短時間でのインシデント処理を要するシステムの構築方式(2)
-障害対応手段の決定-

佐藤　雅之†　大塚　亮†

三菱電機株式会社　情報技術総合研究所†

1. はじめに

社会インフラを担うミッションクリティカルシステムは、インシデント発生により機能不全に陥ることは許されない。一方、インシデントの発生を完全に抑えることは不可能であり、インシデントが発生しても短時間で復旧するシステムが求められている。本課題を解決するため、インシデントの発生を受けてから復旧に向けた対応手段を短時間で決定する構成管理拡張方式を考案した。本書では、構成管理拡張方式の概要と有効性の評価結果について報告する。

2. ミッションクリティカルシステム

ミッションクリティカルシステムとは、常に安定して稼動することが求められている、さまざまな社会インフラを担うシステム（金融システム、電力システムなど）である。

図 1 に検討対象となるシステムを示す。このシステムにおいては、次のように構成している。

- システム全体を冗長化する(システム A および、システム B)。
- サーバ、ネットワーク機器などは、個々に、３台以上により冗長化する。
- サーバ、ネットワーク機器など、計、数百台で構成し、監視装置により監視を行う。
- 監視によりインシデントを検出した場合、障害対応手段の判定を行う。

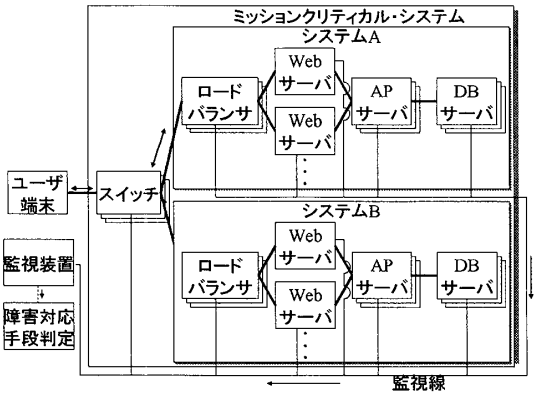

図1. 検討対象システム

A method of constructing system which is needed processing incident in short time.

Masayuki Sato, Ryo Otsuka

Information Technology R&D Center, Mitsubishi Electric Corporation.

3. 障害対応手段の判定に関する課題

ミッションクリティカルシステムは、インシデントの発生に対して、迅速に対応手段を決定し、復旧を図る必要がある。また、構成変更があったとしても、障害対応手段の設定が容易であることも重要である。

本書では図１のようなシステムの構築にあたって、次の条件を課して検討を行った。

- 各サーバや機器において障害が発生した場合に、１分で障害対応手段を決定
- 構成変更への対応が容易

4. 障害対応手段の判定方式

障害対策手段の判定方式は、図２のような方式がある。

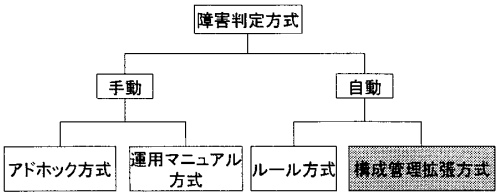

図 2. 障害対応手段判定方式の分類

- アドホック方式…インシデントから、運用者が都度、障害手段の判定を行う。
- 運用マニュアル方式…インシデントから、運用者が運用マニュアルに沿って、障害対応手段を検索する。

しかし、これらの方式は、運用者のスキルに依存する部分があり、また運用マニュアルの検索時間にばらつきがあるなど、常に 1 分で障害対応手段を判定できる保証がない。

一方、障害対応手段を決定するまでの時間がある程度計算可能な方式として、ルール方式がある。

- ルール方式…あらかじめ作成しておいた if～then で記述した複数のルールに従って、検出されたインシデントから、自動的に障害判定を行う。

ルール方式は、ルールとして定められた条件の成否判定を行う方式あるため、高々、条件を全て判定するだけの時間しか必要としない。し

かし、作成されたルールがシステム全体で矛盾なく、同時に、一つのみ成立するようにルール全体を見直す必要があるため、メンテナンスは困難である。

5. 構成管理拡張方式

ミッションクリティカルシステムでは、構成アイテムの管理のため、名称、状態などを管理する CMDB[1](=Configuration Management Database。構成管理データベース)を用いることが多い。

構成管理拡張方式は、CMDB を拡張し、障害および障害対応手段を管理する拡張 CMDB を用いる。図３に拡張 CMDB のクラス構成の例を示す。

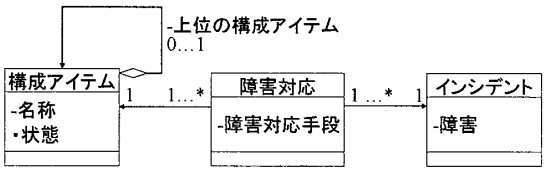

図 3. 拡張 CMDB のクラス構成の例

構成管理拡張方式は、ある構成アイテムに関して監視装置により、インシデントを検出された場合に、次を入力として、拡張 CMDB を検索し、上位の構成アイテムをたどり、障害に対応した障害対応手段を得る方式である。

- 構成アイテム
- 構成アイテムで発生した障害

なお、ここでいうインシデントとは、特に、ある構成アイテムにおいて、故障などの障害が発生し、システムの監視手段などにより検出されたイベントを指す。

構成管理拡張方式による障害対応手段の判定の例を示す。図１のシステムの構成アイテムが図４の構成であるとき、構成アイテム DISK-2 である障害が発生したことが検出されたが、DISK-1 が稼働していることにより、上位の構成アイテム RAID-1 においては、障害が発生していない状態を考える。この状態では、拡張 CMDB に記載される RAID-1 の障害対応手段に従う。例えば、DISK 交換作業のスケジューリングなどの障害対応手段を用いると、判定する。

6. 構成管理拡張方式の評価

構成管理拡張方式による障害対応方式の評価について示す。本方式の有効性について、設計の段階で求める必要があり、時間性能については、TPC-C[2](= Transaction Processing Performance Council Benchmark C)との比較により、概算の障害判定時間を求めた。

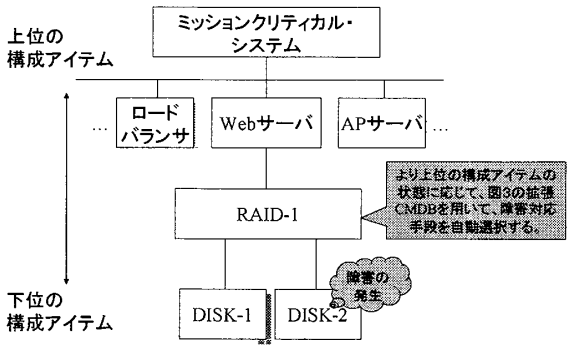

図 4. 構成管理拡張方式による障害対応手段の判定

TPC-C は、特定の H/W、DB を使用する条件で、1 分間で処理できる TPC-C トランザクションの処理数を示す。TPC-C トランザクションは、新規オーダの追加を行う内容であり、30,000 行からの select などを実施する。

本方式を適用したシステムにおける、障害判定トランザクションの内容を TPC-C トランザクションと比較すると、高々1000 行からの select であり、十分に小さい計算量であった。これにより、本システムにおいては、1 分で障害判定が可能であるといえる。

メンテナンス性については、図３のようにクラスを構成することで、特定の構成アイテムに対する障害対応手段などをメンテナスすることにより、全体の整合性が取れるため、ユーザが全体のルールの整合性を管理する必要のあるルール方式に比べ、メンテナンスが容易であるといえる。

7. おわりに

1 分間で障害対応手段を判定し、かつ、システムの構成変更に対して、容易に対応可能な障害対応手段判定方式を考案し、評価を行った。結果、本方式が有効であることが求められた。今後は、本方式を様々なシステムに適用し、検証を重ねる予定である。

[参考文献]

1. ITIL サービストランジション (It Infrastructure Library), Office of Government Commerce, The Stationery Office, 2008
2. TPC-C , Transaction Processing Performance Council , http://www.tpc.org/tpcc/