

指紋照合機能搭載型 IC カードによる本人認証方式

飯野 徹, 岩瀬史幸, 坂野 鋭, 中嶋秀樹
株式会社 NTT データ
E-mail: iino@rd.nttdata.co.jp

あらまし

本報告では, 指紋認識技術を利用した IC カードの所有者確認方式における脅威を洗い出し, 考えられる対策を実施したシステムの一実装形態を提案する. 従来までに検討されている指紋認識技術と IC カードを組み合わせた本人認証システムでは, IC カードへの実装可能性を論じたものが多く, 想定される脅威に関する分析, 及びその対抗手段に関する検討が不足していた. そこで, 本報告では当該本人認証システムにおいて, 機器構成と個々の構成要素の両面から脅威を分析し, 脅威に対する対策を組み入れた実装形態として, 指紋照合機能搭載型 IC カードを利用したシーケンスフローを示した.

和文キーワード 本人認証, 指紋認識, IC カード, バイオメトリクス

Secure implementation method for person authentication system using a smartcard and fingerprint recognition technology

Toru Iino, Noriyuki Iwase, Hitoshi Sakano, Hideki Nakajima
NTT Data Corporation
E-mail: iino@rd.nttdata.co.jp

Abstract

We clear up about threats in person authentication system that configured by fingerprint recognition technology with a smartcard. We also suppose how to protect against the threat. The discussions in present articles about the system was limited only how to implement smartcard and fingerprint recognition technology. So there is less argument about analysis of possible threats and countermeasure. First, we analyze the threats caused by a system structure and a devise itself. Then we show an example of sequence flow and system configuration method that remove the threats.

英文 key words person authentication, fingerprint recognition, smartcard, biometrics

1.はじめに

本報告では、指紋認識技術^{[1][2]}を利用した IC カードの所有者確認方式における脅威を洗い出し、考えられる対策を実施したシステムの実装形態を提案した。

これまでも IC カードを利用したシステムにおける所有者確認手法が提案されているが、その多くは次のような2段階で構成されている。まずあらかじめ IC カード内に設定した PIN (Personal Identification Number) と入力された PIN を IC カード内で照合する。次に、照合結果をカード内のデータへの読み書き権限や、鍵を用いた演算処理の実行許可権限へ反映する。もし、照合が失敗した場合は、カード内のデータや鍵を用いて外部との通信を行う次のステップに進めない。このようにして、IC カード内にシステム提供者が要求するセキュリティの仕組みを組み入れることによりシステムの安全性を確保しようとしている。

しかし、PIN としては、誕生日などカード所有者にとって忘れにくい情報が設定されることが多く、逆に第三者にとって推測し易い状況を招く結果となり、必ずしもセキュリティの高い所有者確認方式とはならないことが指摘されていた。

一方、PIN に代わるカードの本人認証方式としてバイオメトリクス^[3]、すなわち人間の生物学的な特徴を自動認識することによる本人認証技術が検討されている。指紋認識技術に代表されるバイオメトリクスと IC カードを組み合わせることにより、IC カードの所有者確認をより厳密に出来るばかりではなく、認証精度が 100% でないというバイオメトリクス単独利用での弱点を補強することができる。何故なら、IC カードの所持と指紋認証結果の両方を確認することができるため、指紋認証単体に比べてより厳密な本人認証が可能となるからである。

このような背景から、最近、指紋認識技術と IC カードを組み合わせ使用することが期待されるようになっていく。しかし、これまで検討されている本人認証システム^{[4][5]}は、単に IC カードへの実装可能性を論じたものが多く、想定される脅威の分析や、その

対抗手段に関する検討までには至っていない。実際のシステム化にあたってはセキュリティの観点からより現実に即した詳細な分析が求められる。

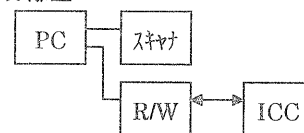
以下では、現時点で考えられる IC カードと指紋認識技術を組み合わせた本人認証システムの可能な構成について議論する。次に、これらを組み合わせたシステムについて、セキュリティ診断の観点から考えられる脅威の分析を行い、対策方法を示す。最後に、これらの対策を踏まえた本人認証システムの実装例を示す。

2.機器構成

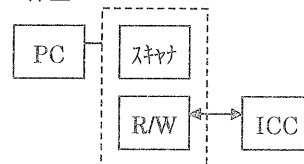
IC カードと指紋認識技術を組み合わせて本人認証を行う場合、指紋照合装置（または指紋スキャナー）、IC カードリーダ・ライタ（以下 R/W と略す）、IC カードの3つの機器が必要である。これらの機器の組み合わせ方法は、図1のように大きく3つに分類できる。

- 1) R/W とスキャナーを分離(分離型)
- 2) R/W とスキャナーを一体化(一体型)
- 3) IC カードとスキャナーを一体化(ワカード型)

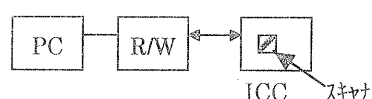
1) 分離型



2) 一体型



3) ワカード型



PC: パソコンなど

スキャナ: 指紋照合装置またはスキャナー

R/W: IC カードリーダ・ライタ

ICC: IC カード

図1 IC カードと指紋認識の組み合わせ方法

上記の構成において、指紋照合処理を行う箇所は、

I：パソコン

II：指紋照合装置^[6]

III：IC カード

IV：パソコンと IC カードの両方

V：指紋照合装置と IC カードの両方

の 5 ケ所が考えられる。

ここで、パソコンなどと比較して処理能力が劣る IC カードで指紋照合処理を行う^{[7][8][9]}場合には、適正なセキュリティを確保した上で、トータル処理時間を短縮することを考え、他の機器と処理を分担して行う必要がある。その対応方法として、IV および V の 2 パターンを入れている。

3. 組み合わせシステムにおいて想定される脅威

まず一般の本人認証システムにおける脅威について示し、その後に図 1 の各組み合わせ方式におけるセキュリティへの脅威を考察する。

本人認証システムのセキュリティについては、電子商取引実証推進協議会(ECOM)の「本人認証技術における評価基準」^[10]にまとめられている。評価基準の 1 つである脅威対抗性の項目に関して、以下に参照して示した。

- (1) 認証用所有物に対する脅威対抗性
- (2) 提示情報入力装置における脅威対抗性
- (3) 認証パスにおける脅威対抗性
- (4) 検証点における脅威対抗性
- (5) トレーサビリティ

IC カードに個人の指紋テンプレートを格納する本人認証システムについて、上記項目を適用した場合、表 1 のように対応させることができる。

上記の脅威対抗性の項目において、機器構成が関係するものは 3 および 4 である。この 2 つの脅威の考え方と対策は以下になる。

表 1 脅威対抗性の項目における語彙解釈例

認証用所有物	IC カードまたは、IC カードに格納する指紋テンプレート
提示情報入力装置	指紋スキャナー
認証パス	指紋照合装置、IC カード、PC、IC カードリーダ・ライタ機器間
検証点	指紋照合装置、PC、IC カード

3 の脅威は、各機器間のパス中に流れる指紋テンプレートの盗聴や改竄である。4 の脅威は、照合結果の盗聴や改竄である。これらの脅威を防ぐ 1 つに、指紋テンプレートや照合結果が認証パス間に流れる回数を少なくする方法がある。

そこで、図 1 の様々な組み合わせ方法に対して、セキュリティ情報である指紋テンプレート、および照合結果が各機器間を通る回数を考える。なお、図 1 での「スキャ」は、単なる指紋スキャナーではなく、指紋照合装置とし、装置自体で指紋照合が可能であるとした。

このときの、登録時の指紋テンプレートに関する各認証パス通過回数を表 2 に示す。

表 2 登録時の指紋テンプレートの各認証パス通過回数

機器構成	認証パス回数
分離型	3
一体型	1
IC カード型	0

また、認証時における指紋テンプレートの各認証パス通過回数は表 3 のようになる。

表 3 認証時の指紋テンプレートの各認証パス通過回数

機器構成	照合箇所				
	I	II	III	IV	V
分離型	3	3	3	5	6
一体型	3	1	1	4	2
IC カード型	4	0	0	6	0

表 4 は、指紋照合結果が各認証パス通過回数を示したものである。I、および II では各認証パス通過が多くなること分かり、照合結果を単に IC カードへ

返す方法はセキュリティ上、大きな問題があることが示される。一方、Ⅲ、Ⅳ、およびⅤではいずれも回数はゼロとなり、改竄の機会をなくすることができる。これは、IC カードに指紋照合機能を搭載するのが望ましいことを示している。

表4 照合結果の認証パス通過回数

機器構成	照合箇所				
	I	II	III	IV	V
分離型	2	3	0	0	0
一体型	2	1	0	0	0
わカード型	2	0	0	0	0

表2, 3, 4の全ての回数の合計を表5に示す。

表5 各組み合わせにおける認証パス通過合計回数

機器構成	照合箇所				
	I	II	III	IV	V
分離型	8	9	6	8	9
一体型	6	3	2	5	3
わカード型	6	0	0	6	0

表5より、認証パス通過回数が少ない、網掛けの部分がセキュリティの観点では優れていると考えられる。

つまり、分離型は通常の機器を組み合わせで構成することが可能であるが、セキュリティの観点からIC カード所有者確認には向いていないと考えられる。一体型やわカード型では、PC 上に個人の指紋テンプレートが流れないため、プライバシーをより強固に保護しており、IC カード所有者の確認に向いている機器構成であると考えられる。

脅威抵抗性の項目について、反対に機器構成に依存しない脅威としては(1),(2),(5)となるが、次にこれらについて考察する。以下に、各項目毎の具体例を示す。

『認証用所有物に対する脅威抵抗性(1)』の脅威例

- ・ IC カード自体の盗難や偽造。
- ・ IC カード内の指紋テンプレートの盗難や改竄。

『提示情報入力装置における脅威抵抗性(2)』の脅威例

- ・ 指紋スキャナーでの不法な情報採取。
- ・ 指紋スキャナーから取り込んだ情報の漏洩。
- ・ 指紋スキャナーからの出力結果のすりかえ。
- ・ 偽造した指紋を読みとらせる。
- ・ 指紋スキャナーの盗難や偽造。

『トレーサビリティ(5)』の脅威例

- ・ 照合履歴の不正な削除。

次にIC カードを利用する観点から対策例を示す。ここでは、1 から5のそれぞれの脅威に対する対策方法を検討するにあたり、デバイス単体や運用で対策すべき項目については省略した。

脅威1の対策例

IC カードから不正に情報を抽出する行為や改竄行為を防止するため、IC カード内の指紋テンプレートは、必要な認証行為を成功した場合のみ、読み書きのアクセスを可能とする。

脅威2の対策例

指紋スキャナー自体の耐タンパ性、および偽指対策に依存するため、ここでは論じない。

脅威3の対策例

認証時や登録時に伝送路上を流れる指紋テンプレートはセッションキーで暗号化し、盗用された場合においても流用不可能にする。

また、テンプレートの完全性を確保するために指紋テンプレートに認証コードを付与し、使用時に当該コードの確認を行う^[11]。

脅威4の対策例

IC カード内で最終的な指紋照合を行うⅣ、Ⅴの場合、IC カードから全ての指紋テンプレートを読み出さずに最終的な照合をIC カード側で行い、IC カード内の当該テンプレートの漏洩を防ぐことができる。

また、指紋照合が OK となるまで繰り返し攻撃す

脅威に対しては、指紋テンプレートが不正と判断された回数を IC カードに保持し、設定した回数を越えた場合に指紋テンプレートをロックし、使用できないようにする。

脅威5の対策例

IC カード内に照合履歴を残し、必要な認証を行わなければ改変できないようにする。

4. システム実装例

以上の対策を考慮し、指紋照合機能搭載型 IC カードを利用した本人認証システムにおける登録フローおよび認証フローの一例を図2、3に示す。

IC カードと端末間をやり取りするデータは、セッションキーにより暗号化を行っている。また照合時には、IC カード内の指紋テンプレートを全て読み出さずに端末側で指紋一次照合を行い、カード側で最終的な指紋照合を行っている。なお指紋一次照合においては、指紋テンプレートの認証コードをチェックする。

また、指紋テンプレートの登録や読み出しの前には必要な認証を IC カード側で行い、不正なノードからのテンプレートの抽出、改竄を防止している。

端末側と IC カード側で指紋照合処理を分担する方法は、指紋照合アルゴリズムにも依存するが、ここでは特徴点抽出方式^{[12] [13] [14]}を例に説明する。

指紋テンプレートは、指紋の特徴点の種類・指紋の特徴点の位置座標、登録した指の位置情報などが含まれていると仮定する。IC カードから指紋テンプレートの一部である登録した指の位置情報を読み出し、端末では当該データと照合側指紋テンプレートを用いて指紋の回転や位置ずれの補正を行う(指紋一次照合)。次に補正結果を IC カードへ送信し、IC カード内で指紋特徴点のマッチングおよびスコア算出を行う。

本方式では、個人の秘密情報である指紋の特徴点に関する情報を、IC カードから出さずに照合を行うことが可能となるため、登録側の指紋テンプレートの保護と指紋照合結果を、安全にカードに反映することができる。

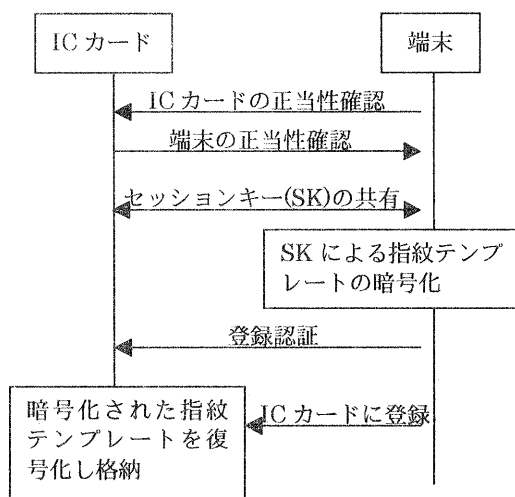


図2 IC カードへの指紋テンプレートの登録方法

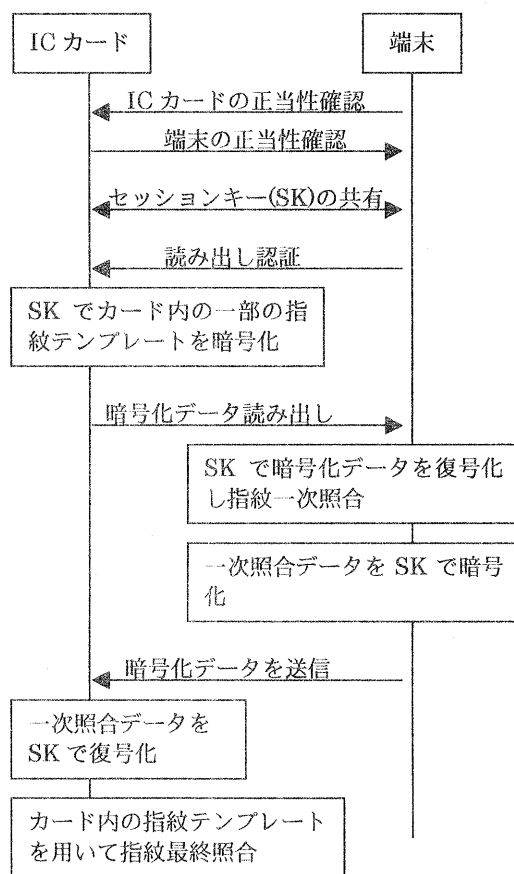


図3 IC カードによる指紋照合方法

なお、図2, 3では、カードと端末の両方の正当性をチェックしているが、端末が信頼できる場合はカードのみの正当性をチェックしても良い。

このような構成により、3.で洗い出した脅威の大半を防ぐことが可能となる。

5.まとめ

今後ICカードが普及する中で、システムに応じてICカードを用いた多種多様な認証方法が求められると考えられる。本報告では、指紋認識技術を利用したICカードの所有者確認方式における脅威を洗い出し、実現可能性とともに考えられる対策を施した指紋照合機能搭載型ICカードを利用した実装形態について考察し、報告を行った。

参考文献

- [1] 内田 薫: “指紋照合による本人認証”, 情報処理学会誌, pp1078-1083, Vol.40, No.11, 1999
- [2] 藤原秀人, 鷺見和彦, 大森 正: “指紋判別装置”, 三菱電機技報, Vol.72, No.5, pp.40-43, 1998
- [3] 坂野 鋭: “バイオメトリック個人認証技術の動向と課題”, 信学技法, PRMU99-29, pp.75-82, 1999.6.
- [4] 瀬戸洋一: “バイオメトリクスを用いた本人認証技術”, 計測と制御, pp395-401, Vol.37, No.6, 1998
- [5] Nalini K. Ratha and Ruud Bolle: “18 SMARTCARDBASED AUTHENTICATION”. , pp369-384. In Anil K. Jain et al. , ed. BIOMETRICS Personal Identification in Networked Society, Kluwer Academic Publishers. 1999
- [6] 重松智志, 森村浩季, 町田克之: “1チップ指紋認証LSI”, 電子情報通信学会, 信学技報, ED99-67, SMD99-41, ICD99-49, 1999-06
- [7] 瀬戸洋一, 三村昌弘, 石田修一: “ICカード実装型指紋照合による本人認証技術の開発”, 信学会シンポジウム SCIS2000-D01, 2000/1
- [8] 磯部義明, 三村昌弘, 瀬戸洋一: “W4 生体認識技術の開発動向”, 日本機械学会 IIP2000 情報・知能・精密機器部門講演会論文集, No.00-10, 2000, pp14-18
- [9] 霍 日洪, 村山隆彦, 平田真一, 細田泰弘: “ICカードに適した指紋認証システム”, 信学会シンポジウム SCIS2000-D02, 2000/1
- [10] 本人認証技術検討 WG 報告書, “本人認証の評価基準 (第1版)”, 平成10年3月, 電子商取引実証推進協議会, http://www.ecom.or.jp/qecom/about_wg/wg06/h9doc/98wg6doc.pdf
- [11] The BioAPI Consortium: “1.5 BIRs and Template”, pp.14, in “BioAPI Specification” Version 1.00, 2000/3
- [12] 浅井 他: “マニユーシャネットワーク特徴による自動指紋照合一特徴抽出過程一”, 信学論, Vol.J72-D-II, No.5, pp.724-732, 1989
- [13] 浅井 他: “マニユーシャネットワーク特徴による自動指紋照合一照合過程一”, 信学論, Vol.J72-D-II, No.5, pp.733-740, 1989
- [14] 笹川耕一, 磯貝文彦, 池端重樹: “低品質画像への対応能力を高めた個人確認用指紋照合装置”, 信学論, Vol.J72-D-II, No.5, pp.707-714, 1989