指紋認証を利用したデータ通信ソフトの開発

匂坂　剛*　安藤昌弘*

Development of Data Communication Software Used by Fingerprint Authentication

SAGISAKA Takeshi*, ANDO Masahiro*

抄録

通信相手と相互認証を行った上で、サーバを介さずデータを「直接手渡し」するようなデータ通信ソフトの試作開発を行った。相互認証には、ユーザ名、パスワード及び指紋認証を利用することで本人確認を確実なものとした。

指紋認証では、照合を厳密にするほど認証エラーが増加し、ソフトウェアの使用感が悪くなった。また、通信の暗号化に利用した IPSec の通信速度に対する影響を測定したが、10Mbps 程度の通信では、ほとんど影響がないことがわかった。

キーワード：ＩＴ，通信，指紋認証，ピアツーピア

１　はじめに

平成１７年１２月、政府は「ＩＴ新改革戦略」で平成２０年を目途にＩＰｖ６への移行を表明した [1)]。今後、情報通信機器は直接通信（ピアツーピア）が主流となることは間違いない。同時に、あらゆる企業・団体に対し情報セキュリティの確保が求められている。

現在、個人や企業間での情報のやりとりは主に電子メールが利用されているが、情報漏洩の多くは内部からであることから、電子メールでは組織内部の人にメールを受信されたり、のぞき見されるおそれがある。通常、電子メールは本人確認方法がＩＤ・パスワードだけであり、なりすまし防止としては弱い。

そこで、本研究では今後の情報通信がピアツーピアで行われること想定し、本人確認方法として指紋認証を用いた、情報を「直接手渡し」するようなデータ通信ソフトの試作開発を行った。

* 電子情報技術部

２　開発ソフトウェアの仕様

本研究で開発するソフトウェアに必要となる基本要件としては以下の３点がある。

(1)通信ソフトであること

(2)通信相手との指紋認証が可能であること

(3)通信の暗号化ができること

ソフトウェアの概念図を図１に示す。

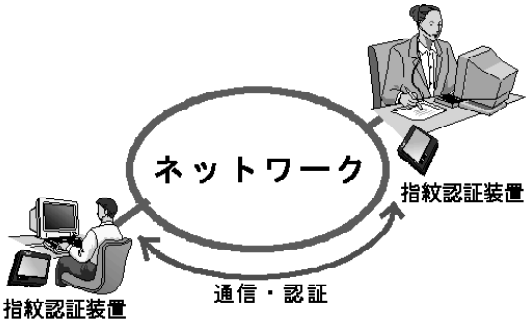

図１　データ通信ソフトの概念図

2.1 通信ソフト

通信ソフトとしては、ピアツーピア通信を想定しているが、汎用性を考えて現段階では、WinSock を使ったソケットプログラムとした。

開発環境は、microsoft Visual C++ 6.0 で WinSock API を利用した。

通信ソフトとしての仕様は、次のとおり。

(1)相手からの通信要求を受ける為の待受機能

(2)相手への接続要求を行うクライアント機能

(3)文字チャット機能

(4)ファイル送受信機能

2.2 指紋認証

認証部分には、本人確認方法として発展して来ているバイオメトリクス認証の中でも、最も普及が見込まれる「指紋認証」を利用することとした。もちろん、ユーザ名・パスワード認証も行う。

開発環境は、microsoft Visual C++ 6.0 で、指紋認証開発キットとして サイレックス・テクノロジー（株）の DF-SDK Ver2.4 を利用した。

サイレックス社の SDK を選択した理由は、指紋認証の処理に合わせて API が個別に用意されているため、こちらでのカスタマイズがしやすいと考えたためである。

認証部分の仕様は次のとおり。

(1)ユーザ名、パスワード認証機能

(2)指紋認証機能

(3)ユーザデータの登録・保存機能

2.3 暗号化

通信部分の暗号化については、IPv6 では標準となる IPSec を利用することとした。これは Windows XP に標準でインストールされている。（但し、使用には IPSec ポリシーの設定が必要）。

また、パスワードや指紋認証情報を保存するユーザデータについては、本ソフトウェアで暗号化することとした。

開発環境は、microsoft Visual C++ 6.0 で 暗号化ツールとして microsoft Crypt API を利用した。

３　開発結果及び考察

3.1 データ通信ソフト

開発したデータ通信ソフトのフローチャートを図２に示す。

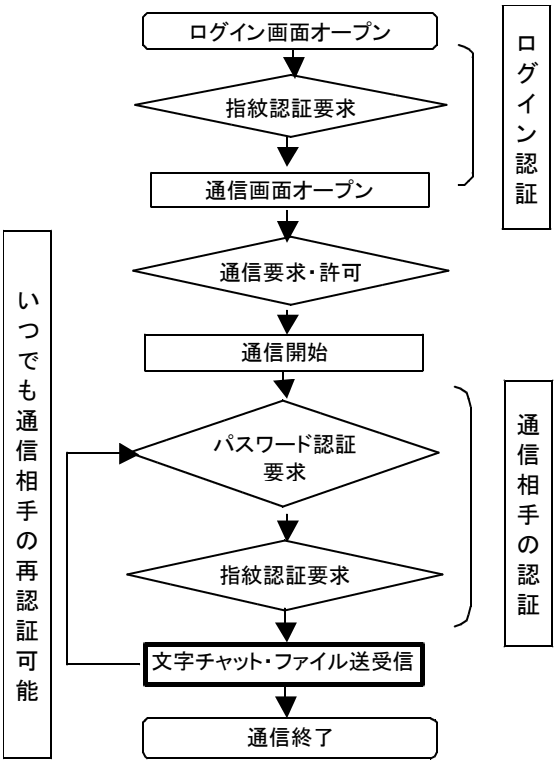

図２ データ通信ソフトのフローチャート

まず、ソフトウェアを起動した本人がユーザデータに登録されているか、ログイン指紋認証を行う。ログイン画面を図３に示す。

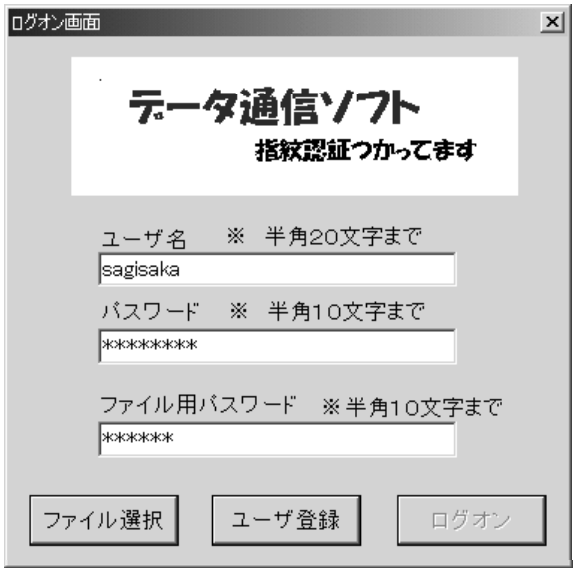

図３ データ通信ソフトのログイン画面

ここでまずパスワード認証を行い、認証されたら指紋認証が要求される。指紋取り込み画面を図４に示す。

図４　指紋取り込み画面

指紋認証ができたら通信画面に移動する。通信画面を図５に示す。通信にはあらかじめ通信相手の IP ｱﾄﾞﾚｽと接続ポート番号が必要である。

図５　通信画面

この画面上で、文字チャットやファイル送受信を行う。また、「認証要求」ボタンを押すことで、通信中に相手の認証確認を行うことができる。通信中であれば、相手への認証要求は何度でも行うことができる。

3.2 指紋認証

認証用の指紋データの登録には連続して３回の指紋採取を行い、最適なデータを登録するようにした。通常、指紋には１００点ほどの特徴点がある。指紋鑑定において同一性を示すのに何点の特徴点の一致が必要であるか明確にはなっていない。警察などでは経験則から１２点を目安にしていると言われている[2)]。

要求される一致点を増やすと認証に失敗し、何度も指紋を取り直すことになる。一致点を減らせば認証しやすくなり使用感は良くなる。どのレベルで折り合いを付けるかがポイントである。

そこで、本ソフトウェアでは、ログイン認証に 12 ～ 15 点、通信相手認証に 10 ～ 12 点の一致を目安とした。

また、同じ指であっても取り込む指の部分が違っているだけで照合に失敗する。指紋の登録時にはどの指かだけでなく、だいたいどの部分かについても決める必要があるなど、人間自身も指紋認証に慣れる必要があることがわかった。

3.3 暗号化の影響

IPSec を使うことで、どのくらい通信速度に影響が出るか測定した。２台のパソコン（CPU:P4 1.6GHz, memory:256MB）を１つの HUB を介してピアツーピアで接続し、本ソフトウェアでファイルを送受信したときの通信速度である。HUB は 100Base-Tx と 10Base-T を使って比較した。

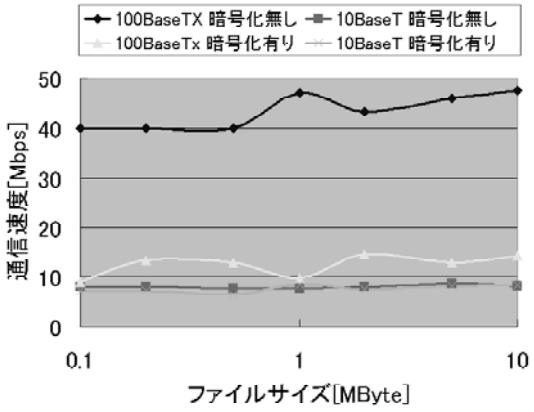

図６　通信速度の比較

100BaseTx で通信した場合は、暗号化なしで 40M ～ 50Mbps の速度であったものが、IPSec を

使用したところ 10M ～ 15Mbps 程度になった。

10Base-T で通信した場合は暗号化に関わらず、ほぼ 7M ～ 8Mbps であった。

このことから、IPSec は 10Mbps 程度の通信環境では、ほとんどボトルネックにならないことがわかる。

４　まとめ

開発した「指紋認証を利用したデータ通信ソフト」には次の様な特徴がある。

(1)サーバを使用せずピアツーピア通信を行う。

(2)指紋認証を利用することで、本人確認をより確実にしている。

(3)ユーザデータについてはソフトウェア内で暗号化し、通信については IPSec を使用する。

指紋認証を利用したシステムは徐々に広がってきている。手軽な認証方法であるだけでなく、ID・パスワードを打てない手が不自由な方やキーボード操作に不慣れな方にも向いているため、用途は広い。

今回開発したソフトは、今後のユビキタス時代でソフトウェアに必須の要件となると考えられる「通信」「認証」「暗号化」を全て含むものであり、新規システム開発だけでなく、既存システムの更新などにも利用することができると考える。

参考文献

1) 日刊工業新聞, 2006.1.16

2) 斉藤指紋鑑定事務所, http://www.kanshiki.com/5.html, 2005.10.15

3) Lewis Napper：WinSock2 プログラミング改訂第２版, ソフトバンクパブリッシング, (2005)

4) 粂井康孝：猫でもわかるネットワークプログラミング, ソフトバンクパブリッシング, (2005)