平成 14 年度

学士学位論文

SAS-2 認証を用いたファイル遠隔操作方式

A Remote Control System using SAS-2

1030276　　田岡 慎也

指導教員　　清水 明宏

2003 年 2 月 12 日

高知工科大学 情報システム工学科

要 旨

SAS-2 認証を用いたファイル遠隔操作方式

田岡 慎也

近年，インターネットの爆発的な広がりにより，携帯端末上での i-mode サービスやインターネットカフェ等の様々なサービスが提供されるようになった．

このような中で，会社や教育機関等の公の場においても，クライアント/サーバシステムが利用されるようになり，個人のファイルがファイルサーバによって管理されるようになった．これに伴い，出先からファイルサーバにファイルの送受信を行うサービスが考えられている．

ファイルサーバへのアクセス方法として代表的なものに，FTP(File Transfer Protocol) が挙げられる．しかし，ファイアウォールが設置されてあるイントラネット内へのアクセスは困難である．

そこで本論文では，通信に HTTP(Hyper Text Transfer Protocol) 及び SMTP(Simple Mail Transfer Protocol) を用い，認証部には SAS-2(Simple And Secure password authentication protocol， Ver.2) を適用することにより，出先端末の環境に依存せず，安全性の高いファイル送受信サービスを提供するシステムを提案する．

キーワード　ファイル送受信，HTTP，SMTP，SAS-2，電子メール

Abstract

A Remote Control System using SAS-2

In recent years, the Internet systems are increasing, and various services are offered on the Internet and personal digital assistants. C/S systems come to be used on companies and educational facilities. For that reason, individual files are managed by a file server. So, we research the service which transmits and receives files from a destination to a file server. A famous access method to a file server is FTP(File Transfer Protocol). However, accesses into a intranet with a fire wall are difficult.

In this thesis, I produce a new system using HTTP(Hyper Text Transfer Protocol), SMTP(Simple Mail Transfer Protocol), and SAS-2(Simple And Secure password authentication protocol, Ver. 2). Such system does not dependent on environments of a destination terminal and offeres secure contents communication services.

key words File service, HTTP, SMTP, SAS-2, E-mail

目次

第 1 章　はじめに **1**

第 2 章　遠隔ファイル操作技術 **3**

2.1　VPN による遠隔データ操作方式 3

2.2　認証サーバ経由でのダイヤルアップ IP 接続を用いた遠隔データ操作方式 . 4

2.3　FTP による遠隔データ操作方式 4

2.4　Pop-up Mail による遠隔データ操作方式 4

第 3 章　ファイル遠隔操作方式 **6**

3.1　3 者間ファイル転送方式 6

3.1.1　概要 6

3.1.2　3 者間ファイル転送 7

3.1.3　ファイル転送システム構成 8

3.2　SAS-2 を用いたファイル操作 9

3.2.1　セキュリティの確保 9

3.2.2　SAS-2 認証 10

表記記号の定義 10

前処理 10

認証処理 11

3.2.3　ユーザ認証 12

3.2.4　中継サーバシステム構成 13

初期登録 13

転送処理 13

閲覧要求 13

データベース 14
3.2.5 ファイルサーバシステム構成 14
3.2.6 SAS-2 認証を用いたファイル転送プロトコル 15
3.3 中継サーバ，ファイルサーバ間での電子メールの流れ 16
3.3.1 ファイル受信操作時における電子メールの流れ 16
3.3.2 ファイル送信操作時における電子メールの流れ 17

第 4 章 試作システム **19**
4.1 試作システム環境 19
4.1.1 認証画面 21
4.1.2 メイン画面 22
4.1.3 ファイル受信処理 23
4.1.4 ファイル送信処理 25
4.2 評価 27

第 5 章 今後の課題 **31**
5.1 実装システムに対する課題 31
5.2 評価項目に対する課題 32

第 6 章 おわりに **33**

謝辞 **34**

参考文献 **35**

図目次

2.1 Pop-up Mail サービス 5

3.1 3 者間ファイル転送方式 7
3.2 ファイル転送システム全体図 8
3.3 認証処理の流れ 12
3.4 SAS-2 認証を用いたファイル転送プロトコル 15
3.5 ファイル受信時における電子メールの流れ 16
3.6 ファイル送信操作時における電子メールの流れ 18

4.1 認証フェーズ 21
4.2 メイン画面 22
4.3 ファイル受信画面 23
4.4 ファイル受信の流れ 24
4.5 ファイル送信画面 1 25
4.6 ファイル送信画面 2 26
4.7 CPU 負荷率．1 28
4.8 CPU 負荷率．2 28
4.9 CPU 負荷率．3 29
4.10 CPU 負荷率．4 29

表目次

4.1　ファイル受信時間 27

第１章

はじめに

今日あらゆる情報は電子化・デジタル化されるようになり，従来複雑であった作業もコンピュータにより高速な処理が実現されるようになりつつある．現在，コンピュータは私達の身近に存在し，生活の一部として欠かせないものとなっているのが実状である．

コンピュータの技術革新に伴い，インターネットが広く普及している．インターネットの普及と携帯型のパソコンの発達により，今やインターネットは企業や研究者だけでなく，安価で使い易いネットワークとして，私たちの一般の生活において多くの場で利用され，あらゆる層の人達の日常的なものとして溶け込んでいる．これに伴い，電子メールがコミュニケーションの手段として広く用いられるようになった．

電子メールの需要の幅は一般家庭を始め，携帯電話，インターネットカフェ，ホテル，企業，飲食店にまで広がりを見せ，今後はさらに電子メールに限らず，ネットワーク上に存在する付加価値の高い電子データを安全に取得可能な方法が必要になることは十分に考えられる．

現在クライアント/サーバシステムにより，個人や企業単位で独自にイントラネットを形成し，個人のファイルから重要ファイルまでファイルサーバに保存できるようになった．このようなことから，ファイルサーバは，イントラネット内でのファイル保存という点では大いに活躍している．しかし，出張や会議等においてイントラネット外である出先に出向いた際，急遽ファイルサーバに蓄積されている情報が必要となる場合，必要ファイルを得ることができず，困難を生じるという問題も残している．特にビジネスにおいてパソコンを使用するものにとって，イントラネット内に蓄積された電子データを出先において有効に活用できるかが重要となる．

こういった現状をふまえると，インターネット上でファイルの操作ができるようになることはビジネスユーザにとっては非常に有効である．

上述してきたように，今や莫大な人数がインターネットユーザとしてその利用価値を見出しており，コンピュータ及びインターネットの使用頻度はそのセキュリティの枠を越え，無秩序に，広範囲にまで及んでいる．インターネット上で電子データを送受信しようとした場合，悪意を持った第三者によって盗聴される危険性があるため，セキュリティの確保が非常に重要となる．しかし，一般にセキュリティをより強固なものにするほど通信や各端末の処理に要する負荷が上昇してしまう．特に，これから更に普及するであろうインターネット家電等の処理能力の高くない端末では，端末における負荷が問題となることが予想される．

本研究では，インターネットを介し，電子メールからより汎用的にイントラネット内に蓄積された電子データ全般を対象として，安全かつ効率の良いファイル送受信方式である電子データ遠隔操作方式についてのプロトコルを提案し，そのシステム構成について考案する．

第 2 章

遠隔ファイル操作技術

電子データの遠隔操作によるファイル送受信サービスに対しての需要の高まりについて第 1 章でも述べた．

ファイル送受信サービスとして，VPN(Virtual Private Network)，認証サーバ経由でのダイヤルアップ IP 接続，FTP 等が挙げられる．

2.1 VPN による遠隔データ操作方式

VPN とは，公衆ネットワーク (Public Network) 上で仮想的にユーザ専用のネットワークを実現したものである．

古くは，キャリアの内線サービスに接続し企業における各支社・支店間で内線通話を可能にする音声 VPN を指していた．しかしデータ通信 (特に Web 等の IP データ) が爆発的に急増し，トラフィックに占めるデータ/音声の割合が逆転した現在では，データ通信向けの VPN としての認識が強くなっている．

ファイル送受信方式においても利用効率の高いものとして期待できたが，出先の端末の環境をあらかじめ設定しておき，利用に応じて環境を変更する必要が生じる．

2.2　認証サーバ経由でのダイヤルアップ IP 接続を用いた遠隔データ操作方式

認証サーバ経由でのダイヤルアップ IP 接続を用い，コールバックを利用したユーザ認証を行うという方法も考えられる．しかし，この方法では VPN と同様に出先の端末の環境の変更が余儀なくされる．出先ではダイヤルアップのために設定を必要とし，サーバ側には利用者の電話番号を登録しておかなければならないので出先において，データ取得に緊急を要する場合実用性に欠けることが考えられる．

2.3　FTP による遠隔データ操作方式

FTP による遠隔データ操作方式は一般的に認知度が高く，広く利用されている方法であり，第 1 章でも述べたが，企業や教育機関のイントラネットでは，重要ファイルや個人ファイルの流出を防ぐため，ファイヤウォールを設置してある．そこで，出先端末においてポート番号の指定を行い，ファイヤウォールを回避しなければならない．また，ログイン時の ID，Password 情報や転送中のデータは全てそのままのデータとして流れてしまうことから，セキュリティ面で危険度が高いことがいえる．

2.4　Pop-up Mail による遠隔データ操作方式

内部ネットワークのメールサーバから，中継サーバを経由し，電子メールを送受信することのできる Pop-up Mail サービスがある．

Pop-up Mail とはメールサーバーにアクセスし，自分宛のメールを取り出すためのプロトコルである．ダイヤルアップ IP 接続の場合，インターネットに常時接続されているわけではないので，メールが返送されないように，一時的にプロバイダのメールボックスに保管される．そのメールをユーザーがダイヤルアップ IP でプロバイダに接続してメールボックスから自分宛のメールを取り出すためのプロトコルである．

Pop-up Mail サービスではこのようなプロトコルのもと，インターネット環境下にあるパソコンがあれば，セキュアなネットワーク環境下を前提とした上で，国内外を問わずに安全かつ確実なメール転送が実現でき，メールのやりとりが可能になる．電子メールの転送を内部ネットワークのメールサーバと，インターネットに接続された中継サーバ，出先の端末の 3 者間で行うサービスであり，転送プロトコルは，HTTP により中継サーバにアクセスし，SMTP を利用しメールサーバへのアクセスを行う．これによりインターネットに接続している端末の Web ブラウザから，中継サーバへアクセスすることのみで外部から電子メールを送受信することが可能である．

昨年度の研究成果より Pop-up Mail サービスを用いた 3 者間でのファイル転送方式を利用した遠隔コンテンツ操作方式の基本プロトコルが提案された．しかし認証プロトコルの確立，安全性の問題から本研究の目的とするシステムの実装を行うまでには至っていない．

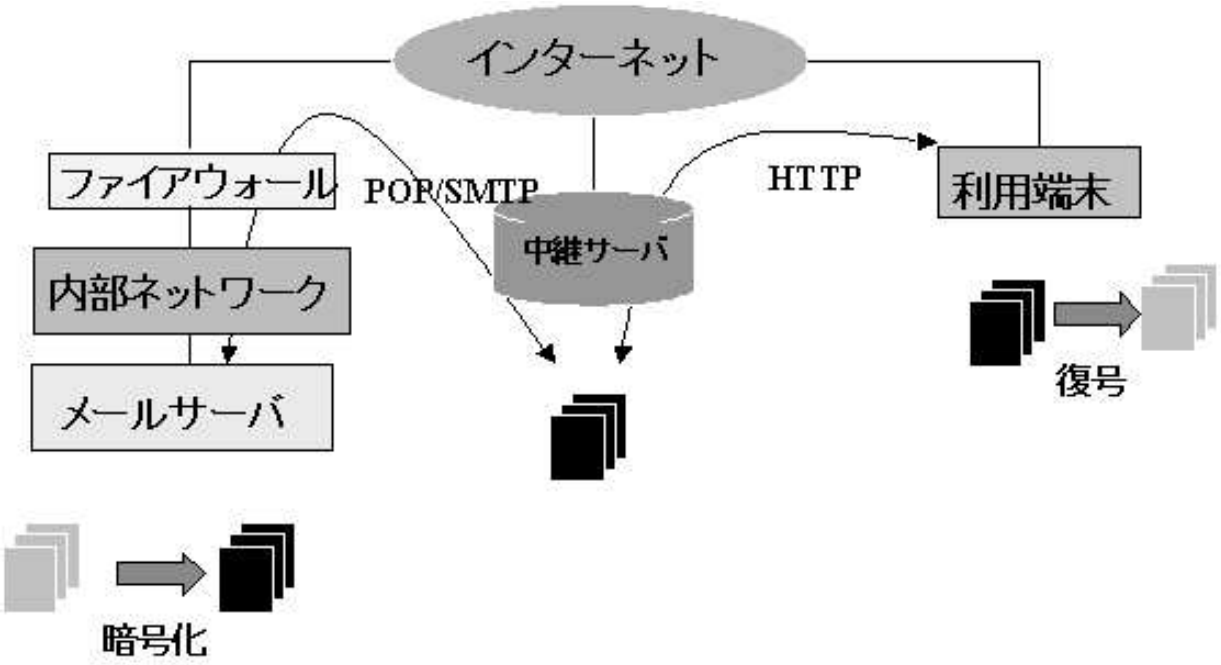

図 2.1　Pop-up Mail サービス

第 3 章

ファイル遠隔操作方式

3.1　3 者間ファイル転送方式

3 者間ファイル転送方式では，イントラネット内に設置されてあるファイアウォールに依存せず，出先の端末 (ユーザ) における環境変化等の負担をかけないサービスを提供する．

3.1.1　概要

電子メールとは，コンピュータ同士で手紙のやり取りができるシステムであり，電子メールを使えば，世界中とリアルタイムでメッセージを交換することが可能となる．また，電子メールは文章だけでなく，画像や音声等のデジタルデータを送信することも可能であることから，相手が電子メールを持ったユーザーであれば，世界中どこにでもメッセージ及びデータを届ける事が可能である．このため，出先において，ユーザが利用しているプロバイダ経由で，ファイアウォール内の電子メールを送受信することが可能となる．更に，ユーザから送信された電子メールは，一時メールサーバに蓄積されるため，相手が不在でも届ける事ができる．

このような利点を有する電子メールを用い，本研究では，ファイルサーバ側のメールサーバとユーザの利用端末の間に中継サーバを用い，3 者間で電子メールの転送を行う．

中継サーバにファイルを要求，取得することのできる電子メール変換機能を持たせ，WWW(World Wide Web) を通して電子メールの送受信操作を行う．この方式を用いることで，ユーザは転送される電子メールを中継サーバに蓄積させることにより，電子メールを受信するまで回線を保持する必要がなくなる．そのため，ユーザ端末における電子メール送

受信時の回線負荷が軽減されると共に，出先端末にかかるファイル操作処理負荷も軽減できることが予想される．

3.1.2　3 者間ファイル転送

ファイルサーバと出先の端末の間には中継サーバ (Web サーバ) を置き，出先と中継サーバ間の通信には HTTP を用いる．また，各認証時に情報が更新されるワンタイムパスワード方式である，SAS-2 認証方式を用いたユーザ認証を行うことにより，第 3 者による盗聴や成りすましを防ぐ．

中継サーバとファイルサーバ間では POP/SMTP を用い，電子メールによりファイルの操作を行うこととする．

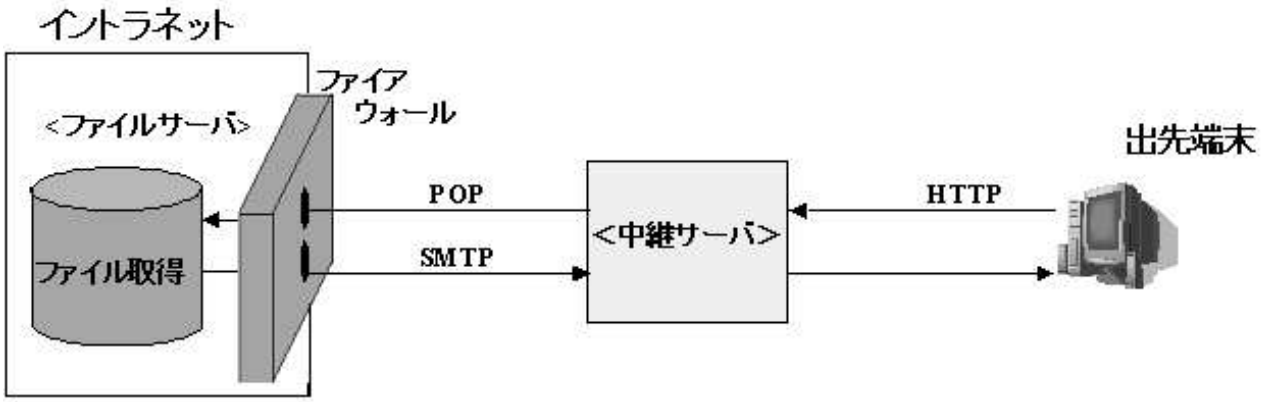

図 3.1　3 者間ファイル転送方式

3.1.3　ファイル転送システム構成

出先から HTTP 通信により，Web サーバである中継サーバにアクセスする．中継サーバには，SMTP サーバを設置することで，SMTP を用いて電子メールを送信することができる．

SMTP は，インターネットのメール配送システムの中核をなすアプリケーションプロトコルである．クライアントが SMTP サーバへメッセージを送信する部分と，メッセージをサーバからサーバへ中継する部分を担当している．これに対して，POP はメールサーバに届いたメールをユーザが端末から読み出す際に使うプロトコルである．ネットワークを通して，ユーザの変わりにサーバへログインし，メールの到着状況を調べ，新着メールを読み出す操作を行う．

これらを利用し，以下のような動作を行う．

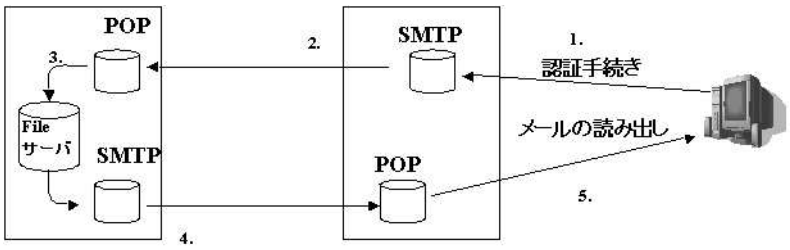

図 3.2　ファイル転送システム全体図

1. 認証手続きが完了すると，欲しいファイルの情報を，アクセスポイントを通って，中継サーバ内の SMTP サーバが取得する．
2. 中継サーバ内の SMTP サーバは，メールの内容部分に，欲しいファイルの情報を添付し，そのメールをファイルサーバ側の POP サーバに送信する．
3. ファイルサーバ側の POP サーバは，メールを受け取ったことをファイルサーバに通知する．
4. ファイル操作終了後，ファイルサーバから受け取った情報をメールに添付し，そのメールを中継サーバに送信する．
5. 中継サーバに届いたメールは，ユーザに通知される．

3.2 SAS-2 を用いたファイル操作

3 者間でのファイル操作を行う上でのユーザ認証及び個々のサーバにおける役割等を以下に示す.

3.2.1 セキュリティの確保

ユーザ認証とは，システムまたはアプリケーションに対してユーザを識別するためのシステムである．このシステムを利用して，特定情報へのアクセス制御を行い，情報の保護を実現することができる.

遠隔ファイル操作方式では，ファイルの操作を行うにあたり，セキュアな認証システムを提供し，ユーザが安心して利用できることが大前提となる．そこでパスワード認証を用い，ユーザが安心して使えるシステムを提案する.

パスワード認証とは，主に ID とパスワードを入力することにより成立する．ネットワーク上をパスワードそのものが流れるため，容易に成りすましが可能である．そこで，第 3 者が回線上および中継サーバ，メールサーバ内から正規のユーザのパスワード情報を取得できないようにすることが重要となる．更に，システムにおいてファイル転送部分が最も重要であり，認証部分において処理負荷がかかりすぎないようにすることが求められる.

上記の要件を満たす認証方式として，本研究室で提案された SAS-2 認証方式を用いたユーザ認証を提案する.

SAS-2 認証方式は各認証毎に送受信されるデータを変更することにより，安全に認証を行うワンタイムパスワード認証方式である．携帯端末での利用を見据え開発された認証方式であるため，処理負荷が少ない．また，クライアント/サーバ間での相互認証が可能であることやアルゴリズムのバリエーションが数パターンあるため，ユーザにより高い安全性を提供することができる.

3.2.2　SAS-2 認証

ユーザ認証部に用いる SAS-2 認証の手順は以下の通りである．

表記記号の定義

ID:ID

S:Password

n:認証回数を示す 0 以上の整数

N_n:n 回目の認証で使用する乱数

E，F，H:ハッシュ関数 (一方向性関数)

α ，β :マスク情報

$\oplus$:排他的論理輪

＋:加算

←:出力

前処理

1. ユーザは，ID と S を入力すると同時に N_n を生成し登録しておく．その後，入力情報と乱数を用い，

   $\mathrm{A} = \mathrm{E}\ (\mathrm{ID},\ \mathrm{S} \oplus N_n)$

   を計算する．

2. ユーザは $\mathrm{A} = \mathrm{E}\ (\mathrm{ID},\ \mathrm{S} \oplus N_n)$ と ID を安全なルートでサーバに送信する．

3. サーバは，認証時に使用するためのデータである ID と A を登録する．

認証処理

1.　ユーザは ID，S を入力すると，入力情報と登録してある N_n を用いて，A = E (ID，S $\oplus$ N_n) を計算する．

ユーザは乱数 N_{n+1} を生成し登録する．そして入力情報と乱数 N_{n+1} から次回認証情報である C = E (ID，S $\oplus$ N_{n+1}) を生成し，ハッシュ関数 F を用いて，F(C) = F(ID，C) を計算する．

さらに

α =C$\oplus$(F(C) + A)

β =F(C)$\oplus$A

の計算を行う．

2. ユーザは，α，β，ID の 3 つのデータをインターネット等の一般的なネットワークを用いてサーバに送信する．
3. サーバは，送られてきた情報に対し，事前に保持しておいたデータを用いユーザ認証を行う．

ユーザから送られてきた，β に対し，所持しておいた A を用いて β $\oplus$A を行い，F(C) を取り出す．

取り出した F(C) を用いて α $\oplus$(F(C)+A) から C を取得する．

サーバは F(ID，C) を計算し，β $\oplus$A の計算より取り出した F(C) と比較する．

F(C) と F(ID，C) が一致すれば認証成功となり次に進むが，一致しなければ認証失敗となりこの時点で終了する．

4. サーバは，次回の認証のために，C を A の替わりに保存し D = H(ID，F(C)) を計算する．
5. サーバは，D をインターネット等の一般的なネットワークを用いてユーザ側に送信する．
6. ユーザは，H(ID，F(C)) を計算し，サーバ側から送信されてきた D との比較を行う．

D = H(ID，F(C)) ならばサーバ，クライアント間での相互認証が成立する．

3.2.3　ユーザ認証

ID，Password を入力する際の認証処理手順は以下のようになる．

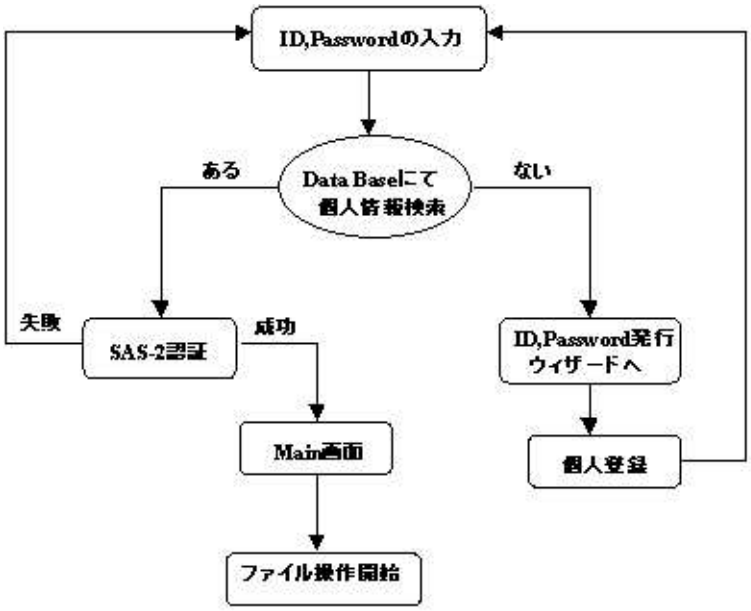

図 3.3　認証処理の流れ

認証処理は出先端末とファイルサーバ間で行うことを述べた．

ユーザは ID，Password をどこかに登録しておかなければ，毎回 ID，Password の発行を行わなければならなくなる．ユーザの手間を省くことを考え，ID，Password を中継サーバのデータベースに蓄積しておく．

中継サーバに情報を蓄積することにより，出先端末では認証処理毎に ID，Password 情報を中継サーバ経由でファイルサーバにアクセスし，認証処理を行う．これにより，ユーザの手間を省くことができると共に，ファイル転送メイン画面にてユーザ認証情報と前回までのファイル情報をデータベースに蓄積することができるので，個人環境が整備され，ユーザ個人の制限を持たせることができる．

3.2.4 中継サーバシステム構成

電子メールを用いた遠隔ファイル操作方式において，中継サーバは電子メールの送受信を行うという大きな役割を持つ．

初期登録

ユーザはまず WWW を通して，ID，Password，メールアドレスを中継サーバに初期登録する．初期登録された情報は，中継サーバ内に置かれてあるデータベースにユーザのメールアドレスに対応したユーザ ID として保管される．

出先からログインの要求がくると，中継サーバからファイルサーバへ，ID と SAS-2 認証で必要な情報を電子メールに乗せ通達する．

転送処理

ユーザからファイル操作要求を受けると中継サーバは，ユーザとファイルサーバ間での認証を行うため，メールサーバへ電子メール転送を開始する．初回登録の際，ユーザからアクセス要求を受け生成された，ユーザ ID とパスワード情報があらかじめ中継サーバに蓄積されている．このユーザ認証情報とファイル操作コマンドをファイルサーバ側のメールサーバに電子メールで送信する．

ファイルサーバ側のメールサーバでは，届いた電子メールから認証情報を引き出す．ファイルサーバにてユーザ認証を行い，認証が成功するとファイル操作を行い，相互認証情報とファイル操作結果を電子メールで中継サーバに送信する．

閲覧要求

ファイルサーバから送られてきた相互認証情報とユーザ側の相互認証情報が一致し，相互認証が成功すると，中継サーバは，ユーザが取得したいファイル情報またはユーザが

送信したいファイル情報を WWW ブラウザで閲覧できる HTML(Hyper Text Markup Language) 形式で出力する.

データベース

中継サーバではユーザの管理にあたり，データベースを用いることとする．このデータベースにおける役割を以下に示す.

- 各ユーザの ID，Password の管理・・・初回認証時に ID，Password が発行された時，その情報を保管し，次回から ID，Password を入力するとただちに個人環境に入れるようにする.
- 前回のファイル情報の保管・・・前回までに取得してあるファイルを保管，蓄積しておく.
- 各ユーザのメールアドレスの保管・・・ID，Password と同様に，毎回アクセス先のメールアドレスを登録しなくていいようにするため，メールアドレスを保管しておく.

3.2.5　ファイルサーバシステム構成

ファイルサーバは，基本的に中継サーバの指示のもと，出先端末との認証処理と中継サーバへのファイル送信，また，中継サーバから送信されてきたファイルのアップロードを行う．メールサーバで受け取った情報をファイルサーバに送り，ファイルサーバは受け取った情報から処理を行う.

出先にて急遽ファイルが必要となった場合を想定し，あらかじめ環境の設定を必要としない.

3.2.6 SAS-2 認証を用いたファイル転送プロトコル

本研究では，ユーザ認証の対象として出先端末とファイルサーバ間を考える．

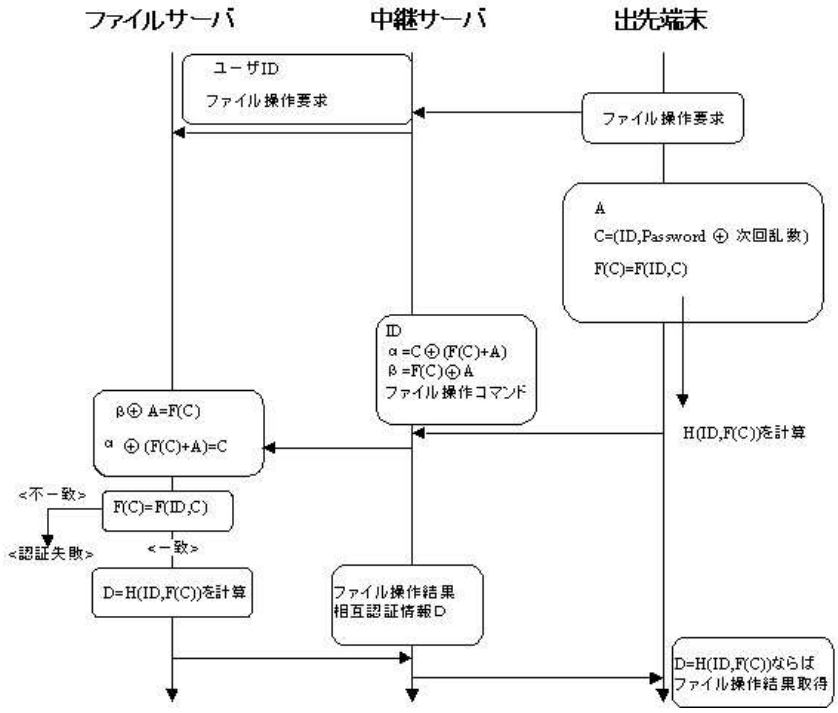

図 3.4 SAS-2 認証を用いたファイル転送プロトコル

出先端末は，認証に必要なデータを中継サーバ経由でファイルサーバに送信する．まず，出先端末から，認証に必要なデータを暗号化して HTTP 通信を用いて中継サーバに送る．中継サーバに送られてきたデータは，そのままの形で電子メールに添付しファイルサーバに送信される．ファイルサーバは送られてきた情報を保持しておく．次に出先端末で A，C，F(C) を計算した後に，ID，α，β，ファイル操作コマンドを暗号化し中継サーバ経由でファイルサーバに送信する．出先端末では相互認証用の H(ID，F(C)) を計算し保持しておく．ファイルサーバでは認証処理を行い，認証が成功すると，ファイル操作を開始する．また，相互認証用のデータも計算しておく．ファイル操作が完了すると，ファイルサーバから中継サーバへ，ファイル操作結果，相互認証情報を暗号化したものを電子メールに添付し送信する．

出先端末は保持しておいた相互認証用の H(ID，F(C)) と送られてきた相互認証情報を比

較し，相互認証が成功するとファイル操作結果を得られる．

3.3　中継サーバ，ファイルサーバ間での電子メールの流れ

本研究では，ファイルサーバから出先端末にファイルを受信する場合と，出先端末からファイルサーバにファイルを送信する場合の遠隔ファイル操作方式を提案する．

3.3.1　ファイル受信操作時における電子メールの流れ

図 3.5 にユーザがファイルサーバから出先端末にファイルを受信操作する際の，中継サーバとファイルサーバ間の電子メールの流れを示す．

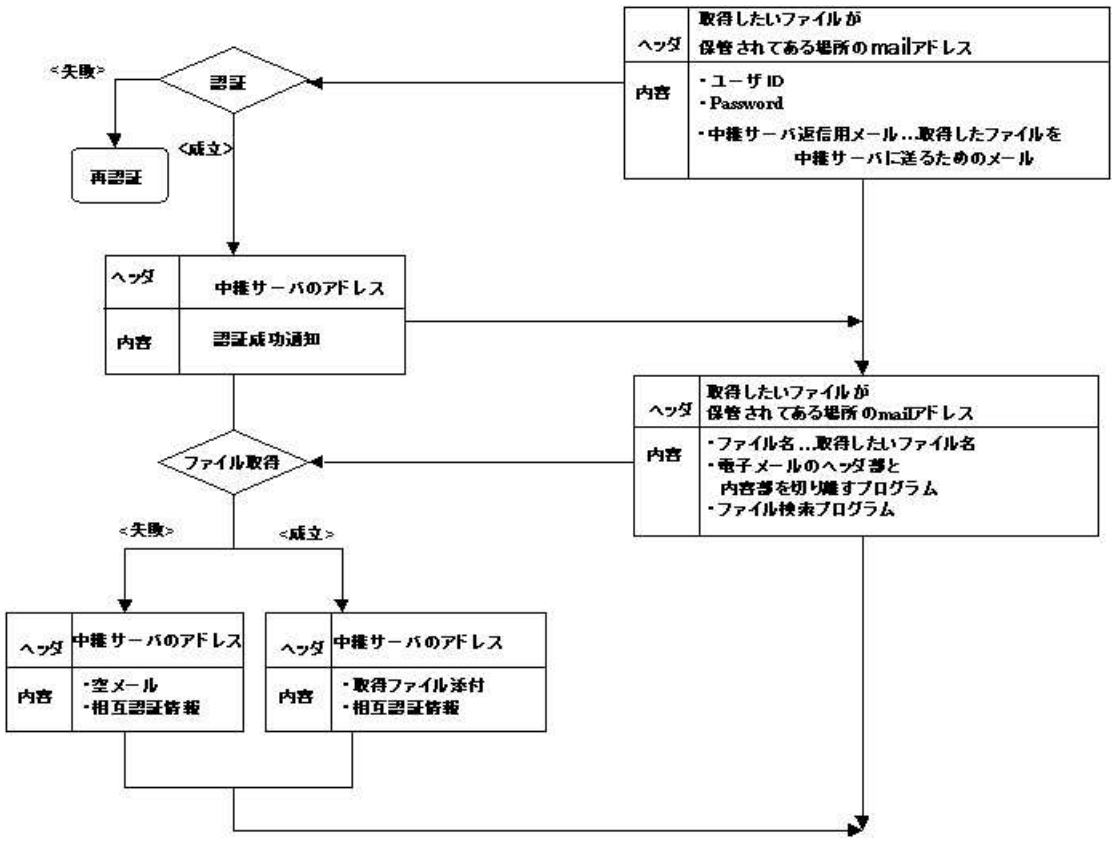

図 3.5　ファイル受信時における電子メールの流れ

まず，中継サーバからユーザ ID，Password，中継サーバ側のメールアドレスを添付した

電子メールをファイルサーバ側に送信する．

ファイルサーバでは受け取ったユーザ認証情報から SAS-2 認証を開始する．認証が成功すれば，中継サーバに認証成功が電子メールで通知される．認証成功が通知されると，中継サーバは，ユーザから取得要求があったファイル名と電子メールのヘッダ部分と内容部分を切り離すプログラム，ファイル検索プログラムの 2 つのプログラムを電子メールに添付しファイルサーバに送信する．

ファイルサーバではファイル検索プログラムが作動し，取得要求のあったファイルの検索が開始される．ファイル検索が終了すると，ファイル検索結果と SAS-2 認証における相互認証情報を電子メールに添付し，中継サーバに送信する．

ユーザは，出先端末において計算し，保持しておいた相互認証用のデータとファイルサーバから中継サーバに送られてきた相互認証情報を比較し，相互認証が成功するとファイル取得結果を得られる．

3.3.2　ファイル送信操作時における電子メールの流れ

図 3.6 にユーザが出先端末からファイルサーバにファイルを送信操作する際の，中継サーバとファイルサーバ間の電子メールの流れを示す．ファイル受信操作に比べ，出先側から一方的にファイルサーバにファイルを送信するため，認証処理以降の手順が少ない．

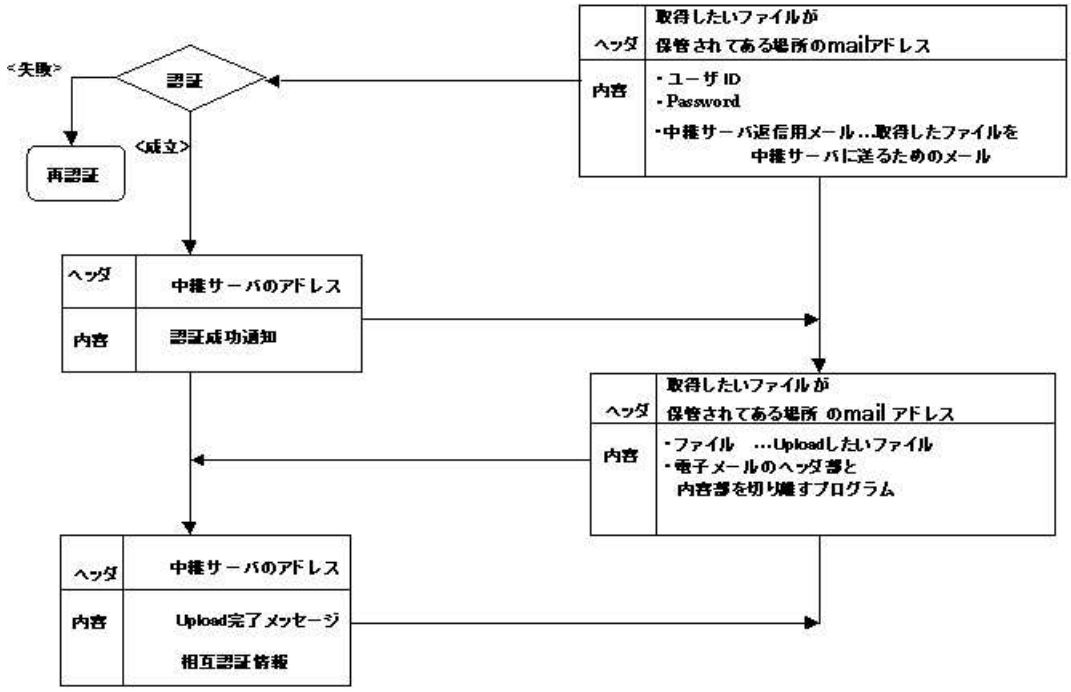

図 3.6　ファイル送信操作時における電子メールの流れ

ファイル受信操作時と同様に，中継サーバからユーザ ID，Password，中継サーバ側のメールアドレスを添付した電子メールをファイルサーバ側に送信する．

ファイルサーバでは受け取ったユーザ認証情報から SAS-2 認証を開始する．認証が成功すれば，中継サーバに認証成功が電子メールで通知される．認証成功が通知されると，中継サーバは，ユーザの送信命令に従い，電子メールに指定されたファイルと電子メールのヘッダ部分と内容部分を切り離すプログラムを添付し，ファイルサーバ側に送信する．

ファイルサーバは受け取ったファイルをホームディレクトリ以下の特定のフォルダに保存し，ファイル受信完了メッセージと，SAS-2 認証における相互認証情報を電子メールに添付し，中継サーバに送信する．

ユーザは，出先端末において計算し，保持しておいた相互認証用のデータとファイルサーバから中継サーバに送られてきた相互認証情報を比較し，相互認証が成功するとファイル送信結果を得られる．

第 4 章

試作システム

第 3 章までで述べてきた，出先端末，中継サーバ，ファイルサーバの 3 者間でのファイル操作を実現するため，以下のような試作システムを構築した．

4.1　試作システム環境

＜出先端末＞

- CPU:Pentium　345MHz
- メモリ:128MB
- HDD:4GB
- OS:Windows2000SP2
- Web ブラウザ:IE6.0SP2

＜中継サーバ＞

- CPU:Celeron1.5GHz
- メモリ:256MB
- HDD:40GB
- OS:Windows2000SP2
- Server:AN HTTPD1.4
- System:PHPversion4.2.2

- ServletEngine:ApacheJServ1.1.2
- Data Base:MySQL3.23
- SMTP Server:Radish ver1.0.0
- POP Server:PS.PoP3

＜ファイルサーバ＞

- CPU:Celeron1.2GHz
- メモリ:256MB
- HDD:40GB
- OS:Windows2000SP2

上記のような試作システム動作環境を用意した．ファイル操作処理負荷のかかることを想定し，中継サーバマシンには比較的高スペックマシンを用意し，出先端末には一般的なユーザを想定し，比較的低スペックのマシンを用いた．

4.1.1　認証画面

ユーザは，ファイルサーバへ Web ブラウザを用いてアクセスすることを前提としている．そのため，試作システムでは図 4.1 のようなログインフォームを作成した．ID と Password を入力し，ファイルサーバへ送信するこれにより SAS-2 認証が行われる．

初めて利用するユーザは，下記に示してある ID 発行ウィザードに進み初期登録ができるようになっている．

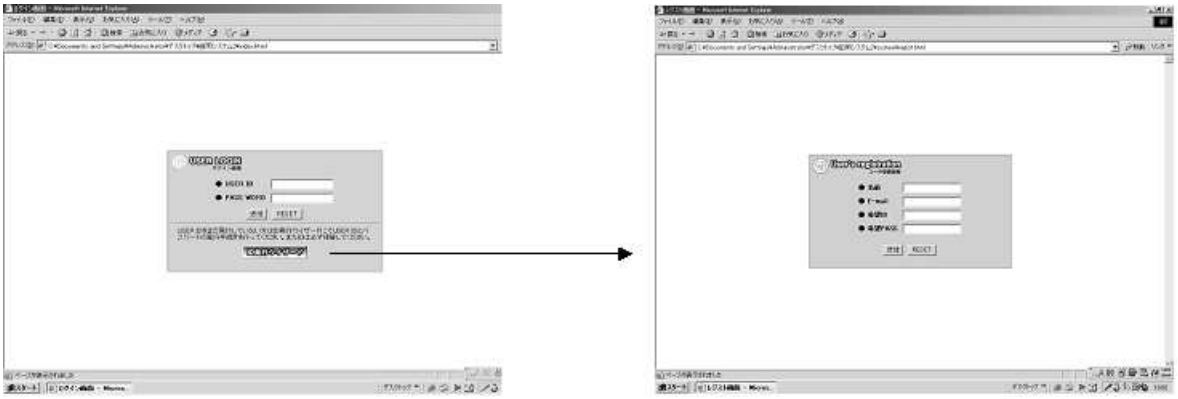

図 4.1　認証フェーズ

初期登録では，名前の他に，アクセスしたいファイルサーバ先のメールアドレス，SAS-2 認証を行うための，ID，Password を登録する．ここで登録されたデータは，中継サーバのデータベースに蓄積され電子メールによるファイル操作が可能となる．

4.1.2　メイン画面

ユーザは，SAS-2 認証が成立すると，図 4.2 で示すメイン画面に移る．

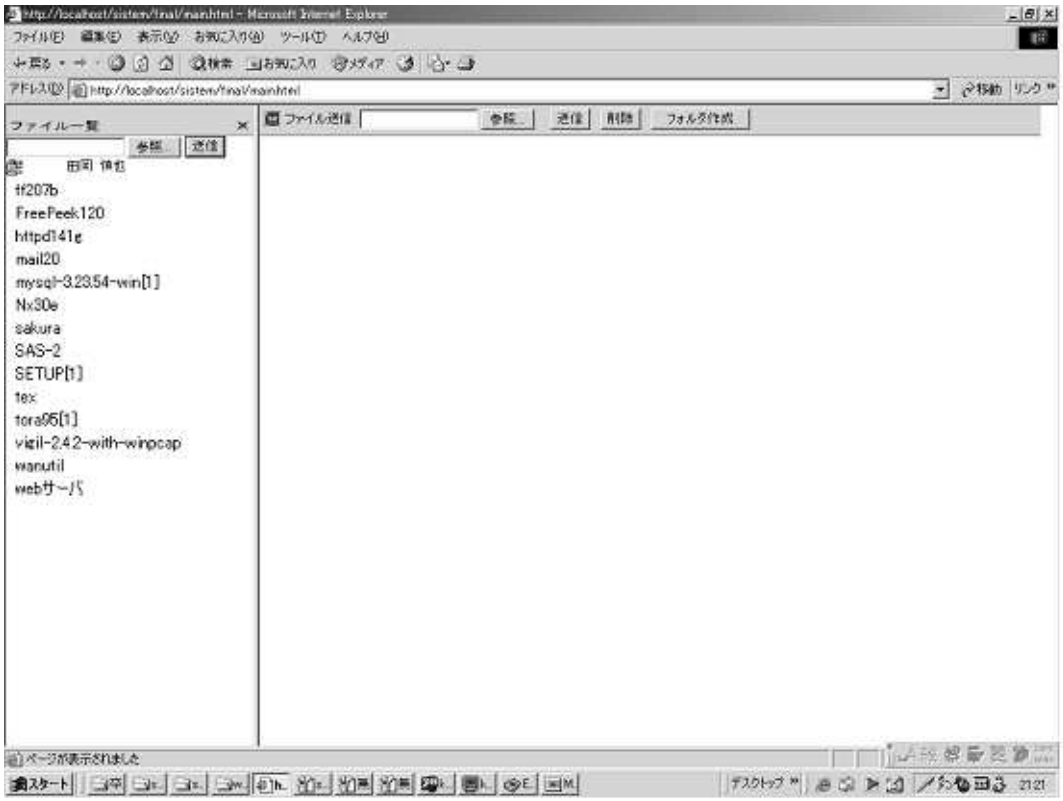

図 4.2　メイン画面

メイン画面では，画面左側にてファイル受信操作が出来るようにしてある．参照ボタンでファイルを階層状態で表示し，コマンド送信ボタンにてファイル取得が可能となる．

ファイル送信操作は画面右側上部である．これもファイル受信の場合と同様に，参照ボタンで今使用しているパソコン内にあるファイルの一覧を見ることができ，コマンド送信ボタンからユーザは出先端末からファイルサーバにファイルをアップロードすることができる．

ユーザができるだけ使い易いようにインターフェースを作成した．

4.1.3　ファイル受信処理

ファイルサーバにどのようなファイルがあるのか検索を行う場合，欲しいファイルが置かれてあるディレクトリ名を送信フォームに打ち込み参照ボタンを押す．これによりファイルサーバ内にある指定したディレクトリ以下のファイルが画面左側に表示される．

ファイル取得の場合，ユーザは出先にて欲しいファイルを選び，送信フォームにファイル名を打ち込み送信ボタンからデータを送信する．

出先端末からデータが送信されファイルサーバにファイルがあれば画面右側に取得されたファイルが表示されるようになる．なお今までに出先端末にて要求を出し，中継サーバ内のデータベースに蓄積してきたファイル情報も画面右側に表示されるようになっており，新しく取得したファイルは，それらの一番上に表示される．

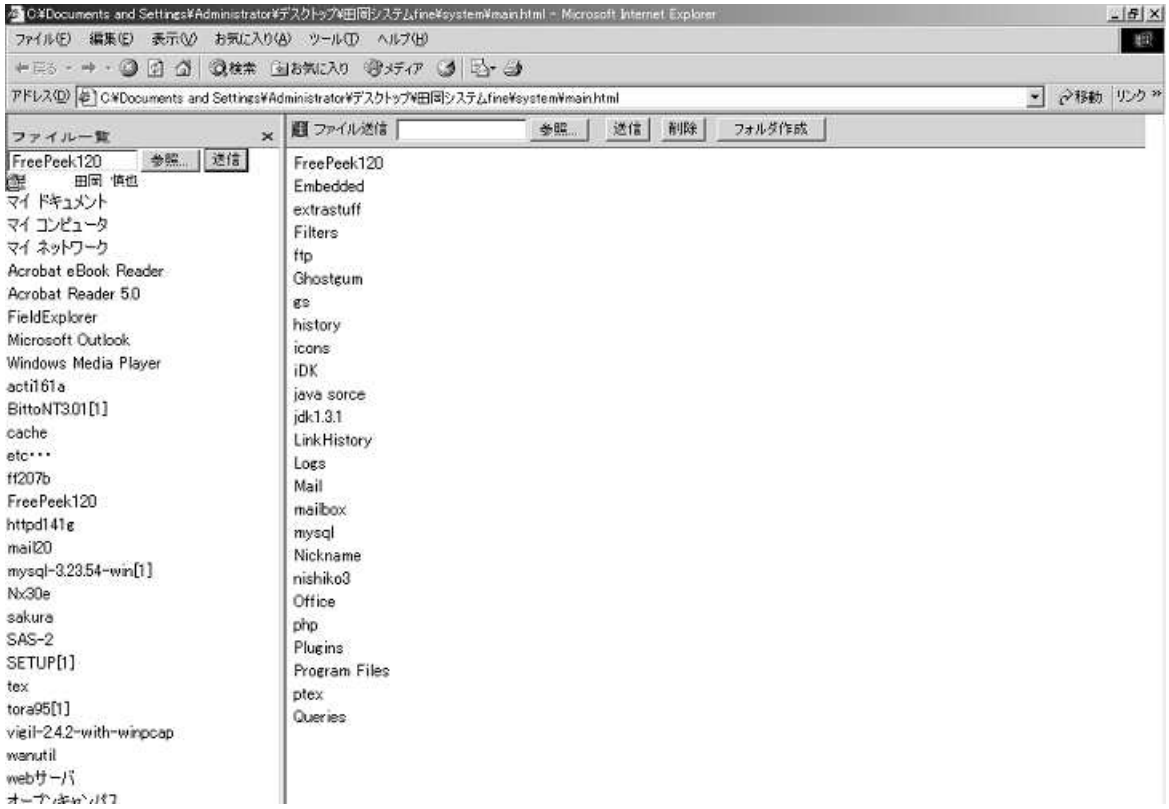

図 4.3　ファイル受信画面

ファイル一覧の閲覧処理は，ファイルそのものを取得してくるのではなく，ファイル名のみを抽出する方法をとる．これにより，ファイルそのものを取得するよりもクライアント/サーバにかかる処理負荷及びファイル操作時間が軽減される．

ファイル受信における一連の流れは以下の通りである．

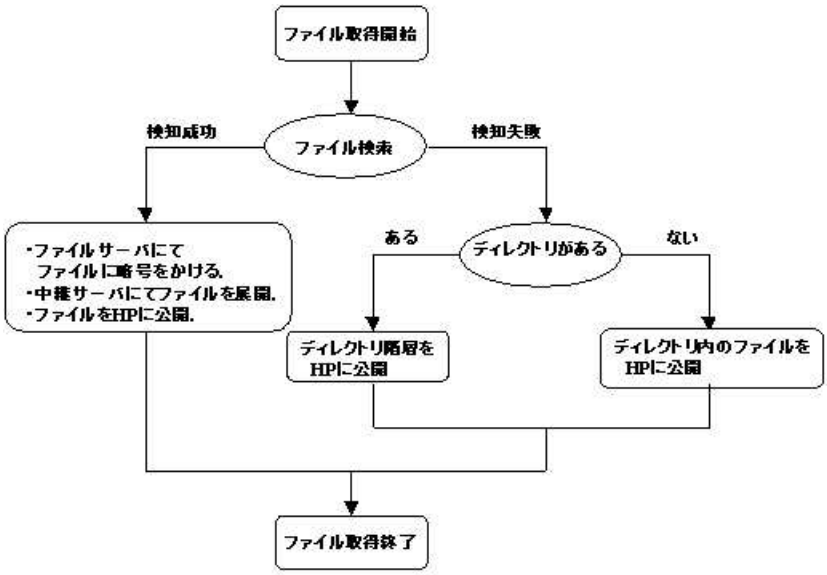

図 4.4　ファイル受信の流れ

ユーザから送信されたファイル受信命令に従い，ファイルサーバでは指定されたファイルがあるかどうかの検知を開始する．指定されたファイルがある場合はそのファイルを暗号化し，中継サーバに送信する．中継サーバではファイル取得後，ファイルを展開し，ホームページにファイル取得情報を公開することにより一連の流れが終わる．しかし，指定したファイルがディレクトリである場合は，ディレクトリ階層を返すようになる．

4.1.4　ファイル送信処理

ファイルを出先からファイルサーバにアップロードする際の手順は以下の通りである．

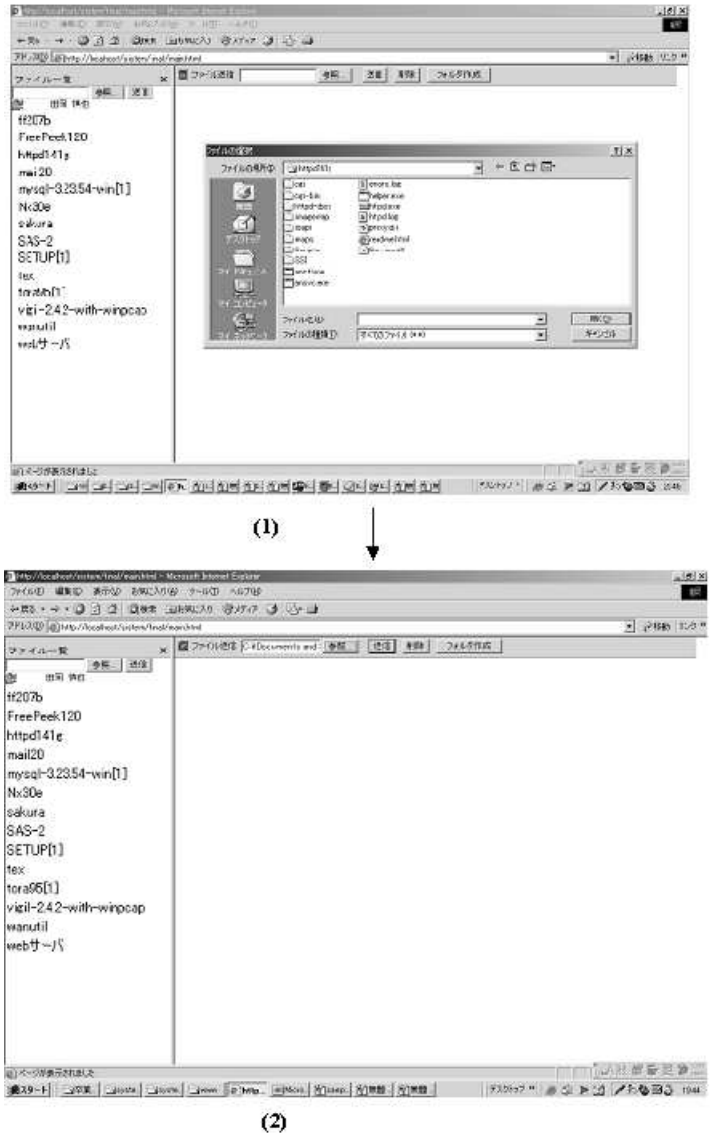

図 4.5　ファイル送信画面 1

ユーザが参照ボタンを押すことにより，図 4.5 の (1) のように出先の端末内にあるファイルが表示される．この中からユーザがアップロードしたいファイルを選ぶ．ファイルを選び確定すると，図 4.5 の (2) のように自動的にファイル送信フォームにファイル名が書き込まれる．

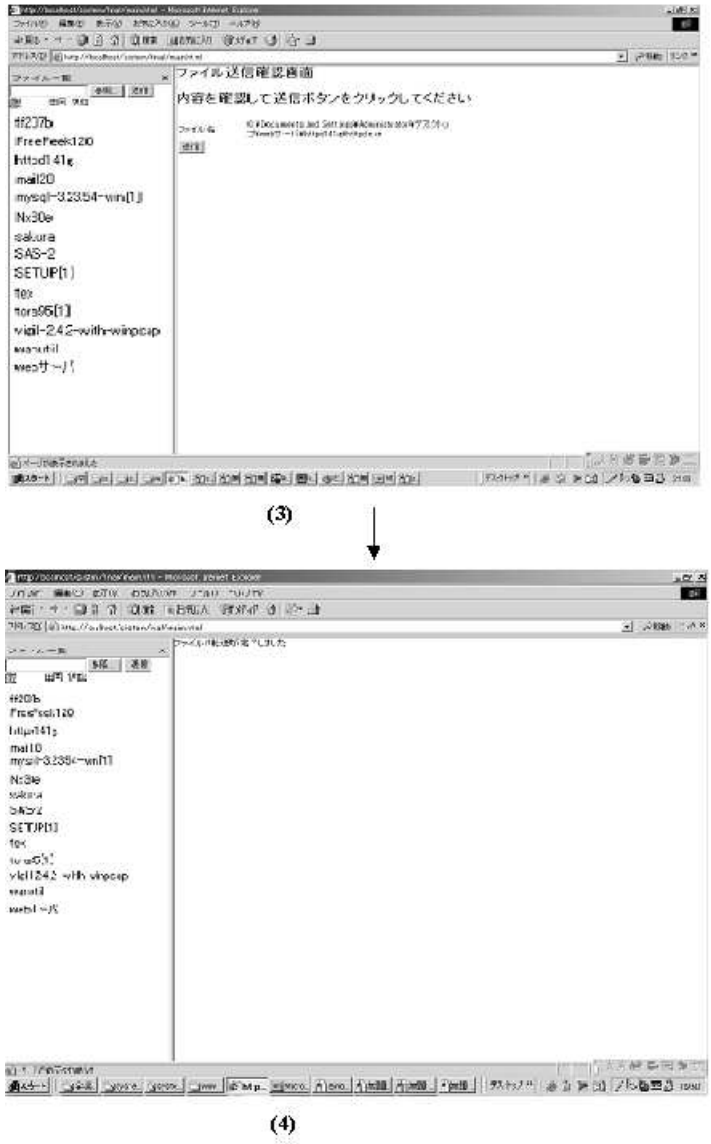

図 4.6　ファイル送信画面 2

図 4.6 の (3) はファイルをアップロードする際の最終確認画面である．ファイルが間違っていなければ送信ボタンを押すことにより指定ファイルがファイルサーバに送信される．何のトラブルもなくファイルのアップロードに成功すれば図 4.6 の (4) の送信完了通知が返ってくる．

図 4.6 の (3) の送信ボタンはメール送信に直結してあるため，メールによる転送トラブルが起こり転送失敗の場合に限り，ファイル転送失敗通知が表示される．

4.2 評価

処理手順の多いファイル受信操作において，以下の 2 点の測定を行った．

- 出先端末からファイル取得要求を出し，ファイル取得処理完了後，出先端末がファイル取得結果をホームページ上で得られるまでの時間の測定．
- 出先端末からファイル取得要求を出し，ファイル取得処理完了後，出先端末がファイル取得結果をホームページ上で得られるまでの出先端末での CPU 負荷率の測定．

ファイルの大きさを 11 パターン用意し，それぞれのファイルに対して取得にかかる時間の計測を行った結果を表 4.1 に示す．

KByte	50	100	150	200	250	300
Time(Second)	6.532	7.514	8.535	9.707	10.969	12.420

KByte	350	400	450	500	1000
Time(Second)	14.113	15.996	16.226	17.278	36.846

表 4.1 ファイル受信時間

小さなファイルの受信操作であるが，電子メールと HTTP 通信を用いての，3 者間でのファイル操作のため，転送処理に時間がかかるという結果が得られた．

11 パターンのファイル受信操作を行う際に，出先端末にかかる CPU 負荷を計測した．

計測結果を図 4.7，図 4.8，図 4.9，図 4.10 に示す．

なお，図 4.7 は 50KByte，100KByte，150KByte，200KByte，図 4.8 は 250KByte，300KByte，350KByte，400KByte，図 4.9 は 450KByte，500KByte，図 4.10 は 1MByte のファイル受信の際に出先端末にかかる CPU 負荷率の結果である．

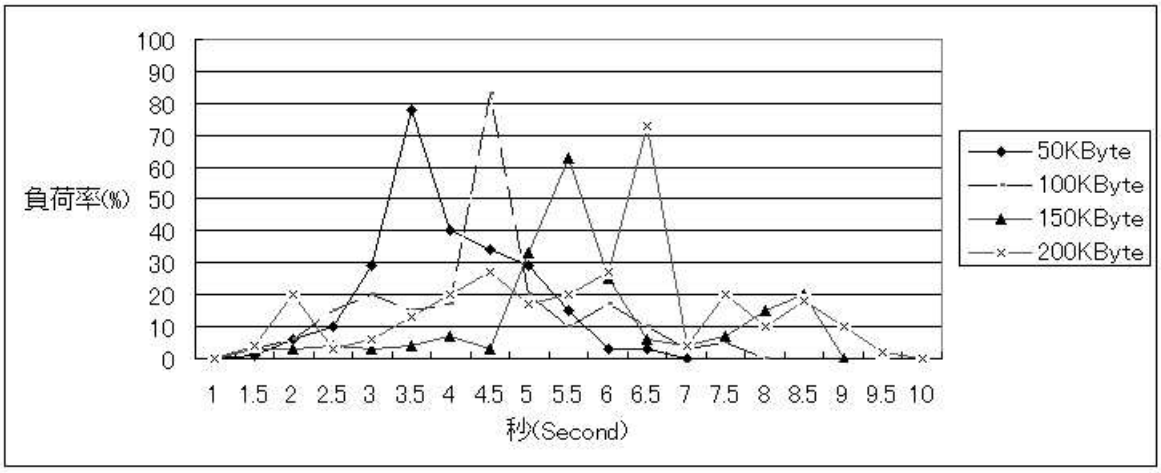

図 4.7　CPU 負荷率．1

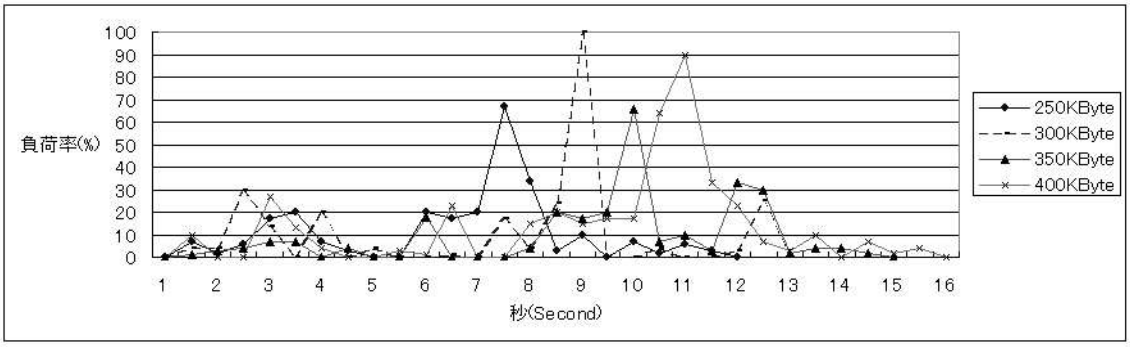

図 4.8　CPU 負荷率．2

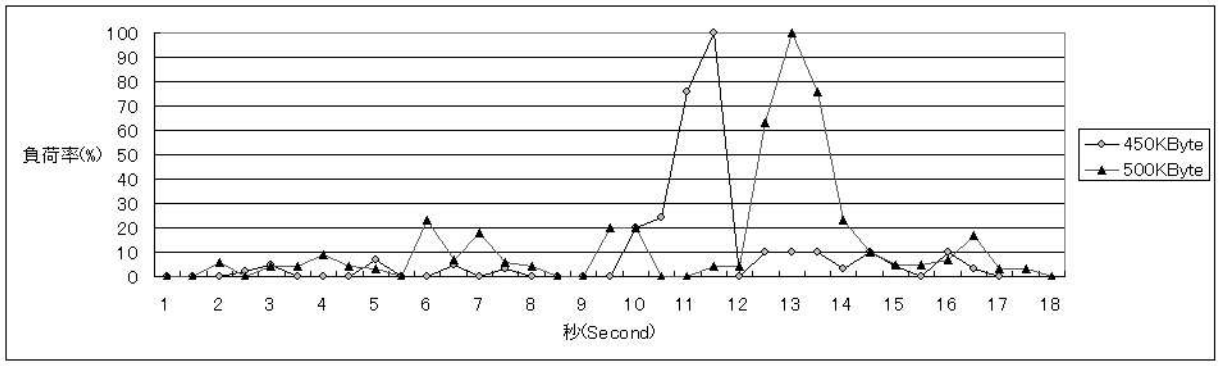

図 4.9 CPU 負荷率．3

図 4.10 に示す 1MByte のファイル受信操作における出先端末の CPU 負荷率は，処理負荷の変動の大きな部分を抜粋してグラフにした．

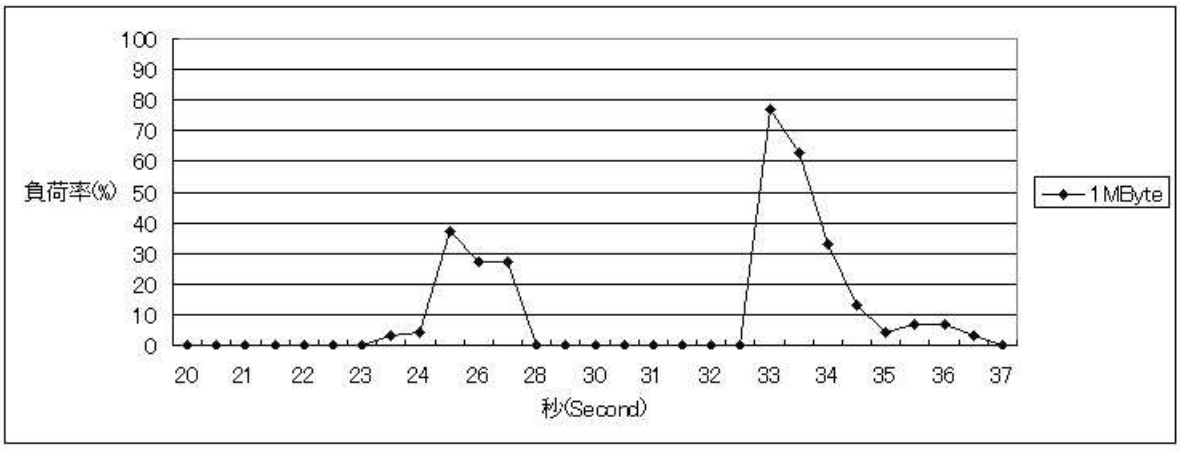

図 4.10 CPU 負荷率．4

ファイル受信操作における出先端末の CPU 負荷率の計測より以下のような結果が得られた．

- どの大きさのファイルにおいても，最大負荷値は違えど，ほぼ同様の一定な波形である．
- ファイル受信操作後半に最大負荷値が見られる．
- 最大負荷値以外の波形は低い値で安定している．
- 最大負荷値は 1 秒から 2 秒以内に低い値に戻り，波形が安定する．
- 最大負荷値は 60%から 100%の間にある．

今回の評価実験からファイル操作に時間はかかるが，出先端末に与える処理負荷が少ないシステムであることが証明された．

ファイル取得操作において出先端末では，ファイル取得命令を中継サーバに送った後，ファイル取得情報が送り返されるまで待ち状態に入るゆえに，ファイル取得情報を得た時のみ出先端末の CPU 負荷が大きく変動したと考えられる．CPU にかかる大きな負荷はファイル操作全体から見ると短い時間であり，システム全体として出先端末にかかる負荷は少ないといえる．このことから，本システムは比較的低いスペックのマシンでのファイル操作が実現できる．

第 5 章

今後の課題

5.1 実装システムに対する課題

本研究では，システム構成を提案し，容易にファイル操作ができるシステムを実現した．しかし，認証情報，ファイル操作コマンド，ファイルの暗号化を行うというまでには至っていない．そこで，認証情報，ファイル操作コマンド，ファイル等に対して，出先端末とファイルサーバ間に鍵共有を施し，暗号化，複合化を行うことでよりセキュアなシステムを構築しなければならない．さらに暗号化処理を行うことにより，現段階のシステムよりもファイル操作に時間がかかることも予想される．

電子メールによるファイルの添付は 1MByte までが限度であり，それを超えると処理が重くなったり，電子メール送信ができない場合が生じる．そこで 1MByte を超えるファイルに対して，1 つのファイルを分割し電子メールに添付することで大きなファイルに対応していかなければならない．

出先端末からファイルサーバ内のファイルを削除したり，ディレクトリを作成する等，システムに拡張性を持たせることも必要である．

また，出先端末のローカルファイルへのアクセス方法や通信トラブルからの回復手段の確立も考えていく．

5.2　評価項目に対する課題

評価項目の課題として，以下のようなものが考えられる．

- サーバにかかる負荷実験を行わなければならない．今回ファイル取得時にかかる出先端末にかかる負荷実験を行ったが，サーバにかかる負荷実験も行い，どういったスペックマシンがサーバ環境に最適である実験する必要がある．
- 様々な回線においてネットワークトラフィックを測り，ネットワークに及ぼす負荷を計測する．
- 実際に使ってもらうことによりインタフェースの評価を行い，ユーザの使い易いものに改良する．

第 6 章

おわりに

本研究では，ファイルサーバと出先の端末の間に中継サーバを置き，3 者間でのファイル操作方式を提案し実装した．出先端末と中継サーバ間の通信には HTTP を用い，中継サーバとファイルサーバ間では POP/SMTP を用いることで，出先端末の環境に依存せず，セキュアなファイル送受信を行った．また，評価実験の結果より，比較的低スペックマシンでのファイル操作も可能であることがわかった．

今後はシステムを拡張し，より実用的なものへと改良していくことが必要である．

謝辞

高知工科大学工学部情報システム工学科 清水 明宏教授には，研究室配属以来，就職活動，卒業研究を含め，学生生活全般に渡って懇切なる御指導，貴重な御教示を賜った．ここに深謝申し上げる．

高知工科大学大学院 工学研究科 基盤工学専攻 情報システム工学コース 2 回生 辻 貴介氏には，研究内容について有益な語義論をいただき御指導を賜った．

高知工科大学大学院 工学研究科 基盤工学専攻 情報システム工学コース 1 回生 大垣 文誉氏，上岡 隆氏，河村 智氏，高知工科大学 情報システム工学部 4 回生 池上 奈津子氏，岸田 光生氏，小西 竜也氏，永井 慎太郎氏，奈良 裕介氏，藤本 卓氏 3 回生の福冨 英次氏をはじめ皆さんに御協力頂いた．ここに記して謝意を表する．最後に在学中に様々なご助言，ご指導を頂いた諸先生方に深謝申し上げる．

参考文献

[1] 堀岡 力, 戸田 昌浩, 清水 明宏, NTT ヒューマンインタフェース研究所, “電子メール転送サービス方式の検討”, pp.38-40, 1997-09

[2] T. Tsuji, T. Kamioka, and A. Shimizu, “Simple and secure password authentication protocol, ver.2(SAS-2), ” IEICE Technical Report, OIS2002-30, vol.102, no.314, pp.7-11, September 2002.

[3] 西沢 直木

“PHP による Web アプリケーションスーパーサンプル”

ソフトバンクパブリッシング株式会社

[4] Steven Holzner

“Java プログラミング Black Book”

株式会社インプレス

[5] 電子メールのセキュリティ

http://www.ipa.go.jp/security/fy12/contents/smime/email_sec.html