M-5　モバイル端末における多重インタラクティブ個人認証システムの提案

A Proposal of Multi Interactive Person Authentication System Using Mobile Phone

長谷 容子　青木 輝勝　安田 浩
Yohko Hase　Terumasa Aoki　Hiroshi Yasuda

東京大学大学院工学系研究科
Graduate School of Engineering, University of Tokyo

1．まえがき

インターネットの急激な発展により、情報ネットワーク・インフラは、従来の「便利さが優先されるフェーズ」から「社会のインフラとしての信頼性が問われるフェーズ」に移ってきていると言える。個人認証技術は、その信頼性を支える最も重要な技術の一つであり、これまでにもさまざまな研究がなされてきた。例えば、個人認証の方法として、「パスワード等の個人が持つ秘密情報を利用したもの」、「IC カード等の個人所有物を利用したもの」、「指紋等の個人固有の生体的特徴を利用したもの（バイオメトリクス）」、「手指動等の個人の行動特性を利用したもの」[(1)]等の検討が盛んにおこなわれている。しかしながら、従来の研究の多くは、それぞれ個人の手法の認証精度を向上させることを主眼にしたものが多く、ネットワークを利用したアプリケーションサービスを提供するシステムの一部として位置付けられる個人認証技術という視点から必要とされる機能や手法については、あまり検討されていない。

そこで本稿では、従来の個人認証技術における共通した課題とその解決の方向性について整理し、その解決の要件を満たす一つの具体的なシステムイメージとして、多重インタラクティブ個人認証システムを提案する。

2．従来の個人認証技術における課題と解決の方向性

従来の個人認証技術は、大きく「秘密情報による認証」、「所有物による認証」、「バイオメトリクスによる認証」に分けることができる。これらに共通した課題として、以下のことをあげることができる。

- 各認証技術ごとに、その特徴ゆえに 100%解決することが困難であるという本質的な課題が存在している。（例えば、秘密情報による認証では、パスワード等の秘密情報が簡単なもの（短いパスワード等）であれば破られる可能性が高く、複雑なもの（長いパスワード等）であると利便性が著しく低下する等）
- 常に単一の認証方法だけでは、悪意を持った第三者等によって、集中的な攻撃を受ける可能性が高く、破られる危険性が増す。また、実際に破られた場合のシステム全体への影響が大きい。
- 各認証方法において、付加的なハードウェア装置や設備等を併用することによって、セキュリティレベルを上げることが期待できるが、利便性は低下してしまうことになる。

そこで、本稿では、モバイル端末を利用した個人認証を考えるにあたり、これらの課題を解決するために、大きく２つの方向性をあげる。

（1）　トータルとしての認証精度やセキュリティ・レベルに配慮し、認証の方法や回数を複数にする。バイオメトリクスを組合せて認証する方法は、既に議論されているが、ここではバイオメトリクスだけに限らないで考えることにする。

（2）　モバイル端末が持つ特徴を考慮する。従来の固定端末（デスクトップ PC 等）にはなかった利便性や機能性を生かすとともに、弱点を補う配慮をする。

3．モバイル端末における多重インタラクティブ個人認証システムの概要と具体的な適用の例

２で上げた解決の要件を満たす１つの具体的なシステムイメージとして、本稿では、多重インタラクティブ個人認証システム（図１）を提案する。多重インタラクティブ個人認証システムは、以下のようなサブシステムと機能から構成される。

＜認証インフラ・システム（アプリケーション・サービス用）＞
（１）認証手段パレット・サブシステム
①パスワード認証機能、②PKI 認証機能、③バイオメトリクス認証機能、…
（２）認証手段設定サブシステム
①アプリケーション・セキュリティレベル管理機能、②クライアント認証環境判定機能、③認証精度設定機能、④認証手段組合せ設定機能
（３）認証結果判定サブシステム
①個別認証結果判定機能、②トータル認証結果判定機能

＜認証インフラ・システム（クライアント端末用）＞
（１）クライアント入力サブシステム
①利用者環境入力機能、②利用者認証申請機能

このシステムを具体的に適用した例として、以下のような認証方法をあげることができる。

＜例１＞サービス利用者が雑踏の中で携帯電話を利用した個人認証をおこなう場合
サービス利用者が、「自分が現在雑踏の中にいること」、及び、「利用したいアプリケーション名」をアプリケーション・サービスサイトへ伝えることにより、アプリケーション・サービス側でその特定のアプリケーションに要求されるセキュリティ・レベルを判断し、そのレベルに対応した認証精度や認証手法の組合せを設定

して、サービス利用者に指示する。認証手法の組合せとして、「指紋認証」と「耳の画像による認証」を選択した例を図２に示す。

＜例２＞サービス利用者が、あらかじめ予定していた特定の場所において、携帯電話を利用し個人認証をおこなう場合
サービス利用者が、「自分があらかじめ予定していた特定の場所にいること」、及び、「利用したいアプリケーション名」をアプリケーション・サービスサイトへ伝えることにより、アプリケーション・サービス側で、その特定のアプリケーションに要求されるセキュリティ・レベルを判断し、そのレベルに対応した認証精度や認証手法の組合せを設定して、サービス利用者に指示する。認証手法の組合せとして、「GPS の値、スケジュール・データ、特定の場所における画像データの照合によって認証」する方法を選択した例を図３に示す。

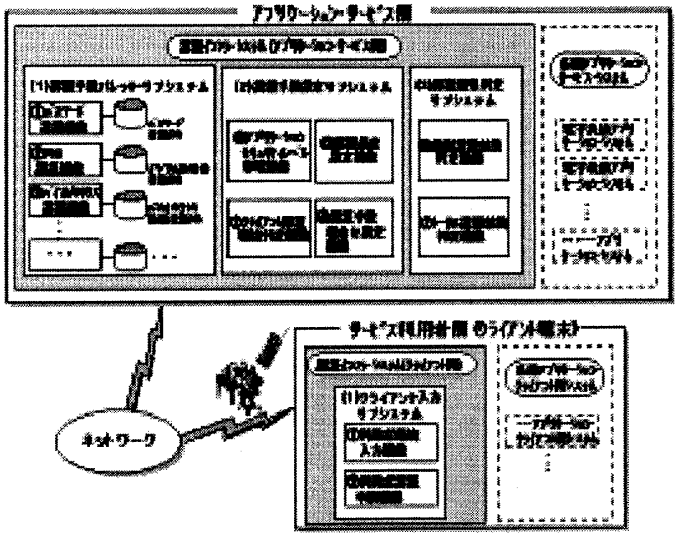
４．まとめ

本稿では、モバイル端末を利用して個人認証をおこなう際に考慮すべき用件を検討し、一つの具体的なシステム・イメージとして、「モバイル端末における多重インタラクティブ個人認証システム」を提案し、実際に適用した認証の例を示した。

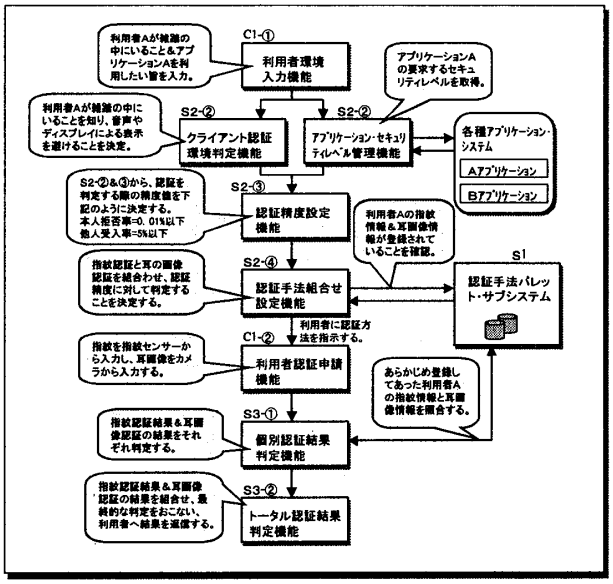
本システムによれば、認証手法の組合せによる効果だけでなく、モバイル端末という特性を積極的に利用した新しい認証手法のさまざまな実現が可能となる。

今後は、「安全性」、「利便性」、「経済性」、「社会的受容性」等の視点から評価実験をおこない、本システムの有効性を更に検討していきたい。

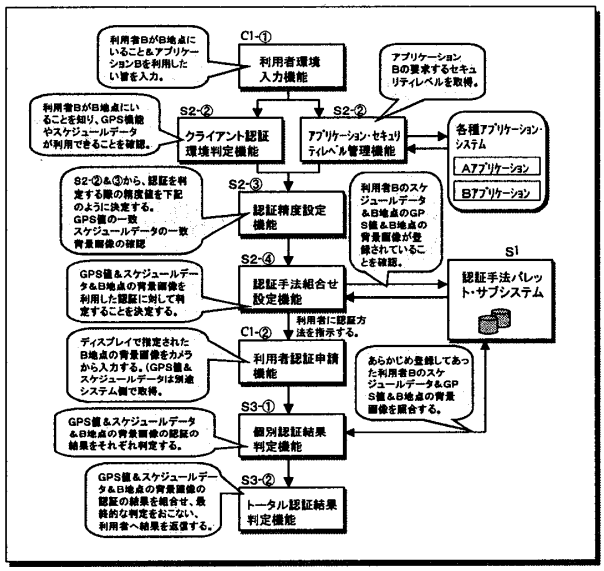
［図１］多重インタラクティブ個人認証システムイメージ



［図２］サービス利用者が、雑踏の中携帯電話を利用した個人認証をおこなう場合の例



［図３］サービス利用者が、あらかじめ予定していた特定の場所において、携帯電話を利用した個人認証をおこなう場合の例



［参考文献］

（１） 長田礼子，尾崎哲，青木輝勝，安田浩，“手指動からの特徴抽出によるリアルタイム個人認証“,電子情報通信学会論文誌 D-II, Vol.J84-D-II, No.2, pp.258-265, 2001.

（２） 坂野鋭，“バイオメトリクス個人認証技術の動向と課題“, 信学技法，PRMU99-29, pp. 75-82, June 1999.

（３） 長谷容子，青木輝勝，安田浩，“多重インタラクティブ個人認証システムの提案”電子情報通信学会 2002 年総合大会 A-7-14，2002.

（４） 長谷容子，青木輝勝，安田浩，“モバイル端末における多重インタラクティブ個人認証システムの提案” 電子化知的財産・社会基盤研究報告，2002.