バイオメトリクスによるモバイルエージェント保護とセキュアなエージェント指向サービスアーキテクチャについて

岡宅泰邦*

Mobile agent oriented system architecture for providing a secure service by biometrics

* Yasukuni OKATAKU

ABSTRACT

This paper prescribes an approach for providing a secure service in network environments by mobile agents (MAs) which are authenticated and protected by biometric information of their owners. By combining biometric information with shared secret information, a robust one-time key can be created to protect mobile agents and guarantees that they are totally belong to the agent's owner. The MA stores his/her finger print information encrypted by the one-time key, and authenticated by a biometric certification server (BCA server) which manages the each agent's SVM (support vector machine) classifier. The proposed security architecture would provide a mobile agent oriented secure service in the insecure network environments.

Key Words: security, biometrics authentication, mobile agent, SVM, support vector machine,

1 はじめに

生体情報は個人固有の情報であるため，認証のための秘密鍵を持ち歩く必要がなく本人認証できるという大きな利点がある．その一方，生体情報のモバイルエージェント（以下，MAと記す）への活用時における課題として，下記のような欠点が挙げられる．

(a): 生体情報読取装置によって読み取られる指紋や顔画像などの生体特徴情報(テンプレート)は，読み取り毎に全ビットデータが一致するとは限らないため，端末や認証局(BCA)サーバでの認証時に無視できない他人受理率(FAR: false accept rate)や本人拒否率(FRR: false reject rate)が常に存在する．また，いったん盗まれると代替が困難となる．

(b): BCAサーバは，膨大なテンプレート情報を常時安全に管理する必要があり，その管理負荷は大きい．また，サーバでは，各種の認証機器毎の照合エンジンを用意しておく必要がある．

(c): 単一のテンプレートによる認証では，偽指紋等による他人なりすましの危険性が高い．一方，マルチモーダル認証機能を端末に装着するのはコスト高となる．どこからでもMAを利用するには環境整備コストが高くなる．

(d): モバイルエージェント自身の所有者を特定できる方法がなかった．すなわち，MA自身の改ざん検知や暗号化はできても，そのMA自身が真正保持者により生成されたものかどうか判断はできない．以下，２章でMA保護手段について，３章でバイオメトリクス特徴データ(テンプレート)から生成した擬似生体鍵を活用したMA保護アーキテクチャ，４章でサポートベクターマシン(SVM)による本人認証手法，５章でSVM認証実験，６章でサービス指向アーキテクチャ、7章で考察そして，８章で今後の課題について論じる．

2 モバイルエージェント(MA)の保護

上述した(a)～(d)の課題に対処する方法を本章で検討する．

*情報工学科

2007年9月26日受付

2.1 バイオメトリクス認証について

(a)に対しては，複数のテンプレート情報による判定を行うことでエラー率を低減させる．また，生のテンプレート情報でなく，取り消し可能なようにテンプレートを変形することでテンプレートの取り消し可能な手法が提案されている[1]．

(b)に対しては，BCAサーバでのテンプレート管理負担をなくすことが考えられるが，ニューラルネットを利用した方法が提案されている[2]．証明者端末で証明者のテンプレート情報を訓練データとして学習させ，暗号化した学習済み重みベクトルを認証サーバに登録するものである．証明者は必要に応じて，重み情報の取消し・再登録を行うことにより，サーバでのテンプレート管理負担は解消される．本論文でもサーバでの管理負担の解消を目指す点では同じであるが，テンプレート学習方法にSVM（サポートベクターマシン）[3]を用いてその有効性と実用性について論じる．また，SVMを本人と非本人の音声を区別する手段として有効であることが報告されている[4]．

(c)に対しては，マルチモーダル認証をBCAサーバで実行させることとし，端末で生成されるモバイルエージェントには，生体情報読取装置で収集した複数のテンプレートをモバイルエージェント内部に擬似生体鍵[5]で暗合化して格納することで解決する．これにより，偽指紋等を用いて不正利用される危険性がより低減される．

(d)に対しては，モバイルエージェント（以下MAと略す）内部にテンプレート情報を格納させ，

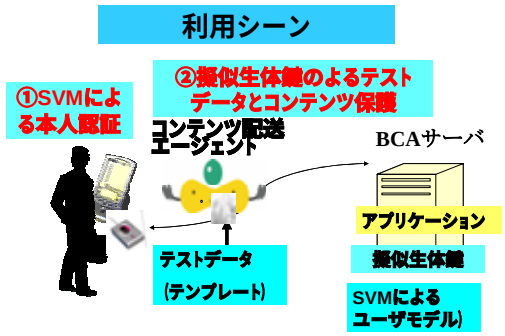

図１利用シーン

それをサーバで認証することにより，MAの真正保持者が誰であるかを確認する．本論文では，サーバに登録したユーザの特徴情報（学習モデル：サポートベクター，ラグランジュ乗数，閾値から構成）で検証するためのテストデータ（テンプレート情報）をMAに擬似生体鍵で暗号化して格納し，MAがサーバに移動して認証を受けるものである[6]．

2.2 利用シーンと利点

図１にSVMによるユーザ認証と擬似生体鍵によるMA保護方式の利用場面を示す．サービス利用者は，①PCやモバイル端末から指紋などの生体情報を①SVMによる本人認証をBCAサーバから受けた後，②擬似生体鍵で秘匿したいコンテンツ情報を暗号化したMAがBCAサーバに移動して，必要な仕事を実行する．

擬似生体鍵とSVM方式の利点は，BCAサーバには生体情報そのものは保持されない為，サーバからの漏洩の心配がない．従来の生体情報装置では，メーカ毎に仕様が異なるためBCAサーバは，ユーザが利用する機種毎の認証システムに対応する必要があり，事実上マルチベンダーシステムには対応できない．一方，SVM方式では学習モデルと判定器(プログラム)を登録するだけであるため，指紋センサー等の認証機器の仕様に依存しないという利点がある．

3 擬似生体鍵

生体情報から得られるテンプレートと秘密乱数から生成する擬似生体鍵について論じる．クライアント端末とBCAサーバで共通の擬似生体鍵pTemp(k)の生成を以下の手順で生成する．擬似生体鍵は端末とサーバで共通の秘密鍵であり，FAR，FRRともゼロで，鍵の頑健性は共通鍵方式と同等である．MAの暗号や署名に使用する．

Step-1: テンプレートを作成する．今回，指紋テンプレートとし図２に示すように，隣接するマイニューシャ(minutia)である分岐点(bifurcation point)や端点(end point)間に含まれる隆線(ridge)であるリレーション(relation)数を用いた[7]．１つの指紋に含まれる分岐点と端点から5～8程度を選択してテンプレートを作成し，耐タンパ装置に格納しておき，個人IDとの対で管理する．

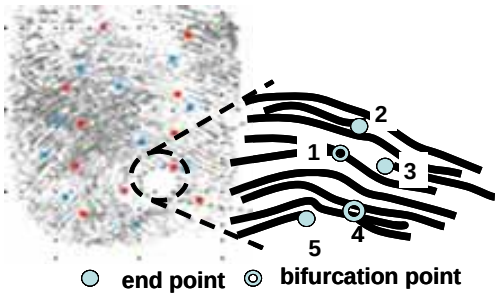

図 2 指紋特徴データ（テンプレート）例

Step-2: テンプレートが，個人固有の擬似生体鍵生成の核となる．K氏の２つのテンプレートを利用した場合は以下のように生成する．

Template(K) = (Template（人差指）‖ Template(中指）)

Step- 3:秘密乱数(=SR(K, m), m=1,…, M)とTemplate(K)より，擬似生体鍵pTemp(K, m) = hash{Template(K)‖SR (K, m) }, m=1,…, Mを生成する．ここで，hash関数はSHA_1である．複数のアプリケーションサービスに対応するため，必要個数分の擬似生体鍵を生成する．

Step-4: 擬似生体鍵pTemp(K, m)を公開鍵方式により，BCAサーバに配布する．Template，SR，pTempを自身の耐タンパ装置に格納する．

Step-5: 本人認証用のSVMテンプレートの暗号化および，MAの署名・暗号用にワンタイム擬似生体鍵OneTime(K, J) = hash[challenge(K)‖pTemp(K, J)]を生成する．ここで，challenge(K)は公開乱数である．

4 SVMによる指紋認証

サポートベクターマシン(SVM)による指紋認証方式について記す．

4.1 指紋テンプレートのSVMによる学習と認証

サポートベクターマシン(SVM)は，図３に示すように，対象データ空間を２つのクラスに分類する機械学習方式の１つであり，本実験では，SVMソフトウェアとしてSVM^{light} [8]を用いている．SVM^{light} は学習器と分類器から構成されている．認証能力の検証実験は，学習と認証の２つのフェーズから成っている．

・学習フェーズでは，

Step-1)：本人と他人の指紋テンプレートの抽出と入力データの作成，

Step-2)：SVM^{light}の学習器による学習，

を行い学習モデルを生成する．

・認証フェーズでは，

Step-3)：新たに生成した本人のテンプレート情報（SVMテストデータ）をサーバに送信し，登録済みの学習モデルと分類器により本人判定（クラス分類）

を行い予測値yi （= sign （$\mathbf{w}_t \boldsymbol{x}_i$ − b)）を算出する．算出値yiが+1近傍かそれ以上で本人と判定する．ここで，$\mathbf{w}_t$は学習済み重みベクトル，$\boldsymbol{x}_i$は学習用テンプレートベクトル，bが閾値である．他人のテストデータでは，-1近傍であることが多いが，類似したテンプレートや学習モデルの精度により+1近傍と判定される可能性がある．

4.2 入力データの生成と学習

指紋テンプレートとし図２に示すように，隣接するマイニューシャである分岐点(bifurcation point)や端点(end point)間に含まれる隆線であるリレーション(relation)数を用いる．１つの指紋に含まれる分岐点と端点から5～8程度を選択して入力データを作成する．例えば，図２の番号1と周囲４点間のリレーションはベクトルで$\boldsymbol{z}_1$ = ^{t}(1, 0, 2, 3)と表現でき，k個のマイニューシャ$\boldsymbol{z}_j$(j = 1, 2, ..., k)) から入力ベクトル $\boldsymbol{x}_i = {}^t(z_{i1}, z_{i2}, .., z_{ik})$を作成する．

作成した証明者と複数の非本人の入力ベクトル$\boldsymbol{x}_i$ をSVM^{lightt}で学習させ，ラグランジュ係数，閾

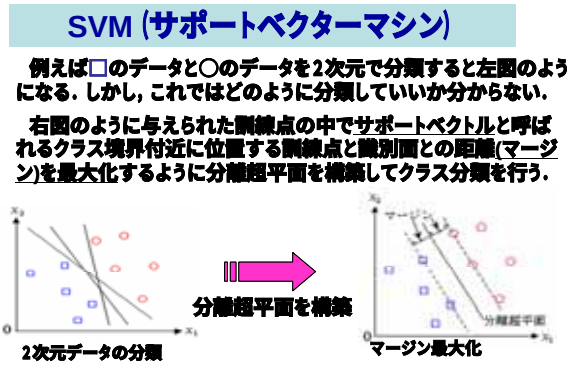

図３ 2次元データによるSVM概念の説明

値，サポートベクターから構成されるユーザの学習モデルを生成する．学習したユーザのモデルはワンタイム擬似生体鍵で暗号化しサーバに送信・登録する．MAを利用するユーザは，擬似生体鍵で暗号化した本人のテストデータ（テンプレー

ト）を認証サーバに送付し，登録された学習モデルで認証テストを受け，合格すればMAの利用を許可される．同一指の学習は，非本人のテンプレートの組合せが異なる複数の入力ベクトルにより複数の学習モデルを生成し，認証テストに用いる．これは，同一指を複数の学習モデルにより総合判定することで，他人受け入れの危険度を最小化するためである．

5 SVM認証実験

複数の証明者の特定指のテンプレートによる学習（学習に用いたカーネル関数は線形）と認証実験結果を以下に示す．リレーション情報は，異なる2本の各々について，本人および４～５名の非本人の１本の指あたり５～8個のマイニューシャから抽出した．１つのSVM学習データ（＝入力ベクトル）は，本人の1本の特定指と複数の非本人の3組合せから3種類の学習モデルを生成しさらに，特定指の3種類(1本指2種類とと2本指1種類)組合せにして都合９学習モデルを作成した．

5.1 特定指によるSVM認証実験結果

2人の証明者K, Mの特定指のテンプレートによる学習と認証実験結果を以下に示す．２名の証明者の判定結果を図4a, 4bに示す（△，□，◇は3学習モデル）．各認証時に用いる本人テストデータは，リレーションが学習時と完全に一致する場合(図中のA)からリレーション読取り誤差がある場合(図中のB～G)さらに，マイニューシャの取りこぼし(サブベクトル欠落)がある場合(図中H, I)の本人認証結果(SVM予測値)を示す．ここでHは，2つのサブベクトルが欠落しかつ読取り誤差が13%であることを示す．両証明者とも，点線で囲ったIのデータを除くと，本人予測値は+1近傍であるが，同誤り率の増大により予測値は低下傾向にあることがわかる．特に，マイニューシャの欠落の同予測値へ与える影響が顕著である．仮に本人認識の閾値を+0.７以上とすると，読取り誤差が低い場合は他人受理率(FAR)，本人拒否率(FRR)ともゼロである．一方，読取り誤差が大きい場合でも，3学習モデルのうち最大予測値を判定に用いることでFRRがゼロに近づくことが期待できるが，図2.aの実験点I(25%欠損)のように欠損データが大きいと，3モデルとも閾値以下となる場合がある．

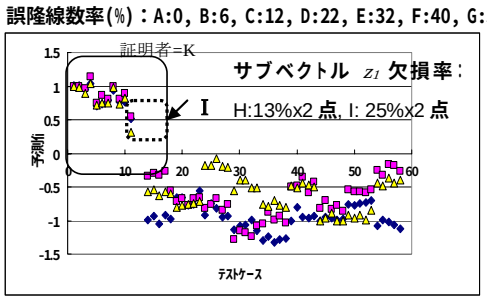

図4a 3学習モデルによる証明者Kの人差し指の判定

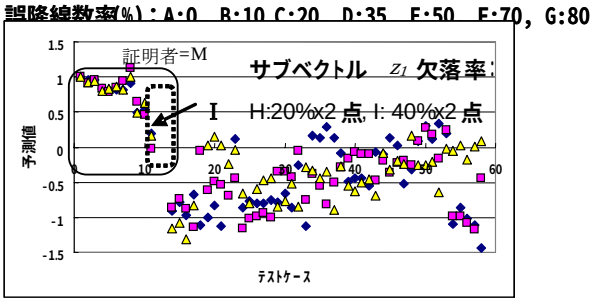

図4b 3学習モデルによる証明者Mの人差し指の判定

表１は，予測値の閾値を0.7とした時の証明者Kの４本の各指における2つのFRRとFARを示している．FRRが大きくなる条件は，大きな欠損データが存在する場合であり，リレーション読取り誤差の影響は少ない．

表1　3モデルでの指１本でのFRR，FAR率(%)

	証明者=K	親指	人差指	中指	薬指
FRR	model1	31	15	23	23
	model2	8	0	23	8
	model3	31	15	23	15
FRR Iを除く	model1	11	0	11	0
	model2	0	0	11	0
	model3	11	0	11	0
FAR	model1	0	0	0	0
	model2	0	0	0	0
	model3	0	0	0	0

5.2 2本の指によるSVM認証実験結果

証明者K, Mの2本の指テンプレートによる学習と認証実験結果を図5.a，5bに示す．非本人の学習とテストデータも2本の指テンプレートを使用している．入力ベクトル$\boldsymbol{x}_i$の次元数は1本の場合の2倍となる．図5bでは，サブベクトル$\boldsymbol{z}_i$欠損率がI(40%x2点)のうち1点の予測値が3モデルすべてで0.5以下となっているが，認証性能が欠損パ

ターン率に依存することを示している．読取り/欠損誤差が大きくなければ，1本指と2本指での認証性能に違いはない．

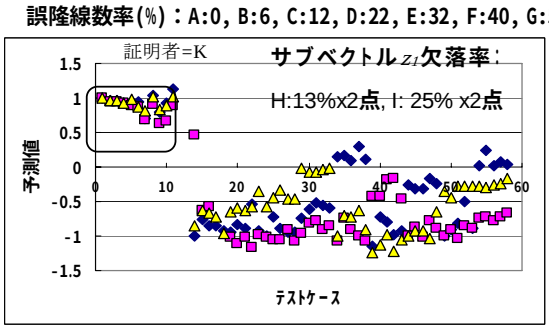

図5a 3学習モデルによる証明者Kの2本指の判定

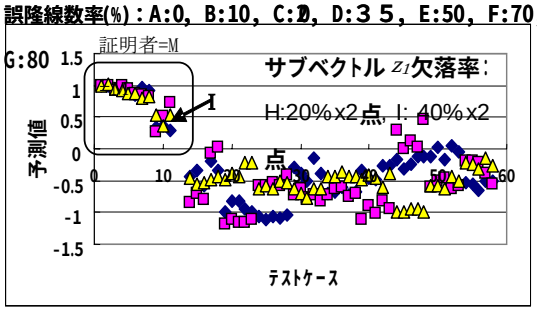

図5b 3学習モデルによる証明者Mの2本指の判定

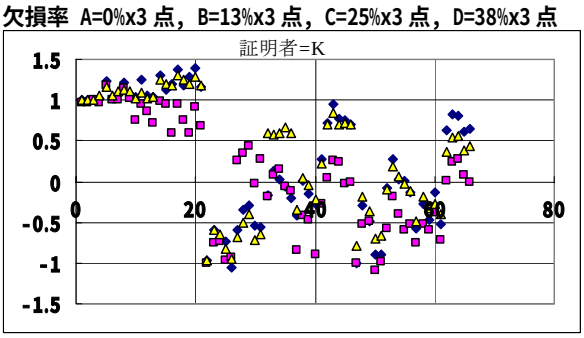

図6a シャッフル時3学習モデルによる中指の判定

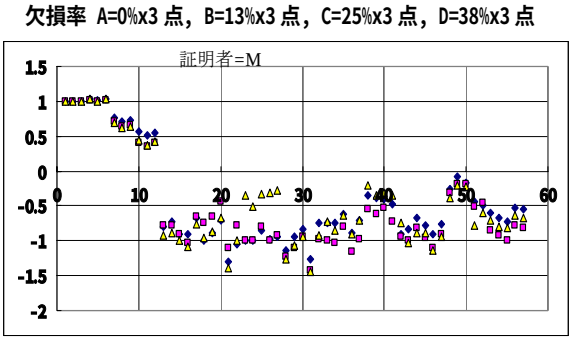

図6b 3学習モデルによる薬指の判定

5.3 サブベクトルのシャッフル時SVM認証実験結果

証明者本人のテンプレートである入力ベクトル $\boldsymbol{xi} = t(z_{i1}, z_{i2}, .., z_{ik})$は，暗号化されて認証サーバに送付されるとはいえ，生体の特徴情報そのものであるため一旦，漏洩するとその代替は困難となる．サブベクトル$z_{i1}, z_{i2}, .., z_{ik}$をランダムにシャフリングした入力ベクトル$x'_i$を本人訓練データとして使用できれば，取消し可能な生体認証(cancelable biometrics authentication)の可能性が開ける．証明者Kの中指と薬指のサブベクトルを3通りのパターンでシャッフルした時の実験結果を図6a, 6bに示す．認証時のサブベクトル読取り誤差がFARに大きく影響するケースが図6.aであり，同誤差がFRRに影響するケースが図6.bである．シャッフルして作成した学習用ベクトルは，不特定多数の非本人と類似する危険性が増大することを図6.aは示している．一方，図6bでほぼ+1と予測された非本人も他の２つの学習モデルによる予測値は0.5以下であることから，複数モデルによる認証が有効であると考えられる．

図7a，7bは2本の指によるシャッフル時の3学習モデルによる2名の証明者の判定結果である．証明者Kの予測値は証明者Mに比べて，全体的にプラス側にシフトしているが，証明者Mの方が本人と非本人の分離が良好である．図6の場合と同様，シャッフル時の方が判定精度は低くなっている．

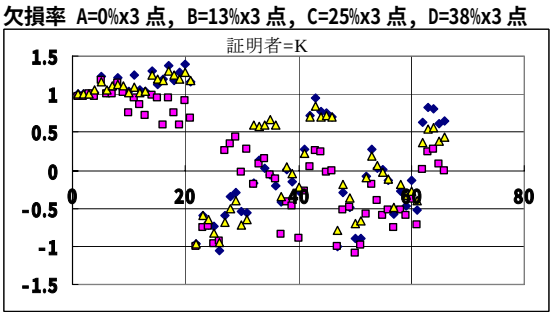

図7a シャッフル時3学習モデルによる2本指の判定

表2は証明者Kの４本の各指のサブベクトルをシャッフルした時のFRRとFARを示している．シャッフル時の特徴は，FARが非ゼロとなるケースが発生していることである．FRRについては，欠損率と読み取り率双方が影響している．

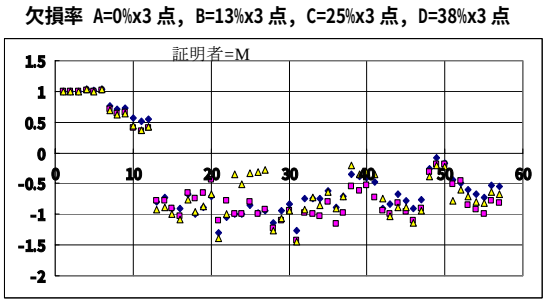

図7b　3学習モデルによる2本指の判定

表2　3モデルでの指１本のシャッフル時FRR, FAR率(%)

	証明者=K	親指	人差指	中指	薬指
FRR	model1	50	33	50	0
	mode2	33	0	50	0
	model3	50	0	17	17
FRR C, D除く	model1	33	0	50	0
	mode2	0	0	33	0
	model3	33	0	33	22
FAR	model1	0	0.09	0	0.02
	model2	0	0.15	0	0
	model3	0	0.02	0	0

5.4 全学習モデル平均によるSVM認証精度

９学習モデル（特定指各1本と2本指の各３モデルX3）による個別判定結果の算術平均総合判定する場合を考える．４名の証明者（=K, M, X, Y）の非シャッフル時の総合判定結果を図8～図11に示す．各図中の実線が9モデルの平均値である．非本人判定はモデル依存であるが，不特

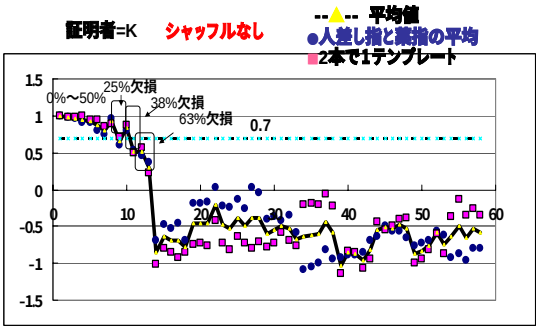

図8　3学習モデルによる証明者Kの判定

定多数の非本人を想定する必要があるため，１テンプレートにつきモデル数は多い方が非本人判定の信頼度は向上する．

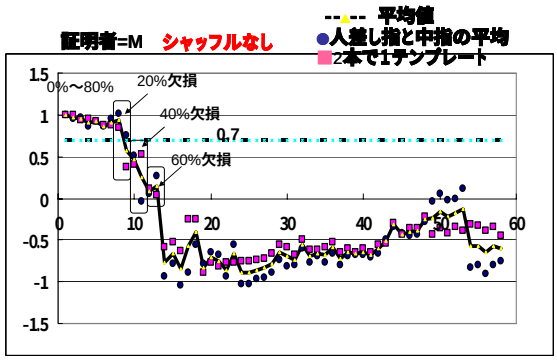

図9　3学習モデルによる証明者Mの判定

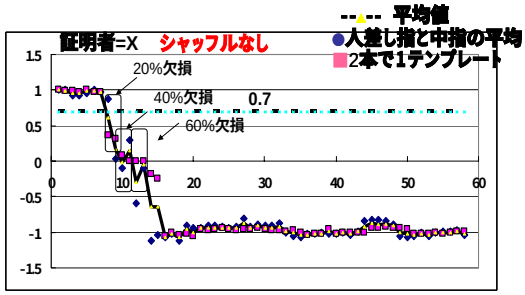

図10　3学習モデルによる証明者Xの判定

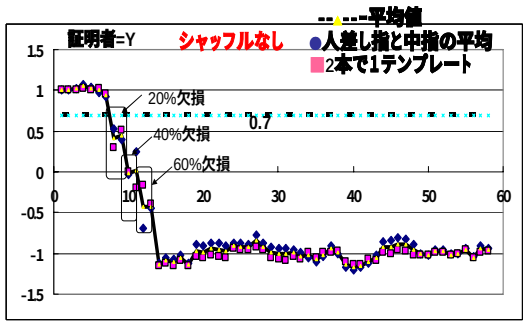

図11　3学習モデルによる証明者Yの判定

シャッフル時の総合判定結果を以下の図12～図15に示す．

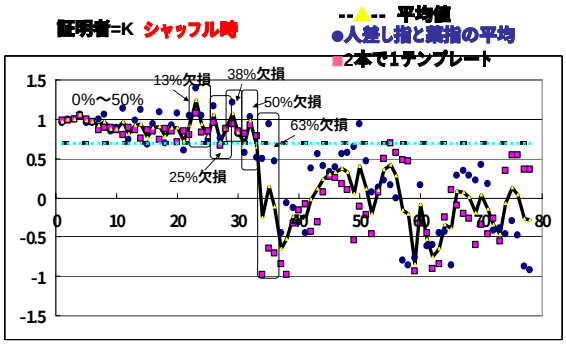

図12 シャッフル時3学習モデルによる証明者Kの判定

以下にシャッフル時の総合判定結果を図12～図15に示す．非シャッフル時と同様，平均化することにより，非本人のモデルによるばらつきが平滑化され，認証精度は向上することがわかる．

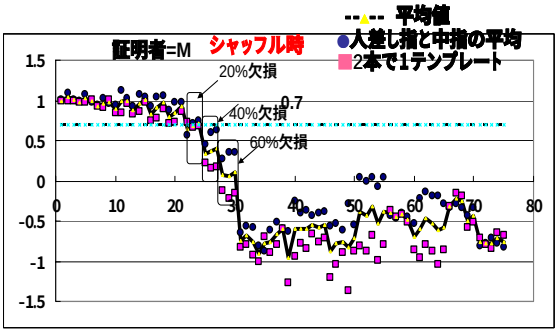

図13 3学習モデルによる証明者Mの判定

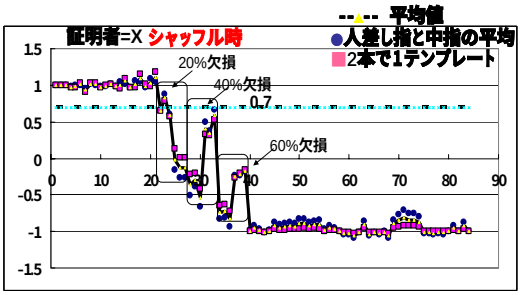

図14 シャッフル時3学習モデルによる証明者Xの判定

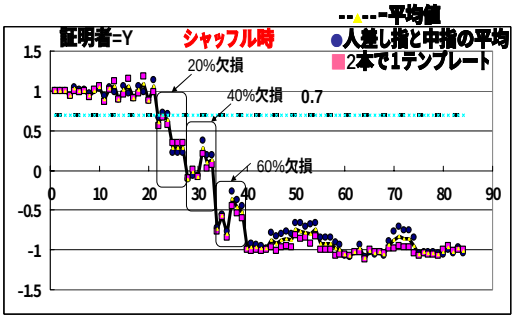

図15 3学習モデルによる証明者Yの判定

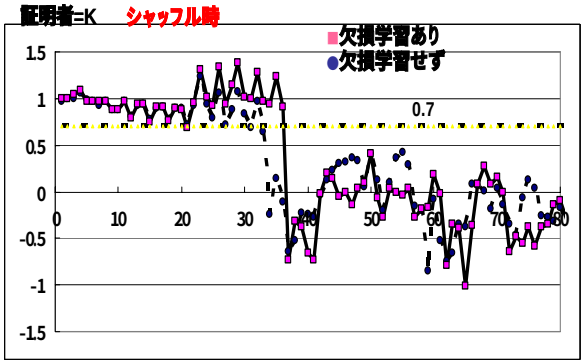

図16 読取り欠損想定時の証明者Kの判定

5.5 読取り欠損を想定した場合の全学習モデル平均による認証精度

生体情報読取り時のマイニューシャ不鮮明による読み飛ばしを想定して，想定定欠損パターンを

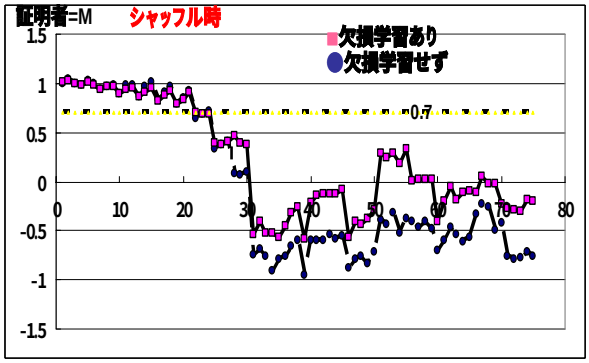

図17 読取り欠損想定時の証明者Mの判定

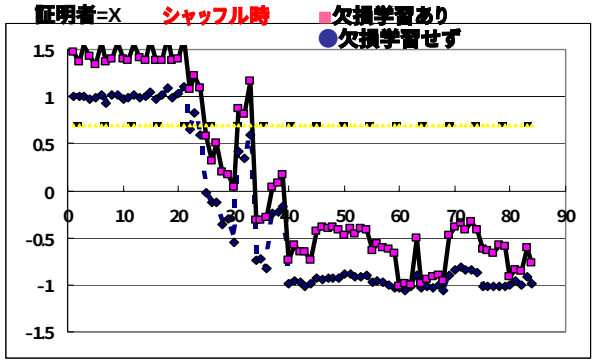

図18 読取り欠損想定時の証明者Xの判定

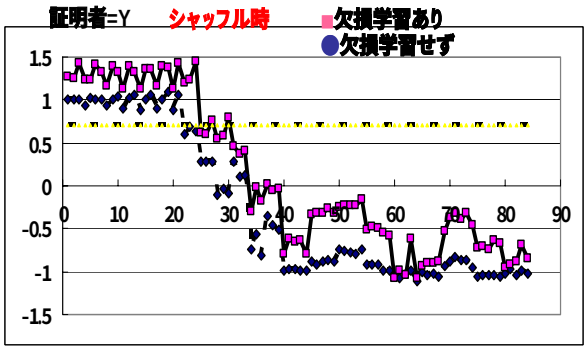

図19 読取り欠損想定時の証明者Yの判定

学習させた場合の総合判定結果を図16～19に示す．ここで，認証テストには，学習時の欠損部位とできるだけ重ならない入力ベクトルを用いた．図16が図12，図17が図13，図18が図14，図19が

図15にそれぞれ対応している．図16では認証精度は向上するが，図17では本人の認証精度の向上程度に比べ, 非本人の判定精度が劣化しているが，閾値(=0.7)を超えることはないので，FAR=0は保証されている．図18，19の証明者に関しても, 欠損を想定した学習の効果があることがわかる．

表３に図16～図19でのFRRをまとめて示す．隆線数の読取り誤差のFRRへの影響はほとんどなく，判定値が0.7を下回るのは1点(証明者K)のみである．一方，マイニューシャの読取り失敗(=欠損データの発生)に対するFRRへの影響は証明者個人間で大きく，判定の閾値を0.6に設定した場合で0%～50%の範囲で，0.5に設定した場合で0%～17%の範囲で分布する．

表３ 本実験での4人の証明者のFRR

FRR	閾値=0.7				閾値=0.6				閾値=0.5			
証明者	K	M	X	Y	K	M	X	Y	K	M	X	Y
0～80%の範囲で誤差	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	0.05	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
欠損率20%	0.00	0.67	1.00	1.00	0.00	0.00	0.67	0.50	0.00	0.00	0.50	0.50
	0.00	**1.00**	**0.50**	**0.33**	**0.00**	**0.00**	**0.50**	**0.17**	**0.00**	**0.00**	**0.17**	**0.00**
欠損率40%	0.33	1.00	1.00	1.00	0.00	1.00	1.00	1.00	0.00	1.00	1.00	1.00
	0.00	**1.00**	**0.50**	**0.83**	**0.00**	**1.00**	**0.50**	**0.83**	**0.00**	**1.00**	**0.50**	**0.50**
欠損率60%	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
	0.00	**1.00**	**1.00**	**1.00**	**0.00**	**1.00**	**1.00**	**1.00**	**0.00**	**1.00**	**1.00**	**1.00**

上段：欠損を学習せず
下段：想定欠損を学習

6 サービス指向アーキテクチャへの応用について

以上の生体情報をベースとした暗号鍵生成と認証手法をMA保護に適用することで, MAベースのサービス提供の可能性が開ける．例えば，ネットワークを介したビジネスを信頼できるものにするには, これまでのビジネスの主流であった対面での販売や交渉等のサービス形態に暗黙的に保証されていた信頼感や安心感等の安全性が担保されている必要がある. 信頼感や安心感等の安全性を担保する機能をMAに保持させることにより, 従前と同等の安全性をネットワーク上でのビジネスに付与するサービスアーキテクチャを実現し, ネットワーク上での様々なサービスの質の向上を図ることが可能にと考えられる．図20にMA指向サービスの構成イメージを示す.

従前の対面サービスと同等の信頼性をネットワーク上でのビジネスに付与するために, あたかも本人と対面しているリアリティをMAに付与する必要がある．そのため，擬似生体鍵によるサービスの暗号化とサポートベクターマシン(SVM)による本人認証によりMAが提供するサービス(コンテンツなど)の安全性と信頼性を確保するものである.

7 考察

以上の実験結果を踏まえて，本セキュリティ方式の有効性について考察する.

7.1 擬似生体鍵について

擬似生体鍵pTempは，TemplateとSRから一方向性関数により生成するので，pTempには生体情報そのものは含まれず, サーバから漏洩しても単に代替すればよい．また,ユーザが管理するので，自由に更新が可能である．pTempの頑健性は共通鍵方式に同じであり，１つのTemplateと複数のSRから複数pTempを生成し，署名や暗号の多重化を施すことで頑健性を向上させることができる．また，pTempが盗まれたかどうかをサーバ側で検証する方法として, サーバはクライ

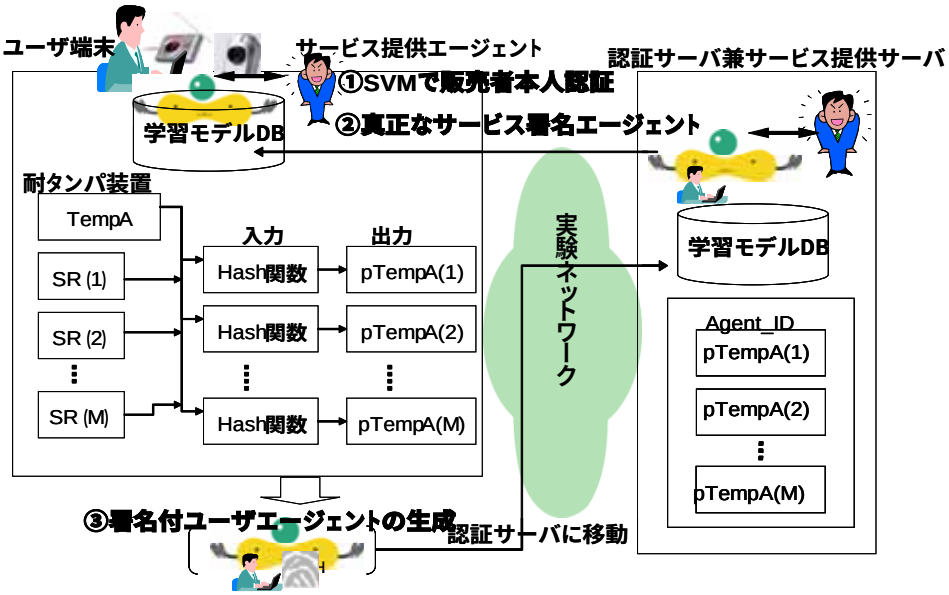

図20 エージェント指向サービスの構成

アントに対してpTemp生成に使用したSR値をクライアントに要求する方法が考えられる. この場合，SRは別のpTempとチャレンジで生成したワンタイム鍵あるいは, 公開鍵方式で暗号化してサーバに送信しておく．pTempからは生体情報が陽に読み取れないため，SVMによるユーザ認証時に以下のようなプロトコルを挿入して, ユーザ本人とpTempとの結び付きを保証する.

プロトコル：

Step_1: ユーザ側で，認証時にサーバに送信するサポートベクター(x_i: support vector)とpTempから一方向性関数によるハッシュ値h(=hash(x_i ‖ pTemp)を算出し，サーバにサポートベクターと共に送信する.

Step_2: サーバ側がSVM認証で本人確認できた場合，受信x_iとユーザのpTempからハッシュ値を算出し，pTempがSVMで認証した本人の所有であることを確認する.

以上のプロトコルを挿入することにより, コンテンツを格納したMAが真性保持者から派遣されたことが確認できる. 本プロトコルにより，鍵単体のみでは鍵の漏洩に対する脆弱性をカバーすると共に, MA流出時での追跡が可能になる. すなわち，ハッシュ値“hash(x_i ‖ pTemp)”が，ユーザのMA固有の生体情報を含むフェロモン因子の役割を果たす.

7.2 SVM学習モデルには何本の指が有効か

入力ベクトルx_iの次元は抽出するマイニューシャ数に比例するが, 今回の実験では１本の指あたりで5～10で，ベクトル次元は20～40である．２本指では２倍の次元となるが, 処理時間は無視できる範囲である．図４a,bと図５a,bを比較してわかるように，1本の指と２本の指での認証性能に大きな違いはない．悪意ある攻撃を想定すると，学習モデル生成はユーザ側で簡単に実行できるので，２本以上の異なる特定指による複数学習モデルによる総合的な判定が有効と考えられる.

7.3 取消し可能なSVM学習モデルの可能性

入力ベクトルx_iを構成するサブベクトルz_jをシャッフルして生成するx'_iを本人の擬似テンプレートとして利用する場合，組合せ数の点から2本指によるx'_iのほうが好ましい. 前章で記述したように, 本実験範囲ではFARはほぼゼロであるがその一方，FRRの危険度はオリジナルx_iでのFRRより大きくなる危険がある．異なる２本の指f1とf2からx'_i(f1)，x'_if2)，x'_i(f1, f2)で学習モデルを生成する際，z_jの読み落としを想定することでFRRが

ある程度低減することが分かった. 本実験では非本人集合が異なる3組の学習モデルを採用したが, より多くの学習モデルによる判定でFARとFRRの一層の低減化が可能であるかの検討が必要である.

7.4 対面ビジネスと同等な信頼感付与について

SVMによる本人認証と本人と関連付けられた擬似生体鍵によるMA保護機能が，ユーザとサービス提供者間の相互信頼実現に寄与可能との知見を得ることができた. 対面ビジネスと同等な信頼感を与えることができるサービスアーキテクチャを確立するには，MAプラットフォーム”Freedia”上に擬似生体鍵とサポートベクターマシン(SVM)を組込み，その有効性を実証実験環境により検証する必要がある.

8 今後の課題

本論文では，SVMを利用した利用者のバイオメトリクス認証により本人確認を確実に行うとともに，擬似生体鍵により実世界（所有者）と仮想世界(MA)の関連付けをより強固にし，仮想世界でのMAの完全性を保証するアーキテクチャを提案した. サービスアーキテクチャの確立に向けた今後の課題を以下に記す.

課題１：考察で記したように，より多くの被験者データによる実験によりSVMによる指紋認証の精度向上手法を確立する.

課題２：顔やしぐさ等の指紋以外の特徴情報へのSVMの適用を試み，指紋との併用によるマルチモーダル認証の確立を図る.

参考文献

[1] N. Ratha, J. Connel, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, vol. 40, no. 3, pp. 614-634, (2001).

[2] 永井彗，菊池浩明，尾形わかは，西垣正勝, ZeroBio－秘匿ニューラルネットワーク評価を用いた指紋認証システム，CSS2006, (2006).

[3] 大北剛（訳），N. Cristianini and J. Shawe-Taylor, サポートベクターマシン入門．共立出版 (2005).

[4] 小島 摩里子，川波 弘道，猿渡 洋，松井 知子，鹿野 清宏，非可聴つぶやき声を用いた個人認証, SCIS(2006).

[5]岡宅泰邦，明石正則，吉岡信和，本位田真一，生体情報から生成する秘密情報によるモバイルMA保護方式について，平成18年度 電気・情報関連学会中国支部第57回連合大会, (2006).

[6] 岡宅泰邦，常国絵里子，本位田真一，SVMのバイオメトリクス認証への応用について，第49回自動制御連合講演会, (2006).

[7] 画像電子学会（編），星野幸夫（監），指紋認証技術，pp.48/49，電機大出版局.

[8] T. Joachims, SVMlight "Support Vector Machine", http://www.cs.cornell.edu/People/tj/svm_light/index.html, (2004).

[9] 石川 冬樹，吉岡 信和，田原 康之，本位田 真一，階層構造制御に注目したMAフレームワークとそのマルチメディア応用, 電子情報通信学会論文誌 「ソフトウェアエージェントとその応用」特集号Vol. J88-D-I No.9 pp 1402/1417 (2005)