

## トランザクション概念の拡張による業務継続性の検討

原嶋 秀次† 正岡 良規††

† 株式会社 東芝 ソフトウェア技術センター 〒212-8582 川崎市幸区小向東芝町 1

†† 株式会社 東芝 SI技術開発センター 〒183-8512 東京都府中市片町 3- 22

E-mail †shuji.harashima@toshiba.co.jp ††yoshinori.masaoka@toshiba.co.jp

あらまし ドキュメントの共有やメールなど情報システムは組織の活動インフラであり、機能停止は大きな影響を及ぼす。本稿では、トランザクション概念を拡張した業務トランザクションを導入し、業務継続性への利用について述べる。これにより、システム機能の継続のみでなく、代替工場での生産などといった現実世界の状況に応じた業務の復旧が容易となる。

キーワード 業務継続性 トランザクション

## Extending a concept of transactions for business continuities

Shuji HARASHIMA† and Yoshinori MASAOKA††

†Software Engineering Center, Toshiba Corporation

1 Komukaitoshiba-cho, Saiwai-ku, Kawasaki-shi, Kanagawa, 212-8582 Japan

††Systems Integration Technology Center, Toshiba Corporation

3-22 Katamachi, Fuchu-shi, Tokyo, 183-8512 Japan

E-mail: †shuji.harashima@toshiba.co.jp ††yoshinori.masaoka@toshiba.co.jp

**Abstract** Information systems play the important role in many organizations, supporting their activities. We extended a concept of transactions to support business continuities of organizations. By using this concept, we can restart business activities easily.

**Keywords** business continuity, transaction

### 1. はじめに

企業をはじめとする様々な組織において、情報システムはその活動インフラであり、機能停止は組織の活動に直接的な影響を及ぼす。従って、システムのリスク対策は、組織運営上の重要な課題となっている。本稿では、物理的破壊への対策の1つとして、トランザクション概念の拡張による業務継続性の実現

について述べる。

業務継続性実現のためのシステム対策としては、広域クラスターやSAN(Storage Area Network)によるデータの広域リPLICATIONなどがおこなわれているが[1]、これらはシステムの機能を継続させるための技術であり、実際の業務継続を直接的にサポートするものではない。

業務トランザクションは、実際の状況に応じた業務の再開処理を容易とするための概念であり、災害発生後の復旧が現実的に即した形で実行できる。本稿の構成は次の通り。2章は業務継続性の概要を述べる。3章で業務トランザクションについて述べ、4章でその業務継続性への応用を述べる。5章は、業務継続性実現に関する関連動向、6章はまとめと今後の課題である。

## 2. 情報システムのリスクと業務継続性

### 2.1.業務継続性

システムのリスクには、サイバー攻撃、システム障害や物理的破壊（物理的リスク）、運用に伴うリスク（運用リスク）が考えられる。我々は、これらに対するシステムの総合的なリスク対策について、検討をおこなっている[2]。本稿では、このうち物理的リスクの対策について、業務継続性という観点での検討をおこなう

業務継続性とは、災害などが発生した際に、ある組織の業務を継続できることを言う。

『IT に関する非常時対策を採っていない企業が、壊滅的な被害を受けた場合、5年以内に40%の確率で倒産する。』というレポート[3]も存在するほど、その対策は重要である。官公庁においても、公的インフラとしてその影響は大きく対策が検討されている。

### 2.2.現状の対策技術と課題

図 2-1 に情報システムのリスクとISO17799[4]で定められた対策を示す。対策においては、システムの対策のみならず、組織としての総合的な対策が必要であることがわかる。システム対策へのブレークダウンとしては、Share による業務継続性の対策レベルなどがある[5]。データバックアップの有無、遠隔地への保管、システムの多重化などによりレベル分けされる。具体的な指標としては、リカバリーポイント目標(RPO: Recovery Point Objective)、リカバリータイム目標(RTO: Recovery Time Objective)などが用いられ、構築・運用時のコストなどを考慮した上で最適のレベルを選択することになる。

これらはいずれもシステムのデータを保護し、その機能の継続を目的としたものである。しかし、代替工場での生産再開といったケースを想定すると、たとえもとの工場で生産済みの製品があっても、製品が被害を受けていれば再生産が必要であり、単にシステムが復旧するだけではなく、現実世界の状況を踏まえた再開が必要である。これは必ずしも物理的な被害を受けた場合のみでなく、現実世界の業務の不都合にも応用が可能であり、業務の確実性をあげるのに有効である。

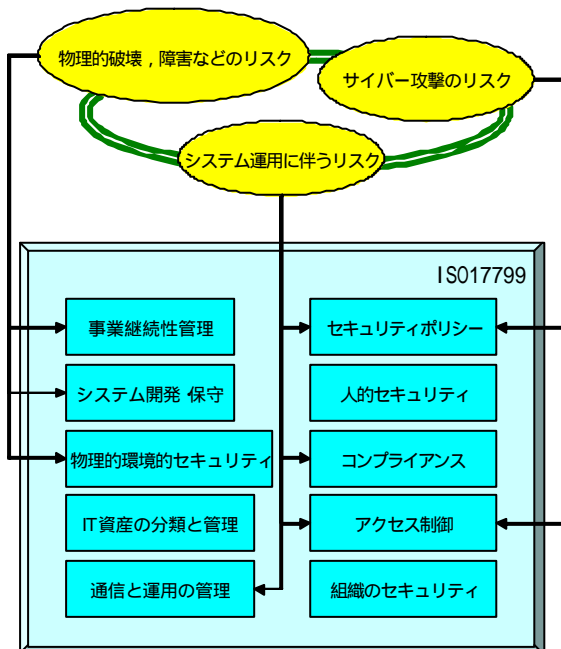


図 2-1 情報システムのリスクと対策

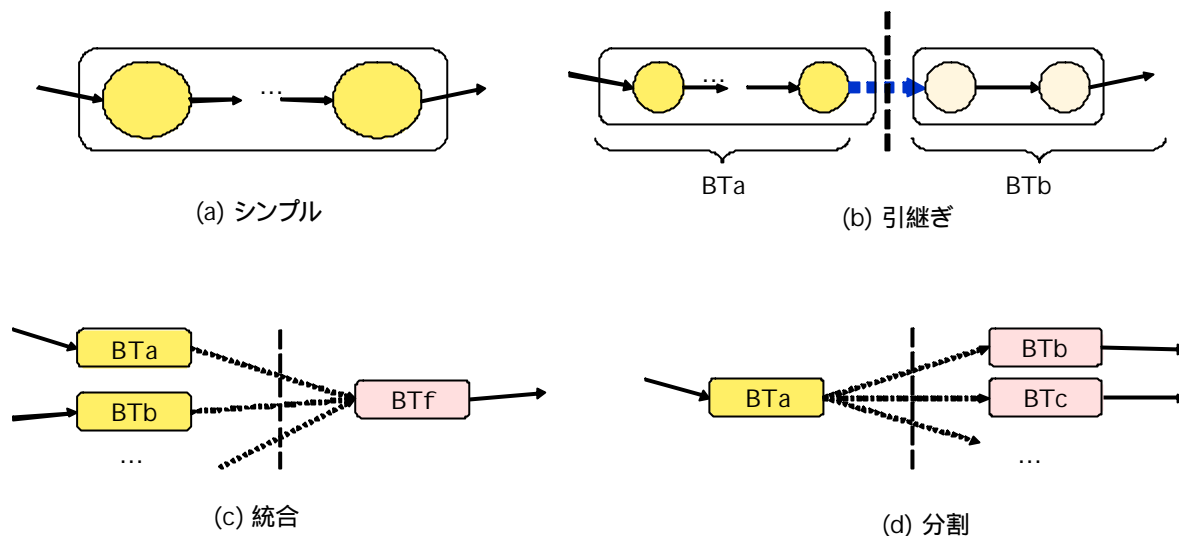


図 3-1 業務トランザクションの基本パターン

### 3. 業務トランザクション

#### 3.1. 業務トランザクションとは

業務とは、たとえば注文を受けてから在庫確認、出庫指示、配送指示、代金回収までを含む一連の流れを指す。システムで処理されるのは、ワークフローのようにこの一連の流れの場合もあるし、受注処理や在庫確認などの個別の処理の場合もある。

業務トランザクションはシステム上の処理のみでなく、人間による処理も含んだ概念である。たとえば、出庫指示は単に指示伝票の印刷処理だけではなく、人間による商品の出庫も管理対象とする。すなわち、業務トランザクションの状態は業務の状態そのものである。業務トランザクションの考え方はワークフローと同様であるが、処理のアポートや4章で述べる状態に応じた復旧などを考慮する。

業務トランザクションの基本的パターンを図3-1に示す。シンプルな業務トランザクション(a)は、複数の処理(ステップ)で構成されたものである。ステップには現実世界の業務を伴うものも含まれる。また、ステップの並行

実行や条件分岐、後戻りなども想定される。引継ぎ(b)は、ある業務トランザクションの結果を他の業務トランザクションが引継ぐものである。受注とそれに関連する月次の請求業務との関係が引継ぎに相当する。統合(c)および分割(d)は複数の業務トランザクションの間での引継ぎである。

#### 3.2. 業務トランザクションの検討

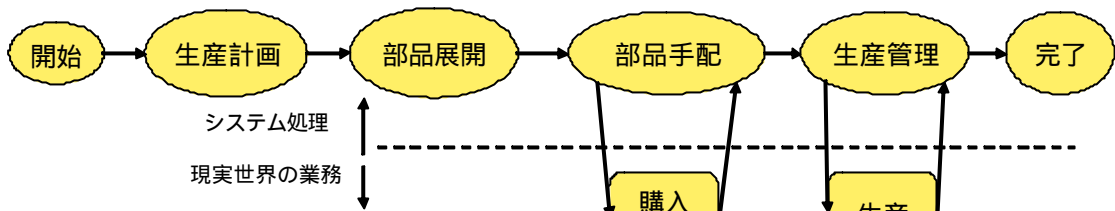
ここでは、業務トランザクションについて、具体例により特徴を考察する。

##### a. 製造

生産計画 - 部品展開 - 調達 - 製造という一般的な製造の流れを想定する(図3-2)。部品手配や製造といった現実の処理も管理対象となる。製造トランザクションの目的は、生産状況の把握であり、特徴は次の通り

- 現実世界の処理を含めた、全体の状態管理が必要
- 複数の製造トランザクションにより共有されるステップがあり得る(共通部品のロット生産など)
- 実行状況を0/1ではなく、進捗(%)で

製造 1



製造 2

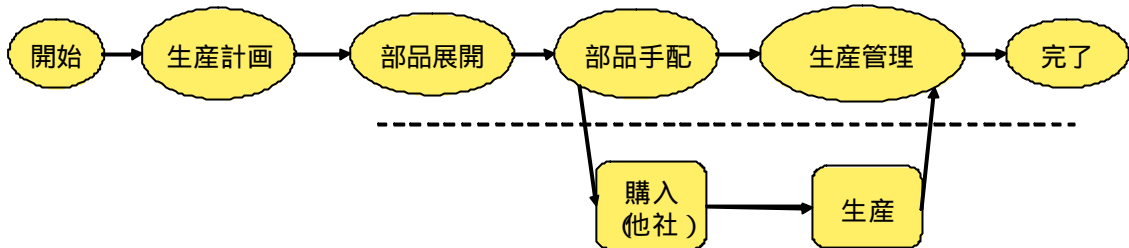


図 3-2 製造における業務トランザクションの例

管理する必要がある

また、復旧に関してはつぎの特徴がある。

- 別の生産拠点での再開などでは、終了済みステップの再実行が必要な場合がある
- 障害前の処理のキャンセル・破棄が必要となることがある。(障害発生前の見積もり回答など)

b.販売

見積もり、受注、請求の3つのトランザクションで構成される(図 3-3)。販売状況の把握が目的である。特徴は次の通り

- 見積もり 受注 請求への引継ぎあり(多対1もあり)

復旧に関しては次の特徴がある。

- 見積もり:終了後に障害が発生した場合、内容(納期、価格など)変更する必要がある
- 請求:基本的にやり直しはない(あるとすれば領収書の再送ぐらい)

c.オンライン販売

航空券のチケットレス販売を想定する。予約-支払い-チェックインのフローを管理する。特徴は次の通り

- フローの一部が顧客自身にある(予約 支払いなど)
- 顧客側の予約 決済 チェックインなどの処理順序はシステム側でチェックする必要がある
- さらに、処理期限がある(予約便が発発するまで)

復旧に関しては、システムが復旧すればよく、現実世界の業務(顧客側の処理状況)は考える必要がない(瞬間的な処理のみである)。

### 3.3. 業務トランザクション管理の枠組み

上述の議論をもとに、業務トランザクションの管理の枠組みを述べる。

a.基本機能

- 構成(フロー)の定義
- 要求の受付、インスタンスの管理(起動、実行状態管理、完了)

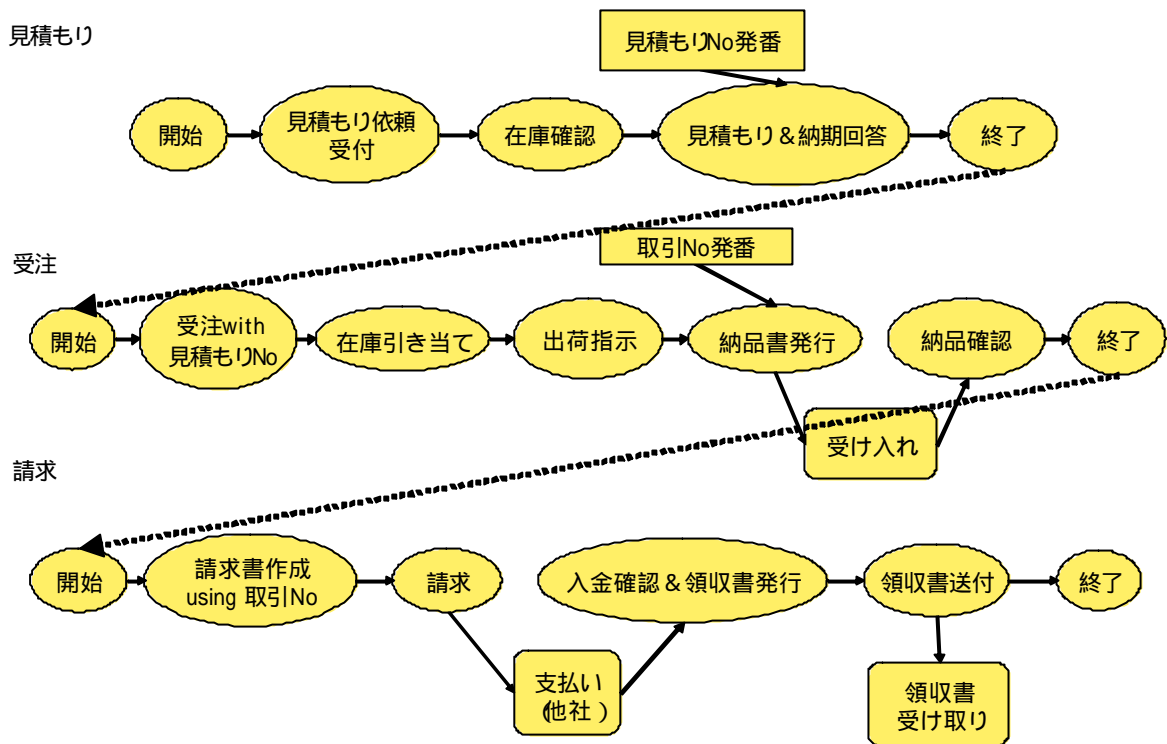


図 3-3 販売における業務トランザクションの例

- 現実の業務の処理状況の検出
- 進捗管理機能 (0/1 ではなく, %による管理)
- 引継ぎ, 分割, 統合の状態管理機能 (IDの引継ぎなどを含む)
- 引継ぐトランザクションの外部からの起動
- 引継ぎの有効期間の設定

業務トランザクションの管理概要を図 3-4 に示す。

## 4 業務トランザクションを用いた業務継続性対策

### 4.1. 方式概要

図4-1 に業務トランザクションを利用した障害復旧の概要を示す。これを可能とするためには,

- 実行完了後の管理情報保持
- キャンセル

- 障害発生後のフロー変更などの機能が必要となる。

管理情報をSAN などにより代替候補の工場にリプリケーションしておく。災害発生後には, 状況を確認しながらそれぞれの業務トランザクションを再開する。本方式は, 広域クラスターによる瞬時の引継ぎなどを目的としたものではなく, 代替工場で生産する際の部品の調達先の変更や生産工程の変更など, 人間による状況の把握と判断が入る業務の再開支援が目的であり, 現実的にもっとも必要とされる手段であると思われる。業務トランザクションにより, “業務の状態”を簡単に把握でき, 再開が容易となる。

### 4.2. 有効性の考察

リスク対策は個々のケースに応じた評価が必要であり, 一般的な検討は困難であるが, 本方式の特性を知るとい意味で, DEA(Data Envelopment

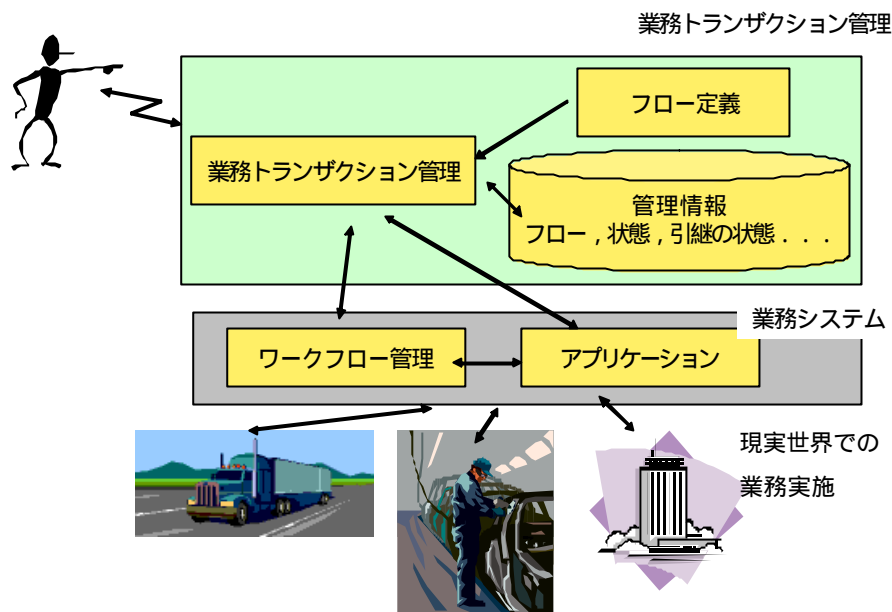


図 3-4 業務トランザクションの管理概要

Analysis)[10]による効率性比較をおこなった。入力として、構築コスト、運用コストを、出力としてRPO、RTOの逆数を利用した(いずれも概算による想定値。また、RTOは、システムの復旧時間ではなく、実際の業務が再開されるまでの想定時間)。結果を図4-2に示す。RTOの短縮効果が10%程度と仮定して、業務トランザクション導入に伴うコスト増加が10%程度であればこれまでの方式より効率的である。RTOの短縮効果が大きければ、より大きいケースでは40%以上のコスト増加でも効率性が失われないことがわかる。本方式は効率性に優れていることがわかる。

## 5. 関連研究

業務トランザクションに関連した研究としては、トランザクション、ワークフロー、

WebServicesにおけるトランザクションなどがある。

トランザクションの研究は[6]などにまとめられている。既に述べたように、これらはシステム処理を対象としたもので、現実世界の業務の状況の把握は考慮されていない。

ワークフローは、本報告の研究に近い技術である。特に企業間連携を想定したインターワークフロー[7][8]は、業務全体の管理という点ではほぼ同様の問題意識をもった技術である。我々の研究は、これに再開時に状況や環境を意識する機能を付け加えたものであるといえる。また、今後はトランザクション間の競合制御などを検討する予定である。

WebServicesのトランザクション[9]は、インターワークフローとほぼ同様の問題意識である。プロトコルレベルでの規格化の動きもあり、本研究においても対応を検討する予定である。

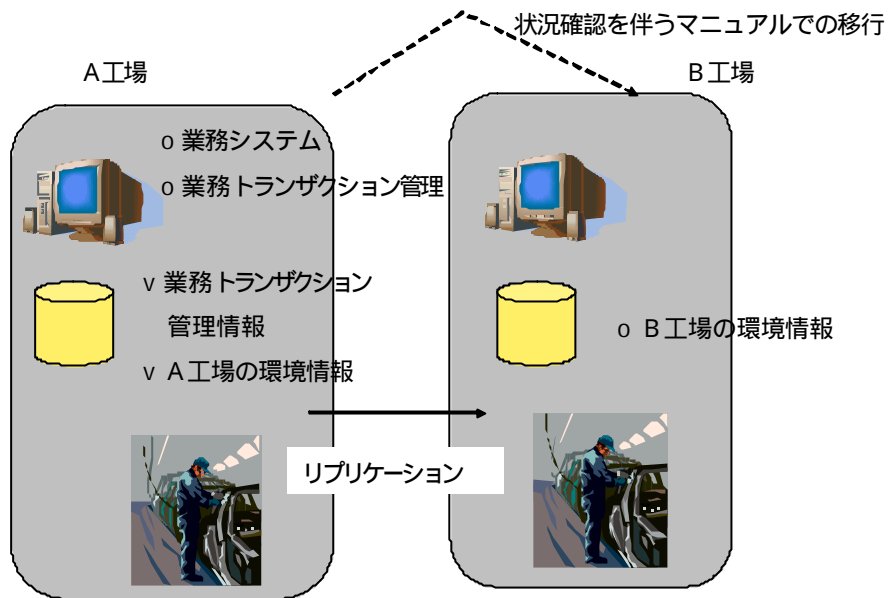


図 4-1 業務トランザクションによる復旧

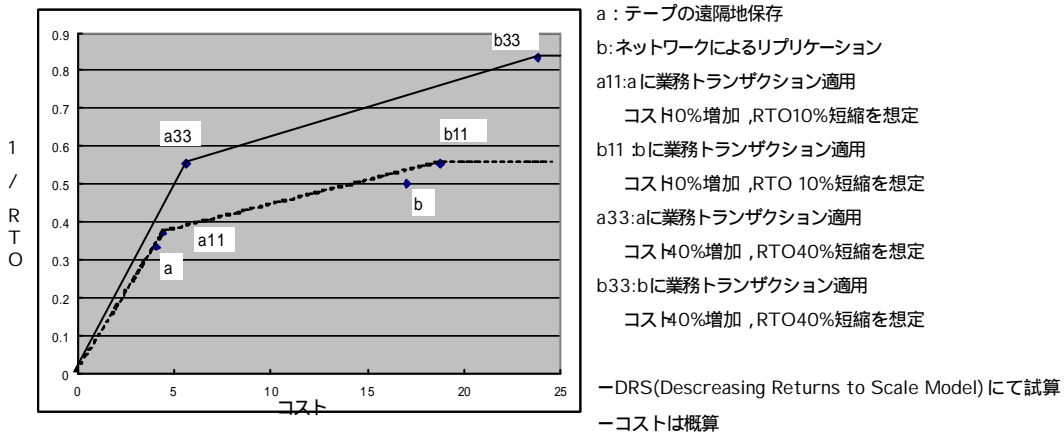


図 4-2 DEA による効率性比較 (試算)

## 6. まとめと今後の課題

本報告では、業務トランザクションの概念を導入し、業務継続性への適用方法を述べた。これにより、現実世界の状況に応じた業務の再開が可能となる。

今後、業務トランザクションのより現実的な例について検討し、モデルの実用性を高めるとともに、システム上での実現方式についてより具体的検討をおこない、業務トランザク

ションの利用方法を確立したい。

## 参考文献

- [1] 喜連川編著, ストレージネットワークング, オーム社, 2002.7.
- [2] 駒津他, “ビジネス コンティニューイティ技術”, 東芝レビュー vol.57, No.12, 2003.1. <http://www.toshiba.co.jp/tech/review/index.html>よりリンクあり

- [3] 栗原, “第 14 回今こそ日本企業も不測事態における業務計画を!”, Gartner Column, <http://www.zdnet.co.jp/enterprise/0109/17/01091788.html>
- [4] 中尾他, JIS X 5080:2002 情報セキュリティマネジメントガイド, 日本規格協会, 2002.12..
- [5] “Business SURVIVAL”, 日本 IBM, <http://www-6.ibm.com/jp/storage/solution/survival/2.html>
- [6] ジムグレイほか著, 喜連川監訳, トランザクション処理 概念と技法 (上・下), 日経BP社, 2001.10.
- [7] Mehmet Sayal et.al., “Integrating Workflow Management Systems with Business-to-Business Interaction Standards”, IEEE 18<sup>th</sup> International conference on Data Engineering(ICDE2002). San Jose California, U.S.A. 2002.3.
- [8] David Hollingsworth “Workflow Management Coalition The Workflow Reference Model”, The Workflow Management Coalition Specification, <http://www.wfmc.org/standards/standards.htm>, 1995.1.
- [9] “Business Transaction Protocol”, OASIS BTP Committee Specification1.0.3, June 2002. <http://www.oasis-open.org/home/index.php>よりリンクあり
- [10] 刀根, 経営効率性の測定と改善, 日科技連, 2001.2.