

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5946212号
(P5946212)

(45) 発行日 平成28年7月5日(2016.7.5)

(24) 登録日 平成28年6月10日(2016.6.10)

(51) Int. Cl. F 1
G 0 6 Q 3 0 / 0 6 (2012.01) G 0 6 Q 3 0 / 0 6 3 0 0

請求項の数 7 (全 15 頁)

(21) 出願番号	特願2012-157753 (P2012-157753)	(73) 特許権者	000005049 シャープ株式会社
(22) 出願日	平成24年7月13日(2012.7.13)		大阪府大阪市阿倍野区長池町2番2号
(65) 公開番号	特開2014-21610 (P2014-21610A)	(74) 代理人	100114258 弁理士 福地 武雄
(43) 公開日	平成26年2月3日(2014.2.3)	(74) 代理人	100125391 弁理士 白川 洋一
審査請求日	平成27年7月1日(2015.7.1)	(72) 発明者	平川 功 大阪府大阪市阿倍野区長池町2番2号 シャープ株式会社内
		審査官	大野 朋也

最終頁に続く

(54) 【発明の名称】 ローカルサーバ装置、端末装置、コンテンツストア装置、プログラム、コンテンツ配信方法およびコンテンツ配信システム

(57) 【特許請求の範囲】

【請求項1】

端末装置が公衆ネットワークに接続できない限定エリアに存在する場合に前記端末装置にコンテンツを配信するローカルサーバ装置であって、

前記公衆ネットワーク上に存在するコンテンツストア装置から前記限定エリア内でのみ配信する仮コンテンツを取得する限定エリア用通信部と、

前記取得した仮コンテンツを保存する仮コンテンツ保存部と、

前記仮コンテンツに前記限定エリアの識別情報を加えて、仮購入用コンテンツを生成する仮購入用コンテンツ生成部と、

前記限定エリア内でのみ有効な第1の認証情報に基づいて、前記端末装置の認証を行なう端末認証部と、を備え、

前記認証済みの端末装置から要求があったときは前記認証済みの端末装置に対して前記仮購入用コンテンツを配信することを特徴とするローカルサーバ装置。

【請求項2】

公衆ネットワークに接続できない限定エリアに存在する場合に、ローカルサーバ装置からコンテンツを取得する端末装置であって、

通信インタフェースとして機能する通信部と、

前記ローカルサーバ装置との認証が済んだ後、前記ローカルサーバ装置から取得した仮購入用コンテンツを保存する保存部と、

前記取得した仮購入用コンテンツからコンテンツデータを抽出するDRM(Digital Ri

ghts Management) 制御部と、

前記取得した仮購入用コンテンツから抽出した付加情報およびユーザの正規の認証情報である第2の認証情報から、前記仮購入用コンテンツと前記第2の認証情報とに紐づく付与情報を生成する情報抽出部と、を備え、

前記公衆ネットワークに接続できる状態になったときに、前記第2の認証情報を用いて前記公衆ネットワーク上に存在するコンテンツストア装置との認証を行ない、認証が済んだ後で、前記コンテンツストア装置へ前記付与情報を送信し、前記コンテンツストア装置から正式コンテンツを取得することを特徴とする端末装置。

【請求項3】

端末装置またはローカルサーバ装置が公衆ネットワークに接続できる通信エリアに存在する場合に前記端末装置または前記ローカルサーバ装置にコンテンツを配信する、コンテンツストア装置であって、

前記ローカルサーバ装置に固有のローカルサーバ装置識別情報および仮コンテンツ毎に付与する仮コンテンツ付与用識別情報から、仮コンテンツ付与情報を生成する仮コンテンツ付与情報生成部と、

前記仮コンテンツ付与情報および正式コンテンツから、前記ローカルサーバ装置に配信する仮コンテンツを生成する仮コンテンツ生成部と、を備え、

前記公衆ネットワークを介して前記ローカルサーバ装置との認証が済んだ後で、前記ローカルサーバ装置に対して、前記仮コンテンツを配信することを特徴とするコンテンツストア装置。

【請求項4】

端末装置が公衆ネットワークに接続しているときに、前記端末装置から仮購入用コンテンツと前記第2の認証情報とに紐づく付与情報を取得し、前記付与情報から、前記仮購入用コンテンツに関する情報およびユーザの正規の認証情報である第2の認証情報によって認証ができた場合は、前記端末装置に対して、正式コンテンツの配信を行なうことを特徴とする請求項3記載のコンテンツストア装置。

【請求項5】

端末装置が公衆ネットワークに接続できない限定エリアに存在する場合に前記端末装置にコンテンツを配信するローカルサーバ装置のプログラムであって、

前記公衆ネットワーク上に存在するコンテンツストア装置から前記限定エリア内でのみ配信する仮コンテンツを取得する処理と、

前記取得した仮コンテンツを保存する処理と、

前記仮コンテンツに前記限定エリアの識別情報を加えて、仮購入用コンテンツを生成する処理と、

前記限定エリア内でのみ有効な第1の認証情報に基づいて、前記端末装置の認証を行なう処理と、

前記認証済みの端末装置から要求があったときは前記認証済みの端末装置に対して前記仮購入用コンテンツを配信する処理と、の一連の処理をコンピュータに実行させることを特徴とするプログラム。

【請求項6】

端末装置が公衆ネットワークに接続できない限定エリアに存在する場合に前記端末装置にコンテンツを配信するコンテンツ配信方法であって、

前記公衆ネットワーク上に存在するコンテンツストア装置から前記限定エリア内でのみ配信する仮コンテンツを取得するステップと、

前記取得した仮コンテンツを保存するステップと、

前記仮コンテンツに前記限定エリアの識別情報を加えて、仮購入用コンテンツを生成するステップと、

前記限定エリア内でのみ有効な第1の認証情報に基づいて、前記端末装置の認証を行なうステップと、

前記認証済みの端末装置から要求があったときは前記認証済みの端末装置に対して前記

10

20

30

40

50

仮購入用コンテンツを配信するステップと、を少なくとも含むことを特徴とするコンテンツ配信方法。

【請求項 7】

請求項 1 記載のローカルサーバ装置と、請求項 2 記載の端末装置と、請求項 3 記載のコンテンツストア装置と、から構成されるコンテンツ配信システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、端末装置が公衆ネットワークに接続できない限定エリアに存在する場合に端末装置にコンテンツを配信する技術に関する。

10

【背景技術】

【0002】

従来から、コンテンツを配信するシステムが知られている。例えば、特許文献 1 には、試聴コンテンツをダウンロードするかどうかとは関係なく、いつでも試聴コンテンツを試聴することができる技術が開示されている。この技術では、サーバは、端末のユーザ ID と、配信した試聴プレーヤの情報とを記憶しておき、端末からアクセスがあり、試聴要求があった場合に、その試聴プレーヤ情報と端末情報とを確認して更新し、試聴コンテンツを配信する。ユーザから正式コンテンツの配信要求があった場合、端末情報と試聴コンテンツの配信情報を確認した上で、試聴コンテンツに紐づけられた正式コンテンツを配信する。

20

【先行技術文献】

【特許文献】

【0003】

【特許文献 1】特開 2006 - 79179 号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

例えば、地下鉄車内や航空機内など、端末が公衆ネットワークとの接続ができずに、即時にセンターのサーバとアクセスできない場合、センターはコンテンツの配信やユーザ ID 等の確認（認証）をリアルタイムで行なうことができない。この場合、このような限定されたエリア（限定エリア）において、あらかじめローカルサーバを設け、ローカルサーバへコンテンツを配信し、ローカルサーバが代わりに認証して、試聴コンテンツの配信を行ない、ユーザがセンターと接続できる状態になった場合に、正式のコンテンツの配信要求をセンターに送出して、正式コンテンツの配信する方法が考えられる。

30

【0005】

しかし、センターの側からすると、正式コンテンツをユーザではなく、一旦ローカルサーバへ配信するのは、コンテンツの保護の観点から望ましくない。また、ユーザの側からすると、ローカルサーバが正規のものであるかどうかを確認することができず、ユーザが正規の認証情報をローカルサーバへ送信するのは危惧がある。ユーザが、センターと接続できるようになった際に、改めてコンテンツの配信要求を行なうことは煩雑である。このような場合、自動的に接続できるようにしておく方法も考えられるが、それまでに端末内にユーザが正規の認証情報を保持し続けることは、昨今の端末のオープン化の中で、悪意の下で作製されたアプリケーションにより認証情報を奪取される危惧がある。

40

【0006】

本発明は、このような事情に鑑みてなされたものであり、端末装置が公衆ネットワークへの接続ができない限定エリアに存在する場合であっても、コンテンツを利用することができ、かつ限定エリア外に出た場合に安全に正式コンテンツを購入することを可能とするローカルサーバ装置、端末装置、コンテンツストア装置、プログラム、コンテンツ配信方法およびコンテンツ配信システムを提供することを目的とする。

50

【課題を解決するための手段】

【0007】

(1) 上記の目的を達成するために、本発明は、以下のような手段を講じた。すなわち、本発明のローカルサーバ装置は、端末装置が公衆ネットワークに接続できない限定エリアに存在する場合に前記端末装置にコンテンツを配信するローカルサーバ装置であって、前記公衆ネットワーク上に存在するコンテンツストア装置から前記限定エリア内でのみ配信する仮コンテンツを取得する限定エリア用通信部と、前記取得した仮コンテンツを保存する仮コンテンツ保存部と、前記仮コンテンツに前記限定エリアの識別情報を加えて、仮購入用コンテンツを生成する仮購入用コンテンツ生成部と、前記限定エリア内でのみ有効な第1の認証情報に基づいて、前記端末装置の認証を行なう端末認証部と、を備え、前記認証済みの端末装置から要求があったときは前記認証済みの端末装置に対して前記仮購入用コンテンツを配信することを特徴とする。

10

【0008】

この構成により、コンテンツの配信や認証を行うセンターが公衆ネットワーク等を通じて外部に存在するコンテンツ配信システムにおいて、公衆ネットワークへの接続ができなくなる状態が生じる限定エリアにおいても、限定エリア内でコンテンツを利用することができる。また、限定エリア外においても安全に正式コンテンツを購入することができる。ユーザが限定エリア内で購入した仮購入用コンテンツについては、ユーザが公衆ネットワークに接続できる状態になった場合に、自動的にコンテンツストア装置にアクセスすることでユーザが再度購入手続きを行なわなくても、正式コンテンツを購入することが可能となる。

20

【0009】

(2) また、本発明の端末装置は、公衆ネットワークに接続できない限定エリアに存在する場合に、ローカルサーバ装置からコンテンツを取得する端末装置であって、通信インタフェースとして機能する通信部と、前記ローカルサーバ装置との認証が済んだ後、前記ローカルサーバ装置から取得した仮購入用コンテンツを保存する保存部と、前記取得した仮購入用コンテンツからコンテンツデータを抽出するDRM(Digital Rights Management)制御部と、前記取得した仮購入用コンテンツから抽出した付加情報およびユーザの正規の認証情報である第2の認証情報から、前記仮購入用コンテンツと前記第2の認証情報とに紐づく付与情報を生成する情報抽出部と、を備え、前記公衆ネットワークに接続できる状態になったときに、前記第2の認証情報を用いて前記公衆ネットワーク上に存在するコンテンツストア装置との認証を行ない、認証が済んだ後で、前記コンテンツストア装置へ前記付与情報を送信し、前記コンテンツストア装置から正式コンテンツを取得することを特徴とする。

30

【0010】

この構成により、コンテンツの配信や認証を行うセンターが公衆ネットワーク等を通じて外部に存在するコンテンツ配信システムにおいて、公衆ネットワークへの接続ができなくなる状態が生じる限定エリアにおいても、限定エリア内でコンテンツを利用することができる。また、限定エリア外においても安全に正式コンテンツを購入することができる。ユーザが限定エリア内で購入した仮購入用コンテンツについては、ユーザが公衆ネットワークに接続できる状態になった場合に、自動的にコンテンツストア装置にアクセスすることでユーザが再度購入手続きを行なわなくても、正式コンテンツを購入することが可能となる。

40

【0011】

(3) また、本発明のコンテンツストア装置は、端末装置またはローカルサーバ装置が公衆ネットワークに接続できる通信エリアに存在する場合に前記端末装置または前記ローカルサーバ装置にコンテンツを配信するコンテンツストア装置であって、前記ローカルサーバ装置に固有のローカルサーバ装置識別情報および仮コンテンツ毎に付与する仮コンテンツ付与用識別情報から、仮コンテンツ付与情報を生成する仮コンテンツ付与情報生成部と、前記仮コンテンツ付与情報および正式コンテンツから、前記ローカルサーバ装置に配

50

信する仮コンテンツを生成する仮コンテンツ生成部と、を備え、前記公衆ネットワークを介して前記ローカルサーバ装置との認証が済んだ後で、前記ローカルサーバ装置に対して、前記仮コンテンツを配信することを特徴とする。

【0012】

この構成により、コンテンツの配信や認証を行うセンターが公衆ネットワーク等を通じて外部に存在するコンテンツ配信システムにおいて、公衆ネットワークへの接続ができなくなる状態が生じる限定エリアにおいても、限定エリア内でコンテンツを利用することができる。また、限定エリア外においても安全に正式コンテンツを購入することができる。

【0013】

(4) また、本発明のコンテンツストア装置は、端末装置が公衆ネットワークに接続しているときに、前記端末装置から仮購入用コンテンツと前記第2の認証情報とに紐づく付与情報を取得し、前記付与情報から、前記仮購入用コンテンツに関する情報およびユーザの正規の認証情報である第2の認証情報によって認証ができた場合は、前記端末装置に対して、正式コンテンツの配信を行なうことを特徴とする。

【0014】

この構成により、ユーザが限定エリア内で購入した仮購入用コンテンツについては、ユーザが公衆ネットワークに接続できる状態になった場合に、自動的にコンテンツストア装置にアクセスすることでユーザが再度購入手続きを行なわなくても、正式コンテンツを購入することが可能となる。

【0015】

(5) また、本発明のプログラムは、端末装置が公衆ネットワークに接続できない限定エリアに存在する場合に前記端末装置にコンテンツを配信するローカルサーバ装置のプログラムであって、前記公衆ネットワーク上に存在するコンテンツストア装置から前記限定エリア内でのみ配信する仮コンテンツを取得する処理と、前記取得した仮コンテンツを保存する処理と、前記仮コンテンツに前記限定エリアの識別情報を加えて、仮購入用コンテンツを生成する処理と、前記限定エリア内でのみ有効な第1の認証情報に基づいて、前記端末装置の認証を行なう処理と、前記認証済みの端末装置から要求があったときは前記認証済みの端末装置に対して前記仮購入用コンテンツを配信する処理と、の一連の処理をコンピュータに実行させることを特徴とする。

【0016】

この構成により、コンテンツの配信や認証を行うセンターが公衆ネットワーク等を通じて外部に存在するコンテンツ配信システムにおいて、公衆ネットワークへの接続ができなくなる状態が生じる限定エリアにおいても、限定エリア内でコンテンツを利用することができる。また、限定エリア外においても安全に正式コンテンツを購入することができる。ユーザが限定エリア内で購入した仮購入用コンテンツについては、ユーザが公衆ネットワークに接続できる状態になった場合に、自動的にコンテンツストア装置にアクセスすることでユーザが再度購入手続きを行なわなくても、正式コンテンツを購入することが可能となる。

【0017】

(6) また、本発明のコンテンツ配信方法は、端末装置が公衆ネットワークに接続できない限定エリアに存在する場合に前記端末装置にコンテンツを配信するコンテンツ配信方法であって、前記公衆ネットワーク上に存在するコンテンツストア装置から前記限定エリア内でのみ配信する仮コンテンツを取得するステップと、前記取得した仮コンテンツを保存するステップと、前記仮コンテンツに前記限定エリアの識別情報を加えて、仮購入用コンテンツを生成するステップと、前記限定エリア内でのみ有効な第1の認証情報に基づいて、前記端末装置の認証を行なうステップと、前記認証済みの端末装置から要求があったときは前記認証済みの端末装置に対して前記仮購入用コンテンツを配信するステップと、を少なくとも含むことを特徴とする。

【0018】

この構成により、コンテンツの配信や認証を行うセンターが公衆ネットワーク等を通じ

10

20

30

40

50

て外部に存在するコンテンツ配信システムにおいて、公衆ネットワークへの接続ができなくなる状態が生じる限定エリアにおいても、限定エリア内でコンテンツを利用することができる。また、限定エリア外においても安全に正式コンテンツを購入することができる。ユーザが限定エリア内で購入した仮購入用コンテンツについては、ユーザが公衆ネットワークに接続できる状態になった場合に、自動的にコンテンツストア装置にアクセスすることでユーザが再度購入手続きを行なわなくても、正式コンテンツを購入することが可能となる。

【0019】

(7) また、本発明のコンテンツ配信システムは、上記(1)記載のローカルサーバ装置と、上記(2)記載の端末装置と、上記(3)記載のコンテンツストア装置と、から構成される。

10

【0020】

この構成により、コンテンツの配信や認証を行うセンターが公衆ネットワーク等を通じて外部に存在するコンテンツ配信システムにおいて、公衆ネットワークへの接続ができなくなる状態が生じる限定エリアにおいても、限定エリア内でコンテンツを利用することができる。また、限定エリア外においても安全に正式コンテンツを購入することができる。ユーザが限定エリア内で購入した仮購入用コンテンツについては、ユーザが公衆ネットワークに接続できる状態になった場合に、自動的にコンテンツストア装置にアクセスすることでユーザが再度購入手続きを行なわなくても、正式コンテンツを購入することが可能となる。

20

【発明の効果】

【0021】

本発明によれば、コンテンツの配信や認証を行うセンターが公衆ネットワーク等を通じて外部に存在するコンテンツ配信システムにおいて、公衆ネットワークへの接続ができなくなる状態が生じる限定エリアにおいても、限定エリア内でコンテンツを利用することができる。また、限定エリア外においても安全に正式コンテンツを購入することができる。ユーザが限定エリア内で購入した仮購入用コンテンツについては、ユーザが公衆ネットワークに接続できる状態になった場合に、自動的にコンテンツストア装置にアクセスすることでユーザが再度購入手続きを行なわなくても、正式コンテンツを購入することが可能となる。

30

【図面の簡単な説明】

【0022】

【図1】本実施形態に係るコンテンツ配信システムの概略構成を示すブロック図である。

【図2】コンテンツストアの概略構成を示すブロック図である。

【図3】ローカルサーバの概略構成を示すブロック図である。

【図4】端末装置の概略構成を示すブロック図である。

【図5】端末装置の動作例を示すフローチャートである。

【図6】ローカルサーバの動作例を示すフローチャートである。

【図7】コンテンツストアの動作例を示すフローチャートである。

【図8】コンテンツストアの動作例を示すフローチャートである。

40

【発明を実施するための形態】

【0023】

本実施形態は、コンテンツの配信や認証を行うセンターが公衆ネットワーク等を通じて外部に存在するコンテンツ配信システムにおいて、公衆ネットワークへの接続ができなくなる状態生じる限定エリアにおいても、エリア内でコンテンツを利用でき、かつエリア外においても自動的に安全に正式のコンテンツを購入できるしくみを提供する。例えば、地下鉄や飛行機内などの公衆ネットワークへ接続することできず、コンテンツの購入サーバへアクセスすることができない限定エリアにおいて、仮コンテンツを格納するローカルサーバと、仮購入用コンテンツを限定したエリア内に配信するために限定エリア内の端末と認証を行い、仮購入用コンテンツを配信するアクセスポイントとを設ける。

50

【 0 0 2 4 】

コンテンツストアは、あらかじめ限定エリアへ、仮コンテンツを配信しておく。公衆ネットワークへ接続することのできないエリアにある端末は、アクセスポイントと仮の認証を行なって、ローカルサーバへ接続し、仮購入画面から仮購入手続きを行い、仮購入用コンテンツを購入してダウンロードを行う。その際に、端末では仮購入用コンテンツの情報と、ユーザの正規認証情報とから、その後購入サーバにアクセスできるようになった際にサーバと認証を行うための認証情報を生成する。

【 0 0 2 5 】

その後、端末が公衆ネットワークへ接続できる状態になった際に、端末は公衆ネットワークを通じてコンテンツの購入サーバへ自動的にアクセスして、作成した仮購入用コンテンツの情報と、ユーザの正規認証情報とから作成した情報とから本決済を行い、正式コンテンツの再ダウンロード等を行う。

10

【 0 0 2 6 】

本明細書では、正式コンテンツではなく“仮のコンテンツ”であって、コンテンツストアおよびローカルサーバに単に保存されている状態のコンテンツを、「仮コンテンツ」と呼称し、ローカルサーバが、仮コンテンツに限定エリアの識別情報を加えて端末装置用に加工したものを「仮購入用コンテンツ」と呼称する。

【 0 0 2 7 】

図 1 は、本実施形態に係るコンテンツ配信システムの概略構成を示すブロック図である。コンテンツ配信システムにおいて、コンテンツストア 1 は、正式コンテンツおよび仮コンテンツを配信するコンテンツ配信部 3 と、ユーザの認証を行なう認証部 5 と、を備えている。また、コンテンツストア 1 は、公衆ネットワーク 7 に接続されている。端末 2 3 は、公衆通信送受信局 9 を介して公衆ネットワークに接続し、無線通信を行なう。

20

【 0 0 2 8 】

限定エリア 1 5 は、例えば、地下鉄や飛行機内などの公衆ネットワークへ接続することのできないエリアであり、限定エリア内ローカルサーバ 1 7、限定エリア内アクセスポイント 1 9、および端末 2 1 を含む。ただし、地下鉄の車両が車庫に入った状態や飛行機が飛行場に停止している状態などでは、限定エリア内ローカルサーバ 1 7 は、限定エリア用配信機 1 3、限定エリア送受信局 1 1、公衆通信送受信局 9 を介して、公衆ネットワークに接続することが可能である。すなわち、限定エリア内ローカルサーバ 1 7 は、コンテンツストア 1 と通信を行なうことが可能となる。

30

【 0 0 2 9 】

図 2 は、コンテンツストアの概略構成を示すブロック図である。ローカルサーバリスト 1 0 1 は、正式のローカルサーバとして登録したローカルサーバを特定する情報をリスト化して保存する。仮コンテンツ用付与情報生成部 1 0 3 は、仮コンテンツ付与用固有情報、ローカルサーバ情報から、仮コンテンツに付与するための情報を生成する。仮コンテンツ付与用固有情報 1 0 7 は、仮コンテンツ毎の固有の情報である。通信部 1 0 9 は、公衆ネットワークを通じてローカルサーバや端末装置と通信を行なうためのインタフェースとして機能する。ローカルサーバ認証部 1 1 0 は、ローカルサーバとの認証を行なう。端末認証部 1 1 1 は、端末装置との認証を行なう。

40

【 0 0 3 0 】

情報照合部 1 1 3 は、コンテンツを配信する際に、ローカルサーバリスト 1 0 1 や、後述するユーザリスト 1 1 5 と情報を照合し、照合が成立した場合に、コンテンツ配信の指示を出力する。ユーザリスト 1 1 5 は、正式のユーザとして登録したユーザを特定する情報をリスト化して保存する。正式コンテンツ保存部 1 1 7 は、正式コンテンツを保存し、認証が成立した端末装置からの要求に応じて、正式コンテンツを出力する。ローカルサーバ配信コンテンツ生成部 1 1 9 は、正式コンテンツに対し、ローカルサーバ情報や、コンテンツ識別情報を付与し、また、DRM (Digital Rights Management) 制限情報や、視聴時間の制限、エリアの限定、画質劣化処理などを行ない、ローカルサーバで配信するための仮コンテンツを生成する。仮購入用コンテンツ情報抽出部 1 2 1 は、端末装置から送

50

信された仮購入用コンテンツに関する情報から、ユーザ情報、コンテンツ情報、ローカルサーバ情報を抽出する。

【 0 0 3 1 】

以上のように構成されたコンテンツストアは、ローカルサーバに対して、以下のように機能する。すなわち、限定エリア内のローカルサーバ毎に付与する限定エリアローカルサーバ識別情報と、仮コンテンツ毎に付与する仮コンテンツ付与用個別情報とから、仮コンテンツ付与情報を生成する。この仮コンテンツ付与情報と、正式コンテンツとから、限定エリアローカルサーバで配信するための仮コンテンツを生成する。仮コンテンツは、正式購入コンテンツにDRMを施して、時間限定や、視聴エリア限定のような形で閲覧を限定しても良いし、正式コンテンツの一部分のみとしたり、質を落としたりするなど、正式購入コンテンツと差をつけても良く、正式コンテンツとは異なる制限を設けることとする。コンテンツストアは、公衆ネットワークなどを通じて、限定エリアローカルサーバと通信・認証を行い、正しい限定エリアローカルサーバであることを確認した後、限定エリアローカルサーバに、対応した仮コンテンツを配信する。

10

【 0 0 3 2 】

また、コンテンツストアは、端末装置に対して、以下のように機能する。すなわち、端末装置と通信し、端末装置が限定エリア内ローカルサーバで購入した仮購入用コンテンツおよびユーザ情報に紐づく付与情報を抽出する。ローカルサーバの識別情報に紐づく情報が付与されている場合は、それも抽出し、正しいローカルサーバを通じて配信したものであるかどうかを検証し、集計して、どのローカルサーバから配信したのかなどの統計を取ってマーケティングなどに生かせるようにしても良い。抽出した付与情報から、仮購入用コンテンツに関する情報 および端末装置の正規の認証情報を抽出し、それが正しいものであるならば端末装置が正規のものであり、また、端末装置が仮購入したコンテンツが正しいものであると判断して、対応する正式コンテンツの配信を、端末装置に対して行う。

20

図3は、ローカルサーバの概略構成を示すブロック図である。限定エリア用配信機通信部201は、公衆通信網（公衆ネットワーク）とのインタフェースとして機能する。仮コンテンツ保存部203は、公衆ネットワークを介してコンテンツストアからダウンロードした仮コンテンツを保存する。仮購入用コンテンツ生成部205は、仮コンテンツに対して、ローカルエリア識別情報211を加えて、端末装置に配信する仮購入用コンテンツを生成する。対端末通信部207は、端末装置と通信するインタフェースとして機能する。コンテンツストア認証部209は、コンテンツストアとの認証を行なう。端末認証部213は、端末装置との認証を行なう。例えば、悪意のある端末装置リスト等もここに含まれる。

30

【 0 0 3 3 】

以上のように構成されたローカルサーバは、地下鉄の車両の車庫や空港等の、公衆ネットワークを通じてコンテンツストアへ接続できる状態にあるときに、コンテンツストアと認証を行う。コンテンツストアとの認証終了後、コンテンツストアから限定エリア内でのみ配信する仮コンテンツの配信を受け、保存する。仮コンテンツには、ローカルサーバの識別情報を付加しても良い。限定エリア内で、端末装置が通信を求めてくると、端末装置が、限定エリア内での通信が可能である対応端末であることを識別し、認証する。認証は、端末装置もしくは端末装置に搭載されているアプリケーションが、本システムに対応しているかどうかのみを判別するようにすればよいが、例えば、悪意のあるユーザを排除したり、ユーザのレベルによって、配信する仮購入用のコンテンツを変えるなど、ユーザの識別情報を端末装置から受信し、ユーザレベルでの識別を行っても良い。認証後、端末装置へ仮購入できるコンテンツのリストを送付する。端末装置から、コンテンツの購入要求があれば、仮購入用コンテンツを配信する。

40

【 0 0 3 4 】

図4は、端末装置の概略構成を示すブロック図である。通信部301は、ローカルサーバや公衆ネットワークとの通信インタフェースとして機能する。情報抽出部303は、ローカルサーバからの受信情報から付加情報とコンテンツとを分離し、付加情報を解析し、

50

抽出する。コンテンツ保存部 305 は、ローカルサーバまたは公衆ネットワークから受信したコンテンツを保存する。表示情報生成・制御部 307 は、コンテンツに対し、DRM 情報などにより視聴制限を行なう制御を行なうと共に、端末装置のユーザインタフェースに表示させるための表示情報を生成する。UI (ユーザインタフェース) 部 309 は、ユーザに対する情報の出力を行ない、ユーザの操作を入力として受け付けるインタフェースとして機能する。

【0035】

情報送出处 311 は、認証情報や、付与情報を送付する。仮購入用コンテンツ情報保存部 313 は、仮購入用コンテンツに関する情報を保存する。DRM 制御部 315 は、仮購入用コンテンツを再生する際に、視聴制限や、意図的な画質劣化などを起こさせるための制御を行なう。購入画面作成部 317 は、ユーザが、仮購入用コンテンツを購入する際の入力画面を作製する。端末情報 319 は、限定エリア内でのみ有効な第 1 の識別情報や、ユーザの正規の識別情報である第 2 の識別情報を保存する。付与情報生成部 321 は、仮購入用コンテンツから抽出した付加情報およびユーザの正規の認証情報である第 2 の認証情報から、仮購入用コンテンツと第 2 の認証情報とに紐づく付与情報を生成する。ユーザ入力情報判別部 323 は、UI 部 309 から入力された情報が、ユーザの正規の識別情報である第 2 の識別情報であるかどうかを判別し、第 2 の識別情報が入力された場合は、付与情報生成部 321 に出力する。

【0036】

以上のように構成された端末装置は、限定エリア内でローカルサーバとの通信・認証を行う。認証する際は、ローカルサーバに対してはユーザの正規の認証情報(第 2 の認証情報)は送信しない。端末情報、若しくはユーザの正規の認証情報とは異なり、ユーザを識別するための識別情報(第 1 の識別情報)を送信する。認証後、端末装置は、ローカルサーバから、そのローカルサーバで購入することができる仮コンテンツのリストの配信を受け、UI 部 309 に表示する。

【0037】

ユーザが諸望の仮コンテンツを選択すると、購入希望情報がローカルサーバへ送信され、ローカルサーバから仮購入用コンテンツが配信される。この時、配信された仮購入用コンテンツが、正規のローカルサーバからのものであるかどうかを検証し、正規のローカルサーバであった場合のみ表示し、正式購入のためのコンテンツストアに送信する付与情報を生成する。これにより、悪意の下で構成されたサーバから、例えば、ユーザが望まない広告目的のコンテンツの配信を受けることを防ぐことができる。

正規のローカルサーバからのものであるかどうかの検証は、仮購入用コンテンツに付随しているローカルサーバの識別情報と(コンテンツストアが付与する)、ローカルサーバが付与したローカルサーバの識別情報とが一致するかを検証することによって行なう。仮購入時、若しくは仮購入用コンテンツのダウンロード時に、端末装置は、合わせて、正規の認証情報の入力画面を、UI 部 309 を通じて表示させ、ユーザからの正規の認証情報の入力を受ける。入力された正規の認証情報と、仮購入用コンテンツに付与されている情報とから、コンテンツストアに送信する付与情報を生成する。

【0038】

ユーザが入力した正規の認証情報は、付与情報生成後、消去することで安全を保つことが可能となる。付与情報には、コンテンツの識別情報とユーザの識別情報に紐づく情報が含まれることとなるが、さらにこれに、仮購入用コンテンツにローカルサーバの識別情報が含まれる場合、ローカルサーバに紐づく情報が含まれるようにしても良い。このように、端末装置は、ユーザの正規の認証情報と、仮購入用コンテンツに付与されている情報とから、端末装置がコンテンツストアと接続できる状態になった時に認証を行い正式コンテンツの配信を受けるための付与情報を生成する。

【0039】

端末装置が、公衆ネットワークを通じてコンテンツストアへ接続できる状態になり、かつ、仮購入用コンテンツの購入を行っている場合、上記付与情報をコンテンツストアへ送

10

20

30

40

50

信する。この情報に基づいて、コンテンツストアにより仮購入用コンテンツおよびユーザ認証情報が正規のものであると判断されると、コンテンツストアから正式コンテンツが配信される。仮購入用コンテンツを、正式コンテンツにDRMを施して生成している場合は、DRMを外すことで正式コンテンツとすることで、ダウンロードする時間を短縮しても良い。また、仮購入用コンテンツは、制限時間経過時、限定エリア外に出たときになどに、削除を行うようにしても良い。

【0040】

次に、本実施形態に係るコンテンツ配信システムの動作について説明する。まず、端末装置の動作について説明する。図5は、端末装置の動作例を示すフローチャートである。ユーザがコンテンツの購入を希望し(ステップS1)、端末装置がコンテンツストアと通信を行なう(ステップS2)。次に、端末装置が限定エリア内に存在するかどうかを判断する(ステップS3)。端末装置が限定エリア内に存在している場合は、仮購入画面を表示する(ステップS5)。次に、ユーザがコンテンツを選択し、仮購入する(ステップS6)。次に、コンテンツストアと通信可能であるかどうかを判断し(ステップS8)、コンテンツストアと通信が可能でない場合は、ユーザが仮購入用コンテンツを視聴できるようにし(ステップS9)、ステップS8に遷移する。一方、ステップS8において、端末装置がコンテンツストアと通信が可能である場合は、ステップS10に遷移する。

10

【0041】

ステップS3において、端末装置が限定エリア内に存在している場合は、正規購入画面を表示する(ステップS4)。そして、ユーザが正式コンテンツを選択し、購入する(ステップS7)。次に、認証を行なった後、正式コンテンツを配信し(ステップS10)、ユーザが正式コンテンツを視聴できるようになる(ステップS11)。

20

【0042】

図6は、ローカルサーバの動作例を示すフローチャートである。ローカルサーバが、コンテンツストアと通信が可能である状態で、コンテンツストアとの認証を行なう(ステップS101)。次に、ローカルサーバは、コンテンツストアから仮コンテンツを受信する(ステップS102)。次に、仮コンテンツへローカルサーバ識別情報を付与し(ステップS103)、端末装置から、通信要求があったかどうかを判断する(ステップS104)。端末装置から、通信要求がない場合は、ステップS104の判断を繰り返し、端末装置から、通信要求があった場合は、端末装置の認証を行なう(ステップS105)。この認証で、端末装置が正規であるかどうかを判断し(ステップS106)、正規でない場合は、不正端末として、リスト化する。一方、正規であった場合は、仮購入用コンテンツリストを端末装置に送付する(ステップS107)。次に、購入要求があったかどうかを判断し(ステップS108)、無い場合は、ステップS108の判断を繰り返す。一方、ステップS108において、購入要求があった場合は、仮購入用コンテンツを端末装置に配信する(ステップS109)。

30

【0043】

図7は、コンテンツストアの動作例を示すフローチャートである。まず、ローカルサーバに対する動作を示す。ローカルサーバからの通信依頼があると(ステップS201)、ローカルサーバに対する認証を行ない、ローカルサーバの識別を行なう(ステップS202)。次に、仮コンテンツを生成し(ステップS203)、仮コンテンツに対し、ローカルサーバ識別情報を付与する(ステップS204)。次に、対ローカルサーバコンテンツ配信リストを更新し(ステップS205)、ローカルサーバへ仮コンテンツを配信する(ステップS206)。

40

【0044】

図8は、コンテンツストアの動作例を示すフローチャートである。ここでは、端末装置に対する動作を示す。端末装置からの通信依頼があると(ステップS301)、端末装置に対する認証を行ない、また、端末装置の識別を行なう(ステップS302)。次に、端末装置から付与情報を受信したかどうかを判断し(ステップS303)、付与情報を受信していない場合は、通常動作を行なう。一方、ステップS303において、端末装置から

50

付与情報を受信した場合は、付与情報からコンテンツ情報、ユーザ情報、ローカルサーバ情報を抽出する(ステップS304)。次に、ユーザ情報が正しいかどうかを判断し(ステップS305)、正しくない場合は何もせず、正しい場合は、ローカルサーバ情報が正しいかどうかを判断する(ステップS306)。ステップS306において、ローカルサーバ情報が正しくない場合は、何もせず、正しい場合は、ローカルサーバ情報と、コンテンツとを対比し、対ローカルサーバコンテンツ配信リストと一致しているかどうかを判断する(ステップS307)。一致していなければ何もせず、一致していた場合は、ユーザへ正式コンテンツを配信する(ステップS308)。

【0045】

以上説明したように、本実施形態によれば、コンテンツの配信や認証を行うセンターが公衆ネットワーク等を通じて外部に存在するコンテンツ配信システムにおいて、公衆ネットワークへの接続ができなくなる状態が生じる限定エリアにおいても、限定エリア内でコンテンツを利用することができる。また、限定エリア外においても安全に正式コンテンツを購入することができる。ユーザが限定エリア内で購入した仮購入用コンテンツについては、ユーザが公衆ネットワークに接続できる状態になった場合に、自動的にコンテンツストア装置にアクセスすることでユーザが再度購入手続きを行わなくても、正式コンテンツを購入することが可能となる。

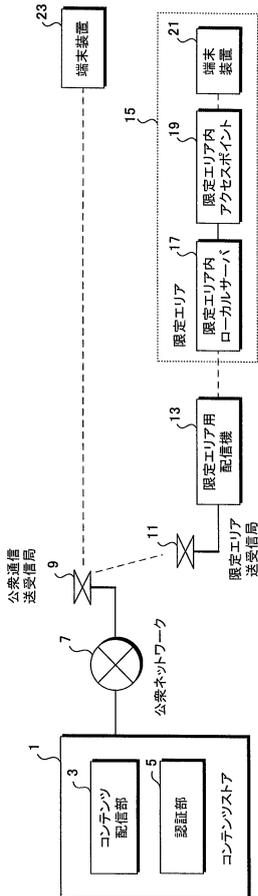
【符号の説明】

【0046】

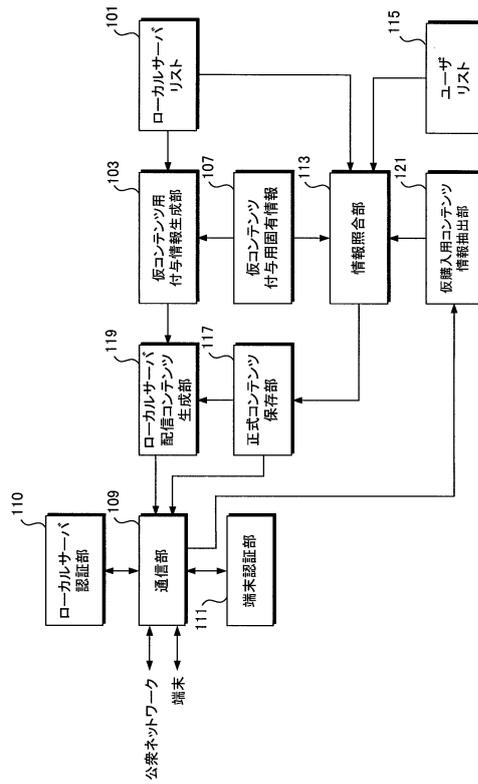
1	コンテンツストア	20
3	コンテンツ配信部	
5	認証部	
7	公衆ネットワーク	
9	公衆通信送受信局	
11	限定エリア送受信局	
13	限定エリア用配信機	
15	限定エリア	
17	限定エリア内ローカルサーバ	
19	限定エリア内アクセスポイント	
21	端末装置	30
23	端末装置	
101	ローカルサーバリスト	
103	仮コンテンツ用付与情報生成部	
107	仮コンテンツ付与用固有情報	
109	通信部	
110	ローカルサーバ認証部	
111	端末認証部	
113	情報照合部	
115	ユーザリスト	
117	正式コンテンツ保存部	40
119	ローカルサーバ配信コンテンツ生成部	
121	仮購入用コンテンツ情報抽出部	
201	限定エリア用配信機通信部	
203	仮コンテンツ保存部	
205	仮購入用コンテンツ生成部	
207	対端末通信部	
209	コンテンツストア認証部	
211	ローカルエリア識別情報	
213	端末認証部	
301	通信部	50

- 3 0 3 情報抽出部
- 3 0 5 コンテンツ保存部
- 3 0 7 表示情報生成・制御部
- 3 0 9 U I 部
- 3 1 1 情報送出部
- 3 1 3 仮購入用コンテンツ情報保存部
- 3 1 5 D R M 制御部
- 3 1 7 購入画面作成部
- 3 1 9 端末情報
- 3 2 1 付与情報生成部
- 3 2 3 ユーザ入力情報判別部

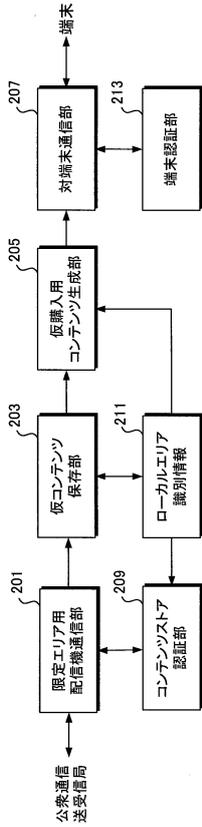
【 図 1 】



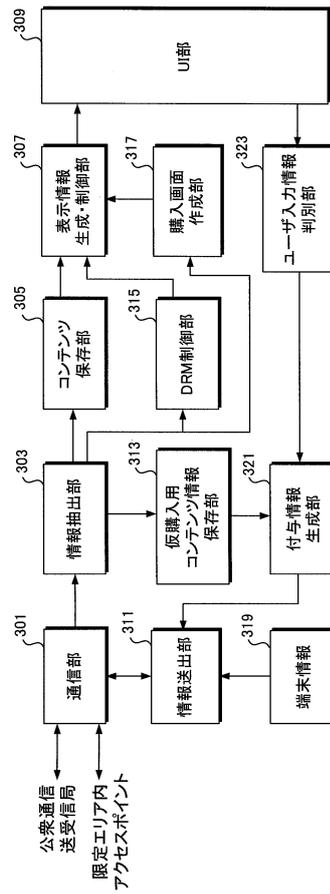
【 図 2 】



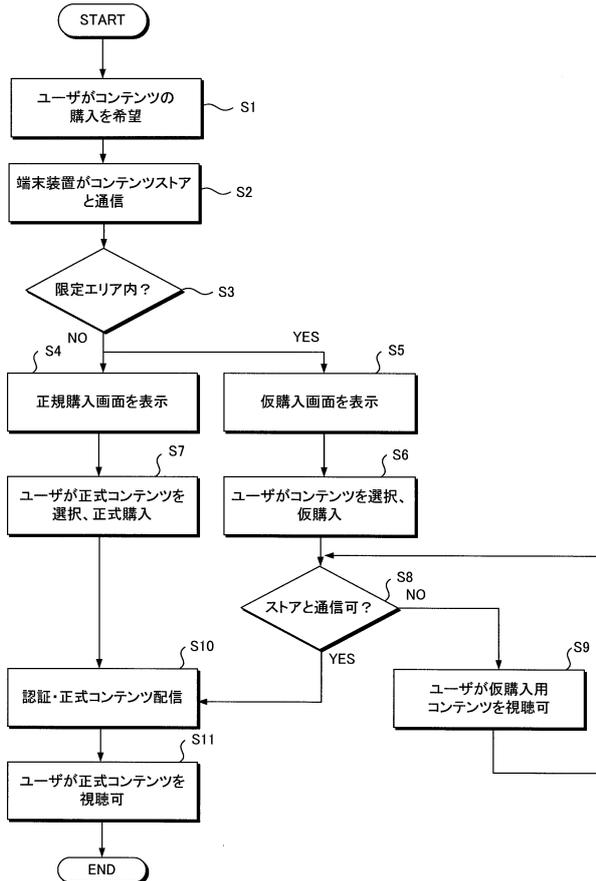
【図3】



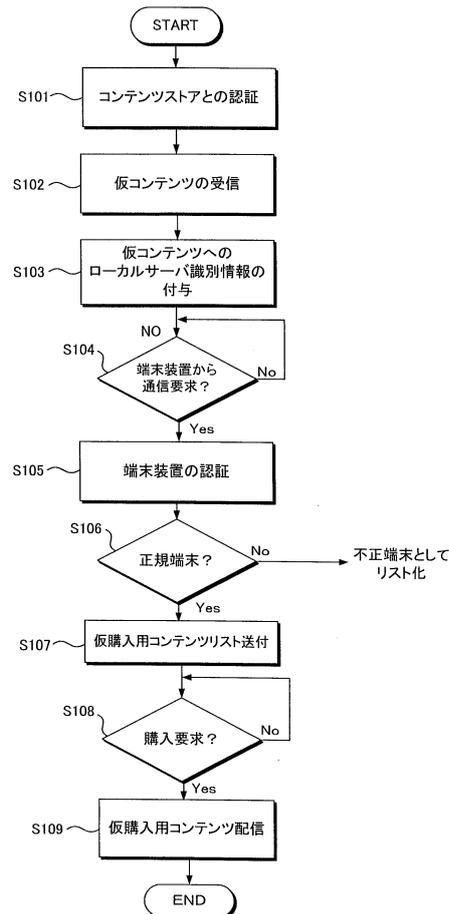
【図4】



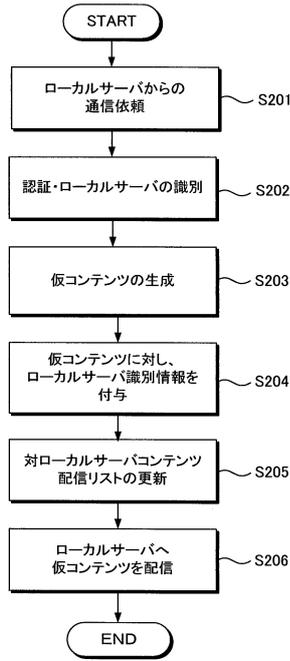
【図5】



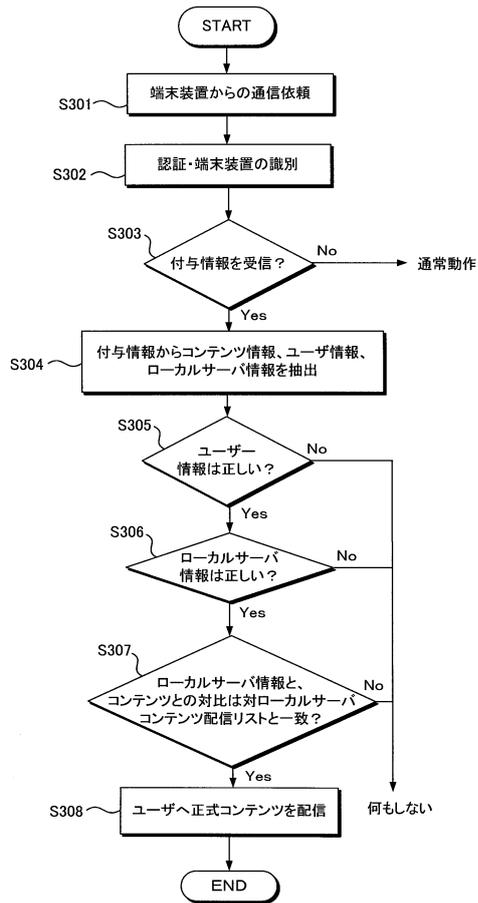
【図6】



【 図 7 】



【 図 8 】



フロントページの続き

- (56)参考文献 特開2006-245873(JP,A)
特表2012-501509(JP,A)
特開2004-220464(JP,A)
特開2004-157784(JP,A)
特開2007-043440(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06Q 10/00-99/00