3S-01

インターネットにおける再試行型障害検知方式

新保 宏之　　井戸上 彰　　加藤 聰彦
KDD 研究所

1　はじめに

インターネットの普及に伴い、各種のネットワーク障害が発生しており、その障害検知が重要な課題になっている。この状況を反映して、障害検知を行うためのシステムやソフトウェアが多数発表されているが、これらのシステムはネットワーク管理者が自ネットワーク内の障害を監視することを目的としており、自ネットワーク外で障害検知や、インターネットを利用しているユーザが障害の原因を知る仕組みは存在しない。

筆者らはユーザからの申告に基づき、申告された通信を再試行することにより障害の検知を行う方式を提案している [1]。本稿では提案方式について、その詳細を述べる。

2　通信再試行による障害検知

2.1　概要

通信再試行による障害検知方式は、ユーザからの障害申告を受けた障害検知サーバが、その通信を実際に再試行することにより障害検知を行う方式である。

TCP/IP 通信における障害は、経路異常やネットワークの輻輳などといったIPプロトコルにおける障害と、プロトコル手順誤り、サーバの未稼動、サーバの輻輳などといった上位プロトコル (TCP、HTTP 等) における障害に大別される。それぞれのプロトコルにおける障害を検知するために、障害検知サーバは IP レベルと上位プロトコルレベルの 2 種類の通信再試行を行う。

インターネットは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構成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、外部ネットワークから詳細な調査を許すことはセキュリティ上の問題があると考えられる。そのため、通信再試行は障害検知サーバを企業や ISP (Internet Service Provider) などのネットワークに 1 台ずつ設置し、これらの障害検知サーバが協調することで行う。

2.2　要求される機能

IP レベルにおいて通信再試行による障害検知を実現するには、ルータの経路テーブルを参照しながら、通信経路をたどる仕組みが必要になる。さらに、ユーザ端末から申告の対象となっている端末 (以降対象端末) の経路と、対象端末からユーザ端末の経路が異なることがあるため、両方の経路に関して調査を行う必要がある。また、ネットワーク輻輳監視のためには、ルータのインターフェイスのパケット廃棄率などを定期的に監視する必要がある。

上位プロトコルレベルにおける通信再試行を実現するためには、上位プロトコルのクライアントの機能が必要になる。加えて、クライアント機能には、サーバ輻輳を検出するために応答速度や転送スループットの計測を行うための仕組みが必要になる。

さらに、障害検知サーバ間で協調するための仕組みが必要である。また、通信再試行自体を制御する機能や、ユーザからの障害申告を受け付けるためのユーザインタラクション機能も必要である。

3　設計概要

2 節で示した要求を満たす、本方式を実行するための障害検知サーバの設計を行った。障害検知サーバは 3 部分から構成されている。

- IP レベル再試行部

IP レベルの再試行及びネットワーク輻輳監視を行う。IP レベルの再試行に必要な経路テーブルや、ネットワーク輻輳の検出に必要なルータのパケット廃棄率などの情報取得に SNMP [2] を用いている。

- 上位プロトコルレベル再試行部

インターネットでは様々な上位プロトコルが用いられているが、今回の設計では最も使用されているアプリケーションである WWW に関するプロトコルである TCP、HTTP、DNS を取り扱うこととした。上位プロトコルレベル再試行では、これらのプロトコルのクライアント機能を持ち、転送スループットの計測、ファイルの存在の確認、サーバの稼動確認などを行うことが可能である。

- 制御部

申告された障害の識別するための Failure ID の割当、障害検知サーバ間での協調機能、Web ベースによりユーザからの障害申告の受付を行うユーザインタラクション機能、再試行時に必要なソフトウェアの起動を行う機能を実現する。

4　動作概要

提案方式を実行する障害検知サーバの動作を述べるために、図1のようなネットワークを想定する。図1において、Network1 及び 3 は企業や学校などのネットワーク、Network2 は ISP のネットワークを想定している。ここでは、クライアント C1 のユーザが何らかの理由により WWW サーバ S3 にアクセス不可能な状況を想定している。

"Procedure of Internet Failure Detection Based on Communication Retrial"
Hiroyuki Shinbo, Akira Idoue and Toshihiko Kato
KDD R&D Laboratories Inc.

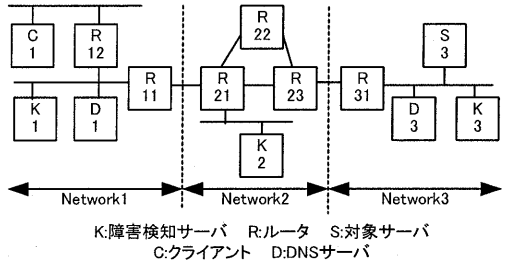

図 1　ネットワーク構成

4.1　通信再試行手順の全体的な動作

ユーザが自分の属するネットワークの障害検知サーバ (K1) に障害を申告すると、K1 は Network1 内の通信再試行を行う。その後、K1 はサーバ S3 方向の次のネットワークである Network2 の障害検知サーバ K2 に通信再試行を依頼するために「障害検知要求」を送信する。Network2 における通信再試行が終了すると、K2 は S3 方向の次の障害検知サーバである K3 に障害検知要求を送信する。通信再試行が S3 の属するサブネットまで行われると、K3 は逆方向の通信再試行、すなわち C1 方向への通信再試行を行う。逆方向の通信再試行もこれまでと同様に行われ、最終的に K1 が障害検知要求を受け取ることにより通信再試行が終了する。

IP レベル再試行は通信経路をたどり、経路の状況を確認するために行うので、障害検知要求を受けた各ネットワークで実行される。上位プロトコルレベル再試行は、ユーザ端末が属するネットワークと、対象端末が属するネットワークで行い、その結果を比較することにより、障害原因がサーバ輻輳か、ネットワーク輻輳かの判断を行っている。上位プロトコルレベル再試行と IP レベル再試行は同時に実行され、対象端末が属するネットワークでの上位プロトコルレベル再試行の実行は、障害検知要求によって指示される。

障害などの理由により、それ以上の通信再試行が不可能であると障害検知サーバが判断した場合、その障害検知サーバはユーザから障害申告を受けた障害検知サーバに対して「再試行不能通知」及び障害が発生するまでの再試行の結果を送信し、通信再試行を打ち切る。

4.2　各ネットワークにおける通信再試行の手順

Network1 を例にとり通信再試行の詳細な手順について述べる。図 2 はその手順を示している。

最初に、ユーザが障害検知サーバの Web ページにアクセスし、URL とその理由を HTML フォームに入力することで、障害申告を行う。次に、障害検知サーバは障害申告を識別するための Failure ID の割当を行う。その後、対象端末のホスト名から IP アドレスを得るために DNS サーバに名前解決を依頼する。この際に、Network1 内の DNS サーバ (D1) 及び対象端末を管理している DNS サーバ (D3) の両方に名前解決を依頼し、その結果が一致しているかどうかの確認を行う。D3

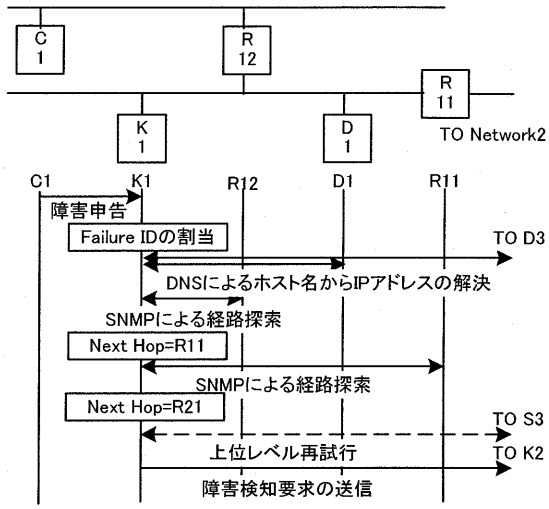

図 2　Network1 における通信再試行手順

の IP アドレスはドメイン名からそれを管理している DNS サーバを知るための要求を D1 に送信することで得ている。もし、対象端末側の DNS サーバにアクセスできない場合、K1 は DNS サーバに対する IP レベル再試行を実行する。

IP アドレスを得ると、K1 は Network1 内における IP レベル再試行を行う。最初に、静的にコンフィグレーションされているルータの一覧から、ユーザ端末の Next Hop となるルータを決定し、そのルータに対して対象端末への Next Hop となるルータを SNMP によって決定する。同様にして、Network1 内において、Next Hop ルータを順番に決定し、Network1 内での通信経路をたどる。Next Hop ルータが Network1 の範囲外である R21 になると、IP レベル再試行を終了し、次のネットワークの障害検知サーバ K2 に障害検知要求を送信し、Network2 における通信再試行を依頼する。

K1 は、IP レベル再試行と同時に上位プロトコルレベル再試行を実行する。ユーザの申告した URL の示す HTML ファイルに他 WWW サーバへの参照があった場合、そのサーバに対する IP レベル／上位プロトコルレベル再試行も実行する。

通信再試行によって得られた結果は、Failure ID に関連付けてログに記録される。

5　おわりに

本稿では提案方式に要求される機能について述べ、提案方式を実行する障害検知サーバの設計及び動作について述べた。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、September 2000.

[2] J. Case et al., “A Simple Network Management Protocol (SNMP),” RFC1157, May 1990.