6X-7

ディザスタリカバリ技術を活用した リアルタイム秘密動画転送システムの検討

高野 広之† 遠藤 祐輔† 鈴木 秀一† 上野 洋一郎† 宮保 憲治†

† 東京電機大学大学院 情報環境学研究科

1 はじめに

近年，ネットワークインフラの広帯域化や端末の高性能化に伴い，インターネット上での動画配信サービスの利用が増加している．その影響を受け，動画コンテンツの不正ダウンロードや違法コピー，盗聴に対するセキュリティ面での課題も認識されつつある．本稿では，クラウドコンピューティング技術とインターネット接続された PC，携帯端末等を高速ストリーム暗号により融合して，安全かつ低コストで重要データを配送するための DRT（Disaster Recovery Technology）の応用技術を秘密動画配信に適用した場合の評価結果を述べる．

2 実験システム概要

本実験システムでは IP カメラ(AXIS-M1033)より毎秒 30 枚の画像データ(JPG) と音声データ(μ-law)を取得し，学内に配備した DRT エンジンを使用してフレーム毎にストリーム暗号処理・一体化処理・分割・複製処理を行った．ストリーム暗号処理では 512bit の乱数を暗号鍵とした排他的論理和演算を行う．また，30 フレーム毎に暗号鍵の更新を行い，SSL-VPN を経由して再生端末に暗号鍵を転送する．一体化処理による攪拌回数はデータの攪拌処理に十分な回数として 6 回を採用した．再暗号化に用いる暗号は 512bit の乱数を暗号鍵とした排他的論理和演算を行う．動画像の断片データは 2 つの経路に分散し，中継サーバ 2～6 台を介して再生端末まで UDP を用いて伝送する．中継サーバⅠ～Ⅵはそれぞれ，クラウドサービス「さくらのクラウド」，「GMO クラウド」を用いて北海道と東京に仮想サーバを立ち上げ，中継サーバとして活用した．断片データの経路選択はシャッフリング後に，中継サーバに対して均等に分散するように設定した．中継サーバの仕様を表 1 に，音声データと画像データのフォーマットを表 2 に，DRT エンジンの処理フローを図 1 に，実験システムの構成を図 2 に示す．

表 1. 中継サーバ仕様

	CPU/MEM	場所
Ⅰ	1 コア/1GB	北海道
Ⅱ	1 コア/512MB	東京
Ⅲ	1 コア/1GB	北海道
Ⅳ	1 コア/512MB	東京
Ⅴ	1 コア/1GB	北海道
Ⅵ	1 コア/512MB	東京

表 2. 音声データ，画像データのフォーマット

	フォーマット	ビットレート
音声	μ-law	64 kbps
画像	JPG(640×480 画素)	約 1200 kbps

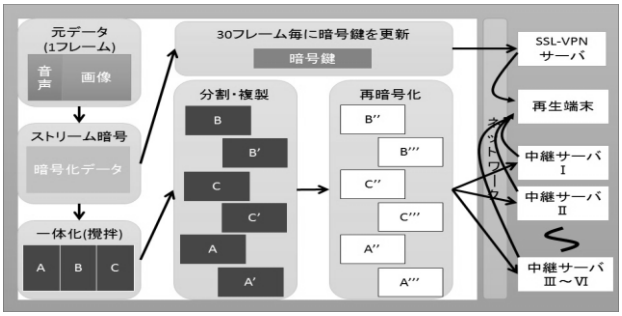

図 1. DRT エンジンの処理フロー

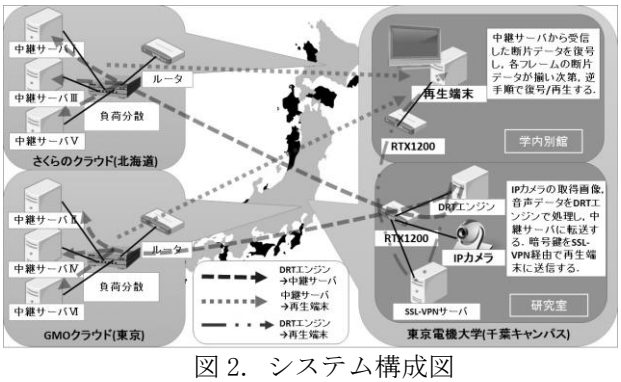

図 2. システム構成図

3 実験内容

図 2 に示す実験システムにおいて，再生端末側で 5 分間リアルタイム再生及び録画保存した時の動画像品質の評価結果を以下に述べる．

本実験では伝送路の帯域リソース等は十分確

Study on real-time secure video transmission system by making use of Disaster Recovery Technology.
Hiroyuki TAKANO† Yusuke ENDO†
Shuichi SUZUKI† Yoichiro UENO† Noriharu MIYAHO†
†Graduate School of Information Environment, Tokyo Denki University
13jkm19@ms.dendai.ac.jp

保されていることを想定した．断片データの複製数は 2 に設定し，断片データの分割数，中継経路数，中継サーバの負荷分散数をパラメータとした動画像のフレームレートと遅延時間への影響を評価した.中継経路数 1 の場合には「さくらのクラウド」を立ち上げて中継サーバとして活用した．ここで，遅延時間の定義は DRT エンジンでの処理開始から，再生端末での復号処理終了までの時間である．表 3 に実験パラメータを示す.

表 3. 実験パラメータ

分割数	複製数	中継経路数	負荷分散数
20～40	2	1～2	1～3

4 実験結果と考察

分割数と負荷分散数をパラメータとした，中継経路数 1 の場合のフレームレートへの影響を図 3 に示す．図 3 において，分割数 20 から 30 まではフレームレートは低い傾向を示すが，分割数が 35 になった段階で急激に増加する．この理由は，分割数 20 から 30 までは断片データをパケット化した際のサイズがイーサネットの MTU サイズである 1500byte を越えるので，ネットワークでフラグメンテーションが発生するためである．分割数が 35 では，断片データをパケット化した時のサイズは 1500byte を越えなくなるため，ネットワークでのフラグメンテーションは発生しない．すなわち，分割数が 20 から 30 までは，分割数 35 の場合よりも送出パケット数が多くなり，ネットワークでの処理工程が増えることが裏付けられる.

上述したフレームレートへの影響の結果から，実験システムの動画像品質では分割数の適用領域は 35 付近と判断できるため，分割数のパラメータを 30 から 40 の範囲に設定し，遅延時間の測定を行った．中継経路数 1 の場合の測定結果を図 4 に，中継経路数 2 の場合の測定結果を図 5 に示す．図 4 において，分割数が 30 から 35 では遅延時間が減少する傾向にあり，分割数が 35 から 40 では遅延時間が増加する傾向にある．分割数 30 から 35 では，上述したネットワークでのフラグメンテーションが 分割数 35 から発生しなくなるために，遅延時間が減少する．分割数 35 から 40 に関しては，単純に送出パケット数が多くなったことにより，遅延時間が僅かに増加する結果になった．この傾向は図 5 においても同様である.

遅延時間の観点から見て最適な分割数である 35 では，中継経路数が 1 の場合でも 2 の場合でも，遅延時間は約 50ms となっており，IP 電話において固定電話並の品質とされるクラス A でのエンドエンド遅延が 100ms 以内であることから，遅延時間の面では音声通話において十分適用可能なシステムであると確認できる.

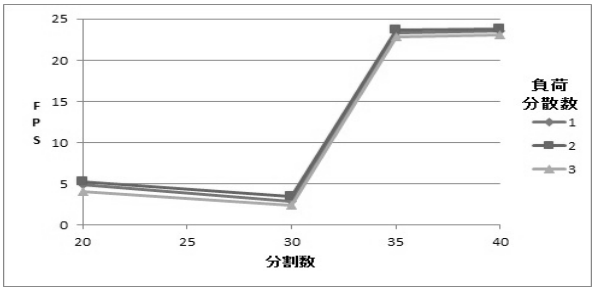

図 3. 中継経路数 1 の場合のフレームレート

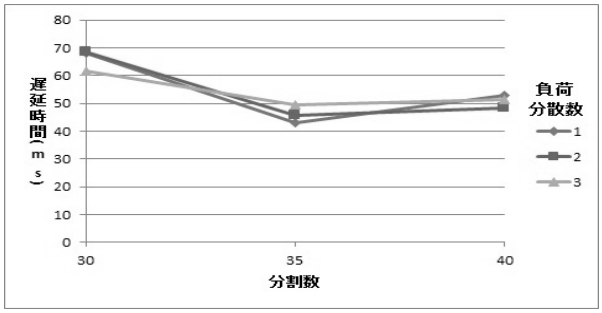

図 4. 中継経路数 1 の場合の遅延時間

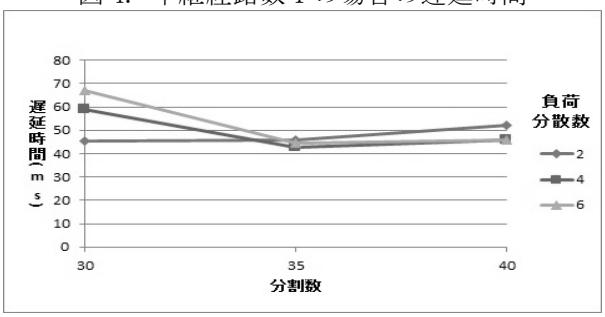

図 5. 中継経路数 2 の場合の遅延時間

5 むすび

DRT 技術を適用することにより，セキュアな秘密動画像配信を実現できる可能性を示した.

今後は，通信帯域を圧縮するための動画圧縮コーデックへの適用，遅延や輻輳の少ない経路を選択するためのアルゴリズムの実装，ユーザの要求する画像品質を満足できるための指標について検討を進める予定である.

参考文献

[1]N.Miyaho, Y.Ueno, S.Suzuki, K.Mori, K.Ichihara, "Study of a Secure Backup Network Mechanism for Disaster Recovery and Practical Network Applications" IARIA Journals, vol. 3, no.1 &2, pp. 266-278, 2010.
[2] Y.Ueno, N.Miyaho, S.Suzuki, .K.Ichihara, "Performance Evaluation of a Disaster Recovery System and Practical Network", IARIA Journals, vol 4 no 1 & 2,pp.130-137, 2011.
[3]特許第 4296304 号（登録）,特願 2006-088020, "ディザスタリカバリ装置及びディザスタリカバリプログラム及びその記録媒体及びディザスタリカバリシステム"
[4]特許第 4385111 号（登録）,特願 2008-262704 "セキュリティレベル制御ネットワークシステム"
[5]特許 4538585 号（登録）特願 2008-209152 "ネットワークシステム"