論 文 の 内 容 の 要 旨

論文題目　Study on Effective Network Management for Enterprise Networks
企業網におけるネットワーク管理の効率向上に関する研究

氏名　　浅見　徹

ネットワーク管理システムは，電話交換網全盛の Telecommunications Management Network（TMN)以来の伝統のあるテーマである．代表的な OSI 管理では，ネットワーク管理を，(1)障害管理，(2)課金管理，(3)構成管理，(4)機密管理，(5)性能管理の五つにカテゴリー分けし，主としてネットワーク管理の機能分類や管理プラットフォームを中心に研究がなされてきたが，現実のネットワークの運用では，これらは相互に密接に関係しているため，マルチベンダー化した通信機器を組み合わせて新規サービスに迅速に対応しなければならないインターネット時代には，これだけではネットワーク管理の効率化には結びつかなくなっている．実際に ISP（インターネット・サービス・プロバイダ）や企業網の管理では，複数の部署や運用技術に差のある運用者が連携して，多様な機器の設定を行っているが，同一企業内でも複数の管理ドメインに分かれインタフェース上の不整合や運用の一貫性がないこと，運用知識の継承ができないことから少数の運用者に依存した体制になっていることが多い．近年，ルール・ベース・システムが，ファイヤーウォールや SPAM メールのフィルタに広く利用されるようになり，大規模ルール・ベース・システムに由来する誤設定の危険も払拭できない．このように，ISP や企業におけるネットワーク管理の実態は，労働集約的であり，構成ミスや機器の追加，運用ポリシー変更に伴い，たゆまないネ

ットワークの改修・改善作業が不可欠となっている．一方，主要な管理プロトコルであるＳＮＭＰは，アーキテクチャ上，制御プレーンとデータ・プレーンが分離していないことから，ネットワークリソースが潤沢でない企業網では特に，障害時にネットワーク運用の可制御性が保障できないことも問題となる．また，TMN 等では重視されていないが，ネットワーク管理においては，ユーザとの窓口であるヘルプデスクの役割は重要であり，この効率向上は，即，管理全体の効率向上にもつながる．上記を踏まえ，本研究では，多岐にわたるネットワーク管理の中で，企業網におけるネットワーク管理の効率化，特に構成管理とそれに関係した障害復旧手順の高速化，ならびにヘルプデスク作業の効率向上を中心に手法の提案と評価を行っている．

第一に，制御プレーンとデータ・プレーンが分離していないＳＮＭＰのアーキテクチャを踏襲しつつ，障害時にネットワーク運用の可制御性を改善する方式の提案をする．ここでは，特に OSI 管理の構成管理作業に起因する障害検出とその復旧方法に絞っている．企業網は，構成変更に伴う障害が多い．既存のルータ等のネットワーク機器では，設定パラメータをファイルに収容し，運用時にファイルを適宜ロードすることによって運用状態を変更できるようになっているものがある．この場合，新しいパラメータセットでの運用時に障害が発生したときに，直ちに前のパラメータセットでの運用に戻し障害が構成管理上のミスに起因するのか，あるいはハードウェア障害等，他の原因によるものかを迅速に判断できる．ここで，ネットワークの運用パラメータを前のバージョンのパラメータセットに戻して運用することを「ロールバック」と呼ぶ．これを個々のネットワーク構成要素だけでなく，ネットワーク全体に一般化し，ネットワークの運用パラメータの全体をバージョン管理して構成管理に起因する通信障害から効率よく復旧することを目指す．このため，分散バージョン管理の概念を導入し，通信障害時に被管理機器群が同値関係を持った部分集合に自動的に分割され，構成誤りに起因する通信障害から，明確に定義された部分集合単位でロールバックすることにより，非同期処理に伴う二次障害を最小にとどめることができるポーリングベースのプロトコルを提案し，復旧時間の上限がネットワーク規模に対して線形に増加することを示す．また，最大輻輳箇所の管理トラヒック量がネットワーク規模に依らずネットワーク・ノードの周辺ノードの数で決まるアルゴリズムを示した．

第二に，ネットワーク運用者がユーザや初歩的運用者からの種々の問い合わせを受け，回答する際の作業効率の向上を図るため，ヘルプデスクの運用知識の改善方法を提案する．具体的には，ヘルプデスクの問題解決知識を決定木の形で与え，その運用時に問題解決するたびに，回答（決定木の終端ノード）利用回数をカウントアップし，この利用回数（利用率）と元の決定木から，元の決定木と論理的に等価かつ問題解決効率が向上した決定木を得る方式と，その高速化手法，ならびに質問応答間の文脈を考慮した最適化手法を提案した．医療診断のような診断知識を対象とする帰納学習の枠組みの中では，QuinlanのID3に代表される決定木による方法が，有力な学習手法として認められている．決定木による診断（ここではネットワーク運用上の種々の問題に対する問題解決）では，学習に使用す

る問題解決事例の数が多いほど問題解決結果の統計的な信頼性は高くなるが，実際の応用では，あらかじめ十分な量の学習事例を集めておくことが困難な場合がある．一つの解決策として，実際に決定木を問題解決に用いた結果から個々の終端ノードの利用率を求め，それから擬似的な学習集合を生成し，それを元に決定木を再構築して問題解決効率(回答に至るまでの平均検査回数)の良い決定木を得る方法が考えられるが，学習集合を構成する事例に含まれる多くの属性に関して値が未観測となり，既存の学習方式を適用することは難しい． そのため，(1)決定木から学習集合を再構成する際，各属性の値の値域を既知の事例を使って求め，(2)問題解決事例に対する個々の終端ノードN_Lの利用率$P(N_L)$，未観測属性の数，各未観測属性の値域から，生成すべき最小の学習集合の大きさMを求め，(3)終端ノードN_Lに対して$M \cdot P(N_L)$に比例する個数の擬似的問題解決事例を生成し，(4)未観測の属性がある場合は，属性の値が値域を一様分布するよう事例を生成することにより学習集合を再構成し，(5)これにQuinlanのID3-IVアルゴリズムを適用することにより，元の決定木と論理的に等価かつ問題解決効率（ここでは質問応答の回数）の向上した決定木を生成できる．シミュレーション結果では，質問応答回数が平均で６％から１０％削減できる．提案方法では，問題解決知識の効率が，ヘルプデスクの運用に伴って向上する特長があるが，実際の質問応答型の問題解決へ応用する場合，連続する質問(属性値獲得手続き)が，文脈上の制限から分離できないことがある．この問題を解決するため，(6)連続する関連質問を一つの拡張属性としてまとめた上で決定木を再構成し，その後で拡張属性の部分を再展開する手法を提案し，同手法により質問の文脈を保存しつつ効率のよい決定木を得ることができることを示した．

第三に，ネットワーク管理の基本である端末識別子に関して論じている．企業網やＩＳＰでは，プライベートアドレスやダイナミック・アドレスといった接続箇所（前者）や接続時点（後者）に依存したＩＰアドレスで運用されている場合が多い．首尾一貫した端末識別子はネットワーク運用者の日々の管理だけでなく，ヘルプデスクにおけるユーザとの対話の効率向上にも重要である．ここでは，メールの管理ドメインの弁別からスタートしたFQDNがネットワーク管理境界を定めるのに適していることを利用して，インターネット上で一意に定まるFQDN (Fully Qualified Domain Name)を端末識別子に使ってネットワークを管理することを目標に，ネットワークを再構成する．IPv4 アドレス枯渇への対策としてIPv6 が開発されてきたが，Dynamic DNSを拡張したFQDNベースの解決策も可能である．先ず，DHCPサーバとDNSアプリケーションゲートウェイを連携させることにより， FQDNをグローバル端末識別子とするネットワークの構築が可能であることを示す．この構成方法では，IPv4 アドレスをパケット配送ラベルとして用い，FQDNをグローバル端末識別子として使用する．FQDNは論理的には無限の，実装上の制約下でも２０バイト以上が可能であるため，IPv4 グローバルアドレス数 ｘ min(IPv4 プライベートアドレス数，TCP/UDPポート数) = 2.4×10^{14}台の端末を収容可能であり，60 億人の世界人口に比して十分大きく，IPv4 アドレス枯渇を回避できる．端末の数が１００台から２００台という中規模企業網を想定し，

そこでIP電話サービスを行う場合，呼損率 0.1 で 20 アーランのときに 23，30 アーランのときに 32 が必要なグローバルIPv4 アドレスであることから，クラスCのグローバルIPv4 アドレスを持つ企業は，十分な品質のIP電話が可能であることが分かる．この方式では，FQDN 管理をするネットワークに属する端末，DHCP，DNS，NATだけに改修が限定されること，移動端末への拡張も，ホーム（移動元）ドメインのDNSサーバ，DHCPサーバ，NATと移動先ドメインのDNSサーバ，DHCPサーバ，NATの拡張をするだけで対応が可能であり，必要なところから逐次ネットワークを改変することで対処できるメリットがある．欠点は，比較的小さなトラヒック（2.2kbit/s）でNATへのDoS(Denial of Service)攻撃が可能であること，DHCPサーバ固有の問題であるIPアドレス再利用時のセキュリティ・ホールにある．