2007.03.09
Zero BIO

情報セキュリティマネジメントから見た生体認証の考察

情報セキュリティ大学院大学　　内 田　勝 也
Institute of Information Security　　Katsuya Uchida

１．はじめに

認証システムとして、パスワードが利用されてきたが、パスワードの問題点は 20 年以上も前から指摘されてきた．　このため、文字を記憶するためのパスワード以外の方法として、いくつかのものが提案されているが、その１つに生体認証がある．

生体認証は、利用者固有のものを利用することで記憶することもないため、非常に関心が高まっているが、いくつかの問題点も顕在化してきている．

本稿では、それらについて検討した．

２．個人認証について

情報処理システムでは、その利用者がシステムを利用する正当な者であるかを判断する方法を個人認証と言う．

個人認証を考える場合､以下の３つの要素があり、これらの１つあるいは複数を使って個人の認証を行う．

① 持っているもの(SYH: Something You Have)
② 知っているもの(SYK: Something You Know)
③ 自分自身(SYA: Something You Are)

ここで、「①持っているもの」には、磁気カードや IC カード等、個人に配布したものがある．

「②知っているもの」には、パスワードや暗証番号がある．パスワードや暗証番号以外に、「②知っているもの」として、最近提案されている位置記憶認証 （ピクチャーパスワード[1] 、画像パスワード[2]等）などがある．

「③自分自身」を利用するものが、本稿で述べる生体認証（バイオメトリックス認証）で、利用者の身体的なものを利用して認証を行う．

個人認証を行う場合、一般的には、利用者、認証サーバの二者間で行われるが、信頼できる第三者を含めた形で行われるものもある．

３．生体認証について

生体認証は、人間の体の一部を認証情報として利用する個人認証である．現在、生体認証としては、①指紋、②網膜、③虹彩、④顔、⑤静脈、⑥声紋、⑦DNA 等がある．システムの価格、大きさ、判断までの時間等の制約により、現時点で利用できる主なものは、指紋、指静脈程度である．

このような生体認証を利用する場合、生体認証そのもの及び、実装段階でいくつかの問題点も指摘されている．

3.1 生体認証自体の問題点

① アナログ型認証： 生体認証では、上記に述べた DNA を除いて、全てアナログ情報を利用している．このため、認証として利用するには、アナログ情報をデジタル情報に変換して利用している．

② 本人拒否率と他人受容率： アナログ型での認証であることに関連しているが､本人を拒否(本人拒否率）したり、他人を受容する（他人受容率）可能性をゼロにできない（図１）．

③ 標準的テスト手段： 各生体認証システムにおいて、認証精度についてはテスト方式を定めたものがあるが、装置全体をカバーしていない．静脈等や顔認証等の認証システムの精度評価方法[3][4]はあるが､各認証機器全てがこの方法を標準として利用しているとは限らない．このた

め、同一種類の認証機器の精度比較が適切行うことが難しい.

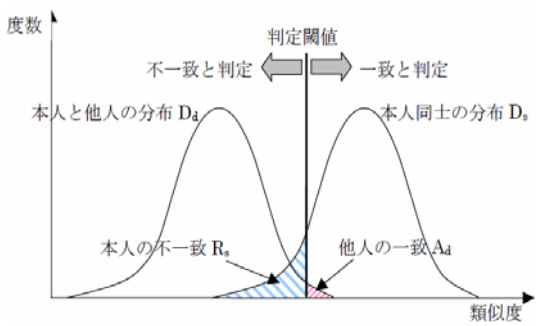

図１　本人拒否と他人受容の関係

（財）情報処理振興協会、「本人認証技術の現状に関する調査報告書」2003 年 より
・本人と判定する閾値の設定（中央縦棒の位置）により、本人を拒否（図のＲｓの部分）したり、他人を受容（図のＡｄの部分）することがある

3.2 生体認証の実装上の問題点

① 人体損傷の危険性： 人間の体の一部を利用しているため、その一部を切り取られる恐れがある．実際、2005 年 3 月にマレーシアで、指紋認証を利用している高級自動車の所有者が指を切り取られる事件[5]が発生している.
このような事件は、映画や SF の世界だけと考えられていたが、生体認証の利用は、こうした事件が現実の世界で発生する可能性があることを示している.

② システム利用不可能車の存在： 人間の生体を利用しているため、登録できない個人が発生することがある．このため、システム構築を行う場合、システムを利用できない人の取扱を考える必要がある．他の認証システムを代替手段として利用する場合には、代替手段のセキュリティレベルが、生体認証より低い場合には、システム全体のセキュリティレベルが代替手段と同じになり、生体認証を導入する意味がなくなることを考えておく必要がある.

③ 社会的受容性： ある種の生体認証システムでは社会的に受け入れられ難いものがある．例えば、指紋認証は、日本では刑法犯や外国人登録に長年利用されてきたため、指紋認証について社会的な受容性を高める必要がある.
このため、指紋認証システムを導入する場合、事前に十分な検討が必要になる.

④ 導入費用： 従来のパスワード方式から比べ、１端末当たりの導入費用が高い． 最近は、ノート PC 等に指紋認証等の生体認証装置が標準で導入されているケースも見られ、導入費用も急速に低下しているが、従来のパスワードから比較すると高価である.
また、サーバー（センター）側にも、特別なソフトウェアが必要な場合もあり、更に、費用がかかることがある.

⑤ 複数システムへの対応の困難さ： 複数システムで生体認証を利用する場合、各システムが生体認証を同一方式で対応していないと、複数のシステムで利用できないことがある.

⑥ システムの構築方法により、生体データが漏洩した場合、システム全体が崩壊してしまう可能性がある.

⑦ 偽造やなりすましなどを含めた生体認証への攻撃研究が進んでいないため、どの様な脆弱性があるかの研究が遅れている.

４．生体認証における課題の解消に向けて

数年前に社会問題化した磁気ストライプを利用した銀行のキャッシュカードの悪用対策として、生体認証が大きく注目され、多くの金融機関で導入がなされている．しかし、信頼できる認証システムとして生体認証が利用できるような環境を確立することが大切と思われる.

① 信頼性テストの確立： 一部の生体認証の精度評価方法が JIS 化されているが、全ての製品がこの方式を採用していない．各製品が標準化された評価方法を採用することが大切になろう.

② 生体認証がアナログ型の認証を行っている限り、本人が拒否されることがある。このため、その適用システムを十分に検討する必要がある. 現状の生体認証の導入システムをみる限りにおいて、必ずしも適切なシステムへの利用とは言えないものがある. このことは、長期的にみると、生体認証の信頼性を失う恐れがある.

③ 以上を含めて、生体認証及び、その導入のための基準あるいは、ガイドライン的なものの作成が課題であろう.

５. おわりに

認証システムとして生体認証は、多くの優位性を持っているが、最近の導入状況をみていると拙速の感がある.

生体認証の利用が適切でなければ、情報セキュリティを確保できなくなるだけでなく、生体認証自体の信頼を損ねることになる可能性があるのではないだろうか.

参考文献

[1] NIST, “Picture Password: A Visual Login Technique for Mobile Devices” http://csrc.nist.gov/publications/nistir/nistir-7030.pdf

[2] 鹿島一紀,“画像の位置情報による本人認証方式の研究開発　画像パスワード GATESCENE（ゲートシーン）”, 情報処理学会、コンピュータセキュリティ, Vol.2000 No.68, pp121-127, 2000 年 7 月

[3] JIS TR X 0079:2003 血管パターン認証システムの精度評価方法

[4] JIS TR X 0086:2003 顔認証システムの精度評価方法

[5] BBC News「Malaysia car thieves steal finger」http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

著者略歴

内田　勝也（うちだ・かつや）

電気通信大学 電気通信学部卒、 中央大学大学院理工学研究科修了. 博士（工学）

2001 年 11 月中央大学研究開発機構. 2002 年より、中央大学にて、21 世紀ＣＯＥプロジェクト「電子社会の信頼性向上と情報セキュリティ」事業推進担当、2003 年より、情報セキュリティ人材育成プロジェクトの推進等.

2004 年 4 月より、情報セキュリティ大学院大学 助教授. 2007 年 1 月より、教授. 情報セキュリティマネジメントシステム、リスクマネジメント、有害プログラム、検疫システム、情報法科学（Information Forensics）等の研究・教育に従事.