動画像ストリームに対するケーパビリティに基づくアクセス制御

松本 広志[1]　　新城 靖[2]　　宮地 力[3]

1. はじめに

動画像に対してアクセス制御を行った上で共有をしたいという要求が高まってきている。たとえば、スポーツのコーチングの分野では、複数の団体が所有している動画に対してアノテーションを行い、動画像ストリームとして共有をしたいという要求がある[1]。この時、各団体が用いているストリーミングサーバが異なることがある。そのような場合であっても、統一的なアクセス制御を行う必要がある。コーチは動画像ストリームに対してアクセス権を持っているが、選手は持っていないことがある。このような場合には、コーチが選手に一時的に動画像ストリームに対するアクセス権を与えることができれば利便性が高まる。

従来のアクセス制御リスト（Access Control List: ACL）を用いる場合、新たなユーザにアクセス権を与えるためにはいちいち ACL を書き換える必要がある。ACL にユーザのグループを設定する方法も考えられるが、この場合はグループに新たなユーザを登録する必要がある。いずれの場合も ACL の維持コストやユーザ管理のコストが高くなってしまう。

本研究ではケーパビリティに基づくアクセス制御を実現することでこれらの問題を解決する。ケーパビリティとは、オブジェクトへの操作を行う権利を含む参照である。ケーパビリティの重要な性質として、他人に渡すことが可能であるということがあげられる。あるユーザがあるオブジェクトにアクセスできるケーパビリティを持っていたとき、そのケーパビリティを他のユーザに渡すと、受け取ったユーザもまた同様にそのオブジェクトにアクセスできるようになる。この性質を利用することで、ACL をいちいち書き換えることや、ユーザのグループに新たなユーザを登録することなく、新たなユーザにアクセス権を与えることができる。これにより、ACL の維持コストもユーザ管理のコストも抑えたアクセス制御を行うことが可能になる。

独自のアクセス制御を導入する場合、配信サーバのソースコードが公開されていないときには配信サーバ本体を書き換えることができない。この問題に対して本研究では、動画像ストリームに対するアクセス制御を、プロキシを用いて行うことで解決する。この方法の利点は、ストリーミングサーバを変更することなく、外付けで独自のアクセス制御が追加できることである。また、同じ通信プロトコルを用いる複数のストリーミングサーバに対して、1 つのプログラムで対応することができるという利点もある。

2. ケーパビリティとプロキシの実装

本研究では、動画像ストリーミングに対するケーパビリティに基づくアクセス制御をプロキシとユーザ管理サーバにより実現する。ストリーミングサーバとクライアント間にプロキシを設けて、プロキシだけがストリーミングサーバと通信できるようにする。ユーザ管理サーバは独自のユーザ管理と独自のアクセス制御を集中的に行う。ユーザ管理サーバは、クライアントからの要求に対して、それが認められるものであればケーパビリティを生成して返す。

本研究ではケーパビリティとして以下の情報を暗号化したものを用いる。

- ストリーミングサーバ上のストリームデータの URL
- 有効期限
- 利用回数

1 筑波大学情報学類
College of Information Sciences, University of Tsukuba.
2 筑波大学システム情報工学研究科コンピュータサイエンス専攻
Department of Computer Sciences, University of Tsukuba.
3 国立スポーツ科学センタースポーツ情報研究部
Department of Sports Information, Japan Institute of Sports Sciences

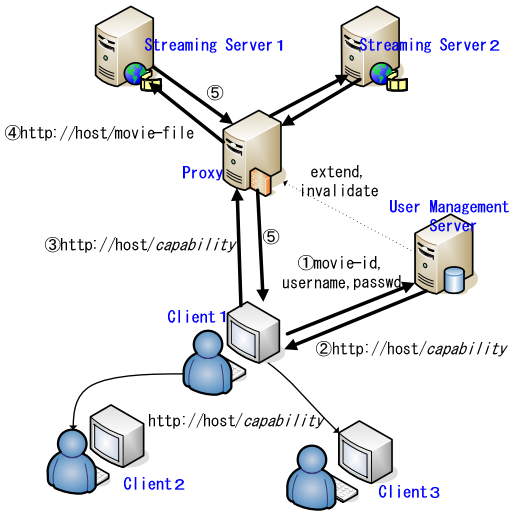

図１ クライアントからストリーミングサーバへのアクセス手順

クライアントがストリーミングサーバにアクセスする手順を以下に示す（図１）。

(1) クライアントはストリームデータに１対１に割り当てられた ID と、ユーザ認証のための情報（たとえばユーザ名とパスワード）をユーザ管理サーバに送る。

(2) ユーザ管理サーバは、独自のユーザ認証と独自のアクセス制御を行う。アクセスが許可された場合はプロキシのホストとケーパビリティを含んだ URL を送り返す。許可されなかった場合はエラーを送り返す。

(3) クライアントは受け取ったケーパビリティを含む URL をプロキシに送る。

(4) クライアントから URL を受け取ったプロキシは、ケーパビリティを復号化してストリーミングサーバ上のストリームデータの URL、有効期限、利用回数といった情報を取り出す。プロキシは有効期限、利用回数をチェックする。それらが有効であった場合、プロキシは、ストリームデータの URL に従ってストリーミングサーバに接続する。

(5) プロキシは、サーバから送られた応答を受け取り、それをそのままクライアントに送る。

ケーパビリティを持っているユーザは、それを他のユーザに渡すことができる。ケーパビリティを渡す方法として、電子メールやインスタントメッセンジャーで送る方法や、Web ページに置く方法がある[2]。

ケーパビリティには有効期限と利用回数を設定する。これにより、ケーパビリティが濫用されるのを防ぐ。また、必要に応じて期限延長や無効化を可能にする。その場合は、クライアントがユーザ管理サーバに要求を送り、ユーザ管理サーバがプロキシに有効期限の延長や無効化の要求を送る。

プロキシの実装にはプログラミング言語 Java を用いている。ストリーミングサーバとしては Windows Media Server のコンポーネントである Windows Media サービス 9 を用いている。各ノード間の通信は HTTP を用いている。

現在、有効期限と利用回数制限を持つケーパビリティの実装を完了し、期限延長と無効化の実装を行っている。

3. おわりに

本研究では動画像ストリームに対するケーパビリティに基づくアクセス制御を実現する。ケーパビリティを用いることにより、ACL の書き換えやグループメンバの登録を行うことなく、新たなユーザに一時的にアクセス権を与えることができるようにする。プロキシを用いることで、ストリーミングサーバを書き換えることなくアクセス制御を可能にする。

現在、ストリーミングサーバは Microsoft 社の Windows Media Server のみを対象としている。今後は Real 社の Real Media Server や Apple 社の Darwin Streaming Server でも使えるようにする。

実装したプロキシは、国立スポーツ科学センター（JISS）の映像データベースプロジェクトで利用される予定になっている[1]。

参 考 文 献

[1] 国立スポーツ科学センター(JISS), 映像 DB 構築プロジェクト, 映像 DB の全体概要 (2005). http://movie-master.ijiss.jp/moviewiki/.

[2] Shinichi Suzuki, Yasushi Shinjo, Toshio Hirotsu, Kazuhiko Kato, and Kozo Itano, “Capability-based Egress Network Access Control for Transferring Access Rights, ”Third International Conference on Information Technology and Applications(ICITA’2005) , No.2, pp.488-495, Sydney, Australia, July 2005.