部分復元可能な秘密分散システムの分割方法による復元速度の評価

2018年2月20日

1180347 竹中壮磨

情報学群

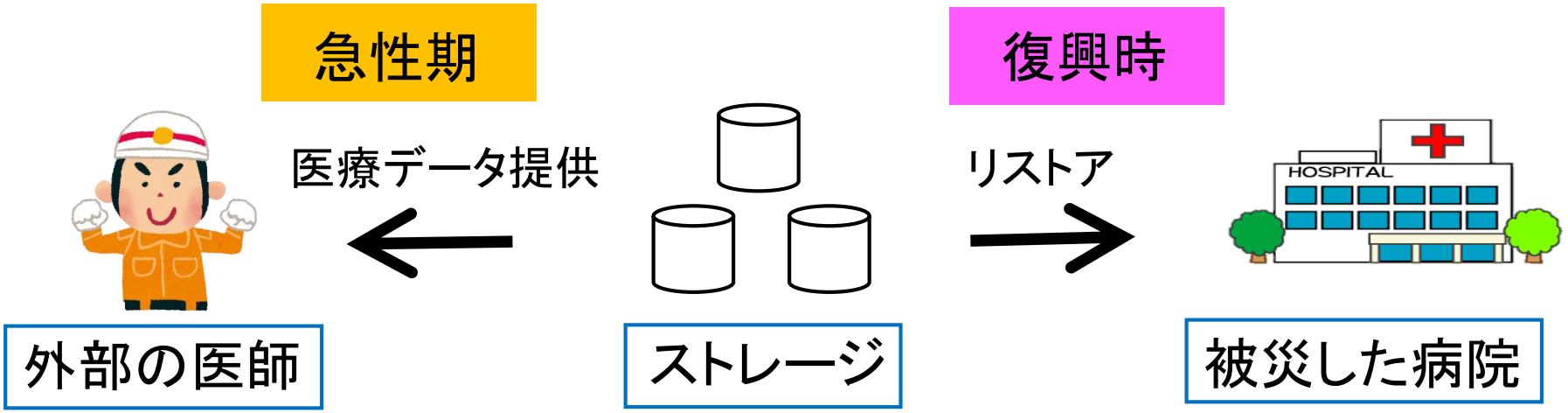
ネットワーク信号処理研究室

研究の背景(1/2)

東日本大震災により医療データが流出し
被災地での医療行為に支障

医療データを遠隔地に分散バックアップ

被災地での医療行為に分散バックアップした医療データを活用



研究の背景(2/2)

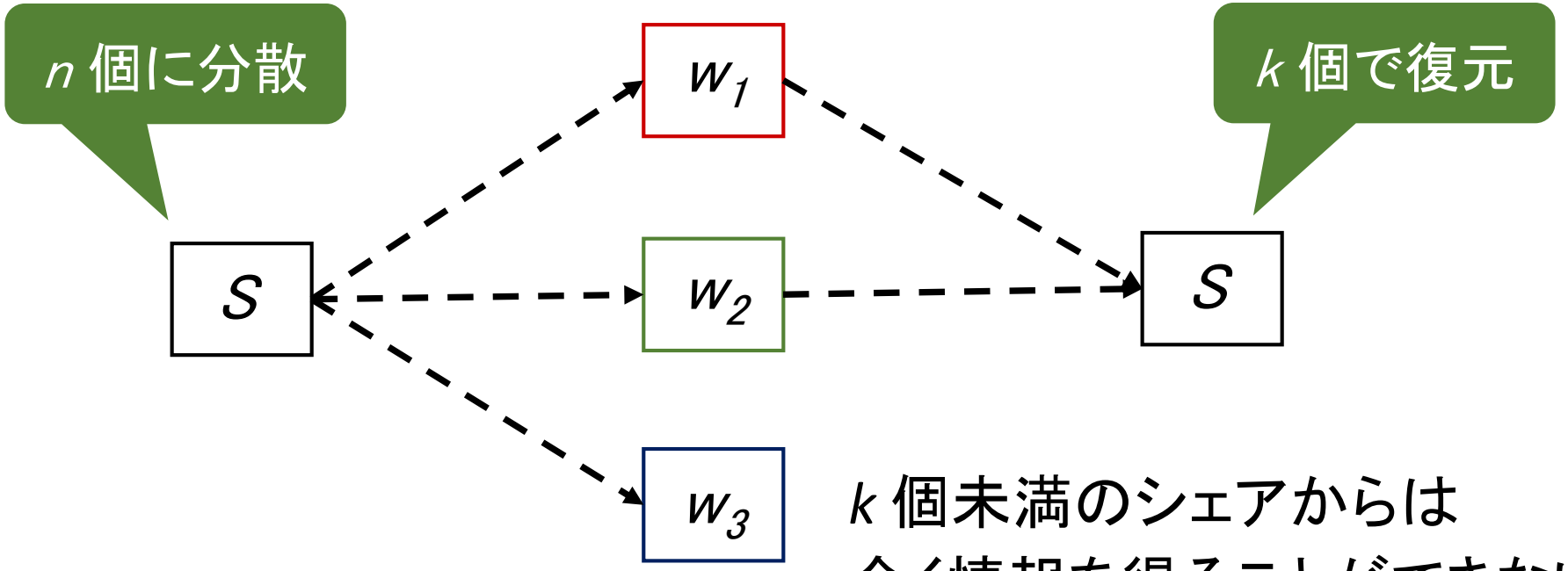
医療データは個人情報であるため、必要な情報のみを提供する必要がある

部分復元可能な秘密分散システム(田中麻実,2015)

提案されたシステムは演算量が大きいため、復元速度が遅く、緊急的に医療データを必要とする災害時に適さない

(*k*,*n*) しきい値秘密分散法

データの冗長化と秘匿化に優れている
しかし、部分復元はできない



k 個未満のシェアからは
全く情報を得ることができない

部分復元可能な秘密分散システム

意味のある項目ごとにデータを分割

S

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

各分割データに分割データサイズ分だけ左シフトして直和をとると元データとなる

分割

S_1 S_2 S_3

l_1 l_2 l_3

分散 分散 分散

$w_{1,1}$ $w_{1,2}$ $w_{1,3}$

$w_{2,1}$ $w_{2,2}$ $w_{2,3}$

$w_{3,1}$ $w_{3,2}$ $w_{3,3}$

結合

復元

$w_{1,1}$ $w_{3,1}$

$w_{1,3}$ $w_{3,3}$

$W_1 \Pi_{m=3}^{2} 2^{l_m} + W_3$

S'

l_1, l_2, l_3

データ長

$(\Pi_{m=3}^{2} 2^{l_m}, \quad 0, \quad 1)^T$

紐付け情報

データSが表現できる
GF(2^m)上で演算を行う

部分復元可能な秘密分散システムの演算量

データSが表現できる拡大体GF(2^m)上で演算を行う

1回の乗算にm^2の演算量

復元まで何時間もかかる

データサイズと乗算にかかる演算量

データサイズ	mの値	1回の乗算にかかる演算量
2KB	16,000	256,000,000
3KB	24,000	576,000,000

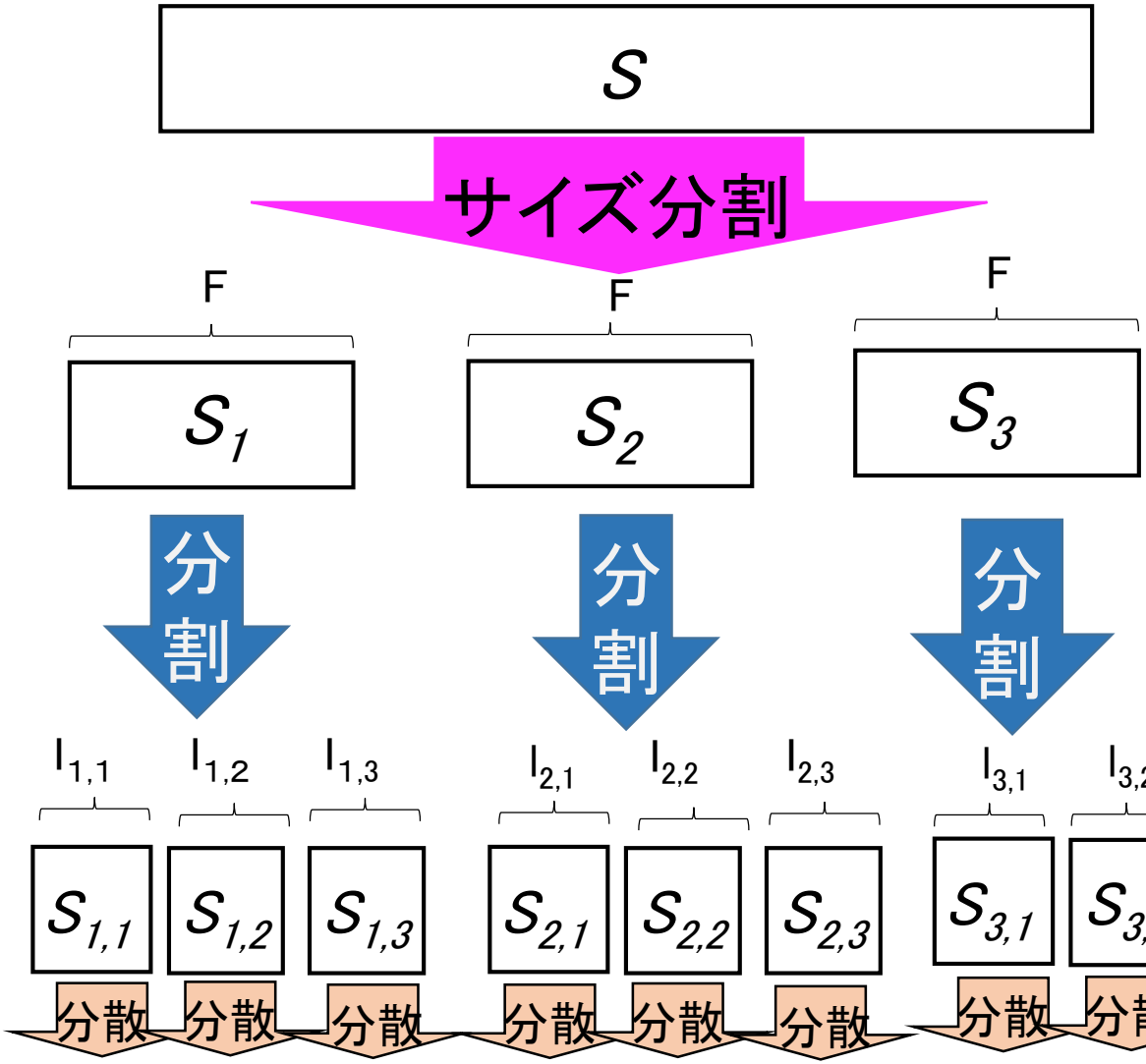
研究の目的

- 課題
  - 部分復元可能な秘密分散システムは演算量が大きく、復元速度が遅い
  - 災害時には緊急的に医療情報を提供する必要がある

データサイズによる分割を行った部分復元可能な秘密分散システムの提案

分割サイズによる復元速度の評価

データサイズによる分割を行った部分復元可能な秘密分散システムの流れ



分散したいデータ Sが
$GF(2^m)$で表現できるとすると
$GF(2^{m/3})$上で演算を行う

先行研究と提案手法の分散と部分復元の方法(1/3)

先行研究の分散方法

分散したいデータSを意味のある項目ごとに分割 S_i (i = 1,2,3)
S_i の分割長を l_i とすると

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

S_i を(k,n)閾値秘密法で分散し、シェアw_{ij}(j = 1,2,･･･,n)を生成
w_{ij}(j = 1,2,･･･k)のシェア行列Wと紐づけ情報uを用いて

$$Wu = \begin{pmatrix} w_{11} & \cdots & w_{31} \\ \vdots & \ddots & \vdots \\ w_{1k} & \cdots & w_{3k} \end{pmatrix} \left(\prod_{m=3}^{2} 2^{l_m}, \quad 2^{l_3}, \quad 0\right)^{T}$$

部分復元用シェアWuを作成する

先行研究と提案手法の分散と部分復元の方法(2/3)

提案手法(データサイズによる分割)の分散方法

Sを一定のサイズFで分割 S_t (t = 1,2,3)

S_t を秘匿部分が選択できるように分割 $S_{t,i}$ (i = 1,2,3)

$S_{t,i}$ の分割長を $l_{t,i}$とすると

$$S = (2^F)^2 \prod_{m=3}^{2} 2^{l_{1,m}} S_{1,1} + (2^F)^2 2^{l_{1,3}} S_{1,2} + \cdots + 2^F S_{2,3} + \cdots + 2^{l_{3,3}} S_{3,2} + S_{3,3}$$

$S_{t,i}$ を(k,n)閾値秘密法で分散し、シェア$w_{t,i,j}$(j = 1,2,…,n)を生成

$w_{t,i,j}$(j = 1,2,…k)のシェア行列Wと紐づけ情報 u を用いて

$$Wu = \begin{pmatrix} w_{111} & \cdots & w_{331} \\ \vdots & \ddots & \vdots \\ w_{11k} & \cdots & w_{33k} \end{pmatrix} \left(\prod_{m=3}^{2} 2^{l_{1,m}}, \quad 2^{l_{1,3}}, \quad 0, \quad \prod_{m=3}^{2} 2^{l_{2,m}}, \cdots, \quad 2^{l_{3,3}}, \quad 1 \right)^T$$

部分復元用シェアWuを作成する

先行研究と提案手法の分散と部分復元の方法(3/3)

先行研究

部分復元シェア Wu を復元する

$$\begin{pmatrix} w_{11} & \cdots & w_{31} \\ \vdots & \ddots & \vdots \\ w_{1k} & \cdots & w_{3k} \end{pmatrix} (\Pi_{m=3}^{2}\ 2^{|m},\quad 2^{|3},\quad 0)^{T}$$

S'

提案(データサイズによる分割)

部分復元シェア Wu を復元する

$$\begin{pmatrix} w_{111} & \cdots & w_{331} \\ \vdots & \ddots & \vdots \\ w_{11k} & \cdots & w_{33k} \end{pmatrix} (\Pi_{m=3}^{2}\ 2^{|1,m},\quad 2^{|1,3},\quad 0,\quad \Pi_{m=3}^{2}\ 2^{|2,m},\ \cdots,\quad 2^{|3,3},\quad 1)^{T}$$

$$= \begin{pmatrix} w_{111} & \cdots & w_{131} \\ \vdots & \ddots & \vdots \\ w_{11k} & \cdots & w_{13k} \end{pmatrix} (\Pi_{m=3}^{2}\ 2^{|1,m},\quad 2^{|1,3},\quad 0)^{T} + \cdots + \begin{pmatrix} w_{311} & \cdots & w_{331} \\ \vdots & \ddots & \vdots \\ w_{31k} & \cdots & w_{33k} \end{pmatrix} (\Pi_{m=3}^{2}\ 2^{|3,m},\quad 2^{|3,3},\quad 1)^{T}$$

S_1'

S_2

S_3

項を取りし、
それぞれを復元すると

$$(S_1',\quad S_2,\quad S_3)\ ((2^{F})^{2},\quad 2^{F},\quad 1)^{T}$$

S'

データサイズによる分割を行った部分復元可能な秘密分散システムの演算量 (1/2)

分散したいデータをS, Sを表現できるGF(2^m) を選択

SをサイズFでf個に分割したものをS_t (t = 1, …, f)

S_tを秘匿部分を選択できるように,d個に分割したものを$S_{t,i}$(i = 1,…,d)

$S_{t,i}$を(k,n)しきい値秘密分散法で分散

復元時(最終結合を除く)

GF($2^{m/f}$)上で, $k^3 + (f+1)k^2 + dfk$ 回の乗算が必要

データサイズによる分割を行った部分復元可能な秘密分散システムの演算量 (2/2)

S のデータサイズを*2KB*

S をサイズ F で f 個に分割したものを S_t

S_t を秘匿部分を選択できるように,8bit単位で分割する

$S_{t,i}$ を(2,3)しきい値秘密分散法で分散

分割サイズ F	サイズによる分割数 f	分割数d	復元時の乗算にかかる演算量
8,000bit	2	1,000	257,280,000,000
128bit	125	16	73,924,608
16bit	1000	2	2,051,072

まとめ

サイズによる分割によって部分復元可能な秘密分散システムの復元速度を速めた

分割サイズによる復元速度の評価を行うために、実証実験で計測しようとしている