鍵配送によるセキュアなダウンロード型映像再生手法の検討

6G－1

楢原佳織　大森信行　稲垣博人
日本電信電話株式会社　NTTサイバーソリューション研究所
{kaori, ohmori, inagaki}@aether.hil.ntt.co.jp

1. はじめに

近年インターネット常時接続サービスの拡大化、高速化が進み、ストリームで映像を配信するサービスが急増している。しかし、インターネットはベストエフォート型で帯域が保証されないためストリーム配信を行うと、再生の中断や遅延といったの問題が発生する。ストリーム配信の欠点を回避する方法として、コンテンツをあらかじめ再生端末にダウンロードする手法が用いられる。ダウンロードの場合、コンテンツの不正なコピーや利用を防ぎ、特定のユーザのみにコンテンツの再生を許可する仕組みが必要になる。

我々は、このようなダウンロードのためのポータルと端末およびそれらのプロトコルを提唱している。ダウンロードのための端末では、擬似的なプッシュ型データ転送（スマートプル）を実現するテレポーリングプロトコル（TPP）[1]、各種メッセージングを行うコンテンツ・ダウンロード・プロトコル セット（CDPS）を実装可能とする。

本手法では、特に、ダウンロードするコンテンツをセキュアに再生するダウンロード型映像再生手法を提案する。本手法では、事前に暗号化された映像等のコンテンツをクライアント側の端末に蓄積しておき、クライアント側からコンテンツ視聴の要求がある都度、暗号を解く鍵を配信し、クライアント側でコンテンツを復号化する。

A Proposal of secure contents rendering method using On-Demand de-ciphering
Kaori Narahara, Nobuyuki Ohmori, Hirohito Inagaki
NTT Cyber Solutions Laboratories, NTT Corporation
1-1 Hikarinooka Yokosuka-shi Kanagawa 239-0847 Japan

2. システム概要

2.1. 構成

本システムを構成するのは、A.映像を再生するクライアント端末、B.復号化のためのキーを配信するキーサーバー、C.ビデオを暗号化するコンテンツ作成端末、D.ユーザの利用状況を管理する管理端末である。以下に各機能の詳細を説明する。

A. クライアント端末

クライアント端末は、メディアプレイヤー（例えばWindows Media Playerなど）、リアルタイムビデオストリームアンロッカー（鍵がかかったビデオストリームのアンロック；復号化をリアルタイムで行う。以下、ビデオアンロッカーと呼ぶ）からなる。

B. キーサーバー

キーサーバーは、クライアント端末のビデオアンロッカーからの要求に従いキーを配信する。Web サーバーは、受け取った要求に該当する復号鍵をデータベースから取り出し、鍵を要求したクライアント端末に配信する。データベースには、復号鍵やユーザの利用状況が保存されている。

C. コンテンツ作成端末

エンコーダー（例えば、Windows Media Encoder）によりビデオデータを圧縮し、ビデオファイルロッカーにより配信するビデオファイルのコンテンツを暗号鍵より暗号化し、鍵がかかったビデオファイルを作成する。暗号化は、時間単位毎（例えば1分毎）に行う。

2.2. 処理手順

ここで図1より処理の流れを説明する。

①コンテンツ作成

ビデオデータをエンコーダーにより圧縮する。これを原ビデオファイルと呼ぶことにする。ビデオファイルロッカーにより原ビデオファイルを暗号化し、鍵のかかったビデオファイル（これを鍵ビデオファイルと呼ぶことにする）を作成する。クライアント端末は、再生する鍵ビデオファイルに対応した復号鍵を持つキーサーバーに鍵を要求する必要がある。鍵を要求するキーサーバーは、鍵ビデオファイルで指定されている。

②コンテンツの配信

鍵ビデオファイルは、ダウンロード配信機能により、クライアントに配信される。大容量メディアであれば、予め配布することも可能である。

③再生

ユーザが、視聴したいビデオを選択するとビデオプレイヤーが起動される。この際、ユーザはあらかじめ、ビデオアンロッカーを立ち上げておく。ビデオアンロッカーは、キーサーバーへアクセスし、最初のキーを取得する。次にビデオアンロッカーはビデオプレイヤーを立ち上げ、アンロックされたビデオストリームをビデオプレイヤーに供給する。ビデオアンロッカーはキーサーバーから鍵の配信を連続的に受け、逐次アンロック（復号化）する。この際に、キーサーバーはユーザ、タイトル毎に払い出したキーに対応する時間を記録する。クライアントは、これと同時に、キーを順次ファイルに保管する。再度視聴するときは、キーサーバーへアクセスせずに、このファイルから鍵を取り出しつつ再生を行う。

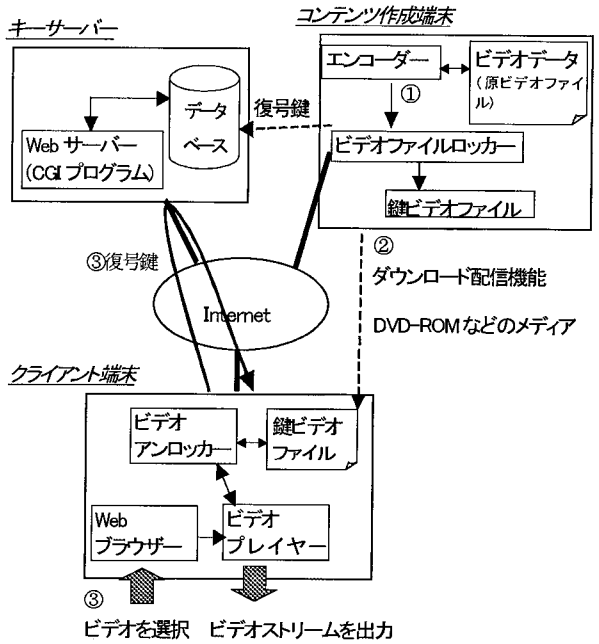

図1 システム構成

3. まとめ

ダウンロードにより、ユーザが求めるコンテンツをセキュアに再生する手法を提案した。本手法の特徴として、暗号化されたコンテンツをあらかじめクライアント端末にダウンロードしておき、鍵のみをインターネット経由で配信する。これにより、ダウンロードしたコンテンツの不正な利用を防ぎつつ、高品質な映像の再生が可能となる。今後はシステムのインプリメントと実験システムで評価を行う。

参考文献

[1] 岸田 他,"インターネット・アクセス・トラヒック制御技術 TellePolling－システム構築のためのアプリケーション・インタフェース－",第 58 回情処全国大会,3P-4,1999