

3S-03

インターネットの障害検知のための原因推定手法に関する一考察

新保 宏之

横田 英俊

廣瀬 功一

井戸上 彰

加藤 聰彦

KDD 研究所

1 はじめに

インターネットが広く利用されるようになり、様々なネットワーク障害が大きな影響を及ぼしている。インターネットは多数のネットワークが複雑に接続されているネットワークである。このため、ユーザやネットワークオペレータは、自ネットワーク以外において発生した障害が、どの場所で発生しているのか、また障害の原因は何かということを知ることは非常に困難である。

現在、筆者らはユーザから障害申告のあった通信を再試行することにより、インターネット全体における障害検知を行うための手法を検討している [1,2]。また、ルーティングプロトコルのモニタによる経路情報監視 [1,3]、SNMP (Simple Network Management Protocol) を用いたハードウェア障害監視 [1] に関する手法の検討を行っている。本稿では、インターネットにおける障害検知のための原因推定手法に関する考察を行う。

2 障害検知のための原因推定手法

2.1 原因推定に対する要求条件

インターネットにおける障害検知のための原因推定手法には、次のような要求が存在すると考えられる。

- 通信再試行によって検知された障害の原因推定及び障害を申告したユーザへの通知
- 各ネットワークにおける、通信再試行、経路情報監視、ハードウェア監視から得られた障害情報のオペレータへの通知
- 障害情報のインターネット全体での共有

これらの要求を満たすために、次に示す 3 機能を検討している。

(1) 原因推定機能

通信再試行において検出された障害の原因をその症状、経路情報監視、ハードウェア障害監視の情報を元に推定し、その結果をユーザに通知するための機能である。

(2) ネットワーク管理機能

各ネットワークにおいて、通信再試行によって得られた障害情報、経路情報監視による経路変更情報、ハードウェア障害監視によるハードウェア障害情報をオペレータに通知するための機能である。

(3) 障害情報配布機能

通信再試行で得られた障害及びその原因をインターネット全体に配布し、障害情報を広く共有するための機能である。

2.2 各機能に対する要求条件

(1) 原因推定機能

インターネットは企業や ISP などの独立して管理されている多数のネットワークが相互に接続されているネットワークである。あるネットワークに対して、外部のネットワークから原因推定を行うための情報を得ることはセキュリティの面から困難であると言える。そのため、原因推定手法に関して次のような仕組みが必要になる。

- 最初に、通信再試行が実行された各ネットワークにおいて、通信再試行時の症状、経路情報監視、ハードウェア障害監視によって得られた情報から障害に関する原因推定を行う。
- 次に、全ての原因推定を行った結果を 1 箇所に集め、それを元にユーザから障害申告のあった通信の原因推定を行う。

インターネットにおける障害は様々な要因が複雑に組み合わされて発生する。そのため、各ネットワーク内及び全体的な原因推定手法としては、障害内容とその要因のデータベースを作成し、そのルールを用いて推定を行う仕組みが必要になると考えられる。

また、原因推定結果をユーザに通知するためのユーザインタラクション機能も必要である。

(2) ネットワーク管理機能

経路の変更やハードウェア障害はネットワークに与える影響が非常に大きいため、それらの事象が発生したら即座にオペレータに通知するための仕組みが必要である。通知に詳細情報へのポイントを示すことにより、障害への素早い対応が可能になると考えられる。

また、効率的なネットワーク管理のためには、収集された情報を分かりやすく表示する機能が必要である。具体的には GUI を用いて、ルータの物理的な接続図、ルータの論理的な接続を示すネットワークポロジ図及びその変更履歴、特定の 2 地点間における経路の変更履歴、ハードウェア障害発生箇所を图示する機能が必要になると考えられる。

(3) 障害情報配布機能

障害情報の配布のためには、配布を行う仕組みの他に、得られた障害情報を一意に識別するための仕組みが必要である。これは同じ情報が複数の経路を通して配布されることにより、情報のループや古い情報が配布

される可能性が存在するからである。

配布された障害情報は、各ネットワークのオペレータやインターネットのユーザから参照される必要がある。そのため、ネットワーク管理機能への組み込みや、ユーザとのインタラクション機能が必要になると考えられる。

3 設計方針

本節では、2節で示した要求を満たすような提案方法を実現するための方針について述べる。

検討を行っている機能の一部分は、各ネットワーク内で実行する必要がある。そのため、各機能は各ネットワークに存在している通信再試行を実行するための障害検知サーバ [2] 上で動作させる。

3.1 原因推定機能

原因推定機能は次のようにして実行する。

- 各ネットワークにおける原因推定は、各ネットワークにおける通信再試行が全て終了した後に実行する。推定結果は「原因推定通知」によって、ユーザから申告を受けた障害検知サーバに通知する。
- ユーザから申告を受けた障害検知サーバに障害検知要求が戻り、全ての通信再試行が終了すると、ユーザから申告を受けた障害についての原因推定を行い、その結果をユーザに通知する。ユーザへの推定結果の通知には電子メールを用いる。

図 1 に通信再試行と原因推定機能の動作概要を示す。ユーザが障害申告を行うと、K1 は Network1 内の通信再試行を行い、再試行終了後に障害検知要求を K2 に送信する。再試行によって Network1 内での障害が検知された場合、その症状、経路情報監視、ハードウェア障害監視の情報から、Network1 内での障害原因の推定を行う。障害検知要求を受け取った K2 は、Network2 内の通信再試行を行い、再試行終了後に障害検知要求を K3 に送信する。再試行によって Network2 内において障害が検知された場合、その症状、経路変更監視、ハードウェア障害の情報から Network2 内の障害原因推定を行う。推定結果は原因推定通知によって K1 に送付される。障害が存在しない場合、その旨の通知が原因推定通知によって行われる。K3 以降においても同様に通信再試行、原因推定が行われる。最終的に障害検知要求が K1 に戻り、K1 が全ての障害検知サーバから障害原因通知が到着したことを確認すると、その情報を元にユーザから申告を受けた障害の原因推定を行う。その後、原因推定結果がユーザに通知される。

3.2 ネットワーク管理機能

オペレータへの通知は、経路変更監視やハードウェア障害監視からの通知を受けて行う。オペレータへの通知には電子メールを用い、電子メール中に URL を埋め込み、Web ブラウザを用いてアクセスすることで詳細な情報を得られるようにする。

収集された情報の表示のために、必要に応じて、通

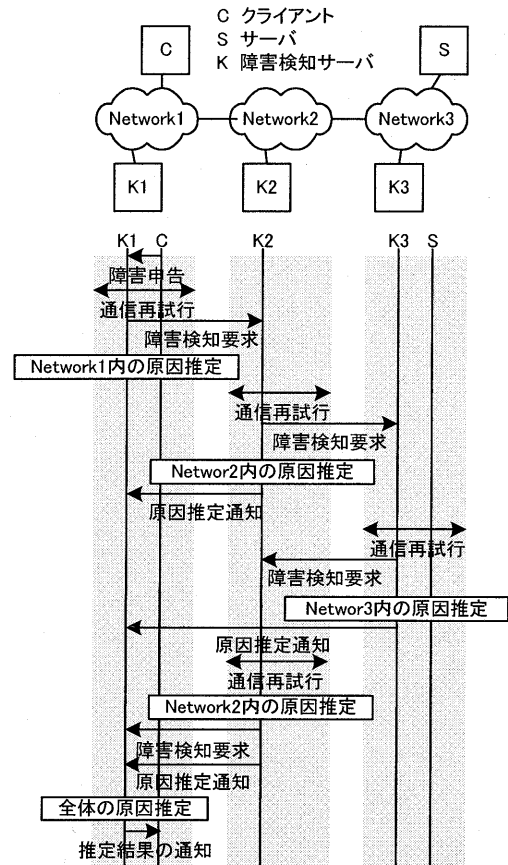


図 1 原因推定機能の動作概要

通信再試行、経路変更監視、ハードウェア障害監視からの情報取得を行う。

3.3 障害情報配布機能

各障害検知サーバに存在する障害情報の交換は、定期的に障害検知サーバ間で障害情報の集合を同期させることで行う。障害情報は、最初に通知する障害検知サーバにより付加された識別子を用いて識別される。

また、障害情報を、ネットワーク管理機能の GUI および障害検知サーバ上の Web ページに掲載することにより、ネットワークオペレータならびにユーザからの参照を行えるようにする。

4 おわりに

本稿では通信再試行、経路情報監視、ハードウェア障害情報監視の情報から原因推定を行う手法に関する考察を行った。なお、本研究は通信・放送機構からの委託研究「ネットワーク障害検知技術の研究開発」に基づき行われたものである。

参考文献

- [1] 加藤、井戸上、"網状態の監視と通信再試行を用いたインターネット障害検知方式"、信学技報 SSE2000-126、2000年9月。
- [2] 新保ほか、"インターネットにおける再試行型障害検知方式"、本大会予稿、2001年3月。
- [3] 横田ほか、"インターネットにおける障害検知のための経路変更監視方式"、本大会予稿、2001年3月。