生体識別技術のPKIへの適用に関する一考察

5T－1

辻　宏郷 、太田 英憲 、坂上　勉
三菱電機(株) 情報技術総合研究所

1. はじめに

PKI(Public Key Infrastructure)は、公開鍵暗号技術を用いて電子署名や暗号化を実現するための基盤技術である。一方、本人確認の手段として、生体識別技術を用いる認証機構に関する注目が高まっている[1]。本稿では、PKI における認証技術の一部として、生体識別技術を適用し、安全性および操作性を向上するための検討結果について報告する。

2. PKIと認証システム

2. 1 認証システムのモデル

ISOの認証フレームワーク標準[2]では、認証対象として、通信相手そのものを認証する場合(エンティティ認証)と、データ発信者を認証する場合(データ発信元認証)の二通りに分類しており、認証に用いる認証情報(AI: Authentication Information)として、以下の三種類の情報を定義している。

- **要求認証情報**(claim AI)
  認証要求者(認証を要求するエンティティ)のみが保有する情報。知識、保有物、身体的特徴など。
- **交換認証情報**(exchange AI)
  認証要求者と認証確認者(要求された認証を確認するエンティティ)の間で、認証を実行するために交換する情報。要求認証情報を元に、何らかの演算操作等を用いて作成する。
- **確認認証情報**(verification AI)
  認証確認者が、認証を実行するために、予め保有する情報。交換認証情報との間で、何らかの演算操作等を行うことで、認証を実行する。要求認証情報と同一の場合(例、パスワードや共通鍵)と、同一でない場合(例、公開鍵暗号の秘密鍵と公開鍵)がある。

2. 2 PKIにおける認証機構

PKI では、公開鍵暗号アルゴリズムの秘密鍵(Private Key)を用いた電子署名に従って、データ発信元認証やエンティティ認証を実現している。また、秘密鍵使用時に、鍵管理デバイス(ICカード等)のパスワードを用いた使用者のエンティティ認証を行うことによって、第三者による鍵の不正使用を防止している(図1)。

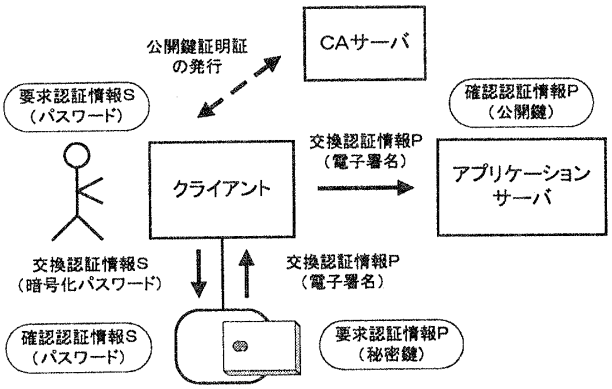

図1 PKIにおける認証機構の例

3. 生体識別技術を用いた認証機構

生体識別技術を用いた認証機構においては、生体識別情報入力装置を用いて認証要求者の生体識別情報(指紋等)を入力し、交換可能形式に変換した後(ベクトルデータ化)、認証確認者(認証サーバや認証判定プログラム)に送信する。確認者は、生体識別情報(指紋ベクトル化データ等)との間で判定処理を行い、要求者のエンティティ認証を実行する(図2)。

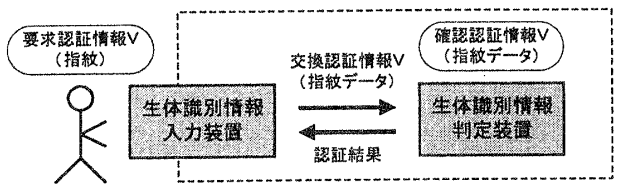

図2 生体識別技術を用いた認証機構の例

A Study of Applying Biometrics Technology to Public Key Infrastructure
Hirosato TSUJI, Hidenori OHTA and Tsutomu SAKAGAMI
Information Technology R&D Center, Mitsubishi Electric Corporation

4. 生体識別技術のPKIへの適用

4. 1 適用方針

一般に、情報セキュリティシステムにおける認証は、認証要求者のみが保有する複数の情報の組合せを用いて実現する。例えば、図1に示した PKI における認証機構では、パスワード(知識)とICカード(保有物)の組合せである。本節では、PKI における認証用情報の一つとして、盗用可能なパスワードの代わりに、認証要求者の身体的特徴(指紋、声紋、網膜など)に対する生体識別技術の適用例を検討する。

4. 2 適用モデルと評価

(1) クライアントで生体識別認証を行う場合

電子署名およびパスワードを用いた認証機構をそのままとし、パスワードの代わりに生体識別情報(指紋等)をユーザが入力可能とするモデルを図3に示す。本例では、クライアントにおいて生体識別判定を行い、判定に成功した場合、予めクライアントに埋め込んでおいたICカード用のパスワードを、自動的にICカードに送信する。クライアントの変更のみで実現可能であるが、生体識別判定用の情報およびパスワードを、クライアント毎に安全な形で保持する必要がある。

(2) 生体識別用認証サーバを設置する場合

(1)の変形として、生体識別情報に基づいた判定を行う認証サーバを別途設置するモデルを図4に示す。図1と図2の認証機構を組み合わせた形であり、生体識別判定用情報を一元管理可能となるが、認証プロトコルが複雑化し、パスワード管理は避けられない。

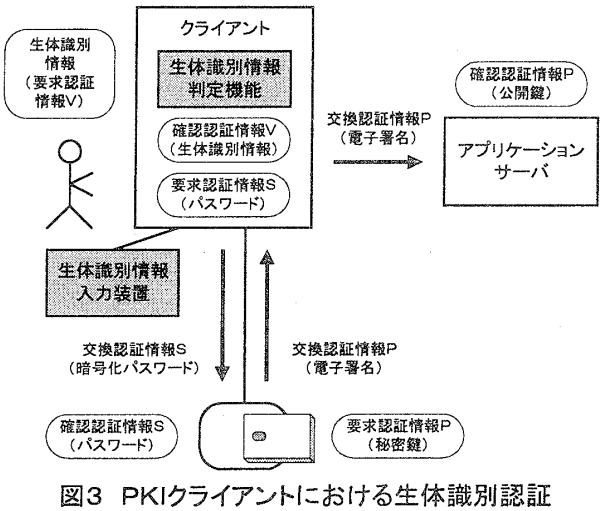

図3 PKIクライアントにおける生体識別認証

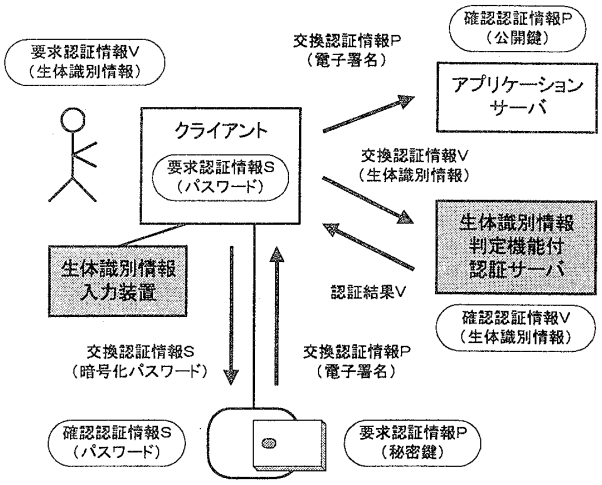

図4 認証サーバを設置した生体識別認証

(3) 生体識別機能付きICカードを使用する場合

生体識別情報に基づく認証機能をICカード上に実装し、パスワード管理を不要としたモデルを図5に示す。ICカードOS上のプログラミングが必要となるが、認証プロトコルを簡略化でき、かつ安全性も高い。

5. おわりに

PKI における認証技術の一部に生体識別技術を適用することを検討した。今後は、検討を継続すると共に、システムの試作を行う予定である。

参考文献

[1] 菅, "バイオメトリクス認証の動向", 第29回ECOMセミナー, 1999.

[2] ISO/IEC 10181-2, "Security frameworks for open systems: Authentication framework", '96.

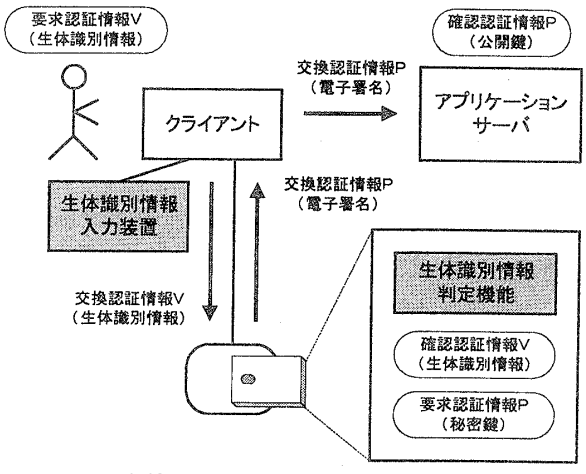

図5 生体識別認証機能付きICカードの利用