要 旨

秘密分散データの部分秘匿化復元の検証

田中 麻実

秘密分散法を用いて個人情報が含まれる医療データを分散バックアップするという取り組みがある．平常時は医療機関ごとに医療データのバックアップを行い，災害時にバックアップデータを活用しようとするものである．医療データには個人情報が含まれているため，災害時派遣された医療従事者が診察に不必要なデータを閲覧することは問題である．バックアップデータから患者の診察に必要なデータのみを閲覧することができれば，外部から派遣された医師は患者に対して適切な処置を行うことができる．しかし，秘密分散法はデータを部分的に秘匿したまま復元することはできない．

そこで本研究では，(k, n) しきい値秘密分散法を用いてデータを部分的に秘匿したまま復元する方法を提案し，提案方法の評価を行っている．データを分割してからシェアを作成し，シェアを結合する際に秘匿部分にマスクをかけることで，データを部分的に秘匿している．しかし，何らかの方法でシェアを入手することができれば，データを不正に復元される恐れがあるため，不正復元を防ぐアクセス制限方法を示している．アクセス制限により，管理者の意図しないユーザがデータを復元することを防ぐことができる．

キーワード　秘密分散法，部分秘匿化復元

Abstract

Verification of partly concealed reconstructing of secret sharing data

TANAKA Asami

To prevent medical data from loss and leak, there is the distributed backup system using secret sharing scheme. In this system, medical data ware backed up to network storages for each medical institution in normal time. When the disaster occurs, backup data is used for medical examination to victims. Disaster Medical Assistance Team (DMAT) should not be see data other than needed data in the medical examination. DMAT can examine and treat when needed data can be seen. However, secret sharing scheme cannot conceal a part of data when distributed data is reconstructed.

In this paper, the reconstruction method to conceal a part of data using (k, n)-threshold secret sharing scheme has been proposed and evaluated. Data is divided private part and public part. In proposed method, shares are made from divided data. Shares in private part are concealed by dummy data when shares are bonded, and bonded shares are reconstructed. However, shares are obtained fraudulently, data can be reconstructed. As a solution against this vulnerability, the access limitation method of shares have been represented. The access limitation can be prevented from illegal reconstructed.

key words secret sharing scheme, partly concealed reconstructing