ヒューマンテクノロジーズ
指紋照合技術のセキュリティ

■指紋照合の流れ

指紋照合センサによる指紋照合は、下図のように実行されます。この際、一般的にはいくつかのポイントでセキュリティホール（指紋データが漏洩する等の問題が発生する可能性）が生じますが、ヒューマンテクノロジーズの指紋照合では、それらに対してそれぞれ対策がなされています。

① センサ上で指紋画像の取得

センサに指を置くことによって、指紋画像を取得します。
この際、一般的には、指紋の偽造による不正が考えられます。
ヒューマンテクノロジーズの指紋照合技術では、二次元イメージの排除、物理的な指の検知、センサイメージ以外の排除によって対策がなされています（※ａ）。

② 指紋画像をPCに転送

センサによって取得された指紋画像はPCに転送されます。
この際、一般的には、ケーブル信号の盗聴・偽造による不正が考えられます。
ヒューマンテクノロジーズの指紋照合技術では、チャレンジ＆レスポンス方式による暗号化で対策がなされています（※ｂ）。

PC

③ 指紋画像からの特徴点の抽出・保存

指紋画像から、特徴点の抽出を行います。
この際、一般的には指紋データの流出・盗難等の不正が考えられます。
ヒューマンテクノロジーズの指紋照合技術では、マニューシャ法による特徴点抽出・保存を行います。これにより、万が一保存されたデータが流出・盗難にあった場合でも、元の指紋の形を復元する事は不可能です（※ｃ）。

④ すでに保存してある別の特徴量との比較

保存されている特徴データと一致した場合、指紋照合の完了となります。

※ａ：詳細は裏面（３）
※ｂ：詳細は裏面（１）
※ｃ：詳細は裏面（２）

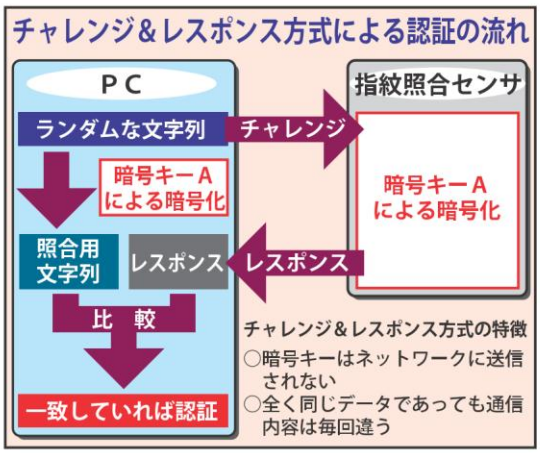
■指紋照合技術のセキュリティホールへの対策

1）ケーブル信号の盗聴・偽造は不可能です

一般的には、指紋照合センサ上で取得された指紋の画像をPCに転送する際に、ケーブル信号の盗聴などで指紋画像取得されてしまう危険性があります。また、指紋画像を取得できないまでも、盗聴したデータと同じデータを擬似的に流すことによって、本当の指ではないのに照合されてしまう可能性があります。

ヒューマンテクノロジーズのセキュリティ

ヒューマンテクノロジーズの指紋照合センサのファームウェアは、指紋の画像を取得すると同時に、チャレンジ＆レスポンス方式で画像を暗号化して送信しています。USBケーブルの途中で信号を解析されても、指紋画像の復元は不可能です。また、生成される暗号は毎回異なるため、盗聴したデータと同じデータを擬似的に流すことは不可能です。



2）指紋データが流出・盗難にあっても大丈夫です

一般的には、保存されている指紋データが何らかの形で漏れた時、そこから指紋画像が復元されてしまうと、重要な個人の認証情報が流出してしまう可能性があります。

ヒューマンテクノロジーズのセキュリティ

ヒューマンテクノロジーズの指紋照合技術では、保存されたデータから指紋画像を復元する事が不可能なマニューシャ法（特徴点抽出法）をベースとした技術を採用しています。

さらに、保存する特徴データは128ビットで暗号化されているため、仮に保存されている指紋データが流出・盗難にあった場合でも、肝心の「指紋そのものの形」が外部に漏れる心配はありません。

一般的に現在実用化されている指紋照合技術には、他に
○パターンマッチング方式
○周波数解析方式
○位相相関方式
等がありますが、一部では保存されたデータからの指紋画像の復元が可能となります。

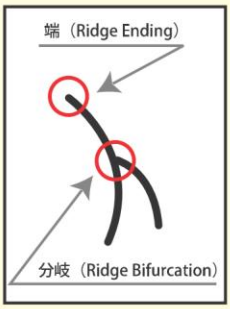
マニューシャ法（特徴点抽出法）とは

人間の指紋には、およそ100程度の特徴点があります。特徴点とは、指紋の隆線が、線でなく別の形をしているポイントのことを指します。

同じ場所に特徴点がある確率は 1/10 程度とされています。このうち12点の一致を確認できれば、10の12乗ぶんの１（１兆ぶんの１）となり、全人類の10倍（10本の指）をカバーできます。これを元に照合を行うのが、12点法と言われ、日本の警察機構ではこの照合法を利用しています。世界的には、フランスの17点が最も多い例となります。弊社の指紋照合では、20～30の特徴点を使い、照合を行っています。

■特徴点の情報
・特徴点の種類
・特徴点の向き（ただし点（Dot）に向きは存在しません）
・特徴点から最も近い別の隆線までの距離
・分離角度（分岐（Ridge Bifurcation）・分離（Ridge Divergence）・島（Enclosure）のみ）
・中心点からの座標

■特徴点と特徴点の間の情報
・特徴点間の距離
・特徴点間の角度
・２つの特徴点の間にある線分の数



これらの数学的情報を、数値化して保存したのが、特徴データになります。

特徴データは、上で示したように、特徴点およびそれらの間の関係性の情報のみを保持しています。つまり、指紋の大部分を占める、「特徴点のない部分の線」がどのような形をしているのか、データから復元することはできません。

3）指紋の偽造を防ぎます

一般的には、指紋そのものを偽造することにより、システムを騙すことの出来る可能性があります。

ヒューマンテクノロジーズのセキュリティ

ヒューマンテクノロジーズの指紋照合技術では、以下の対策がなされています。

○二次元イメージの排除
ノイズパターンの判定により、写真やフィルムなどの二次元イメージは排除されます。また、光学センシングの原理上、二次元イメージは指と判定されません。

○指の検知
ある程度の水分を含有していない指は、原理上画像として取り出すことはできません。

○センサイメージ以外の排除
チャレンジ＆レスポンス認証により、電子的に偽造された指紋データは認証の対象になりません。

※ゼラチンなど、人間の指に極めて組成・水分含有量が近い物質によって、極めて精巧な偽造指を作成することは可能です。現在の技術水準では、このような精度で作成された指紋による偽証を100%防止することは不可能ですが、ヒューマンテクノロジーズの指紋照合ではこうした不正の可能性を極めて低い水準に保っています。

※指紋照合ソリューションパッケージ『DigitalPersona Pro』では、万が一の誤認証からシステムを守るため、指紋を認証するときに「指紋暗証番号」を要求する設定が可能です。

H&T HUMAN TECHNOLOGIES
http://www.h-t.co.jp/