6X-5

# ディザスタリカバリ技術を活用したロバスト秘密動画転送システムの検討

遠藤 祐輔† 高野 広之† 上野 洋一郎† 鈴木 秀一† 宮保 憲治†
† 東京電機大学大学院 情報環境学研究科 情報環境学専攻

## 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転送するための DRT（Disaster Recovery Technology）の応用技術を述べる．

## 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，SSL-VPN で使用する暗号アルゴリズムを表 3 に，DRT エンジンの処理フローを図 3 に，実験システムの構成を図 4 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 (kbps) |
|---|---|---|
| 音声 | μ-law | 64 |
| 画像 | JPG(640×480 画素) | 約 1200 |

表 3. SSL-VPN で使用する暗号アルゴリズム

| | アルゴリズム |
|---|---|
| 公開鍵 | RSA |
| 共有鍵 | AES-128-CBC |

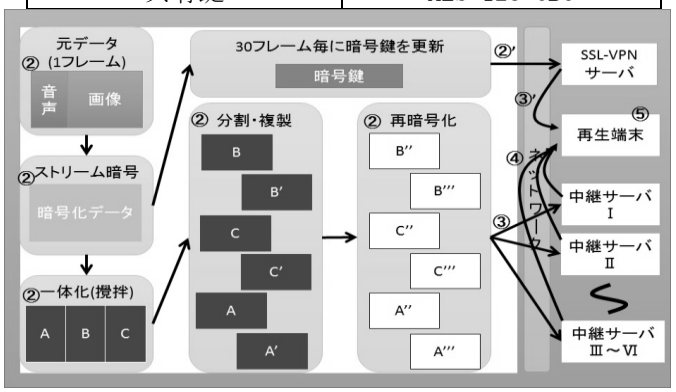


図 3. DRT エンジンの処理フロー

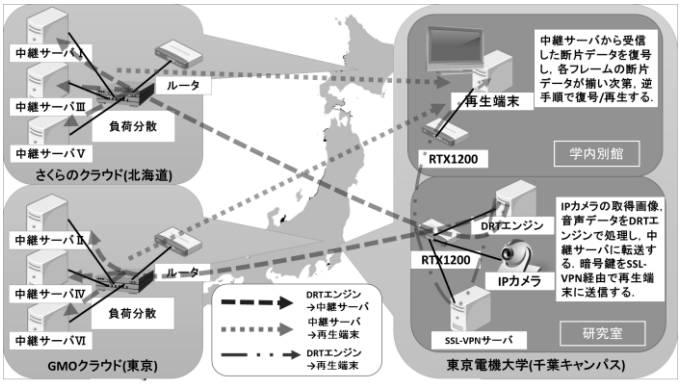


図 4．実験システム構成図

## 3．実験内容

図 4 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．

ファイル一体化処理を行った場合には，少なくとも分割後に複製された断片データの中の任意の 1

---

「Study on secret moving video distribution system by making use of Disaster Recovery Technology」
Yusuke ENDO† Hiroyuki TAKANO†
Yoichiro UENO† Shuichi SUZUKI†
Noriharu MIYAHO†
†Graduate School of Information Environment, Tokyo Denki University

つが回収する必要がある．実用上問題ない再生機能が必要な場合には複製数を十分にとる必要がある．一般に，複製数を増やすとファイルサイズが大きくなるため，遅延時間への影響を考慮して複製数を決定する必要がある．

本実験では伝送路の帯域リソース等は十分確保されていることを想定した．中継路数を増やすことでロバスト性が期待できる．断片データの分割数は断片データサイズが MTU(1500byte)以下となる 40 に設定し，断片データの複製数，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復元率への影響を評価した．中継経路数１では「さくらのクラウド」を用いて中継サーバを構築した．ここで，復元率の定義は送信したフレームに対して，復元できたフレームの割合である．表 4 に実験パラメータを示す．

表 4. 実験パラメータ

| 分割数 | 複製数 | 中継経路数 | 負荷分散数 |
|---|---|---|---|
| 40 | 1～3 | 1～2 | 1～3 |

## ４．実験結果と考察

複製数と負荷分散数をパラメータとした，中継経路数１の場合の復元率への影響を図 5 に示す．図 5 において，複製数１では復元率が 65%～78%と極端に低い値となる．この理由は，複製を行わない場合,1 パケットのロスや遅延が影響するためである．複製数が 2 の場合は復元率が 90%以上，複製数 3 では 98%以上となり，複製の効果があることがわかる．また，負荷分散数 2 では 1 の場合と比べすべての複製数で復元率が高くなった．負荷分散数 3 で復元率が低い理由は，中継サーバが行う処理が断片データの転送処理のみであり，各中継サーバの性能に余裕があったため，負荷分散による効能よりもロードバランシング処理が複雑化してしまう影響が大きいためだと考えられる．

中継路数２の場合の復元率への影響を図 6 に示す．図 6 において中継路数 1 の場合と比べると，複製数による復元率の差が小さいことがわかる．この理由は中継路数 2 の場合は立地的に近い GMO クラウドを併用しているため，パケットロス率が低いためと考えられる．負荷分散数についても中継路数１の場合と同様の事が言える．負荷分散数 2 と 4 の差が少ない理由は，さくらと GMO それぞれ 2 台ずつのため，中継路数 1 の場合の負荷分散数２と同様の処理となるためである．しかし，複製数３としたときも復元率は 91%程度となった．この理由は，遅延時間や処理性能の異なるクラウドを併用しているためであると考えられ，バッファ等の考慮が必要である．中継路数が１の場合では複製数 2，中継路数 2 の場合でも複製数 3 で 90%以上の復元率となり数フレームの損失となっており，十分適用可能なシステムであると確認できる．

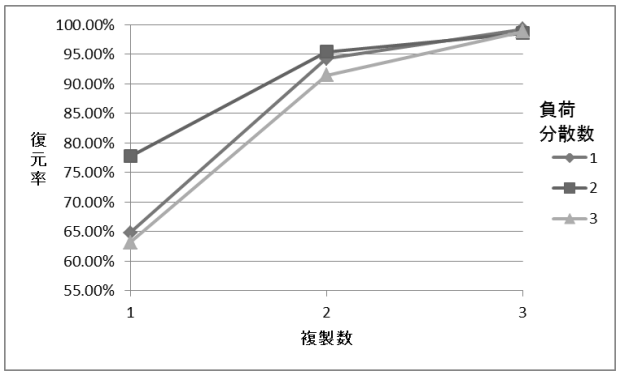


図 5．さくらのクラウドを用いた場合の，複製数と負荷分散数による復元率への影響

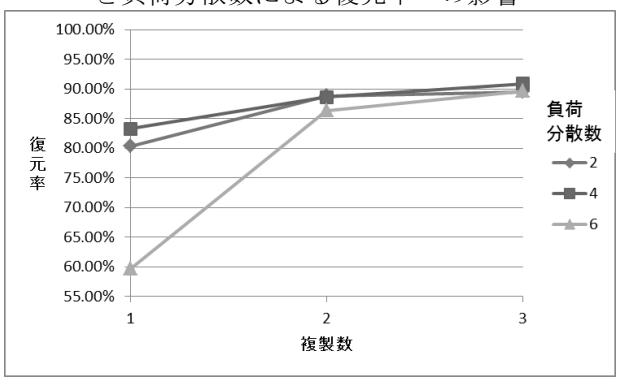


図 6. 中継経路数２の場合の，分割数と負荷分散数による復元率への影響

## ７．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．複製数を上げることで，復元率を高めることができ，複製数を 2 以上とれば必要十分な再生能力が確保できた．

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",