2D-1

電子商取引システム適用に向けた構成制御技術の開発

松浦　陽平†　　飯塚　剛†
吉川　幸司†　　西岡　篤史†　　北川　哲也†
三菱電機株式会社†

1. はじめに

インターネットを使用した電子商取引システムは一定の地位を確立し、現在では、二酸化炭素などのガス排出権取引までもがオンラインで行われつつある。このような取引は、BtoB、BtoC といった枠を超えた生活基盤に関わる取引であり、システムの高いサービス継続性が求められている。

また、昨年 10 月に公表された経済産業省「情報セキュリティ総合戦略」[1]の中でも、サービス継続に関するガイドライン整備や、被害軽減手段の検討が事故対応策の戦略の一つとしてあげられており、以下に示す技術が改めて注目されている。

・ 障害が発生してもサービスを提供可能な、耐障害システム構築技術
・ 障害情報を迅速に管理者に通知するための、システム障害検出技術

本稿では、電子商取引システムにおける上記技術開発について説明する。

2. システム要求

2.1. システム概要

一般的な電子商取引システムを図 1 に示す。システムは複数の参加者がインターネットからアクセスするウェブベースのシステムであり、以下の層から構成される。

・ セキュリティ層
ファイアウォールによるパケットフィルタリング、ユーザ認証サーバによるクライアント認証を行なう。
・ プレゼンテーション層
クライアントからのリクエスト処理、および画面生成を行なう。
・ アプリケーション層
クライアントからのリクエスト処理に応じた取引業務処理を行なう。

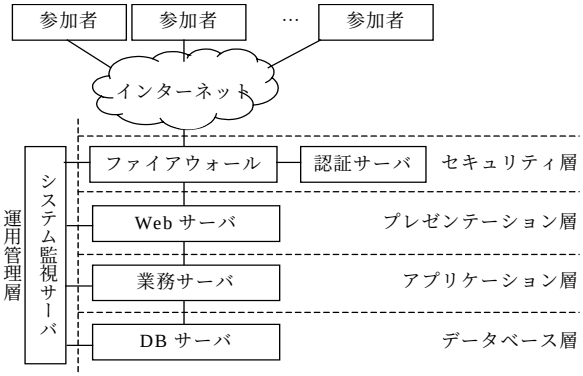

図 1 システム構成例

・ データベース層
取引商品、および履歴等の情報を保存する。
・ 運用管理層
システム内で発生する障害イベント、性能監視、セキュリティ監視を行なう。

2.2. システム要求

それぞれの層におけるシステム要求について述べる。

・ セキュリティ層、プレゼンテーション層
全てのユーザは、セキュリティ層を経由しプレゼンテーション層に接続するため、セキュリティ層には高い信頼性が求められる。また、プレゼンテーション層の障害は、システム外からはサービスの停止とみなされるため、セキュリティ層同様、高いサービス継続性が求められる。(停止時間：0 秒～10 秒)
・ アプリケーション層
全てのユーザがアプリケーション層に接続する訳ではないが、業務処理の中核となる層であり、取引情報の欠損防止対策が求められる。(停止時間：～60 秒)
・ データベース層
アプリケーション層同様、全てのユーザがデータベース層に接続する訳ではないが、取引結果の欠損防止対策が求められる。(停止時間：～300 秒)
・ 運用管理層
運用管理層の障害によるサービス停止は無いため、他の層と比較して高いサービス継続性は求められない。

Development of System Management Technologies for Online Trading System
†Yohei MATSUURA, †Tsuyoshi IIZUKA,
†Koji Kikkawa, †Atsushi NISHIOKA, †Tetsuya KITAGAWA
†Mitsubishi Electric Corporation

3. 課題

3.1. 耐障害システム構築

前述の要求を踏まえ、実現可能な技術をマッピングする必要があるが、そのために可用性とデータ復旧目標を確認し、最適なシステム構成を検討する必要がある。データ復旧目標とは、データをいつの時点まで復旧させる必要があるかを示す指標である。図 2 に各層との可用性/データ復旧目標との関係を示す。

3.2. システム障害検出

障害検出は、汎用的な障害検出プロトコルを用いる方法やコンポーネント専用の API を用いる方法等様々なものがあるが、それぞれを制御可能な構成制御フレームワークの開発や、ポーリング間隔等の検出パラメータの妥当性を検討する必要がある。

4. 課題解決に向けた取り組み

4.1. システム構成の検討

一般的に、高信頼なシステム構成を実現するためには、以下の方式が利用される。

- ロードバランサ
  外部リクエストを負荷に応じて、複数のサーバに振り分ける方式である。可用性を向上させることが可能であるが、高コストであり、データの同期機構を別途考慮する必要がある。
- アクティブ/アクティブ型クラスタ
  複数のサーバを連携させ、一つの仮想的なサーバとして利用する方式である。それぞれのサーバ上でアプリケーションは起動されているが、実際にサービスするのはその中の一つである。
- アクティブ/スタンバイ型クラスタ
  アクティブ/アクティブ型クラスタと異なり、アプリケーションは同時に複数のサーバで起動しない。低コストな反面、可用性は低下する。

それぞれの方式をシステム要求に基づき、図 2 にマッピングし、各層への適用を検討した結果、表 1 を得た。

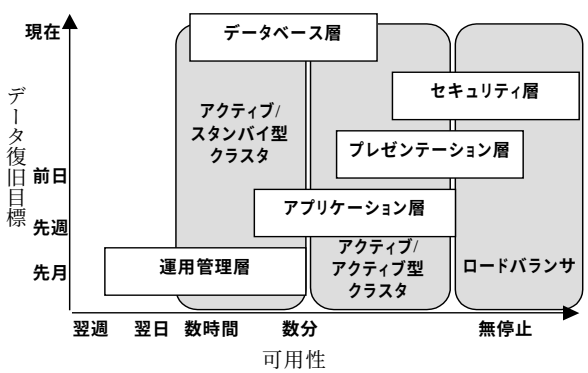

図 2 各層の位置づけ

表 1 各層の構成

各層	業務復旧方式
セキュリティ層	ロードバランサ
プレゼンテーション層	ロードバランサ
アプリケーション層	アクティブ/アクティブ型クラスタ
データベース層	アクティブ/スタンバイ型クラスタ
運用管理層	無し

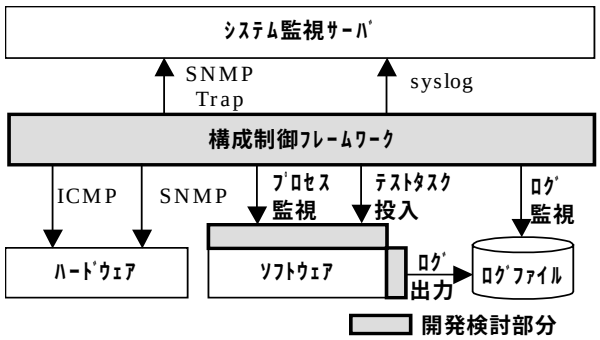

図 3 障害検出方法の検討

4.2. 構成制御フレームワークの開発

システムの障害検出として、今後のシステム拡張・展開を考慮し、汎用的な検出方法を組み合わせた構成制御フレームワークを開発、監視プラットホームを統一化する方法を検討した(図 3)。ハードウェア障害、およびソフトウェア障害それぞれについて、下記方法を用いた。

- ハードウェア障害
  ICMP(コンポーネントの生死確認)、および SNMP Trap（コンポーネント内の障害確認）を組み合わせた。
- ソフトウェア障害
  プロセス監視(アプリケーションの生死確認)、テストタスク投入(アプリケーションのサービス可否確認)、およびログ監視(アプリケーションの状態確認)を組み合わせた。

5. おわりに

本稿では、電子商取引システムにおける構成制御の要求・課題についてまとめ、システム構成の検討や構成制御フレームワークの開発といった、サービス継続性を高めるための対策について述べた。さらなるサービス継続性向上のためには、広域災害等を考慮したシステム間連携技術が必須であり、これらの技術は、今後広く適用されていくと考えられる。

今後は、市場動向をふまえながら、引き続き検討を実施していく。

参考文献

[1]経済産業省 商務情報政策局 情報セキュリティ政策室 : http://www.meti.go.jp/policy/netsecurity/strategy.htm