プロキシを用いたシステム移行方式

大越 冬彦、村澤 靖

三菱電機株式会社 情報技術総合研究所

1. はじめに

企業間のプライベートネットワークにおけるデータ転送システムで更新時期を迎えているものが多い。これらは組織内部に閉じた環境で通信を行うものであり、インターネット上のシステムにおける移行作業とは異なる課題が存在する。今回これらの課題をプロキシを導入することにより解決し、システム移行を円滑に進める方式を提案する。

2. 対象システム

今回対象としたシステムは数百社の企業のユーザ間でのデータ転送を FTP をベースとして行うシステムである（図１）。

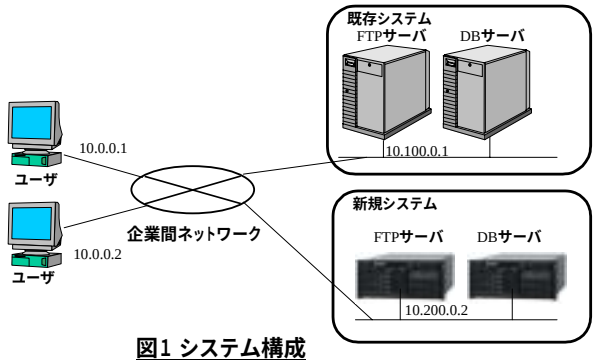


図1 システム構成

このシステムを更新するに当たり、安全性の観点から新規システムを別拠点のデータセンターに設置することとした。このため新規システムのサーバ IP アドレスの変更が必要となるが下記の点が課題となった。

・このシステムのユーザは企業間のプライベートネットワークによって接続しているため、サーバの指定に DNS を使用せずに IP アドレスを直接使用している。このためシステム側のネットワーク構成を変更する場合、ユーザ側のサーバ IP アドレス設定の変更が必要となる。しかしユーザ数が多いため、移行と同時に全てのユーザ設定の変更を一斉に行うことが困難である。

・上記を解決するために、既存システムに手を加え、新規システムにアクセスを転送する等の機構を組み込むことが考えられるが、このシステムは無停止運転のため改修や試験に必要な作業時間の確保が難しい。

・移行後、新規システムに問題が起きた場合、既存システムに復帰させる場合が考えられるが、この場合もユーザ設定の再変更が必要である。

3. プロキシによるシステム移行

これらの課題を解決するために、FTP での既存システムへのアクセスを新規システムに誘導する FTP プロキシを開発した。

（１）システム移行前にプロキシを設置する。プロキシ

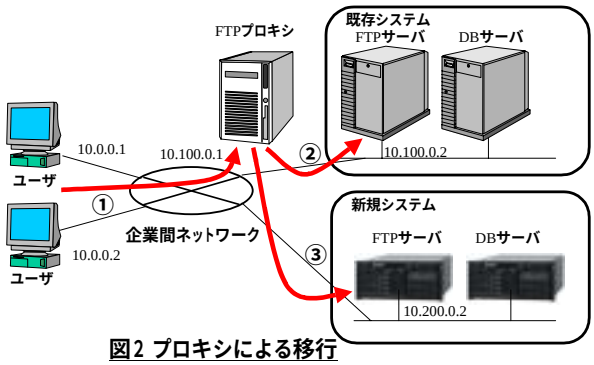


図2 プロキシによる移行

は現行システムのサーバの IP アドレスを置換し、ユーザからのトラフィックを一旦受信後、現行システムのサーバに中継する。（図２①②）

（２）システム移行後、プロキシはデータセンターに設置した新規システムのサーバにトラフィックの中継を行う。（図２①③）

（３）新規システムに問題が発生した場合、プロキシの中継先を既存システムに戻すことで対処する。

（３）プロキシはすべてのユーザが IP アドレス設定を変更し終わるまで、既存システムの IP アドレスでのアクセスを担保することで、ユーザ側 IP アドレスの変更を緩やかに行うことが可能となる。

4. 必要要件

FTP プロキシを実現するに当たり、必要な要件は以下の通りである。

4.1. 透過性

既存のユーザとの間の通信に影響を与えないために FTP プロトコルについての下記の点が要件となる。

（１）コマンド・応答

FTP の制御コネクション上で伝達される FTP クライアントからの FTP コマンド及び FTP サーバからの応答をそのまま転送する必要がある。またファイル転送を中止する際に送出される TELNET オプションによる割り込みもそのまま転送する。

（２）データコネクション

FTP では１つのファイル転送の前にデータコネクションを確立し、それを用いてファイルを転送する。この際に用いる IP アドレス、TCP ポート番号は制御コネクション上で事前に通知される。プロキシでファイル転送を中継するためには、この一連の手順において IP アドレス、ポート番号をプロキシのものに変換するとともに、FTP サーバ及び FTP クライアントに対して個別にデータコネクションを確立する必要がある。

（３）コネクション切断

FTP ではファイル転送時、データ送出元からのデータコネクションの正常切断をもって転送の正常終了としている。この正常切断が正しく通信相手に伝わらない場合、通信相手とファイル転送結果の相違が発生する可能性がある。このため正常切断と異常切断（リセット、タイム

Proxy for system migration.
Fuyuhiko OHKOSHI,Yasushi MURASAWA
Information Technology R&D Center, Mitsubishi Electric Corporation

アウト）を区別し、通信相手に伝達する必要がある。

4.2. 性能

プロキシが存在しない場合に比較して
・コネクション確立時間
・ファイル転送時間
の著しい性能劣化を避けることが必要である。

5. 構成

これらの要件を前提に FTP プロキシを Linux 上において実装した。S/W 構成を図３に示す。

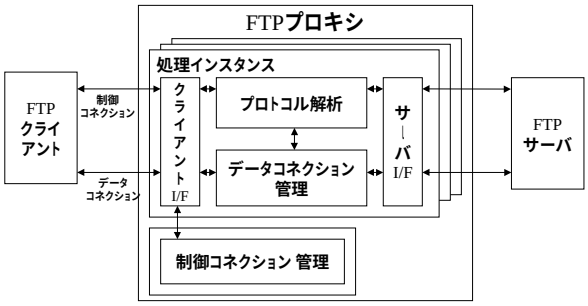


図3 S/W構成

動作の概略は以下の通りである。
（1）FTP クライアントからの制御コネクションは制御コネクション管理部によって受信され、処理インスタンスを作成する。
（2）生成された処理インスタンスは FTP サーバとの間で制御コネクションを確立、FTP クライアントから FTP コマンドを受信し、それをサーバに転送する。FTP サーバからの応答も同様にして、クライアントに転送される。
（3）データコネクション生成に関連した FTP コマンド（PORT コマンド）及び応答（PASV コマンドに対する応答）を受信した場合、プロトコル解析部によって解析され、データコネクション管理部に伝達される。
（4）データコネクション管理部はそれを基に、データコネクション確立を行う。
（5）確立されたデータコネクション間でデータの中継を行うことでファイル転送が中継される。

6. 考察

FTP プロキシを実装した結果、要件とした点について下記の結果を得た。

6.1. 透過性

（1）コマンド・応答
基本的なコマンド及び応答は受信後、データコネクションに関わるもの以外はそのまま送信することで透過性を確保できた。ファイル転送を中止する際の TELNET オプションによる割り込みも TCP 帯域外データを転送することで通信相手に転送中止を伝達することを可能とした。
（2）データコネクション
データコネクション確立に関連した PORT コマンド及び PASV コマンドに対する応答には、IP アドレスと TCP ポート番号が含まれる。このためプロトコル解析部でそれらの値の変換を行うとともに、データコネクション確立を行うことで透過性を確保した（図４）。
（3）コネクション切断
正常切断、異常切断については相手からの切断理由を判定し、正常切断では TCP FIN、異常切断では TCP RST を送信することした。通信相手がダウンしている際のタイムアウトについては、他方の通信相手とコネクションが確立されている場合にはタイムアウトを発生させることが不可能なため、そのコネクションに TCP RST を送信し異常切断とすることによりエラーの伝達を可能とした（図５）。

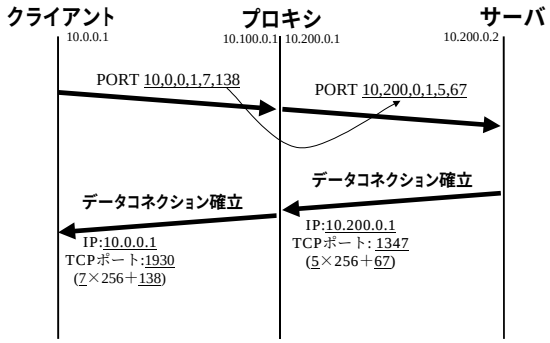


図4 プロキシによるPORTコマンドの置換

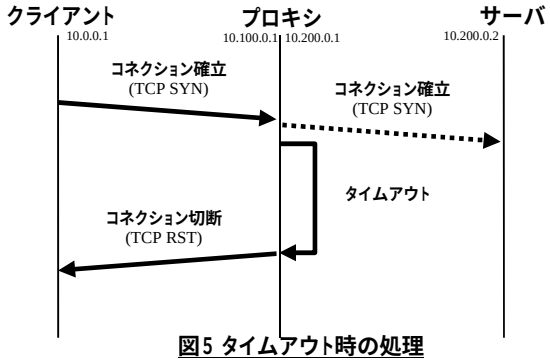
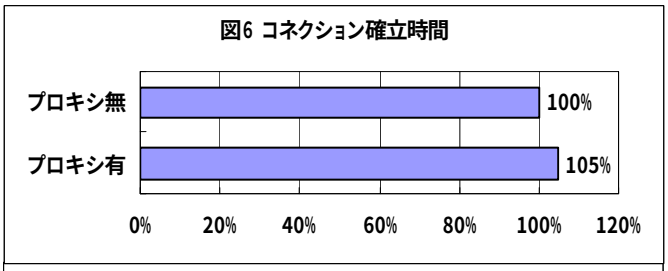
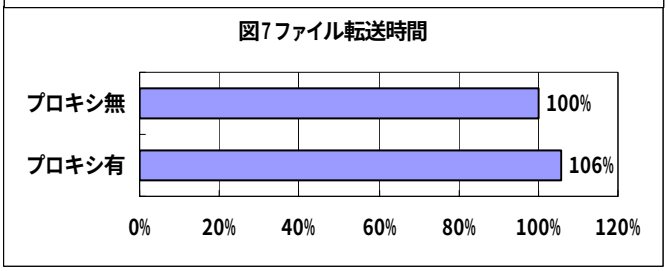


図5 タイムアウト時の処理

6.2. 性能

FTP プロキシのコネクション確立時間とファイル転送時間を図６、７に示す。（Pentium III 866MHz PC 及び 100M bits/s LAN 上を用いて測定）





両者ともプロキシ無しの場合の 5%程度の劣化となり、実用上問題ないと判断した。

7. 結論

今回開発した FTP プロキシを用いることにより、システム移行を円滑に進める方法を確立した。今後、他プロトコルで構成されたシステムについても応用を図っていく。

参考文献

[1] Postel, Jon, and Joyce Reynolds, "FILE TRANSFER PROTOCOL", RFC 959, DARPA, October 1985.