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‡

名城大学理工学部†　　名城大学理工学部‡

1. 研究背景

インターネットが普及した今日、ネットワークは様々な分野で活用されるようになり、それに比例するように、ネットワークセキュリティへの関心はますます高まっている。そのセキュリティ技術の一つである認証技術において、人間の身体的特徴を利用する生体認証があり、現在様々な用途で使用されている。ネットワーク環境にも生体認証を利用した認証技術は存在するが、認証段階までは定義してあってもその後の通信方法を定義しているものは少ない。本論文では、生体情報を利用した認証方法を利用するとともに、その後のネットワークをセキュアに通信できるシステムを提案する。

2. 従来の生体認証システム

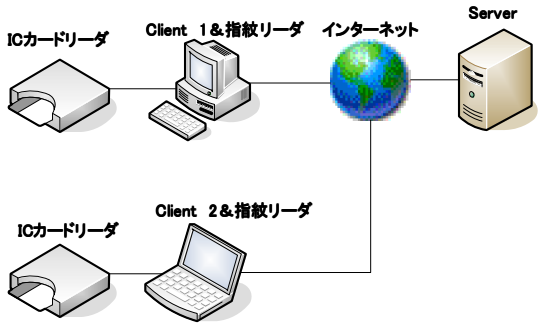

図1　システム構成図

図 1 は従来システムの構成図である。この構成は提案システムにも適用される。

Client にはあらかじめ IC カードリーダおよび生体認証装置が備え付けられている。また IC カード内には、生体情報テンプレート S および秘密鍵 Prs が保持されており、これらを使用して認証を行う。

従来方式の処理シーケンス例を図 2 に示す。

IC カード内には、生体情報テンプレート T&秘密鍵 Prs が、Server 内には公開鍵 Pus が、あらかじめ格納されている。また、User が異なる Client でもシステムを利用できるよう、Client 内には情報は保持させれない

1. 取得した生体情報を IC カードに送信する。IC カードは、テンプレート T と比較を行い、User の認証を行う
2. 認証が正しければ、IC カードは秘密鍵 Prs の開錠を行い、Server へ認証要求を行う。Server は IC カードを認証するためのチャレンジコードを送信する。
3. IC カードは秘密鍵 Prs を利用して、署名およびレスポンスを作成し、Server に送信する。Server はこれにより User の認証を行う
4. Server から Client に対して必要な情報を送信する

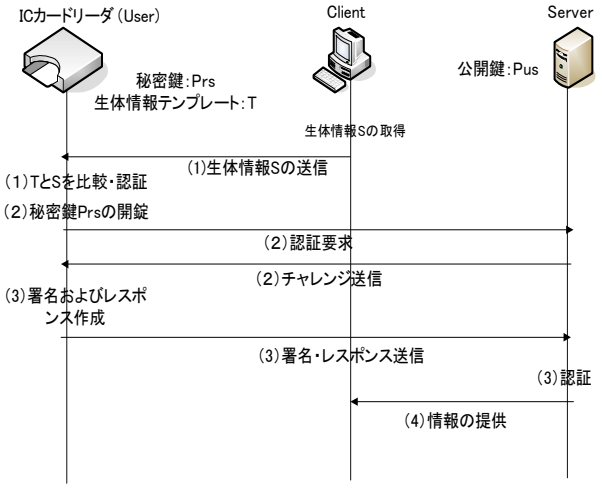

図 2.従来方式シーケンス

本システムでは、耐タンパ性を持つ IC カードに User の情報を保持させる事により、高いセキュリティを確保している。また、Client が特定の情報を所持していないため、IC カードを利用できればどの Client からでも、情報を取得することができる（Client に依存しない）。

しかし、生体情報を IC カードに送信する際、平分で流されているため、生体情報が漏洩する可能性がある。また、Server から Client に対して情報を送信する際、Client に情報を保持させていないため、暗号化および Server の認証ができず、セキュリティを確保できない。そのため、Server の成りすまし及び情報の盗用の危険性がある。

3. 提案方式

従来方式の利点を損なわず、欠点を解決するため、生体情報 S の暗号化および Server→Client 間での情報送信時のセキュリティを確保するための方法を提案する。

Secure network communication using biometrics

† Masakatsu Maeba
Department of science and engineering , Meijo University
‡Akira Watanabe
Department of science and engineering , Meijo University

3.1. 生体情報 S の暗号化

Client にあらかじめ情報を所持させないことを前提としている。そこで、IC カード内にユーザの秘密鍵 Prc だけでなく公開鍵 Puc を保持させることとする。IC カードは Client から生体情報を受取る前に、Puc を Client に渡す。Client は Puc を用いて生体情報を暗号化し IC カードに送信する。

3.2. Server→Client での情報送信時のセキュリティの確保

Server から Client への通信には、認証と暗号化を同時に実現する必要があり、このためには、２点間でのみ知りうる情報（暗号鍵）を共有する必要がある。Client はあらかじめ所持している情報がないため、その都度 Client に情報を保持させなければならない。そこで、Client 自身が暗号鍵となる乱数 R をその都度生成し、それを IC カード経由で安全に Server に送信することにより乱数 R の共有を実現する。R を用いることにより認証と暗号化を同時に実現できる。

具体的な流れは以下のとおりである。

1. Client が乱数 R を生成し、生体情報を IC カードに送信する際に一緒に渡す
2. IC カードから Server に R を含めた認証情報を送信する
3. Server は受け取った R で暗号化および認証情報を作成し、Client に送信する
4. Client は保持している R を用いて復号および Server の認証を行う

このように、すでに確保してある、Client⇔IC カード・IC カード⇔Server 間の認証を利用することによって、Client⇔Server 間で情報の安全な共有を確保し、認証を実現する。

4. 提案方式の処理シーケンス

上記の提案をふまえた上での、提案方式の処理シーケンスを図 3 を用いて説明する。

初期情報として、IC カードには、IC カード・Server 間用公開鍵 Pus、生体情報テンプレート T、IC カード・Client 間用秘公開鍵ペア Prc&Puc、ユーザ ID：IDu を格納しておく。Server には Pus に対応する鍵 Prs を格納する。この Prs はユーザ ID と１対１対応している。Client には、初期情報は格納させない。

＜シーケンス＞

1. IC カードは公開鍵 Puc を Client に送信する
2. Client は生体情報 S を取得し、暗号鍵（乱数）R を生成する。そして、S および R を PUC で暗号化（Puc[S|R]）する。
3. Client は、Puc[S|R]を IC カードに送信する
4. IC カードリーダは Puc[S|R]を Prc で復号し、T と R を比較・認証を行う。結果が正しければ、R を Pus で暗号化する。また、Pus[R]||IDu のハッシュ値をとる。これらに、IDu を付加し Server への認証パケットを生成する。
5. Pus[R]||IDu|H(Pus[R]||IDu)を Server へ送信する
6. Server では、受け取った情報を IDu に対応した Prs で復号し IC カードの認証を行う。認証結果が正しければ、提供情報 D および R を R で暗号化（R[D|R]）する
7. Server は R[D|R]を Client へ送信する。
8. Client は、受け取った R[D|R]をあらかじめ保持している R で復号し、復号結果の R で Server の認証を行う

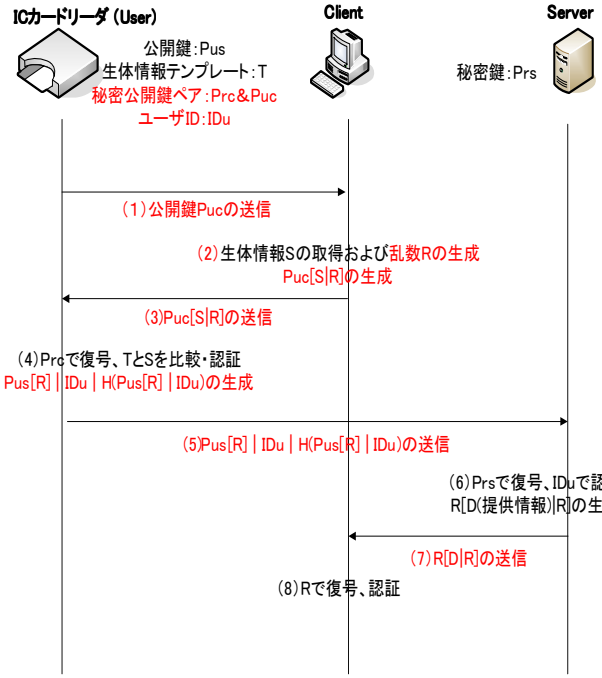

図 3.提案方式シーケンス

5. まとめ

既存システムの問題点である、生体情報の暗号化・Server→Client 間のセキュリティの確保についての提案を行った。本提案システムはサービス提供部分の処理を明確にし、セキュリティを確保しているので、あらゆるサービス分野に応用可能であると思われる。

今後は、システムを実際に構築し、システムの定量的な比較及び、更なる改善を進めていく。

＜参考文献＞

[Ⅰ]渡邊、厚井、井手口、横山、妹尾：
“暗号鍵を用いたセキュア通信グループの構築方法とその実現”
情報処理学会論文誌 Vol.38 No.04－025

[Ⅱ]ユビキタス時代のバイオメトリクスセキュリティ
著：瀬戸　洋一　出版：日本工業出版