4.3 動画像配信の認証システムの構築

4.3.1 目的

ネットワークを利用したアプリケーションやサービスは、インターネットの普及とともに急速に発達した。たとえば、暗号化技術やWWWのコンテンツを扱うための技術の向上により、インターネット上には多くのショッピングモールが登場した。また、新聞や雑誌などのメディアもインターネット上で講読できるようになり、バックナンバーを有料で取得できるといったサービスも提供されている。さらに、ADSLやFTTHなどの普及によってオフィスや家庭がインターネットに接続するための加入者線が広帯域化するにつれ、いままで実現できなかった動画像配信も普及してきた。春と夏の高校野球大会は本学が技術協力してインターネット配信されているし、人気アーティストのコンサートも有料配信されるようになっている。韓国などでは地上波で放送されたドラマがインターネット上で有料配信されることが一般的になりつつある。

電子図書館もまた、上記のようなインターネットの普及にともなって発展してきたネットワークサービスのひとつである。初期の電子図書館は、既存の文献を電子媒体によってインターネット経由で提供すること、および、電子化された情報の特徴を活かした強力な情報検索機能を提供することが主眼に置かれていた。しかし、インターネット上で提供されるアプリケーションやサービスが多様化するにつれ、電子図書館も単に既存図書館を電子化するだけではなく、多様なサービスを提供することが求められるようになった。今では静止画や動画、音声といったさまざまなデジタルコンテンツを配信するような、いわば情報館としての役割を果たすことが一般的となりつつある。

本学の電子図書館はこのような流れに先んじて、さまざまなマルチメディアコンテンツをネットワーク経由で提供している。このようなコンテンツのなかには、利用許諾などの条件により閲覧できる利用者が制限されているものがある。また、一般に提供されているサービスの中にも、前述のような有料のものや会員登録制のものなど、ある意味で利用者を制限するものが多い。このようなサービスを享受するためには、本人確認やアクセスの正当性を確認するために認証が必須となる。HTTPを利用してコンテンツをダウンロードするものの場合、サービスがWWWで閉じているため、HTTPの枠組みで利用されている認証や、WWW ページ上のフォームにユーザ名とパスワードを入力することによって認証するものがほとんどである。

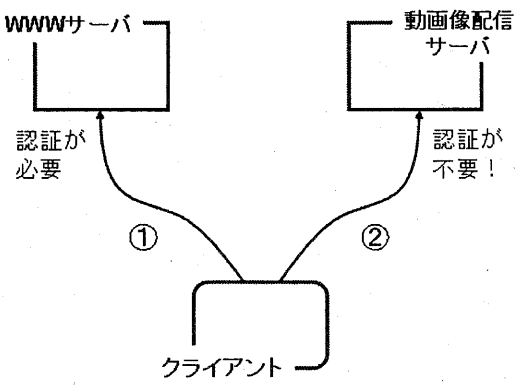

図 1 認証が回避できる場合

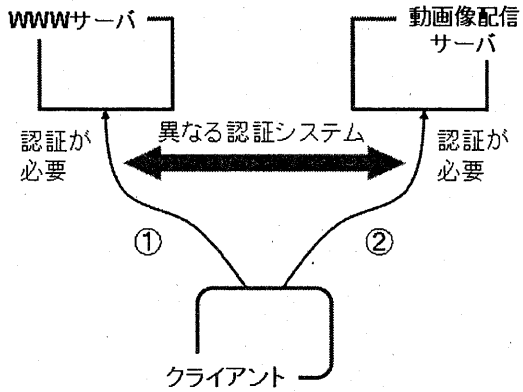

図 2 それぞれで認証が必要な場合

一方、動画像の配信には WWW サーバと異なるサーバを用意し、クライアントからアクセスするためのプロトコルも RTSP などの専用のものを利用することが多い。現在提供されている動画像配信サービスの中には、動画像への URL を取得するためのアクセスのみを制限し、あらかじめ URL がわかっていれば認証を回避できるものも多い（図 1)。また、WWW と動画像配信サービスの認証を分離しているものもある。この場合は WWW 上で動画像配信の URL とともにユーザ名とパスワードが通知される。これらの情報は動画像配信サーバにアクセスした際に入力しなければならず、利用者の手間が増加する（図 2)。

上記の問題を解決するために、本学電子図書館では WWW での認証を配信サーバに引き継ぐためのシステムを構築・運用している。このシステムは、動画像配信サーバに対してアクセスする際にも再認証をおこなうことなくアクセス制限をかけることができる。また、コンテンツごと、および、アクセスもとのネットワークアドレスブロックごとに認証の要・不要を設定することができる。

4.3.2 動画像配信

動画像や音声の配信に関し、IETF (Internet Engineering Task Force)では主に RTP と RTSP というふたつのプロトコルが標準化されている。

RTP (Real-Time Protocol)は動画像を配信するためのプロトコルで、RTP データ転送プロトコルと RTP 制御プロトコル(RTCP; RTP Control Protocol)から構成されている。RTP データ転送プロトコルはシーケンス番号によるパケット廃棄の検出や再生のタイミングを指定するタイムスタンプなどの機能を持つ。一方、RTP 制御プロトコルは、受信品質のフィードバックや動画像と音声の同期処理などを受け持つ。

RTSP（Real-Time Streaming Protocol）は、配信サーバから送信される動画像の再生や停止、巻き戻し、早送りなどを、手元のビデオデッキを操作するか

のように制御するためのプロトコルである。また、プロトコルの仕様は意図的に HTTP 1.1 を拡張したものとなっており、HTTP に対する拡張機能の多くがそのまま利用できる。このため、認証方式として Basic 認証と Digest 認証もサポートすることができる。しかし、HTTP で送信したユーザ名とパスワードを RTSP で再送するための標準的な枠組みはなく、クライアントの実装に大きく依存する。現在、WMT9 を再生できるクライアントは Windows Media Player 9 しかなく、上記のような仕組みは実装されていない。また、RTSP での Basic 認証は、認証情報が平文のままで送信されるために危険がともなう。WWW へのアクセスでは、Basic 認証で送信されるパスワードは HTTPS によって守ることができる。仕様上は RTSP でも SSL/TLS を利用することができるが、いまのところ実装されているものはない。

4.3.3 構築システム

本節では、本学で構築したシステムについて述べる。

4.3.3.1 概要

本学電子図書館の WWW サーバは Sun Microsystems 社の Solaris 上に構築されており、基本的な認証も WWW 上でおこなわれる。また、電子図書館の動画像コンテンツ配信には Microsoft 社の Windows Media Technology 9（以下、WMT9）を採用しており、配信サーバは Windows 2003 Server に付属の Windows Media Service（以下、WMS）を利用している。WMS は RTSP の認証をサポートしているが、認証に利用するデータベースは内部のものしか利用することができない。したがって、WWW 上の認証情報を直接 WMS に引き継ぐことはできない。

そこで、本学では NetCache という機器と RADIUS を利用して認証情報を間接的に引き継ぐシステムを構築・運用している。このシステムでは、動画像配信サーバの URL やコンテンツの中身をあらわすメタデータにクライアントがアクセスする際、そのクライアントに対して動画像に対するアクセスを一時的に許可する。以下では、この仕組みについて説明する。また、RTSP の早送りや巻き戻し、さらには連続したコンテンツ再生に関する問題点とその解決方法についても述べる。なお、システムの設定に関する詳細な情報は、付録に掲載する。

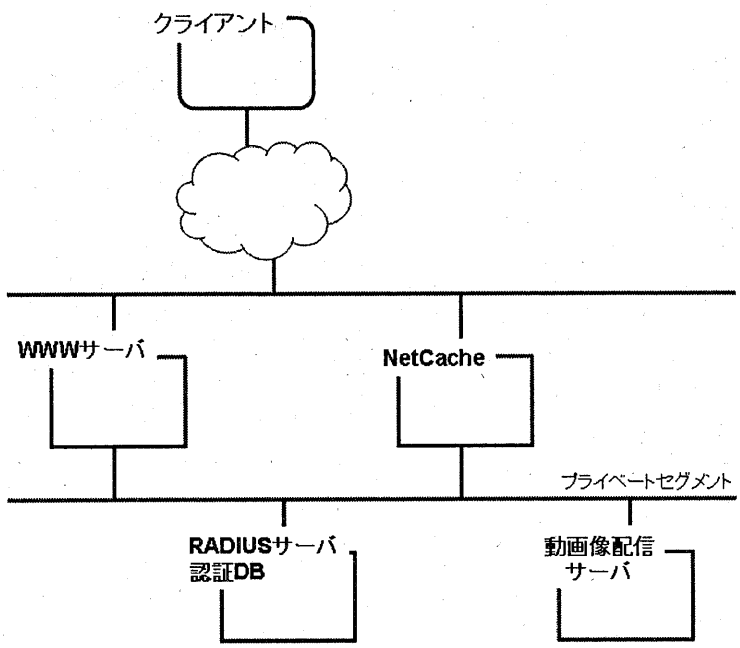

図 3 システムの概要

4.3.3.2 認証情報の引継ぎ

図 3 に本システムの構成図を示す。このシステムでは、Network Appliance 社の NetCache を利用している。この機器は、動画像や WWW などのコンテンツをキャッシュすることでサーバの負荷を軽減するもので、エンドユーザの近くに配置することを意図している。しかし、特に動画像配信においては配信サーバの直近にリバースプロキシとして配置し、ストリーミングアクセラレータのように使われることも多い。また、クライアントからのアクセスを RADIUS によって認証することが可能である。

クライアントは以下の手順で動画像にアクセスできる。

1. クライアントは WWW サーバにアクセスする。このアクセスには認証が必要となる。
2. クライアントが動画像へのリンクを手繰る。
3. リンク先は CGI となっており、RADIUS サーバの認証 DB に対してクライアントの IP アドレスや動画像の配布ポイント、および、認証の有効期限を登録する。有効期限は、クライアントが動画像を受信し始めるまでとし、本学では 20 秒としている。また、同時にこの CGI はクライアントへアナウンスファイル（asx ファイル）を送信する。

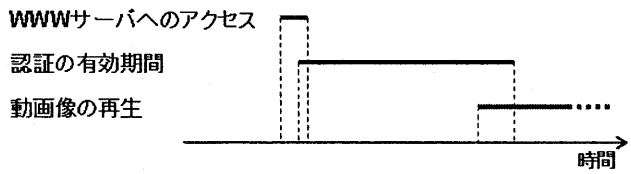

図 4 再生開始時のようす

4. アナウンスファイルを受信した WWW ブラウザは動画像プレイヤを起動する。
5. 動画像プレイヤは再びアナウンスファイルを受信し、その内容にしたがって NetCache へアクセスする。
6. NetCache はクライアントの IP アドレスやアクセス先の配布ポイントなどの情報を RADIUS サーバに送信する。
7. RADIUS サーバは受信した情報と認証 DB の内容から、アクセスの可否を決定して応答する。
8. アクセスが許可された場合は、NetCache が動画像配信サーバへアクセスし、クライアントへコンテンツを配信する。

再生を開始するときのようすを図 4 に示す。

4. 3. 3. 3 再生の中断

利用者は、動画像再生中に早送りや巻き戻しなどをおこなうことがある。この場合、配信はいったん中断され、指定された条件であたらしく再生を開始する。また、WMT のアナウンスファイルを利用すると複数のコンテンツを連続して再生することができるが、この場合もコンテンツの切り替え時に再生の停止が発生する。前節の手法で WWW サーバから認証を引き継いだ場合、動画像配信サーバとのセッションの開始には有効期限がある。したがって、早送りや巻き戻し、あるいはコンテンツの連続再生などで再生が停止すると、再びセッションの開始を試みたとしても、認証に失敗することになる。

本システムでは、上記の問題に対応するため、再生停止から一定時間内の再生開始を許可している。NetCache には、課金を目的としたセッションの監視機能があり、再生の開始や停止などの情報を取得することができる。これを利用して再生の停止を検出し、認証 DB へ認証情報を再登録する。有効期限内であれば再びセッションを開始できる。

4.3.4 今後の課題

本システムで利用している認証にはクライアントのIPアドレスを利用しているため、厳密な意味で認証できているわけではない。たとえば、WWW サーバにアクセスして認証 DB への登録が終了した時点で、すばやく他のクライアントにIPアドレスを付け替えることにより、そのクライアントで動画像へアクセスすることができる。しかし、認証情報の有効期限を適切に設定することで、ある程度の問題を回避することができる。逆に、有効期限を短くすると、ネットワーク距離が遠いクライアントが期限内にアクセスできない事象が発生する。したがって、クライアントの分布によって適切な有効期限を決定しなければならない。本学ではほとんどのクライアントが学内であることを勘案し、前述のように有効期間を20秒としている。

また、IP アドレスによってクライアントを識別するため、通信路上にアドレスを変換する媒体が存在している場合には、期待通りの動作をしない。たとえば、NAT を介して通信するクライアントの場合、同一のグローバルアドレスに変換されるクライアント群はすべて単一のクライアントとして認識されてしまう。また、WWW ブラウザがプロキシサーバを経由するように設定されている場合、認証 DB に登録されるIPアドレスはプロキシサーバのものとなる。そのため、動画像プレイヤのプロキシ設定がブラウザのものと異なる場合は、本システムでは認証を引き継ぐことができない。

このような問題を解決するためには、アナウンスファイルを取得する際に一時的な ID を発行し、動画像にアクセスする際にその ID を指定する方法がある。今後はこの方式を利用した場合の、再生の中断への対応を検討する。

参考文献

RTP: A Transport Protocol for Real-Time Applications, RFC3550
Real Time Streaming Protocol (RTSP), RFC2326
NetCache, http://www.netapp.com/products/netcache/netcache_family.html
Windows Media Technology, http://www.microsoft.com/windows/windowsmedia/default.aspx

付録

A　利用環境

本学で利用している環境は以下のとおり。

- WWW サーバ：Apache 2
- RADIUS サーバ：GNU Radius 1.1
- 認証データベース：PostgreSQL 7.4

WWW サーバでは CGI を利用し、アナウンスファイルへのアクセスに対して認証 DB へ必要な情報を登録する。

B　認証 DB の設定

認証 DB では、ふたつのテーブルを利用している。radius_auth は WWW サーバが認証情報を登録するために利用する。

- distpoint character varying(80) NOT NULL（動画像の配布ポイント）
- clid inet NOT NULL（クライアントの IP アドレス）
- expire bigint NOT NULL（有効期限、1970/1/1 からの秒数）

また、本システムでは radius_acl というテーブルも併用している。これはアドレスブロックと配布ポイントの組で認証を必要としないものを登録する。

- distpoint character varying(80) NOT NULL（動画像の配布ポイント）
- allowfrom cidr NOT NULL（認証なしでアクセスを許可するアドレス）

C RADIUS サーバの設定

C. 1 NetCache 用辞書

NetCache 用辞書を以下のとおり用意する。

```
VENDOR  Netapp          789
ATTRIBUTE       Vendor-Netapp-1         1       string  Netapp
ATTRIBUTE       Vendor-Netapp-2         2       integer Netapp
VALUE           Vendor-Netapp-2         IP-Authentication       1
VALUE           Vendor-Netapp-2         User-Authentication     2
ATTRIBUTE       Vendor-Netapp-3         3       integer   Netapp
VALUE           Vendor-Netapp-3         Authentication-Failed   1
VALUE           Vendor-Netapp-3         Authorization-Failed    2
VALUE           Vendor-Netapp-3         Other                   3
ATTRIBUTE       Vendor-Netapp-4         4       string  Netapp
ATTRIBUTE       Vendor-Netapp-5         5       string  Netapp
```

C.2 RADIUS ユーザファイル

NetCache からの問い合わせに対して SQL を参照するために、以下のような

```
NetCache Auth-Type = SQL
        User-Name = NetCache,
        Class = 0x414243
```

users ファイルを用意する。

C.3 SQL 参照設定

SQL を参照して問い合わせに返答するために、sqlserver ファイルを用意する。特に、データベースに問い合わせる部分は以下のとおり。

```
doauth yes
auth_db wms

auth_query  SELECT 'PASSWORD' as password ¥
            FROM radius_auth auth FULL JOIN radius_acl acl ¥
            USING (distpoint) ¥
            WHERE ¥
                ( auth.distpoint = '%C{Vendor-Netapp-1}' ¥
                  AND auth.clid = '%C{Calling-Station-Id}' ¥
                  AND auth.expire > EXTRACT(EPOCH FROM TIMESTAMP 'now') ) ¥
              OR ¥
                ( acl.distpoint = '%C{Vendor-Netapp-1}' ¥
                  AND acl.allowfrom >>= '%C{Calling-Station-Id}' ) ¥
            LIMIT 1
```

また、PASSWORD の部分は D.で設定したパスワードを GNU RADIUS が利用している方式で暗号化したものにする。

D NetCache の設定

動画像へのアクセスに対し、RADIUS へ問い合わせるように設定する。この際、Send URL/Use IP Authentication Protocol を有効にする。

E 認証登録 CGI

認証登録用 CGI ファイルは、アナウンスファイルを生成してクライアントに送信するとともに、認証 DB の radius_auth テーブルにエントリを追加する。