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

1220388　森岡　弘貴　【 ネットワーク信号処理研究室 】

1　はじめに

広域災害に備え医療情報を保全し，被災地での診療に活用することが求められている．医療情報の保全手法として (k,n) しきい値秘密分散法によるバックアップが挙げられる．診療に用いる医療情報は最新のものが望まれることから，医療情報の随時バックアップが必要となる．しかし，災害時は電源やネットワーク等のリソース不足や，傷病者の増加によって作成される医療情報が増加し，この時に随時バックアップを行うとリソースの圧迫が想定される．本研究では災害時の不足しているリソースの圧迫を避け，秘密分散の処理量の削減を目的として，部分更新と最新のシェアの検索を提案する．

2　医療情報の部分更新

本項では，部分更新と最新の医療情報の検索について述べる．

2.1　部分更新を可能とする方法

部分更新の流れを図 1 に示す．提案方法は更新するデータ S を項目ごとに分けたデータを $S_i(i=1,2,3)$,S_i のデータ長を l_i とする．S は式 (1) で表される．

$$S = S_1 \prod_{m=2}^{3} 2^{l_m} + S_2 2^{l_3} + S_3 \tag{1}$$

前回と変更のある部分のデータを S_2 とする．S_2 は更新が必要なため，分散すると，W_2 が得られる．S を復元できるように計算する紐付け情報

$$U = \begin{pmatrix} \prod_{m=2}^{3} 2^{l_m} & 2^{l_3} & 1 \end{pmatrix}^T \tag{2}$$

を作成する．復元する際は，得られたシェア W_2 とストレージにあったシェア W_1, W_3 を集め，U と計算し，復元することによって，

$$S_1 \prod_{m=2}^{3} 2^{l_m} + S_2 2^{l_3} + S_3 = S \tag{3}$$

を復元できる．これを利用して部分更新を行っている．

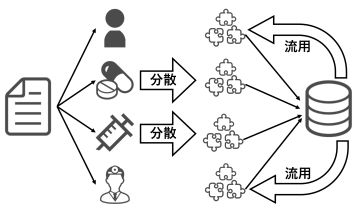

図 1　部分更新の流れ

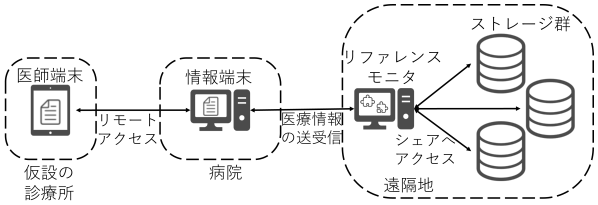

図 2　提案システムの構成

2.2　医療情報の検索

部分更新では前回のシェアが必要となる．秘密分散データを用いた医療情報検索システムを利用して誰のシェアかまで絞った後に，医療情報内の作成日時とデータの種類が記されている項目のみを部分復元し，検索する方法を提案する [1]．従来の方法では，医療情報を全て復元してから検索をしていたが，提案方法は復元するデータ量が削減するため，検索速度が向上する．また，作成日時が分かることで最新のシェアを検索するだけでなく，ある期間に作成された診療録を検索が可能なため，災害時の診療に利用が可能となる．

3　更新・利用可能な秘密分散バックアップシステム

提案システムの構成を図 1 に示す．シェア等を保管するストレージ群と，検索や分散の処理を行うリファレンスモニタ，医療情報を保管する情報端末，医師が手元に持ち診療に用いる医師端末で構成される．これらの端末は不正なアクセスを防止するべく，各端末を登録し，照合があっていた場合のみ通信を行う．各構成デバイス間は個人情報等を通信するが，通信回線に専有線を用いた場合，安全な通信が可能だが，被災し回線が遮断された際に復旧が進むまで通信が不可能なためインターネットを介して通信する．この場合，盗聴の危険性があるが「災害時における要援護者の個人情報提供・共有に関するガイドライン」より，簡易迅速な手続きで情報の提供と共有が行わなければならないことから，個人情報の保護よりも人命救助を優先しインターネットを介した通信を行う．

4　まとめ

本研究では分散するデータ量の削減を目的として，部分更新と最新のシェアの検索方法を提案した．

参考文献

[1] 中村巴，福冨英次，福本昌弘，“ 部分復元可能な秘密分散法におけるシェア間の係数の差の比較による医療データの検索 ”，SCIS2020，3C1-4，2020.