生体情報から生成する秘密情報によるモバイルエージェント保護方式について

岡宅　泰邦*，明石　正則**，吉岡　信和***，本位田　真一****

A method for protecting a mobile agent by secret information derived from bio-metric information

*** Yasukuni OKATAKU*, Masanori AKASHI** ,**

Nobukazu YOSHIOKA* and Sinichi HONIDEN******

ABSTRACT

This paper prescribes an approach for authenticating and protecting mobile agent in a client-server type authentication system. By combining biometric information and 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 created pseudo-biometric key doesn't contain FAR (false accept rate) or FRR (false reject rate).

1 はじめに

近年，モバイルエージェントをコンテンツ配信などに適用するさまざまな試みが提案されている[1]．また，指紋等の生体情報を利用したセキュリティ機器の導入も進みつつある．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，生体情報のエージェント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ことはないため，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):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．どこからでもモバイルエージェントを利用するには環境整備コスト高となる．

(c):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，モバイルエージェント自身の改ざん検知や暗号化はできても，そのエージェント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．

本論文は以上の課題点に対して，生体情報の持つ利点を最大限に活かしながら，ネットワーク上を移動するモバイルエージェントを保護する手法について提案するものである．

2 解決手法

以上の(a)，(b)，(c)の問題点を解決して，モバイルエージェンの自由で安全な活用を実現するために，以下のような手段を講ずることにより，問題解決を図るものである．

(a):生体情報から得られるテンプレートそのものをエージェント認証に用いないで，テンプレートと秘密乱数から擬似生体鍵を生成し，耐タンパ装置内とBCAサーバに格納しておき，擬似生体鍵をエージェントの暗号や署名に使用する．擬似生体鍵は端末とサーバで共通の秘密鍵であるためFAR, FRRともゼロで，鍵の頑健性は共通鍵方式に同じである．しかしながら，耐タンパ装置が盗難され偽指紋等を用いて不正利用される危険性がなお存在する．

(b):マルチモーダル認証をBCAサーバ側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，指紋・顔・虹彩・手書きサインなどの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．

(c):モバイルエージェントに真正保持者固有のエージェントであることを示す情報をエージェント内部に保持することで解決

*情報工学科　** 日本テレコム(株)
*** 国立情報学研究所　**** 国立情報学研究所，東京大学

2006年9月25日受付

する．モバイルエージェント内部の時間的に不変な領域(例えば，プログラムコード部や不変データ部であるが，一番簡単な指標はagent_IDで，これはチャレンジレスポンスにおけるチャレンジ情報で，公開されている)と耐タンパ装置内の擬似生体鍵で算出されるハッシュ値= h(擬似生体鍵 ‖ agent_ID)をモバイルエージェント内部に格納させる．すなわち，BCAサーバ側は，移動してきたモバイルエージェント内部の複数のテンプレートの認証後に，該当するユーザの擬似生体鍵でハッシュ値を検算して成功すれば，モバイルエージェントが真正保持者により生成されかつ，当該モバイルエージェントが真正保持者固有のものであることが保証される．

プレートと記す）登録処理を行う．テンプレートは耐タンパ装置に格納しておき，個人IDとの対で管理する．テンプレートが，個人固有の擬似生体鍵生成の核となる．ここで，agentID=個人IDとする．一例として，K氏のテンプレート(= Template)は以下のように生成する．

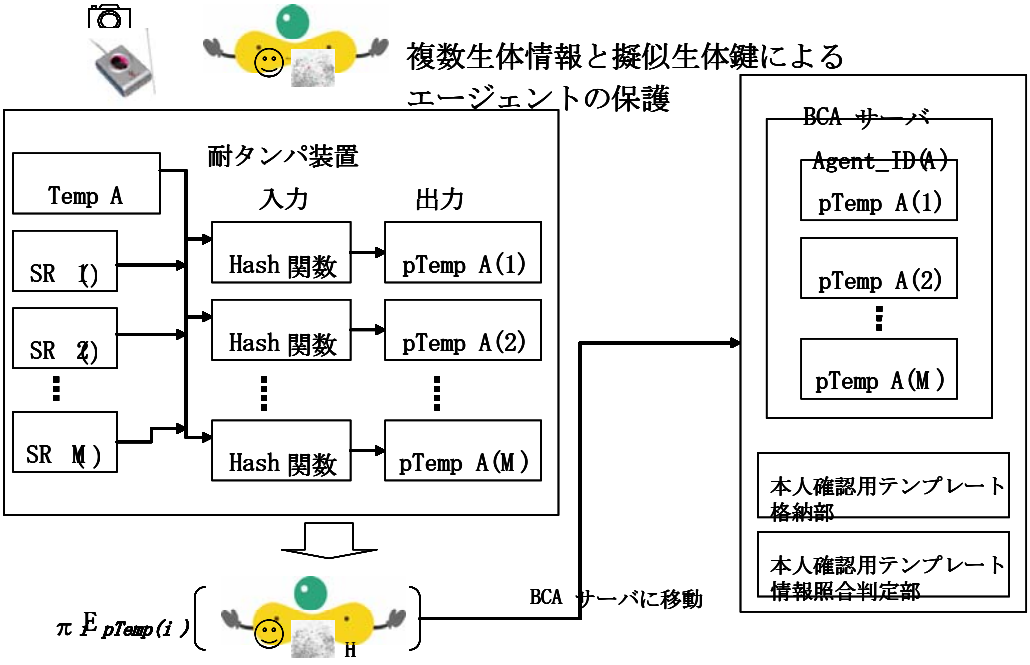
Template(K) $\stackrel{def}{=}$ Template（人差指）‖Template(中指) ‖Template(薬指)

b):秘密乱数，テンプレート管理XML-DB処理：K氏の個人ID(=agentID(K)毎に，秘密乱数(=SR(K, m))，Template(K)，agentID(K)をXMLで管理する．agent(K)は複数個のSR(K, m), m=1, 2, …, Mを登録できる．

c):ワンタイム擬似生体鍵 pTemp(k, J)の生成・付与処理：pTemp（K, J）= h[challenge(K) ‖ Template(K) || SR（K, J）]，鍵長は160bitで，hash関数hはSHA_1を使用する．challenge(K)は公開乱数である．アプリケーションサービス単位にpTemp(K, J)を生成する．

d):pTemp(K, J)でagent(K)の暗号化処理：例えば，3つのpTemp(K, J)による暗号の3重化処理 = $E_{pTemp(K,3)}[\ E_{pTemp(K,2)}[\ E_{pTemp(K,1)}$ [agent_body]]]も可能である．

e):改ざん検証用事前処理：pTemp(K, 1)でagent(K)コード部のハッシュ値H_K=



$\pi E_{pTemp(i)}$：複数の擬似生体鍵で多重暗号化

図1 擬似生体鍵によるエージェントの保護

3 クラス構成

クライアトと認証サーバ側におけるクラス構成を下記に示す．

3.1 クライアト側の構成

以下の機能構成となっている．

a):指紋センサーによる登録処理：本人認証用でなく，エージェント用認証･暗号用鍵生成のための生体特徴データ（以下，テン

h(pTemp(K, 1)‖agent(K)コード部)を算出し，{challenge(K), H_K}をagentに添付する．

3.2 認証サーバ側の構成

agent(K)のワンタイム擬似生体鍵pTemp(K, J)の認証：サーバ側のテンプレート管理XML-DBより，移動してきたagent(K)からpTemp(K, J)を再計算し，改ざんの有無を検証するとともに，エージェントの真正性を確認する．

4 考察

本提案手法の見込まれる有効性について検討する．

4.1 なりすましに対する防衛力について

ユーザとサーバでの相互認証に使用する共通秘密鍵がユーザのテンプレートをベースに一方向性関数を用いて生成されるため，単に鍵そのものの真正性を保証するのでなく，ユーザその人を認証することができ，生体認証の持つ利便性を保持することができる．他人がなりすますには，テンプレート情報を盗み出す必要がある．また，本提案の擬似生体鍵はいつでも取り消しが可能でかつ，新たな擬似生体鍵の生成も簡単にできるという利点があるので，外部からの脅威に対して頑健である．

4.2 認証と暗号の頑健性について

本文では，SHA-1で擬似生体鍵を生成しているので，その鍵長は160ビットで，3DES[3]暗号の強度に等しい．

4.3 他人受理率(FAR)と本人拒否率(FRR)について

指紋や掌などによる認証では，無視できないFARとFRRが存在するのに対して，本提案手法では，従来のディジタル鍵認証方式と同様，FARやFRRはゼロである．

5 おわりに

今後，モバイルエージェントのプラットフォーム上[2]に実装し，動作検証を行う．本研究の一部は，平成18年度の総務省「戦略的情報通信研究開発推進制度」の支援を受けて実施したもので，ここに記して謝意を表す．

参考文献

[1] 吉岡信和，田原康之，本位田真一，モバイルエージェントによる柔軟なコンテンツ流通を実現するアクティブコンテンツ，情報処理学会論文誌：データベース，Vol.44, No.SIG 1(TOD 20) pp 45-57 (2003年12月号).

[2] 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モバイルエージェント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年9月号).

[3]ブルース・シュナイアー，暗号技術大全，ソフトバンクパブリッシング(2003年6月).