分散データの部分秘匿化復元の検証

1150324　田中麻実　【 福本研究室 】

1　はじめに

高知県では南海トラフ大震災に備え，医療データを県外に分散バックアップし，バックアップした医療データを災害時に利活用する計画が進められている [1]．医療データは個人情報を含むため，バックアップする際には医療データを秘匿する必要がある．しかし，災害時にバックアップデータを用いて診察するためには，医療データが患者本人であるものと判断するために個人情報が必要となる．分散バックアップすることでデータの冗長化ができるが，同時に情報漏えいのリスクが高くなるため，分散バックアップに (k,n) しきい値秘密分散法を用いる [2]．本研究では (k,n) しきい値秘密分散法で分散されたデータを一部秘匿したまま復元できる方法を提案する．

2　データの部分秘匿化復元

(k,n) しきい値秘密分散法はデータを n 個の分散情報 (以降シェアと呼ぶ) に分散し，シェアを k 個以上集めるとデータが復元できる．復元は，完全復元か，復元不可能のどちらかであり，部分復元は困難である．

2.1　部分秘匿化復元の提案手法

(k,n) しきい値秘密分散法で分散したデータを部分秘匿化復元するための構成を図 1 に示す．各 $S_i(i = 1,\ldots,4)$ のデータサイズ l_i とし，図の灰色部分を秘匿するために結合ベクトルを

$$U_2 = \left(\prod_{m=2}^{4} 2^{l_m}, 0 \prod_{m=i+2}^{4} 2^{l_m}, 2^{l_4}, 1\right)^{\mathrm{T}} \qquad (1)$$

とする．分散時には，S_1, S_2, S_3, S_4 それぞれに (k,n) しきい値秘密分散法を用いて，ネットワーク上にある複数のストレージに分散する．復元時にはストレージからシェアの集合 W_1, W_2, W_3, W_4 それぞれからシェアを k 個集め，U_2 を用いてシェアの集合を結合し，復元すると，$S_1 \prod_{m=2}^{4} 2^{l_m} + 0 + S_3 2^{l_4} + S_4 = S'$ となり S_2 部分が秘匿化された S' を得ることができる．

部分秘匿化復元可能かどうかのシミュレーションを行った．3 桁の 10 進数をランダムに選び，10 の位の部分秘匿化復元が可能かを確認する．10 の位の値が 0，それ以外の位の値が復元されていれば部分秘匿復元可能と判断する．シミュレーションの結果，10 の位の値が 0，それ以外の値が復元されていた．よって部分秘匿化復元ができていることがわかった．

2.2　シェアへのアクセス制限

U_i は l_i から作成できるため, ユーザが W にアクセス可能であれば S を復元できる．そのため，シェアに対してアクセス制限をかける必要がある．シェアへのアクセス制限方法を示す．まず，リファレンスモニタのみに W へのアクセス権限を持たせ，シェアを取得する時はリファレンスモニタに問い合わせるようにする．次に，U_i の作成を管理者に限定し管理させる．またあるシェアの集合 W_i を含まないシェア群を $\boldsymbol{G}_i$ を作成する．管理者が作成した U_i と $\boldsymbol{G}_i$ に同じラベルをつけ，U_i'，$\boldsymbol{G}_i'$ と表す．U_i' と $\boldsymbol{G}_i'$ の対応表を作りリファレンスモニタにわたす．管理者はユーザに対して U_i' の配布を行う．この時 U_i' 以外の U_b' をユーザが保持していた場合 U_i' の配布を行わない．リファレンスモニタはユーザの保持している U_i' と対応する $\boldsymbol{G}_i'$ からシェアを集めユーザに渡す．この時ユーザが U_i' 以外の U_i でアクセスしてきた場合 $\boldsymbol{G}_i'$ を渡さない．このアクセス制限により，ユーザが不正に結合ベクトル U_i を作成しアクセスしてきたときはリファレンスモニタが要求を破棄し，ユーザが U_b' を保持した状態で U_i' の取得要求を送ってきたとき管理者が要求を破棄するため，ユーザが管理者の意図しないシェアに対してのアクセスを防ぐことができる．

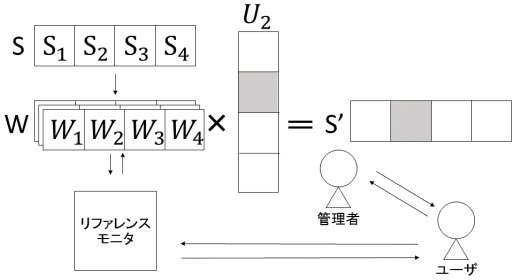

図 1　部分秘匿化復元の構成図

3　まとめ

本研究では (k,n) しきい値秘密分散法で分散されたデータを一部秘匿したまま復元する方法を提案した．提案方法では，ユーザ一人に対してのアクセス制御を想定しているため，ユーザが複数人協力すると S が復元できる．よってアクセス制限の方法を工夫する必要がある．

参考文献

[1] 福本昌弘, “南海トラフ巨大地震に対する医療情報の保全のための高知県での取り組み,”Mercato, 東北情報通信懇談会, Vol.89, pp.18–20, 2014.

[2] A.Shamir, “How to Share a Secret,” Communication of the ACM, Vol.22, No.11, pp.612–613, Nov. 1979.