要 旨

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

田中麻実

東日本大震災の津波によって電子カルテが損失したことにより，被災地での医療行為に支障が出た．これを受けて高知県の病院では電子カルテを遠隔地にバックアップする取り組みが始められている．さらに遠隔地にバックアップした電子カルテを災害時の医療行為に活用することが期待されている．医療データは個人情報であるため，災害時の医療行為に必要な情報のみを提供する必要がある．そこで，バックアップデータから必要な情報のみを復元する秘密分散法を用いた部分復元アルゴリズムを提案した．提案した部分復元アルゴリズムは，部分復元に必要な情報が第三者に入手されると不正復元される可能性がある．

本論文では不正復元を防いだ部分復元可能な秘密分散システムを提案している．提案システムでは部分復元を行うための情報を必要とする．その情報を用いることによって必要最低限の患者の情報を DMAT に提供することができる．しかし，部分復元に必要な情報が第三者に入手された場合不正復元される可能性があるため，不正入手を防ぐ要件を定義している．要件を満たす対策を施すことによって，安全に医療データの部分復元を行うことができる．

キーワード　分散バックアップ，秘密分散法，部分復元

Abstract

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

Asami TANAKA

The medical treatment in the area affected of disaster was difficult because medical data lost in the tsunami of great east japan earthquake. In order to prevent medical data from being lost, the hospitals in Kochi have started the remote backup plan. Moreover, by providing the required information of treating victims from backup data such as name, blood type and medicine information, Disaster Medical Assistance Team (DMAT) can treat victims outside the hospital at the acute stage of disasters. Because medical data is personal information, it is necessary to provide the minimum required patient information. The restoration method has been proposed to confine more decoding data than necessary decoding data. In order to provide the patient information, the proposed method owns the decoding control information. However, it is possible to illegally decode in case the leaked the decoding control information.

In this paper, the restoration structure to prevent from illegal decoding has been proposed. To prevent from illegal decoding, the structure control information has been defined to prohibit the decoding control information leakage. In addition, the requirement has been defined to prevent the structure control information from being leaked. The experimental results suggested that it is possible to prevent from illegal decoding by satisfying the requirements.

key words distributed backup, secret sharing scheme, confied decodning