

安全なシステム移行のためのシステム試験方法

秦野 克彦† 住野 寛† 保坂 奈緒美† 佐藤 雅之††
 †三菱電機情報ネットワーク株式会社 インターネットシステム部
 ††三菱電機株式会社 情報技術総合研究所

1. はじめに

従来のソフトウェア工学のシステム試験では要求通りのものが開発されたかどうかが焦点であり、開発された新システムが既存システムから移行できるかどうか、移行のためのシステム試験はどのようなものであるべきかについてはあまり触れられていない。システム移行に関する検討項目には少なくとも次の3点がある。

- (1) システムが持つ機能の継続性
 新システムで既存サービスと同じことが提供されていると保証できれば、まず、最低限、移行可能な状態だとみなすことができる。
- (2) ユーザ情報の継続性
 既存システムを利用している全てのユーザに新システムを利用できることを保証できれば、新システムになっても旧システムに残っているデータを引き取る手段を用意することにより新システムに移行可能である。
- (3) 全ユーザに対する利用継続性
 既存システム中にあるユーザデータ等の動的なデータを新システムでも利用できることを保証できれば、ユーザ側に何も変更を与えずに(意識させずに)新システムに移行可能である。

本発表ではこれらを踏まえて、弊社で運用している EDI システムの移行とそのためシステム試験の取り組みについて述べる。

2. 新システムへの安全な移行方法に関する検討

2.1 MIND-EDI システムの移行

MIND-EDI システムは EDI(Electronic Data Interchange) システムの一種である。EDI システムとは、商取引の手順においてやり取りされる取引情報を、電子的に交換することを目的とした情報システムである。例えば、企業間で物品を購入する等の商取引の際には、購入物品に対して見積、発注、受注、出荷、納品、検収といった手順を経る。EDI システムは、各々の手順に対応する取引情報のある定められた形式で受信し、必要があれば取引相手毎に仕分け配信する。MIND-EDI システムでは、受信や配信は CII 形式や CSV 形式で行われおり、公衆網、ISDN 網、専用線、イ

ンターネット網を通じて、全銀 BSC 手順、全銀 TCP/IP 手順、FTP、HTTPS といった通信プロトコルで取引情報を交換している。また、取引情報を FAX に出力する形で配信することができる。

MIND-EDI システムはこうした取引情報交換サービスを、中心となる汎用機および複数の Unix サーバで提供している。システム移行の方針は、システムを中心機能である仕分機能を汎用機から Unix サーバにダウンサイジングすることである。システム移行の前後におけるシステム構成を図 1 に示す。

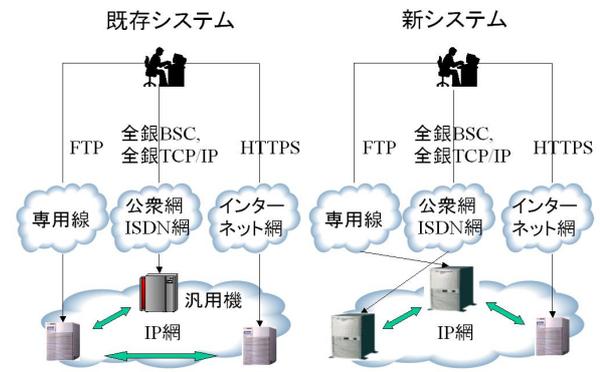


図 1 MIND-EDI システム システム移行前後のシステム構成

2.2 システムが持つ機能の継続性

本システムの基本機能は受信した取引情報データを宛先相手に配信することである。この場合、異なる宛先相手に配信(誤配信)したり、同じものを配信(二重配信)したりしてはならない。この機能の継続性を示すためには、既存システムも移行後の新システムも A 発 B 宛のデータを受信したら必ず B 宛に配信され誤配信や二重配信がない、という条件を満たす必要がある。ここでは、ブラックボックス型の試験として伝送経路を網羅するユーザデータ伝送試験を検討した。

2.3 ユーザ情報の継続性

既存システムには静的なデータとしてのユーザ情報が、全銀手順で通信するユーザは汎用機上のデータベースに、FTP で通信するユーザは EDI-FTP 用のデータベースに、HTTPS で通信するユーザはまた別のデータベースに存在する。一方で、新システムでは、ユーザ情報は Unix サーバ上の Oracle データベースに統合される。ユーザ情報の継続性を示すためには、既存システムのユーザ情報が漏れなく新システム上に適切に存在する必要がある。ここでは、異なるデータベースから統合されたユーザ情報を生成しなければならないことを考慮して、次の 2 種類の試験方法を検討した。

- (1) ユーザ情報のデータ整合性検査
- (2) 実ユーザデータを利用したユーザ存否検査

An Approach of System Test for System Migration
 Katsuhiko HATANO†, Hiroshi SUMINO†, Naomi HOSAKA†, and Masayuki SATO††
 †Mitsubishi Electric Information Network Corporation IS Dept.
 ††Information Technology R & D Center, Mitsubishi Electric Corporation
 E-mail: hatano.katsuhiko@mind.co.jp

2.4 全ユーザに対する利用継続性

既存システムには動的なデータとして、受信して配信待ちのユーザデータと、課金データおよび処理履歴としてのログが存在する。一方で、新システムには、こうしたデータは全くない。全ユーザに対する利用継続性を示すには、これらのデータが新システムに漏れなく存在する必要がある。ここでは、次の2点について検討した。

- (1) ユーザデータの計数
- (2) 二重課金の検査

3. システム試験の実施

3.1 MIND-EDI システムの移行過程とシステム試験

通常、システムの移行過程では、はじめに既存システムがあり、まず、既存システムに新システム用の新たな要素が加わった試験システムとなる。次に、試験システムは目的の新システムから切り戻し可能な切替システムとなる。最後に、切り戻しを実施しない切り替えによって試験システムは新システムとなり移行が完了する。切替システムが新システムに近ければ近いほど、移行後に発現する初期運用上の問題を少なくすることができる。我々は、試験システムと切替システムで各々次の試験を実施した。

試験システム: 実ユーザデータを利用した運用試験の実施

- (1) ユーザ情報のデータ整合性検査
- (2) 実ユーザデータを利用したユーザ存否検査

切替システム: 新システムへの移行試験の実施

- (1) 伝送経路を網羅するユーザデータ伝送試験
- (2) ユーザデータの計数

なお、二重課金の検査については、新システム用のソフトウェアにユーザデータ処理時の課金処理実行有無を選択する機能があったため、実施する必要がなかった。

3.2 実ユーザデータを利用した運用試験

ユーザ情報の継続性を確認するために、試験システムでは、既存システムが受信した実ユーザデータを受信した時、全く同じ結果が得られることを確認する運用試験を実施した。実ユーザデータは3ヶ月分を用いた。試験システムと新システムとの違いは、実ユーザからデータを受信できず配信もできないことである。これは試験中に誤って実ユーザに取引情報データを配信しないようにするためである。

- (1) ユーザ情報のデータ整合性検査

形態の異なる3つのデータベースから生成されたユーザ情報は、新たなデータベーススキーマに基いて統合された。一部のユーザでユーザ情報に不整合を生じる結果となった。

- (2) 実ユーザデータを利用したユーザ存否検査

実ユーザデータを新システムが受信したところ、新システムでは不正データとみなされる場合のあるデータを送っているユーザが存在することがわかった。

これらにより、ユーザ情報の不整合や、不正とみなされるユーザデータの存在がわかり、問題になる移行前に対処することができた。

3.3 新システムへの移行試験

システムが持つ機能の継続性と全ユーザに対する利用継続性を確認するために切替システムでは限られた時間内で切り戻し可能な範囲で限定的な試験を実施した。切替システムと新システムとの違いは、切替システムは試験用ユーザからのみユーザデータを受信し配信できることである。

- (1) 伝送経路を網羅するユーザデータ伝送試験

既存システムでは、擬似ユーザ同士で定期的にデータ伝送するシステム監視機構を導入している¹⁾。本試験では物理的な伝送経路(数十パターン)を網羅するように擬似ユーザと試験データを準備した。本試験の実施により、切り戻しを明確に判定できた、また、切り戻した後も元に戻ったことを同様に判定できる点が有効だった。

- (2) ユーザデータの計数

MIND-EDI システムは日曜日がメンテナンス日でシステムが停止する。そのため、移行試験としては切替は日曜1日以内で切り戻すことが可能でなければならない。そのために、ユーザデータの計数は人手を介さず短時間で終了させるために計数プログラムを準備した。

4. おわりに

本稿では、最初に既存システムを安全に新システムに移行するための検討項目を示した。次にMIND-EDI システムの移行に対して、移行のための検討項目を踏まえたシステム試験方法を検討した。

MIND-EDI システムの移行では、まず、3ヶ月間分の実ユーザデータを試験システム上で処理した。すると、ユーザ情報の不整合や、不正とみなされるユーザデータの存在がわかり、問題になる移行の前に対処することができた。

また、切り戻し可能な移行試験として、伝送経路を網羅するユーザデータ伝送試験を実施した。この方法は切り戻しの要否を明確に判定できるだけでなく、切り戻し後の正常動作判定としても有効であった。また、既存システム中の動的なデータが移行できたかどうかに関して、ユーザデータの計数プログラムを作成し限られた時間内に移行試験を終えることができた。

最後に、ユーザに新システムへ移行したことを意識させないことが今回の移行方針であった。しかしながら、多様化するサービスへの対応を重ねてシステムが複雑化しており、システム試験は非常に難航した。システム規模がある程度大きくなると、別にそれにふさわしい移行アプローチがあるのかもしれない。例えば、FTP のユーザはHTTPS で通信してもらおうといったように、逆にユーザに積極的に働きかける移行のアプローチでどのような違いが出るか取りこんでみたい。

参考文献

- [1] 佐藤 雅之ほか: "End-to-End 監視によるアプリケーション監視システム", 情処全大 (2005-3)