4ZG-1

連結可能匿名化された医療情報の安全管理措置の検討

平井　徹也[†]　福田　洋治[‡]　廣友　雅徳[††]　毛利　公美[‡‡]　中井　敏晴[†††]　白石　善明[†]

†名古屋工業大学　‡愛知教育大学　††佐賀大学

‡‡岐阜大学　†††国立長寿医療研究センター

1. はじめに

近年，生体から得られた試料や情報をデータベース化して医療分野の研究を支援するバイオバンクの構想が進んでいる[1]．例えば，6 カ所の国立高度専門医療研究センター（以下，NC とする）で組織される事業では，文献[2]の「試料等の収集・分譲の在り方」に則って，要件・手続等を検討している．そのうえで，試料・情報提供者から適切な同意が得られており倫理審査で承認されている場合，各 NC で収集した試料等は連結可能匿名化された状態で他研究機関に提供される予定である[1]．収集した試料等（以下，医療情報とする）は，連結可能匿名化により，匿名化された医療情報（以下，臨床研究用データとする），個人識別情報，この 2 つの対応表（以下，連結情報とする）の 3 つに分けて保管される．連結情報は，臨床研究用データと個人識別情報を連結するものである．

電子的な医療情報に対する安全管理措置として，連結情報を物理的にアクセスできないようにする方法が一例としてあげられている[3]．連結情報にアクセスし，臨床研究用データに対応する個人を特定する操作を一括して行うシステムを構成し，ネットワークを通じてアクセスできれば，研究機関は個人識別情報が保管されているサーバに直接アクセスすることなく臨床研究を行える．

一方で，ネットワークを通じてデータにアクセスできるようにすることで情報が流出するリスクが高まる．例えば，流出した連結情報から個人が特定されるなどのリスクがある．連結情報に対して安全管理措置を施しつつ，臨床研究用データと個人識別情報を対応付ける必要がある．

本稿では，個人識別情報に直接アクセスせず，暗号化されている連結情報にアクセスした後に，間接的に個人識別情報と臨床研究用データを対応付けて臨床研究を進めることができる情報システムの実現に向けて，まず，情報セキュリティの観点から脅威の分析を行う．次に，脅威分析の結果から安全管理措置について検討し，課題を抽出する．最後に，課題を解決する技術を導入した個人識別情報非可視型連結可能システムの構成を検討する．

2. 課題の抽出

文献[4]では，企業における情報セキュリティのリスクを要因の所在の観点から分類・整理しており，その文献[4]の分類の仕方にさらに流出経路の観点を加えて，整理したものが表 1 である．作為的であるか，不作為的であるかは悪意の有無による．

文献[3][6][7]で電子的な医療情報を扱う際の 4 つの安全管理措置（組織的安全管理措置，人的安全管理措置，物理的安全管理措置，技術的安全管理措置）が示されている．医療施設ごとに定められたポリシによる組織的安全管理措置だけでは盗聴，誤操作・誤設定などの脅威を防ぐのは難しい．ネットワーク上でやり取りされるパケットからの復元，または，不作為なヒューマンエラーなどの脅威が情報セキュリティの脆弱な部分を突き，システムが攻撃される可能性があるからである．表 1 に示

表 1　情報セキュリティの脅威の分類
（文献[4],[5]をもとに作成）

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="2">内部要因（情報へのアクセス権限を持つ部内者の行為や，社内システムの障害に起因するもの）</th><th colspan="2">外部要因（情報へのアクセス権限を持たない部外者の行為や，不測の災害・事故に起因するもの）</th></tr>
<tr><th>作為的事象</th><th>不作為的事象</th><th>作為的事象</th><th>不作為的事象</th></tr>
<tr><td rowspan="3">アクティブ</td><td>物理的要因による流出・破壊</td><td>1)不正な情報の持ち出し
2)内部犯罪・内部不正行為</td><td>―</td><td>3)盗難
4)不法侵入</td><td>―</td></tr>
<tr><td>ネットワークからの流出・改ざん・偽造・破壊</td><td>5)不正な情報の持ち出し
6)内部犯罪・内部不正行為
7)不正プログラムの実行</td><td>―</td><td>8)不正アクセス
9)ワーム・ウィルス
10)サイバー攻撃
11)不正なプログラムの実行
12)なりすまし</td><td>―</td></tr>
<tr><td rowspan="2">パッシブ</td><td>物理的要因による流出・破壊</td><td></td><td></td><td></td><td>13)紛失・置き忘れ
14)災害・事故</td></tr>
<tr><td>ネットワークからの流出・改ざん・偽造・破壊</td><td colspan="4">15)管理ミス
16)目的外使用
17)誤操作・誤設定
18)システム障害
19)盗聴
20)バグ・セキュリティホール</td></tr>
</table>

21)証拠の非保全：全体

したネットワーク上のパッシブな攻撃には，組織的安全管理措置と技術的安全管理措置を施さなければならない．

連結情報の内容がわからなければ，臨床研究用データと個人識別情報を連結できないので，ネットワーク上でやり取りされるデータのうちで連結情報に着目して脅威に対抗することを考える．具体的には，ネットワークを通じてデータをやり取りする際に，第三者に盗み見られたり改ざんされたりされないよう連結情報を暗号化する．パッシブな攻撃のうちネットワーク上の流出・改ざん・偽造・破壊に分類される脅威に対抗するために連結情報を暗号化して保管し，暗号文のまま参照できるようにすることを課題の一点目としてあげる．

また，臨床研究用データと個人識別情報を関連付けて閲覧する際に，データを直接結合して表示すると，匿名化されていない医療情報を持ち出せる．結合した医療情報を持ち出せない，または紙などの物理媒体に残せないようにする．アクティブな攻撃のうち物理的要因による流出・破壊に分類される脅威に対抗するために臨床研究用データと個人識別情報を直接結合せずに閲覧できるようにすることを課題の二点目としてあげる．

3. 個人識別情報非可視型連結可能システム

3.1. 構成要素

図 1 にシステムの構成を示す．

[登録者]　医療情報を登録ホストに登録する．

[閲覧者]　閲覧ホストに検索ワードを入力し，関連付けられた該当する臨床研究用データと個人識別情報を閲覧する．

[登録ホスト]　登録者から医療情報を受けとり，医療情報を連結可能匿名化し，連結情報を連結情報保管サーバに，臨床研究用データを臨床研究用データ保管サーバに，個人識別情報を個人識別情報保管サーバにそれぞれ保存する．

[閲覧ホスト]　閲覧者から検索ワードを受けとり，連結情報保管サーバ上に保管されている連結情報を参照する．連結情報をもとに該当する臨床研究用データを臨床研究用データ保管サーバから，個人識別情報を個人識別情報保管サーバからそれぞれ取得し，閲覧者に関連付けて表示する．

[連結情報保管サーバ]　登録ホストから連結情報を受けとり，保存する．また，閲覧ホストから検索ワードを受けとり，該当する連結情報を検索し，検索結果を応答する．

[臨床研究用データ保管サーバ]　登録ホストから臨床研究用データを受けとり，保存する．また，閲覧ホストから臨床研究用データ取得要求を受けとり，該当する連結情報を応答する．

Security Management of Linkable Anonymous Medical Information
† Tetsuya HIRAI and Yoshiaki SHIRAISHI・Nagoya Institute of Technology
‡ Youji FUKUTA・Aichi University of Education
†† Masanori HIROTOMO・Saga University
‡‡ Masami MOHRI・Gifu University
††† Toshiharu NAKAI・Research Institute National Center for Geriatrics and Gerontology

[個人識別情報保管サーバ] 登録ホストから個人識別情報を受けとり，保存する．また，閲覧ホストから個人識別情報取得要求を受けとり，該当する個人識別情報を応答する．

3.2. 前提

パッシブな攻撃のうちネットワークからの流出・改ざん・偽造・破壊に分類される脅威とアクティブな攻撃のうち物理的要因による流出・破壊に分類される脅威以外に対しては，文献[5]の 6 章に示されている基本的な安全管理措置を施して対抗することとする．

3.3. 動作フェーズ

[登録フェーズ] 登録者は，登録ホストに医療情報を入力する．登録ホストは，医療情報を連結可能匿名化し，連結情報，臨床研究用データ，個人識別情報を作成する．登録ホストは，連結情報を暗号化し，検索タグを付ける．登録ホストは，各保管サーバに連結情報，臨床研究用データ，個人識別情報を保存する．

[閲覧フェーズ] 閲覧者は，閲覧ホストに検索ワードを入力する．閲覧ホストは，検索ワードを暗号化し，暗号化した検索ワードを連結情報保管サーバに入力する．連結情報保管サーバは，検索タグを使って暗号化された検索ワードに該当する暗号化された連結情報を検索し，該当する暗号化された連結情報を閲覧ホストに応答する．閲覧ホストは，連結情報を復号し，臨床研究用データ保管サーバ，個人識別情報保管サーバから臨床研究用データ，個人識別情報を取得する．閲覧ホストは，臨床研究用データと個人識別情報を直接結合せずに閲覧者に表示する．

3.4. 臨床研究用データと個人識別情報の閲覧

課題の 2 点目について，臨床研究用データと個人識別情報を関連付けて出力する際に，ビューワを使い，複数の画像を直接結合せずに表示すること，通信路を暗号化し，パケットからファイルを復元できないようにすること，画面キャプチャと印刷を禁止することを規程として定めることで解決する．

4. 評価

3 章のシステムは情報セキュリティの脆弱な部分を突く脅威に対して安全管理措置が施されていることを確認する．

医療情報を直接結合されないので，1)-4)アクティブな攻撃のうち物理的要因による流出・破壊に分類される脅威，5)-7)内部要因のうちの作為的事象のネットワークからの流出・改ざん・偽造・破壊に分類される脅威，13)紛失・置き忘れ，15)管理ミスに対抗できる．閲覧ホストにアクセスする際に，認証と通信路の暗号化をすれば，8)不正アクセス，11)不正プログラムの実行，12)なりすましに対抗できる．連結可能匿名化された医療情報は，3 つのサーバに分散して保管されているので，10)サイバー攻撃に対抗できる．連結情報を暗号化し，暗号文のまま参照することができれば，16)-20)パッシブな攻撃のうちネットワーク上の流出・改ざん・偽造・破壊に分類される脅威に対抗できる．3.2 章で示した基本的な安全管理措置で示されている，不正ソフトウェア対策，災害等の非常時の対応，アクセスの記録により，9)ワーム・ウィルス，14)災害・事故，21)証拠の非保全の脅威に対抗できる．

5. 関連システム

医療情報を連結可能匿名化して保管する他のシステムと提案システムを比較する．

特殊匿名化システム[8]は，検査，実験，試験などで取り扱われる検体情報を匿名化する．チューブに付されたコードと匿名化の際に発行されたバーコードの対応表を持ち，個人を特定することができる．一方で，検体ごとに対応表が作られるので，臨床研究用データの経時的な利用ができない．匿名バンク[9]は，個人識別情報と臨床研究用データに統一 ID を付すことで，個人の特定，経時的な利用が可能である．一方で，対応表を持たず，統一 ID により紐づけられているので，個人の特定が容易になる．DICOM 画像の個人情報保護のための匿名化システム[10]は，柔軟に匿名化ポリシの変更ができる．3 つの置換法があり，連結可能な置換法では，データ要素を符号化・復号する．しかし，システム内で符号化・復号しており，対応表の保持については想定していない．また，閲覧時の臨床研究用データと個人識別情報の結合についても想定していない．

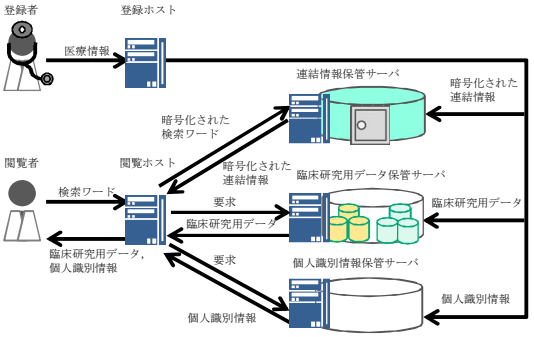

図 1 システムの構成

提案システムは，臨床研究用データと個人識別情報の関連付けた閲覧と臨床研究用データの経時的利用が可能である．また，連結情報が暗号化されているので，個人を特定できない．したがって，提案システムは他の医療情報を連結可能匿名化して保管するシステムと比較して，臨床研究で個人の特定が必要な場合に優れている．

6. おわりに

本稿では，個人識別情報に直接アクセスせずに，暗号化されている連結情報にアクセスすることで間接的に個人識別情報と臨床研究用データを連結する情報システムの実現に向けて，情報セキュリティの観点から脅威の分析をした．そのうえで，安全管理措置について検討し，連結情報を暗号化して保管し暗号文のままで参照できるようにすること，臨床研究用データと個人識別情報を直接結合せずに閲覧できるようにすることの二点を課題として抽出した．

これらの課題を解決する個人識別情報非可視型連結可能システムの構成を検討した．連結情報の参照では，登録の際に連結情報に検索タグを付しておき，暗号化した検索ワードと検索タグを照らし合わせられるようにした．臨床研究用データと個人識別情報の閲覧では，臨床研究用データと個人識別情報を直接結合せずに表示することで，医療情報を結合する手がかりや直接結合された実体が存在しないままで閲覧できるようにした．

提案システムは，情報セキュリティの脆弱な部分を突く脅威に対処できることを確認した．提案システムと医療情報を連結可能匿名化して保管するシステムを比較し，個人を特定しながらの臨床研究に優れていることを示した．

参考文献

[1] ナショナルセンター・バイオバンク・ネットワーク：ナショナルセンター バイオバンク ネットワーク プロジェクト(online)，入手先〈http://www.ncbiobank.org〉（参照 2012-11-26）
[2] 文部科学省，厚生労働省，経済産業省：「ヒトゲノム・遺伝子解析研究に関する指針」の見直しについて(2012)
[3] 日本医師会：医療情報システムを安全に管理するためのしおり，日本医師会 医療 IT 委員会(2010)
[4] 舘 剛司：外部の脅威に対するセキュリティ技術の動向，ビジネスコミュニケーション，Vol.43，No.10，pp.14-17(2006)
[5] JNSA セキュリティ被害調査ワーキンググループ：2011 年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～(online)，入手先〈http://www.jnsa.org/result/incident/2011.html〉（参照 2012-9-22）
[6] 厚生労働省：医療情報システムの安全管理に関するガイドライン(2010)
[7] 文部科学省，厚生労働省，経済産業省：ヒトゲノム・遺伝子解析研究に関する指針(2008)
[8] 日本システム開発株式会社：特殊匿名化システム(online)，入手先〈http://www.nsk.co.jp/dev/case/pdf/tokusyutokumeika.pdf〉（参照 2012-09-20）
[9] 株式会社 日立ソリューションズ：匿名化情報管理サービス 匿名バンク(online)，入手先〈http://www.hitachi-solutions.co.jp/tokumei〉（参照 2012-09-20）
[10] 鈴木 秀宣，天野 雅史，財田 伸介，久保 満，河田 佳樹，仁木 登，上野 淳二，西谷 弘：DICOM 画像の個人情報保護のための匿名化システム，電子情報通信学会論文誌，D vol.J91 - D，No.6，pp.1656-1662(2008)