:32:05」との間にメディアサーバ104にサブミットされた検証情報は、メディアサーバ104によってうまく妥当性検査され得る。このようにして、ストリーミングクライアント102によって最近ダウンロードされたのではない広告コンテンツに対して生成された検証情報(たとえば、より早い時点で別のストリーミングクライアントによって生成された検証情報)をストリーミングクライアント102が使用するのを防止することができる。

40

50

【 0 0 2 7 】

いくつかの実施形態では、セッション識別子302は、ノンス310およびタイムスタンプ308を含んでよい。たとえば、ノンスに関連する2進表現またはテキストが、セッション識別子302に関連する2進表現またはテキストと連結されてよい。ノンス310は、乱数または疑似乱数とすることができる。ノンス310を使用してリプレイアタックを防止することができる。このようにして、各アドベリファイア300につき異なるノンス310がアドサーバ108によって生成されてよく、それにより、別のストリーミングクライアントによって生成されたかまたは別の時点で生成された検証情報をストリーミングクライアント102が使用するのを防止される。有効なノンスを含む検証情報は、メディアサーバ104によってうまく妥当性検査され得る。いくつかの実施形態では、ノンスは、タイムスタンプに対して相対的な有効時間ウィンドウ内で使用される場合にのみ、うまく妥当性検査され得る。

10

【 0 0 2 8 】

セッション識別子302中のタイムスタンプの代わりにまたはそれに加えて、シーケンス番号が使用されてもよい。シーケンス番号は、アドサーバ108によって生成されてよい。たとえば、アドサーバ108は、すべてのアドストリーム中で送られる各アドベリファイアについて、または特定のアドストリーム中で送られる各アドベリファイアについて、シーケンス番号を繰り返すことができる。このようにして、ストリーミングクライアント102によって受け取られる各アドベリファイアに順番が付けられてよく、したがって、異なるアドベリファイアからの検証情報をストリーミングクライアント102が再使用することが防止される。有効なシーケンス番号を含む検証情報は、メディアサーバ104によってうまく妥当性検査され得る。

20

【 0 0 2 9 】

セッション識別子302は、ストリーミングクライアント識別子312を含んでよい。ストリーミングクライアント識別子は、IPアドレス、IPアドレスとポート番号の組合せ、または他の識別情報など、ストリーミングクライアント102を識別するのに使用可能な任意の情報とすることができる。ストリーミングクライアント識別子312は、別のストリーミングクライアントによって生成された検証情報が、広告コンテンツがダウンロードされたことの妥当性検査のためにストリーミングクライアント102によって使用されるのを防止することができる。正しいストリーミングクライアント識別子を含む検証情報は、メディアサーバ104によってうまく妥当性検査され得る。

30

【 0 0 3 0 】

アドベリファイア300は、本体指定子304を含んでよい。いくつかの実施形態では、本体指定子304はバイト範囲314を含む。バイト範囲314は、広告コンテンツの、1つもしくは複数の部分、またはすべてを示すことができる。たとえば、100~200のバイト範囲は、広告コンテンツのバイト100~200に記憶されたデータを示すことができる。バイト範囲314が本体指定子304中で指定されているときは、ストリーミングクライアント102は、バイト範囲によって示されるデータのハッシュを実施して、メディアサーバ104に提供されることになる検証情報にハッシュを含めることが、要求されてよい。いくつかの実施形態では、本体指定子304はヌルとすることができる。本体指定子がヌルであるときは、ストリーミングクライアント102は、ハッシュを含まない検証情報をメディアサーバ104に提供することができる。

40

【 0 0 3 1 】

アドベリファイア300は、デジタル署名306を含んでよい。デジタル署名306は、アドサーバ108によって記憶された暗号鍵を使用してアドサーバ108によって生成されてよい。本体指定子304がヌルであるときは、デジタル署名306は、タイムスタンプ308、ノンス310、および/またはストリーミングクライアント識別子312など、セッション識別子302に関連する情報を使用して生成されてよい。デジタル署名306は、この情報のいくらかまたはすべてを暗号鍵で暗号化することによって作成されてよい。本体指定子304がバイト範囲314を示すときは、デジタル署名306は、アドサーバ108によって、セッション識別子302に関連する情報を使用して、かつ/または示されたバイト範囲に関連する広告コン

50

テンツデータのハッシュを使用して、生成されてよい。好ましい一実施形態では、共有秘密鍵を使用して、広告コンテンツデータのハッシュに基づいてデジタル署名が作成される。

【0032】

図4は、一実施形態による、アドコンテンツがストリーミングクライアントによってダウンロードされたことを検証するための例示的な流れ図である。動作402で、アドサーバ108とメディアサーバ104とが暗号鍵関係を確立する。たとえば、アドサーバ108は、共有秘密鍵を生成し、共有秘密鍵をメディアサーバ104に送ることができる。別法として、アドサーバ108は、公開-秘密鍵ペアを生成し、公開鍵をメディアサーバ104に送ることができる。

10

【0033】

動作404で、メディアサーバ104は、メディアコンテンツを求める要求をストリーミングクライアント102から受け取ることができる。動作406で、メディアサーバ104は、メディアコンテンツをストリーミングクライアント102にストリーミングすることができる。動作408で、メディアサーバ104は、広告コンテンツをアドサーバ108に要求するよう、ストリーミングクライアント102にシグナリングすることができる。いくつかの実施形態では、ストリーミングクライアント102は、メディアコンテンツを要求してメディアサーバ104から受け取る前に、広告コンテンツをアドサーバ108に要求してアドサーバ108から受け取ることができる(すなわち、動作404~406は、任意選択の動作とすることができる)。

【0034】

20

ストリーミングクライアント102は、広告コンテンツをアドサーバ108から受け取ることができる。広告コンテンツとともに、1つまたは複数のアドベリファイア300が送られてよい。アドベリファイア300は、デジタル署名306を含んでよい。ストリーミングクライアント102は、1つまたは複数のアドベリファイア300に基づいて検証情報を生成することができる。動作410に示されるように、メディアサーバ104は、検証情報をストリーミングクライアント102から受け取ることができる。

【0035】

動作412に示されるように、メディアサーバ104は、ストリーミングクライアント102から受け取った検証情報を使用して、ストリーミングクライアント102への広告コンテンツのストリーミングを妥当性検査する(すなわち、広告コンテンツがストリーミングクライアント102によってダウンロードされたかどうか判定する)ことができる。たとえば、検証情報がデジタル署名306を含むときは、メディアサーバは、動作402でアドサーバ108から受け取った鍵を使用して、デジタル署名を検証することができる。検証情報がセッション識別子情報302を含むときは、メディアサーバ104は、セッション識別子情報をチェックすることができる。判定414で、ストリーミングクライアント102から受け取られた検証情報が、ストリーミングクライアント102が広告コンテンツをアドサーバ108からダウンロードしたことを示すかどうか、メディアサーバ104によって判定される。広告コンテンツのダウンロードが妥当性検査された場合は、動作416に示されるように、メディアサーバ104は、ストリーミングクライアント102へのメディアのストリーミングを継続することができる(またはメディアのストリーミングを開始することができる)。広告コンテンツのダウンロードが妥当性検査されない場合は、動作418に示されるように、メディアサーバ104は、ストリーミングクライアント102へのメディアのストリーミングを中断することができる。いくつかの実施形態では、ステップ408~418は、メディアストリームの送達中に1回または複数回繰り返されてよい。

30

40

【0036】

通常、ストリーミングクライアント102が、広告コンテンツを要求するようメディアサーバ104によってシグナリングされて、その後でアドベリファイアに関連する情報を提供することができなかった場合、メディアサーバ104は、ストリーミングクライアント102へのメディアコンテンツのストリーミングを中断することになる。

【0037】

50

複数のアドベリファイアがアドサーバ108からストリーミングクライアント102に送達されたときは、メディアサーバ104は、アドベリファイアのすべて(または、いくつかの実施形態ではサブセット)が妥当性検査されるまで、ストリーミングクライアント102へのメディアコンテンツのストリーミングを防止することができる。

【0038】

図5は、アドベリファイア300中でバイト範囲314が指定されているときに、アドコンテンツがストリーミングクライアント102によってダウンロードされたことを検証するための例示的な流れ図である。動作502で、アドサーバ108とメディアサーバ104とが暗号鍵関係を確立する。たとえば、アドサーバ108は、共有秘密鍵を生成し、共有秘密鍵をメディアサーバ104に送ることができる。別法として、アドサーバ108は、公開-秘密鍵ペアを生成し、公開鍵をメディアサーバ104に送ることができる。一実施形態では、アドサーバ108は、セキュアプロトコルを使用して共有秘密鍵を送ることができ、たとえば、鍵を認証するのに使用できる証明書とともに鍵を送ることができる。

【0039】

動作504で、ストリーミングクライアント102は、メディアコンテンツをメディアサーバ104に要求することができる。動作506で、ストリーミングクライアント102は、メディアコンテンツをメディアサーバ104から受け取ることができる。動作508で、ストリーミングクライアント102は、広告コンテンツをアドサーバ108に要求することができる。たとえば、206に示されたように、ストリーミングクライアント102は、アドに関するシグナルをメディアサーバ104から受け取ることができる。いくつかの実施形態では、ストリーミングクライアント102は、メディアコンテンツをメディアサーバ104に要求してメディアサーバ104から受け取る前に、広告コンテンツをアドサーバ108に要求してアドサーバ108から受け取ることができる(すなわち、動作504~506は、任意選択の動作とすることができる)。

【0040】

動作510で、ストリーミングクライアント102は、広告コンテンツをアドサーバ108から受け取ることができる。広告コンテンツとともに、1つまたは複数のアドベリファイア300が送られてよい。アドベリファイア300は、デジタル署名306および指定されたバイト範囲314を含んでよい。動作512に示されるように、ストリーミングクライアント102は、指定されたバイト範囲314に基づいてハッシュを生成することができる。動作514で、ストリーミングクライアント102は、ハッシュとデジタル署名306とを含む検証情報を、メディアサーバ104に送ることができる。

【0041】

動作516に示されるように、メディアサーバ104は、動作502でアドサーバ108から受け取った鍵をハッシュに適用して、得られた値をデジタル署名306と比較することができる。判定518で、メディアサーバ104は、動作516の比較の結果が合致するかどうか判定することによって、ストリーミングクライアント102への広告コンテンツのストリーミングを妥当性検査する。メディアサーバ鍵をハッシュに適用する結果として得られた値がデジタル署名306と合致する場合は、動作520に示されるように、メディアサーバ104は、ストリーミングクライアント102へのメディアのストリーミングを継続することができる(またはメディアのストリーミングを開始することができる)。得られた値がデジタル署名306と合致しない場合は、動作522に示されるように、メディアサーバ104は、ストリーミングクライアント102へのメディアのストリーミングを中断することができる。いくつかの実施形態では、ステップ508~522は、メディアストリームの送達中に1回または複数回繰り返されてよい。

【0042】

図6は、ブラウザベースのメディアプレーヤ114によって広告コンテンツがストリーミングクライアント102にダウンロードされたことを検証するための例示的な流れ図である。動作602で、アドサーバ108とメディアサーバ104とが暗号鍵関係を確立する。たとえば、アドサーバ108は、共有秘密鍵を生成し、共有秘密鍵をメディアサーバ104に送ることができる。別法として、アドサーバ108は、公開-秘密鍵ペアを生成し、公開鍵をメディアサー

バ104に送ることができる。一実施形態では、アドサーバ108は、セキュアプロトコルを使用して共有秘密鍵を送ることができ、たとえば、鍵を認証するのに使用できる証明書とともに鍵を送ることができる。

【0043】

動作604で、ストリーミングクライアント102は、メディアコンテンツをメディアサーバ104に要求することができる。動作606で、ストリーミングクライアント102は、メディアコンテンツをメディアサーバ104から受け取ることができる。動作608で、ストリーミングクライアント102は、広告コンテンツをアドサーバ108に要求することができる。たとえば、206に示されたように、ストリーミングクライアント102は、アドに関するシグナルをメディアサーバ104から受け取ることができる。いくつかの実施形態では、ストリーミングクライアント102は、メディアコンテンツをメディアサーバ104に要求してメディアサーバ104から受け取る前に、アドコンテンツをアドサーバ108に要求してアドサーバ108から受け取ることができる(すなわち、動作604~606は、任意選択の動作とすることができる)。

10

【0044】

動作610で、ストリーミングクライアント102は、アドコンテンツをアドサーバ108から受け取ることができる。1つまたは複数のアドベリファイア300が、ブラウザクッキーまたはアノニマスコード中で、ストリーミングクライアント102に送られてよい。ブラウザクッキーまたはアノニマスコードは、デジタル署名を含んでよい。612に示されるように、メディアサーバ104は、1つまたは複数のアドベリファイア300をブラウザクッキーまたはアノニマスコードから取り出すことができる。たとえば、ストリーミングクライアント102は、ブラウザクッキーもしくはアノニマスコードをメディアサーバ104に送ることができる、または、メディアサーバ104は、他の方法でブラウザクッキーまたはアノニマスコードをストリーミングクライアント102から得ることができる。メディアサーバ104は、ブラウザクッキーまたはアノニマスコードを解析して、アドベリファイア300を得ることができる。

20

【0045】

動作616に示されるように、メディアサーバ104は、動作602でアドサーバ108から受け取った鍵を使用して、ブラウザクッキーまたはアノニマスコード中のアドベリファイアから得られたデジタル署名を検証することができる。判定618で、メディアサーバ104は、デジタル署名を検証できるかどうか判定することによって、ストリーミングクライアント102への広告コンテンツのストリーミングを妥当性検査する。デジタル署名が検証される場合は、動作620に示されるように、メディアサーバ104は、ストリーミングクライアント102へのメディアのストリーミングを継続することができる(またはメディアのストリーミングを開始することができる)。デジタル署名が検証されない場合は、動作622に示されるように、メディアサーバ104は、ストリーミングクライアント102へのメディアのストリーミングを中断することができる。

30

【0046】

いくつかの実施形態では、ストリーミングクライアント102上でのメディア再生は、Adobe Flashメディアプレーヤプラットフォームなどのメディア再生アプリケーションを使用して実施されることがある。Adobe Flashメディアプレーヤは、ブラウザ116中で、または、メディア再生アプリケーション112などのスタンドアロンアプリケーションとして、稼働することができる。Adobe Flashは、ローカル共有オブジェクト(local shared object)(LSO)を使用して、ウェブサイトに関連するかまたはAdobe Flashアプリケーションに関連するデータを記憶する。たとえば、LSOが、ストリーミングクライアント102の記憶媒体に記憶されて、メディアサーバ104によって得られてよい。アドベリファイアは、図5に関して説明されたフローに従って、ブラウザクッキーの代わりにLSOを使用して、クライアントに送られてクライアントから取り出されてよい。このようにして、クッキーをブロックするようにユーザがブラウザ116を構成した場合でもやはり、LSOを使用してアドベリファイアを送達することができる。

40

【0047】

50

図7は、前述のエンティティまたはコンポーネント(たとえば、ストリーミングクライアント102、メディアサーバ104、および広告サーバ108)のいずれかを実装するのに使用できるコンピュータシステムの例示的なブロック図である。コンピュータシステムは、様々な実施形態により、ハードウェアおよびソフトウェアコンポーネントの組合せとして実装される場合がある。コンピュータシステムは、本明細書で論じられる方法のいずれか1つまたは複数をシステムに実施させるために実行され得る1組の命令を含んでよい。コンピュータシステムは、コンピュータの形の特定のマシンとして実現されてよい。システムは、このシステムによって行われることになるアクションを指定する1組の命令(逐次的もしくは他の方法の)を実行できる、サーバコンピュータ、パーソナルコンピュータ(PC)、または任意のシステムとすることができる。さらに、単一のシステムのみが示されているが、

「システム」という用語はまた、本明細書で論じられる方法の1つまたは複数を実施するための1組の(または複数組の)命令を個別にまたは合同で実行するシステムの任意の集合も含むものとして理解されるべきである。

10

20

30

40

50

【0048】

コンピュータシステムは、プロセッサ702(たとえば中央処理装置(CPU))と、実行中のプログラムコードを記憶できるメモリ704と、不揮発性記憶装置706とを備えてよく、これらはすべて、バス700を介して相互と通信する。システムはさらに、ビデオ表示ユニット708(たとえば、液晶表示装置(LCD)または陰極線管(CRT))を備えてよい。システムはまた、英数字入力デバイス710(たとえばキーボード)と、コンテンツソースを受け取るためおよびコンテンツストアを送達するためのネットワークインターフェースデバイス712とを備えてよい。

【0049】

不揮発性記憶ユニット706は、本明細書に記載の方法または機能のいずれか1つまたは複数を組み入れた1組または複数組の命令(たとえばソフトウェア)が記憶され得る機械可読媒体を含んでよい。命令はまた、システムによって命令が実行される間、完全にまたは少なくとも部分的に、メモリ704内および/またはプロセッサ702内にあってよく、メモリ704およびインジェスチョンプロセッサ702もまた機械可読媒体を構成する。

【0050】

本開示の読後には、さらに他の実施形態が当業者によって思い描かれることが可能である。他の実施形態では、有利なことに、上に開示された本発明の組合せまたはサブコンビネーションを作ることができる。コンポーネントの例示的構成は、説明の目的で示されるものであり、本発明の代替実施形態では、組合せ、追加、再構成などが企図されることを理解されたい。よって、本発明は例示的な実施形態に関して説明されたが、多くの修正が可能であることを当業者なら認識するであろう。

【0051】

たとえば、本明細書に記載のプロセスは、ハードウェアコンポーネント、ソフトウェアコンポーネント、および/またはこれらの任意の組合せを使用して実装されてよい。いくつかの場合では、ソフトウェアコンポーネントは、有形の非一時的な媒体が備わったハードウェア上で実行されるように、またはこの媒体とは別個のハードウェア上で実行されるように、有形の非一時的な媒体上で提供されてもよい。したがって、明細書および図面は、限定的ではなく例示的な意味で考えられるべきである。しかし、特許請求の範囲に示される本発明のより広範な主旨および範囲を逸脱することなく様々な修正および変更が明細書および図面に加えられてもよいこと、ならびに、本発明が後続の特許請求の範囲内のすべての修正および均等物をカバーするものとするのは、明白であろう。

【符号の説明】

【0052】

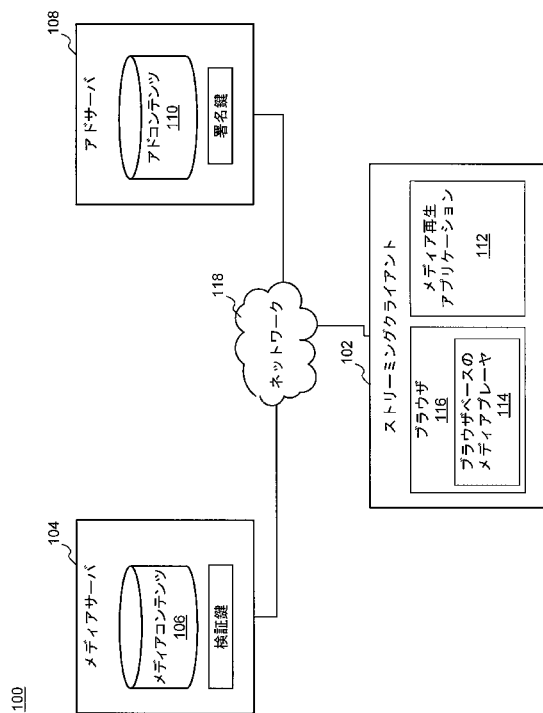
- 100 システム
- 102 ストリーミングクライアント
- 104 メディアサーバ
- 106 メディアコンテンツデータベース

- 108 アドサーバ
- 110 アドコンテンツデータベース
- 112 メディア再生アプリケーション
- 114 ブラウザベースのメディアプレーヤ
- 116 インターネットブラウザ
- 118 ネットワーク
- 300 アドベリファイア
- 302 セッション識別子
- 304 本体指定子
- 306 デジタル署名
- 308 タイムスタンプ
- 310 ノンス
- 312 ストリーミングクライアント識別子
- 314 バイト範囲
- 700 バス
- 702 プロセッサ
- 704 メモリ
- 706 不揮発性記憶装置
- 708 ビデオ表示ユニット
- 710 英数字入力デバイス
- 712 ネットワークインターフェース

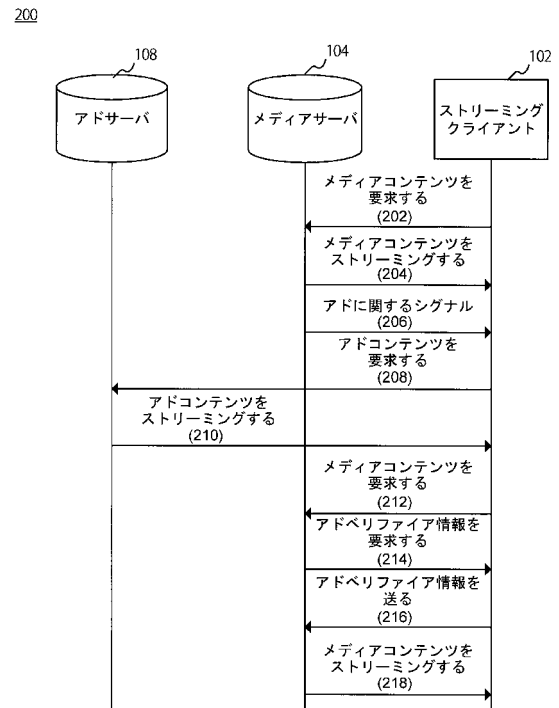
10

20

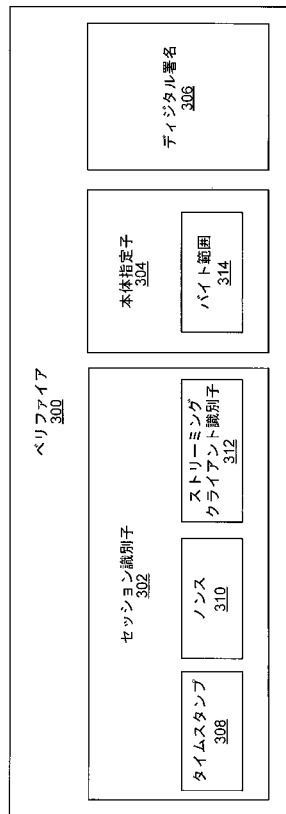
【図 1】



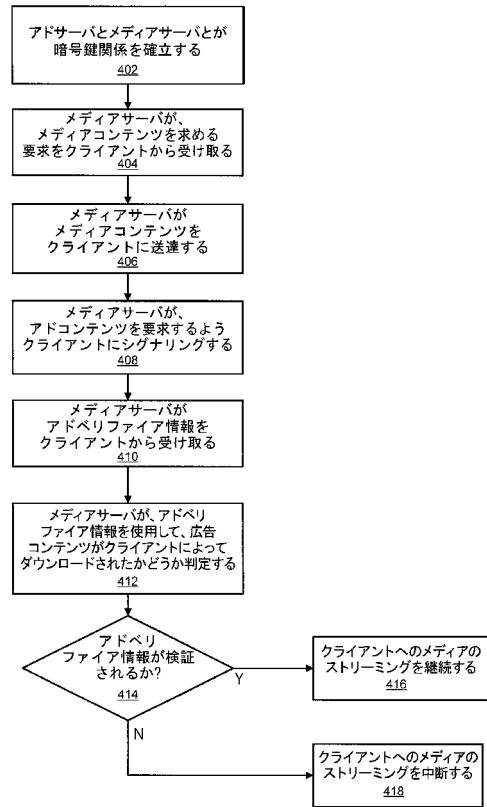
【図 2】



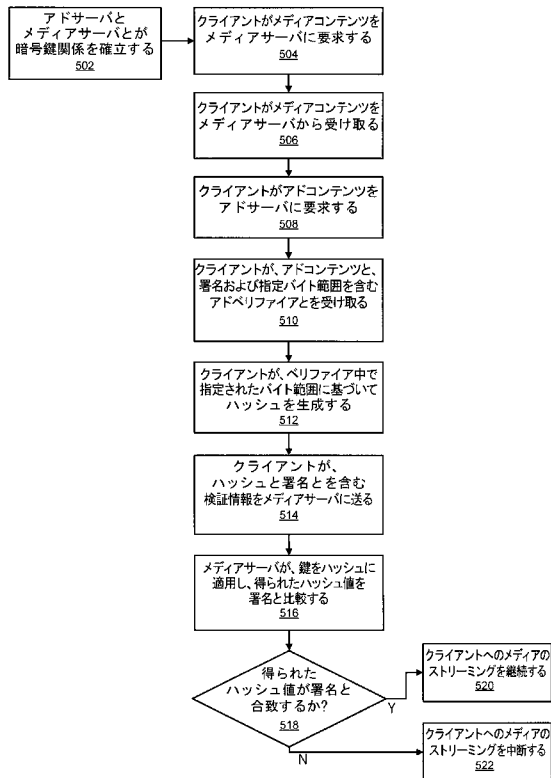
【図 3】



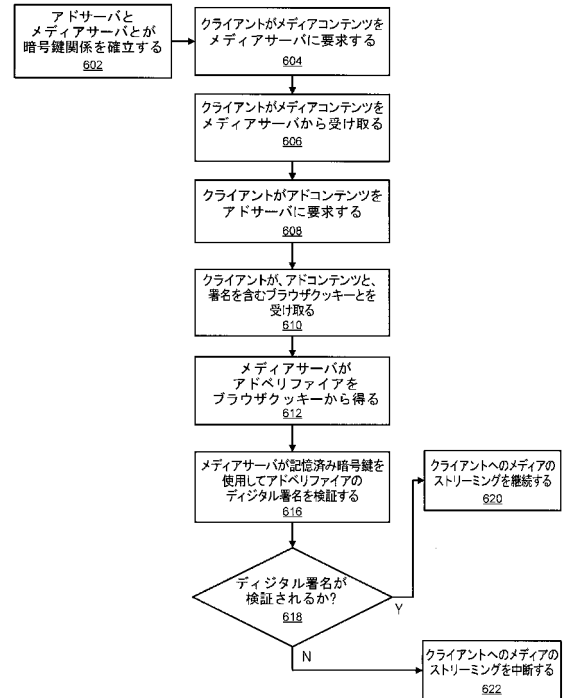
【図 4】



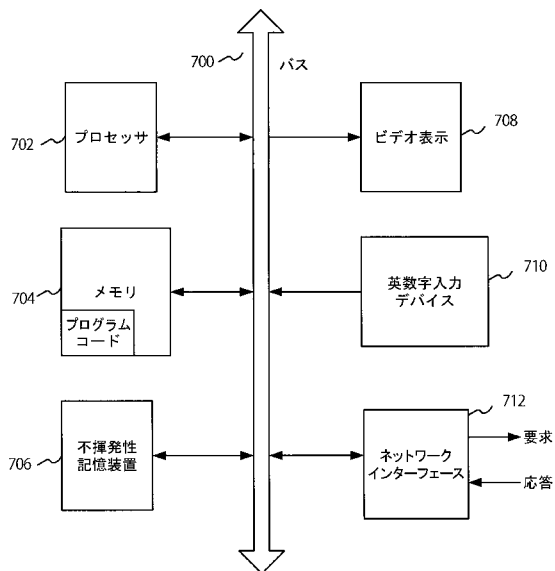
【図 5】



【図 6】



【図 7】



【手続補正書】

【提出日】平成27年1月5日(2015.1.5)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

ストリーミングクライアントによって広告コンテンツを広告サーバに要求するステップと、

前記広告コンテンツを前記広告サーバから受け取るのに応答して1つまたは複数のベリファイアを前記広告サーバから受け取るステップと、

前記ベリファイアに関連する情報をメディアサーバに送るステップであって、前記メディアサーバが、前記ベリファイアに関連する前記情報に基づいて前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査するように構成されたステップとを含むプロセッサ実装方法。

【請求項 2】

ベリファイアが、共有秘密暗号鍵に基づくデジタル署名を含み、前記共有秘密暗号鍵が前記広告サーバおよび前記メディアサーバによって記憶され、

前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査することが、前記共有秘密暗号鍵にさらに基づく、請求項1に記載の方法。

【請求項 3】

ベリファイアが、公開-秘密暗号鍵ペアに基づくデジタル署名を含み、

前記公開-秘密暗号鍵ペアの秘密暗号鍵が前記広告サーバによって記憶され、

前記公開-秘密暗号鍵ペアの公開暗号鍵が前記メディアサーバによって記憶され、
前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査することが、前記公開暗号鍵にさらに基づく、請求項1に記載の方法。

【請求項4】

前記ペリファイアが、セッション識別子、本体指定子、およびデジタル署名、のうちの少なくとも1つを含む、請求項1に記載の方法。

【請求項5】

セッション識別子が、タイムスタンプ、ノンス、およびクライアント識別子、のうちの少なくとも1つを含む、請求項4に記載の方法。

【請求項6】

本体指定子がバイト範囲を含み、前記ストリーミングクライアントが、前記バイト範囲に対応するデータのハッシュを生成する、請求項4に記載の方法。

【請求項7】

ペリファイアが、ISOベースメディアファイルフォーマットに従ってフォーマットされたメディアファイルの自由空間ボックスに含まれる、請求項1に記載の方法。

【請求項8】

前記ペリファイアが広告ストリーム内のランダムな場所に位置する、請求項1に記載の方法。

【請求項9】

ペリファイアがブラウザクッキー中で前記広告サーバから受け取られる、請求項1に記載の方法。

【請求項10】

ペリファイアがローカリーストアドオブジェクト中で前記広告サーバから受け取られる、請求項1に記載の方法。

【請求項11】

ストリーミングクライアントのプロセッサによって実行可能なプログラムコードを記憶するためのコンピュータ可読記憶媒体であって、前記プログラムコードが、

広告コンテンツを広告サーバに要求するためのプログラムコードと、

前記広告コンテンツを前記広告サーバから受け取るのに応答して1つまたは複数のペリファイアを前記広告サーバから受け取るためのプログラムコードと、

前記ペリファイアに関連する情報をメディアサーバに送るためのプログラムコードとを含み、前記メディアサーバが、前記ペリファイアに関連する前記情報に基づいて前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査するように構成された、コンピュータ可読記憶媒体。

【請求項12】

前記ペリファイアが、セッション識別子、本体指定子、およびデジタル署名、のうちの少なくとも1つを含む、請求項11に記載のコンピュータ可読記憶媒体。

【請求項13】

セッション識別子が、タイムスタンプ、ノンス、およびクライアント識別子、のうちの少なくとも1つを含む、請求項12に記載のコンピュータ可読記憶媒体。

【請求項14】

本体指定子がバイト範囲を含み、前記バイト範囲に対応するデータのハッシュを生成するためのプログラムコードをさらに含む、請求項12に記載のコンピュータ可読記憶媒体。

【請求項15】

メモリと、

前記メモリに結合されたプロセッサとを備えるクライアントデバイスであって、前記プロセッサが、

広告コンテンツを広告サーバに要求するステップと、

前記広告コンテンツを前記広告サーバから受け取るのに応答して1つまたは複数のペリファイアを前記広告サーバから受け取るステップと、

前記ベリファイアに関連する情報をメディアサーバに送るステップであって、前記メディアサーバが、前記ベリファイアに関連する前記情報に基づいて前記クライアントデバイスへの前記広告コンテンツのストリーミングを妥当性検査するように構成されたステップとを含む方法を実施するためのプロセッサ実行可能命令で構成された、クライアントデバイス。

【請求項 16】

前記ベリファイアが、セッション識別子、本体指定子、およびデジタル署名、のうちの少なくとも1つを含む、請求項15に記載のクライアントデバイス。

【請求項 17】

セッション識別子が、タイムスタンプ、ノンス、およびクライアント識別子、のうちの少なくとも1つを含む、請求項16に記載のクライアントデバイス。

【請求項 18】

本体指定子がバイト範囲を含み、前記バイト範囲に対応するデータのハッシュを生成するためのプログラムコードをさらに含む、請求項16に記載のクライアントデバイス。

【請求項 19】

メディアサーバによってストリーミングメディアをストリーミングクライアントに送るステップと、

前記ストリーミングクライアントによって広告コンテンツを広告サーバから受け取るの
に応答して、1つまたは複数のベリファイアに関連する情報を前記ストリーミングクライアントから受け取るステップであって、前記ベリファイアが前記広告コンテンツに関連するものであるステップと、

前記ベリファイアに関連する前記情報に基づいて前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査するステップであって、前記妥当性検査が不成功である場合に、前記ストリーミングメディアを送る前記ステップが停止されるステップとを含むプロセッサ実装方法。

【請求項 20】

ベリファイアが、共有秘密暗号鍵に基づくデジタル署名を含み、前記共有秘密暗号鍵が、前記メディアサーバと、前記広告コンテンツを提供する広告サーバとによって記憶され、

前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査するステップが、前記共有秘密暗号鍵にさらに基づく、請求項19に記載の方法。

【請求項 21】

ベリファイアが、公開-秘密暗号鍵ペアの秘密暗号鍵を使用して生成されたデジタル署名を含み、

前記公開-秘密暗号鍵ペアの前記秘密暗号鍵が、前記広告コンテンツを提供する広告サーバによって記憶され、

前記公開-秘密暗号鍵ペアの公開暗号鍵が前記メディアサーバによって記憶され、

前記ストリーミングクライアントへの前記広告コンテンツのストリーミングを妥当性検査するステップが、前記公開暗号鍵にさらに基づく、請求項19に記載の方法。

【請求項 22】

前記ベリファイアに関連する前記情報が、署名と、前記広告コンテンツに対応するデータの少なくとも一部のハッシュとを含み、前記広告コンテンツのストリーミングを妥当性検査するステップが、公開暗号鍵を前記ハッシュに適用して結果値を得て、前記結果値を前記署名と比較するステップを含む、請求項19に記載の方法。

【請求項 23】

前記広告コンテンツのストリーミングを妥当性検査するステップが、ブラウザクッキー内に含まれるデジタル署名を妥当性検査するステップを含む、請求項19に記載の方法。

【請求項 24】

前記広告コンテンツのストリーミングを妥当性検査するステップが、ローカリーストアドオブジェクト内に含まれるデジタル署名を妥当性検査するステップを含む、請求項19

に記載の方法。

【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/US14/17749
A. CLASSIFICATION OF SUBJECT MATTER IPC: H04N 7/10(2006.01) USPC: 725/32 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) U.S. : 725/32		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7,353,383 B2 (SKINGLE) 01 April 2008 (01.04.2008), see entire document.	1-5, 10-13, 15-17, 19-21, 24
A	US 7,187,771 B1 (DICKINSON et al.) 06 March 2007 (06.03.2007), see entire document.	1-24
Y, P	US 8,769,270 B2 (ORSINI et al.) 01 July 2014 (01.07.2014), see entire document.	6-9, 14, 18, 22, 23
Y, A	US 2007/0100768 A1 (BOCCON-GIBOD et al.) 03 May 2007(03.05.2007), see entire document.	7, 22
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 28 September 2014 (28.09.2014)		Date of mailing of the international search report 03 OCT 2014
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201		Authorized officer William Krynski Telephone No. 571-272-1700

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US

(72)発明者 ケヴィン・アール・フォール

アメリカ合衆国・カリフォルニア・9 2 1 2 1 - 1 7 1 4・サン・ディエゴ・モアハウス・ドライブ・5 7 7 5

(72)発明者 ファティ・ウルピナル

アメリカ合衆国・カリフォルニア・9 2 1 2 1 - 1 7 1 4・サン・ディエゴ・モアハウス・ドライブ・5 7 7 5

F ターム(参考) 5B084 AA01 AA02 AA12 AB07 AB13 AB31 AB34 AB35 BA02 BB15

CB04 CB22 CD09 DB02 DC02 DC13

5L049 BB08