社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（51）
2005－CSEC－28（51）
2005／3／23

1CD Linux を利用した ネットワークエッジ監視装置の開発

†三浦　健次郎,　†扇谷　篤志,　‡虎渡　昌史

†三菱電機株式会社、　‡三菱電機インフォメーションシステムズ株式会社

企業内ネットワークのＩＰネットワークへの統合が進み、その重要性が増した結果、ネットワーク構築技術の高度化が進んだ。一方、現状これらの高度化・複雑化したネットワークを十分に管理するための運用管理技術が開発・適用されているとはいい難い。

本稿では「ユーザ視点」という新たなメトリックの管理情報を既存の運用管理システムに加えることで補完し、運用管理を高度化する手法を提案する。またこの手法の適用にあたり課題となる展開コストの問題を１ＣＤブートＬｉｎｕｘ(KNOPPIX)を利用することにより解決することを提案し、開発したネットワークエッジ監視装置について述べる。

The Development of the Edge Network Management Device By using 1CD Linux

†Kenjiro MIURA,　†Atsushi OGIYA,　‡Masashi TORATO

†Information Technology R & D Center, Mitsubishi Electric Corporation
‡Mitsubishi Electric Information Systems Corporation

Today, an enterprise IP network becomes more important because the wide variety of applications (SNA, VoIP, video streams and so on) are integrated on it. On the other hand, it becomes more difficult to manage because of its growing complexity.

In this paper, we propose the Edge Network Management Device for better network management. It collects the availability and performance information of each client(user) network to the servers. So it's useful for analyzing the extent of a failure impact or warning productivity by response delay. And we have implemented these management functions on CD bootable Linux (KNOPPIX) for deployment cost reduction.

1. はじめに

今日、企業ネットワーク（ＩＰネットワーク、ホスト基幹網、電話網）はＩＰネットワークへの統合が進み、同一のネットワーク上にメールやＷＥＢなどのベストエフォート型のトラフィックのみならず、ホストコンピュータやＶｏＩＰ等の遅延やジッターなどの影響を受けやすいシステムのトラフィックも流れるようになってきている。

このように様々なシステムが統合されたネットワークにおいて、障害や通信品質の劣化がおきるとその影響は大きくなる。すなわち、システム停止により直接的な損害の発生や対外的な信用の毀損が生じ、性能劣化により生産性の低下が生じる。このためネットワーク構築に際しては高可用性や通信品質を確保するための様々な技術が取り入れられてきている。

また、一定規模以上の企業システムでは安定稼動管理のために、既にネットワーク管理システムを導入している場合が多い。

しかし、現状のネットワーク管理システムには次のような課題がある。

①障害の影響範囲や原因の迅速な把握が困難

システムの冗長化、仮想化が進み、従来のように単一サーバの稼働監視に対応付けて、業務システムの可用性を把握しにくくなっている。現状の運用管理の現場では機器故障を検出することが中心であり、ある障害によってユーザにどのような影響が及んでいるのかを迅速に把握しにくいという課題がある。

②ユーザからみた性能管理が不十分

現状の性能管理はルータやサーバのＣＰＵ使用率や回線使用率等のシステムリソース監視が主眼であり、ユーザがどの程度のレスポンスでシステムを利用できているのかを定量的に把握できていない場合が多い。

そこでこれらの課題を解決するために、ネットワークシステムをユーザ視点から監視するための分散監視装置（ネットワークエッジ監視装置）を開発した。本稿ではその内容について述べる。

具体的には、２章においてモデルネットワークシステムを想定（定義）し、現状のネットワーク運用管理方法と課題について整理する。次に３章で２章で明らかにした課題の解決策を検討し、４章で検討結果に従って開発した本監視装置の内容について説明する。最後に５章で今後の課題等について述べる。

2. 背景

2.1. 監視対象ネットワーク

最初に監視対象ネットワークのモデル構成を説明する。本稿では図１のようにデータセンターを中心に複数の支店が広域網（ＷＡＮ）を介して接続される形態を想定する。

近年ブロードバンド化の進展によりWANが高速化し、距離による料金格差も小さくなってきている。また、サーバはデータセンターに集中化した方が運用管理費用の削減が可能となる等の理由でこのようなネットワーク構成が増加している。

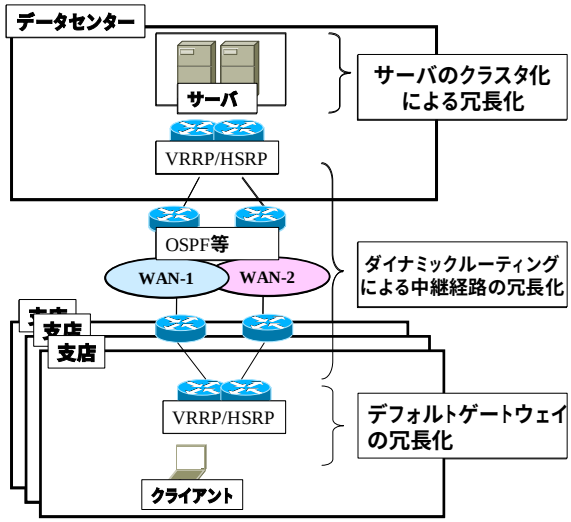
システムリソースである、サーバやネットワークについて見ると、サーバはクラスタ化技術により、ネットワークはOSPF[1]を初めとするダイナミックルーティング技術やVRRP[2]、HSRP[3]等の冗長化技術により高可用性が確保されている（図１）。すなわちシステムは単一故障点を排除するように設計されている。

また、業務アプリケーションはＷＥＢ３階層化設計の適用が進み、複数のサーバ（ＷＥＢアプリケーションサーバ、ＤＢサーバ）が連携して１つの業務システムが成立する構成が増加した。さらに電話のＩＰネットワークへの統合も進んでいる(VoIP)。

2.2. 現状の運用管理と課題、要件

次に運用管理の現状を整理する。ネットワーク管理は一般に①構成管理②障害管理③性能管理④機密管理⑤課金管理に分類できる。

このうち、④機密管理及び⑤課金管理については各組織のポリシーに依存し一般化しにくいので本稿では扱わない。以下、構成、障害、性能管理について現状の運用管理の課題と求められる要件をそれぞれ検討する。



VRRP:Virtual Router Redundancy Protocol(RFC 3768)
HSRP:Hot Standby Router Protocol(Cisco)
OSPF:Open Shortest Path First(RFC2328)

図 1 監視対象ネットワーク

①構成管理

多くの統合運用管理製品ではSNMPのMIBを利用することによって、ＩＰネットワークの論理的な接続や機器構成（機器のインターフェース数等）を検出し、グラフィカルマップに表示することができる。

しかし、統合管理装置はネットワーク全体を対象にするものであるため、監視対象機器（特にネットワーク機器）が増加するとマップで状況を視認しにくくなる。また、高可用化されたシステムでは単一故障があっても動作上問題ない場合があり、判断が難しい場合もある。

従って、統合管理装置で収集した構成管理情報やその他の補完情報を、様々な側面から分析・表示する機能が望まれる。例えば、ネットワークレイヤ毎に可用性を表示したり、ユーザ側のセグメントからみた可用性の視点で構成管理マップを表示する機能が考えられる。

②障害管理

現状は、ルータやサーバ等のインターフェースに対して周期的に(ICMPやSNMP等で)ポーリングを行い、そのレスポンスの有無により障害を検出する方法がとられる場合が多い。

この方法でポーリング対象の障害は検出できるものの、障害によってどのような影響が及んでいるかについて迅速に判断することが困難な場合が多く

なっている。監視対象の冗長化、仮想化、により物理的な機器との対応付けが単純でなくなり、障害時に出るメッセージの解釈が難しくなっているからである。特に大規模なシステムにおいては、障害の影響範囲の切り分け迅速化は重要課題である。

③性能管理

現状は、ネットワーク機器やサーバから SNMP 等を使ってＣＰＵ・メモリ利用率、回線使用率等をモニタリングし、システムリソース（サーバ、ネットワーク機器、回線）不足が生じていないことを監視しているのが通常である。これらの情報により、性能遅延の原因分析を行うことは可能である。

しかし、性能管理の目的はクライアント側でのレスポンス悪化によって業務効率が落ちていないかという点を監視することにある。現状は回線使用率やＣＰＵ利用率からクライアント端末でのレスポンス値を類推しているに過ぎない場合が多い。

また、VoIP 等、エンド・トゥ・エンドでの遅延やジッターを一定品質に保つことが重要なシステム[4]も増えていることから、ユーザ側で通信のレスポンス値を実際に計測し、ユーザ視点で性能を定量的に把握することが重要になりつつある。

3. 課題を解決する運用管理方式の検討

２章で検討したように、構成管理及び障害管理については、障害時の影響範囲を迅速に特定する方法が課題であった。また、性能管理については、ユーザ視点での性能監視が課題であった。これらの課題に対しては以下のような方式による対策が考えられる。

①イベントコリレーション方式

本方式はイベント間の相関関係をパターン定義しておき、一連の障害イベントシーケンスが定義パターンに当てはまるかどうかをチェックすることで、障害分析を自動化する機能である。

障害時に発生するメッセージ間には一定のパターンがある場合がある。例えば、ルータの故障によりサーバのセグメントへの到達性がなくなった場合、「ルータ障害」メッセージの他にそのセグメントの「サーバ障害」メッセージが出る。このような場合、根本原因の「ルータ障害」メッセージのみ表示するとととともに、関連する部分をマップ表示できると、状況把握しやすくなる。但し、イベントの相関関係の定義が難しくなりがちである。

②オブジェクト間の依存関係チェック方式

冗長化ルータ（VRRP/HSRP）などのような冗長構成の系では片系が故障しても、ユーザは継続してシステムを利用することが可能である。このように複数の機器で１つの機能が構成される場合、その関係をネットワーク管理の構成データベース中に保持しておけば、障害時にその関係をチェックすることにより影響度の判断を迅速化できる。監視対象オブジェクト間の関係定義の方法や、関係をどうやって自動検出するかを検討する必要がある。

③クライアント側からの監視方式

クライアントネットワーク側にも監視装置を配置し、ダミーパケットをサーバ等に送信することで、クライアントエリアからのサーバの稼働確認や応答時間を監視する方式である。本稿の監視装置はこの方式を採用している。方式としてはシンプルだがクライアント側に監視装置を設置することで、データセンター側で収集できないエンド・トゥ・エンドの監視情報を収集することができる利点がある。

①、②のアプローチはシステム側からの監視アプローチの高度化で、障害影響度分析において有効であるが性能監視の課題はこれだけでは解決しにくい。

一方、③のアプローチは、ユーザ側からの監視アプローチでシステム側からの監視だけでは収集が難しかった、構成・障害管理情報（ユーザ側からみたシステムの構成・可用性）、性能管理情報（ユーザが体感している応答性能）を収集することができ、従来のシステム側からの運用管理情報と補完的に使うことで運用管理の高度化を目指すアプローチである。ここで多数の監視装置を分散配置する場合に如何に展開コストを抑えるかが問題である。

ソフトウェアのみで監視機能を実装し、これを各サーバ等にインストールして使う方法も考えられるが、①インストール作業が発生する、②インストールＯＳ毎に各バージョンを用意しなければならない③インストールするマシンが兼用マシンだとマシン高負荷時に計測誤差が生じることありうる、等の問題が考えられる。

そこで、ＣＤブートＯＳ(KNOPPIX[5])を使って各監視機能を実装することを検討した。

ＣＤブートＯＳを使うと、①インストール作業自体が不要になる（ＣＤを複製するのみで良い）、②設置作業のノンインテリ化が可能になる（電源を入れるだけで監視機能が動作するようにカスタマイズ可能）、③監視専用になるので他のソフトの負荷の影響を廃除可能、④予め動作環境を定めて試験ができるので監視機能の品質保証がしやすくなる、等のメリットが考えられる。

欠点としては、ハードウェア等のコストがかかる

ことだが、低価格ＰＣとオープンソースを利用することでコスト削減することにした。また、エッジ管理装置によるトラフィックの増加は、ブロードバンド化が進んでいるため対処可能であると考える。

4. CD ブート Linux を利用したエッジ監視装置

4.1. 概要

本章では開発したエッジ監視装置について説明する。

①監視システムの全体構成

まず、エッジ監視装置のシステム内での利用形態は図２の通りである。大規模なネットワーク全体のシステムリソースの監視はデータセンター側の統合監視装置を使う。図２の支店側（エッジ側）に開発した監視装置を設置し、ユーザ側からも監視情報を収集することで、統合監視装置を補完する。

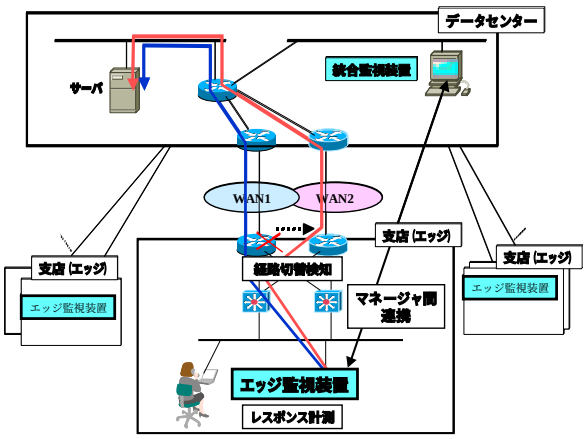


図 2 監視システム全体構成図

②エッジ監視装置の構成

エッジ監視装置のハードウェアは開発段階では低価格のＰＣを利用して行った。参考までに開発マシンの仕様を表１に示す。

表 1 開発マシンの仕様

CPU	Pentium4 266GHz
メモリ	512M byte
FDD	3.5 型　内蔵 FDD
CD-ROM	24 倍速
HDD	なし
NIC	10/100 Base-T
I/F	USB 2.0 x 2port
BIOS	CD ブート対応

OS は前述の通り、KNOPPIX をベースしてカスタマイズを行った。監視用のデータベースとして PostgreSQL を、SNMP のライブラリとして Net-SNMP を利用している。

これらの OS やミドルウェア上に運用監視プログラムを開発した。運用監視用のＧＵＩはブラウザを利用する仕様とした。

また、運用時には監視対象とするサーバのＩＰアドレス等の設定情報を与える必要がある。これらの設定情報は設置場所によって異なるため、内蔵のフロッピーディスクから読み込むことで対応することにした。

また、ＭＴＢＦ向上のためハードディスク無しの構成をデフォルトの構成としている。これにより、監視装置を設置する場合に、現地では必要なメディア（FD,CD 等）をセットして電源を入れるだけでよく、運用管理について特に知識がなくても設置作業が可能となる。

4.2. 機能

次に主な監視機能を説明する。

①構成・障害管理機能

本監視装置は統合監視装置を補完する使い方が主な使い方になるが、各クライアントエリア内でも簡易な障害監視ができるように、構成管理マップと障害監視用のイベントブラウザを開発した。

障害により発生したイベントはこの「障害監視ブラウザ」の機能により監視することができる。

図３は障害監視用ＧＵＩの例である。障害の発生日時、発生したホスト名（ＩＰアドレス）、内容、重要度、対応状況等をＷＥＢブラウザで確認することが可能である。

図 3 障害監視用 GUI 例

②経路監視機能

サーバのホスト名（又はＩＰアドレス）を設定することで、監視装置から指定したサーバまでの経路を定期的にICMPで探索し、結果をデータベースに保存する機能である(tracerouteと同様の機能)。

また、ルータ等の故障によりサーバに到達できなくなった場合や、代替経路に切り替わった場合に、経路の状態変化を上位の監視装置にを通知することができる(SNMP-TRAP)。

統合監視装置側では、通常ルータ等の機器故障を検出できるので、各クライアントネットワーク側からみた経路変化の情報や可用性情報を合わせることで影響をより詳細に把握することが可能である。

また、ルータのソフトウェアのバグや設定ミス等の原因によって、経路のフラッピング（不安定化）が起こるような障害も検出が容易になる。

図4は経路監視用の画面例である。RIPを使ってダイナミックルーティングネットワークを構築し、10秒単位でサーバまでの経路監視している。RIPの場合収束が遅いため、経路が一旦切れた後、代替経路に切り替わっていることがわかる。

図 4 経路監視画面の例

③応答性能監視機能

ユーザが使っているサーバのレスポンスを計測する機能である。計測対象はIPアドレス又はURLで指定し、ＩＰ層レベルの遅延(ICMP)とアプリケーションレベルの遅延(HTTP)を計測することができる。また、一定のしきい値を超えた場合に上位の監視装置に通知する（SNMP-TRAP）ことも可能である。

この機能により、エンド・トゥ・エンドの遅延を定量的に把握することが可能になり、SLA(Service Level Agreement)違反を検出しやすくなる。また、統合監視装置等で収集するシステムリソース情報（ルータ・サーバのＣＰＵ使用率、回線使用率等）と合わせることで、因果関係の分析が容易になる。

図５は応答性能監視機能の画面例である。

デフォルトではPINGとHTTPをサポートしているが、その他のプロトコルについても必要ならば追加は可能である。

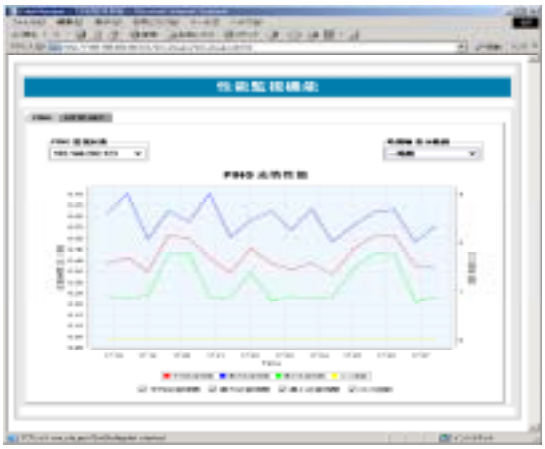


図 5 性能監視 GUI の例

④その他の機能

回線の使用率等をSNMP MIBを利用して表示する機能等のMIBアプリケーションを開発した。但し、標準MIBでカバーできる範囲には限界があるため、実際には各ネットワークに導入されている機器の拡張 MIB を利用してカスタマイズしていく必要があるだろう。

また、収集したデータをローカルの USB メモリに保存するコマンドなど、管理コマンド群も開発した。デフォルトではハードディスクレスの構成にしており、データをDRAM上にのみ保持しているが、USB メモリ等にバックアップすることも可能である。

⑤KNOPPIXのカスタマイズ

KNOPPIXで行ったカスタマイズは、起動の自動化、リモートからの認証機能の追加、設定情報の読み込み部分、ＧＵＩデスクトップ等の不要機能の削除等である。

4.3. 評価

現在、実装が終わり、試験用ネットワークでテストしている段階である。

ＣＤブートＯＳを使うことによって、監視機能の動作に支障がでることを懸念したが、特に問題は出ていない。

ブートには多少時間がかかるものの（２～３分程度）、ＧＵＩも含めて各機能は問題なく動作している。また、監視装置自体のＣＰＵ負荷も表１のハードウェア構成では、低負荷である。今後、ポーリング対象や周期を増減させた場合のＣＰＵ負荷、メモリ使用率等の性能を定量的に計測する予定である。

さらに、ＣＰＵや搭載メモリの削減などコスト削減に向けたチューニングや実システムへの適用検討などを行って行く予定である。

5. おわりに

本稿では、クライアント（エッジ）側のネットワークに監視装置を設置し、エッジ側からみた可用性や経路の状態、応答性能を監視・計測することでネットワーク運用管理の高度化を図ることを提案した。

また、このような監視機能をソフトウェアのみで実装し、端末にインストールする方法では展開時にコストがかかる等のデメリットが考えられるため、CD ブート OS 上に実装し、インストールや設置作業をノンインテリ化し、展開時のコスト低減化を図ることを提案した。

さらに、実際に機能を実装し試験環境でＣＤブート方式の監視装置で実用に耐えうることを確認した。

今後は、統合管理装置とエッジ監視装置の連携を緊密にし、エッジ監視装置で収集した情報を有効活用する方式の検討など、さらなる運用管理の高度化について検討していきたい。

また、実用化、製品化にあたってはオープンソースのライセンスの検討やコミュニティへのフィードバックなども検討課題であると考えている。

参考文献

1) F. Baker, R. Coltun,”OSPF Version 2 Management Information Base.”, IETF RFC1850, Nov 1995.
2) R. Hinden, Ed.. April, “Virtual Router Redundancy Protocol (VRRP). “, IETF RFC3768, Apr 2004
3) T. Li, B. Cole, P.Morton, D. Li., “Cisco Hot Standby Router Protocol (HSRP).”, IETF RFC2281, Mar 1998.
4) 総務省：「IP ネットワーク技術に関する研究会報告書」3 章.IP 電話の品質(平成 14 年 2 月 22 日), http://www.soumu.go.jp/s-news/2002/020222_3.html
5) KNOPPIX Japanese edition, http://unit.aist.go.jp/itri/knoppix/index.html