5G－9

指紋によるWWWアクセスシステムのセキュリティに関する一検討

中村 浩，馬場 義昌，貞包 哲男，藤井 照子，妹尾 尚一郎
三菱電機（株）情報技術総合研究所

1．はじめに

インターネットの急速な普及により，ネットワークを介して様々なサービスの享受が可能になってきている．このような多様なネットワークサービスでは，フリーなサービスばかりではなく，特定の個人を対象とした有料のサービスも多く，サービスの利用制限をするためのネットワーク上での個人認証が必須となっている．そこで我々は，バイオメトリクス（指紋）によって個人を認証するプラットフォームを提案し，WWWアクセスシステムへの適用を検討してきた．本稿では，指紋情報の取得から，指紋照合が行われる認証サーバまでのセキュリティについて検討を行ったので，報告する．

2．ネットワーク構成

指紋によるWWWアクセスシステムのネットワーク構成を，図1に示す．指紋取得装置(FPR)とユーザ端末間は，RS-232Cなどのシリアルインタフェースで接続され，ユーザ端末から認証サーバまでは，WANあるいはLANにより接続される．

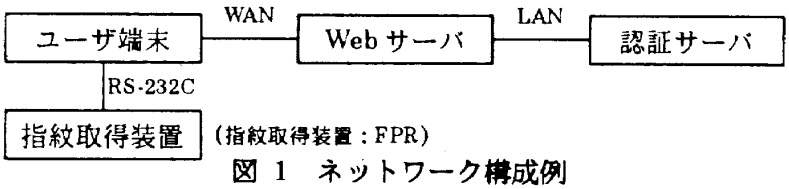

図 1 ネットワーク構成例

3．セキュリティ機能

主に，ネットワーク上での脅威に対抗するためのセキュリティ機能について記述する．

①FPR－ユーザ端末間　スタンドアロンでの使用を考慮すると，シリアルインタフェースに閉じたセキュリティ（暗号化・認証）の確保が必須である．暗号化機能の実現には，FPR内のCPUパワーを考慮し，計算量の少ない共通鍵方式が望ましい．また，乱数を使用したメッセージ認証も必要である．

②指紋情報の暗号化　FPRから認証サーバまでのトータルセキュリティを考慮すると，指紋情報の暗号化が必須である．FPRが多数設置される場合は，認証サーバの公開鍵で指紋情報の暗号化を行う公開鍵方式が望ましい．しかし，公開鍵方式は計算量が多いため，実装には工夫が必要となる．また，指紋情報のネットワーク転送時の盗聴や，Webサーバ上の不正（アプリケーションサーバ管理者の不正指紋情報の取得など）を考慮し，リプライ攻撃を不可能にする必要がある．

③システム管理　上記セキュリティを確保するためには，各種セキュリティ情報（鍵等）の設定・変更は，権限を与えられたシステム管理者のみが行わなければならない．しかし，指紋による認証だけでは，アクセスすることができなくなる恐れもあるため，パスワードによる初期化機能が必要となる．

4．まとめ

指紋によるWWWアクセスシステムのセキュリティ機能について検討を行った．今後，開発したシステムへ適用し，性能等を評価する予定である．

参考文献

[1] 貞包他：バイオメトリクスによるリモート個人認証のWWWへの適用，信学会 総合大会(1998).

Security Considerations of WWW Access System Using Fingerprints

Hiroshi NAKAMURA, Yoshimasa BABA, Tetsuo SADAKANE, Teruko FUJII, and Shoichiro SENO
Information Technology R&D Center, Mitsubishi Electric Corporation