

トラブルチケットと連携した障害アラーム管理システム

大越 冬彦、菅野 幹人

三菱電機株式会社 情報技術総合研究所

1. はじめに

MSP (Managed Service Provider) などの運用管理において大規模システムにおける障害アラーム管理を効率良く実現するために、障害アラーム受信から、発生要因の判定、トラブルチケットの発行までを自動的に行う障害アラーム管理システムを開発した。

2. 従来システムの課題

情報通信システムの大規模化により障害アラーム管理システムでは、管理対象の機器数及び種類の増加に伴って、処理しなければならない障害アラームの数及び種類が増えてきている。従来の障害アラーム管理システムでは障害アラームの処理を人手で実施していたため、障害特定に時間がかかっており、これ以上のシステムの大規模化に対応することが困難になってきている。その詳細は以下の通りである。

(1) 誤報アラームの存在

管理対象機器の種類によって発生する障害アラーム全てが必ずしも障害を示すものではない場合がある。このために、対応の要否について確認作業を実施する必要があった。

(2) 工事による障害アラーム確認

管理対象機器の更新作業などの工事によってネットワークが通信不能になり、障害アラームが発生する。この場合には工事予定との照合を行う必要がある。また工事終了時の確認作業も必要であった。

(3) 障害の判定

オペレータが障害アラーム内容を見て本当の障害かどうかを判定し、障害と判定した場合に手動にてトラブルチケットを発行していた。このため、オペレータのスキルなどによって判定基準が左右される可能性があるとともに、トラブルチケット作成に手間がかかっていた。また同一の障害から複数の障害アラームが重複して発生する場合があります、既にトラブルチケットが発行されているかどうかを確認する必要があった。

3. 本システムによる解決方法

本システムは、受信した障害アラームの発生要因を自動的に判定することで、管理対象で実際に発生している障害に対する複数の障害アラームを特定する。それらの障害アラームから自動的にトラブルチケットを発行することにより実際に発生している障害と障害管理単位であるトラブルチケットを一致させる。これらにより、障害の特定時間の短縮を実現し、大規模システムでの障害アラーム管理を可能とする。(図1)

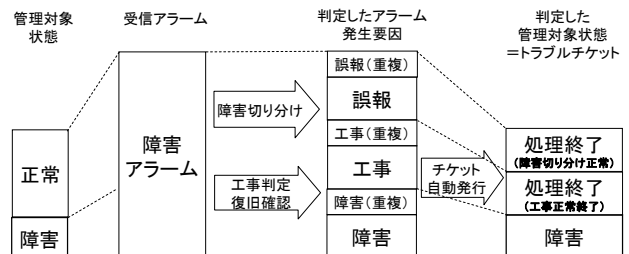


図1 本システムの処理

本システムでは以下を実施する。

(1) 自動障害切り分け処理

障害アラーム受信時に、アラームの真偽判定および解析時に必要な詳細情報を取得するために自動的に障害切り分け処理を実施する。

(2) 工事判定/復旧確認処理

事前に定義された工事情報と障害アラーム内容を照合して、工事による障害アラームであれば障害として扱わない。また工事終了予定時刻に復旧確認処理を自動実行することにより、工事が予定通り終了したかどうかを自動確認する。

(3) トラブルチケット自動発行

障害アラームを受信した場合にトラブルチケットを自動発行し、障害アラーム情報をトラブルチケットに関連付ける。その際に同一機器で発生した障害アラームは同じトラブルチケットに関連付ける。

4. 実現方法

図2に本システムの構成を示す。統合アラーム管理サブシステムによって自動切り分け処理と工事判定/復旧確認処理を実現するとともに、その結果をトラブルチケット管理サブシステムに転送することによりトラブルチケットの自動発行を実現している。

Alarm management system with a trouble ticket.
Fuyuhiko OHKOSHI, Mikihito KANNO
Information Technology R&D Center, Mitsubishi Electric Corporation

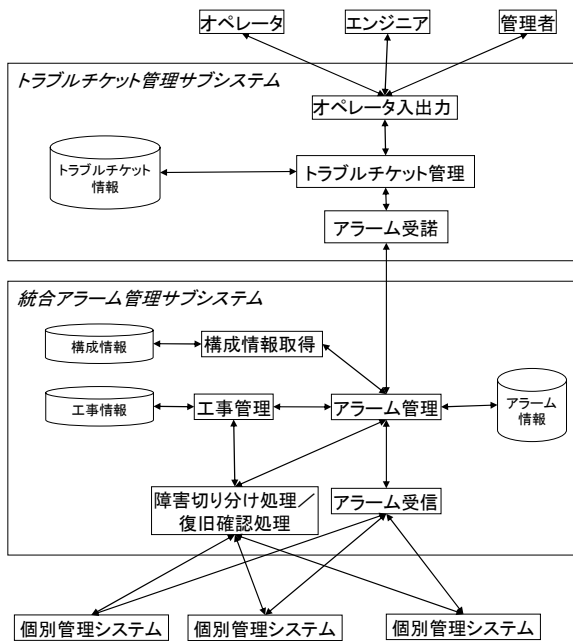


図2 システム構成

(1) 自動障害切り分け処理

統合アラーム管理サブシステムの機能を用いて、障害アラーム受信時にその機器の構成情報に応じた外部コマンドを発行し、自動障害切り分け処理を実施する。

① 構成情報取得

個別の管理システムからの障害アラームを本システムでの共通形式に変換した後、構成情報と照合することで、障害切り分け処理に必要な情報を取得する。

② 障害切り分け処理

構成情報を元に必要であれば障害アラーム発生元の機器に対して適切な障害切り分け処理を実行する。切り分け処理の結果は障害切り分け処理アラームとして受信し、既に存在するトラブルチケットに追加し、障害切り分け処理結果が正常であれば、障害アラームを誤報とみなしてトラブルチケット処理を終了、異常であれば障害とする。

(2) 工事判定/復旧確認処理

統合アラーム管理サブシステムの機能を用いて、工事情報を記録した外部データベースをアクセスすることにより、工事判定を行う。また工事終了時に自動的に外部コマンドを発行することにより、復旧確認処理を実施する。

① 工事判定

障害アラームの発生原因が工事であるかどうかを判定するために、事前に登録された工事情報と障害アラームのホスト名、時刻、メッセージ内容を比較して一致すれば工事に伴った障害アラームとし、トラブルチケットを工事中とする。

② 復旧確認処理

工事終了時に機器が正常に復旧しているかどうかの復旧確認処理を行う。復旧確認処理の結果は復旧確認処理アラームとして受信し、既に存在するトラブルチケットに追加する。復旧確認処理結果が正常であれば、工事は正常終了したとしてトラブルチケット処理を終了し、異常であれば工事で異常が発生したとしてトラブルチケットを障害とする。

(3) トラブルチケット自動発行

発生した障害アラームの対応状況を管理するためトラブルチケット管理サブシステムの機能を用いて、解析状況の入力、専門エンジニアへのエスカレーションや、管理者による問題解決時の承認処理などを実施する。また統合アラーム管理サブシステムと連携することで、障害アラームから自動的にトラブルチケットに情報を転記することとした。

① アラーム受諾

統合アラーム管理サブシステムにおいて処理が終了した障害アラームの情報はトラブルチケット管理サブシステムに転送される。

② トラブルチケット管理

転送された障害アラーム情報を元にトラブルチケットを自動発行する。この時に同じ機器についての対応処理が終了していないトラブルチケットが存在していた場合、このトラブルチケットに障害アラーム情報を追加する。トラブルチケットが無ければ新たなトラブルチケットを発行する。

③ オペレータ入出力

オペレータには障害と判定されたトラブルチケットのみ表示されている。工事中、障害切り分け中、復旧確認中とされたものについては通常は表示されないが、ユーザからの電話などによる照会を受けた場合に、これらのものも表示できるようにしている。

5. 結論

本システムにより、受信した障害アラームの発生要因を自動的に判定することで、管理対象で実際に発生している障害に対する複数の障害アラームを特定することが可能となった。またそれらの障害アラームから自動的にトラブルチケットを発行することにより実際に発生している障害と障害管理単位であるトラブルチケットを一致させた。これらによって、障害特定時間の短縮を実現し、大規模システムでの障害アラーム管理を可能とした。

参考文献

村澤 靖, 菅野 幹人: インシデント統合運用監視システムの開発, 2005 電子情報通信学会ソサイエティ大会, B-14-11 (2005)