

# 指紋認証トークンシステム

ネットワーク上で利用できる情報サービスの拡大により、本人認証の重要性がこれまで以上に増す中、パスワードに代わる便利で確実な本人認証手段として指紋認証に対する関心が高まっています。ここでは、「いつでも」「どこでも」「登録した人だけ」が、さまざまなサービスを簡単に安心して利用できることをコンセプトとした、キーホルダサイズで個人専用の指紋認証トークンシステムについて紹介します。

すとう ひろき しげまつ きたし  
 首藤 啓樹 / 重松 智志  
 はた の たかひろ やまぐち ぶから  
 羽田野 孝裕 / 山口 力  
 あかざき ゆきお まちだ かつゆき  
 岡崎 幸夫 / 町田 克之

NTTマイクロシステムインテグレーション研究所

## 本人認証の重要性と生体認証技術の動向

インターネットやローカルエリアネットワークで提供される情報サービスを安心・快適に利用するためには、通信の安全を確保する暗号やPKI (Public Key Infrastructure) 技術に加えて、利用者の正当性を確認する本人認証が不可欠です。従来は、パスワード認証が本人を特定する手段として幅広く使用されてきましたが、パスワードは忘却を防ぐために誕生日、電話番号、家族の名前等の個人属性を含むことが多く、他人による推測が容易となる問題を含んでいました。

このような背景を踏まえ、忘れてたりなくしたりする心配がなく他人が本人になりすますことが困難な生体情報を使った本人認証技術に対する関心が高まっています。生体情報を利用した代表的な本人認証技術として指紋認証、掌形認証、顔認証、虹彩認証、署名認証、音声認証等があります。各種生体認証の認証精度、コスト、受容性（違和感や抵抗感なく利用できること）等の特徴を比較したものを表1に示します。生体情報を利用した

本人認証の中で、認証精度とコストのバランスという観点からもっとも実用化が進んでいるのが指紋を用いた認証技術といえます<sup>(1),(2)</sup>。指紋認証技術の主な適用分野を表2に示します。

据え置き型の指紋認証装置を導入した事例<sup>(3)</sup>はすでに報告されていますが、モバイル環境における本人認証の拡大に伴い、さらに多くの分野への適用が期待できます。

モバイル環境で、「いつでも」「どこでも」「登録した人だけ」が利用できる

指紋認証装置を実現するためには、従来型の指紋認証装置が持つ次の課題を解決する必要があります。

専用の認証ソフトウェアやドライバソフトウェア等がインストールされた特定のシステムでしか利用できない。

装置の大きさやケーブルの必要性等のため持ち運びには向きでない。

利用者の指紋データをシステム側が管理することへの不安感。

表1 生体認証技術の比較

生体情報	認証精度 (%)		コスト	使いやすさ	受容性
	本人拒否	他人受理			
指紋	-0.1	-0.1	低	高	登録に心理的抵抗感
掌形	-0.15	-0.15	中	高	容易
顔	1~	1~	中	中	容易
虹彩	-0.1	-0.001	高	中	登録に手間
署名	3~	3~	低	高	容易
音声	1~	1~	中	高	容易

表2 指紋認証技術の適用分野

分野	適用先
一般	入退室管理、自動車等の鍵、医療
電子機器	PC/PDAのログイン、データベースへのアクセス管理
電子商取引	ATM、自動販売機、キャッシュカード、クレジットカード、電子マネー、金融決済
行政	健康保険証、パスポート、運転免許証、各種証明書類

ここでは、指紋がパスワードの代わりとなり、携帯型で個人専用をコンセプトとする「指紋認証トークンシステム」について紹介します。

### 指紋認証トークンとは

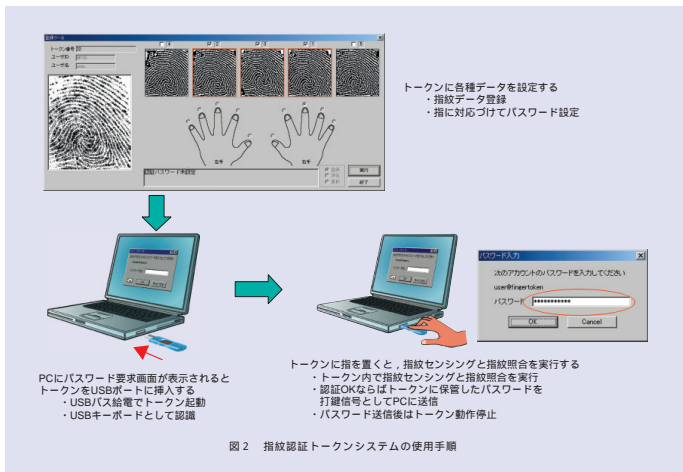
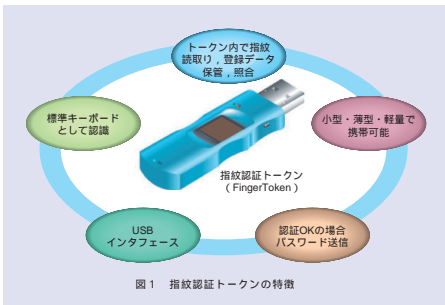
指紋認証トークン(FingerToken)は、指紋センシング、指紋データ登録および照合までの一連の処理を装置内で完結できる指紋認証機能を持った個人専用のパスワード保管ツールです。指紋認証トークンの特徴を図1に示します。

指紋認証トークンはPCのUSBコネクタに接続すると標準キーボードとして認識され、指紋センシングで得た指紋データとトークン内に保管する登録指紋データを照合します。指紋認証の結果、本人であると確認されると、

キーボードで入力したようにトークン内に保管するパスワードをPCに送信します。

その構成は、静電容量型指紋セン

サ、登録指紋データ保管用不揮発性メモリ、および指紋照合用CPUからなり、小型・軽量で携帯することができるのでさまざまな環境において便利



で確実な本人認証装置として利用可能です。

指紋認証トークンシステムの使用手順を図2に示します。指紋認証トークンを使用する際には、最初にトークン内に指紋データの登録と指に対応したパスワードの設定を行います。指紋登録を完了したトークンは、アプリケーション等の本人認証の場面において利用可能となります。アプリケーション等を起動しようとして、PCにパスワード要求画面が表示されたとき、USBポートにトークンを挿入します。トークンは指置き待ち状態となるので指を指紋センサ表面に置くと、指紋センシングと指紋照合が実行されます。本人であると認証されると、トークン内に保管する指に対応したパスワードがPCに送信され、アプリケーション等の起動が可能になります。パスワード送信後、トークンは動作停止状態となり電力を消費しません。

### 指紋認証トークンのメリット

指紋認証機能を持つ個人専用のパスワード保管ツールである指紋認証トークンを用いると「いつでも」「どこでも」「登録した人だけ」が安心して情報サービスを利用できる環境を実現できます。次に、指紋認証トークンが持つメリットを概説します。

従来のパスワード認証を用いたアプリケーションに簡単に指紋認証導入が可能

PC側に専用ソフトウェアやドライバソフトウェア等をインストールする必要がないので、従来のパスワードを用いるアプリケーションに指紋認証を簡単に導入できます。またパスワードを用いるアプリケーションを一切変更することなく指紋認証を導入することが可能なため、新たなシステム構築の必

要が全くありません。

さらに、固定パスワードだけでなく、指紋を暗証番号としてワンタイムパスワード<sup>\*1</sup>を生成する機能も内蔵し、より強固なセキュリティを要求されるシステムにも適用できます。

推測しにくい複雑で長いパスワードを用いることが可能

幅広く使用されているパスワードによる本人認証は、ランダムな文字の組み合わせで長いパスワードを設定することでセキュリティは向上するといわれていますが、実際には覚えやすいパスワードを使うか、あるいは複雑なパスワードを書きとめてしまうことが多く、セキュリティ上の弱点となります。指紋認証トークンでは、あらかじめ指紋データにパスワードを対応させて記憶させ、指紋認証が成功すると対応するパスワードがPCに送信されます。そのため、今までのように登録したパスワードを覚えたり、メモをとる必要もないので、従来のパスワード認証の持つ問題を解消できます。

また複数の指紋データを登録し、それぞれに異なるパスワードを設定できるので、アプリケーションごとに異なるパスワードを設定し、異なる指で認証させることが可能です。

指紋データは指紋認証トークン外に出ないので安心

登録指紋データは指紋認証トークン内に保管され、利用者が管理できるので、プライバシーを気にする利用者も安心して使用できます。また指紋センシングと照合処理も装置内で行われ、指紋データは装置外に出ないので指紋データに対する守秘性（情報が見られない、あるいは認められていない人によって引き出されることがない）に優れています。

優れた耐タンパ性

指紋認証トークン内に保管されている指紋データやパスワード等保護すべき個人情報への脅威（不正参照、不正改ざん等）に対処するため、指紋認証トークンではハードウェアとソフトウェアの両面から耐タンパ性<sup>\*2</sup>に優れた装置構成となっています。さらに装置内の個人情報は指紋認証により保護されており本人しか利用できないので、指紋認証トークンを安心して使用できます。

利用者に合わせて認証のカスタム化が可能

極端な乾燥指や多汗指、あるいは肌荒れ等、指先の状態により指紋照合率は影響を受けます。指紋認証トークンは個人専用のため、照合率が改善するように個々の装置の指紋読取り条件や照合条件を利用者に合わせて最適化することができます。

### 応用例と今後の展開

情報システムへのアクセスや情報サービスの利用において、本人認証の手段には強固なセキュリティが問われると同時に利便性の良さが求められています。従来の技術では両者を同時に満足させることは困難でしたが、指紋認証トークンを本人認証に使うことによりセキュアでユーザフレンドリな情報システムを構築することが可能となります。表3に指紋認証トークンシステムの主な仕様を示します。

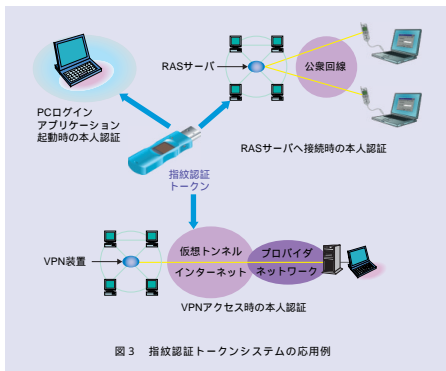
小型・軽量で携帯することができるので、自分専用のトークンを持ち歩き、

\*1 ワンタイムパスワード：認証のために1回しか使えない使い捨てパスワード。パスワードを盗まれても、2度と使用できないため、二次利用による攻撃を防ぐことができます。

\*2 耐タンパ性：外部からの不正アクセスによる装置内部データの参照や改ざんを困難にし、また不正アクセスの痕跡を残すことなどができること。

表3 指紋認証トークンシステムの仕様

機能	指紋センシング 指紋登録データ保管(最大10指) 指紋照合 パスワード送信(指ごとに最長63文字) ワンタイムパスワード生成
指紋センサ	静電容量型CMOS指紋センサ
外部インタフェース	USB1.1(バス給電)
動作環境	Windows98SE, ME, 2000, XP
認証時間	2秒以下/1指
サイズ	22mm x 75mm x 10mm
重量	17g



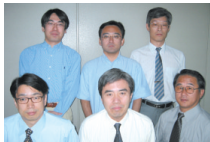
「いつでも」「どこでも」「登録した人だけ」がさまざまな情報システムにおいて、安心・快適にサービスを利用することができます。例えば、図3に示すように、PC端末における各種アプリケーションを起動するための本人認証、リモートアクセスサービス(RAS)サーバへアクセスする際のワンタイムパスワードを用いた本人認証、高セキュリティが要求される仮想専用網(VPN: Virtual Private Network)通信における本人認証に対して指紋認証ト

クンを適用することができます。

さらに、指紋による本人認証機能とワンタイムパスワードを組み合わせた便利で確実な本人認証システムは、インターネットや社内ネットワークを使ったサービスへの適用が期待できます。今後、指紋認証トークンを利用してユビキタスサービスへの幅広い展開を図っていく予定です。

#### 参考文献

- (1) 岡崎・久良木: "指紋を用いた本人認証技術の動向," NTT R&D, Vol.51, No.3, pp.189-193, 2002.
- (2) 菅: "個人認証・特定技術の現状と課題," 信学誌, Vol.85, No.6, pp.401-404, 2002.
- (3) <http://www.sw.nec.co.jp/library/jirei/nttdata/>



(後列左から) 重松 智志 / 羽田野 孝裕 / 首藤 啓樹  
(前列左から) 岡崎 幸夫 / 山口 力 / 町田 克之

利便性が高く安心して利用できる指紋認証装置の市場は、今後急速に拡大していくことが予想されます。タイムリなプロダクトアウトを目指し、指紋認証関連技術の研究開発を進めていきます。

#### 問い合わせ先

NTTマイクロシステムインテグレーション研究所  
第一推進プロジェクト  
TEL 046-240-2176  
FAX 046-240-2212  
E-mail suto@aec1.ntt.co.jp