分散システムによるLAN構成管理方式の検討

2O－2

窪田 歩　片岸 一起　浅見 徹
国際電信電話株式会社 研究所

1. はじめに

企業内LANの大規模化に伴い，管理者によるネットワークの全容の把握の困難さが増大している．加えて，ネットワーク機能の利用が容易になり，エンドユーザでも各種の設定変更をし得るようになってきているため，誤設定等による障害が多発し，その復旧作業も困難になってきている．我々は，設定変更等に起因する障害からの復旧を容易にするには，ルータや各種サーバの設定を一括してバージョン管理することが有効と考え，ソフトウェア開発の際に用いられるバージョン管理システムを用いたネットワーク構成のバージョン管理システムを提案した[1]．しかしながら，大規模なネットワークの構成を一箇所で管理することは，効率や管理権限の面から問題が大きい．そこで本稿では，各管理ドメイン毎に管理用のエージェントを設け，エージェント間の通信によりネットワーク全体の設定変更履歴の管理や，誤設定による障害発生時のロールバックによる復旧等を可能とする手法を提案する．

2. 単一ホストによる管理における問題

文献[1]において我々が提案した単一の管理ホストによるネットワーク構成のバージョン管理システムは，ルータや各種サーバプログラムの設定ファイル群を管理対象とし，これらを全て一箇所に集めて集中的にバージョン管理し，必要に応じて過去の設定データをネットワーク上に配送する機構を提供するものであった．これは誤設定に伴う障害発生時の原因調査，復旧作業を簡便化する上では有効であるものの，管理対象がWAN回線を経由してつながっている場合などには各管理対象の設定情報のアップロードやダウンロードなどの管理用トラヒックの大きさが問題となる．また近年のコンピュータネットワークでは，多くの場合サブネットワーク等の各管理ドメインは対等の権限を持ち，各種の設定変更等は独立に行うので，全てを集中管理する事は管理権限の面でも問題がある．そこで以下に述べるように，ネットワークを組織上，また効率面で適当と思われる単位のサブドメインに分割し，各サブドメイン毎に管理エージェントを設け，エージェントの協調動作によりネットワーク全体の構成管理を行うことを考える．

"Study on A LAN Configuration Management System with Distributed Agents." by Ayumu KUBOTA, Kazuki KATAGISHI and Tohru ASAMI
KDD R & D Laboratories

3. 分散システムによるネットワーク構成のバージョン管理

各管理ドメイン毎に構成情報のリポジトリを設け，ドメイン毎に構成情報のバージョン管理を行うものとする．これにより，遠隔管理ホストによるデータの収集や，管理ホストからのデータの配信によるトラヒックを抑制するとともに，管理権限をドメイン毎に独立させる．その上で，各ドメインにエージェントを配し，以下に挙げる機能を持たせることで，より高度なネットワークの構成管理が実現できると考えられる．

(1) **変更履歴の開示** アプリケーションの動作にネットワーク内で行われた設定変更に起因すると考えられる障害が発生した場合，その原因の推定を可能にするために，各ドメイン内の変更履歴を開示し，ネットワーク全体の変更履歴をその変更内容も含めて調査可能にする．

(2) **構成変更の通知** あるドメインのDNSサーバの変更に伴い，外部ドメインのDNSのブートファイルの更新も必要になる場合のように，各ドメインで行った変更が外部に波及する場合には，他のドメインのエージェントに対し必要な情報を通知する．

(3) **変更処理の同期** (2)のように，多数のドメインに波及する変更を実施する際には，エージェント間で同期をとって変更処理を行うことも可能にする．

(4) **エージェント間通信機能の確保** 誤まった設定変更がなされた場合でもエージェント間の通信は確保されるように，特定の設定変更後にエージェント間の通信が途絶した場合は，ロールバックにより自動的にエージェント間のコネクションを再確立する機構を用意する．

(5) **主要通信機能の確保** (4)と併せて，メールの送受信，各種DBへのアクセス，マルチキャストデータグラムの配信等，ドメイン間で行われる主要な通信に関して設定変更時にエージェント間で相互にチェックを行い，障害が検出された場合にはロールバックを行う機構を用意することで，主要な通信機能を確保する．

上記の項目の中で，変更実施時に通信機能を確保するためのエージェント間の通信手順等については文献[2]にて検討を行っているので，ここではドメイン間の変更の波及について述べる．

4. 外部に波及する変更の処理

各ドメインにそれぞれ個別の管理者が存在し，独自にドメイン内のネットワーク構成の管理を行っている場

合, 個々の管理者は他のドメインの管理情報の詳細を把握していない. そのため特定ドメインで行われた変更が他のドメインに波及する場合, 変更を行ったドメインの管理者が, 波及先のドメインでどのような変更を実施すればよいのかを把握して, 具体的処理内容までを各ドメインに通知することは困難である. そこで, 各種サーバのアドレスなど, 外部の設定ファイルから参照されるような構成情報の一覧を各ドメイン毎に用意し, その内容を更新するような変更を行う際には, 更新内容 (サーバの新しいアドレス等) を各ドメインに通知するのみにとどめ, 通知を受けたドメインで通知内容に応じた具体的な変更処理を実施することとする. これにより, 外部ドメインにおける構成管理の詳細を把握する必要はなくなる.

他のドメインから提示された上記の構成情報一覧を基に, 必要な設定ファイル群を自動生成・変更する機構を用意すれば, 前節 (3) のエージェント間で同期をとっての自動的な変更処理も可能となる. 実際上, 外部に波及するような変更はさほど多くはないので, 既存のネットワークにおける各種設定ファイル内で, 外部ドメインの情報を参照している部分を全て抽出することで, 変更処理の自動化機構を各々のドメインに用意することは十分に可能と考えられる.

5. システムの構成と動作概要

図1に示すように, バージョン管理用のリポジトリを各ドメイン毎に配し, 管理対象とする設定ファイル群の所在等の情報を記述したファイルを用意して, これをもとにリポジトリへのデータの登録, ネットワーク上へのデータの復元を行う. また各ドメインで用いられる記述ファイルとは別に, 前述の外部ドメインが参照する情報の記述ファイルを用意し, 外部に波及する変更に対処する. ルータ等の管理対象に関しては誤設定時にも管理ホストからのアクセスを可能とするために, コンソール用のシリアルポートを利用し, 管理ホストとの間を内線電話網等を経由した接続も行う.

各ドメインにおいて実施される設定変更は各ドメインの管理ホストで一元的に行うものとする. 管理者はリポジトリから最新の設定ファイルを取り出して変更を加えたのち, 管理ホスト上で更新処理を起動する. ここで, エージェントが他のドメインのエージェントと連携し, 変更通知, 動作確認, 新規データのリポジトリへの登録, 変更前へのロールバック (障害検知時) を行う.

6. 考察

障害発生時に, 直近に行われた変更をキャンセルして正常時の構成を復元することは容易であるが, 障害の検出が遅れることにより, 障害とは関係のない種々の変更が既に実施されている場合は復元処理が単純には行えない. この場合, 単純に取り消したい変更の前の時点の

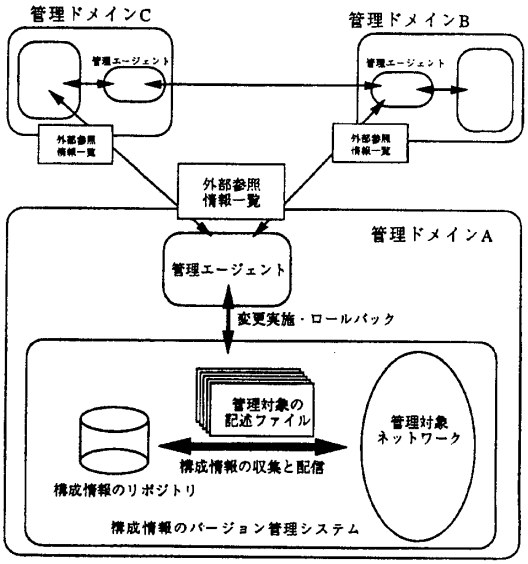

図 1: システム構成図

構成を復元させてしまうと, 後に実施された, 障害とは関係のない変更も取り消されてしまう. 取り消したい変更の差分のみを取り出して, 最新の設定ファイル群に対しリバースパッチをあてることなどが方策として考えられるが, リバースパッチが正常に実施できる保証はない上, 場合によっては後に行われた変更に影響を与えることもありうる. そのため, 過去に行われた特定の変更のみをキャンセルする場合, その処理を完全に自動化することは難しく, 管理者の介在が不可欠である. ただしこの場合でも過去の構成情報や変更の差分を取り出して調べることが可能であるので, 障害対応は容易になっている. 基本的にロールバック処理は, 変更実施時にエージェント間通信によって即時に障害が検出された場合の対応として行うものとし, その他の場合には正常時における構成情報や変更差分を提示することで, 管理者による原因の調査と障害対応を容易にすることを主眼としたサポートが現実的であり, かつ効果的であると考えられる.

7. おわりに

本稿では, 分散配置したエージェントを用いて行うバージョン管理機能をベースにしたネットワーク構成管理手法について検討した. 最後に日頃御指導頂く KDD 研究所 村上所長に感謝します.

参考文献

[1] 窪田 他, "ネットワーク構成のバージョン管理システムの一試作", 信学技報 IN-95-151, (Mar.1996).
[2] 浅見 他, "LAN 構成管理における分散バージョン管理プロトコルの検討", 情報処理学会第 53 回全国大会, (1996).