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(1) -障害検出・復旧方式-

大塚　亮†　　佐藤　雅之†

三菱電機株式会社　情報技術総合研究所†

1. はじめに

金融システムや電力システムなど、社会の重要なインフラを担うミッションクリティカル・システムが障害によりシステムダウンをした場合、ダウンしている時間が長くなればなるほど社会へ与える影響は大きくなる。しかし、どれほど高信頼なシステムを構築していたとしても、障害の発生を完全に抑えることは不可能である。そのため、ミッションクリティカル・システムには、障害発生から短時間で復旧できることが求められている。ところが、一般的なミッションクリティカル・システムでは、障害発生時のインシデント処理に長い時間を要することが多く、このことが大きな課題となっている。そこで、この課題を解決するための障害検出・復旧方式を考案した。本書ではこの方式の概要について報告する。

2. システム障害事例

表 1 に近年発生したミッションクリティカル・システムの障害事例を示す。この表から、ミッションクリティカル・システムが長時間システムダウンをすると、社会に多大な影響を及ぼすことが分かる。

表1. 過去の障害事例

年/月	障害事例	影響	復旧時間
2002/4	銀行の勘定系システムがトラブル	口座振替未処理約 250 万件。銀行の損害約 18 億円。	1 か月
2005/11	証券取引所の証券取引システムがダウン	全銘柄取引停止。	7 時間
2007/5	航空会社の搭乗システムがダウン	130 便が欠航、306 便に遅れ。	8 時間
2007/10	鉄道各社の自動改札システムがトラブル	660 駅の約 4400 台の改札機が使用不能。約 260 万人に影響。	5 時間

A method of constructing system which is needed processing incident in short time.
Ryo Otsuka, Masayuki Sato
Information Technology R&D Center, Mitsubishi Electric Corporation.

3. インシデント処理

図 1 にシステムに障害が発生した場合の一般的なインシデント処理の流れを示す。インシデント処理は障害が発生した後、障害検出、障害対応方法判定、障害対応方法実施、の 3 つのステップを経てシステムを復旧させる。

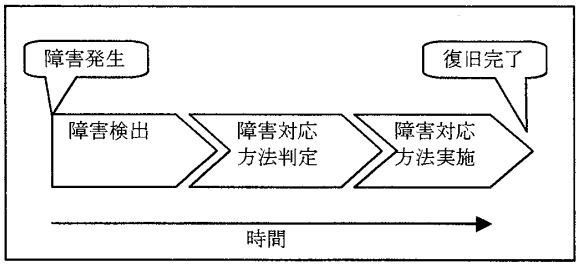

図1. 一般的なインシデント処理の手順

4. 検討システムの課題

検討対象のシステムは、100 台のサーバと 1000 台のネットワーク機器で構成されるミッションクリティカル・システムであり、システム A とシステム B に 2 重化され、さらに各機器についても 3 台以上に冗長化されている（図 2 参照）。このようなシステムにおいて、インシデント処理を 7 分[1]で完了させなければならない要件が課せられている。この課題についてインシデント処理のステップごとに検討する。

4.1. 障害検出

全ての機器に監視ツールが導入されておらず、監視ツールが導入されていない機器で障害が発生した場合、運用管理者が障害を確認するまでに長い時間を要するという課題がある。

4.2. 障害対応方法判定

システムに障害が発生した場合、一般的に運用マニュアルを用いて対応方法を判定しているが、この方式では判定に要する時間が一定しないという課題がある。

4.3. 障害対応方法実施

システムは障害の発生を抑止するように設計されてはいるが、復旧対策までは考慮されていない。もし障害が発生した場合は、対応方法が複雑になるため、復旧させるまでに長い時間を要するという課題がある。

4.4. ステップ間の連携

運用管理者は検出された障害情報を運用管理室の監視端末で確認し、表示された障害情報から運用マニュアルを用いて対応方法を判定し、現場の機器室等で処置を実施する。この方式では各ステップで異なる端末や媒体を用いており、インシデント処理に長い時間を要する原因となっている。

5. 考案した障害検出・復旧方式

図 2 にこれらの課題を解決するために考案した障害検出・復旧方式の概要を示す。以下にその詳細を述べる。

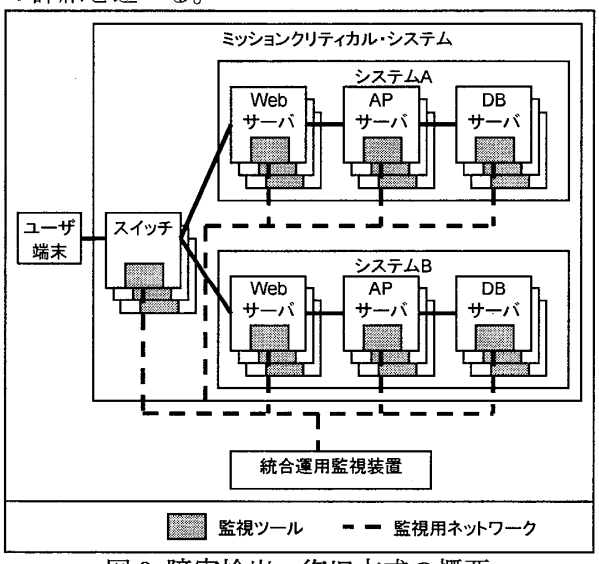

図 2. 障害検出・復旧方式の概要

5.1. 障害検出

システムを構成する全ての機器に監視ツールを導入し、さらに、後述の統合運用監視装置で異なるベンダーの監視ツールからの情報を統合的に監視する。この方式により、障害情報を一元的に管理でき、発生した障害を短時間で確認できる。

5.2. 障害対応方法判定

統合運用監視装置に、検出された障害情報を基に構成管理拡張方式[2, 注]により判定された障害対応方法を表示させる。この方式により、障害対応方法を短時間で取得できる。

[注]構成管理拡張方式とは、障害ケースと障害対応方法を管理する拡張した構成管理データベースにより障害対応方法を判定する方式

5.3. 障害対応方法実施

システムを構成する機器毎に想定される障害とその対応方法を策定し、この対応方法を統合運用監視装置から実施できるようにシステムを設計する。この方式により、簡単な操作で障害対応方法を実施できるシステムを構築でき、障害発生時には短時間で復旧することができる。

5.4. ステップ間の連携

各ステップを簡単な操作で実行できる統合運用監視装置を構築し、運用管理者はこれを用いてインシデント処理を行う。この方式により、各ステップ間をスムーズに実行でき、短時間でシステムを障害から復旧させることができる。

6. 障害検出・復旧方式の評価

図 2 のシステムに対して、考案した方式を適用した。以下にその評価について述べる。

6.1. 障害検出

監視ツールを導入し、2 分で 100 台のサーバと 1000 台のネットワーク機器を監視できた。

6.2. 障害対応方法判定

構成管理拡張方式によって 1 分で障害対応方法を判定できた。

6.3. 障害対応方法実施

システムを構成する機器毎に障害とその対応方法を策定し、システムを再構築した。例として、システム A で重大な障害が発生した場合は統合運用監視装置のスイッチを操作してシステム B へ系切替える。この方式により 2 分で障害対応方法を実施できた。

6.4. ステップ間の連携

統合運用監視装置を構築し、これにより、同一の端末で各ステップを実行でき、効率良くインシデント処理を行なえた。

以上より、考案したインシデント処理では、システムに障害が発生してから 7 分以内で復旧できることを確認した。

7. おわりに

システムで障害が発生してから短時間で復旧する障害検出・復旧方式を考案し、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. 朝日大学マーケティング研究所, 銀行窓口・ATM での待ち時間に関するマーケティングデータ～第 1 弾～, トピックスリサーチ, 2006
2. 佐藤雅之, 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-, 情報処理学会第 71 回全国大会, 2009