生体認証を利用したセキュアネットワーク通信

11300j124　前羽理克
渡邊研究室

1. はじめに

現在、人間の身体的特徴を利用する生体認証を利用した、ネットワークセキュリティ技術が注目され、使用されている。しかし、認証方法は定義しても、その後の通信方法を定義しているものは少ない。本研究論文では、生体認証を使用して、認証からその後の通信までのセキュリティを考慮したシステムを提案する。

2. 既存の生体認証システム

図 1 は指紋認証を利用したネットワークシステムの構成図である。

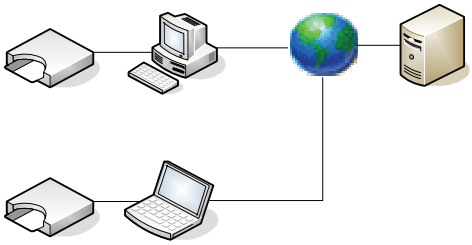

図 1　システム構成図

Client には、IC カードリーダ、指紋リーダを備える。IC カードは、生体情報テンプレート T および秘密鍵 Prs を、Server は公開鍵 Pus を保持する。また、User が異なる Client を利用できるように、Client 内には認証に使用する情報は保持させない。

以下に、既存システムにおける基本的な処理の流れを記す。

1. 指紋リーダから取得した指紋情報 S を Client を通じて IC カードに送り、IC カード内のテンプレート T で認証する。
2. 認証が通ると、サーバからチャレンジコードを取得し、秘密鍵 Prs でレスポンスおよび署名を作成して Server へ送る。
3. Server は受け取った情報で認証を行い、認証が通れば Client に User の求める情報を送信する。

上記既存システムには以下の 2 つの課題がある。すなわち、生体情報 S を平分に流していることによる S の盗用、Client に情報を保持させていないため Server から Client への送信時のセキュリティ（暗号化・認証）が確保できないことによる、情報の盗用の危険性である。

3. 提案方式

提案方式では、生体情報の暗号化のために、IC カード⇔Client 間で使用する専用の公開鍵ペアを利用して、暗号通信を行う。Client に情報を保持させることはできないので、IC カードに公開鍵ペアを保持させ、通信時に公開鍵を Client に渡すことにより、Client⇔IC カード間に安全な通信路を確保する。

Server⇔Client 間の暗号・認証を確実に実現するためには Server・Client 間で秘密の情報を共有しなければならない。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 に情報を保持させる必要がある。しかし、システムの性質上 Server および IC カードから Client に安全に情報を渡す方法はない。そこで、Client 自身が暗号鍵 R を生成し、すでに確保している Client⇔IC カード＆IC カード⇔Server の認証を利用して、Server へ送信し安全な共有を実現する。そして、R で Client⇔Server のセキュリティを確保する。以上のように、すでにある認証を利用して、新たな暗号・認証機能を構築する。

以上を踏まえた上での、提案システムの処理シーケンスを図 2 に示す。

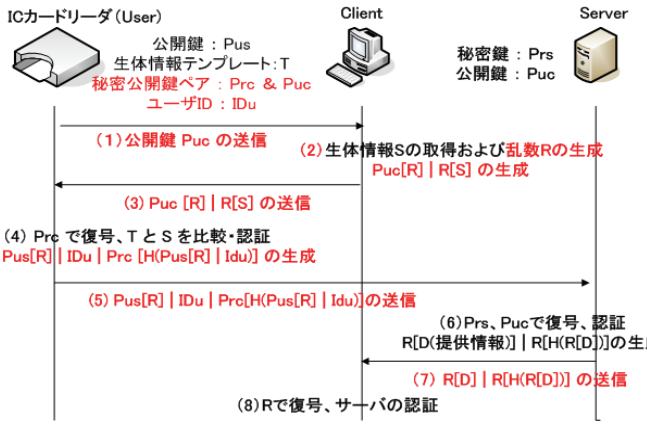

図 2　提案システム処理シーケンス

4. まとめ

既存システムの課題であった、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解決する提案を行った。本提案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たので、あらゆるサービス分野に応用が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および更なる改善を進めていく。

参考文献

[1] 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とその実現，情報処理学会論文誌 Vol.38 No.04-025
[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.