

「ネットワーク口座データ振り込みシステム」の検討

5 F - 9

*瀧塚令子、**八幡勝也、***波多江武文、*伊藤篤、*浅見徹

*(株)KDD 研究所、**産業医科大学、***(有)ソフトウェアプロ

1. はじめに

インターネットのユーザ間で大容量データを転送する場合、データの送達確認と転送の信頼性確保ができないという問題がしばしば発生する。また、これまでのファイル転送サービス[1]では、送信の度に端末から、サーバにデータ転送する時間がかかり、高速のデータ転送ができないという問題があった。さらに、大勢の人とネットワーク上でファイルのやりとりを行う場合、相手アドレスやパスワードの管理が個人レベルでは困難であるという問題がある。そこで、これらの問題を解決するため、ネットワーク上にユーザデータを保管するサーバをたちあげ、各ユーザが、そのサーバをデータの銀行口座のように使用することにより、高い信頼性のある高速なデータ転送、送受信のログ等データ転送の状況管理、ユーザデータの保管、ならびにユーザ管理を行う「ネットワーク口座データ振り込みシステム」を検討し、基本機能と操作性を確認するための簡易なプロトタイプを開発した。

2. システムの概要

システムは、インターネットに接続するサーバマシンとサーバマシン上にデータ口座をもつユーザ端末群（以下ドメインと呼ぶ）の集合である。図1は、A、B 2つのドメインから成るシステムの例である。

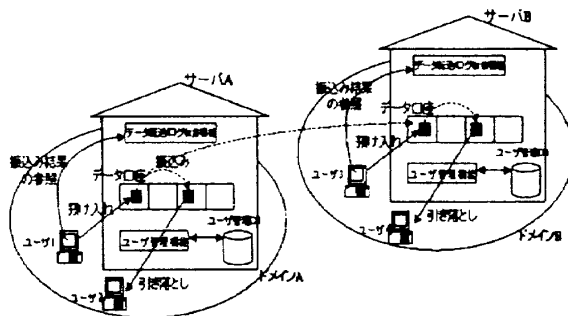


図1 システム構成図

サーバ上には、「データ口座」と呼ばれる各ユーザ専用のデータ領域が存在する。各ユーザはこの「データ口座」領域に、図2に示す操作を行うことができる。データの振り込み作業は、同一ドメイン内の口座間で

も、ドメインの異なる口座間でも行うことが可能である。このように、データ転送作業をサーバ上に設置したデータ口座間で行うことにより、直接ユーザ端末間で転送作業を行うときに比べ、迅速かつ安全なデータ転送が実現できる。尚、通常の利用においては、データの振り込み完了時には、ユーザ端末へのデータの自動ダウンロードではなく、振り込み先のユーザに、ファイルの名前、サイズ、形式を記述したメールを送付することとした。これにより、ユーザは、用途や緊急性に応じて、都合のよい時に、データをダウンロードしたり、口座内においたまま参照することが可能であるため、不要なデータのダウンロードを避けることが可能となる。また、本システムの開発においては、ネットワークに関する知識に乏しいユーザにとって容易に利用可能なインターフェースの構築も検討課題の一つとし、WWWブラウザを用いたGUIを採用した。

ユーザの作業	サーバ機能
データの預け入れ	データのアップロード (ユーザ→サーバ)
データの引き落とし	データのダウンロード (サーバ→ユーザ)
データの振り込み	データの転送 (口座→口座)
振り込み結果の参照	データ転送ログ情報の管理

図2 ユーザの作業とサーバ機能との対応

3. システムの機能

本システムの提供する主な機能は以下の通りである。

- ユーザ管理
- 口座内のデータ管理
- 口座間のデータ転送
- データ転送ログ情報の管理

以下では、まず本システムの構築にあたり留意した点を述べた後、各機能の概要を説明する。

3.1 設計のポイント

- 不正なアクセスの防止
登録ユーザ以外はシステムにアクセスできないようにするとともに、他人の口座をアクセスできないようにすることが必要である。また、ユーザが煩雑さを感じないようにすることも重要である。
- データ転送におけるセキュリティの確保
ドメイン間、ユーザ端末-サーバ間で転送するデータを外から見えなくすることが必要である。また、万が一サーバに侵入された場合でも、他のサーバへのアクセス方法が容易にわからないようにする必要がある。
- 口座アクセス/データ転送履歴の保存

"A Study on Online Data Account System" by *Reiko TAKIZUKA, *Katsuya YAMA TA, ***Takefumi HATAE, *Atsushi ITO and *Tohru ASAMI
*KDD R&DLaboratories, **University of Occupational and Environmental Health, ***Soft Wa vePro

データを送ったこと、データの転送が確実に完了したこと、相手に届いたこと、相手がアクセスしたことを確認できることが必要である。

● ユーザ情報の秘匿

ユーザのパスワード、住所、電話番号など、データの転送に必要でないユーザ情報やユーザのデータ送受信履歴を安全に保管することが必要である。

● 高速な転送

ユーザ端末とサーバの回線に依存せず、高速なデータ転送を実現する。また、同一データを複数の口座に転送する場合、同報転送を行い、高速転送を実現する。

● モバイル環境を含むアクセスの自由度向上

データの預け入れ、振り込み、引き出しの操作は、さまざまな状況で必要となる。このため、モバイル端末を含む環境での利用を実現する必要がある。

3. 2 機能概要

(1) ユーザ管理

システムのセキュリティを維持するため、登録済のユーザのみがシステムを利用可能であり、また、ユーザは、口座を持つドメインのサーバにのみアクセス可能とした。ユーザ登録は、登録申請に伴い、登録先ドメインのサーバ管理者のみが行い、ユーザはパスワード以外のユーザ情報は変更できないこととした。ユーザ情報は、ユーザ名、パスワード、氏名、住所、電話番号、ドメイン名、ユーザ端末アドレス、口座領域の大きさ、データ口座へのパス名等であり、ユーザ管理DBに登録される。システム内の各サーバは、データ転送を行うため必要なシステム内の全ユーザの情報を持つが、他ドメインのユーザに関しては、データ振り込み作業に必要な情報のみである。一方、ユーザは、他のユーザの情報として、ユーザ名、メールアドレス等のデータ振り込み先の決定に必要な情報に限り参照可能である。尚、ユーザ情報を分散DB化することによるセキュリティ向上も検討中である。また、プロトタイプシステムでは、サーバは、ログイン可能なユーザをWWWサーバのアクセス制御機能を用いて、ユーザ名とパスワードで判別するが、システムの安定運用のため、ユーザは、常に唯一の決まった端末からのみシステムを利用するようにすることが望ましい。しかし、実際には、ユーザが自宅や外出先等から、モバイル環境を利用して口座内のデータにアクセスすることが考えられる。このため、MobileIP[4]機能の付加を検討している。ユーザ名とパスワードの入力は、不慣れたユーザにとっては煩雑なので、これをカットスルーする機能の付加も今後の課題である。

(2) 口座内のデータ管理

各ユーザは、ユーザ端末のWWWブラウザを通して、自分自身の口座内のデータのアップロード、ダウンロード、参照、削除を行うこととした。データのアップロード、ダウンロード、参照は、WWWブラウザが有するFTPサーバアクセス機能を用いて実現し、データ削除はCGIプログラムで実現し、ユーザが容易に操作可能とした。また、ユーザ端末から口座へのアクセスにおけるセキュリティを高めるため、SSLまたは、IPsec[2]の利用を検討している。なお、ディレクトリのアクセス権を設定することにより、他ユーザのデータ口座領域へのアクセスを禁止することとした。

(3) 口座間のデータの転送

他のユーザのデータ口座へのデータの振り込み、すなわちデータ転送処理はFTPを用いて実現した。FTPの利点は、データ転送の開始/完了や成功/失敗が明確にわかることである。しかし、FTPは相手サーバへのログインを行うため、このパスワードが漏れるとシステムのセキュリティが保てなくなるという問題がある。そこで、IPsec[2]を利用したサーバ間認証とデータ暗号化機能を付加し、ネットワーク上でのパスワードの漏洩を防ぐような方策が必要となる。また、FTPによるデータの振り込みは一サーバ対一サーバとなるが、転送時間の短縮を考慮すると、複数のサーバにある口座に同時にデータを振り込む機能が必要である。そこで、データ転送にマルチキャスト対応のFTP(MFTP)[3]を利用する等の方策が必要となる。

(4) データ転送ログ情報管理

ユーザがデータの振り込み結果を容易に確認するため、自分の口座からデータを振り込む時点、自分の口座にデータが振り込まれる時点、振込先利用者によるダウンロード時点における転送開始年月日時刻、転送時間、ファイル名、大きさ、タイプ(asciiまたはbinary)等の情報をWWWブラウザ上で参照可能とした。

5. おわりに

本論文では、データを高速かつ安全に転送することを目的とした「ネットワーク口座データ振り込みシステム」の設計方針と機能概要を述べた。今後は、プロトタイプシステムの操作性等を評価するとともに、セキュリティや使い勝手の向上のための改良を行う予定である。最後に、日頃御指導頂く(株)KDD研究所 村谷所長、鈴木副所長、山本副所長に感謝します。

[参考文献]

[1] e-Percol: URL=<http://www-e-percol.ne.jp/>

[2] RFC1825 等: URL=<http://www.ietf.org/html.charters/ipsec-charter.html>

[3] MFTP 等: URL=<http://www.starburstcom.com/>

[4] RFC2002 等: URL=<http://www.ietf.org/html.charters/mobileip-charter.html>