なりすましリスクの低減による、安心・安全な情報基盤の実現

Realization of a safe and secure information infrastructure by reduction of spoofing risk

室木勝行‡
Katsuyuki Muroki‡
†株式会社　SYNCHRO
†SYNCHRO Co Ltd

要旨

小論では、現代社会に於けるセキュリティ上の根本問題となっている、他人による本人へのなりすましリスクの問題に焦点を絞っており、これを低減化するバイオメトリック技術が抱える現状課題の克服策として、一人一台にまで普及が進んだ携帯電話番号との連動による次世代型の認証基盤「開発計画」と、バイオメトリックサービスの「実現構想」について述べている。

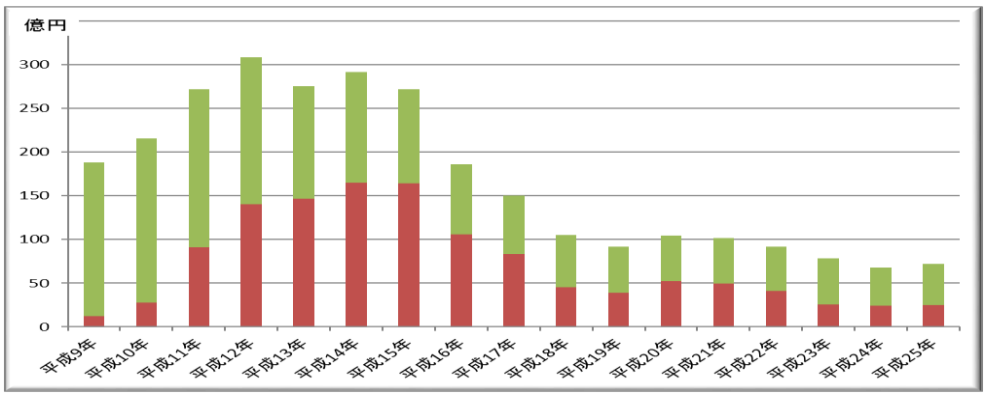
１．　はじめに

消費者と店舗等の間に於ける決済システムを巡り、米国 IT 大手企業の動きが活発になってきている。決済サービスベンチャーは各社各様の決済手法を試行錯誤し、なりすまし対策を打ち出して来ているが、明確な解決策を見出せない状況が続いている。

これらの背景は、ＩＤカードに対する偽造犯罪対抗措置であり、米国はＩＣチップカードの普及が最も遅れており、未だ磁気ストライプ型のＩＤカード環境下でなりすまし被害が多発しているからである。我が国では過去十年間に大半の銀行カードがＩＣ化されたが、読み取り側のカードリーダーの大半が未だ磁気ストライプ型が主流である為、ＩＣカードに磁気ストライプの仕組みが並存している。その結果、我が国の決済実態に占める８３％が、未だに磁気ストライプによる決済の実情である。

一旦流出したＩＤカード情報は「偽造によるなりすまし被害」を多発させており、現在我が国では経済産業省が音頭をとって、2020 年迄に決済環境全てをＩＣカード決済へ移行を図るべく業界全体に働きかけている。国際ブランドのトップである米国ＶＩＳＡでは、2015 年 10 月からクレジット業界の新ルールである「ライアビリティシフト」の導入開始を表明しており、カード偽造犯罪による損失が発生した際には、カード会社と加盟店を管理する加盟店契約会社と強調して、ＩＣカード決済環境に移行していなかった利用店舗側に債務責任を負わせることを周知し始めており、ＩＣ決済環境への移行を企業自ら促そうとする動きが本格化している。なりすましによる損害リスクを決済する店舗側が抱え込む事になる為、店舗運営に於ける決済システム更改の必要性が一気に高まる予想下にある。

我が国クレジットカード業界に於ける事犯推移は図表Ｉの通りで、ＩＣカード化により一定効果を上げている事が伺える一方、ＩＣ化された以降もなりすまし事犯が解決しない現実を物語っている。事犯の原因は「偽造によるなりすまし」では無く「正規カードによるなりすまし」であり、「不正使用」と表現されている。即ち、カードとカードリーダーがＩＣ対応されても、盗用によるなりすまし対策は未解決である事が解る。今後、なりすましリスクの低減を図る為には、「不正利用」の側面も捉え、総合的な解決手法を考案し、現代の個人認証環境に対する「個人認証基盤」を早期に構築する必要性がある。



図表Ｉ＜ 日本国内の「なりすましによる被害額　緑（上段）：不正使用 ／赤（下段）：偽造」＞

２．　なりすまし対策として注目が進む、バイオメトリック（生態認証）

我が国の銀行カードに初めて生態認証情報が搭載されたのは 2004 年。その後、ＡＴＭに静脈認証装置が普及したのが 2007 年。メガバンクを初めとした銀行並びにコンビ内に設置のＡＴＭに普及が進み企業での利用が中心であったバイオメトリックが一般消費者へと認知が進んだ。海外に於いても例えば今年、マレーシアの国民カードに指紋認証データが搭載されたＭＯＣ（Mach On Card）が採用決定する等、「正規カードによる不正利用」側面にも対処を図るべき判断がなされ、カード使用者に対するバイオメトリックソリューションシーンが拡大している。

しかしながら、バイオメトリック普及の一方で、例えば我が国のパスポートに搭載された指紋認証データが、本人の指跡から採取された指紋痕で偽造したシールによってなりすまされる事犯も発生しており、一部のバイオメトリック方式に於いてセキュリティホールが露呈している事にも注目をしなければならない。最近消費者を沸かせた一事例に、ｉフォン上に搭載された指紋認証セキュリティが破られた事件もあり、単にバイオメトリック装置を採用したからと言って完璧では無い。

一方で、携帯電話やＰＣにログオンする際に使用され始めた指紋認証や指静脈認証等は、大いに個人差も伴いますが、空気の乾湿差や寒暖差によって生体認証時に読取れなくなるケースが多数認知されており、安定的に本人認証させる実用性面に於いて問題が散見されている。

今後、バイオメトリックが様々なシーンに於いてなりすまし対策全般の対処法として応用される為には、上述の事例の通り他人を本人と間違えてしまうエラーである「他人受入率」と、本人でありながら、本人と読取れないエラーである「本人拒否率」の二側面を両立し、解決する事が必須である。

３．　次世代型バイオメトリックシステムに求める要件

3.1. バイオメトリックの課題と、課題克服策（Ｉ）

生体の一部を何らかの原理によって読み取り、本人か他人かを識別し、認証する手法の事を生体認証＝バイオメトリックと呼び、一般的に精度を示す主たる指標に他人受入率（FAR）と本人拒否比率（FRR）が起用されている。また、これら指標の多くは、一定人数の被験者を対象に、認証装置メーカー各社がサンプリングテストを繰り返した結果、一定母数のサンプリングデータから本人データと一致する確率から抽出した性能である為、寒暖差や乾湿差等の外的要因による影響を受ける実用環境下では、カタログスペックに記載された性能と実用結果から得られる性能が乖離する事が多い。理由は、FAR を高めるほど FRR を貶めてしまう反比例関係にある両指標を同一人物に当てはめる事に起因している。

解りやすく説明すると、少しの違いも認めない感度調整をし、厳格に他人を排除する「高い FAR」を

重視すると、外的要因から生じる生体側の変化が少しも許容されなくなり、「低い FRR」の維持、即ち実用性を保つ事が困難になってくる。実用性を確保しつつ、セキュリティ性も確保するには、今迄とは別次元に於いて認証の基本性能である FAR と FRR の両立を追求するアプローチを行う事が必要であり、これ等の課題克服策として、人それぞれに安定して読み取り易い身体部位のバイオメトリックデータを個人毎に複数選択できる状態を構築する事で FRR を貶めない様にする「柔軟性」を次世代型バイオメトリックシステムに取り入れる事が肝要である。

3.2. バイオメトリックの課題と、課題克服策（Ⅱ）

前項と重複するが、バイオメトリックセキュリティの性能を示すＦＡＲ（他人受入率）は、一定の被験者を対象としたサンプリングデータを元に抽出された確率論である為、万人に対して完璧に認証性能が保証され得るものでは無い為、バイオメトリック全般、セキュリティ性能の不完全性を前提とした運用がなされるべきである。この認識に立つと、データベースの中から１人対Ｎ人を検索するスキャン型の方式によって本人認証するシステムは、規模が大きくなるほど類似データ（他人）と間違えてしまう危険性が高まる為、規模の大きさによって性能が左右されない１人対１データ比較を行う PIN（Private Identification Number）即ち、ID 入力型のシステムを採択するべき事を、特に力説しておきたい。

更には、セキュリティ性能の不完全性を高次元で克服する策として、上記の PIN とバイオメトリックデータを１対１に紐付けるデータベースを形成する際に、PIN 自体を本人しか入力が出来ない仕組みにしておく対策が有効になる。従って、前項で提唱した「柔軟性」を上げる策とも関係付けて、本人しか入力出来ない PIN に対して複数の個人バイオメトリックデータを紐付け、バイオメトリックの不完全性を両面から克服する策を提唱したい。

3.3. 「新認証モデル」に求める要件骨子

入力時の安全性が高いユニーク PIN（ID）入力方式の採択を前提とする。
＋
環境に応じて複数のバイオメトリック方式が選択できる様にする事で、完全性を追求する。
＋
ワンタイムパスワード（OTP）認証手段による、最終バックアップ手段を完備する。

４．　バイオメトリック「新認証モデル」

4.1. 普遍性と唯一性を兼ね備えた、携帯番号ＩＤの採択

我が国では、一人が一台所有する携帯電話は、機種やキャリアの変更後も同じ番号を踏襲できる様にモバイルポータビリティ制度が定着しており、携帯電話番号は誰もが所有可能な唯一無二の PIN（ID）として活用可能なインフラである。此れに加え、携帯電話は極めて他人に預けられる事が嫌われる性格を持つ個人的所有物である為、自ら他人に貸す又は紛失してしまう等の局面に無い限りは、他人が使用する事が稀な究極的なセキュリティデバイスとしての存在である。新認証モデルでは、携帯電話（番号）を有効活用し、入力時の安全性が高いユニーク PIN（ID）として採択する。

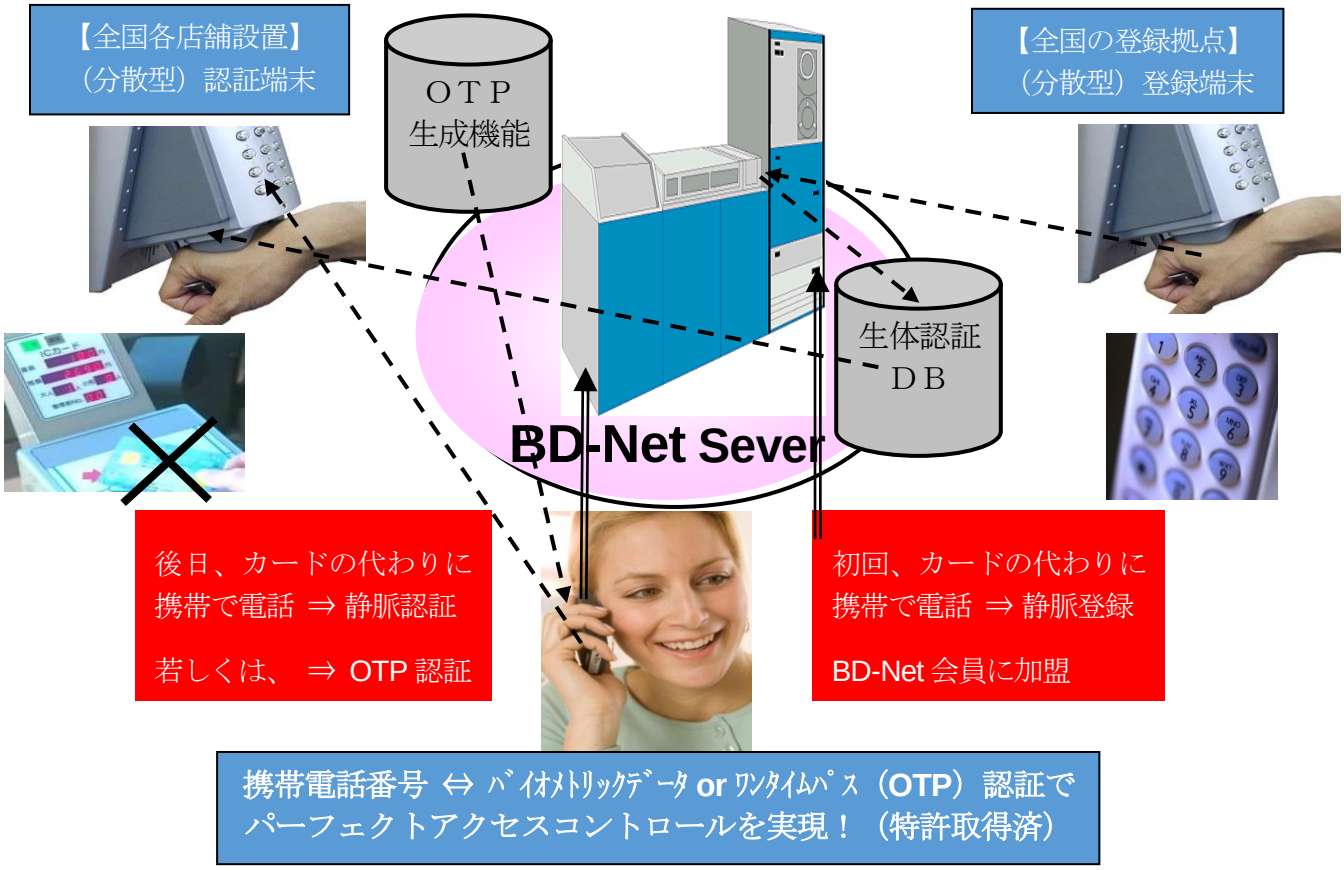
4.2. 柔軟性による完全性の追求、マルチモーダル型システムの設計

前章でも触れたが、バイオメトリックの重要な性能指標である FRR（本人拒否率）は完璧で無い為、ある環境下では、本人にも関わらず認証されない状況に陥る事を予め想定しておかなければならない。このバイオメトリックの課題、即ち不完全性を補う方策として、個々人にとって認証し易いる複数の身体部位を対象に、顔・静脈・虹彩等のバイオメトリックデータとして登録し、外的要因で変化する環境

に応じ、柔軟にバイオメトリック方式の選択が可能なマルチモーダル型システムが有効である。新認証モデルでは、静脈認証を起点としたマルチモーダル型のデータベースを設計に織り込む。

4.3. 最終的なバックアップ認証方式、ワンタイムパスワード認証機能を併設

携帯電話と言う音声通信が可能なデバイスを採択した事により、仮にも何らかの理由で全てのバイオメトリックが機能しない場面に遭遇した際、本人認証を実現する最終手段としてサーバー側が発行するワンタイムパスワードを音声に乗せて本人の携帯電話に通知する機能を用意し、最終的な本人認証手段を確保する仕様とする。此れにより、一般的に生体認証端末が設置されていない自宅等の環境に於いても、ＰＣ等の汎用性の高いテンキー入力端末に対するワンタイムパスワード入力により、図Ⅱの通り、ほぼ現代社会に於けるあらゆる認証シーンに対応が図れる事となる。



図Ⅱ ＜ BD-Net（バイオメトリックネットワーク）の実現構想＞

５．まとめ

以上、現代社会に於けるセキュリティ上の根本問題となっている、他人による本人へのなりすましリスクの問題に焦点を絞っており、これを低減化するバイオメトリック技術が抱える現状課題の克服策として、一人一台にまで普及が進んだ携帯電話番号との連動による次世代型の認証基盤開発計画と、マルチモーダル型のバイオメトリック並びにワンタイムパスワード認証補完による、複合サービスの「実現構想」について報告した。尚、本件「新認証モデル」については、2014 年 5 月に㈱ＳＹＮＣＨＲＯとして全方位的な個人認証シーンを想定してビジネスモデル特許を取得しており、引き続き、各人称シーン毎に必要となる要件を整理し、第二、第三弾の特許を申請している。今後分野別に継続的な発表に努め、社会の認証基盤の強化に於いて貢献してゆきたい。