生体認証を利用したセキュアネットワーク通信

前羽　理克　渡邊　晃

我々の生活を構成する全てのものを、ネットワークで結合するという“ユビキタスネットワーク”という考え方がある。これを実現することにより、我々は“いつでも、どこでも、誰でも”情報を取得することができるようになる。しかし、犯罪者が情報を盗み盗みやすくなると言い換えることもできる。そのため、ユビキタスネットワークを実現するには個人を特定する個人認証技術が非常に重要になる。現在、ユビキタスに対応した認証技術としては、IC カードと生体認証を復号利用するものがある。しかし、既存システムでは非接触型 IC カードとの整合性や処理速度の問題がある。本論文では、生体認証・非接触型 IC カードを利用したユビキタスネットワークに適した認証システムを実現する方法を提案する。

Secure network communication using Biometrics

Masakatsu Maeba　Akira Watanabe

There is a view of the "Ubiquitous network" of combining in a network all the things that constitute our life. By realizing this, we can acquire information now for “anyone,always,anywhere”. However, an offender can also put it in another way as stealing and becoming easy to steal information. Therefore, the individual attestation technology of specifying an individual for realizing a Ubiquitous network becomes very important. Now, as attestation technology corresponding to Ubiquitous, there are some which carry out 復号 use of an integrated circuit card and the biometrics. However, in the existing system, there are adjustment with a No-contact IC card and a problem of processing speed. In this paper, the method of realizing the authentication system suitable for the Ubiquitous network using biometrics and the No-contact IC card is proposed.

1. はじめに

現在、我々の身の周りには、IP 電話や電子商取引など、インターネットを利用したサービスがあふれている。このように、ネットワーク技術は我々の生活に深く浸透しているわけだが、これをさらに発展させたものとして、“ユビキタスネットワーク”[1]がある。ユビキタスネットワークとは、我々の生活を構成するあらゆるものをネットワークで接続し、“いつでも、どこでも、だれでも”情報を取得することができるという構想である。このように、ユビキタスネットワークは我々にさらなる利益をもたらしてくれるが、“情報盗用・なりすまし”など、犯罪者に対しても利益を与えてしまうというリスクを有している。そのため、ユビキタスネットワークを実現するに当たって、情報の盗用を防ぐ暗号技術や、不正アクセスを防止するための認証技術は非常に重要である。

認証技術には、パスワード・磁気カードなど様々なものが存在するが、ユビキタスネットワークに対応した認証技術としては、IC カードと生体認証を利用した物[2]が注目されている。

生体認証は指紋や静脈など人間の身体的特徴を利用するという、個人認証のある種の究極の形である。身体的特徴を利用するため他の認証技術と違い、認証情報の特別な携帯・記憶の必要がないため、ユビキタスに適応した非常に高い利便性を有している。しかし、その反面、生体情報は他の認証情報と違い数に限りがあるため、盗用時のリスクが非常に高いという特徴をもっている。また、生体認証を利用する場合、認証に利用する生体情報テンプレートをあらかじめどこかに保存しておく必要がある。通常の認証の場合、保存場所としては Server などが上げられるが、これは生体情報を他人の手に委ねることになり、User によってはこれを生理的に嫌う場合もある。そこで、これらのリスクを解決するために IC カードが利用される。IC カードは内部に CPU を保持しており、秘密情報を外部に漏らすことなく、暗号・認証を行うことができる。また、外部からの不正なアクセスを防止する耐タンパ性を有している。このように、IC カードは非常に高いセキュリティを有しており、さらに携帯性も高い。この IC カードに生体情報テンプレートを格納させることで、先ほどあげた生体認証の欠点を補うことができる。

ユビキタスネットワークに適応した IC カードを使用する既存の生体認証システムの処理の流れとしては、まず生体情報を抽出し、IC

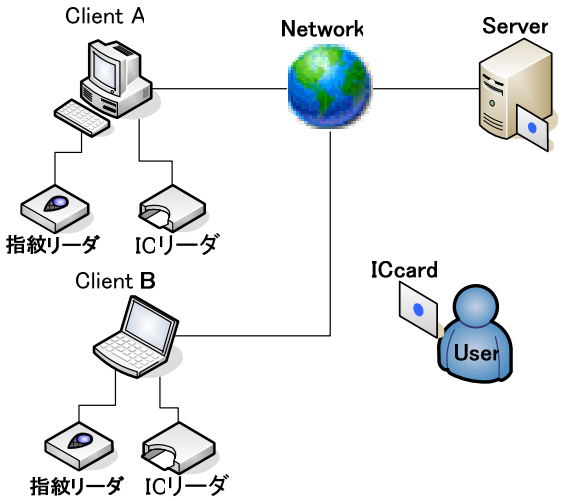


図 1 既存システム構成図

カード内のテンプレートと照合を行う。その照合が正しければ IC カード内に保管してある暗号鍵を利用して、Server と認証を行い IC カード・Server 間でセキュアな通信路を構築する。その後、Client は IC カードを通じて Server とセキュアな通信を行う。以上が一般的な流れである。また、このシステムは Client に認証情報を所持させないことによって、ユーザがどの端末からでも認証を行えるという特徴を有している。しかし、この特徴はシステムの問題点の原因ともなっている。また、近年普及しつつある非接触型 IC カードとの相性を考慮する必要もある。

本研究論文では、既存技術の問題点を解決するとともに、非接触型 IC カードでも認証が可能であるシステムを提案する。

2. 既存指紋認証システム

2.1. システム構成

既存システムの構成を図 1 に示す。この構成は、提案方式でも使用するものである。

システムはネットワークを介して行われる、Client-Server 型の認証システムである。各 Client には IC カードリーダ及び指紋リーダがあらかじめ備え付けられている。Client には固定式以外に、ノート PC のような移動式の端末も存在し、認証サーバに接続できる環境であれば、どこからでも認証が行うことができる。また、ユーザには IC カードを所持させる。これにより、IC カードを所持していればどの端末からでも認証を行うことができる。以上の動作を実現するために、Client には認証に関する情報は所持させない。

Server	IC カード公開鍵：Pui Server 秘密鍵：Prs
IC カード	IC カード秘密鍵：Pri Server 公開鍵：Pus ユーザ ID：IDu
Client	初期情報なし
指紋リーダ	指紋情報：B

表 1 既存システム初期情報一覧

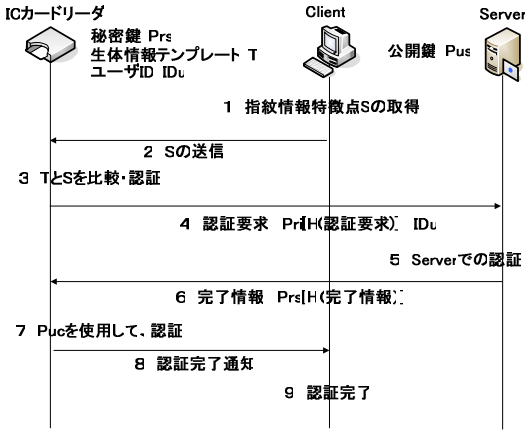


図 2 既存システムシーケンス

また、IC カード（with リーダ）・Client・指紋リーダはあらかじめ暗号通信が可能であるものとする。

2.2. 処理シーケンス

既存システムの処理シーケンスを以下に示す。（図 2）

各機器が保持する初期情報を表 1 に示す。特徴としては、Client には初期情報を保持させない点がある。

1. 指紋リーダより指紋データを取得し特徴点：S を抽出する
2. 抽出した特徴点：S を IC カードに送信する
3. IC カードは受け取った S とあらかじめ保持しているテンプレート：T とを比較・照合する。
4. 照合結果が正しければ、Pri を利用してディジタル署名を作成し、ユーザ ID：IDu とともに送信する。
5. 署名を受け取った Server は Prs を利用して、認証を行う。
6. 認証が通れば、Prs を利用してディジタル署名を作成し、IC カードに送信する。
7. IC カードは、Pri を利用して認証を行う。
8. 認証が通れば Client に対して認証完了通知を送信する。
9. 以後、Client と Server は IC カードを通じて

通信を行う

2.3. 問題点

既存システムは、IC カードを利用した認証という特徴と、Client に情報を保持させないという特徴を有しており、これらはシステムの利点になっている。しかし、これらの特徴は同時に２つの問題点も生み出している。

１つめは、非接触型 IC カードとの互換性である。現在、IC カードは従来の接触型から、より利便性の高い非接触型へと需要が移っている[3]。このことから、非接触型 IC カードの利用も考慮する必要があるが、既存システムでは問題が生じる。接触型 IC カードの場合は、IC カードを差し込むことで物理的に接続でき、ある程度セキュリティを確保することができる。しかし、非接触型 IC カード[4]の場合は、無線で通信するため明確に暗号方法を定義する必要がある。ユビキタスネットワークでの利用を考慮すると、User は任意のリーダを使用できるのが望ましいため、IC カード・リーダ間であらかじめ暗号化のための情報を保持させておくことはできない。そこで、任意のリーダ（Client）でも IC カードとの間で暗号通信を行う方法が必要になる。

２つ目の問題点は、処理速度の遅延がある。既存システムでは、Client⇔Server での通信のたびに IC カードでの処理が発生する。しかし、IC カード内の CPU は PC の物に比べるとはるかに性能が劣る。そのため、速度に遅延が生じてしまう。これを解決するには、生体認証後は Client⇔Server で直接通信する必要がある。

3. 提案方式

２．３節で既存システムの問題点の解決方法として、IC カード・Client 間のセキュリティ、Client・Server の直接のセキュア通信を提案した。この２つをまとめると、IC カード・Client・Server を完全に独立させ、３者間での認証を実現するという結論にたどり着く。この場合、考慮すべき通信経路は、Client⇒IC カード、IC カード⇒Server、そして Client⇔Server の３つが存在する。しかし、既存システムでは、Client に情報を所持させないという特徴から、Client⇒IC カードの暗号化、Clinet⇔Server の暗号化・認証を行うことができない。そこで、Client に情報を所持させないまま、上記の２点を実現する方法を提案する

3.1. 問題点解決方法の提案

暗号及び認証をおこなうには、両端点で情報を所持する必要がある。しかし、Client はあらかじめ情報を保持できないので、処理を実行するたびに情報を取得する必要がある。Client が情報を取得する方法としては、他の場所から取得する方法と Client 自身で生成する方法がある。このように、Client が関わる通信には鍵の取得方法やその時使用する暗号アルゴリズムの選定が重要である。

- **Client⇒IC**

この通信路では認証は生体情報を利用して行うため、暗号通信方法のみ新たに設定する。暗号通信には共通鍵暗号方式と公開鍵暗号方式[5]がある。前者の共通鍵暗号方式は鍵を事前に共有する必要があるが、システムの性質上 Client には鍵を保持させることができないため、利用できない。対して、公開鍵方式で双方向の暗号通信を実現するためには、自分の秘密鍵をそれぞれ所持する必要がある。しかし、今回は Client から IC カードへの通信のみ暗号化できればよいので秘密鍵を所持するのは IC カードのみとし、Client は公開鍵をその都度取得することによって Client⇒IC カードで暗号通信が可能である。よって、Client に情報を所持させずに暗号通信を実現できる。以上の理由により、Client⇒IC カードの暗号化には公開鍵暗号を使用する。

- **Client⇔Server**

この通信路は、別システム（SSL 等の既存の暗号通信システム）を利用することも考えられるが、同システム内で実現するほうがセキュリティ面でも運用面でも実用的である。以上の理由により独自の処理方式を提案する。

Server⇔Client で暗号化および認証を行うにために使用する暗号方式を選定する。

鍵を他の場所から取得する場合、鍵の取得時のセキュリティが重要になる。共通鍵の場合、鍵を暗号化して取得する必要があるが、Client はそれを復号することができない。公開鍵方式の場合、公開鍵は平文で取得することができるが、秘密鍵は暗号化して取得する必要がある。本処理は暗号化および認証が必要であるため、公開鍵のみでは要求される動作を実現できない。よって、鍵を他の場所から取得するのは適当ではない。

次に Client で鍵を生成する方法を考える。Client で鍵を生成する場合、その鍵を安全に Server に送信し、共有できるかが重要である。

しかし、Client⇒Server へ直接かつ安全に鍵を送信することはできない。そこで、Client⇒IC カード、IC カード⇒Server を通じて送信することにする。Client⇒IC カード間の暗号通信はすでに確保してある。また、IC カード⇒Server 間はそれぞれ情報を所持することができるので、暗号通信は実現可能である（具体的な方法はこの後説明する）。よって、この経路を利用することで、Client で生成した暗号鍵を Client・Server 間で安全に共有することができる。この方式を使用するさいには、公開鍵方式は鍵生成に時間がかかるため適当ではない。よって共通鍵方式を使用することにする。また、共通鍵方式は 1 つの鍵ペアで双方向の暗号化・認証を実現することができるため、Client⇔Server の認証処理と暗号通信の両方を 1 つのシステムで実現することができる。

以上の提案方式を利用することで、認証時・認証後の通信に使用する通信路の暗号化・認証を実現することができる。

3.2. 提案システム

3.2.1. 提案システムの機能

既存システムの利点を損なうことなく、新たな機能を加えることによって、新たなシステムを提案する。そのため、システムの機器構成は既存システム（図 1）と同じである。提案システムの機能としては、以下の通りである。

- 現在の社会事情を考慮して、インターネットを介した、Client・Server 型のシステムで、User の認証に生体情報を利用する
- 生体情報の盗用時のリスクを考慮して、生体情報テンプレートは IC カード内に格納する
- User は Client を選ぶことなく、どの端末からでも認証をおこなうことができる
- Client はデスクトップ等の固定式以外に、ノート PC のような移動式の端末も使用可能である
- 指紋から DNA まであらゆる生体認証技術に応用可能である。

3.2.2. システムシーケンス

提案システムのシーケンスを以下に示す。シーケンス内で、

Ea[Z]：データ Z を鍵 a で暗号化したデータ
H(Z)：データ Z のハッシュ値

を示している。また、初期情報は表 2 の通りである。

Server	IC カード公開鍵：Pui Server 秘密鍵：Prs
IC カード	IC カード秘密鍵：Pr Server 公開鍵：Pus ユーザ ID：IDu IC カード公開鍵：Pui
Client	初期情報なし
指紋リーダ	指紋情報：B

表 2 提案システム初期情報一覧

a）ユーザ認証シーケンス（図 3）

初期情報として、IC カードには Client⇒IC カードの暗号化・IC カード⇒Server の認証用秘密鍵：Prc、生体情報テンプレート：T、ユーザ ID：IDu が格納されている。IC カード内の Prc と IDu は 1 対 1 でユニークである。Server には IC カード⇒Server の暗号化用秘密鍵：Prs を格納する。Client には情報は所持させない。また、Prc・Prs に対応する公開鍵 Puc・Pus はネットワーク上に公開されており、各端末はネットを通じて取得できる。

1. IC カードから Client へ公開鍵：Pui を送信する。
2. Client は生体情報リーダを介して、生体情報特徴点 S を取得する
3. Client で Server⇔Client で使用する乱数 R（共通鍵）を生成する
4. S を R で暗号化し、R を Puc で暗号化する。その後、パケット Epuc[R] | R[S] | Puc を IC カードへ送信する。
5. IC カード内で、まず Prc で Epuc[R]を復号し R を取得する。次に取得した R で R[S]を復号し S を取得。
6. S とテンプレート：T とを比較・認証を行う
7. 認証が通れば、R を Pus で暗号化する。次に、Epus[R] | IDu のハッシュをとり Prc で暗号化する。そして、パケット Epus[R] | IDu | Eprc[H(Epus[R] | IDu)]を Server に送信する
8. Server は IDu を参照して、Prc に対する公開鍵：Puc を取得する。
9. Puc で Eprc[H(Eprc[R] | IDu)]を復号し、Eprc[R] | IDu のハッシュ値と比較・認証をおこなう
10. 認証が通れば、Server の秘密鍵：Prs で Epus[R]を復号し R を取得する。
11. 提供情報：D を R で暗号化するともに、そ

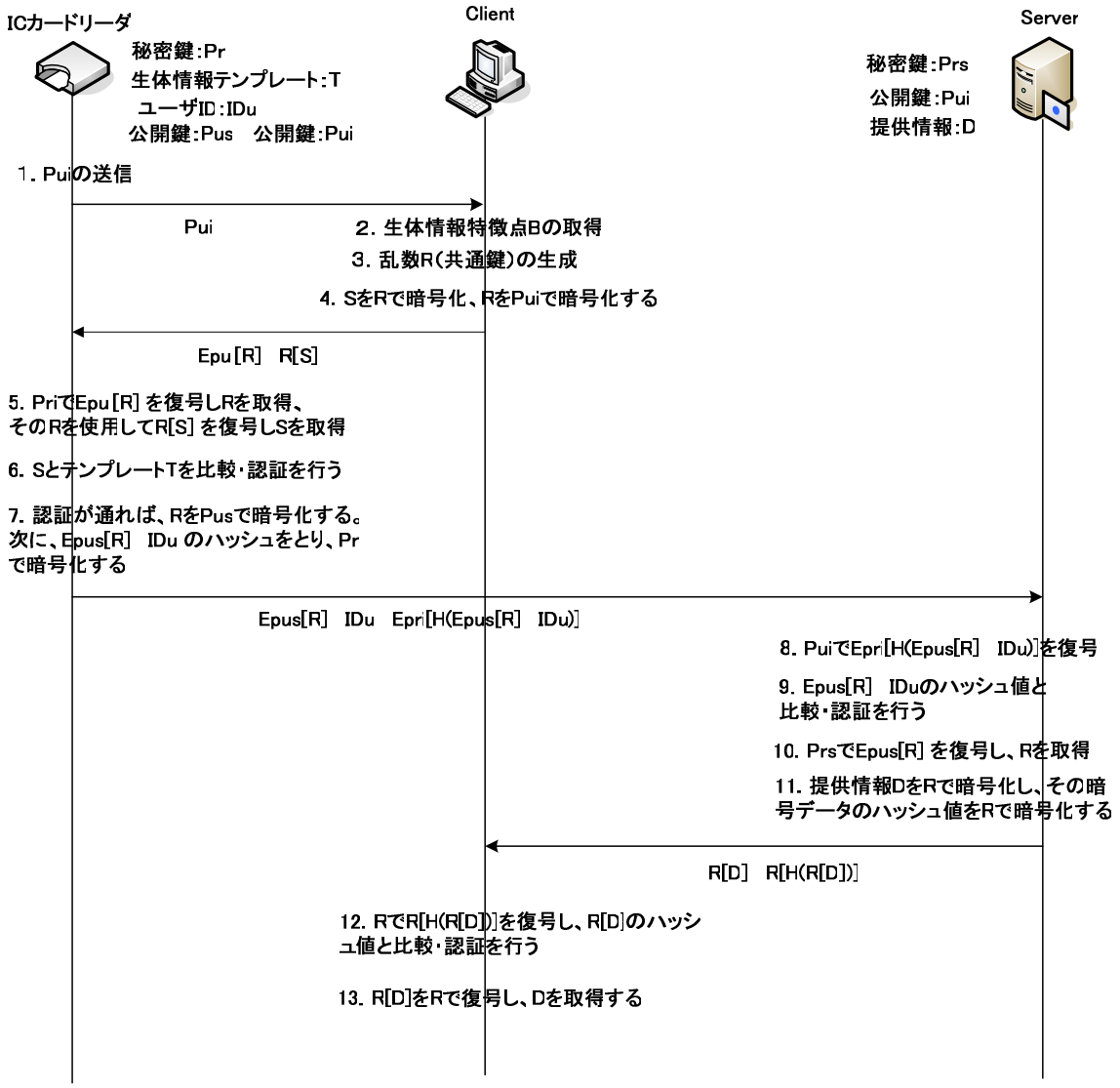


図３ 提案システムシーケンス（認証部分）

の暗号データのハッシュ値をR で暗号化する。その後、R[D] | R[H(R[D])] を Client に送信する

12. Client は R で R[H(R[D])]を復号し、R[D]のハッシュ値と比較・認証を行う。
13. 認証結果が通れば、R[D]を R で復号し D を取得する

b）認証後のセキュア通信シーケンス（図４）

認証後の通信シーケンスを示す。

Client⇒Server 時と Server⇒Client 時の処理は同一である。Client・Server は共通鍵：R をそれぞれ保持している。

1. 送信情報：D を R で暗号化するとともに、その暗号データ：R[D]のハッシュ値を R で暗号化する。その後、R[D] | R[H(R|D)]を相手側へ送信する
2. 受信側は、R で R[H(R[D])]を復号し、R[D]のハッシュ値と比較・認証を行う
3. 認証が通れば、R[D]を R で復号し D を取

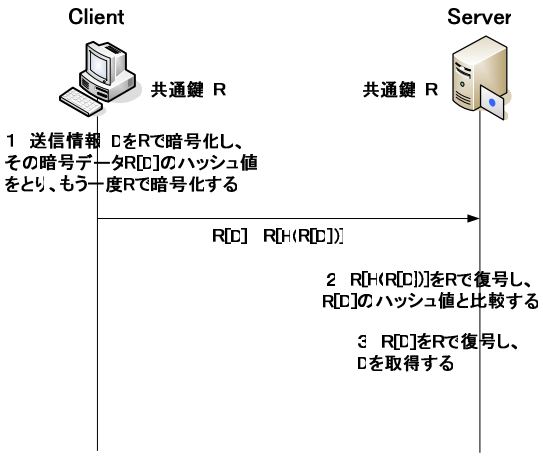


図４ 提案システムシーケンス（認証後）

得する

以上の処理を何度も行うと、送信データから暗号鍵が特定されてしまう可能性がある。そこで、セキュリティを向上したい場合は、R を新たに生成し送信情報として上記のシーケンスに乗せて新しい鍵の共有を簡単にかつ安全に行うことができる。

4. 提案システムの実装

4.1. 開発環境および実装方法

今回は、IC カード・Server・Client の処理それぞれをモジュール化し、PC 内で仮想システムとして実装した。以下に、開発環境および実装方法を示す。

- 開発環境

システム開発の環境は以下のとおりである。

OS　　：Windows XP
CPU　：Athuron　700MHz
メモリ：320Mbyte
コンパイラ：Microsoft Visual C++コンパイラ

- 実装方法

＜暗号・復号処理＞

暗号化および認証動作には、OpenSSL ライブラリ[6]内の暗号アルゴリズムを使用する。OpenSSL ライブラリは種々の暗号アルゴリズムの使用が可能であるが、アルゴリズムの汎用度を考慮して、今回は共通鍵暗号に AES－CBC、公開鍵暗号に RSA、ハッシュ関数に MD5 を使用した。

＜データの送受信＞

提案システムでは、インターネットを通じてデータの送受信を行うが、今回は同一プログラム内でモジュール同士が直接データを受け渡す方式にしている。

＜生体認証＞

特徴点の抽出を行い Client 内に保持されている状態として、プログラム内に格納している。

4.2. 実装に関しての留意点

提案方式のポイントは既存技術では実現ができなかった、各通信路の暗号化・認証を実現したことである。そのため、暗号化・認証処理に関係する暗号アルゴリズム・ハッシュ関数・生体情報に関して、汎用性を持たせるようシステム及びパケットの設計を行った。

5. システム評価

5.1. 提案システムの効果

提案システムでは、IC カードを使用して Server による認証をおこなうさいに必要な通信路すべての暗号化・認証を実現している。このため、認証までの処理動作が既存システムに比べ多くなっている。しかし、提案システムは既存システムに比べ, 成りすまし・情報盗用に対して非常に高いセキュリティを確保できているため、メリットの方が大きい。また、既存システムでは認証までに５回通信をおこなう必要があるのに対し、提案システムでは３回の通信で認証を実現している。ネットワークを利用したシステムの場合、通信時のレスポンスは全体の処理時間に大きく影響を及ぼすため、高い効果が期待できる。さらに、既存システムでは、認証とその後の通信を別システムで実現していたが、提案システムでは機器構成を変更することなく、同一システム内で実現している。このため、提案システムは既存システムからの意向が容易であり、また既存システムに比べて導入・運用・管理が容易であるといえる。

5.2. 処理時間の測定及び考察

実装したシステムで処理時間の測定を行った。測定環境は以下の通りである。

＜測定環境＞

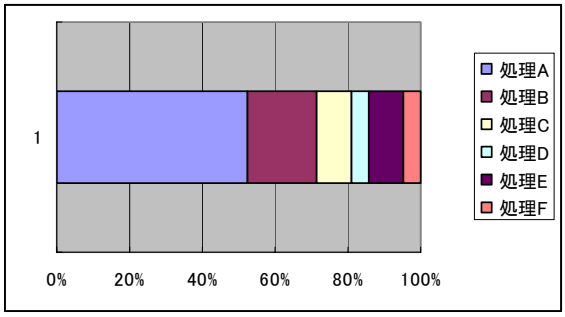
OS　　：Windows XP
CPU　：Athuron　700MHz
メモリ：320Mbyte
共通鍵長：256bit
公開鍵長：1024bit

生体認証でもっとも使用されている指紋認証の場合、指紋情報長は最小 64byte、平均 256～512byte である。また、最近注目を集めている虹彩の情報長は 512byte 程度である。データ長の長いものでは声紋の５Kbyte がある。そこで、提供情報長を 256byte に固定して、生体情報長を 64・256・512・4096byte のときの生体情報の暗号化、パケット作成、復号・認証までの処理時間を計測した。（表 3）

測定の結果、認証時の処理時間は最大 0.021msec であった。提案システムは既存システムと処理がほとんど同じであるため、不足部分を既存システムから参照して考察することができる。つまり、既存システム全体の処理時間が 10msec であるとすると提案システムは多く見積もっても、最大 10.021ms であると推測

処理名	内容
A	生体情報の暗号化・パケットの作成
B	生体情報の復号・認証
C	IC カード⇒Server へのパケット作成
D	認証、共通鍵の取得
E	提供情報の暗号化・パケット作成
F	復号・認証・情報の取得

---各処理内容---



各処理の全体の内訳

生体情報長	64	256	512	4086	(byte)
処理 A	0.01	0.01	0.01	0.011	
処理 B	0.002(0.002)	0.002(0.002)	0.002(0.002)	0.004	
処理 C	0.002	0.003	0.002	0.002	
処理 D	0.001	0.001	0.001	0.001	
処理 E	0.002	0.002	0.003	0.002	
処理 F	0.001	0.001	0.001	0.001	
全体処理時間	0.017	0.017	0.018	0.021	

(単位m秒)

表３ 処理時間測定結果一覧

できる。これは、システムを使用するうえで問題にならない数値の増加であると言える。

また、認証後のセキュア通信を実現するための暗号・認証処理時間も送信情報長 8192byte 時で 0.003msec と、こちらも使用上問題にならない測定結果であった。

以上より、提案システムは通常の使用に十分耐えられるシステムであるといえる。

6. むすび

今回、既存システムの問題点である、認証動作時の各通信路毎の暗号化・認証及び認証後の通信のセキュリティの確保についての提案をおこない、十分な効果が確認できた。提案システムは、既存システムの構成はそのままにし、利点を損なわぬよう設計しているため、既存システムからの移行も容易にできる。さらに、認証後の通信処理シーケンスを明確に設定し、セキュリティを確保したことで、本システムがインターネットを介した、あらゆるサービス分野に応用が可能であると思われる。また１つのシステムで認証からその後のセキュア通信を実現しているので、運用・管理も容易であるという特徴を有している。

今後は、生体情報リーダ・IC カードリーダを実際に使用して、インターネットを介したシステムを構築し、生体情報長を数 Kbyte・提供情報長を数 Mbyte にした場合の実験・測定をおこなっていく。

参考文献

[1] 森川、青山、南：ユビキタスネットワーキングへの道、情報処理学会会誌 Vol.43 No.06-004
[2] 瀬戸洋一：ユビキタス時代のバイオメトリクスセキュリティ、日本工業出版
[3] 影井良貴：IC カードの動向、情報処理学会会誌 Vol.39 No.5
[4] 伊藤雅彦：非接触 IC 技術とその応用、情報処理学会会誌 Vol.43 No.03-016
[5] Richard E,Smith 著、稲村雄 訳：認証技術-パスワードから公開鍵まで-、オーム社
[6] http://www.infoscience.co.jp/technical/openssl/
[7] 渡邊、厚井、井手口、横山、妹尾：暗号技術を用いたセキュア通信グループの構築方法をその実現、情報処理学会論文誌 Vol.38 No.04-025
[8]妹尾、厚井、貞包、中谷、馬場、鹿間：生体認証によるネットワーク個人認証システム、情報処理学会論文誌 Vol44 No.04-1111