技術レポート

指紋認証装置によるテスト環境構築および偽造指紋への耐性試験

指紋認証によってActive Directoryドメインへのログオンを行うテスト環境を構築した。また、ゼラチンによって偽造指紋を作成する実験を行い、指紋認証装置が偽造指紋にどの程度の耐性を持つのか、偽造指紋の作成がどの程度容易かを検証した。本稿ではその結果を報告する。

技術研究部　佐々木達也

1．生体認証技術

ある人が本当にその人なのかを確認する手続きが“認証”である。生体認証（バイオメトリクス認証）とは、生体的な特徴を計測して認証を行う方法だ。生体認証の最大の利点は、その人に固有の生体情報を認証に用いることで、他人による“なりすまし”が困難な点である。ほかにも、記憶や所有物が不要など、ユーザーへの負担が少ないという長所を持つ。

生体認証には、生体情報を読み取る装置が必要だが、この装置が高価だったことで普及を妨げていた。しかし、読み取り装置と認証ソフトウェアの低価格化・高性能化が進んでいる現在、すでに実用化されている入退出管理以外に生体認証を利用する例が増加している。ネットワーク上での本人確認にも生体認証は有効であり、ワークフローに生体認証を利用するなどのソリューションパッケージが販売されるに至っている。近い将来、携帯電話へ指紋認証装置が実装される計画もあり、生体認証の普及に拍車をかける可能性がある。

1.1　指紋認証

生体認証には各種の方式がある中、認証精度が高く機器が安価だという理由から、指紋認証が最も広く普及し得る方式であると言える。実際、現在販売されている生体認証装置は指紋認証装置の種類が最も豊富であり、この傾向は今後も続くと思われる。

指紋が生体認証に適している理由は三つある。

1. 指紋は“最も近い他人”である一卵性双生児でも異なり、世の中に同一の指紋を持つ人間が存在する可能性は870億分の1と非常に小さい。
2. 指紋は外傷に比較的強く、皮下組織のかなり深い部分まで傷が残らない限り、もとの指紋が復活する。
3. 読み取り装置に指を押し当てるだけで認証が行えるので手間がかからない。

一方、指紋認証には欠点もある。指にしわの多い人や手が荒れている人、指紋が磨耗している人は適切な指紋画像を採取できないために指紋認証を利用できない。このような人は一定の割合で存在するため、別の認証方式を提供することが必要になる。ただ、センサーとソフトウェアの進歩により、この問題はいずれ解決されることになるだろう。また、犯罪捜査のイメージから指紋認証に心理的抵抗感を持つ人もいる。プライバシー保護の観点から、指紋情報の管理には細心の注意を払うことが大切である。この問題に関しても、指紋認証が普及し、さまざまなサービスに有効に利用されるようになれば抵抗感は軽減されていくものと思われる。

2．指紋認証を用いたActive Directoryドメインログオン環境の構築

ネットワーク資源へのアクセスコントロールに生体認証を利用するモデルケースとして、指紋認証でActive Directoryドメインへのログオンを行うテスト環境を構築した。

2.1　指紋認証装置 FIU-710

今回テスト環境の構築に用いた指紋認証装置はソニー製のFIU-710というモデルである（FIUはFinger Identification Unitの頭文字）。 FIU-710は指紋画像を取得する方式として静電容量方式を採用している。

FIU-710には“指紋認証機能付トークン”という名称が

図1　FIU-710本体は、小型・軽量で携帯に適している

ついており、指紋の読み取りを行うと同時に物理的なトークンとしての役割も果たす。装置を所持しているユーザー以外はログオンが行えないため、安全性をより高める効果がある。本体は小型・軽量で携帯に便利なように作られており、PCと接続するUSBケーブルと一緒にソフトケースに入れて持ち歩くことができる。トークンとして機能させるために、常に身に付けるような使用が理想的である。

ソニーではFIU-710をPUPPYと呼んでいるが、本稿ではソフトウェアのPuppyと区別する目的で、FIU-710と呼ぶことにする。

2.2　指紋認証ソフトウェア Puppy Suite Version 2.0 Professional

FIU-710用のソフトウェアパッケージPuppy Suite Professionalは、クライアント/サーバー構成になっている。構成の概要を以下に示す。

・サーバーソフトウェア（以下サーバーPuppy Suite）

FIU-710とPuppy Suiteへのユーザーの登録を制御し、セキュリティポリシーを決定する。また、クライアントソフトウェア（後述）に含まれる全機能を備えている。

・クライアントソフトウェア(以下クライアントPuppy Suite)

ユーザーが使用するクライアントPCにインストールするソフトウェア。指紋によるログオンやファイルの暗号化/復号化などの機能を持つ。サーバーソフトウェアのUser Managerの設定によって､ソフトウェアの機能が制限される。

なお、パーソナル版のPuppy Suite Personalも存在する。こちらはサーバーソフトウェアがなく、インストールされたPCごとに完全に独立して動作する。そのため指紋の追加や変更に、管理者による制限を加えることができない。比較的小規模な導入に適したパッケージである。

2.3　Puppy SuiteとFIU-710における指紋情報の扱われ方

“指紋情報をネットワーク上に流さない”のがFIU-710およびPuppy Suiteの設計方針である。指紋照合作業はFIU-710内で完結し、照合結果のみがネットワーク上に流れる。このため、指紋情報をネットワーク上で盗聴される危険がない。

登録された指紋情報（以下テンプレート）はFIU-710のフラッシュメモリに記憶され、外部には取り出せない。よって指紋情報はFIU-710の所持者の責任で管理することになり、プライバシーにも配慮された設計だと言える。

2.4　テスト環境ネットワーク図

Puppy Suite ProfessionalのWindowsログオン機能を利用して、指紋認証によりActive Directoryドメインへのログオンを行うテスト環境を構築した。

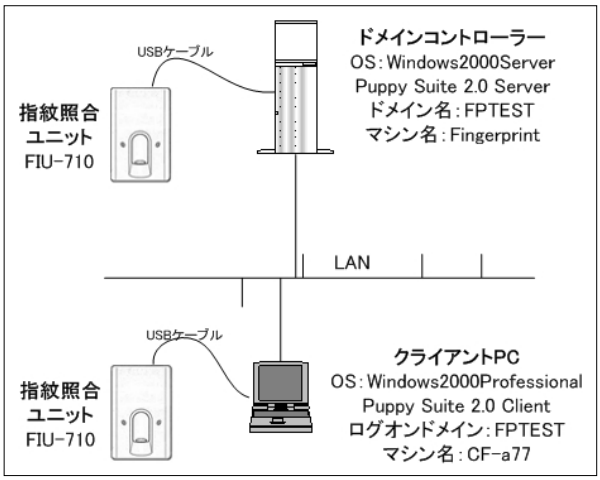


図2　テスト環境ネットワーク図

Windows2000ServerでActive Directoryドメイン（ドメイン名：FPTEST）を構成し、クライアントはノートPCでActive Directoryドメインへのネットワークログオンを行う。ドメインコントローラとクライアントマシンの間はLANで接続した。クライアントマシン、サーバーマシン共に指紋認証によるログオンを行う。

サーバーPuppy Suiteのインストール先はドメインコントローラ上である必要はない。サーバーPuppy Suiteの主な機能はクライアントPuppy Suiteの動作を制御するための情報をFIU-710内に埋め込むことであり、Active Directoryとは直接やり取りを行わない。

2.5　Puppy Suiteのインストール

下準備として、クライアントPCがFPTESTドメインにパスワードでログオンできる通常の環境を構築しておく。つまり､FPTESTドメインのユーザーとしてクライアントPCのユーザーをドメインコントローラ上に登録しておく。

次に、インストール前にセキュリティポリシーを決定しておく。クライアントPCからFIU-710を取り外した時の動

作（スクリーンセーバーの起動・強制ログオフ・シャットダウン・何もしない）をはじめ、設定できる項目は多岐にわたるので、詳細はマニュアルを参照して事前にどのように設定するかを決めておく。

最後にソフトウェアのインストールを行う。

このインストール手順からもわかるように、現在稼動中のActiveDirectoryドメインに指紋認証を追加するようなイメージである。

2.6 ログオンの手順

ここではログオンの手順と認証情報の流れを説明する。図3にある(0)から(5)の流れに合わせて見てほしい。

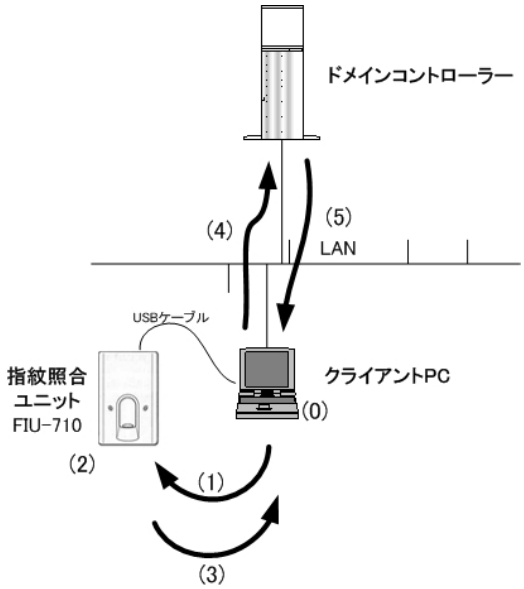


図3　ログオン時の情報の流れ

(0) クライアントPCでCtrl+Alt+Delを押すとログオン画面が出る。なお、この時点でFIU-710が接続されていないとログオン画面が表示されないのでFIU-710がトークンとして働いていることを確認できる。

(0)Puppy Suiteのログオン画面

(1) FIU-710のシャッターを開けると指紋照合ユニットが入力待ち状態になる。

(1)照合作業を促すPuppy Suiteの画面

(2) FIU-710に指を乗せて指紋照合作業を行う。

(2)FIU-710に指を乗せる

(3) テンプレートと入力指紋の照合に成功すると、照合成功の応答を返す。

(4) FIU-710内に保存されているWindowsパスワードとユーザー名を用いて、通常のWindowsログオンを行う。ログオン先もFIU-710内に保存されているドメイン名によって決まる。

(5) Windowsログオンが許可される。

このように、指紋情報は通常のActive Directoryドメインへのログオンが行われる直前でユーザーの確認を行うためにのみ利用され、ネットワーク上を流れることはない。

(5)Puppy SuiteからOKが返される

2.7　実際の使用感と指紋画像登録時の注意点

指の乗せ方のコツは誰でもすぐに掴むことができるだろう。筆者の場合、指紋登録時のサンプル画像採取の6試行が終わった時点でだいたいの感じは掴めた。

ただ、慣れるとどうしても乗せ方がいいかげんになってくるので、登録時に指を強く押し付けてテンプレートを作ると慣れた後の本人拒否率が大きくなってしまう恐れがある。よって、登録時にはセンサー部に軽めに指を押し当てるのがコツである。登録前に指の置き方の練習もできるので、感じを掴んでから登録作業を行うといいだろう。

さらに、登録時に指を軽く乗せたほうがよい理由はもう一つある。マニュアルには「使用中は暖かくなりますが、異常ではありません」との記述があるが、これは少し控えめな表現で、数回連続して照合を行うとセンサー部がかなり熱くなる。指を強く押し当てるのが少々不快に感じるほどの発熱だ。よって、軽く乗せても照合が成功するように、テンプレートの登録時には指を軽めに乗せるほうがよい。

3．偽造指紋への耐性試験

横浜国立大学の松本勉教授らによって、ゼラチンで作った偽造指紋を用いて指紋認証装置をだますことができるという報告がされている（本稿末尾の参考文献より）。これがどの程度簡単なのかを確認するために、実際にゼラチン偽造指紋を作成し、今回構築したテスト環境で照合が成功するかどうか試みた。

3.1　材料と作成方法

・粉末ゼラチン「ゼライス」（マルハ）
　30g、約200円
・板ゼラチン「ゼラチンリーフ」（マルハ）
　30g、約200円
・熱可塑性樹脂「自由樹脂」（ダイセルファインケム）
　35g、約350円

ゼラチンはどこでも手に入る通常の食用のものである。豚の皮から抽出するゼラチンは生体材料であり、人間の皮膚と物性が似通っている。

自由樹脂は60℃以上に加熱すると軟らかくなり、常温で硬化する多目的樹脂である。これも、ホームセンターや模型店などで誰でも簡単に入手することができる。

なお、安全への配慮から偽造指紋作成方法については省略する。以下の文章でも、作成法に関する詳しい記述は避ける。

3.2　結果

照合の確認はPuppy Suite付属の指紋照合テストを利用して行った。これを用いると照合レベルが0〜100のスコアとして画面上で確認できる。Puppy Suiteで設定する1〜5の照合閾値と照合レベルとの関係は表1の通り。閾値5が最も“厳しい”設定である。なお、この情報はマニュアルには記載されておらず、ソニーの担当者から直接聞いたものである。

通常の運用では、照合閾値を3程度に設定するため、偽造指紋がスコアで30以上を出すかどうかが一つの評価基準となる。

表1　照合レベルと照合閾値

照合閾値	照合レベル
1	10以上なら照合成功とする
2	20以上なら照合成功とする
3	30以上なら照合成功とする
4	40以上なら照合成功とする
5	50以上なら照合成功とする

3.2.1　作成開始初日

最初にできあがった偽造指紋は使おうとした時点で溶けはじめ、照合装置に載せるまでに至らなかった。

最初の失敗を踏まえ、作成法を変えて完成したものを照合装置に載せたところ、センサー部の熱によって物凄い勢いで溶け始めた。図4がその時の画像である*1。左が生体指による画像で、これが照合のテンプレートである。右が偽造指による画像で、中央に照合レベルのスコアが表示される（中央の犬はマスコットキャラクターのPUPPY君）。右の画像から、溶けたゼラチンがセンサー部を覆ってし

図4　偽造指がセンサー部の熱によって溶けてしまった

＊1）プライバシー保護のため、指紋画像部分の一部を意図的に隠している。

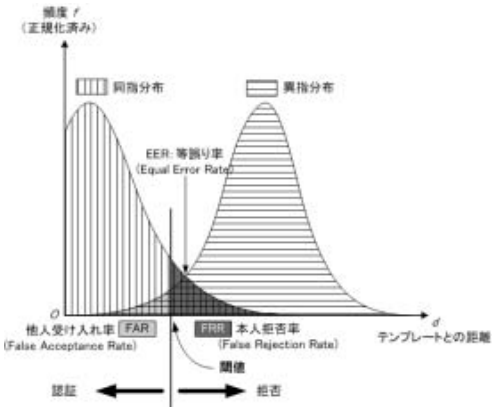
認証精度が確率で示される理由

バイオメトリクスによる認証では、指紋や虹彩などのアナログ計測データに対するパターンマッチング処理が基本であり、統計的な誤差が避けられない。たとえば指紋認証では、指の湿り具合や汚れ具合によって入力データが変動し、同一人物でも照合結果が常に同じになる保証はない。このため、登録されているテンプレート(生体情報データ)と、入力データが一定以上の類似度であれば本人であると認める、ということになっている。

この図は、生体認証の典型例として指紋認証の精度について説明している。

図の横軸は登録されている指紋データ(テンプレート)と、入力されたデータとのハミング距離※を表す。この距離はテンプレートとの一致度を示している。縦軸はその頻度である。テンプレートを登録した指による分布が同指分布、それ以外の指の分布が異指分布だ。閾値より距離の小さいデータが入力された場合は本人と認め、そうでない場合は他人として認証を拒否する。

テンプレートの情報量は有限なので、同指分布と異指分布には重なりが生じる。これにより誤って他人を受け入れてしまう確率(FAR：他人受け入れ率)と、誤って本人を拒絶してしまう確率(FRR：本人拒否率）が生じる（ただし、この図は重なりをかなり誇張して表現していることに注意)。バイオメトリクス製品の認証精度はこれらの確率で評価される。



他人受け入れ率と本人拒否率

距離ではなく一致度をそのまま指標とする場合もあるが、一致度＝最大距離－距離という簡単な関係で結ばれる。Puppy Suiteの“照合レベル”は一致度の一種である。

※2つの値がどれだけ似ているかを表す数値。距離が大きければ似ておらず、距離がゼロなら2つは一致している。

まっている様子がわかる。スコアは当然のごとく0を示している。センサー部にこびりついたゼラチン液は粘性が高く、払拭するのはかなり困難な作業であった。

さらに作成法を変え、数個作成したうちの一個で、初めてスコア30が出た。かなり像は崩れているものの、図5のようにスコアは30を示している（右が偽造指紋)。しかし、安定してスコア30を出すわけではなく、たまたま高得点が出た、という状況であった。センサ部からある程度熱が与えられ、軟らかさがちょうど良くなったことで高いスコアが出たようである。熱を与えすぎてもスコアは下がっていった。

この偽造指紋はテストを続けるうちに指紋表面付近の構造が乱れ、二度と高スコアを出すことはなくなってしまった。

3.2.2 一週間程度の試行錯誤の後

最終的に、スコア75までたどりついた(図6)。 この偽造指紋は像もかなり鮮明で、耐久性も上がった。照合の安定度も増し、連続で高いスコアを出した。

ところが、これを常温で密閉せずに保存したため、週明けに再びテストを行った際には最高でも10点程度までしかスコアは上がらず、加熱によるスコアの上昇もなかった。次ページ図7がその時の画像である。

図5　スコア30が出て照合が成功した

図6　75というハイスコアを出したとき

図7　スコア75を出した偽造指は、しかし時間と共に劣化してしまい、その後の照合では本人と認証されなかった

凹凸がはっきりせず、上で75点を出したものと同一のものとは思えないほど荒れた画像しか得られていない。水分が抜けたことと、各種化学反応や微生物による分解が進んだことなどが原因と考えられる。この偽造指紋は悪臭を放ちはじめていたために捨てざるを得なかった。

3.3　考察

3.3.1　偽造指紋の作成は簡単か？

この問いには一言で答えることはできない。

まず、材料の調達は極めて容易である。安価で、かつ店頭で誰もが入手できるものだけで作成できる。問題は、実際に高い照合スコアを出す指紋の作成が簡単かどうか、という点である。3.2.1でとりあえずスコア30を出せたのは、偽造指紋の作成を開始したその日のことである。よって、照合の安定性を除けば簡単に作成できてしまう、と言える。ただ、安定して高いスコアを出した3.2.2の偽造指紋は、試行錯誤の末にやっと75点までたどりついた、という状況であった。その上、偽造指紋の保存法にも気を遣う必要がある。しかし、偽造指紋の作成開始から一週間程度でスコア75まで達したことを考えると、他のクラック手法に比べれば簡単な部類に入るのかもしれない。

型（ゼラチンを流し込む土台）の作成については触れなかったが、ここにも工夫の余地は残されていると思われる。スコア75を出した偽造指紋は同じ型から作成したものであり、他の型から作成したものでは高得点を出すことができなかった。しかし、型の作成に必ずしも“被害者”（指紋の型をとられる人）の自発的な協力が必要でないと判明したことは一つの発見であった。

前出の松本氏の資料では、机の上に指を押し付けるような格好で型をとっており、この方法は被害者の自発的な協力がないと困難だ。手をまったく動かすことなく数分間じっとしているのは意外に難しいものである。指紋認証機器メーカーは、偽造指紋への言い訳としてこの点をしばしば指摘する。つまり、自発的に偽造指紋の作成に関わったのなら、その時点で被害者に責任が発生するというロジックである。それに対して今回の実験では指に乗せる方法で作った型を使って、実際に認証装置をだますことができた。この方法では、ある程度手を動かしても問題なく型が取れる。

今回の方法以外にも、物体に付着した残留指紋から偽造指紋を作成する方法もある。ただし、この方法は、ゼラチンを用いる点は同じだが高価な機器が必要である。

3.3.2　照合閾値を厳しくして偽造指紋を防げないか？

本物の生体指による照合スコアは、慣れれば常に90点以上を出すことが可能である。これに対し、今回の偽造指紋は最高でも75点にとどまった。この90点と75点の隔たりを利用して、偽造指紋を防ぐことができないだろうか、と考えた。が、3.2の最初に紹介したように、Puppy Suiteの閾値設定の最高値は5で、一番厳しく設定しても照合スコアが50点以上なら本人であると判断してしまう。つまり、今回、約一週間で作り上げた偽造指紋を使った“なりすまし”を防ぐことはできない。

偽造指紋への対策状況をメーカーの担当者に尋ねたところ、ハードウェアをどのようにするか検討中との返答を得た。2000年7月の段階で、すでにゼラチン偽造指紋の危険性を警告する論文が世に出ている。それから３年近い月日が流れたわけだが、メーカーの対応は遅れていると言わざるを得ない。この対応の遅さの原因は、まだバイオメトリクス製品の安全性を評価する公の基準および機関が存在しないという点にあると思われる。ある程度バイオメトリクスが普及してからそうした基準が定まるのか、それとも基準が定まってから普及するのか。いずれにしても第三者機関による安全性の評価が必須であるのは間違いない。評価基準が固まるまでは、メーカー主導の積極的な偽造指紋対策が望まれる。

〈参考文献〉

1. 山田浩二、松本弘之、 松本勉著「指紋照合装置は人工指紋を受け入れるか」『信学技報』（2000年7月号）
2. 松本勉著「セキュリティ技術の弱点を発見したらどうしますか？」『電子情報通信学会誌』（2001年3月号）