秘密分散技術を用いた統合文書管理システム（DACS）内文書の遠隔バックアップ環境の開発

① 対象

阪大病院の病院情報システムに保管されている既存の診療データ

② 研究機関名

研究機関代表施設： 大阪大学医学部附属病院

分担施設： 愛媛大学、京都大学、NRIセキュアテクノロジーズ株式会社

③ 目的

既存の院内の診療情報文書を、秘密分散技術を用いて暗号化かつ分散片化し、複数の拠点に設置するサーバに「遠隔バックアップ」するシステムを構築し、診療データが暗号化された形で遠隔地に安全に保存出来るかどうかの検証を行う。

④方法

秘密分散技術とは、実患者の診療データを暗号化しかつ分散片化することで、各分散片からは情報理論的に元ファイルを復元できない状態にする技術のことである。本研究ではこのもはや個人情報では無い分散片となったデータを病院内ネットワークから外部へ送信し、各拠点に安全に効率よく保管出来るかどうかを検証する。元ファイルとしては大阪大学医学部附属病院の病院情報システムに保管されている実患者のデータを用いるが、外部に送信するデータである分散片は、既に情報理論的に個人情報ではなくなっている。かつ分散片を復元し元の情報に戻すために必要な情報や機材は、すべて阪大病院内のセキュリティの確保されたサーバルームに設置・構築するので、本検証中に病院敷地外へ個人情報（患者情報）が流出することはない。

この仕組みを用いて遠隔地(京都大学、愛媛大学、NRI セキュアテクノロジーズ株式会社が用意するデータセンターを想定)に分散片データが安全に保存出来るかどうかを検証する。この際用いるネットワーク経路は冗長化されており、災害時でも少なくとも一つの経路は利用できる様な仕組みとする。かつ万が一の事も考慮して、今回使用するネットワーク回線は総務省の提供する JGN-X 閉域網と本研究のため専用に用意したルータ等のネットワーク機器を用い、冗長化された専用回線を用意することとする。

本検証で用いる元データが実患者のデータであったとしても、それぞれの分散片データは個人情報ではないので、分散片データを院外に送信することも問題ないと考えている。また一般のネットワークとは隔絶された専用回線を本検証専用に用意することにより、さらに安全性は高まる。

本研究では、さらに、阪大病院が災害等でシステムが破壊され他の拠点でデータの復元

が必要になった場合を想定した検証も行う。この際には、データを復元するための情報や機材を一旦外部の拠点（京都大学を想定）に設置して、各拠点に分散保管された分散片を集め、元データを復元する。この分散片から元データに戻す検証を行う際は、模擬患者のデータ（デモデータ）を用いて検証を行うこととする。すなわち、阪大外で復元されるデータはデモデータであるので、阪大外へ患者情報が流出する事は無い。

⑤意義

秘密分散技術を用いた遠隔バックアップシステムの確立は、低コストでの診療データの冗長性確保を可能とする。また各分散片単独では元のデータを復元できないため、より安全性も高まることとなる。大規模災害時にも迅速に診療データを復元でき、病院の事業継続性確保にも寄与するものと考えられ、引いては患者の利益に供するものと考えている。

⑥個人情報の扱い

阪大病院内部では実際の診療データを扱うがこれは病院の運用管理規定に則って行う。病院外部へデータを出力する前に、連結不可能な匿名化（秘密分散技術による分散化および暗号化）を行う。これにより、院外へ個人情報が流出することはない。

⑦問い合わせ先

大阪大学医学部附属病院医情報部
TEL：06-6879-5900、FAX：06-6879-5903
住所：〒565-0871 大阪府吹田市山田丘 2-15