秘密分散バックアップした医療データの部分復元システムとその安全性評価

1195064　田中麻実　【 ネットワーク信号処理研究室 】

Confined Decoding System for Medical Data Distributed by Secret Sharing Scheme and Its Security Evaluation

1195064　Asami TANAKA　【 Signal Processing and New Generation Network Lab. 】

1　はじめに

医療機関は広域災害に備えて電子カルテを含む医療データを遠隔地にバックアップしている．災害時，DMAT (Disaster Medical Assistance Team) にバックアップした医療データを提供できれば，被災地での医療行為を円滑に行うことができる [1]．医療データは個人情報であるため，患者の診療に不必要な情報の提供を制限しなければならない．そこで秘密分散したデータを部分的に復元するアルゴリズムを提案した [2]．部分復元に必要なデータが第三者に洩れると不正復元される可能性がある．本研究では，部分復元に必要なデータの入手を制限した部分復元可能な秘密分散システムを提案し，提案システムで不正復元される問題点を整理し，不正復元を防ぐ要件を定義する．

2　部分復元可能な秘密分散システム

データの分散バックアップの手法 1 つにデータの秘匿化・冗長化を図る秘密分散法がある [3]．しかし，秘密分散法はデータを部分的に復元することはできない．本節では，部分復元アルゴリズムを用いた部分復元可能な秘密分散システムについて述べる．

2.1　部分復元可能な秘密分散システムの構成

部分復元可能な秘密分散システムの構成について述べる．システムの構成を図 1 に示す．

秘密分散するデータを S，S を項目ごとに分けたデータを $S_d(d=1,2,3)$，S_d のデータ長を l_d とする．復元したいデータを

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

とする．秘密分散アルゴリズムはまず S を

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

となるように分ける (分割)．S_d から秘密分散法を用いてシェア $W_d = \{w_{d1}, w_{d2}, \cdots, w_{dn}\}$ を生成する．S' の

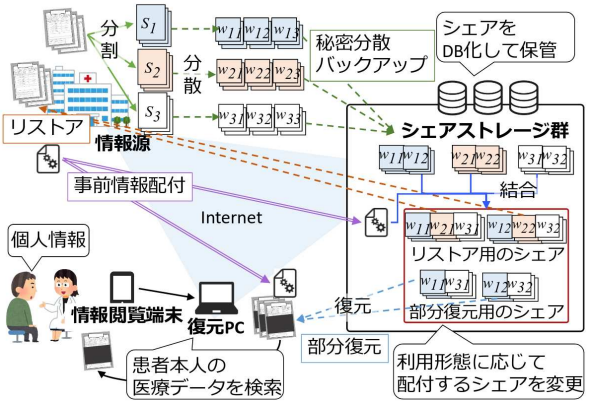

図 1　部分復元可能な秘密分散システムの構成

シェアとなるように計算する紐付け情報

$$U_2 = \begin{pmatrix} \prod_{m=2}^{3} 2^{l_m} & 1 \end{pmatrix}^{\mathrm{T}} \tag{3}$$

を作成する．復元する際は復元したい項目のシェア $\boldsymbol{W}_c = \{W_1, W_3\}$ を集め U_2 と計算し (結合) 復元することによって

$$S_1 \prod_{m=2}^{3} 2^{l_m} + S_3 = S' \tag{4}$$

となり S' を復元することができる．第三者に紐付け情報とシェアを入手されると不正に復元される．そこで情報源の病院は，紐付け情報とシェアの入手を制限するために部分復元の制御データを作成する．

結合したシェアを配付するため，第三者が紐付け情報を入手したとしても結合済みシェアを操作できない．またシェアを入手するためには情報源が作成した制御データが必要となる．よって，データの不正復元を防ぐことができる．

2.2　部分復元可能な秘密分散システムのデータの流れ

提案システムにおける部分復元の手順を述べる．システムの分散から復元までのデータの流れを図 2，図 3 に示す． 情報源は事前情報を配付し，医療データを秘密分散バックアップする．復元 PC はシェアストレージ

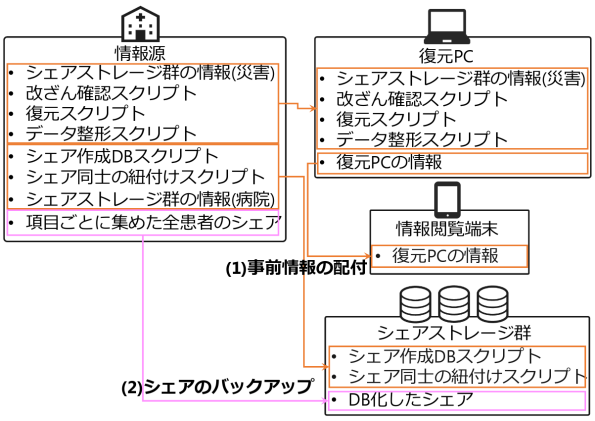

図 2　部分復元可能な秘密分散システムの分散段階

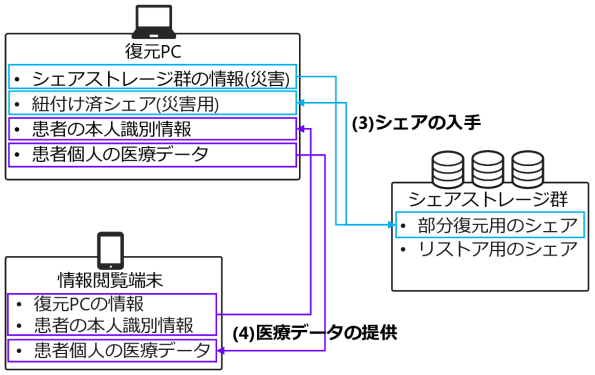

図 3　部分復元可能な秘密分散システムの復元段階

群から部分復元用のシェアを入手し復元する．情報閲覧端末は復元 PC から医師が診療している患者医療データを入手する．以上の手順を踏むことで部分復元を実現している．

3　部分復元可能な秘密分散システムの要件

本節では，提案システムで不正復元される可能性がある点を整理し，不正復元を防ぐ要件を定義する．

情報源が配付する事前情報が第三者に洩れると医療データを不正に復元される可能性がある．事前情報が洩れる条件を図 3 に示す．◯がついているセルは事前情報が洩れない条件を示している．情報源が事前情報を安

盗聴・盗難対策		有	無
端末・操作者	侵入検知		
正当	無		
	有	◯	
不当			
	無		

図 4　事前情報が第三者に洩れる条件

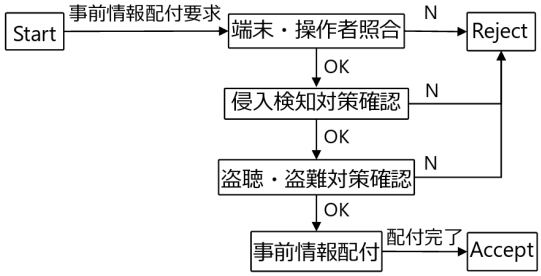

図 5　情報源が事前情報を配付する際の状態遷移

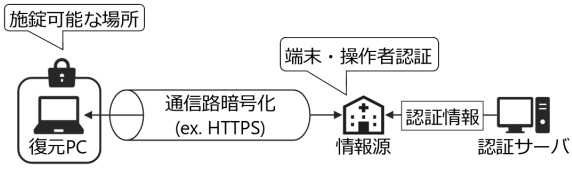

図 6　要件を満たす具体的な対策例の構成

全に配付するためには以下の要件を満たせばよい．

要件　(「端末」⇔「登録端末」)∧(「端末操作者」⇔「登録操作者」)∧「侵入検知」∧「盗聴盗難対策」⇒「事前情報配付」

要件を満たす状態遷移を図 5 に示す．情報源は事前情報を配付する前に，配付先が条件を満たしているかを確認してから事前情報を配付する．1 つでも条件を満たしていない場合は配付を行わない．

要件を満たす具体的な対策例を図 6 に示す．図 6 の対策を施したシステムを実装し，第三者が不正に事前情報を入手できないことを確認した．よって要件を満たす対策を施すことによって事前情報を安全に配付することができる．

4　まとめ

本研究では，部分復元に必要なデータの入手を制限した部分復元可能な秘密分散システムを提案した．さらに，システムで不正復元される問題点を整理し不正復元を防ぐ要件を定義した．要件を満たすことによってシステムを安全に活用することができる．

参考文献

[1] 福本昌弘，“診療情報保全から地域医療連系のための高知県での取り組み,”Mercato, 東北情報通信懇談会, Vol.90, pp.18–20, 2015.

[2] 田中麻実，福冨英次，福本昌弘，“秘密分散バックアップした医療データの部分復元,” 信学技報 IA2015-74, pp.31–36, Dec. 2015.

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