計算システム工学分野

# 在宅医療介護情報連携システムにおける 連結可能匿名化とハイブリッド暗号を組み合わせたセキュアな個人情報管理手法

学籍番号 23413544 氏名　立田　太一
指導教員名　岩田　彰

## 1　はじめに

近年の急速な高齢化により，医療・介護サービスの利用者（以下，利用者と呼ぶ）は急速に増加している．住み慣れた自宅での療養・介護への高齢者のニーズは高く，今後推測されている高齢化の進展によって更なる利用者の増加が見込まれており，多職種・他機関の医療・看護・介護専門職により提供される在宅療養サービスにおいては，より一層の連携強化と効率的なサービス提供が求められる．このような状況の中で，本研究室では業務効率化や情報連携によるサービスの質の向上を目的として，多職種間情報連携を IT により支援する研究を行なってきた．

## 2　在宅医療介護情報連携システム「スマイルネット」

先行研究[1]により情報連携システムサーバ「スマイルネット」を中心に SaaS 型の連携機能の提供を行う方式が提案された．図 1 はスマイルネットシステムの概要を示したものである．スマイルネットでは，インターネット上に OpenVPN を用いてセキュアなネットワークを構築し，利用者の基本情報やサービス提供者の作成するサービス記録，他機関への連携情報等をサーバへ登録し，共有，連携を行う．

先行研究により開発が行われたスマイルネットシステムを用い，在宅療養支援診療所と訪問看護ステーションの間での情報連携について着目し，実証事業を行うことで有用性の確認を行った．今後はより多職種，多数の機関の参加による情報連携を実現していくことが期待されるが，そのような多数の機関が参加する連携システムにおいては，情報漏えいや改ざん等のリスクが高まることが予想される．そのため，プライバシーや個人情報保護の観点から特にサービス利用者の個人情報を保護する必要がある．情報システムにおける機密性の向上では暗号技術により，対象の情報を暗号化することが考えられる．しかし，利用者の基本情報だけでなく，個々のサービス記録の中にも利用者の氏名や生年月日などが含まれているため，リポジトリ内の全ての個人情報に対処するのは困難である．また，暗号化を行った場合には連携する複数の機関が適切に情報を復号できることが求められ，そのための暗号鍵・復号鍵の配送や管理が必要となる．その際，実用性やユーザビリティの観点から，鍵の管理等をユーザが意識せず，簡易な操作で開示先の制御を行えることが求められる．これらの課題を解決するためには次のような機能を満たすことが要件になる．

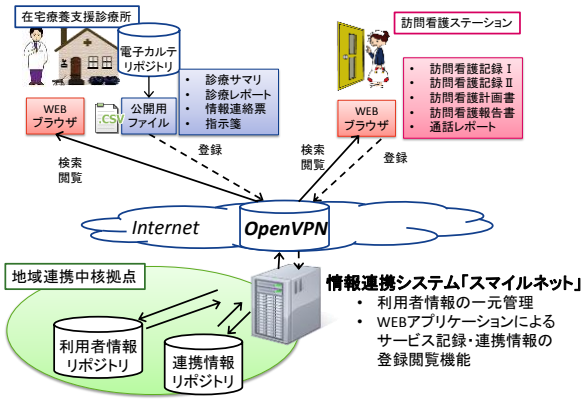


図 1　スマイルネットシステム概要図

［要件となる機能］

（個人情報保護）…リポジトリ内のすべての個人情報に対して暗号技術を用いて暗号化を行うこと．

（開示先制御）…暗号化を行った際に適切な暗号鍵・復号鍵の配送，管理を行うこと．簡易な操作で開示先制御が行えること．

本研究では，これらの要件を満たす個人情報管理を提案し，スマイルネットへの実装を行った．

## 3　提案手法

要件に基づき，連結可能匿名化とハイブリッド暗号を用いて個人情報の一元化及び安全な鍵の配送，管理を行う手法を提案する．図 2 は提案手法におけるサービス記録の登録と閲覧を表したものである．以下手順を説明する．

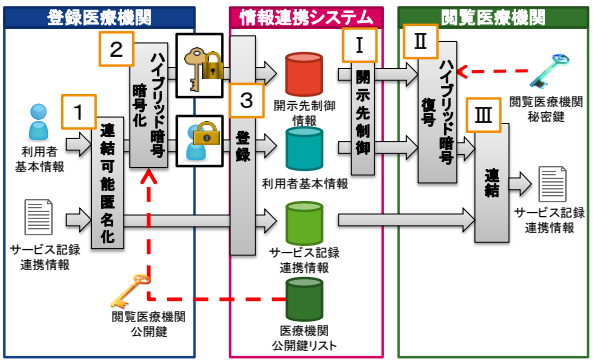


**図２　連結可能匿名化とハイブリッド暗号を用いた提案手法**

［情報登録手順］

1. 連結可能匿名化により，サービス記録・連携情報の匿名化を行い，利用者基本情報へと紐つけることで個人情報の一元化を行う．
2. 利用者基本情報を閲覧医療機関の公開鍵を用いて，ハイブリッド暗号方式により暗号化する．
3. 匿名化されたサービス記録・連携情報及びハイブリッド暗号方式により共通鍵暗号で暗号化された利用者個人情報と公開鍵暗号で暗号化された共通鍵を情報連携システムへ登録する．

［情報閲覧手順］

I. 開示先制御によって暗号化された利用者個人情報と暗号化された共通鍵を閲覧医療機関へ送信する．
II. 閲覧医療機関の持つ秘密鍵で共通鍵を復号し，共通鍵で利用者基本情報を復号する．
III. 利用者基本情報と匿名化されたサービス記録・連携情報を連結し，元のサービス記録・連携情報を復元する．

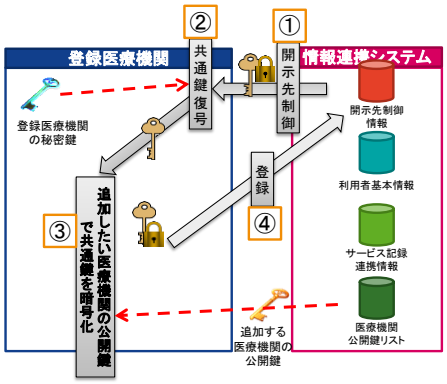


**図３　開示先の追加**

図3は開示先の追加について手順を示したものである．手順は以下の通りである．

［開示先追加手順］

① 開示先制御により暗号化された共通鍵を取得．
② 登録医療機関の秘密鍵で共通鍵を復号する．
③ 開示先に追加する医療機関の公開鍵を取得し，共通鍵を暗号化する．
④ ③で暗号化した共通鍵を開示先制御情報として登録する．

## 4　要件による評価

要件について，提案手法の実装を行ったシステム（スマイルネット2）とスマイルネットとの比較を行った．表1にスマイルネットとの比較を示す．

**表１　スマイルネットとスマイルネット2の比較**

| 要件＼ | スマイルネット | スマイルネット2（提案方式） |
|---|---|---|
| 個人情報保護 | ○ | ◎ |
| 開示先制御 | ○ | ○ |

スマイルネットでは，セキュアなネットワークの構築や認証システムの構築によって，一定の個人情報保護対策が行われた．提案システムではスマイルネットのシステム構築を踏襲し，さらに提案方式による個人情報の暗号化によってシステム内での個人情報の秘匿性の向上や情報漏えいへの対策を行った．また，個人情報の暗号化を行った際でも，ハイブリッド暗号方式の仕組みを利用して，個人情報の再暗号化や鍵の複雑な管理，配送の手間無く，開示先制御を行うことができる．

## 5　まとめ

本研究では多職種間情報連携が求められる在宅療養において，先行研究で提案された医療介護情報連携システム「スマイルネット」をより多職種，他機関で運用することを想定し，課題及び要件を整理した．そして，連結可能匿名化とハイブリッド暗号方式を組み合わせることで，リポジトリ内の個人情報の暗号化と，暗号鍵・復号鍵の配送，管理を行う手法を提案し，実装を行った．

今後の課題として，実運用を通して実証を行い，医療，看護以外の職種を含めた情報連携を行なっていくことが挙げられる．

## 6　参考文献

［1］堀田敏史，堀田賢司朗，白石善明，矢口隆明，岩田彰．“在宅医療・介護におけるセキュアな情報連携方式の一提案”．LOIS，ライフインテリジェンスとオフィス情報システム，110(450)：107-112，February 2011.