# 医用画像の個人情報匿名化ソフトウェアの開発

The development of medical data anonymizing software

山本　啓二*　嶋田　康平*　永井　恒一郎*　塩見　伸幸*　馬場　大輔*　崎　浩典*

Keiji Yamamoto, Kohei Shimada, Koichiro Nagai, Nobuyuki Shiomi, Daisuke Baba, Hironori Saki

昨今の医療施設におけるDICOM画像によるディジタル化の普及に伴い、医用ディジタル画像の取扱いにおいて、医療機関、ならびに関連するメーカが意図することなく個人情報を漏洩してしまうことを防止する必要性がますます高まってきている。その状況下では、医用画像に含まれる個人情報を削除することで匿名化するための技術的なソリューションへの期待は非常に大きい。

我々は、医療支援分野における製品開発（Truedia®/XR等）を通じて医療現場での課題に直面し、医用画像に対するさまざまなノウハウを培ってきた。これらのノウハウを結実し、医用画像中の個人情報を匿名化するためのソフトウェアを、製品WhiteBerry®シリーズとして開発した。本書では、本ソフトウェアの技術的な概要について述べる。

Nowadays It had been very common to deal DICOM image data in medical institutions. Under that circumstances, for medical institutions and medical vendors, importance of the technical solutions to prevent compromising patients' personal information without any intent have grown increasingly. There is rising concern about a solution technology, DICOM data anonymization using automatic-deleting of personal information in medical image data among others.

The medical data anonymizing software package series "WhiteBerry®" our team has developed. We had studied various technical difficulties on dealing medical images in practice through the development of another product "Truedia®/XR" earlier. The applied technical know-how we achieved through the study made it possible to release "WhiteBerry®" series today. This article describes technological outline of the software package.

## 1．まえがき

⑴　個人情報保護法と医療現場の課題

2005年４月、個人情報保護法が全面施行された。同法の施行に伴い、患者等の診療データに含まれる大量の個人情報を取り扱う医療機関も、一般の事業者と同様に、個人情報の保護、そのための管理の強化が求められている。

各種検査装置（X線検査、CT検査、MR検査等々）で撮影される画像には画像そのものに加えて、患者や被験者の氏名、生年月日、年齢等、個人を特定し得る情報が、タグ形式で格納されている。これらの画像はディジタル化されていることで、ポータビリティ（可搬性）は向上しており、院内はもちろん、院外（他施設）との間でも効率的に相互流通させることで、医療の質と効率に寄与している。一方で、可搬性が高いが故に、その内部の個人情報の取扱いについて、より厳格な取扱いが求められている。

⑵　医療現場における個人情報

医療現場における、患者や被験者に関する個人情報は、大別して、以下の目的で取り扱われており、いずれも医療の質を維持／向上する上で、必要不可欠である。

⑷　患者や被験者の正確な識別

診断や検査での取り違えのようなミス・事故を予防するため、本人名での呼びかけや氏名確認は、医療現場における、重要な基本動作となっている。

⑸　医師の診断に対するインプット情報

既往歴はもちろんのこと、年齢および性別、家族構成や、親族の病歴等は、医師が、患者や被験者の症状や検査所見を、より正確に解釈／診断するため、医学的に重要な意味を持つ要素である。

⑶　当社開発ソフトウェアの意義

前項で示したとおり、患者や被験者にとって、より価値の高い医療サービスを実施するために、個人情報の利用は必須である。一方で、その医療サービスを提供する医療機関は、個人情報保護法が規定する個人情報取扱い事業者としての義務を負う。

＊関西事業部 情報通信システム技術部

当社が開発した個人情報匿名化ソフトウェア White-Berryシリーズは、前記個人情報保護法が規定する義務のうち安全管理措置（同法第二十条）に準拠したソフトウェアである。

## 2. ソフトウェアの概要と特長

ここでは、製品概要とその特長について説明する。

WhiteBerryは、すでに複数施設で利用いただいており、日常業務で使用されている。

### 2.1 ソフトウェアの運用例

本ソフトウェアは、主に以下に示す運用で用いられる。

⑴ 地域医療における病診連携（図１）

より精密な検査を行うため、拠点施設に対して、自施設の患者の検査を依頼する場合がある。また、自施設で検査した患者を、他施設へ紹介して診断を依頼する場合もある。

このような、医療施設間の相互運用において、施設間での画像の授受が頻繁に発生するため、この間の画像の運搬もしくは、伝送時に、画像に含まれる個人情報の匿名化／暗号化を行う。

⑵ 院内での画像長期保管

症例によっては、長期間の症例保存が義務付けられているものがある等のため、施設内で長期間、オフライン媒体（DVD−RAM等）で画像を保管する場合がある。

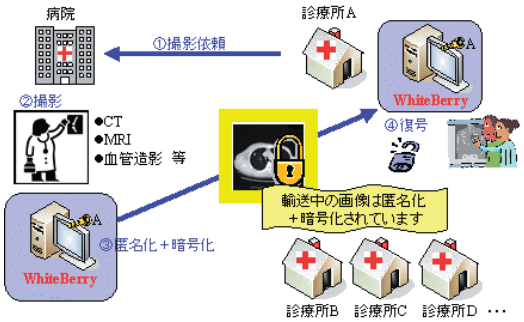


図１　WhiteBerry運用例（地域医療における病診連携）

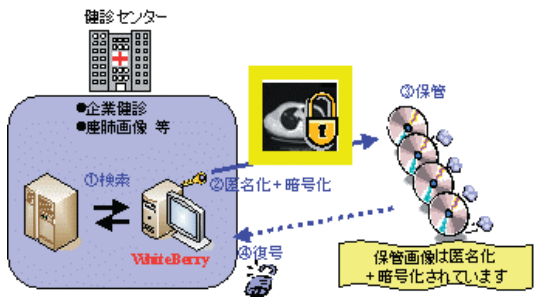


図２　WhiteBerry運用例（院内での画像長期保管）

この際に、画像に含まれる個人情報を暗号化することで、媒体の紛失、盗難時の情報漏洩を予防する。

### 2.2 ソフトウェアの機能概要

本ソフトウェアは、主に以下に示す機能を有している。本節では、各々についての概要を説明する。

⑴ 個人情報 暗号化
⑵ 個人情報 復号
⑶ 改ざん検知（真正性証明）
⑷ PACSサーバインタフェース
⑸ メディアインタフェース

⑴ 個人情報 暗号化

DICOM※1画像中の個人情報を抜き出し（これを、マスクする、と呼ぶ）、個人情報が除去された安全な画像（これを、マスク済みDICOM画像、と呼ぶ）と、個人情報データの２つに分離する。後者の個人情報データを暗号化することで、暗号化された個人情報と、個人情報が除去された安全な画像（万が一流出しても、個人が特定でき得ない画像）が得られる。

⑵ 個人情報 復号

暗号化された個人情報から、個人情報を復号し、マスク済みDICOM画像に注入してやることで、元のDICOM画像に復元する。

⑶ 改ざん検知

本ソフトウェアは、暗号化された個人情報に対して電子署名を添付することにより、個人情報の復号先となるマスク済みDICOM画像がマスクされた時点から一切変更されていないことを保証することができる。電子署名が一致しない場合、つまり、個人情報の復号先であるマスク済みDICOM画像が正しくないと判断される場合、個人情報の復号は行わない。

⑷ PACSサーバインタフェース

本ソフトウェアは、PACS※2サーバとの通信インタフェース（DICOM 3.0準拠）を備えており、ほぼ全ての各社PACS製品との画像通信が可能である。これにより、PACSサーバから検索したDICOM画像を暗号化したり、または、復号したDICOM画像をPACSサーバへ蓄積したり、といったような運用を可能としている。これにより、ある顧客で既に稼動中のPACSサーバと連接するような運用上のニーズがあった場合でも、新しい運用が容易に構築可能となっている。

※１　Digital Imaging and COmmunication in Medicineの略。医用画像に関するフォーマットと通信プロトコルの世界標準規格。

※２　Picture Archiving and Communication Systemの略。医用画像の蓄積装置を指す。

⑸　メディアインタフェース

本ソフトウェアは、DICOMが定める媒体入出力の規格（DICOM Media Storage）にも準拠しており、暗号化したDICOM画像を規格に準じてDVD媒体に書き出したり、また、DVD媒体から画像を読み込み復号したり、といった運用を可能としている。

### 2.3　ソフトウェアの技術要素

本節では、前節の機能を実現するための、本ソフトウェアのコアな技術要素として、以下の項目について述べる。

⑴　公開鍵暗号方式による情報暗号化
⑵　鍵管理
⑶　電子署名
⑷　画像と個人情報の分離

⑴　公開鍵暗号方式による情報暗号化

情報の暗号化には、公開鍵暗号（RSA：4,096bit）＋共通鍵暗号（MISTY1：128bit）を複合させた暗号方式を採用している。W－CDMAの標準仕様に採用され、事実上の世界標準である共通鍵型の暗号方式MISTY※3と、公開鍵暗号方式を組み合わせることにより、より強度の高い情報暗号化を実現している（図３、図４参照）。

⑵　鍵管理

本ソフトウェアでは、暗号処理のための情報（鍵）を、一種のデータベースである鍵リングファイルとして管理している。鍵リングファイルを通して、公開鍵（自分）、秘密鍵（自分）、および公開鍵（他者）と電子署名（自分）の組（複数）を管理することが可能である。（図５参照）

※３　MISTYは、三菱電機㈱の登録商標である。

⑴項で示した暗号方式は、復号先を明確に指定した暗号化を行うため、指定した相手以外のシステムでは、復号することができない。つまり、情報交換可能な組み合わせが、１対１に厳密に規定される。本ソフトウェアは、これらの組み合わせを複数管理することで、１システムが、複数の相手先を指定して、各々向けの暗号化を実施できる（１：多）。すなわち、本ソフトウェアを複数システム分導入することで、多対多（メッシュ状）の画像交換ネットワークを構築することができる。

⑶　電子署名

DICOM画像の暗号化時に、電子署名付きの認証コード（SHA－512）を付加し、画像復号時に真正性の検証を行うことで、医用画像の運搬、および伝送中に、内容の改ざんが行われていないことを保証している。また、

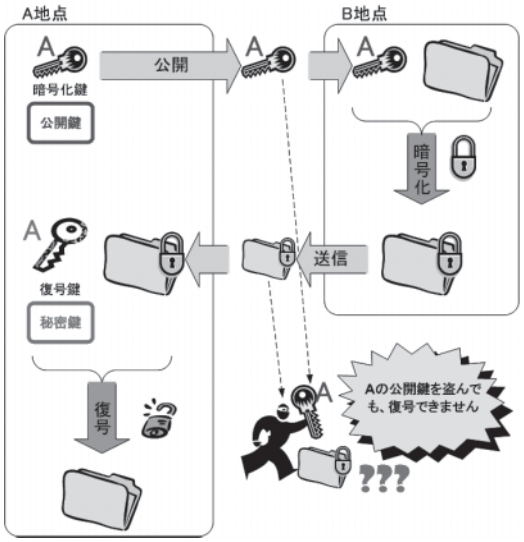


**図３　公開鍵暗号方式 概略**

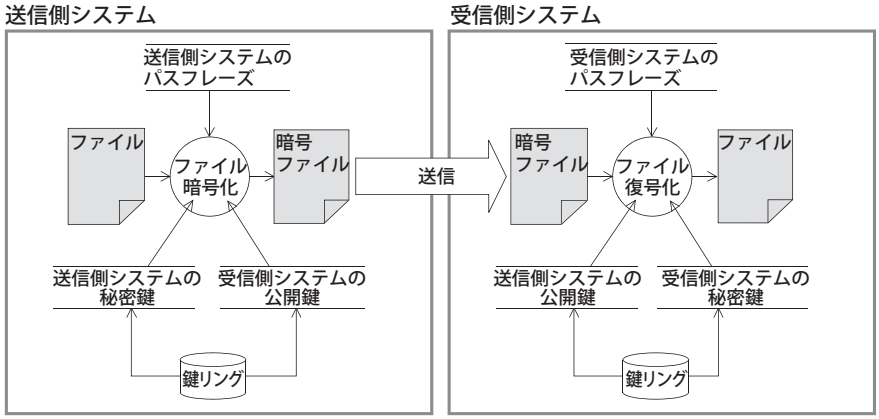


**図４　公開鍵暗号方式原理**

電子署名の内容から、情報提供者（画像送付者）の証明も可能である。（2.2（3）改ざん検知 参照）

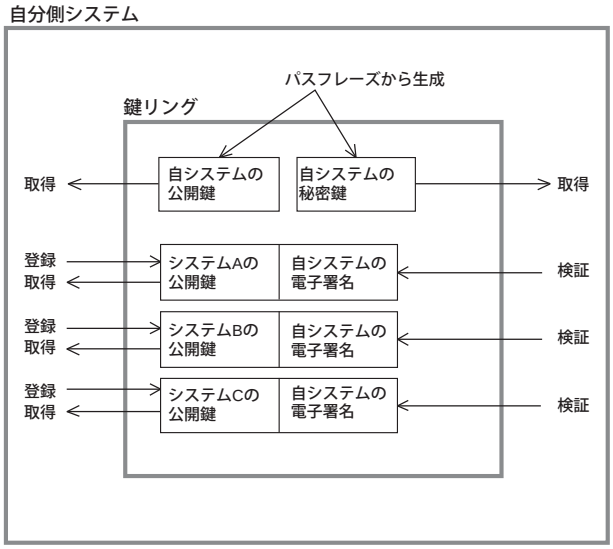


**図5　鍵リングファイルによる鍵管理の概要**

また、2.3（2）鍵管理にも関連するが、他システムから受領した他システムの公開鍵（他システムで暗号化された画像を復号する際に用いる鍵）そのものについても、電子署名により改ざんが無いことを検証しているため、他人になりすまして不正な鍵を交換させられることを防止している。

⑷　画像と個人情報の分離

本ソフトウェアでは、DICOM画像の暗号化を行う際、まず個人情報の抜き取り（マスク）を実施することで、画像と個人情報を分離する。この時、マスクする情報を、表1に示す。これらは、DICOM画像中に、タグ形式で格納されている情報である。これらの情報が抜き取られた後のDICOM画像には、元の情報の代わりに、匿名化された情報（例えば、患者名＝PAT001等）を埋め込む。これにより、万が一、画像が流出した場合でも、その画像が誰の検査画像であるかの特定ができないようになっている。

図6に、個人情報を分離して、暗号化／復号する様子を図示する。

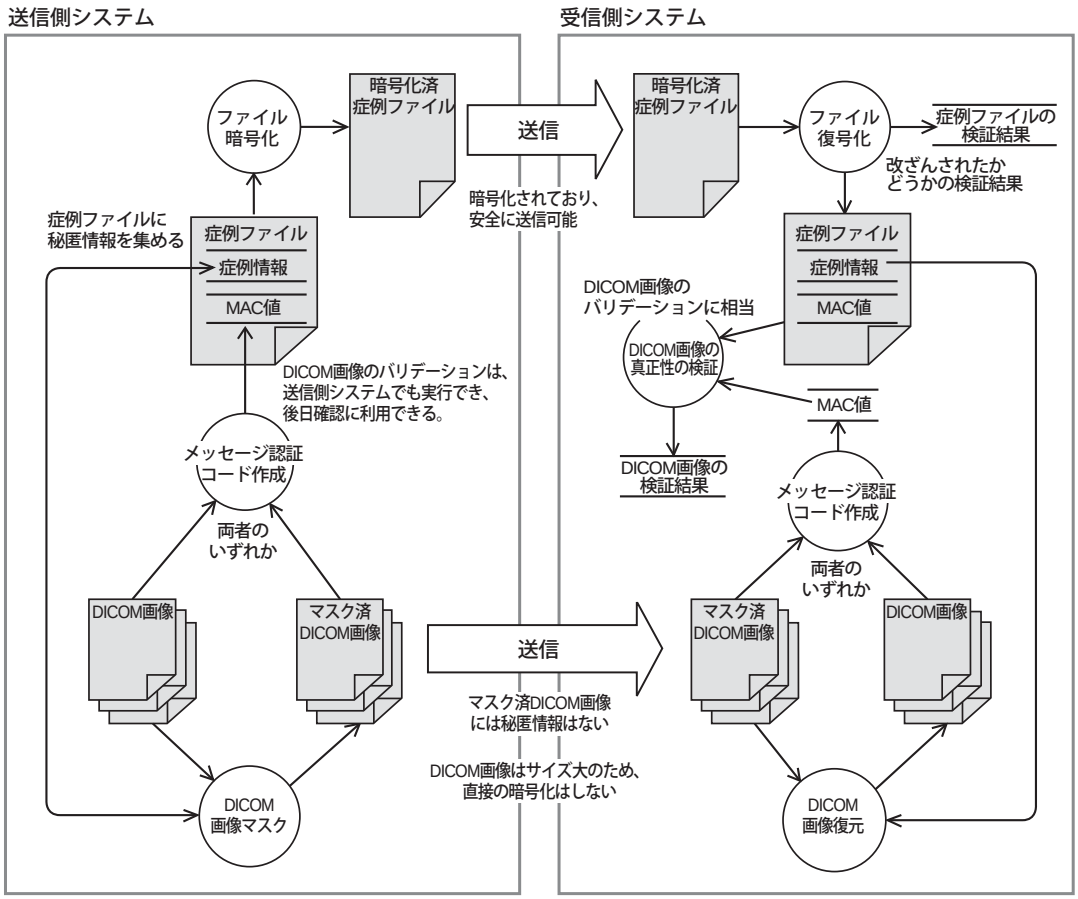


**図6　画像と個人情報の分離の仕組み**

### 3. 製品構成と他技術との関連

本ソフトウェアは、ユーザの用途に応じて、適用技術を取捨選択することで、３つの製品ラインナップを備えている。（表２参照）

・WhiteBerry　　：標準製品
・WhiteBerry/Lite　：機能限定版
・WhiteBerry/Client：簡易操作版

本ソフトウェアは、規制に対峙して課題を抱えるユーザに対して、当社の医療支援システム分野における保有技術の一つであるDICOMインタフェース技術の再利用（Truedia/XRより）、およびデファクトスタンダードである暗号技術MISTYとの融合から生まれた製品である（図７参照）。

表１　マスクするDICOM画像中の個人情報

| No | 情報種類 | |
|---|---|---|
| | タグNo. | 属性 |
| | 患者情報 | |
| 1 | （0010，0010） | 患者名 |
| 2 | （0010，0020） | 患者ID |
| 3 | （0010，0030） | 患者の誕生日 |
| 4 | （0010，0040） | 患者の性別 |
| 5 | （0010，1010） | 患者の年齢 |
| 6 | （0010，1001） | 患者名（別名） |
| 7 | （0010，4000） | 患者コメント |
| | 施設情報 | |
| 8 | （0008，0080） | 施設名 |
| 9 | （0008，0081） | 施設の住所 |
| 10 | （0008，1010） | 機器名 |
| 11 | （0008，1040） | 施設の部門名 |
| 12 | （0010，0021） | 患者IDの発行施設 |
| | 検査情報 | |
| 13 | （0008，1030） | 検査記述 |
| 14 | （0008，0090） | 担当医師名 |
| 15 | （0008，1048） | 記録医師名 |

表２　WhiteBerryシリーズ機能比較表（製品仕様書より）

| 機能 | | WhiteBerry | WhiteBerry/Lite | WhiteBerry/Client |
|---|---|---|---|---|
| 個人情報保護 | 個人情報匿名化 | ○ | ○ | ○ |
| | 個人情報の暗号化 | ○ | — | ○ |
| | 公開鍵方式による暗号化 | ○ | — | — |
| | パスワード方式による暗号化 | — | — | ○ |
| | Privateタグの削除 | ○ | ○ | ○ |
| DICOM対応 | 検索、保存 | ○ | — | — |
| | 取り扱い可能データ（CT、MR、CR、DX、RF、XA　他、DICOM3.0に準拠した画像） | ○ | ○ | ○ |
| その他 | DICOM Media Storage 準拠形式によるメディア・エクスポート | ○ | — | ○ |
| | 改ざんチェック | ○ | — | ○ |
| | メディアからのデータ取り込み | ○ | ○ | ○ |
| | データ保存先指定 | ○ | ○ | ○ |
| | 画像表示 | ○ | — | — |
| | 日本語対応 | ○ | ○ | ○ |

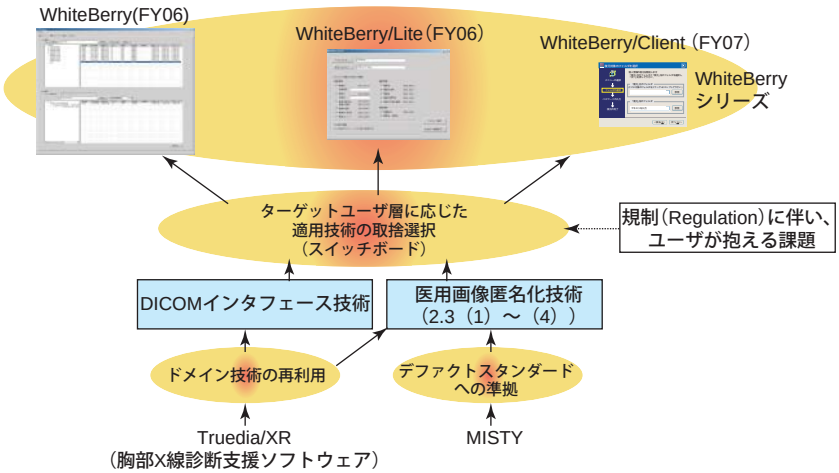


図７　製品構成と他技術の関連

### 4. むすび

当社が開発した、医用画像の個人情報匿名化ソフトウェアWhiteBerryシリーズの開発について述べた。本製品は、既存製品からの資産再利用を行うことで、ユーザが抱える課題に対して、製品化という形で素早く応えることができた。今後も、医療支援分野に限らず、要素技術の新規開発、保有技術資産の蓄積を行う一方、ユーザニーズに対して迅速に技術融合を行う形で、新たな製品開発を目指す。