検索システムの構成による医療データ不正復元の防止

1210390　吉冨　亮平　【 ネットワーク信号処理研究室 】

1　はじめに

広域災害に備え医療データを保全し，被災地での診療に活用することが求められている．そこで，部分復元可能な秘密分散法が提案された [1]．しかし，分散した医療データを検索する仕組みはない．そのため，分散した医療データの素早い検索方法が提案された [2]．検索方法は，ある条件において識別情報が絞られる．識別情報の絞り込みが医療データの不正復元される要因となってはいけない．本研究では，検索方法により生じた識別情報の絞り込みの防止を目的として検索システムの構成を提案する．

2　検索システム構成と評価

検索方法は，医療データのシェアに個人を識別する情報を対応付けて保存している．そのため，医療データを復元するには，識別情報を一意に定め，医療データのシェアの対応を知る必要がある．識別情報の絞り込みは，剰余演算の法を大きくすることで，識別情報を一意に定めることは困難になるため，大した問題ではない．しかし，識別情報の絞り込みにより医療データが不正復元されてはいけない．そこで，識別情報が絞り込まれる要因となるタグ t，タグ作成に使用する p, x の漏えいを防止する検索システム構成を提案し，評価について述べる．

2.1　提案システム構成

攻撃者がストレージ群にアクセスすることができれば，シェアに対応した t は漏えいする．そこで，検索・復元を行う端末をリファレンスモニタと呼び，ストレージ群へのアクセスを制限する．ストレージ群はアクセス元の照合を行う．検索要求により医療データを不正に取得される恐れがあるため，検索要求を行う端末を情報端末と呼び，リファレンスモニタへのアクセスを制限する．リファレンスモニタはアクセス元の照合を行う．それぞれの端末は病院内に設置することで安全は確保される．医師端末は災害時に開設される仮設の診療所での利用が想定されるため，盗難等の恐れがある．そのため，医師端末はどのような情報も保存しないことが望ましい．そこで，医師が診療を行う際は正当な利用者か照合を行い，医師端末から情報端末へリモートアクセスすることで医師端末に保存することなく医療データの閲覧や検索を行う．提案システム構成を図 1 に示す．

2.2　提案システム構成の評価

提案システム構成は，医師端末の安全が保証できないことから盗難や医師の不注意による医師以外の端末利用が考えられる．また，情報端末やリファレンスモニタのなりすましが考えられる．

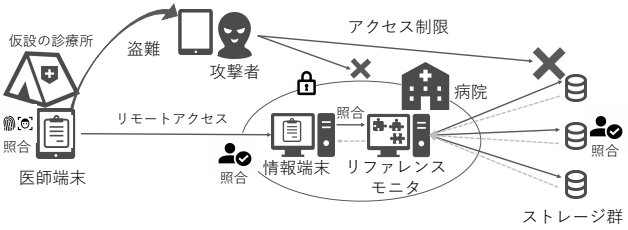

図 1　提案システム構成図

2.2.1　医師端末が盗難された場合

検索・復元を行う端末をリファレンスモニタと呼び，p, x を保存したため，医師端末の盗難による p, x の漏えいを防止できる．また，医師の不注意により医師以外による医師端末の利用が可能な場合，情報端末に対してリモートアクセスの実行が試みられる．しかし，情報端末で医師端末の利用者が正当か確かめる利用者照合を行うことで，医師以外リモートアクセスはできない．

2.2.2　なりすましによりアクセスされた場合

情報端末のなりすましによって検索要求された場合，送信してきた相手が正当な情報端末であるか照合が行われる．また，情報端末での利用者照合がクリアされていない場合，リファレンスモニタにおいて利用者照合を行うことで，不正な検索要求による医療データの取得はできない．ストレージ群では，アクセスしてきた相手が正当なリファレンスモニタであるか照合が行われる．ストレージ群へアクセスされても医療データのシェアと t の保存方法により医療データのシェアの組み合わせを知ることができないため，医療データを不正に復元される恐れはない．

3　まとめ

本研究では，検索方法により生じた識別情報の絞り込みの防止を目的とした検索システムの構成を提案した．提案システムの構成により t, p, x の漏えいを防止することで安全性を担保できると考える．

参考文献

[1] 田中麻実，福冨英次，福本昌弘，“秘密分散バックアップした医療データの部分復元，”信学技報 IA2015-74，pp.31-36，Dec.2015.

[2] 中村巴，福冨英次，福本昌弘，“ 部分復元可能な秘密分散法におけるシェア間の係数の差の比較による医療データの検索，” SCIS2020，3C1-4，2020.