安全・安心・便利な情報サービス、システムに関する研究

大山 永昭 研究室

- 専門分野：医療情報システム，社会情報システム，光情報処理
- Home Page： http://www.isl.titech.ac.jp/~yamalab/
  http://asist.ssr.titech.ac.jp/

研究目的

ICカードや多機能ICチップを利用することで安全な情報交換を行う仕組みに関する研究、安全、安心に個人情報を管理できる情報システムに関する研究、画像処理に基づく暗号化を応用した生体認証に関する研究などを行っています。

研究テーマ

1．個人情報管理のための公的な情報基盤および情報サービスに関する研究

全ての国民が効率的で利便性の高い行政サービスや地域を問わず質の高い医療サービスを受けるためには、現在行政機関や医療機関等が保有し管理している個人情報を、本人が自らの必要に応じて取得・確認・利活用できるようにすることが不可欠です。本研究室では、上記のような取得・確認・利活用のできる安全確実な仕組み（社会情報流通基盤）を整備し、この情報流通基盤を用いて、例えば行政のワンストップサービスや生涯に渡る個人健康管理を実現し、その効果を明らかにするための研究開発に取り組んでいます。

具体的なテーマとしては、個人情報を管理する公的な情報基盤に関する研究として、多機能ICチップを利用することでインターネット経由での施設間の暗号通信を容易に構築できるオンデマンドVPNと呼ばれる技術の開発（図1）や、社会情報様々なサービスに共通で利用できる識別番号のあり方についての研究などを行っています。またこれらの情報基盤に関する技術を応用した情報サービスの研究として、個人の健康情報を生涯にわたって記録し、健康増進や医療の質の向上に役立てるための仕組みとして、PHR（Personal Health Recordの略）と呼ばれる個人健康情報管理システム（図2）を開発し、このシステムを利用した医療機関での実証実験などを行っています。

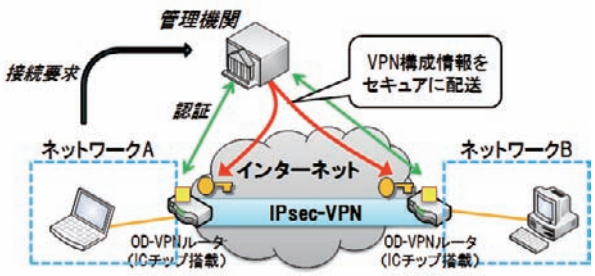

図1　オンデマンドVPN

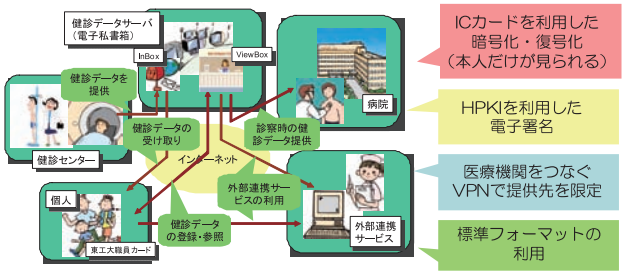

図2　個人健康情報管理システム

2．政府情報システムにおける調達の適正化に関する研究

現在の政府や自治体では、高度な情報システムの利用が一般的ですが、その調達および開発については、より適性な手法の開発が望まれています。その理由としては、システム導入前の段階で、発注者側である政府・

自治体で要求する業務フローと受注者側であるITベンダーで提供予定の情報システムが対応しているかどうかの判断が難しく、システム導入行程が計画通りに進められないことが大きな原因であると考えられます.このような課題に対し、発注者側と受注者側での意思疎通をスムーズにするための業務フロー記述手法として、ITに詳しくない人でも情報システムの処理内容が理解しやすいBusiness Process Model and Notation（BPMN）の利用が進んでいます。本研究では,このようなBPMNの利用を含め、政府情報システム調達における適正化のための指針について検討しています。また、具体的な業務事例として、個人を識別するための番号の利用等に関する法律案（マイナンバー法案）で規定される情報提供業務を実際にBPMNによって表記し、BPMNを利用する際の課題やその対策について研究しています。

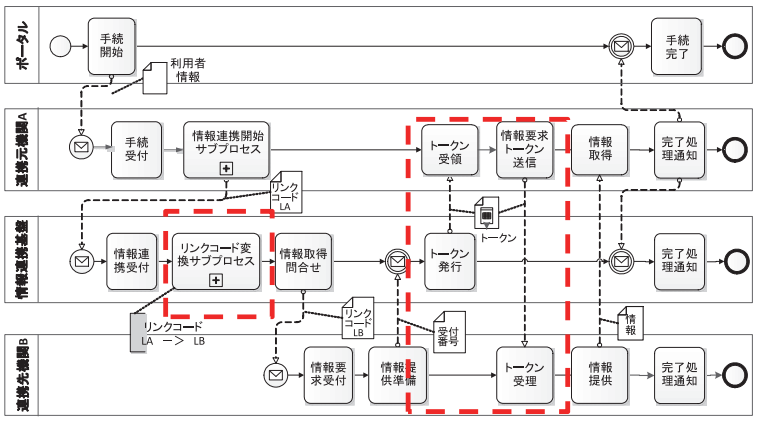

図3　BPMNによる業務フロー記述例

3. パターン認識と暗号の融合による生体認証技術

現在の生体認証は、ノートPCや入退室管理などの閉じた範囲での利用に留まっており、インターネットのようなオープンなネットワーク上での認証にはほとんど利用されていません。その理由は,生体情報の漏洩や、また一度漏洩した生体情報は交換することができないなどの問題があるからです。これに対し我々は、生体情報を暗号の鍵として利用する画像暗号化手法（図4）を開発し、この手法を応用することで、オンライン上でも安全に生体認証を実現する技術について研究しています。また、圧縮センシングと呼ばれる手法を用いることで、生体画像を秘匿した状態で取得し、生体情報を保護しつつ照合を行う技術（図5）の開発についても研究を行っています。

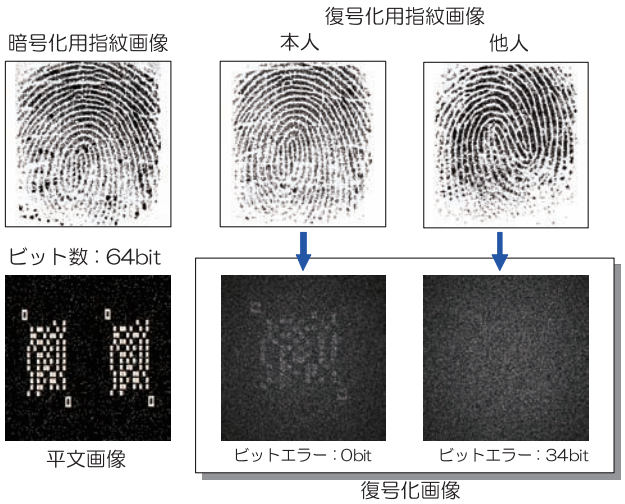

図4　指紋を鍵とする画像暗号化・復号化の例

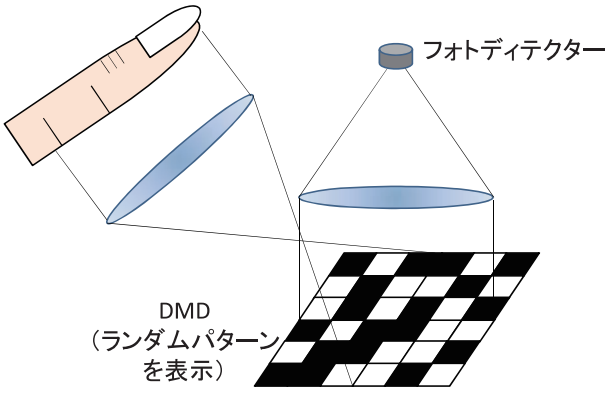

図5　圧縮センシングによる生体画像の取得

●参考文献

1. 御代川ほか：BPMNによる情報提供ネットワークシステムの可視化に関する研究；信学技報、112 (306)、pp.69-74 (2012).
2. H. Tashima, et al. : Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack; Optics Express, 18 (13), 13772-13781 (2010).