携帯端末の動きによる個人認証手法の評価

行方 エリキ† 石原 進†† 水野忠則†††

† 静岡大学大学院 情報学研究科
432-8011 静岡県浜松市城北 3-5-1
eric@mizulab.net

†† 静岡大学 工学部
ishihara@ishilab.net

††† 静岡大学 情報学部
mizuno@mizulab.net

あらまし 筆者らがこれまで提案した携帯端末を用いた動きによる認証手法の評価を行った．提案手法では，携帯端末の動きを３次元加速度センサによって検出し，DP マッチングを用いて認証判定を行う．認証判定時に用いるパラメータは被験者の過去の認証動作から自動設定・更新する．11 人の被験者に同一の認証動作を毎日１ヶ月継続する実験と，25 人の被験者がその各動作の成りすましを試みる実験を通して，提案手法の経年変化・成りすましに対する耐性，そして，認証に適切な動作について調べた．その結果，加速度のダイナミックレンジが大きな，良好な動作を登録することで，FAR を 1% 未満にすることが可能であるということが確かめられた．

An Evaluation of Individual Authentication for Portable Devices using Motion Features

Eric NAMIKATA† Susumu ISHIHARA†† Tadanori MIZUNO†††

†Graduate School of Information,Shizuoka University
Jyohoku 3-5-1, Hamamatsu, Shizuoka, 432-8011 Japan
eric@mizulab.net

††Faculty of Engineering,Shizuoka University
ishihara@ishilab.net

†††Faculty of Information,Shizuoka University
mizuno@mizulab.net

Abstract We evaluated an individual authentication method we have proposed that is based on movement of a mobile device. This authentication method measures the motion of the user's hand with a device using a 3-axis acceleration sensor. We implemented the authentication method using DP matching. A threshold value and master data used in the method is selected automatically and renewed using the user's past movement data. Through experiments that 11 examinees continued doing the same movement for a month and experiments that 25 examinees tried to pass themselves off as the same movement, we confirmed that the authentication method and the parameter renewal algorithm adopts the parameter to the alteration of the user's movement and the resistance to perjuries of the method. We obtained FAR less than 1 % when movements with large dynamic range of acceleration were used for authentication.

1 はじめに

筆者らのグループでは，これまで携帯端末の動きによる個人認証手法を提案し，評価を行ってきた [1] [2] [3]．携帯端末における個人認証は，端末上の個人情報保護や端末を用いた m-コマースの普及により非常に重要になってきており，手軽かつ堅牢な認証手法が求められている．提案手法では，携帯端末に内蔵された 3 次元加速度センサにより動きを検出し，端末を空中で動かすだけの簡便な操作で個人認証を可能としている．

筆者らは，これまで 3 名の動作登録者と 10 名の成りすまし被験者による実験で，提案手法の有効性を確認しているが，被験者数が十分ではなかった．また，提案手法に適した認証用動作の解析も不十分であった．本論文では，個人の経年変化に対する実験，成りすましへの耐性に関する実験，それぞれについて被験者数

を 11 名と 25 名に増やし，提案手法の有効性および，提案手法に適した認証用動作の性質について再検討する．

以下，2 章で提案手法の特徴，認証処理の詳細について述べる．3 章で評価実験とその結果，考察について述べる．最後，4 章でまとめとする．

2 携帯端末の動きによる認証

2.1 特徴

提案手法では，ユーザが自分のサインや絵、記号など適当な動作パターンに基づいて携帯端末を空中で動かし，その動きを利用して個人認証を行う．携帯端末自体の動きを個人認証に利用しているため，パスワードのように，携帯端末の小さなボタンを押す細かい操作が必要なくなる．また，パスワードはその記号列が本人以外のユーザに知られてしまった場合，容易に成りすましができる．パスワードの代わりに指紋認証が搭載されている携帯端末 [4] もあるが，指紋は容易に搾取でき，成りすましも可能であることが報告されている [5]．そのため，指紋データの登録に心理的抵抗を持つユーザがいるという欠点を持つが，本手法では，動きを登録することに対して，ユーザの持つ抵抗感は少ない．また，本人以外のユーザに動作パターンを知られてしまったとしても，その再現が難しく，不正利用される心配がない．不正利用者が登録した認証動作を知らないのならば，他人がその端末を不正利用することはさらに困難となる．

提案手法では，端末自体の個人認証だけでなく，携帯端末を鍵の代わりとして使用する方法も考えられる．例えば，ドアの近くで認証動作を行うとドアが開くというような，従来の物理的な鍵の代わりとしての使用方法が考えられる．このことにより，物理的な鍵の紛失や持ち運びから解放される．

2.2 認証処理

ユーザの認証動作は端末内蔵の 3 次元加速度センサにより検出する．ユーザがあらかじめ，端末に登録した認証動作（以下，マスタデータとする）と認証時に測定した動作（以下，照合データとする）を DP マッチングを用いて照合し，認証判定を行う．

以下，加速度のサンプリングから認証判定にいたるまでの照合手順を 2.2.1 章で，認証判定時に用いるパラメータの自動設定・更新手法については 2.2.2 章で示す．

2.2.1 照合手順

1. **加速度のサンプリング**
   携帯端末に内蔵された 3 次元加速度センサにより，ユーザの認証動作の計測を行う．サンプリングは，端末にあるボタンの押下により開始される．

2. **認証動作区間の検出**
   加速度データのサンプリングを開始してから，ユーザが意図して認証動作を行っている部分を検出する．ボタン押下後の静止状態から加速度が急激に変化した時を認証動作開始とし，動作開始後，一定区間加速度の変化が少なかった時点で認証動作の終了時刻を決定する．

3. **加速度の正規化**
   文字を書く速度が気分や体調によって変化するのと同様に，同じ認証動作を行うときの加速度も操作のたびに微妙に変化する．このような変化によって認証判定に影響が及ぶのを防ぐため，加速度の絶対値の最大値が 1 になるように加速度の正規化を行い，ユーザの気分や体調の違いによって生じる加速度の変化にも耐えられるようにした．

4. **データ長の正規化**
   データ間距離算出の前処理として，マスタデータと照合データのサンプル数を等しくする必要がある．そこで，自然 3 次スプライン補間を用いて，データ長を正規化する．

5. **認証判定**
   認証判定は，マスタデータと照合データの DP マッチング距離間によって判定する．DP マッチングの距離尺度には加速度のベクトル間ユークリッド距離を用いる．x，y，z の各軸についてデータ間距離（d_x，d_y，d_z とする）を算出し，データ長 N で正規化したものを最終的なデータ間距離 D にする（**式 1**）．データ間距離が閾値以下であれば，認証成功とし，それ以上のときは認証失敗とする．マスタデータ，閾値の設定方法については 2.2.2 章で示す．

$$D = \frac{\sqrt{d_x^2 + d_y^2 + d_z^2}}{N} \tag{1}$$

2.2.2 認証判定パラメータの自動設定

ユーザの認証動作は，ユーザが意図していなくても，そのときの気分や経年変化などにより，毎回微妙な変化を起こす．そのため，認証判定時に用いるマスタデータ・閾値をその変化に合わせるようにしてユーザ毎，そして，認証時毎に更新していく必要がある．そこで，本手法では認証動作登録時以外は，過去の認証成功した動作データからマスタデータ・閾値を自動設定・更新する．

1. **初期マスタデータの決定**
   認証動作登録時における初期マスタデータを決定するために，ユーザは同じ認証動作を N 回入力する．ここで，計測した動作データは「有効動作履歴」としてシステムに保持される．保持した各動作データ（$i = 1, 2, \cdots, N$ ）と他の動作データ（$j = 1, 2, \cdots, N : j \neq i$）同士の DP マッチング距離の二乗和を求め，この値を最小にするデータをマスタデータ $\sum d_{\mathrm{ij}}$ とする．

2. **無効動作の除去**
   有効動作履歴中にはなんらかの形で認証動作に失敗したり，または，外乱の影響を大きく受けてしまった場合の動作が含まれていることが考えられる．このような動作は認証判定に悪影響を及ぼす可能性があり，有効動作履歴から除去する．まず，有効動作履歴中の各動作データとマスタデータとの DP マッチング距離 D_i を求め，これらの中央値を D_m とおく．$D_i > bD_m$ となる動作データ M_i を無効動作とし，有効動作履歴から削除する．b は $b > 0$ となる定数である．

3. **初期閾値の決定**
   2.2.2 2．で求めた D_i の平均値 μ と，D_i の標準偏差 σ を求め，$\mu + a\sigma$ を M_i に対する閾値とする．a （$a > 0$） は閾値制御のためのパラメータである．

4. **マスタデータと閾値の自動更新**
   有効動作履歴の更新を行った後，2.2.2 1.，2.2.2 3．に従ってマスタデータ，閾値の更新を行う．有効動作履歴の更新は， 認証に成功した動作データを有効動作履歴に追加登録し，このとき，登録されているデータ数が有効動作履歴最大数 $H_{\max}$ を超える場合は，履歴中の最も古い動作データを削除することによって更新を行う．

表 1: 解析専用 PC の仕様

CPU	Pentium 4 2.00GHz
RAM	504MB
OS	Windows XP Professional

3 評価実験

加速度センサが内臓された実験専用端末を用いて，本人の動作追跡実験と成りすまし実験を行い，提案手法の認証性能，ならびに認証に適した動作について調べた．

3.1 実験環境

実験環境は，実験端末と解析専用 PC をシリアルケーブルでつなげ，認証時，加速度データが随時 PC に送信される仕組みになっている．そのため，実験端末は加速度データ取得のみに使われ，データの解析はすべて PC で行っている．データ解析専用 PC の仕様を **表 1** に示し，実験専用端末の概観，仕様をそれぞれ **図 1**，**表 2** に示す．

データ測定は無風の室内で行い，各被験者に立って，静止した状態で認証動作を行ってもらった．また，ノイズの影響を抑えるため，認証動作を行う際は，実験端末と解析 PC をつなげるシリアルケーブルが他のものと当たらないよう各被験者に注意するよう伝えた．なお，無効動作除去で使う定数 b は 2.0 とし，閾値制御用パラメータ a は 1.5 に設定した．有効動作履歴最大数 $H_{\max}$ は 10 に設定した．

図 1: 実験端末

表 2: 実験端末仕様

サイズ：13 x 4 x 2.5cm
重量： 68.5 g
加速度検出軸数： 3 軸
加速度検出範囲： −4〜4G（重力測定不可）
サンプリングレート： 200 Hz

3.2 実験方法

3.2.1 動作の登録

被験者が提案手法に早く馴染むことができるように，認証動作は，筆記で書き慣れた自分の名前を空中で描く動作のみにした．具体的には，自分の苗字もしくは下の名前を，漢字もしくは平仮名で空中で描くパターンである．また，被験者には自分の名前を空中で書いているイメージで動作を行うようにしてもらった．動作の長さに関しては特に制限を設けなかった．被験者は全員右利きである．

3.2.2 本人の認証動作の追跡実験

本人の認証動作を追跡するための実験を行った．被験者 11 人にシステムに認証動作を登録してもらい，1 日に 3 回，週 5 日の頻度で 1 ヶ月間その動作を行ってもらった．動作の初期登録時，初期マスタデータ・閾値を決定する必要がある．そのため，被験者に十分に（各被験者 10 回以上）動作の練習を行ってもらってから，データ初期登録のために 10 回動作を行ってもらった．なお，初期登録時を含め，動作のデータ測定時は認証判定の成否， DP マッチング距離のフィードバックを被験者に与えていない．

3.2.3 成りすまし実験

成りすましに対する耐性を調べるための実験を行った．25 人の被験者に前述の 11 人の本人動作登録者のうち 8 人分の動作を真似してもらった．成りすましを行う被験者には，それぞれの動作で空中でどんな字を描いているのかを紙面で見せ，さらに成りすまし対象の動作が正面から映っているビデオを数回，被験者が納得するまで見せた．被験者がビデオを見て，ある程度自分で成りすましが可能と判断した直後に，成りすましの動作を各動作に対して 4 回ずつ行ってもらった．

3.3 実験結果

これ以降，2.2.2 章に従って，マスタデータ・閾値を更新したデータを用いた場合，そのデータを更新版と呼び，逆に更新させなかったときは非更新版と呼ぶ．

表 3 に全被験者の更新・非更新版の実験開始後 3 日間と実験終了前の 3 日間における FRR（False Rejection Rate：本人拒否率）を示す．さらに，実験期間を通じての更新・非更新版の FRR と FAR（False Acceptance Rate：他人許容率），各軸における加速度の標準偏差，ダイナミックレンジ，そして認証動作を行ったときの実験端末の動かし方を示した．更新版の FAR,FRR は，1 ヶ月間の各被験者の動作測定値をもとにマスタデータの閾値を計算し，更新が行われた場合のこれらの値にもとづいて認証の成否を判定することにより計算したものである．FAR を除いた被験者の実験結果から求めた．

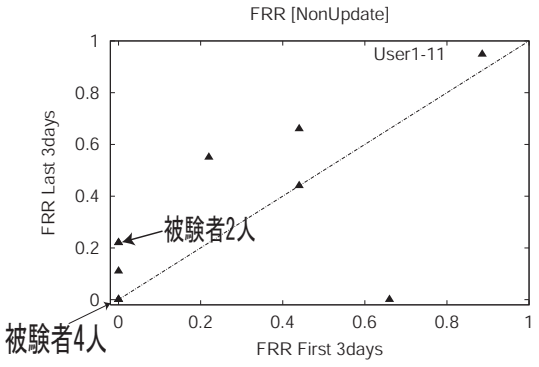

図 2: 非更新版 FRR の変化

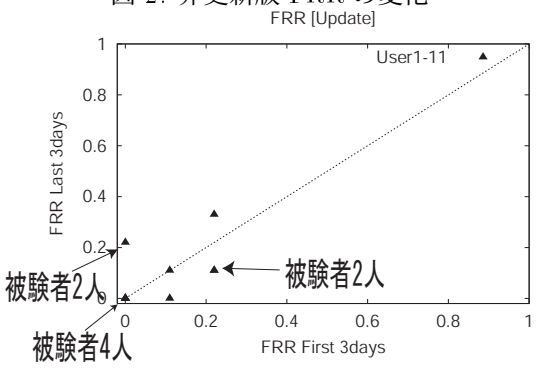

図 3: 更新版 FRR の変化

図 2，図 3 は，それぞれ実験の最初 3 日間と最後 3 日間において，各被験者の非更新版と更新版の FRR 変化を示す．**図 2** の非更新版グラフを見ると，認証判定に初期マスタデータ・閾値を使い続けるため，ほぼ被験者全員の FRR が悪化していることがわかる．これに対し，**図 3** で示す更新版は，一部を除き，被験者に FRR の改善が見られた．また，**図 4** は，実験の最初の 3 日間のみに着目したときの更新版と非更新版の FRR の違いを示している．最初 3 日間の学習だけでも，FRR が減少していることがわかる．

図 5 は被験者の初期マスタデータの長さと認証精度（FAR・FRR）を示したものである．FAR，FRR はともに動作データの長さに関係なく変動しており，今回測定した範囲では，両者に相関は見られない．

図 6 では，更新版・非更新版の FAR の違いを示

表 3: 全被験者実験解析結果

	FRR [NonUpdate]		FRR [Update]		FRR	FRR	FAR	FAR	Standard Debiation			Dynamic Range			Way of
	First 3days	Last 3days	First 3days	Last 3days	NonUpdate	Update	NonUpdate	Update	x	y	z	x	y	z	Movement
User1	0.44	0.66	0.22	0.11	0.57	0.09	0.03	0	0.87	0.47	1.70	6.41	3.55	7.88	arm
User2	0	0.11	0.11	0.11	0.05	0.10	0	0.02	1.49	0.40	1.09	7.90	2.06	6.93	arm
User3	0	0.22	0	0	0.13	0.00	0	0	1.05	0.37	1.36	6.79	2.29	7.33	arm
User4	0.44	0.44	0.22	0.11	0.43	0.10	0	0	1.33	0.65	1.33	7.53	3.56	7.33	arm
User5	0	0	0	0	0.00	0.04	0.45	0.25	0.75	0.20	0.60	4.28	1.20	3.59	wrist
User6	0	0	0	0	0.00	0.00	0.32	0.04	0.78	0.25	0.96	4.98	1.55	5.49	wrist
User7	0	0	0	0	0.00	0.00	1	0.17	0.66	0.18	0.73	3.55	1.01	3.87	arm
User8	0.22	0.55	0.22	0.33	0.39	0.17	0	0.05	1.08	0.43	1.18	6.17	2.57	6.74	arm
User9	0	0.22	0	0.22	0.08	0.04			1.14	0.56	1.51	6.98	3.55	7.64	arm
User10	0.66	0	0.11	0	0.00	0.00			1.14	0.42	1.29	6.80	2.23	7.36	arm
User11	0	0	0	0	0.00	0.00			1.34	0.45	1.51	7.60	2.60	7.74	wrist
Average	0.16	0.2	0.08	0.08	0.15	0.05	0.23	0.07	1.06	0.40	1.20	6.27	2.38	6.54	

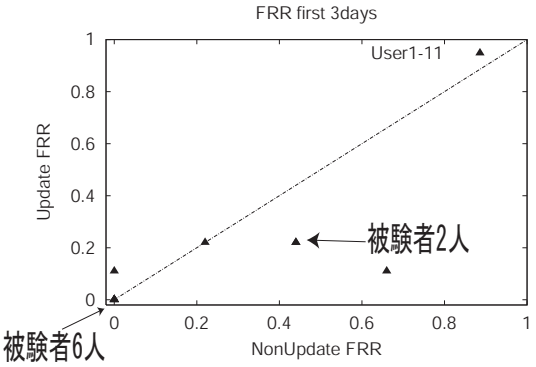

図 4: 最初の 3 日間における FRR の変化

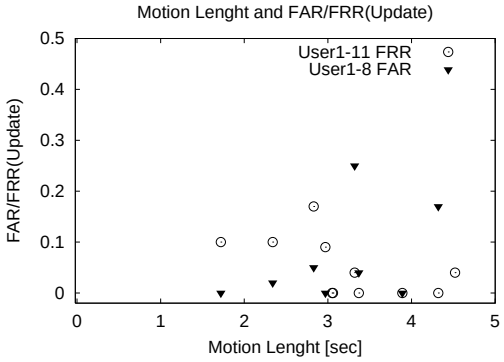

図 5: 初期マスタデータの長さと認証精度

す．更新版のデータを用いることによって，被験者 8 人中， 6 人に改善が見られた．特に，初期の FAR が大きかった USER5,6,7 に学習効果が顕著に見られる（**表 3**）．この 3 人の被験者は，更新の有無にかかわらず FRR=0 であり（**表 3**），本人認証はできるが，実験結果より FAR が 高いことから成りすましも容易にできるという特徴を持っている．また，3 人の被験者に共通する事項として，加速度の標準偏差，ダイナミックレンジが低いことが挙げられる．つまり，これらの被験者の認証動作は速度変化が少なく，全般的にゆっくりとした動作である．**図 7** に，被験者毎の x,y,z 軸のうち，ダイナミックレンジが最大となる値と更新版の FAR を示す．**図 7** からわかるように，ダイナミックレンジが小さいと FAR の値が大きくなり，成りすましがしやすくなる．特に，ダイナミックレンジが小さい被験者のうちの 2 人は端末を手首で動かしている（ **表 3** より，USER 5,6 ）ことから，手首だけの操作だと動きが緩慢になる傾向があると推測される．**図 7** 同様，**図 8** にダイナミックレンジの最大値と FRR の関係を示す．両者の相関は実験結果からは見られない．

3.4 考察

マスタデータ・閾値の更新を行うことによって，被験者 8 人中 6 人が FAR 5% 以下で，うち 3 名は 1% 未満 [1] の認証精度を得ることができた．残る被験者 2 人については，アップデート後も FAR が高かった．その原因として，認証動作が緩慢であったことが挙げられる．成りすましが困難な動作とは，実験結果からダイナミックレンジが大きくなるような動作であるといえる．加速度センサの 3 軸のうち，人間の体に対して前後の方向（図，表中の Y 軸）の加速度の変化は小さかった．加速度のダイナミックレンジが小さい場合に FAR が高くなることを考慮すると，この方向の加速度測定は必ずしも必要ではないことが推測される．従って，より安価な 2 軸加速度センサを用いても同様の認証精度が得られると期待できる．

[1] 今回の実験では．一つの成りすまし対象の動作に対して，25 人の被験者が 4 回ずつ動作を行ったため，FAR 1% 以下の精度は得ることができない．そのため， FAR 0% であった被験者に関しては， FAR は 1% 未満を意味する．

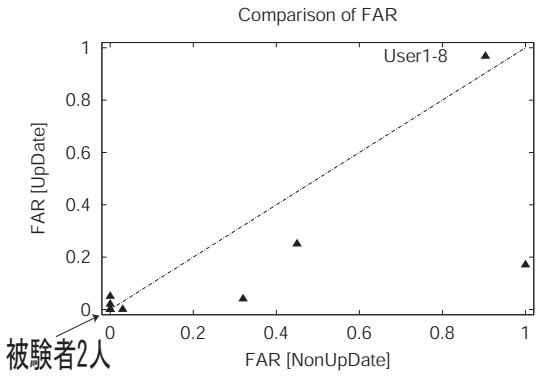

図 6: 更新・非更新版 FAR

被験者の中には，マスタデータ・閾値のアップデートによって FRR の結果が悪化している者もいる．今回の測定では，被験者に認証の成否および DP マッチング距離をフィードバックしていないために起きた可能性も考えられる．被験者になんらかのフィードバックを与えた場合，被験者は動作を改善するよう意識して動作を行うようになり，FRR が改善される可能性がある．今後，フィードバックがあった場合の学習効果についても調べる必要がある．

今回の成りすましの実験では，成りすましを行う被験者に真似をする動作パターンを紙面で見せ，さらにその動作のビデオを被験者が納得するまで見てから成りすましを行ってもらった．実際の利用環境を想定した場合，動作パターンは見ただけでは何を書いているのかを判断するのが難しく，さらに，他人の動作をじっくり見る機会も少ないと考える．このような成りすましを行う側に極めて有利な実験条件を鑑みると，今回得られた 3 人の被験者の 1% 未満という FAR は実用的な範囲にあるとみなしてよいと考える．

4 まとめ

筆者らがこれまで提案してきた携帯端末の動きによる認証手法の最評価を行った．1ヶ月間の本人による動作追跡実験とその動作から成りすましを行う実験において被験者数を増やし，認証精度，適切な認証動作について検討した．

提案手法で用いている認証判定パラメータの自動設定・更新により，FRR，FAR ともに減少し，自動設定・更新手法に学習効果があったことが確認できた．また，ダイナミックレンジが大きくなるような，良好なマスタデータを用いた場合，FRR を 10% 以下，FAR を 1% 未満とできることが確認できた．今後は，フィードバックを与えた場合の学習効果について検討

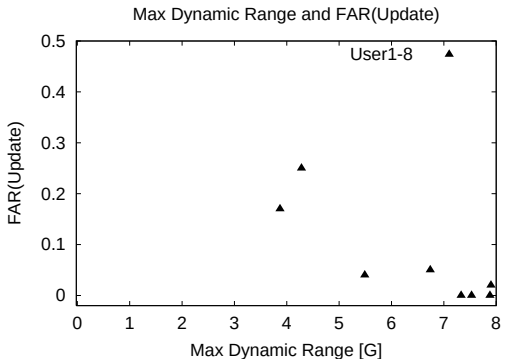

図 7: ダイナミックレンジの最大値と更新版 FAR

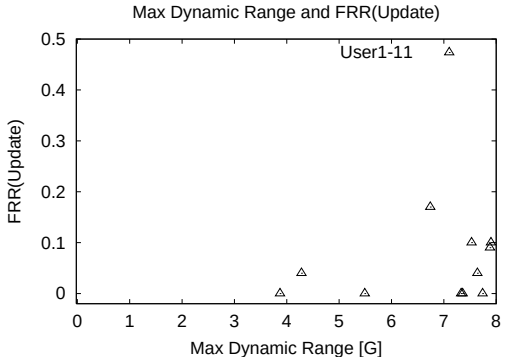

図 8: ダイナミックレンジの最大値と更新版 FRR

していく．

参考文献

[1] 太田, 行方, 石原, 水野: 携帯端末の動きを用いた個人認証 -認証判定パラメータの自動設定- 情処学会 CSS 2003 論文集, Vol.2003, No 15, pp.79–84 (2003-10).

[2] M. Ohta, E. Namikata, S. Ishihara, T. Mizuno: “Individual Authentication for Portable Devices using Motion Features”, in proc. of ICMU2004, pp.100–105 (2004-1).

[3] 行方, 太田, 石原, 水野: 加速度センサ搭載腕時計型端末を用いた腕の動きによる個人認証, 情処学会, 研究報告. HI, vol.2003, No.94, pp.21–26 (2003-9).

[4] http://www.fmworld.net/product/phone/

[5] 遠藤, 平林, 松本: 指紋照合装置は人工指を受け入れるか (その 5), 情処学会研究報告．DPS, Vol.101, No.125, pp.9-16 (2001).

[6] http://www.sony.co.jp/Products/felica/