

視覚障害者に適したプライバシー保護方式の基盤構築

筑波技術大学 保健科学部 情報システム学科

岡本 健

キーワード：プライバシー保護，ID 情報，ペアリング，情報保障

現在、ICT 社会が浸透し、個人の身元を証明するのに生体情報を用いる方法が普及している。この方式は利用者の身体的特徴を利用しており、個人がその特徴を有しているかどうかにより、認証を行う。このような認証方式は、バイオメトリクス認証と呼ばれ、実社会における利用例として、銀行 ATM における手のひら認証や、研究機関で主に用いられている網膜認証等がある。これらの方式では、利用者は最初に本人の身体的特徴をセンタに登録する。このため、もし身体障害者がバイオメトリクス認証を利用する場合、以下のような問題がある。

- 障害に関する情報をセンタに伝える必要があり、利用者の精神的な負担、および著しいプライバシー侵害を導く。
- 身体的な部位の欠損により、認証処理が行えない場合がある。

他にも社会的、技術的な問題が多く残されている。このように現行システムは身体障害者に十分適用可能な方式には至っていないため、身体障害者の利用を考慮にいたった新しいプライバシー保護技術が求められる。

本研究では、実社会において視覚障害者がプライバシー侵害されないことない快適で効率的な方式を提案し、プライバシー保護に関する基盤技術を構築した[1-5]。本研究では、利用者を特定するために、生体情報とは属性情報を使用した。この情報は、ID 情報と呼ばれ、利用者の氏名や住所など、身体障害者に対して精神的負担にならない情報を用いることができる。

ID 情報を公開鍵暗号系における公開鍵として使用することにより、本研究では、以下のような認証処理を行うシステムを構築した。

- 初期段階：最初に利用者はセンタと直接手続きを行い、本人であることを確認する。センタは利用者に ID ベース暗号系に基づく秘密情報を発行する。この情報を公開鍵暗号系における秘密鍵として使用する。
- 認証段階：利用者は秘密鍵を用いて、センタと対話を行い、最終的に署名文を作成する。次に氏名などの ID 情報と共に署名文をセンタに提示する。
- 検証段階：センタは署名文が正しいかどうかを検証する。このとき、署名文が正しければ本人であると受理し、正しくなければ受理しない。

要素技術としては、「ペアリング」と呼ばれる楕円曲線暗号に基づく暗号系を用いる。本研究のアプローチとしては、

- 既存の福祉工学に基づくプライバシー保護技術に対し、伝送効率のよい方式の提案
- 従来は持っていなかった有益な特徴を持つプライバシー保護技術の提案

という流れで行った。また、ペアリングには、超楕円曲線上の双線形写像というものが提案されており、こちらを応用するとステップ数が通常の楕円曲線ペアリングよりも少なくなる可能性がある。ただし、1 ステップの演算量が楕円曲線上の演算よりも大きいため、この問題に対する解決策についても研究を行った。

参考文献

- [1] 岡本健，山口通智，三宅輝久，石塚和重，野口栄太郎，大越教夫：バリアフリーな CAPTCHA の基盤構築：視覚に障害をもつ医療系学生を事例として，暗号と情報セキュリティシンポジウム

- (SCIS2014), 4B2-1, 電子情報通信学会, 2014.
- [2] 山口通智, 岡本健: 人間ロボット判別テストのバリアフリー化のための言語的作問とその自然文生成技法, コンピュータセキュリティシンポジウム (CSS2013), pp.941-948, 3D3-3, 情報処理学会, 2013.
- [3] 山口通智, 中田亨, 岡本健: ユーザ認証での画像視認テストを代替する言語的テスト, 感覚代行シンポジウム 2013, No.4, 2013.
- [4] 山口通智, 中田亨, 岡本健: インターネット上に湧出する文章の特徴とそのチューリングテストのバリアフリー化への利用, 情報科学技術フォーラム(FIT2013), 第3分冊, pp.669-670, K-049, 情報処理学会, 2013.
- [5] 山口通智, 中田亨: 人間ロボット判別テストのバリアフリー化のための言語的作問技法, 情報処理学会研究報告, CSEC, コンピュータセキュリティ, 2013(30):1-8, 2013.