社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006－DSM－40 (9)
2006／3／29

大規模ネットワーク・サーバ運用監視向け インシデント管理システム

菅野 幹人† 大越 冬彦† 村田 篤†
†三菱電機株式会社 情報技術総合研究所

あらまし ビジネスのITシステム依存度が高まっており、複数顧客の異なるITシステムを運用監視するMSP（Management Services Provider）の統合運用監視センターにおいては、監視対象のネットワーク、サーバの運用監視機能の強化が課題となっている。その対応として、ITIL（IT Infrastructure Library）を用いた運用監視業務の高度化、オペレータ作業の効率化、サービス提供の低コスト化を図る必要がある。本稿では、大規模ネットワーク・サーバの運用監視において、アラームを統合管理し、障害発生から障害復旧までを記録するインシデント管理システムを、ITIL注の定義をベースに設計構築したので報告する。

注ITILはOffice of Government Commerceの登録商標である。

Incident Management System for Large Scale Network System

Mikihito kanno† Fuyuhiko Ohkoshi† Atsushi Murata†

†MITSUBISHI ELECTRIC CORPORATION
INFORMATION TECHNOLOGY R&D CENTER

Abstract In this paper, we report ITIL based Incident Management System which records whole life cycle of trouble for large scale network system. As dependency to IT of the business is rising, it is necessary to reinforce operational ability of the integrated operation monitoring center at the MSP. This system achieved sophistication of operation management based on ITIL, improving efficiency of operator's work and reducing service costs.

1．はじめに

企業における IT システムへの依存度が高まっており、IT システムの高可用性が求められている。さらに IT システムを構成するネットワーク機器やサーバ等も増加しており、IT システムの運用監視は、人的リソース確保、コスト増加が問題となっている。MSP（Management Services Provider）の統合運用監視センターは、これらのニーズに対応するため、多数の顧客の様々な IT システムの統合的な運用監視を顧客に代わって実施する運用監視サービスを提供している。統合運用監視センターは、企業のネットワーク機器や IT システムを 24 時間 365 日にわたり監視する機能、監視内容の高機能化、提供サービスの低価格化のためコストダウンを図り他社競合力を強化していく必要がある。さらに運用監視においては、英国で取りまとめられた ITIL（Information Technology Infrastructure Library）と呼ばれる運用監視ガイドラインも出てきており、障害対応処理の

高度化、定型化などに取り組む必要がある。

本報告では、MSPの統合運用監視センターにおける、複数の顧客のネットワークやサーバからなるITシステムを統合的に監視するインシデント管理システムをITILの考え方を取り入れ設計構築したので報告する。

2. ITIL

ITIL[1],[2]は、英国政府のOCTA(Central Computer and Telecommunication Agency)が1980年代後半にまとめたITサービスマネージメントを構築、維持、改善するための情報システム管理基準である。ITILは、BSI(British Standards Institution)によりBS15000として英国標準化され、2005年12月にISO20000として採択されている。ITILを基盤とした運用監視サービスにより、ITシステムの構成情報に基づく運用監視、顧客ごとのサービスレベル契約に基づく障害対応処理、障害が発生する前に障害を未然防止するプロアクティブ運用監視などを実現できる。

3. ITILのインシデント管理

ITILでは監視装置で検知したアラームや、顧客からの連絡などはインシデントとして処理する。インシデント処理の手順としては、下記の①～⑥で処理することが推奨されている。

①インシデントの検知と記録
②インシデントの分類と初期サポート
③インシデント内容の調査
④インシデントの解決と復旧
⑤インシデントのクローズ
⑥インシデントの管理や参照

統合運用監視センターでは、複数の顧客のネットワーク稼動監視やサーバ稼動監視などをネットワーク監視装置やサーバ監視装置で行なっており、顧客ごとに上記障害検知から復旧までの障害対応業務を実施する必要がある。その際、監視サービスの低コスト化のためには、インシデントへの対応をできる限り効率よく処理することが求められる。

ITILのインシデント管理の定義に基づき、従来の統合運用監視センターの課題を以下に整理する。

4. 課題

従来の統合運用監視センターにおける障害検知から復旧までの処理を行うインシデント管理では次の課題があった。

①インシデントの検知と記録

複数顧客の多数の異なるITシステムを遠隔から運用監視を行うため、多数のネットワーク監視装置やサーバ監視装置を利用している。障害対応を行うオペレータは、監視装置ごとに障害検知の確認を行い、障害発生を確認した場合には、手動で障害対応用の管理票であるトラブルチケットを発行し必要事項を記入し障害対応を実施している。このため障害の確認や復旧に時間を要し、トラブルチケット発行基準もあいまいで記録されないケースもあった。

②インシデントの分類

各監視装置では、ネットワーク回線の疎通については ICMP (Internet Control Message Protocol)やSNMP (Simple Network Management Protocol) Trap、サーバについては、プロセス死活監視やログ監視などを実施しており、障害検知した場合にはアラームを発報する。通常は障害のアラームも顧客サイトの拡張工事や長期連休や年末年始のシステム停止により障害とは見なさないアラームを検出する場合がある。さらにネットワークの疎通確認ではルータが一次的に高トラフィック状態となるためにICMPがエラーとなり、一時的な障害状態を検知する場合などもある。このようにアラームには障害アラームと非障害アラームがあり、これらを分類し、障害アラームだけを抽出し障害対応必要なインシデントに対応する必要があるが、監視装置の個別化、工事情報管理、ネット

ワーク高トラフィック状態確認などのシステム化課題があった。

③障害情報管理

インシデントに迅速に対応するためには、障害アラーム情報だけでなく、監視対象のネットワークやシステム構成情報、監視サービスの請負契約情報、顧客別の障害検知時の対応方法、障害検知時の連絡手段・連絡先情報、顧客の工事計画情報など、各種情報が必要となる。これまでは、これらの情報は書類やオンラインデータとして個々に管理され、障害復旧時にオペレータから個別に参照されるため、トラブルチケットの起票記入に時間がかかり、トラブルチケットの類似障害検索も困難な状況であり、効率化が求められていた。

5．システム構成

インシデントの検知と記録、インシデントの分類、障害情報管理の３つの課題へ対応するため、ITIL のインシデント管理を基盤として、ネットワーク・サーバ運用監視のインシデント管理システムを下記のように設計構築した。

ITIL に定義された障害検知と記録、アラーム分類などをシステム化するため統合管理装置を導入し図１のような３階層構造のシステム構成とした。複数のネットワーク監視装置やサーバ監視装置を垂直統合する統合管理装置により、各監視装置が検出したアラームを一元管理する構成とし、発生したアラームを全て記録する。さらに、統合管理装置の上位にトラブルチケット管理装置を導入し、統合管理装置で分類したインシデントに対応して、トラブルチケットを管理する構成とした。

アラームには、障害アラームと障害ではないアラームがあるので、アラームを計画工事（キャリアによる回線借用、顧客サイトの工事、顧客ビルなどの停電）情報に基づき自動的に統合管理装置上で分類するようにした。さらに、ICMP がエラーを検知した場合には、監視対象ルータが高トラフィック状態かどうかを検査するため、障害状態かどうかを切り分ける処理「自動障害切り分け」を自動実行する。これらの分類結果は、トラブルチケット管理装置にアラーム情報として伝達され、トラブルチケットを自動的に発行する。分類種別に応じてトラブルチケットのステータスを「障害」、「工事中」、「障害切り分け中」の３段階で管理し、オペレータには「障害」のトラブルチケットのみを認識対応させ、ITIL 定義のアラーム分類記録を自動化した。

システムで参照する運用情報は、顧客のシステム構成や契約情報、障害時連絡先などを構成情報としてデータベース化し、アラームに記録されている監視対象ホスト名で参照できるようにした。これにより、トラブルチケット自動発行時に、構成情報をアクセスし、障害管理の基本情報をトラブルチケットに自動的に転送し人手による入力レス、トラブルチケットの検索性向上、障害対応の迅速化を実現した。構成情報管理の変更や管理には ITIL の構成管理業務や変更管理業務を業務要件として定義して、情報の新鮮さを保つように運用する。

6．機能とその動作

今回構築したインシデント管理システムの機能とその動作について説明する。

①監視装置による障害検知と記録

監視機能は、監視対象機器を定期的に監視し、障害を検知した場合には、統合管理装置にアラームを送付し記録する。各種監視装置を統合管理装置の直下に増設可能な構成とし、各監視装置が受け持つ監視対象は、監視性能や監視装置がダウンした時の影響を考慮して決定する。監視装置の監視設定により、障害を自動検知し、アラームを統合管理装置に送付することで、アラーム分類を行い、トラブルチケットの発行と

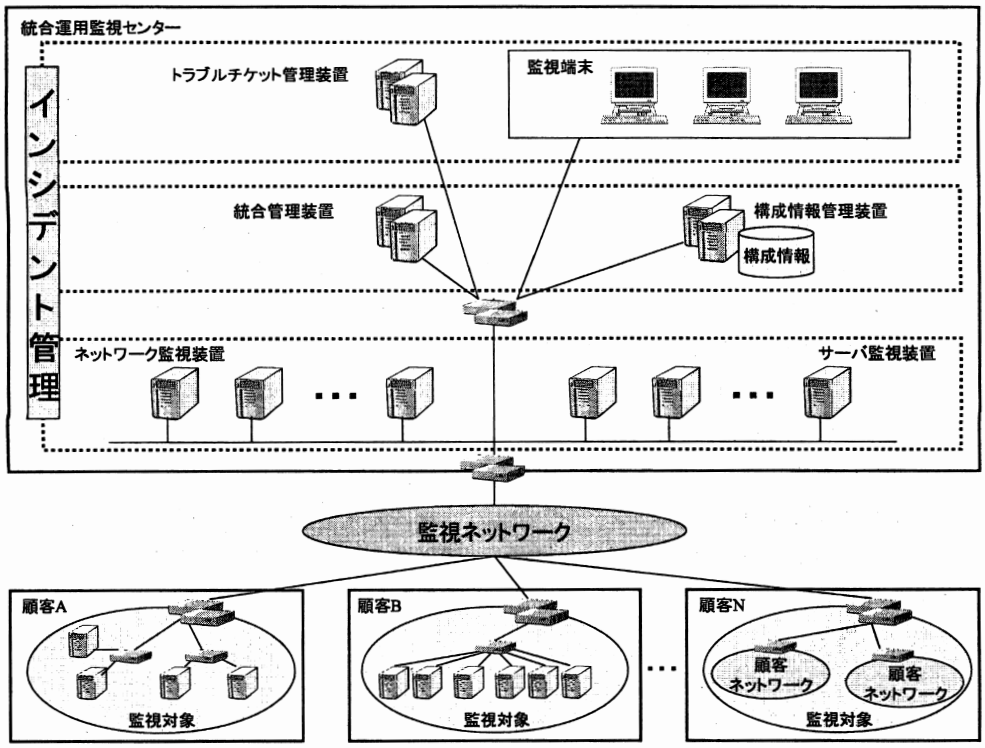

図１　システム構成図

記録をシステムで自動に行うようにする。各監視装置の監視設定については以下の通り。

（１）ネットワーク監視

ネットワーク監視装置は、数百台の監視対象機器であるルータやファイヤウォールなどに対して、ICMP による監視を一定間隔で行い、監視対象機器までの疎通とこれらネットワーク機器の死活を監視する。また、監視対象機器が異常状態に陥った場合には、該当のネットワーク監視装置に対して SNMP Trap を発行する設定を行い、トラップによる異常検知も同時に実施する。さらに定期的に監視対象ルータの回線トラフィック情報など性能情報も SNMP により取得する設定とする。

（２）サーバ監視

サーバ監視装置については、監視対象サーバにサーバ監視装置のソフトウェアを導入し、サーバ死活監視、プロセス監視、ログ監視、ファイルシステム監視、データベース監視、応答性能監視などの監視を詳細に設定する。

②統合管理装置によるアラーム自動分類

アラーム統合管理装置では、送付されたアラームの分類を以下の手順で自動的に実行する。

（１）工事判定

アラームの発生した日付時間とアラームの監視対象ホスト名により、構成情報に格納されている計画工事情報を参照して、該当アラームが工事時間中に発生したアラームかどうかを自動判定。工事に該当するアラームであれば、トラブルチケットを「工事中」ステータスとして自動発行するようにトラブルチケット管理装置に情報を送付する。また工事中アラームを

検出した場合には、該当工事終了予定時間に自動的に該当監視機器に対して ICMP などによる復旧確認を自動的に実行。復旧していれば工事終了と見なし、「工事中」の該当トラブルチケットを自動的にクローズするようにトラブルチケット管理装置に情報を送付する。復旧が確認できない場合には、「工事中」ステータスのトラブルチケットを「障害」ステータスに変更し、オペレータに障害対応を実施させる。

（2）障害判定

工事に該当しないアラームで、ネットワーク機器の ICMP エラーの場合には、ルータが本当に障害であったか、一次的に高トラフィック状態になっただけかどうか確認する自動障害切り分け機能を自動実行する。本切り分け機能が動作している間は、トラブルチケットは「障害切り分け中」ステータスとしてオープンする。本自動障害切り分け機能は、コマンド形式で実装され、障害を検知したルータに対して、ICMP を数分間発行して疎通を確認した後、疎通があればルータに **TELNET** を自動実行してルータ内部の情報を収集する。疎通があれば「障害切り分け中」ステータスのトラブルチケットに収集した情報をリンクして自動クローズし、疎通がなければトラブルチケットを「障害」ステータスとしてオペレータに障害対応させる。 このように統合管理装置上でアラームの分類を自動的に実施し、分類結果に応じてトラブルチケットのステータスを「障害」、「工事中」、「障害切り分け中」として管理する。オペレータには障害である「障害」ステータストラブルチケットにのみ対応させ効率化を図る。

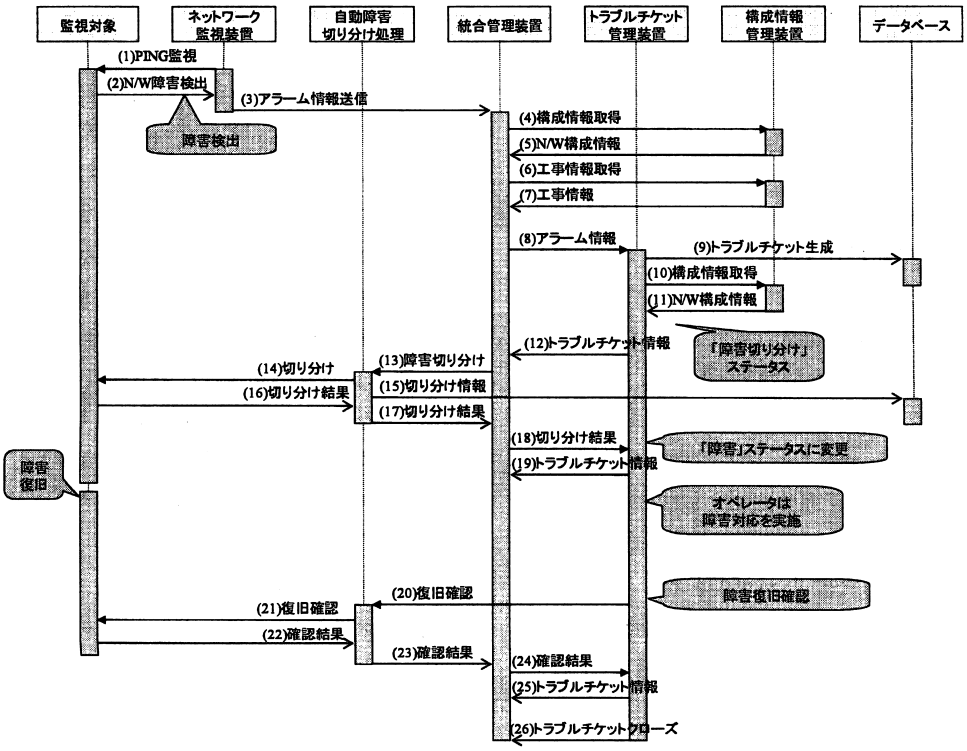

図２　ネットワーク障害検知時の動作

③トラブルチケット管理装置による障害管理

トラブルチケットは発行時に、アラーム情報の一部である監視対象ホスト名などにより構成情報データベースを参照し、トラブルチケットの基本情報については自動的に転記され入力される。オペレータは障害復旧の作業指示を運用手順書に基づき対応し、必要な処置だけをトラブルチケットに短時間に入力記録でき、迅速な障害復旧が可能となる。さらに、人手による入力ではなく、データベースから定型的な語句で転記されるのでトラブルチケットの検索性も向上する。

7. 効果

ITIL をベースとしたインシデント管理システムの実現により次の効果が期待できる。

①拡張性を考慮したシステム構成

インシデント管理システムを新規に構築し、3階層の構成を実現したため、統合管理装置の下に監視装置を自由に増設可能となった。そのため、監視対象の容易な拡張性を実現した。さらにアラーム検知からトラブルチケットの障害時オープンまでを同構成の中で機能的な役割を持たせて自動化し、オペレータの作業効率を向上させた ITIL の定義に基づくインシデント管理システムを構成することができた。

②オペレータ作業効率の向上

従来はアラームの分類については、監視対象機器が少なかったこともあり、オペレータが対応していたが、オペレータの作業効率を向上させるために統合管理装置にて分類処理を機械化した。これによりオペレータは、障害アラームのみに対応することが可能となり、オペレータの作業効率が向上するため、監視対象の規模をさらに拡大できる。さらに、統合管理装置上で、アラームを一元管理することで、ネットワーク監視装置とサーバ監視装置のアラームを同時に参照することにより、同じサイトで1つの原因で発生した障害の把握が一段と容易になり、従来に比べて的確な障害対応を実施できる。

③トラブルチケット活用による障害分析

これまでのトラブルチケットは障害復旧の履歴として記録していたが、構成情報をデータベース化して記録内容を定型化したことで、検索、分析可能な情報とした。蓄積されたアラーム情報とトラブルチケットを活用することで、顧客 IT システムの傾向分析を行ない、ITIL の問題管理に対応し可能となる。トラブルチケットの分析により、障害の傾向や工事の割合、高トラフィック状態で切り分けを実施した機器などが抽出でき、今後さらに能動的な運用監視が実現できる。

8. まとめ

ITIL のインシデント管理プロセスをベースとした MSP の統合運用監視センターのインシデント管理システムについて述べた。今後もさらに増加の一途を辿る多数のネットワーク機器、サーバにおいて、アラーム統合管理システムを導入し、そこにアラーム分類処理、構成情報データベース、トラブルチケットの自動管理機能などを組み込むことにより、障害検知から障害復旧までの迅速化、省力化を実現した。

今後の課題は、本システムの評価を行うとともに、オペレータの障害対応を状況に応じて管理し障害復旧までの手順をナビゲートする機能や障害状況を元にした障害未然防止のためプロアクティブ運用監視機能、顧客ごとの運用監視状況を報告する ITIL 対応レポート生成機能などの実現であると考える。

9. 参考文献

[1]The Stationery Office 出版, 2003, Service Support

[2]The Stationery Office 出版, 2003, Service Delivery