

ITシステムの障害からの復旧を迅速化する支援技術

Technologies for Rapid Recovery from Information Technology System Trouble

あらまし

ITシステムの障害の多くが既知の障害であると言われている。過去のITシステムの障害からの復旧プロセスを形式知化したものを再利用することで、障害からの復旧を迅速化する技術が望まれている。

本稿では、まず、現状のITシステムの障害対応プロセスの課題について述べる。そして、過去に起こったITシステムの障害の症状・対処を蓄積するシンプトンDBを使った、ITシステムの障害対応システムのアーキテクチャについて説明する。つぎに、シンプトンのデータ構造について述べる。さらに、シンプトンDBを使った障害対応ナビゲーション技術とその評価について触れ、最後に障害対応システムのロードマップについて述べる。

Abstract

Since certain problems in information technology (IT) systems reoccur many times, it is becoming necessary to utilize previously acquired knowledge in order to achieve rapid recovery from IT system trouble. This paper outlines a troubleshooting navigation technology that uses a symptom database. After explaining the problems with today's IT system troubleshooting processes, it describes the architecture of a troubleshooting system that has a symptom database storing symptom information and prescriptions acquired from past problems, along with the data structure. It then presents evaluation results that demonstrate the system's effectiveness. Finally, a roadmap for a troubleshooting system is shown.



松本安英 (まつもと やすひで)
クラウドコンピューティング研究センター 所属
現在、ITシステム運用基盤技術の研究開発に従事。

ま え が き

ITシステムは社会・経済活動を支えるインフラとして日常的に広く利用されている。ITシステムが、ひとたび障害を起こすと、単なるシステムトラブルの問題にとどまらず、社会・経済活動への影響は計り知れない。

近年、ITシステムのオープン化が進展してきており、ITシステムはより複雑化し、障害対応や性能劣化に対応するための運用コストが増大する傾向にある。また、オープン化が進展することで、複数の企業の製品を組み合わせたマルチベンダ構成が一般化し、障害の原因箇所を特定する方法がますます複雑化してくる状況にある。

このように複雑化するITシステムの障害に適切に対応するためには、ITシステムが起こす様々な障害に関する情報を構造化して蓄積し、後の障害発生時に再利用することで、迅速な対応を実現する方法が考えられる。

例えば、人間が病気になった場合、熱を出す、頭痛を訴えるなどの症状に関する情報と、薬を飲む、安静にするなどの処方に関する情報から、適切な対応を選択する。このような症状と処方に関する情報をITシステムの障害に当てはめて考えてみる。すなわち、人間の病気と同様の捉え方でITシステムの障害時の症状と処方に関するデータを構造化しデータベースとして蓄積し、障害発生時にこのデータを利用することで、障害復旧作業を迅速化できるのではないかと考えた。

本稿では、まず、現在のITシステムの障害対応の課題を整理し、ITシステムの障害対応のアーキテクチャについて述べる。

ITシステムの障害対応の課題

近年、品質の良いITサービスを提供するために、1980年代後半に英国の政府機関が作成したITサービスマネジメントのベストプラクティスの集大成であるITIL (IT Infrastructure Library)⁽¹⁾が採用されつつある。

ITILでは、障害対応策として二つの概念が導入されている。一つはインシデント管理であり、ITシステムの障害から可能な限り迅速にサービスを復旧することが目標である。もう一つは問題管

理であり、ITシステムの障害の根本的な原因を明らかにして、問題の再発を防ぐことが目標である。本稿は、前者のインシデント管理にフォーカスし、ITシステムの障害からの迅速な復旧を支援する技術開発に関して説明するものである。

インシデント管理では、過去の障害情報を既知の障害情報として活用することが記載されている。障害対応の過去事例の活用には、つぎのような課題がある。

(1) 障害対応ノウハウの管理が属人的

過去事例調査などが属人的なスキルに依存しており、トラブル解決の長期化や人的コスト増に繋がっている。過去の障害情報を検索する場合に用いる検索キーワードの選択、現場から取得したサーバの出力するログや設定ファイルの解析方法、原因特定が困難である場合のエスカレーション（より専門性の高い部門へ作業を依頼すること）の判断基準が、担当者のスキルや経験に依存しており、担当者間で必ずしも共有されていない。

(2) 障害対応ノウハウの構造化が不十分

障害対応の知識を定義する表現形式がフリーフォーマットであった場合、自社製品や他社製品の障害情報を取り入れて充実させるといったメンテナンスが困難となる。このような障害情報の管理方法は、オープン/マルチベンダ化の進んだ現在のITシステムの障害対応には適さない。

つぎの章では、これらの課題を解決するための、障害対応ナビゲーション技術のアーキテクチャについて述べる。

アーキテクチャ

担当者のスキルに依存しない標準的な方法で障害復旧を行うことが重要である。そのためには、障害復旧の詳細な一つ一つの手順を、誰でも同じようにナビゲーションする技術が必要であると考えた。

本技術は、シンプトンDB、シンプトンナビゲータ、CMDDB (Configuration Management Data Base: 構成管理データベース)⁽²⁾から構成される。以下では、図-1に示す障害対応システムのそれぞれの構成要素について述べる。

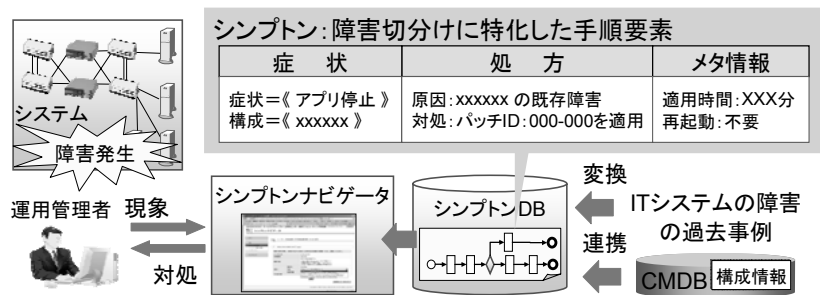


図-1 障害対応システム
Fig.1-Troubleshooting navigation system.



(a) 障害対応手順画面 (b) ツリー表示画面

図-2 ナビゲーション画面例
Fig.2-Symptom navigator screenshot.

● シンプトンDB

シンプトンDBとは、ITシステムの障害対応のために必要となる知識をシンプトンと呼ばれるデータ形式を用いて管理するデータベースである。ITシステムで起こる障害の症状に対して、どのような処方を行えばよいかを知識として管理する。例えば「アプリケーションが停止している」というITシステムの障害の症状に対して、「サーバからログを取得する」といった処方に関する知識を管理する。このように、障害対応の知識をシンプトンで形式化することで、前章で挙げた課題を解決する。

● シンプトンナビゲータ

シンプトンナビゲータは、シンプトンDBから検索した処方に関する知識を、作業者の行う障害対応手順として表示する画面 {図-2 (a)} と、手順の全体像をツリー表示する画面 {図-2 (b)} を持つ。障害復旧作業の担当者は、ITシステムの障害に関する症状をシンプトンナビゲータに入力する。すると

シンプトンDBから入力された症状に関連する情報を検索し、障害復旧に必要な手順がシンプトンナビゲータ (障害対応ナビゲーション) に表示される。表示された手順を実行し、さらに新しい症状を入力する。これを繰り返すことで、障害復旧の手順が順次提示され、担当者のスキルに依存せず障害復旧作業が可能となる (図-3)。

● CMDDB

シンプトンDBで管理している障害対応の手順を実際の障害発生時に適用するためには、手順の中にある抽象的な値を、対象となるITシステムを示す具体的な値に変換する必要がある。例えば、「サーバからログを取得する」という手順を実行する場合には、サーバを実際の値 (IPアドレスやサーバ名) に置き換える必要がある。

そこで、ITシステムの構成情報を管理するCMDDBから、具体的なサーバ名やIPアドレスを取得する機能が必要となる。そのような機能を

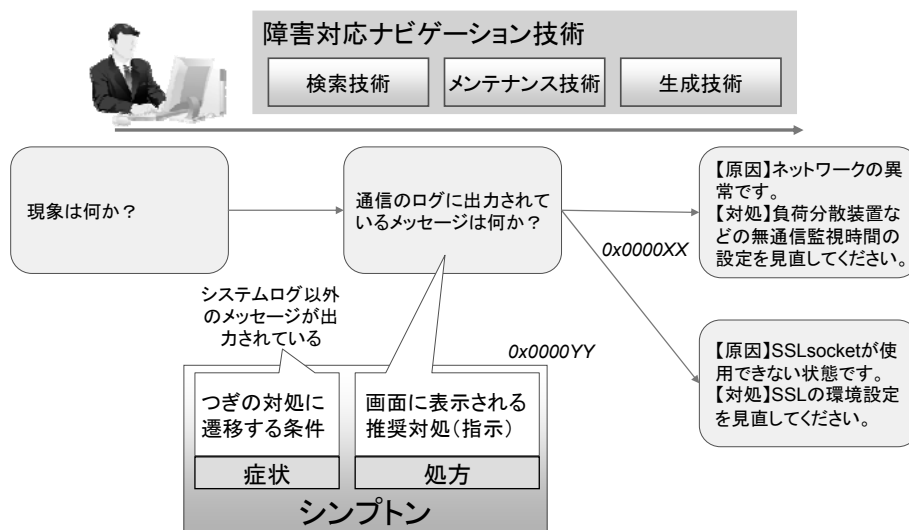


図-3 障害対応ナビゲーションの例
Fig.3-Troubleshooting navigation example.

CMDBとして実現している。

シンプトンのデータ構造

シンプトンDBの中に保存されている障害切り分けに特化した手順要素を「シンプトン」と呼ぶ。シンプトンは図-1に示すように症状・処方・メタ情報から構成されるデータ構造を持つ。

なお、データ構造のそれぞれの構成要素はXML技術を使ってスキーマを定義し、正規化された形式で定義されている。

● 症状

症状とは、シンプトンで示した障害対応の知識を利用する場合の条件を示す情報である。人間に例えると、病気の症状に相当する。具体的には「アプリケーション停止」というような症状が記述されている。シンプトンDBは、入力された症状とシンプトンに記述された症状とをマッチングさせ、該当するシンプトンを出力する。

● 処方

処方とは、シンプトンの症状で示した状況が起こった場合に、実際に行う対処を示す。同じく人間に例えると、症状に対する処方に相当し、「パッチID:000-000適用」というような処方内容が記述されている。この処方内容は、現時点では人間が作業を行う場合もあるが、将来的には運用プロセスを管理する機能に引き継がれ自動実行される。

● メタ情報

メタ情報とは、シンプトンに関連する様々な情報であり、複数のシンプトンが検索結果として出力された場合の選択基準や、シンプトンを検索するためのメタ情報として利用する。

例えば、ある症状が起こった場合、ITシステムに与える影響をリスクとして定義する。また、ある処方を行うために必要となる処理時間の長短を示すことで複数マッチしたシンプトンの選択基準として利用する。さらに、該当するシンプトンがどのような製品に関連するかという情報などをメタ情報として定義することで、特定の製品に向けたシンプトンを検索するといった使い方が考えられる。

障害対応ナビゲーション技術

本章では、シンプトンナビゲータを実現する技術である障害対応ナビゲーション技術について説明する。障害対応ナビゲーション技術は、検索技術、メンテナンス技術、生成技術から構成される(図-3)。

● 検索技術

シンプトンDBの検索処理は次のようになる。

- (1) 検索キーを入力する。
- (2) ある特定のシンプトンがマッチし、その結果を検索状態として記録する。
- (3) マッチしたシンプトンの更に下部のツリーに属するシンプトンを検索対象とする。

この(1)から(3)までの処理を繰り返し、絞り込み検索を実現する。

● メンテナンス技術

実際の障害復旧に対して検索結果で得られたシンプトンが有効であったかどうかを適用率として評価し、シンプトンのメタ情報として保存する。適用率の高いシンプトンほど、障害対処に関する有効性が高いと考える。そして、シンプトンDBを検索する際に、メタ情報に記録された適用率を検索結果の優先順位として利用することで、障害復旧に対して有効性の高いシンプトンが検索結果として得られるようになる。

● 生成技術

ITシステム障害の過去事例の中から、原因に至るまでに着目した症状について、データマイニング技術を用いて抽出し、シンプトンを自動的に生成する。作成したシンプトンについて、過去事例を効率的に切り分けるために、最適化手法を使って提示すべき手順を最適化し、できるだけ少ない手順で障害復旧を可能とする。

障害対応ナビゲーション技術の評価

障害対応ナビゲーション技術の効果を評価するため、富士通の社内システムで試行した。システム規模は310台、サービス数90を対象とした。

まず社内システムの障害対応手順書(29頁)を分析し、作業要素に分解することで130個のシンプトンとして記述し、エラーメッセージが発生した1箇月間の事象について障害対応ナビゲーション技術の適用を行った。

その結果、エラーメッセージが発生した事象

1811件のうち、手順書のシンプトン化を行ったインフラ障害(13%)について、障害対応ナビゲーション技術を用いて解決することができた。障害解決の手順は、ハードウェア、ネットワーク、アプリケーション、システムと非常に広範囲にわたっているため、13%をカバーできたことは価値があると言える。今後、シンプトンの生成技術を適用することでカバー率を上げることができる。

さらに、運用現場からのヒアリング結果に基づいて以下の効果が確認できた。

- (1) 質問応答形式のため、熟練度を問わずに手順を確実に実行することができ、属人性を排除することができる。
- (2) トラブル解決時間を短縮することができる。
 - ・膨大なマニュアルの該当箇所を検索する時間が短縮される。
 - ・作業レポートを自動で作成することにより、作業レポート作成の時間が短縮される。
- (3) 作業ごとの所要時間を記録することで、長くかかった手順や、使ってみて冗長に感じる部分といった、障害対応手順のボトルネックが可視化されるため、その結果を手順修正にフィードバックすることで手順を洗練することができる。

ロードマップ

本アーキテクチャのロードマップを図-4に示す。

障害対応システムの目指すゴールは、ITシステムの障害の予兆を検知し自律的に復旧することである。そのためにまず、障害対応の知識を管理するシンプトンDBを中心とした障害対応アーキテクチャを確立する。その後、シンプトンDBにある知識を

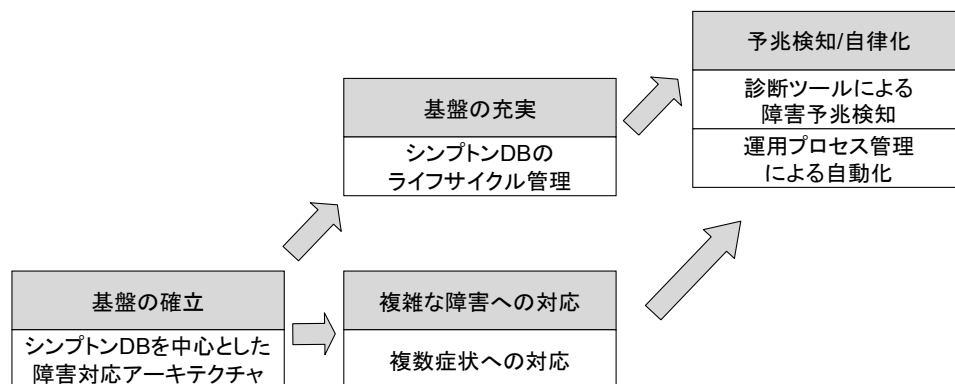


図-4 ロードマップ
Fig.4-Roadmap.

常に進化させるためのライフサイクル管理技術を確立する。ライフサイクル管理技術には、新しい障害に対応した履歴からシンプトンを生成する技術、シンプトンの構造を最適化する技術が含まれる。また、同時に複合的に発生する症状を自動的にパターン化し、再度起こった複合症状が過去のどの障害であるかを高速にマッチングする技術を開発し、複合症状への対応を確立する。さらに、診断ツールを使った障害の予兆検知や、運用プロセス管理を使った自動復旧を行うことで、将来的にITシステムの障害からの自律復旧を実現する。

む す び

本稿では、障害対応システムのアーキテクチャと、その中心的なコンポーネントであるシンプトンDB、

およびシンプトンを活用した障害対応プロセスの迅速化について、その概要を示した。

今後、本アーキテクチャのプロトタイプや実証実験を推進する。さらに、障害切分けに特化した手順要素であるシンプトンに関して、IBM社やCA社と共同で標準化活動に積極的に貢献していく。標準化活動を通じて、複数ベンダ間でのシンプトンの相互利用を推進し、IT業界の発展に貢献していきたい。

参 考 文 献

- (1) ITIL-itSMF Japanオフィシャルサイト。
<http://www.itsmf-japan.org/>
- (2) CMDB。
<http://cmdbf.org/>