利用者制限を可能にするマルチキャスト型ストリーム配送方式

庵　祥子　　三宅　延久
ＮＴＴ情報流通プラットフォーム研究所

概要

インターネットのブロードバンド化に伴い、インターネットにおいて動画などのストリームコンテンツを放送型で提供するサービスへのニーズが高まっている。しかしながら放送型サービスは多数のユーザに同時にコンテンツを配信するため、ネットワークに負荷がかかるという問題がある。また放送型サービスであっても視聴の権利をもったユーザだけが視聴できるようにしなければならないという課題がある。そこで、配送にIPv6マルチキャストを利用してネットワークの負荷の軽減を図るとともに、配送するコンテンツの暗号化と復号鍵の配送先を制御することによって利用者の制限を可能にする「マルチキャスト型ストリーム配送方式」を提案した。またコンテンツの暗号化方式と鍵の配送方式（ユニキャスト/ マルチキャスト）を変えて２通りの実装を行い動作を確認した。

Access control methods for multicast streaming contents distribution

Shoko Ihori,　Nobuhisa Miyake
NTT Information Sharing Platform Laboratories

abstract

As broadband Internet becomes widespread, the need for broadcasting stream contents on the Internet is growing. However, network traffic becomes an issue because broadcasting sends content to multiple users simultaneously. Also, only authenticated users should be allowed to watch stream in a broadcasting system. To satisfy these requirements, a multicast delivery system for stream contents which has an access control function is proposed in this paper. The system reduces network traffic by using IPv6 multicasting, and restricts unauthorized reception by encrypting contents and distributing the decryption key only to authorized users. This paper also proposes two kinds of implementation method -unicast and multicast key distribution methods- and shows that these methods are feasible.

1. はじめに

インターネットのブロードバンド化に伴い、従来はラジオやテレビなどによって提供されていた音楽や映像などのコンテンツを、インターネット放送サービスとして提供する場面が見られるようになった[1].

インターネットで放送サービスを行う場合、同時に多数のユーザにコンテンツを配送しなければならない。しかしながら、複数ユーザに同時にコンテンツ配送を行う際に、各ユーザにコンテンツを個別配送するユニキャスト配送を用いるとネットワークトラフィックが増えてしまう。この問題を解決するには、同報通信が可能なマルチキャスト配送方式を利用することが有効である。

しかしながらマルチキャストで配送されるコンテンツは、マルチキャストアドレスとマルチキャストルーティングさえ設定すれば任意のユーザが取得できてしまい、ユーザのコンテンツへのア

クセス制御が不可能である。アクセス制御が実現されていないと，料金を支払った人、あるいは会員である人のみに配送する等のサービスが不可能になり、インターネット放送に有料コンテンツを導入する際の足かせになりかねない.

そこで本稿では，マルチキャスト型ストリーム配送で提供するコンテンツに関して，資格がある利用者のみに利用を許可するアクセス制御を実現する。

2. 従来のコンテンツ配送方式の考察

情報提供者がユーザにコンテンツを提供する方法として、ストリーム配送方式とダウンロード配送方式がある。本稿では放送サービスに適したコンテンツ配送としてストリーム配送に着目した。

ストリーム配送方式とは、ユーザからの要求あるいは情報提供者側の配送意志をトリガーとして、コンテンツをストリーム形式でユーザに配送する方式であり、ユーザはあたかも放送サービスを受けるがごとくインターネット上のコンテンツを視聴できる。

しかしながら、従来のストリーム配送方式を実際の放送型サービスに適用するにはいくつかの問題点がある。

まず、情報提供者とユーザの関係がある一時点で1対1であることを仮定しているという問題が挙げられる。放送型サービスに対応するためには、情報提供者に対し常に複数のユーザが存在することを考慮しなければならない。また、同時に複数のユーザにコンテンツを配送する場合に、トラフィック量がユーザ数に比例して増大することを避けなければならない。

次にコンテンツの不正利用に対する防御策も必要である。従来のストリーム配送方式ではコンテンツをユーザ端末に保存しないことを前提としているためか、不正利用防止をおざなりにする傾向にあった。ダウンロード型配送のようにコンテンツを暗号化し、その復号鍵であるアクセス権を配布する等の対策が必要である。

3. 放送型サービス適応時の問題点

2 章で従来のストリーム型配送方式について考察した結果、ストリーム型配送方式でコンテンツの放送型サービスを実現する際の問題点は主に3点あることが明らかになった。以下の節でそれらの問題点について述べる。

3. 1 放送型サービスに対応するためのトラフィック増加に関する問題

従来のストリーム配送方式では、情報提供者にユーザが個別アクセスしていたために、情報提供者・ユーザ間の通信が1対1で行われていた。放送型サービスに対応するためには情報提供者・ユーザ間で1対多の通信を用いる必要がある。さらに1対多の通信が行われてもトラフィックがユーザ数に比例して増加しないように、マルチキャスト通信を用いる必要がある。

3. 2 ストリームコンテンツに対応するためのアクセス制御に関する問題

ストリーム配送のコンテンツであっても不正利用に対する防御策は必要である。コンテンツのアクセス制御で一般的な方式としては、ダウンロード配送で行われているカプセル化方式[2]がある。カプセル化方式とは、あらかじめ配送するコンテンツを暗号化し、暗号化コンテンツとその復号鍵にあたるアクセス権をユーザに配送する方式である(図1)。

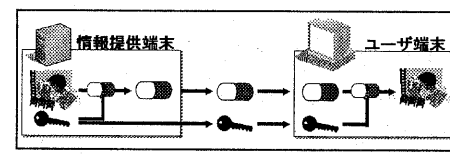

図 1:カプセル化方式

この方式をストリーム配送の放送型サービスに適用するには時間の概念が欠けていることが問題である。従来適用していたダウンロードコンテ

ンツの場合、コンテンツはファイルの単位で扱われ、どのユーザがどのファイルを利用していいのかという情報を管理することによってアクセス制御を行えば十分だった。しかしながらストリームコンテンツの場合は、ある時刻からある時刻までの間だけアクセスを許可したいといった要求がある。このため、ストリーム配送の放送型サービスにおけるアクセス制御では、時間制御の実現も不可欠である。

3.3 放送型サービスに対応するためのアクセス権配送信頼性に関する問題

放送型サービスにおいてカプセル化方式によって時間制御を実現しても、次のような問題が発生する。すなわちカプセル化方式のアクセス制御では、各ユーザに対して利用状況に応じたアクセス権を配布しなければならないが、このアクセス権の配布方法も1対多通信に対応させなければならない。特にアクセス権の配送に遅延が生じると、対応するコンテンツが視聴できなくなるため、アクセス権配送の信頼性を向上させる必要がある。

4. アクセス制御を可能とした放送型ストリーム配送方式の提案

本章では3章で述べた3つの問題を解決し，アクセス制御を可能にする放送型のストリーム型コンテンツ配送方式を提案する.

本方式はカプセル化方式のアクセス制御を採用し、暗号化コンテンツをマルチキャストプロトコルで配送する。視聴を希望しているユーザは特定のマルチキャストアドレスを指定することにより暗号化コンテンツを取得する。復号鍵にあたるアクセス権は視聴資格を持つユーザに対して別途配送する。またコンテンツを単位時間ごとに分割し、その各々についてアクセス権の変更とアクセス権の配送管理を行うことによって、単位時間ごとのアクセス制御を実現している。さらに、暗号化コンテンツよりも早いタイミングでアクセス権を配送することによりアクセス権の到着の信頼性を高めているという特徴も兼ね備える。

3章で述べた問題点である「放送型サービスに対応するためのトラフィック増加に関する問題」についてはマルチキャストプロトコルを利用し、暗号化コンテンツをマルチキャスト配送することで実現する。マルチキャスト技術を導入することにより、ユーザ数の増加に対するトラフィックの増加率を削減することが可能になる。

「ストリームコンテンツに対応するためのアクセス制御に関する問題」についてはコンテンツを暗号化し、暗号化コンテンツと復号鍵にあたるアクセス権を配布することにより特定のユーザのみコンテンツを視聴することを可能にする。また、コンテンツをある単位時間で区切ってアクセス権を変更することにより、アクセス権の利用制御に対して時間制御の導入する。これにより各ユーザは自分が視聴する時間のアクセス権のみを取得することが可能になる。

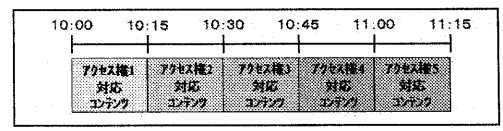

図2:時間制御の実現例

「放送型サービスに対応するためのアクセス権配送信頼性に関する問題」については、暗号化コンテンツよりも早いタイミングでアクセス権を配布することによって暗号化コンテンツが到着した際のアクセス権の到着信頼性の向上を図る。さらにUDPパケット等パケットの到着信頼性が低い場合には切り替え予告通知を行う。切替予告通知とは、アクセス権を切り替える一定時間前に、切替えることを予告する情報をユーザ端末に通知するものである。各ユーザ端末は自端末内に切替え後のアクセス権が到着しているかを確認し、到着していない場合にはサーバへ再送の要求を行う。これによりアクセス権の到着信頼性を高める。

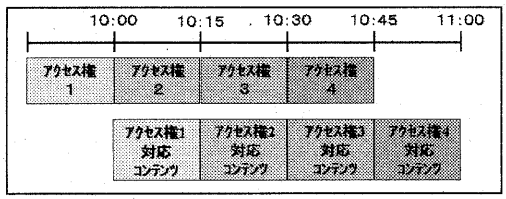

図 3:アクセス権先配りの実現例

5.提案方式の評価

2 章においてストリームコンテンツの放送型サービスを実現する際の問題点について述べた。そこではユーザ数の増加に伴いトラフィック量が増大すること、利用制御・時間制御に関わるアクセス制御が行われていないこと、アクセス制御を行った際のアクセス権の到着信頼性が低いことが問題であった。

4 章で提案したアクセス制御を可能とした放送型ストリーム配送方式は、マルチキャストプロトコルを採用することによりユーザ増加に伴うトラフィックの増加量を削減した。またコンテンツを暗号化しアクセス権を利用することによってユーザの制御を実現し、さらにコンテンツを単位時間で分割しアクセス権を変更することにより時間制御を実現した。またアクセス権を暗号化コンテンツよりも早く配送することによりアクセス権の到着信頼性を向上した。

提案方式と従来の方式を比較を表２にまとめる。

	トラフィック量	アクセス制御（時間制御）	アクセス権到着信頼性
従来型ストリーム配送	多	×	×
提案方式	少	○	○

表 1：提案方式と従来方式の比較

表１より提案方式は放送型でコンテンツ配送を行う際に従来のストリーム型コンテンツ配送よりも優れていることが確認できた。

6.提案方式の実装

提案方式の実装方法について本章で述べる。

まず、ユーザの視聴開始及び視聴終了時の取り扱いについて述べる。ユーザの視聴開始時は、ユーザのメリットを考えユーザの要求後は速やかに視聴が開始できる手法を検討した。その結果、視聴開始時間が現在時刻より前の場合にはアクセス権の切替えタイミングとは別に割り込み処理を行い、視聴を要求したユーザにアクセス権を速やかに配布することを可能とする実装とした。またユーザの視聴終了時は、サーバ等の負荷を考慮し、ユーザの要求後はアクセス権を配送しない実装とした。アクセス権は、常にコンテンツよりも早いタイミングで送付されているため、視聴終了の要求を行っても要求を行ってから2回後のアクセス権の切替え時までコンテンツを視聴することが可能である。

次にコンテンツの暗号化手法、アクセス権の配送方式の検討について述べる。コンテンツの暗号化は２種類の手法が考えられる。１つはアプリケーションレイヤにおけるのコンテンツ暗号化機構の実装であり、もう１つは IPv6 のカーネルレイヤの機構を利用した実装である。前者の場合、アプリケーションレイヤで全てが実現できるため実装や改造が行いやすいことが利点である。後者の場合は、既存の機構を利用することから実装規模が小さいことが利点である。

アクセス権の配送方式についてもＴＣＰによる配送とＵＤＰによる配送の２種類の配送を検討した。ＴＣＰによる配送の場合、通信のリライアビリティが保証されているが多数の端末が同時にセッションを張ると負荷が増大する懸念がある。ＵＤＰの場合は多数の端末と同時に通信を行っても負荷が低いが、通信のリライアビリティがないためアクセス権の到着の信頼性が低いというデメリットがある。

そこで２通りの実装を行った。１つはコンテンツをカーネルレイヤを利用して暗号化し、アクセス権の配送をＴＣＰ（ユニキャスト）で行うユニ

キャストアクセス権配送方式であり、もう１つはコンテンツをアプリケーションレイヤで暗号化し、アクセス権をＵＤＰ（マルチキャスト）で配送するマルチキャストアクセス権配送方式である。

以下に本提案方式の実装環境及びこの２つの実装方式について述べる。

6.1 実装環境

実装環境について述べる。システム構成は主にサーバ系とクライアント系に分類される。サーバ系はコンテンツ配信サーバとユーザ管理サーバ、暗号化サーバがあり、それぞれ CPU が PentiumIII800M でメモリ 512M のＰＣを利用した。ＯＳはコンテンツ配信サーバのみ Windows2000 とし、その他は FreeBSD4.2 とした。

ユーザ系は復号用ユーザ端末と再生用ユーザ端末があり、それぞれ CPU が PentiumIII800M でメモリ 256M のＰＣを利用した。ＯＳは復号用端末が FreeBSD4.2 であり、再生用端末は WindowsMe とした。また、ストリームコンテンツを配送するためのアプリケーションとして既存のオーサリング環境との整合性を踏まえ一般的に広く使われている製品の１つである Windows Media Server および Player を採用した。マルチキャストおよび IPsec を利用するため配送プロトコルは IPv6 とした。

配送で用いる IPv6 と再生に用いるアプリケーション(Windows Media Server)の両方を安定して動作させることが可能な OS がなかったため、ユーザ端末は再生用端末と復号用端末に分割して実装を行った。将来的に IPv6 と再生用アプリケーションの両方が安定的に動作する OS が実現された場合は１台の端末で動作させることができるものと考えている。

6.2 ユニキャストアクセス権配送方式

ユニキャストアクセス権配送方式では，コンテンツを IPv6 のカーネルレイヤの機能である IPsec を利用して暗号化し、復号鍵にあたるアクセス権はサーバから TCP（ユニキャスト）を用いてユーザに配送する方式である.

ユニキャストアクセス権配送方式の詳細について述べる。まずアクセス権サーバがコンテンツの暗号鍵にあたる SA(Security Association)を生成する。ユーザ管理サーバ上のデータベースを参照し利用資格を持ったユーザ端末（復号用）とコンテンツの暗号化を行うコンテンツサーバに生成した SA を IPsec を用いてユニキャストで配送する。ユーザ端末（復号用）とコンテンツサーバは受け取った SA をインストールする。さらにコンテンツサーバはストリームサーバから取得したストリームコンテンツをインストールした SA を用いて暗号化し、マルチキャストで配送する。ユーザ端末は自端末にインストールされている SA を用いて送付されたコンテンツを復号する。すなわち、マルチキャスト型の IKE を行い、マルチキャスト型の IPsec での配送を実現する。

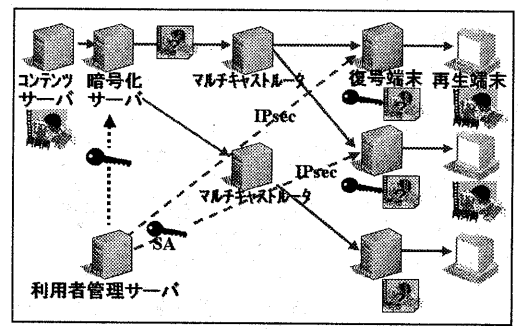

図４：ユニキャスト型アクセス権配送システム

6.3 マルチキャストアクセス権配送方式

マルチキャストアクセス権配送方式では，コンテンツをアプリケーションレイヤで実装した暗号化機構を用いて暗号化し、復号鍵にあたるアクセス権はサーバから UDP（マルチキャスト）を用いてユーザに配送する方式である.

ユニキャストアクセス権配送方式の詳細について述べる。あらかじめユーザはユーザ端末の秘密鍵と対になる公開鍵をユーザ管理サーバに登録す

るものとする。まずストリームサーバからストリームコンテンツを取得した暗号化サーバがコンテンツを暗号化する共通鍵を生成し、暗号化機構を用いてコンテンツを暗号化する。暗号化サーバは、ユーザ管理サーバのデータベースを参照して利用資格を持つユーザの公開鍵を取得する。次にコンテンツの暗号化に用いた共通鍵を、各ユーザの公開鍵で暗号化することで、各ユーザに対応したアクセス権を生成する。その後、暗号化サーバは暗号化コンテンツと各ユーザに対応したアクセス権をマルチキャストで配送する。ユーザは受け取ったアクセス権を自分の秘密鍵で復号し、取り出した共通鍵でコンテンツを復号する。

各ユーザの公開鍵を用いて共通鍵を暗号化する理由は、マルチキャストアドレスとマルチキャストルーティングを設定している全ての人にコンテンツを暗号化した共通鍵が知られてしまうとアクセス権の制御ができなくなるためである。

また、アクセス権を UDP で送付するためにアクセス権の到着信頼性が低いため、アクセス権切替予告を配送することにより、アクセス権の到着信頼性を高めた。

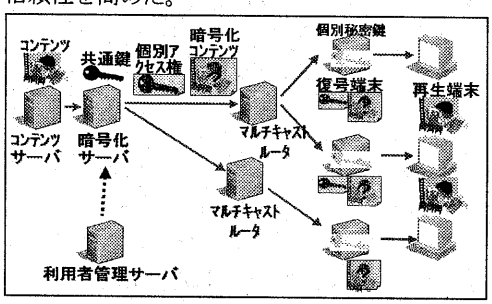

図5：マルチキャスト型アクセス権配送システム

6.4 実装結果

6章で述べた実装システムをユーザ端末9セットに対して運用した結果について述べる。

ユニキャストアクセス権配送方式、マルチキャストアクセス権配送方式の両方式においてユーザ端末9セットに対し安定的にコンテンツを配送できることが確認できた。またコンテンツの途中から視聴を要求したユーザに対しては、両方式とも速やか（1分以内）にコンテンツの閲覧が可能な状態になることを確認した。さらにコンテンツの途中で視聴の中断を要求したユーザに対しては、要求時から数えて2回あとの鍵の切替えタイミングでアクセス権の配送が終了し閲覧不可能状態になることを確認した。

7. まとめと今後の予定

本稿ではコンテンツのストリーム配送を放送型サービスに適用する際に生じる3つの問題点を明らかにした。そしてこの3つの問題点を解決するアクセス制御を可能とした放送型ストリーム配送方法を提案した。また提案した配送方法を暗号化手法とアクセス権の配送方法が異なる2つのシステムの実装を行った。さらにシステムの実装結果について報告し、両システムの動作を確認した。

今後の予定としては、実装した2つのシステムの評価が挙げられる。実装に用いた2種類の暗号化手法および2種類のアクセス権の配送方法についてそれぞれの優位性について評価・検討を行う。また、それぞれのシステムの性能を評価するために、どのくらいのユーザ数をハンドリングできるか等のスケーラビリティの評価もあわせて行う予定である。

[参考文献]

[1] http://channel.goo.ne.jp/stream/index.html
http://www.isize.com/stream/

[2] 明石,森保,寺内:FleaMarket 方式による情報流通システム，情報処理学会論文誌 Vol 39 No.2(1998.2)