指紋アクセス認証によるWebシステム

指紋認証機能付きUSBメモリ，情報通信，セキュリティ，指紋認証，USBメモリ，Web

＊西部保則　Yasunori Nishibe

概　　要

インターネットの普及に伴い増大するネットワーク被害を防止するために，情報通信セキュリティへの要求は日々高まってきている。当社はセキュリティ機器をSAFETYTUBE（セーフティチューブ）シリーズとして製品展開しており，その一環で今回Webシステムにおける個人認証システムを開発した。このシステムは，指紋認証機能付きUSBメモリをアクセス認証用のデバイスとして適用し，同USBメモリに登録された指紋の持ち主だけが，特定のページへアクセスすることが許可されるものである。また，もう一つの特長として，PC操作に不慣れなユーザを想定し，極力平易な操作で扱えるよう心掛けた。実際にはシステムインテグレータと協業して，健康・医療分野への導入も行った。今後，他分野への更なる導入を目指している。

指紋認証機能付きUSBメモリ

1. ま　え　が　き

インターネットの普及に伴い，通信経路上でのなりすまし・盗聴・改ざん・情報漏えいなどの被害が顕在化してくるにつれて，情報セキュリティへの要求が年々高まってきている。

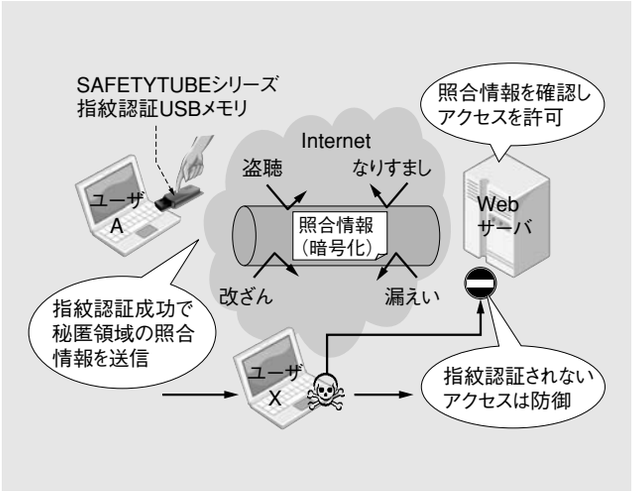
当社ではセキュリティ機器をSAFETYTUBE（セーフティチューブ）シリーズとして展開しており，今後の主力製品とする方針の下，研究開発を進めている。

今回紹介する指紋認証機能付きUSBメモリは，アクセス認証用として活用するネットワークセキュリティ製品である。Webシステムにおいて，アクセスをしてくるクライアント（ユーザ）が信頼できるかどうかをWebサーバ側で検証し，ユーザの要求に応じたページを漏えい防止及び情報の秘匿化を保ちつつ開示できるようにする技術は，医療・教育などの分野で非常に有用とされている。本製品は，まさにこの技術を提供するものである。

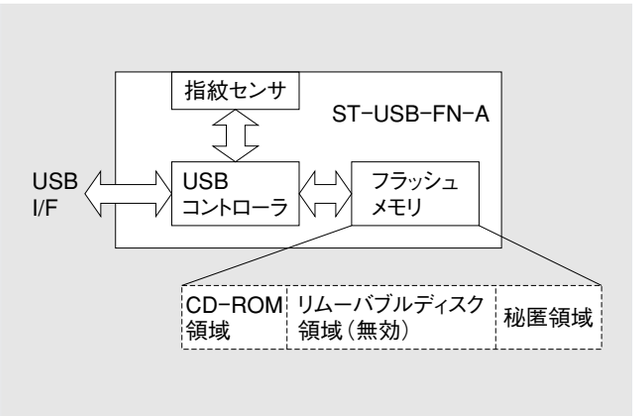
指紋認証機能付きUSBメモリをハードウェアトークンとし，あらかじめ登録された指紋の持ち主にのみ通信を許可する。ユーザは，管理者から支給されるUSBメモリにあらかじめ，自分の指紋情報とID情報を登録する。ID情報は指紋認証に成功しなければ，USBメモリ内から取り出すことはできない。取り出されたID情報は，Webサーバへ送信され照合される。Webサーバは，ユーザの要求に応じたページを表示する。通信経路の保護は汎用の技術であるSSL[注1]を利用するが，エンドユーザ個人を認証する技術を本製品が提供する。

本稿では，指紋認証機能付きUSBメモリのシステム構成や特長について紹介する。

＊電子機器工場



第 1 図　指紋アクセス認証によるWebシステムの構成
USBメモリの所有者にのみWebサーバへのアクセスを許可する。



第 2 図　指紋認証機能付きUSBメモリの内部構成
秘匿領域の情報は，指紋認証に成功しないと取り出せない。

2. システム構成

2.1　全体構成

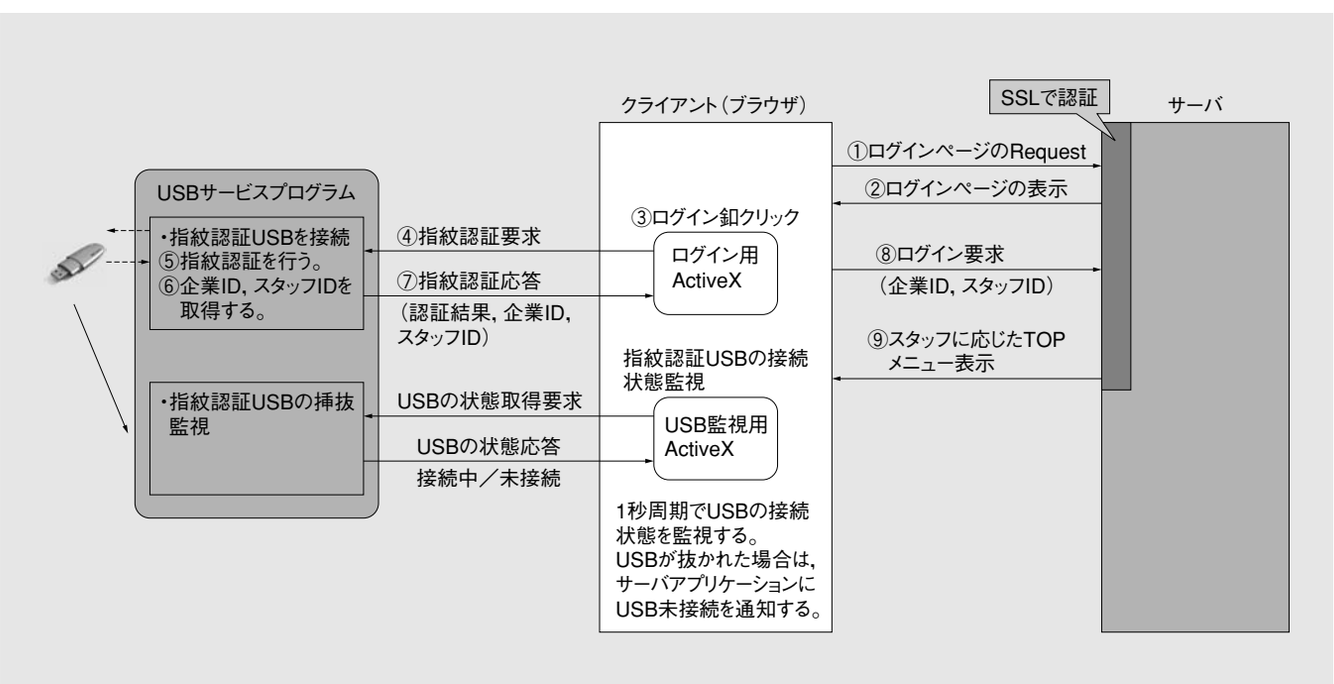
第 1 図にシステムの全体構成を示す。システムは，インターネットやイントラネットを介在して接続されたWebサーバとクライアント（Webブラウザ）で構成される。USBメモリは，クライアントPCに挿入して使用する。

2.2　指紋認証機能付きUSBメモリ

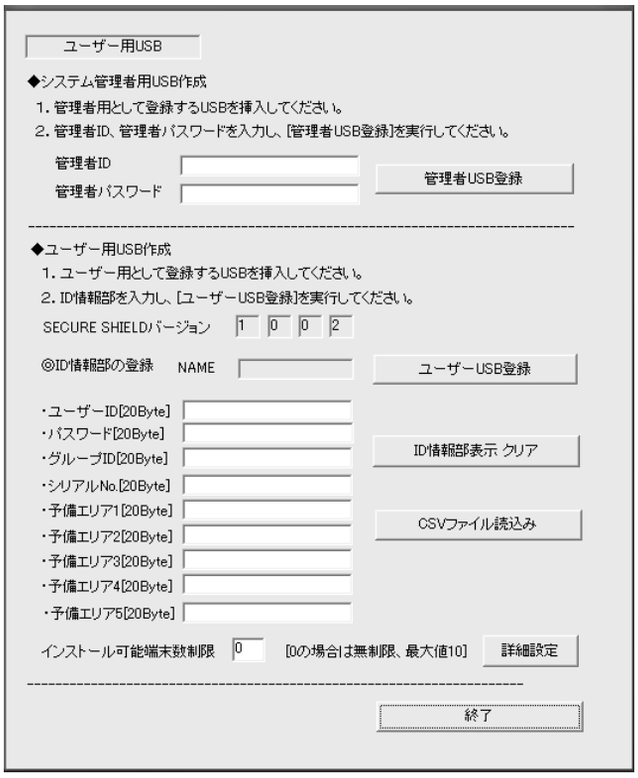
第 2 図に指紋認証機能付きUSBメモリの内部構成を示す。内蔵メモリの内，CD－ROM領域はCD－ROMとして認識される読み出し専用メモリでアプリケーションプログラムが格納される。リムーバブルディスク領域は，通常のリムーバブルディスクとして認識されるが，本装置では使用していない。秘匿領域は，ドライブとして認識されず，特殊なツールを使用して指紋情報やID情報が格納される。秘匿領域の情報は，指紋情報が一致しなければ取り出せないようにハードウェアによるインターロックの仕組みが備わっている。

2.3　プログラム構成

第 3 図にアプリケーションプログラムの構成を示す。アプリケーションはUSBサービスプログラムと2つのActiveX(注2)から構成され，それぞれが連携して機能を実現している。USBサービスプロ



第 3 図　アプリケーション構成
USBサービスプログラムとActiveXが連携して動作する。



第 4 図　認証用USB作成ツールの画面
USBメモリの秘匿領域にユーザのID情報を登録する。

グラムは，ActiveXからの要求に応じて，USBメモリの挿抜監視や指紋認証，及びID情報の読み出しを行う。ActiveXは，ユーザのWebページ上での操作に応じてブラウザから実行され，USBサービスプログラムと連携して個人認証機能を行う。

2.4　各種ツール

2.4.1　認証用USB作成ツール

第 4 図に認証用USB作成ツールの画面を示す。USBメモリの秘匿領域にID情報と属性情報の書き込みを行い，「システム管理者用USBメモリ」もしくは「ユーザ用USBメモリ」を作成する。本ツールはシステム管理者のみが所有・運用し，厳密に管理する。

2.4.2　USB指紋登録ツール

第 5 図にUSB指紋登録ツールの画面を示す。「ユーザ用USBメモリ」に対して，ユーザの指紋情報の登録を行う。本ツールもシステム管理者のみが所有・運用し，厳密に管理する。「システム管理者用USBメモリ」が無ければ使用することはできない。

3.　運　　用

3.1　Webサーバの構築

まず，ID情報照合の仕組みを実装したWebサーバを立てる必要がある。現在当社ではこの製品の販売に際して，I/F仕様を提供してユーザ（システムインテグレータなど）にWebサーバをご用意いただく導入形態を採っている。

第 5 図　USB指紋登録ツール
USBメモリの秘匿領域にユーザの指紋情報を登録する。

3.2　ユーザ用USBメモリの作成

システム管理者立ち会いの下，エンドユーザに指紋情報の登録をしていただくと共に，ID情報の書き込みを行う。作成したUSBメモリはエンドユーザに渡す。

3.3　インストール

エンドユーザがクライアントPCにUSBメモリを最初に挿入した時点で，自動的にインストーラが起動し，アプリケーションのインストールが行われる。

3.4　ログイン

エンドユーザは，USBメモリが挿入された状態で所定のログインページにアクセスをする。ログインボタンをクリックすると指紋認証が求められる（**第 6 図**）ので，USBメモリの指紋センサ部分を登録に使用した指でなぞる。指紋認証に失敗するとログインすることができない。指紋認証に成功すると，自動的に暗号化されたID情報がサーバへ送信される。サーバは受信したID情報を復号化して照合し，結果に応じたページを表示する。不正なID情報の場合は，エラーページが表示される。また，認証後USBメモリを抜くと，直ちに通信が遮断される。USB接続時のみ，アクセスが許可されるからである。

第 6 図　指紋認証画面
指示に従って，指紋センサ部分を指でなぞる。

第 1 表　サポートする動作環境一覧
指紋認証機能付きUSBメモリの動作環境を示す。

OS	Windows2000 SP4	WindowsXP SP2	WindowsVISTA
Web ブラウザ	IE6.0	IE6.0　IE7.0	IE7.0

3.5　メンテナンス

Webサーバ上にアップデート用のアプリケーションプログラムを置いておけば，メンテナンス用のActiveXを通じて，クライアントPCにインストールしたアプリケーションプログラムをリモートでアップデートすることが可能である。

4. 動　作　環　境

第 1 表に本製品の動作環境を示す。

5. む　　す　　び

指紋認証機能付きUSBメモリを使用した個人認証Webシステムを開発した。この技術は様々な業界への適用拡大が期待できる。

今後は，サーバの構築を含めたシステムインテグレーションサービスの提供も取り込みつつ，更なる導入を目指している。エンドユーザ数が増すにつれ，動作環境も多種多様に変化してくることは避けられない。このような環境は，従来当社が得意としてきた専用環境とは性質を異にした新しい分野である。この汎用環境における検証精度を，いかに高めていくかが今後の課題である。

（注記）

注1．SSL（Secure Socket Layer）：インターネット上で情報を暗号化して送受信するプロトコル。

注2．ActiveX：Microsoft社が開発したインターネット関連技術群の総称であり，ここではWebブラウザ上で動的なページを実現するActiveXコントロールを指す。

《執筆者紹介》

西部保則　Yasunoti Nishibe
通信機器ファームウエアの開発に従事