

秘密分散データの 部分秘匿化復元の検証

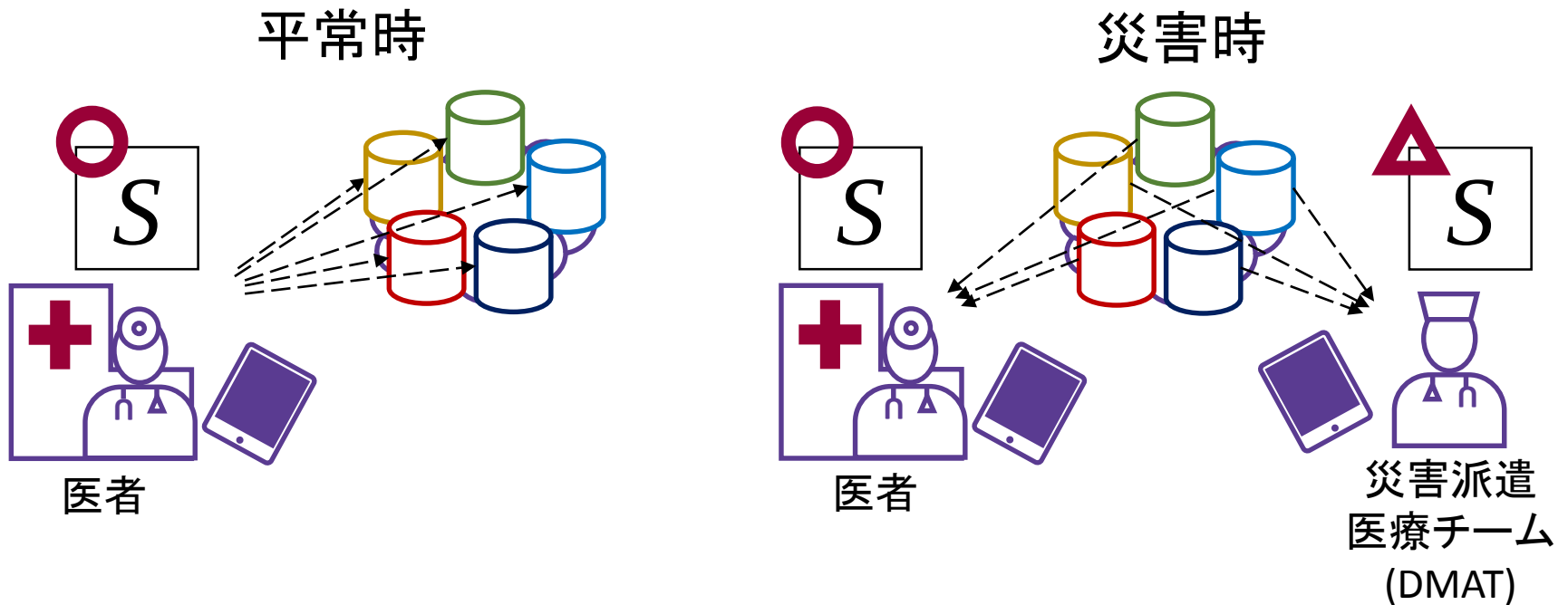
2015年2月16日

情報学群

福本研究室

1150324 田中麻実

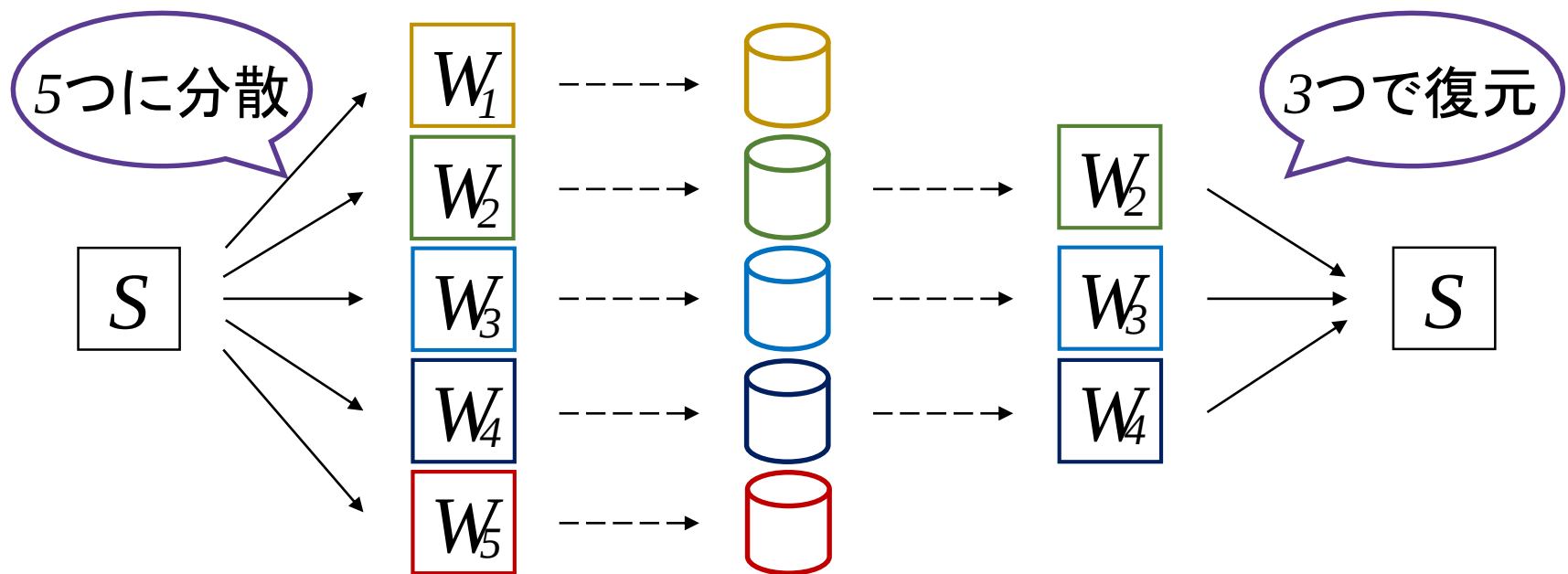
背景・目的



(k,n)しきい値秘密分散法で分散されたデータの
部分秘匿化復元方法の提示,その安全性の検証

(k,n) しきい値秘密分散法

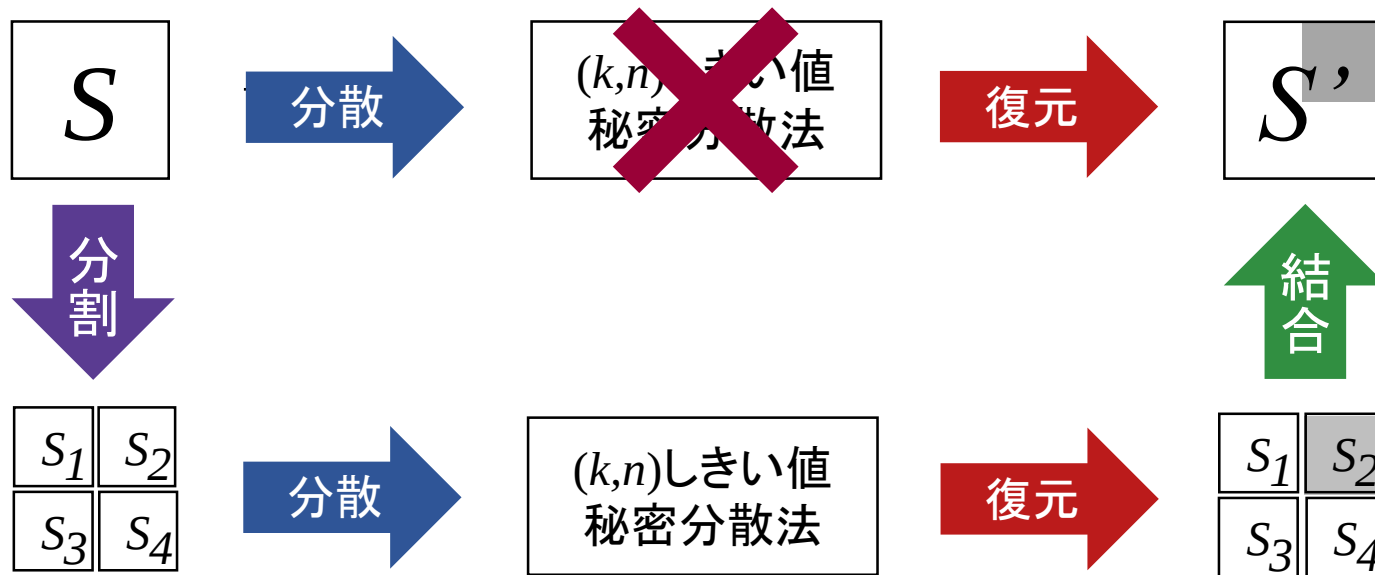
$(5,3)$ しきい値秘密分散



データの秘匿化・冗長化可能

データ分割

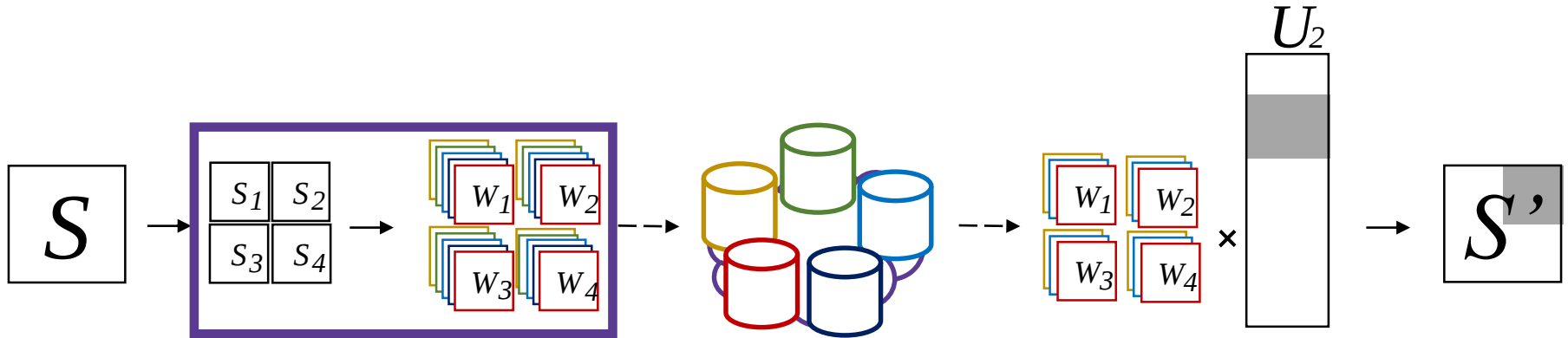
部分的に秘匿して復元不可



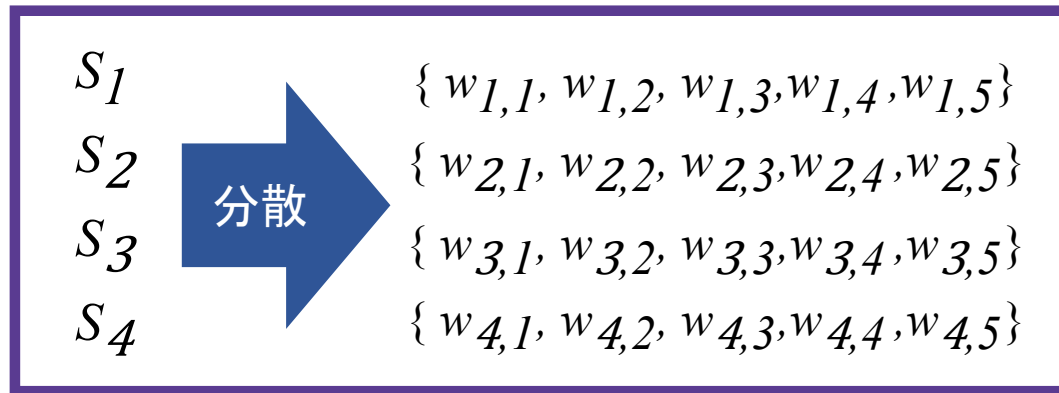
$$S = S_1 \prod_{m=2}^4 2^{lm} + S_2 \prod_{m=3}^4 2^{lm} + S_3 2^{l4} + S_4$$

$$S_1 \prod_{m=2}^4 2^{lm} + 0 + S_3 2^{l4} + S_4 = S'$$

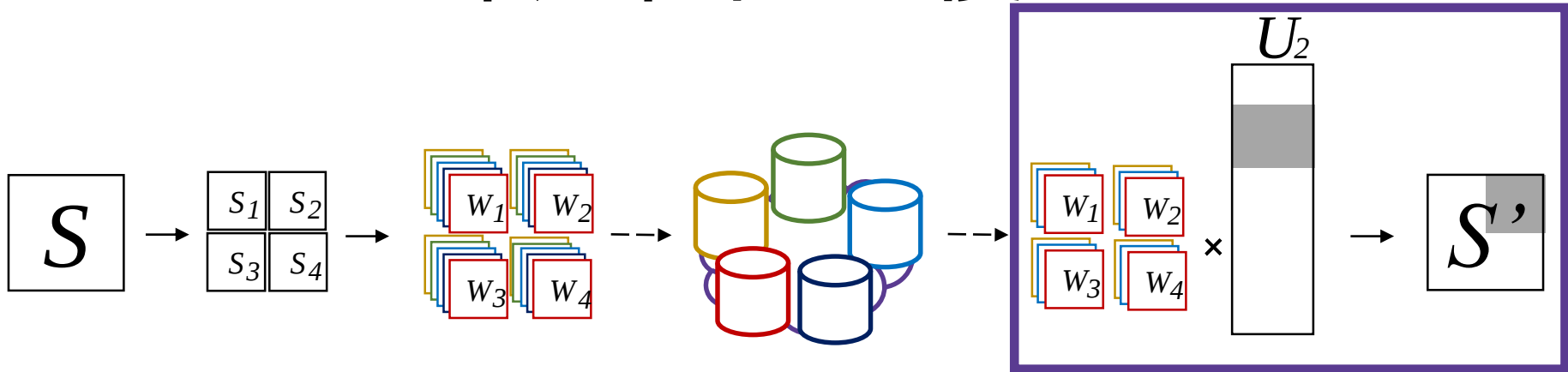
部分秘匿化復元



データを分割し分割データごとに分散



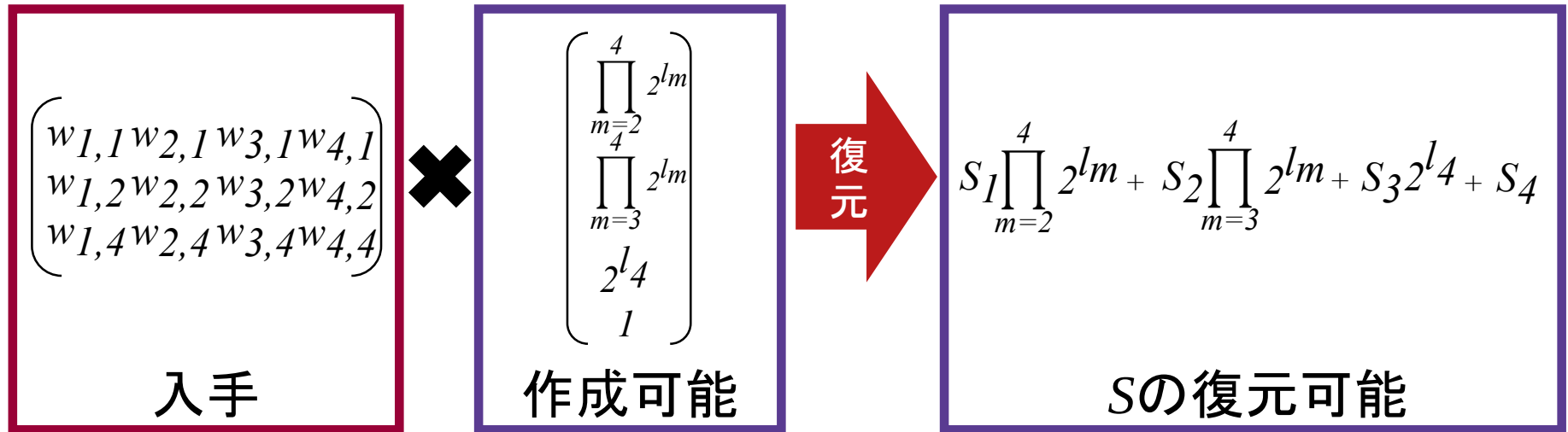
部分秘匿化復元



結合ベクトルを用いてシェアを結合

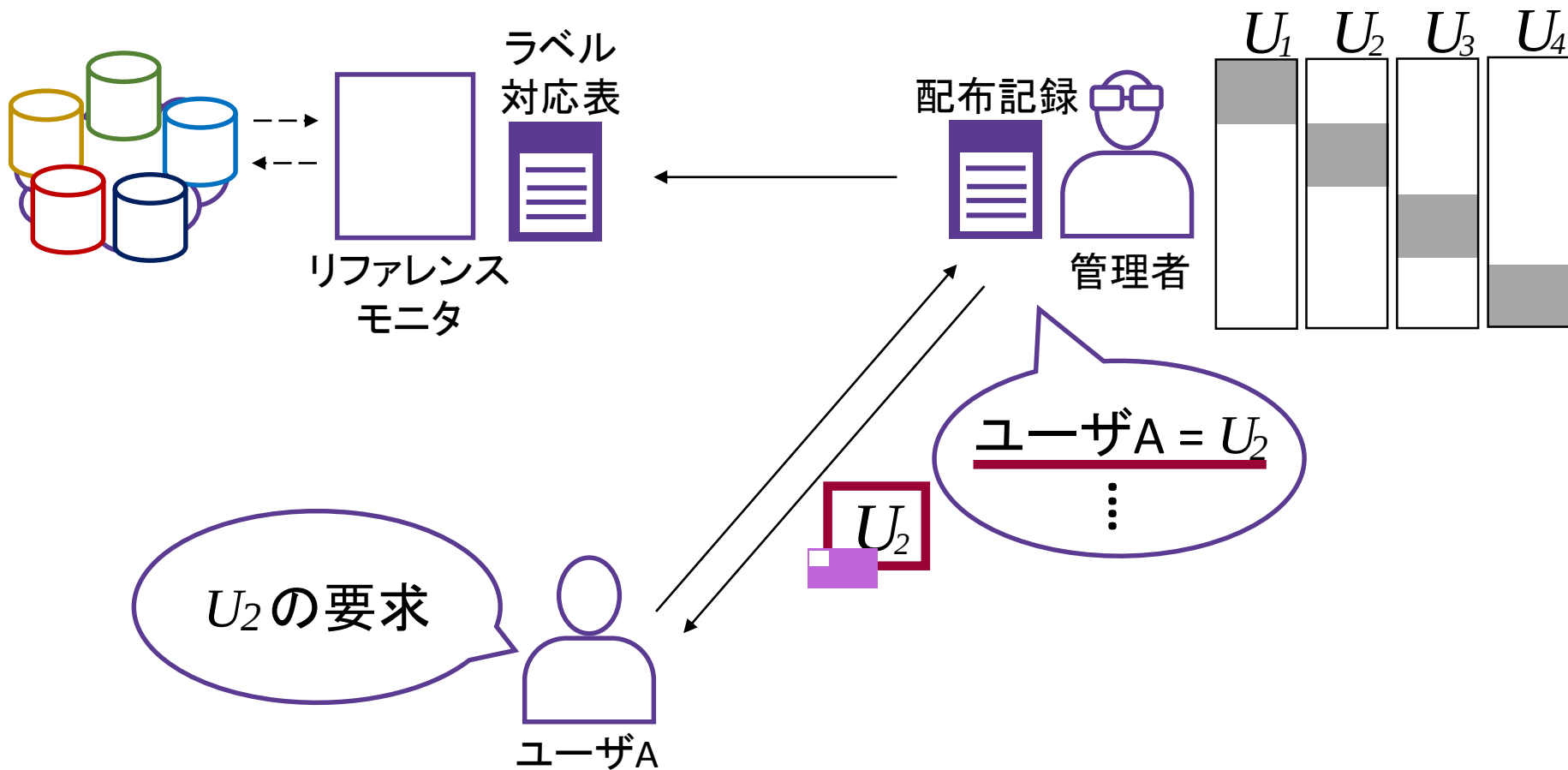
$$\begin{pmatrix} w_{1,1} & w_{2,1} & w_{3,1} & w_{4,1} \\ w_{1,2} & w_{2,2} & w_{3,2} & w_{4,2} \\ w_{1,4} & w_{2,4} & w_{3,4} & w_{4,4} \end{pmatrix} \begin{pmatrix} \prod_{m=2}^4 2^{lm} \\ 0 \\ 2^{l4} \\ 1 \end{pmatrix} \xrightarrow{\text{復元}} s_1 \prod_{m=2}^4 2^{lm} + 0 + s_3 2^{l4} + s_4 = S'$$

不正復元の可能性

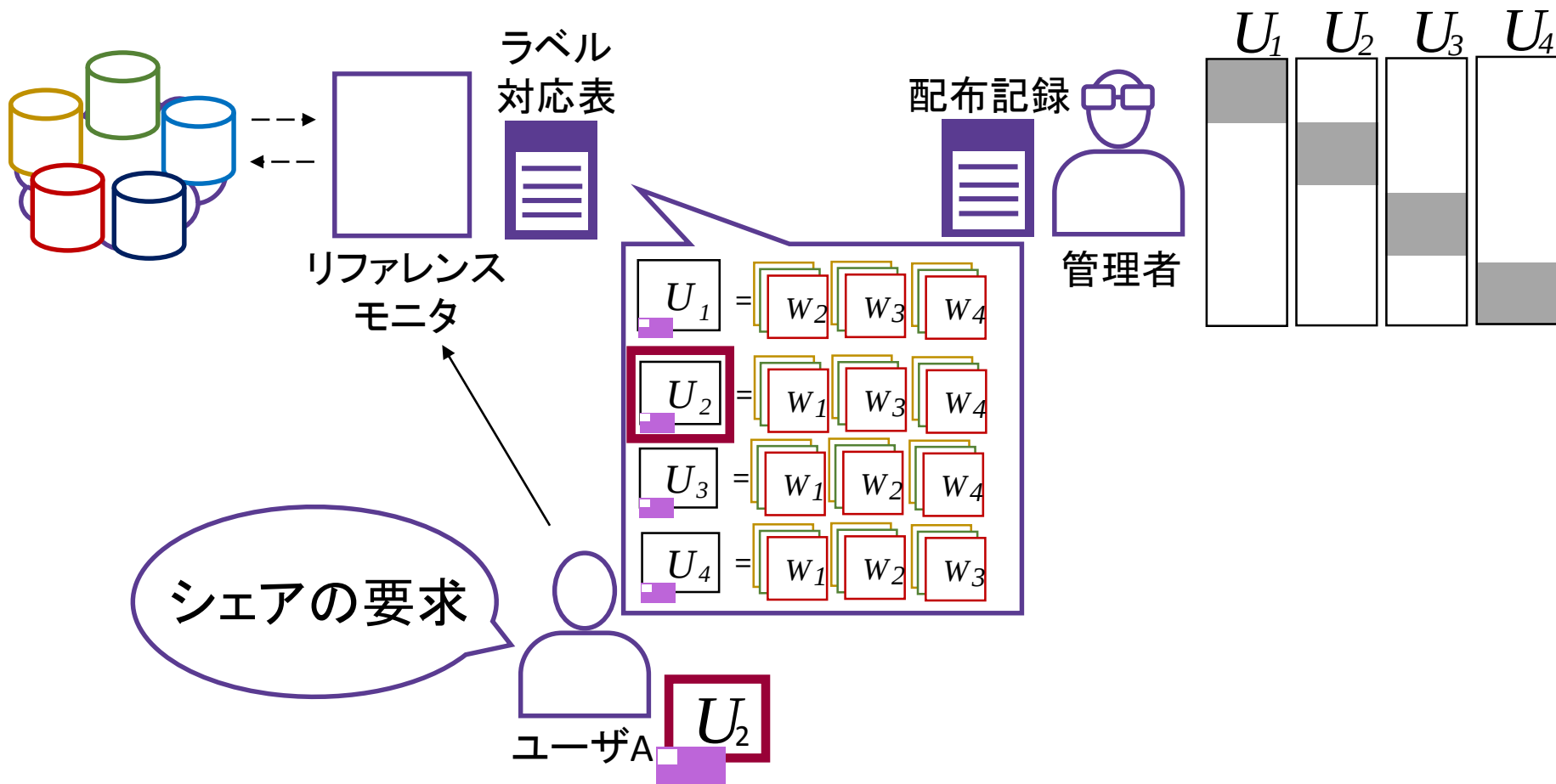


シェアへのアクセス制限

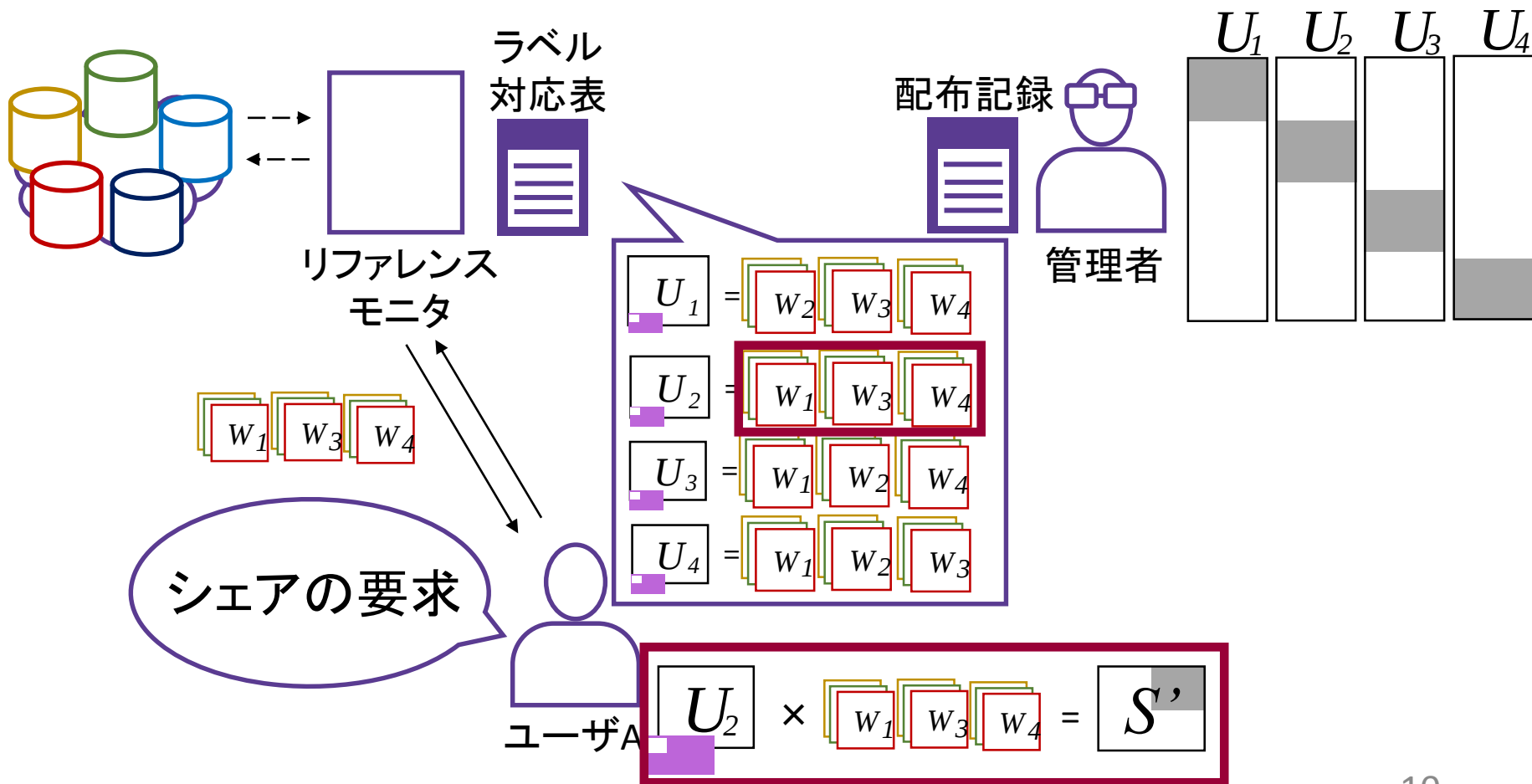
アクセス制限時の シェアへのアクセス手順



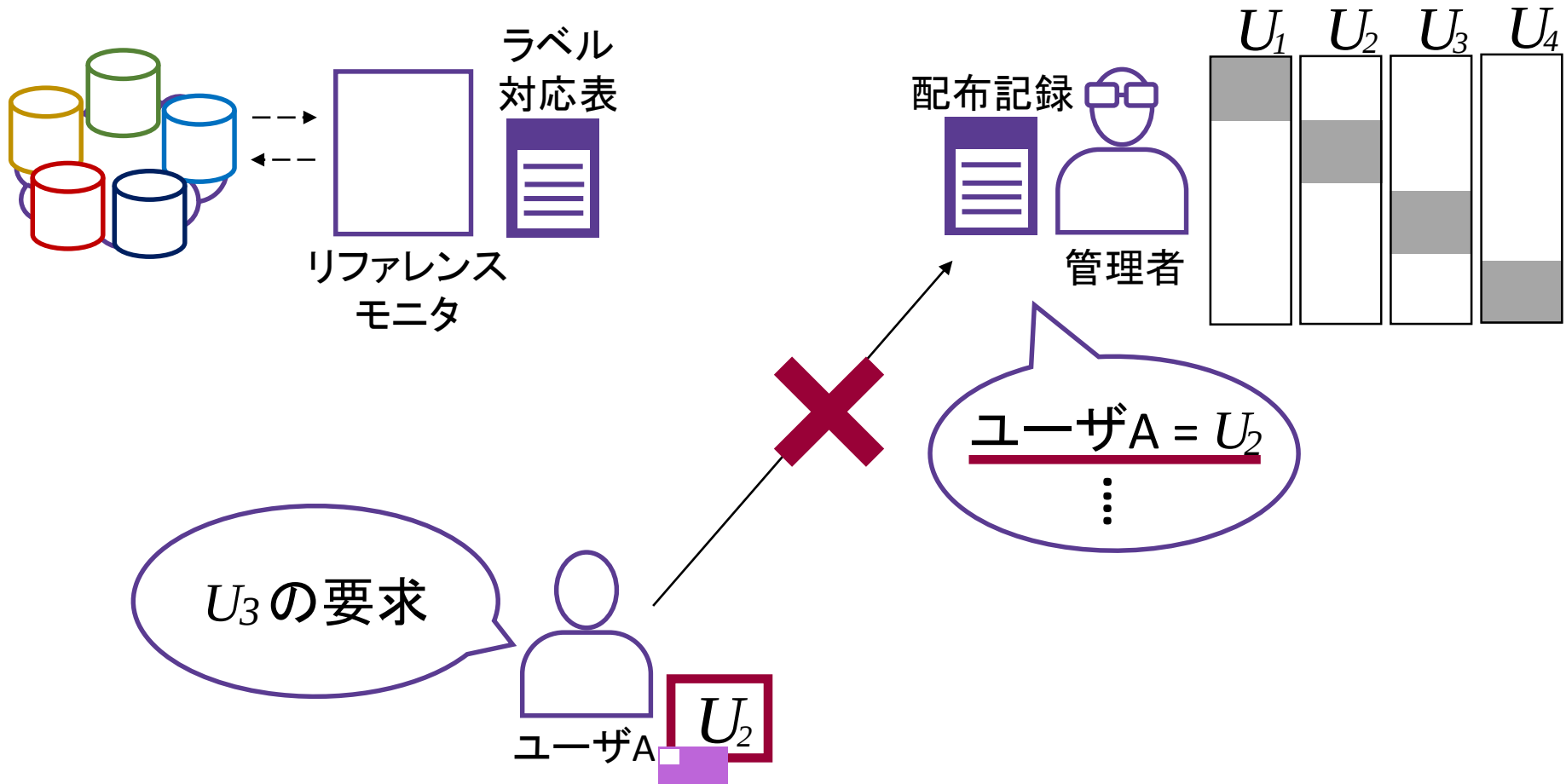
アクセス制限時の シェアへのアクセス手順



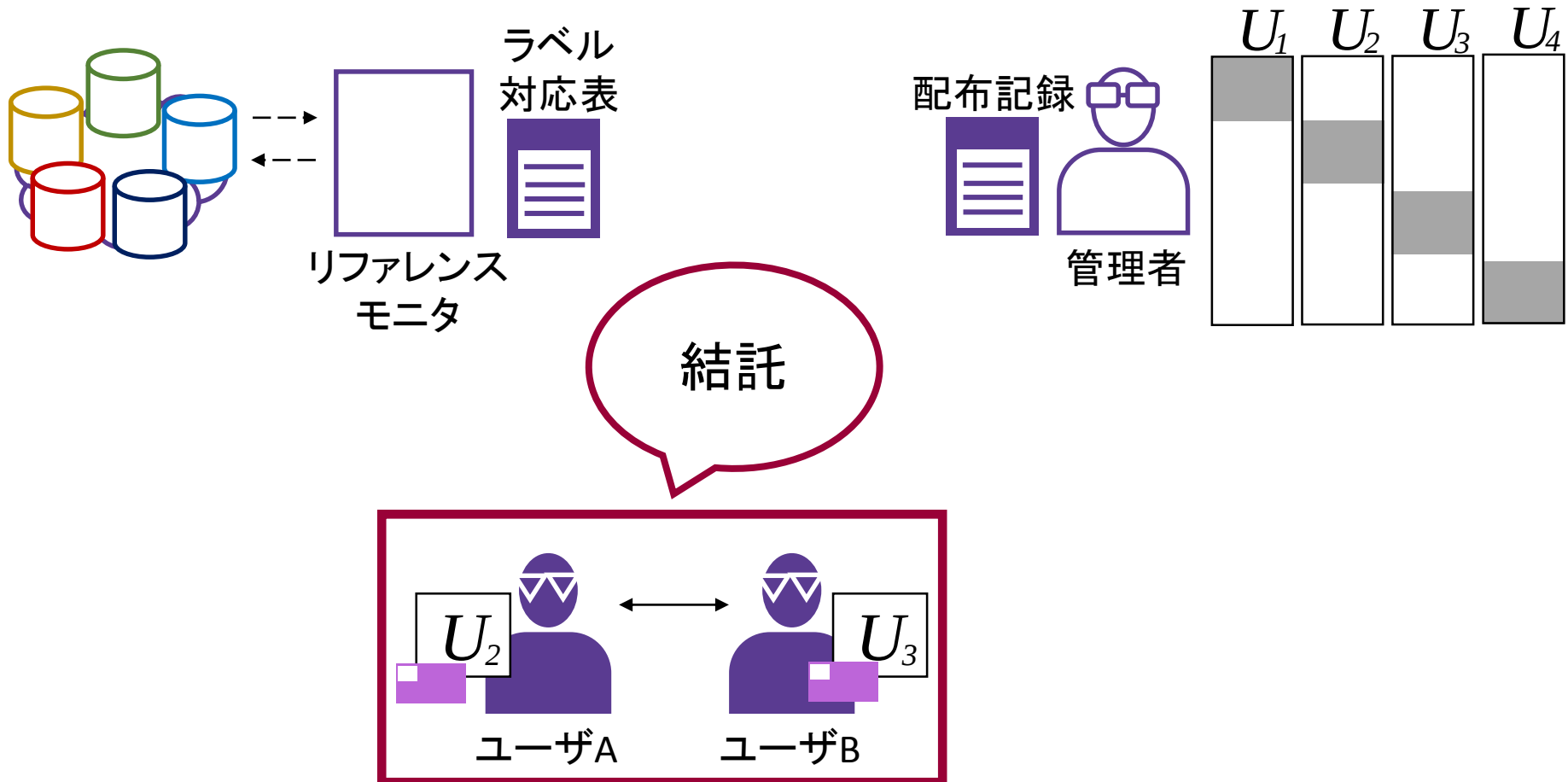
アクセス制限時の シェアへのアクセス手順



管理者が要求を破棄



情報漏えいの可能性



まとめ

- (k,n) しきい値秘密分散法で分散されたデータを部分秘匿したまま復元可能
- アクセスできるシェアを制限
→不正に復元することを防止
- 今後の課題
 - ユーザの結託に対する対策
 - 実証実験