秘密分散バックアップにおける災害医療情報の高速な変更検知および更新手法

明珍　侑樹　【 ネットワーク信号処理研究室 】

1　はじめに

医療情報を遠隔地に安全に保全し，広域災害時に活用する手段として秘密分散法 [1] は有効とされる．しかし従来の手法では一部のデータ更新でも全分散データの再送が必要となり，狭帯域環境において通信遅延が致命的となる．先行研究 [2] では HL7 メッセージをセグメント単位で部分更新する手法が提案されたが，データ本体の修正に伴うヘッダ情報の連動更新により，依然として数 KB 規模の再送が発生していた．本研究では，HL7 の構造的制約に依存せず，バイト単位の差分検知・更新を行うことで構造的オーバーヘッドを排除し，秘密分散するデータ量を極小化するバイトストリーム差分更新を提案する．

2　提案手法とシステム構成

本提案システムは被災地のクライアント端末と複数の分散ストレージ群から構成される．データ更新時，クライアント端末内で前回送信したキャッシュデータと最新データとの差分パッチを IETF RFC 3284 (VCDIFF) に基づき抽出する．この差分パッチに, 検索タグ等のシステム管理情報を含む固定ヘッダを付与して秘密分散処理を施し, 分散ストレージ群へ追記形式で送信する．これにより，クラウドストレージを単なるファイル保管場所として扱えるため，特定のサーバ機能に依存せず，災害時の可用性が向上する．

3　理論解析および性能評価

本手法の有効性を評価するため，1 か所あたりの平均更新サイズを x，更新箇所数を N，分散数を $n = 5$，システム固定ヘッダを $H = 128$ Byte としてコスト関数を定義した．全体サイズ S, VCDIFF 命令ヘッダを 5 Byte とした場合従来手法のコスト C_{full}, 提案手法（差分追記）の通信コスト C_{inc} および削減率 R は次式で近似される．

$$C_{full} = (S + 128) \times 5 \tag{1}$$

$$C_{inc} = \left\{ \sum_{i=1}^{N} (5 + x_i) + H \right\} \times n \approx \{N \times (5+x) + 128\} \times 5 \tag{2}$$

$$R = \frac{C_{inc}}{C_{full}} \approx \frac{(x+5)N + 128}{(S + 128)} \tag{3}$$

以上を比較すると元データ S が大きく更新箇所 N が局所的でかつ単一箇所の更新サイズ x が小さいほど，提案手法の削減効率が最大化ことが読み取れる．

ここで, 標準的な HL7 メッセージ（$S = 3{,}000$ Byte, $C_{full} = 15{,}640$ Byte）を対象に，単一箇所の更新データサイズ x に対する通信削減率および提案手法が従来手法や先行研究手法より優位である限界の損益分岐点を算出した結果を表 1 に示す．

表 1　通信削減率と損益分岐点 ($S = 3{,}000$ B)

更新サイズ x [Byte]	削減率 ($N = 1$)	損益分岐点 (箇所数 N の上限)	
		先行研究	従来手法
16	95.2%	108 箇所	142 箇所
64	93.7%	33 箇所	43 箇所
256	87.6%	8 箇所	11 箇所

表 1 が示す通り，単一箇所更新においては x=16 Byte 時に最大 95.2% の通信量削減を達成し，x=256 Byte の比較的大きな差分であっても更新が 11 箇所以内と局所的であれば，提案手法が最も高い通信削減効果を発揮する．

また，差分処理によるクライアント側の計算負荷増加が懸念されたが，表 2 の通り，差分処理に伴い追加される計算時間を削減される通信時間が上回るため，本提案は妥当であるといえる．

表 2　従来手法と提案手法の遅延比較 ($S = 3{,}000$ B, 1 Mbps)

更新条件		通信 (理論)	計算 (合計)	**総遅延**
サイズ x	箇所 N	[ms]	[ms]	**[ms]**
従来手法 (全量)		120.0	10.8	**130.8**
16 B	10	13.1	34.0	**47.1**
	100	91.2	41.6	**132.8**
64 B	10	32.4	34.8	**67.2**
	100	120.6	44.0	**164.6**
256 B	10	109.2	42.6	**151.8**
	100	121.8	43.8	**165.6**

4　まとめ

本研究では，秘密分散バックアップシステムにおいて，バイトレベルの差分更新手法を提案した．シミュレーション評価により，差分抽出によって増加する計算負荷よりも削減した通信負荷が上回るため, 妥当であることを確認した. 今後は，本提案の計算負荷低減効果を前提としつつも，災害時モバイル端末における省電力化や，実システムを構築し実際のネットワーク環境を介した遅延・削減効果の実証実験が課題である．

参考文献

[1] A. Shamir. How to share a secret. Communications of the ACM. 1979, Vol.22, No.11, p.612-613.

[2] 森岡 弘貴, 福本 昌弘: 災害急性期に医療情報の更新・利用可能な秘密分散バックアップシステム, 高知工科大学 学士学位論文, 2022.