8U-03 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法

庵　祥子　　三宅　延久
NTT情報流通プラットフォーム研究所

1. はじめに

インターネットの普及にともない，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上で提供する放送サービスが登場して来ている[1].

インターネット放送サービスでネットワーク負荷を軽減するためにはマルチキャスト型ストリーム配送が考えられる．しかしながらマルチキャストで配送されたストリームコンテンツの利用者を制限するアクセス制御技術は未だ確立されていない．この制御技術が実現されていないことは，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.

そこで本発表においては，マルチキャスト型ストリーム配送に際して，利用資格がある利用者のみの利用を可能にするアクセス制御を実現し，さらにその制御を一定時間単位で変更可能とする方式の提案を行なう.

2. アクセス制御を実現する際の問題点

従来のアクセス制御には，暗号やスクランブルを施したコンテンツを配信し，このコンテンツに対して利用資格を持つ利用者に対してのみコンテンツのアクセス権(利用者の情報を利用した復号鍵など)を配布する方式がある[2]．しかしこの方式をマルチキャスト型ストリーム配送に適用する場合には，以下の２つの問題がある.

(1)アクセス制御の単位

ストリームコンテンツは蓄積型コンテンツと異なり，ある一定時間のみ視聴する利用者にも対応するために，コンテンツ単位だけでなく時間単位でもアクセス制御を行なう必要がある．アクセス権を単位時間で更新しなければ，長時間に渡ってコンテンツを利用することが可能になり，利用者毎にアクセス時間を制御することが非常に困難になる.

(2)複数利用者に対するアクセス権制御

従来の蓄積型コンテンツの場合，1 回のコンテンツ配送に対してアクセス権の配送は 1 回のみであった．しかしながらコンテンツをマルチキャスト型ストリームで配送する場合，アクセス権をそれぞれの利用者に特化して利用者数分配送しなければならない．そのため利用者数が増大した場合，アクセス権の配布処理に必要とされる時間が増大すると予想される．これはアクセス権の配送の遅延につながる可能性が高いため，ライブ放送のように即時性が重要な場面では問題となる.

3. マルチキャスト型ストリーム配送方式の提案

そこで本稿では 2 章で述べた２つの問題を解決し，一定単位時間での更新を可能としたアクセス権制御付きマルチキャスト型ストリーム配送システムを提案する.

問題の解決の方針としては，アクセス制御の単位については，コンテンツをあらかじめ一定単位毎に区切って暗号化に利用する暗号化鍵を変更し，利用者によって配布する暗号化鍵を制御することにより利用者毎の一定時間単位でのアクセス権の更新を可能にする．また，複数利用者に対するアクセス制御に関しては，アクセス権を事前配布することによりアクセス権の配送遅延を防止し，ライブ放送等の即時性を求められるコンテンツへの対応も可能とする.

同時に複数利用者に対してアクセス権を配布する方法としては，個別にアクセス権を配布するユニキャスト方式と，それぞれのアクセス権をまとめて配布するマルチキャスト方式が考えられる．本稿ではこの両方式について提案する.

Access control methods for multicast streaming contents distribution
Shoko Ihori,　Nobuhisa Miyake
NTT Information Sharing Platform Laboratories

3.1 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，コンテンツのアクセス権をサーバから利用者端末にユニキャストで配送する方式である．本配送方式の場合，アクセス権配送のリライアビリティが保証されるという利点がある．しかしながら個々に通信を行なうために処理時間がかかるために効率的配送方法の採用が必要である．そこで，マルチキャストにおけるIPsecの機構を利用することを提案する．IPsecの機構を利用することにより，効率的にアクセス権の配送を行なう実装ができることが期待される．

3.2 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とは，アクセス権もマルチキャスト方式で利用者端末に配送する方式である．本方式の場合，コンテンツと同様に低負荷で鍵の配送を行なうことができる一方で，鍵の配送におけるリライアビリティがないことや利用者毎に制御できないことが問題となる．そこで鍵配送のリライアビリティ向上のために鍵切替予告を配送することを提案する．鍵切替予告とは，ある一定時間以内にコンテンツのアクセス権を変更することを通知するものである．利用者端末はこの予告を取得した時点で次のアクセス権を取得していない場合は，アクセス権サーバに直接アクセス権を取得しにいく方式である．また利用者毎の制御方法としてアクセス権を各利用者の公開鍵で暗号化することを提案する．

4.マルチキャスト型ストリーム配送システム実装

4.1 ユニキャストアクセス権配送方式

現状ではマルチキャスト用のIKEの機構が確立されていないため独自のIKE機構を実装する．

システム構成をコンテンツサーバ，アクセス権サーバ，利用者端末とする(図 1)．アクセス権サーバはユニキャストで各々の利用者端末と通信しIKEを行なう．アクセス権サーバは利用者端末と交わした鍵をコンテンツサーバに送付し，コンテンツサーバはその鍵を用いてコンテンツを暗号化し，マルチキャストで利用者端末に送付する．定期的なアクセス権の更新は，疑似的なマルチキャストIKEを用いて実現する．

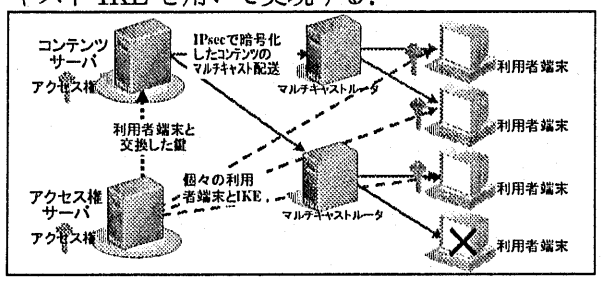

図1：ユニキャスト型アクセス権配送システム

4.2 マルチキャストアクセス権配送方式

システム構成は，アクセス権サーバ，コンテンツサーバ，利用者端末とし(図 2)，利用者端末はあらかじめ公開鍵暗号方式の秘密鍵を保持し，アクセス権サーバはこの公開鍵を持つものとする．アクセス権サーバはそれぞれの利用者端末の公開鍵で暗号化したアクセス権の束をコンテンツサーバに配送する．コンテンツサーバは暗号化されたコンテンツと次回のアクセス権をマルチキャストを用いて利用者端末に配送する．コンテンツサーバは次のアクセス権に切り替える一定時間前に，アクセス権の切替予告通知を複数回コンテンツとともにマルチキャストで配送する．この時点で次回のアクセス権を入手していない利用者端末は，直接コンテンツサーバにアクセス権を要求し取得する．

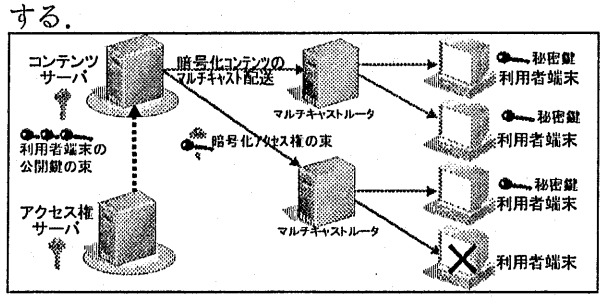

図2：マルチキャスト型アクセス権配送システム

5.おわりに

本稿ではマルチキャスト型ストリームコンテンツ配送におけるアクセス制御を実現する際の問題点を明らかにし，解決する2つの方式を提案した．今後は，評価を行なう予定である．

[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)