

# インターネット障害対策支援システムの提案

萱島 信<sup>†</sup> 寺田 真敏<sup>†</sup> 永井 康彦<sup>†</sup> 清水 英則<sup>‡</sup>

(株)日立製作所 システム開発研究所<sup>†</sup>

(株)日立製作所 ソフトウェア事業部<sup>‡</sup>

## 1. はじめに

近年、インターネットを含むネットワーク情報システムは、企業の情報基盤として重要な役割を果たすようになってきている。インターネットは、不特定多数のユーザが利用しており、今までのネットワークより大規模・広範囲化したシステムであるということと、ユーザの中には悪意を持つ攻撃者も存在しているということが特徴になっている。このため従来のシステムより外乱が多く、セキュリティ上の脅威も増大しているため、障害原因を特定し、迅速に復旧させることが難しいという現状にある<sup>[1]</sup>。

そこで本発表では、インターネットをベースとするネットワーク情報システムを対象として、障害検知・復旧を容易にする「インターネット障害対策支援システム」を提案する。

## 2. 課題

ネットワーク情報システムで障害を防ぐための対策は、システム設計者・構築担当者・運用担当者がシステムのライフサイクルのフェーズごとに個別に考えているのが実情である。担当者の作業を支援する障害対策ツールもまた、個々のフェーズを独立に支援する機能しか提供されていないため、障害対策を効率的に実施する上で、次のような課題が発生している。

- ・ 設計フェーズで策定した各種システム管理ポリシーを活用して、個々の機器を正しく設定した上でシステムを構築できるようにすること
- ・ 運用フェーズで収集した障害情報を活用して、機器設定内容の見直しを図るためのシステム管理ポリシーをブラッシュアップできるようにすること

そこで本研究では、上記の課題を解決するために、システム設計から運用までの作業を極力自動化し、シームレスな管理を支援する「インターネット障害対策支援システム」を実現することを検討してきた。これは、管理対象に埋め込んだエージェントを介して、障害情報の収集と復旧を実行する管理マネージャを設

け、システム管理ポリシー作成支援ツールと、設定診断ツールを連動させることにより、以下の機能を実現するものである。

- ・ システム設計時に策定したシステム管理ポリシーがシステム構築時に抜け漏れなくシステム設定として反映されていることを検査できるようにする
- ・ システム設定に問題がある場合、管理マネージャを用いて設定の修正を行えるようにする
- ・ システム運用時に管理対象機器から収集した障害情報や、特にセキュリティ事象に関してはCERT等のセキュリティ対策組織から報告されたセキュリティホール情報をトリガとして、該当する可能性のある管理対象を特定した上で診断と対策を実施できるようにする

検討中のインターネット障害対策支援システムの全体イメージを(図1)に示す。

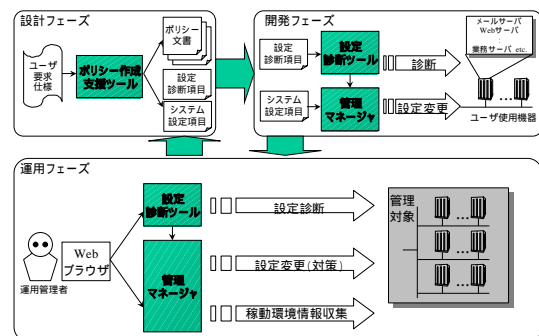


図1 障害対策支援システムイメージ

## 3. インターネット障害対策支援システム

### 3.1 機能要件

課題を解決するために、インターネット障害対策支援システムは以下の機能を提供する。

#### (1) 稼働環境情報収集機能<sup>[2]</sup>

障害の検知や、システムの設定がシステム管理ポリシーどおりに正しく行われているか調査を実施するためには、管理対象となる機器及びネットワークの現時点での設定状態や動作状態を把握することが必要となる。そこで、各管理対象におけるインタ

Proposal of a fault recovery system of the internet services.

<sup>†</sup> Makoto KAYASHIMA, Masato TERADA, Yasuhiko NAGAI: Systems Development Lab., Hitachi, Ltd.

<sup>‡</sup> Hidenori SHIMIZU: Software Division, Hitachi, Ltd

インターネットサービスの稼働環境を把握するための「稼働環境情報収集機能」を準備する。

### (2) フェーズ間連携機能<sup>[3]</sup>

設計フェーズで策定したシステム管理ポリシーは、構築対象のシステムを構成する各機器に対して適切に反映させることが必要である。また、ある機器において何らかの障害が発生した際には、同じ種類の機器に同様の障害がおこる可能性があるため、機器の種類単位でまとめて設定の変更が行えるようにすることが重要である。そこで、設計フェーズと開発フェーズにおける支援ツール間での情報連携を実現する「設計・開発フェーズ間ツール連携機能」を準備する。

また、運用フェーズで機器から得られたログ情報は、設計時に策定したシステム管理ポリシーと運用実態との乖離を評価するうえで貴重な情報である。そこで、この情報を活用し、ポリシーのブラッシュアップを図れるようにすることも必要である。そこで、運用フェーズと設計フェーズにおける支援ツール間での情報連携を実現する「運用・設計フェーズ間ツール連携機能」を準備する。

## 3.2 システム構成要素

上記の機能を包含したインターネット障害対策支援システムは、以下の3つの要素により実現した。

### (1) 管理マネージャ

管理対象や、ベンダ、情報機関より収集した障害関連情報（稼働状況、稼働環境に関する情報、障害要因情報等）を管理し、それらの情報を用いて各種管理対象の動作を集中制御する機能を提供する

### (2) エージェント

管理対象からの自律的情報収集を実現する稼働環境情報収集機能と、各種管理業務を支援するリモート設定変更機能を提供する

### (3) フェーズ間連携アダプタ

(3-1) ポリシー作成支援ツール連携アダプタ  
設計フェーズにおける支援ツールであるポリシー作成支援ツールに対し、単にポリシードキュメントだけではなく、個々の機器に対応した設定ファイルのひな形を作成する機能を提供する

### (3-2) 設定診断ツール連携アダプタ

運用フェーズにおける支援ツールである設定診断ツールに対し、ポリシー作成支援ツールで策

定したポリシーと、実際の設定状況の差分を抽出し、修正版の設定ファイルのひな形を生成する機能を提供する。

インターネット障害対策支援システムのプロトタイプ構成イメージを図2に示す。

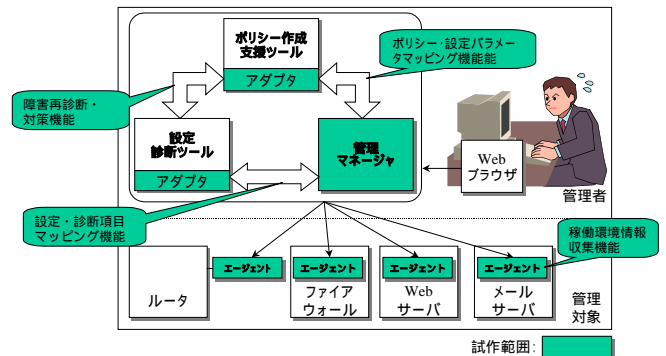


図2 統合運用管理システムイメージ図

## 4. まとめと今後の課題

インターネットをベースとするネットワーク情報システムを対象として、障害検知・復旧を容易にすることを目的とした「インターネット障害対策支援システム」を提案した。本システムを有効に活用するためには、管理対象の開発ベンダがエージェントモジュールを容易に開発できるようにすることが重要である。そのため、エージェントを開発するためのフレームワークと、管理マネージャに新しいタイプのエージェントも簡単に登録できるようにする機構を準備した上で、普及活動を行っていくことが課題である。

## 謝辞

本研究は、通信・放送機構(TAO)の委託研究テーマ「インターネットにおける障害情報の収集及び復旧支援技術の研究開発」の一環として行われているものである。

## 参考文献

- [1] 統合セキュリティ運用管理システムの実現に向けて、萱島他、情報処理学会第62回全国大会、2001.3
- [2] インターネット障害対策支援システムにおける情報収集機能の検討と実装、藤山他、第66回情報処理全国大会、2004.3
- [3] インターネット障害対策支援システムにおける統合設定機能の設定と実装、笠井他、第66回情報処理全国大会、2004.3
- [4] 統合セキュリティ管理システムによるセキュリティポリシー管理方式、甲斐他、第66回情報処理全国大会、2004.3