

複数の監視装置を統合する運用監視技術の開発

金子 洋介[†] 菅野 幹人[†] 村澤 靖[†] 村田 篤[†]

三菱電機株式会社 情報技術総合研究所[†]

1. はじめに

大規模・複雑化した情報システムに対する運用監視業務では、専門的な知識を持つプロフェッショナル運用監視エンジニアによる障害対応が不可欠である。我々は、プロフェッショナル運用監視エンジニアによる迅速な障害対応を実現するため、複数の障害監視装置のインシデント情報を収集・統合し、障害対応に必要な情報と連携して管理する運用監視技術を開発した。

2. 運用監視業務の現状と課題

近年、情報システムの大規模・複雑化は、障害をより複雑にしており、運用監視業務における迅速な障害対応を阻む要因となっている。複雑な障害は定型的な手順での対応が困難のため、専門的な知識を持つプロフェッショナル運用監視エンジニアによる障害対応が必要となる。

プロフェッショナル運用監視エンジニアは、障害対応に必要な様々な情報を参照し、障害原因の分析や障害復旧作業を行う。そのため、障害対応に必要な情報を素早く集めることが、障害対応の迅速化につながる。プロフェッショナル運用監視エンジニアが素早く情報を集める上で、現状の運用監視業務では二つの課題がある。

1. 複数の障害監視装置の参照

情報システムの監視は、サーバ監視装置やネットワーク監視装置など複数の障害監視装置を用いる。複雑な障害の発生時は複数の障害監視装置が障害を検知するため、プロフェッショナル運用監視エンジニアは複数の障害監視装置のインシデント情報を参照しなければならない。

2. 障害対応に必要な外部情報の参照

障害監視装置が上げるインシデント情報だけでは、障害対応に必要な十分な情報を得られない。プロフェッショナル運用監視エンジニアは、データベース参照や、運用ツールの実行により、障害対応に必要な機器や顧客の情報、機器の詳細な状態を別途参照しなければならない。

Development of the Management and Monitoring Technology which Unifies various Monitoring Equipments.
Yosuke Kaneko, Mikihito Kanno, Yasushi Murasawa and Atsushi Murata
Information Technology R&D Center, Mitsubishi Electric Corporation.

3. 目的と実現方式

本開発の目的は、障害対応に必要な情報をプロフェッショナル運用監視エンジニアへ素早く提供し、障害対応の迅速化を実現することである。そのために、以下の二つの運用監視技術を開発した。

1. インシデント情報の一元管理

プロフェッショナル運用監視エンジニアが、複数の障害監視装置のインシデント情報を一箇所から参照できるようにするために、複数の障害監視装置のインシデント情報を統合監視装置で一元的に管理する技術。

2. 外部情報の統合

プロフェッショナル運用監視エンジニアが、障害対応に必要な情報を素早く参照できるようにするために、障害対応に必要な情報を外部のデータベースやアプリケーションから取得し、インシデント情報と統合して管理する技術。

4. 運用監視技術

4.1. インシデント情報の一元管理

インシデント情報の一元管理を実現するために、三つの技術開発を行った。

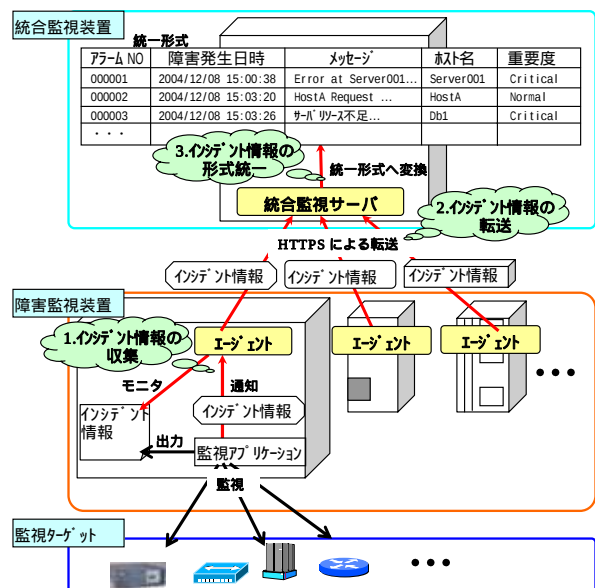


図 4-1 インシデント情報の一元管理

1. インシデント情報の収集

インシデント情報を一箇所で管理するために、各障害監視装置に配置したエージェントがインシデント情報を収集し、統合監視サーバへ転送する方法を用いた。さらに、監視アプリケーションの動作スケジュールやインシデント情報の緊急性に合わせて収集できるようにするために、モニタ方式と通知方式の二つの収集方式を用いた。

[モニタ方式]

監視アプリケーションがインシデント情報を出力するファイルを、エージェントが定期的にモニタしてインシデント情報を収集する方式。

[通知方式]

エージェントが監視アプリケーションからの通知を受けた時に、インシデント情報を収集する方式。

2. インシデント情報の転送

障害監視装置の統合を容易にするために、統合監視サーバとエージェント間の通信はファイアウォールフレンドリな HTTP プロトコルをベースとした。また、機密性の高い情報交換を実現するために、SSL (Secure Sockets Layer) 暗号化通信を用いてインシデント情報を転送した。

3. インシデント情報の形式統一

異なる種類の障害監視装置のインシデント情報を統一した形式で管理するために、統合監視サーバが、収集したインシデント情報を統一形式へ変換する方法を用いた。代表的な監視アプリケーションのインシデント情報から統一形式への変換に対応した。

4.2. 外部情報の統合

外部情報の統合を実現するために、三つの技術開発を行った。

1. データベース自動連携

データベースからインシデント情報に関連した機器や顧客などの情報を取得するために、インシデント情報の収集時に、予め定義した SQL 文を用いてデータベースから自動的に情報を取得する方法を用いた。SQL 文はインシデント情報の統一形式や他の外部情報（データベースアクセス結果やアプリケーション実行結果）を基に自動生成できるようにした。

2. アプリケーション自動連携

ping などの運用コマンドや外部のアプリケーションからインシデント情報に関連した情報を収集するために、インシデント情報の収集時に、予め定義したコマンドを自動実行して結果を取

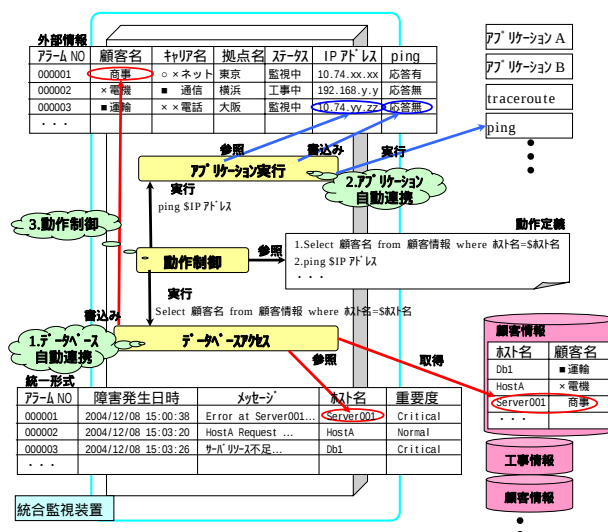


図 4-2 外部情報の統合

得する方法を用いた。コマンド文はインシデント情報の統一形式や、他の外部情報を基に自動生成できるようにした。

3. 動作制御

障害対応に必要な情報を、より詳細に収集するために、データベース自動連携とアプリケーション自動連携の動作順序を任意に定義できるようにした。

5. 運用監視技術の効果

以上の通り説明した運用監視技術を適用することで、以下の効果を得られる。

1. 複数の障害監視装置の参照の迅速化

複数の障害監視装置のインシデント情報を一箇所から統一されたフォーマットで参照できるため、監視効率を向上できる。また、複数のインシデント情報の同時参照により、大規模障害の早期発見、原因の早期特定などの効果がある。

2. 障害対応に必要な外部情報の参照の迅速化

データベースの参照やアプリケーションの実行で得られる外部情報とインシデント情報の統合を実現した。これにより、プロフェッショナル運用監視エンジニアは、障害対応に必要な情報をインシデント情報と同時に参照でき、迅速に障害対応を行うことができる。

6. おわりに

複数の障害監視装置を統合的に管理するインシデント情報の一元管理と外部情報の統合を実現する運用監視技術について報告した。本技術は大規模な運用監視システムや OSS (Operation Support System) への適用が可能である。