アプリケーションレベルの
リモートネットワーク監視システムの研究開発

富士通エフ・アイ・ピー株式会社

■ 執筆者Ｐｒｏｆｉｌｅ ■

髙　橋　浩　二

1997年　富士通エフ・アイ・ピー株式会社入社
製薬業市販後調査支援パッケージシステム
設計・開発を担当

■ 論文要旨 ■

従来のネットワーク監視システムには監視プロトコルの制限，パケットの詳細分析そしてリモート監視といった問題点及び課題がある．そのため，適確なネットワーク監視及び現状分析を行うには高価な専用ハードウェアや専門知識を必要とする．

そこで安価かつ容易にネットワークの監視・現状分析を行うために，ソフトウェアのみによる監視システムの実現性を検討し，三つの重要な技法を考案した．ネットワーク上を流れるすべてのパケットをキャプチャする方法，キャプチャしたパケットをアプリケーションレベルまで分析する方法そしてリモート監視を容易に実現する方法である．

上記三つの技法を組み込んだプロトタイプを用いての検証実験によって，全パケットのキャプチャ，パケットのアプリケーションレベルの分析そしてリモート監視がソフトウェアのみで実現できることを検証した．

今後は本技法のサービスビジネスへの適用や関連技術への応用を行いたいと考える．

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

近年における，ハードウェアの低価格化，ネットワーク機能のOSへの標準的な搭載によって，ネットワークが一般的に利用されるようになった．これに伴い，ネットワークを利用する情報資源は爆発的に増大し，システム管理者によるネットワークの維持活動が重要視されるようになった．しかし，維持活動におけるネットワークの現状分析には，高価な専用ハードウェアや専門知識が要求されるため，現実的には適確な分析が実施されているケースは少ない．これらの社会的背景をふまえ，より安価に簡便にネットワークのふるまいを分析するツールについて研究開発を行った．

２．目的

安価にネットワークの現状分析を行うために，情報収集から収集した情報の分析までのすべての機能を，専用ハードウェアを用いずに，ネットワークに接続されたパソコン上で動作するソフトウェアとして実現する．また，適確なネットワークの現状分析を行うためには，情報収集及び収集した情報の分析を詳細に行うことが重要である．更に，WANなどを利用した大規模ネットワークが一般的になっているため，リモート機能も必要と考えられる．したがって，本研究開発は以下の機能要件を満たすための技術について検討を行い，その技術を用いた監視及び情報収集システムを構築し，その有効性を検証することを目的とした．

（1）すべてのプロトコルのパケットが監視できること
（2）アプリケーションレベルまでパケットが分析できること
（3）大規模LANやWANでもリモート監視，情報収集ができること
（4）上記機能をソフトウェアのみで実現すること

３．問題点及び課題

前章で述べた機能要件を満たすシステムを構築するにあたり，そのシステム構成やネットワーク形態に起因する問題点，そして前章で述べた機能要件を満たすための課題について検討を行った．それらの問題点及び課題を以下に示す．

・監視プロトコル種別の制限
　ソフトウェアで構成される監視システムにおいて，既存のプロトコルドライバの上にシステムを構築すると，監視できるプロトコルがプロトコルドライバに依存してしまう．
・パケットの詳細分析
　一般的に，プロトコルごとのトラフィック量の分析だけでは障害の原因特定ができない．利用アプリケーション，利用端末ごとに分析できるツールが必要となる．
・大規模ネットワークのリモート監視及び情報収集
　ネットワーク監視及びネットワークの詳細な情報収集をリモートで行う機能は，今日の一般的なネットワーク形態を考えると必須である．また分析にかかるコストを低減させるためにも有効と考える．

3．1　監視プロトコル種別の制限

ネットワーク上を流れるTCP/IPやNetBEUIなどさまざまなプロトコルのパケットは，NIC[1]ドライバがプロトコルに関わらずキャプチャし，その上位層のプロトコルドライバが必要なパケットのみ更に上位層に伝達する（**図１：A**）．このプロトコルドライバは，主にハードウェアベンダやOSベンダがプロトコルごとに用意している．通常，監視システムはプロトコルドライバの上位に位置するため，キャプチャできるプロトコルが限定される．この結果，ドライバが組み込まれていないプロトコルに起因するネットワーク障害が発生した場合，監視システムは原因を追求することができない．

3．2　パケットの詳細分析

仮に障害の原因となっているプロトコルに対応したドライバが組み込まれていたとしても，IPのように複数のアプリケーションで使用される汎用プロトコルの場合，アプリケーションレベルで障害原因を特定する必要がある（**図１：B**）．また，ネットワークの現状分析の面でも，より詳細なネットワークのふるまいを監視かつ分析する必要がある．

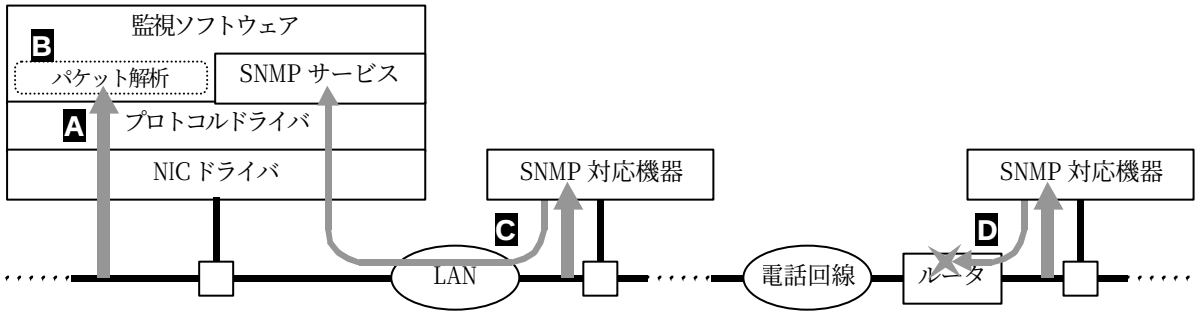


図１　従来の監視システムの構成と問題点

3．3　大規模ネットワークのリモート監視及び情報収集の問題点

大規模ネットワークはルータによって複数のセグメントに分割されている．このため従来の監視システムは，各セグメントに点在するSNMP[2]に対応したネットワーク機器のMIB[3]情報を収集することによりリモート監視を行う構成となっている（**図１：C**）．ここで，MIBの項目は標準MIB項目とネットワーク機器ベンダが自由に機能拡張できる拡張MIB項目があるが，監視システムとルータのベンダを統一するか，もしくは拡張MIBをカスタマイズしなければ有効活用することができない．またMIBに格納される情報自体も通常は概略程度に抑えられ，現状分析が行えるほどの詳細さを持ち合わせていない．またWANを介した遠隔監視において，専用線を用いている場合は問題ないが[4]，電話回線を用いている場合，SNMPパケットで常時ネットワーク情報を収集することは適当でない（**図１：D**）．専用ハードウェアをセグメントごとに配置することによりWANにおけるリモート監視を実現している製品もあるが，専用ハードウェアゆえに，新しいネットワーク技術への対応が困難など柔軟性の低さや監視コストの増大は避けられない．

---

[1] Network Interface Card．パソコンなどのネットワーク機器とネットワークを接続するための機器．
[2] Simple Network Management Protocol．ルータなどのネットワーク機器の監視や制御を行うプロトコル．
[3] Management Information Base．SNMP 対応ネットワーク機器の持つ，自身の動作状況や管理情報を格納したデータベース．この情報の伝達を SNMP で行う．
[4] 利用者の運用規定により SNMP パケットを WAN に流さない場合もある．

４．システムの検討

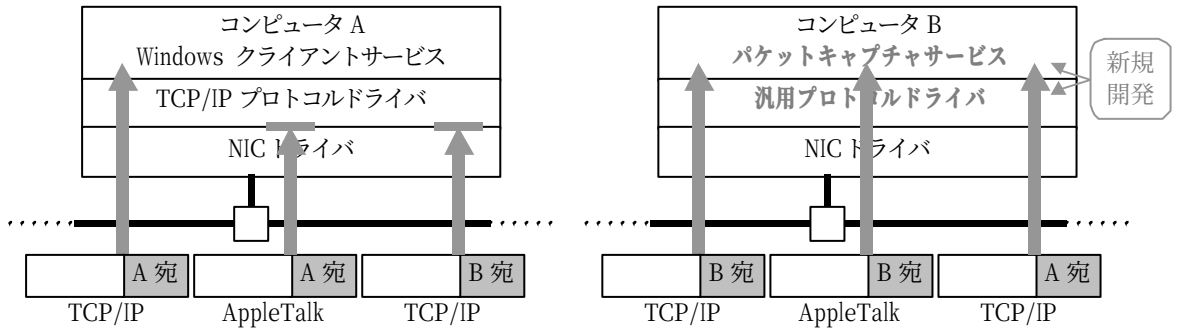
前章で述べたように，既存システムには監視プロトコルの制限，より細かなパケット分析機能の不足，そしてリモート機能の欠如という三つの問題点や課題が考えられる．それらを克服するための解決策について検討を行った．

・汎用プロトコルドライバ
　既存のプロトコルドライバを用いるのではなく，いかなるプロトコルのパケットでもキャプチャできる汎用的なプロトコルドライバを開発し，その汎用プロトコルドライバ上にシステムを構築する．
・パケット詳細分析機能
　上記汎用プロトコルドライバでキャプチャしたパケットの，ヘッダ並びにペイロード上の上位プロトコルヘッダを解析することにより，利用アプリケーションや利用端末の分析を可能とする．
・通信プロトコルを適宜切換えるリモート監視及び情報収集機能
　監視結果などの情報収集を行うにあたり，新システムはエージェント－マネージャ連携の形態を採用する．そして，間に介在するネットワークアーキテクチャに柔軟に対応できる情報伝達方法を考案する．

４．１　汎用プロトコルドライバ

図２（Ａ）に示すように，既存のプロトコルドライバは，ドライバ固有のプロトコルのパケットしかキャプチャを行わない．ネットワーク上を流れるパケットを余さずキャプチャする機能は監視システムとして必須の機能であるが，既存ドライバをキャプチャ機能が用いる場合，監視対象プロトコルのドライバをすべてコンピュータに組み込む必要があり，現実的とはいえない．そこで一つのプロトコルドライバで複数プロトコルのパケットをキャプチャできる汎用プロトコルドライバの開発について検討を行った．

物理ネットワーク上を流れる電気信号化された情報は,NICとそのドライバによりデータリンク層のフレームに変換される．通常のプロトコルドライバは，このフレームをネットワーク層のデータグラム，更にトランスポート層のパケットに変換する過程で，対象とするプロトコルのパケットのみを上位サービスに伝達する．ここで，図２（Ｂ）のようにすべてのプロトコルのパケットを上位のサービスに伝達することで，汎用的なプロトコルドライバとしての機能を実現することができる．



（A）通常のパケットキャプチャ　　（B）今回開発したパケットキャプチャ

図２　通常のパケットキャプチャと今回開発したパケットキャプチャ

４．２　パケット詳細分析機能

汎用プロトコルドライバが上位サービスに伝達するパケットのプロトコルは，ヘッダ情報を解析することで特定することができる．またパケットのペイロードには，そのパケットの上位プロトコルのヘッダ情報も含まれるため，ペイロードを解析することにより，更に上位のプロトコルも特定することができる．したがって，**図３**のように，階層ごとの分析を繰り返すことで使用アプリケーションの特定まで可能となる．この方法を用いることにより，多くのプロトコルについてパケット別，ポート別，アプリケーション別といったさまざまな切口で，負荷集計などの情報収集（**同図：Ｄ**）を行うことができる．

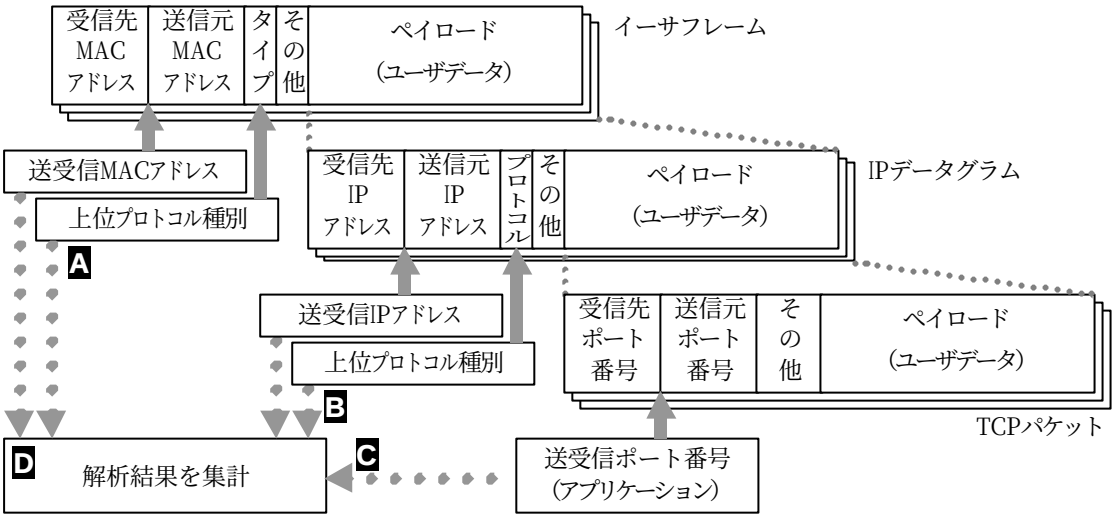


図３　パケットの分析方法

４．２．１　ネットワーク層レベルの解析

イーサネットにおけるデータリンク層のフレームはMACフレームと呼ばれ,そのフレーム形式は二種に大別できる．ISOによって国際標準とされたIEEE802.3形式と，事実上の標準であるEthernet V1及びV2形式である.Ethernet V1及びV2形式のMACフレームは,そのフレームヘッダにE-Typeという領域を持つ．このE-Typeの値を調べることにより，上位層であるネットワーク層でのデータグラムの種別を特定できる（**図３：Ａ**）．IEEE802.3形式のMACフレームは前述の領域を持たないかわりに,SAP値やSNAPという方法でE-Typeと同様の働きを実現しているため，それを解析することによりデータグラムの種別を特定することができる.

４．２．２　トランスポート層レベルの解析

IPまたはIPXをネットワーク層のプロトコルとするトランスポート層のプロトコルの種別は，データグラムのヘッダ情報から容易に特定することができる．いずれのデータグラムのヘッダもトランスポート層でのプロトコル種別を格納した領域を持つので，その値を調べることによりトランスポート層におけるプロトコルを特定することができる（**図３：Ｂ**）.

４．２．３　送信アプリケーションの特定

IPをネットワーク層のプロトコルとするデータグラムの宛先はコンピュータであり，パケットの宛先はポート番号というアプリケーション固有の番号であるため，このポート番号によりアプリケーションを特定することができる（**図３：C**）．

４．３　通信プロトコルを適宜切換えるリモート監視及び情報収集機能

WANなどの大規模ネットワークの監視及び情報収集をリモートで行うにあたり，**図４**に示すように新システムはエージェント－マネージャ連携の形態を用いることにした．各セグメントごとに配置されたエージェントは，自セグメントの監視及び情報収集を行い，その結果を集約サーバであるマネージャに送信する．マネージャは，各エージェントより受信したセグメントごとの監視結果及び収集した情報を集約し，リモート監視を実現する．ただし，結果の送受信自体がネットワークトラフィックの増大を招かないように，集計や分析など一次加工をエージェント側で行うことが必要である．

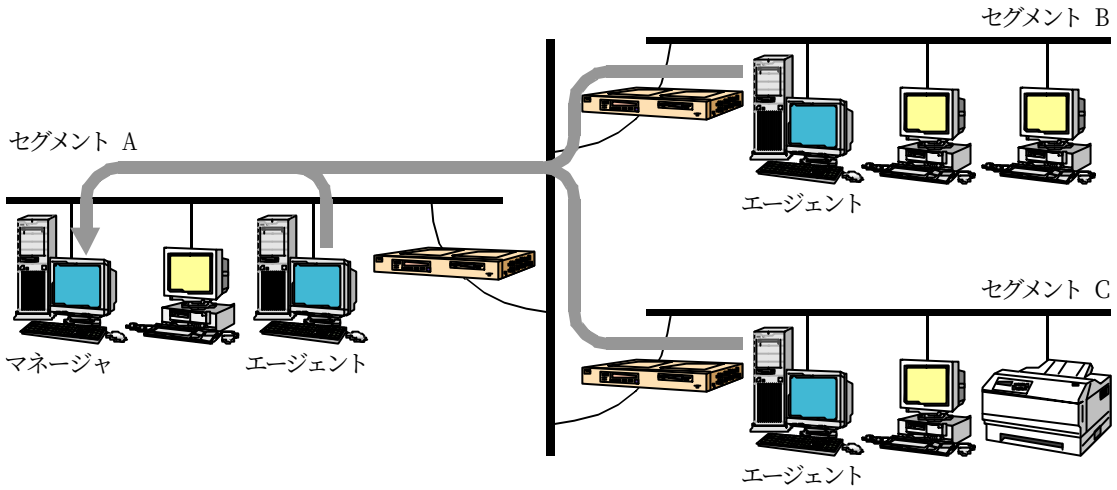


図４　エージェント－マネージャ連携によるリモート監視

ここで，処理結果を送受信するのに使用する通信プロトコルを，エージェント－マネージャ間のネットワークアーキテクチャに応じて柔軟に切り換えることにより，大規模ネットワークにおけるリモート監視を容易に実現することができる．**下図５**のように，例えばルータを経由する場合はSNMP，WANを経由する場合はTCP/IP，インターネットの場合はリアルタイム性は損なわれるが，ファイル媒体に変換した処理結果をFTPでマネージャに転送したり，処理結果をE-mailやHyper Textの形で送信することにより連携を行う．このように，介在するネットワークアーキテクチャによって，情報伝達に用いるプロトコルや伝達媒体を柔軟に切換えることにより，リモート機能が実現できる．

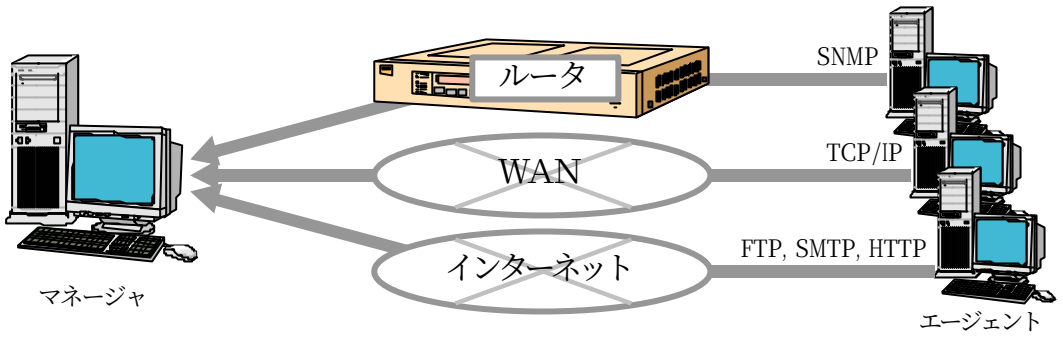


図５　介在するネットワークアーキテクチャに応じた通信プロトコル

また,通信プロトコルの選定において,エージェントは自セグメントを流れるマネージャのセグメントからのパケットをキャプチャし，そのプロトコルを解析することで，動的かつ自動的に通信プロトコルを選定することが可能となる．もちろん，あらかじめ決められたプロトコルリストから順番に通信プロトコルを選定し，そのプロトコルを用いた応答要求メッセージをマネージャに送信し，応答が返ってきたプロトコルを通信プロトコルに採用する方法も考えられる[5].

４．４　システム構成

前節までに述べた解決策を盛り込んだエージェント機能のシステム構成は下図６のようになる．エージェント機能では，汎用プロトコルドライバでキャプチャしたパケットをハードディスク上にログファイルとして記録する機能も実装する．このログファイルはトラフィックのふるまいや障害原因の分析，更に障害発生時の状態の再現といった使用方法が考えられる．

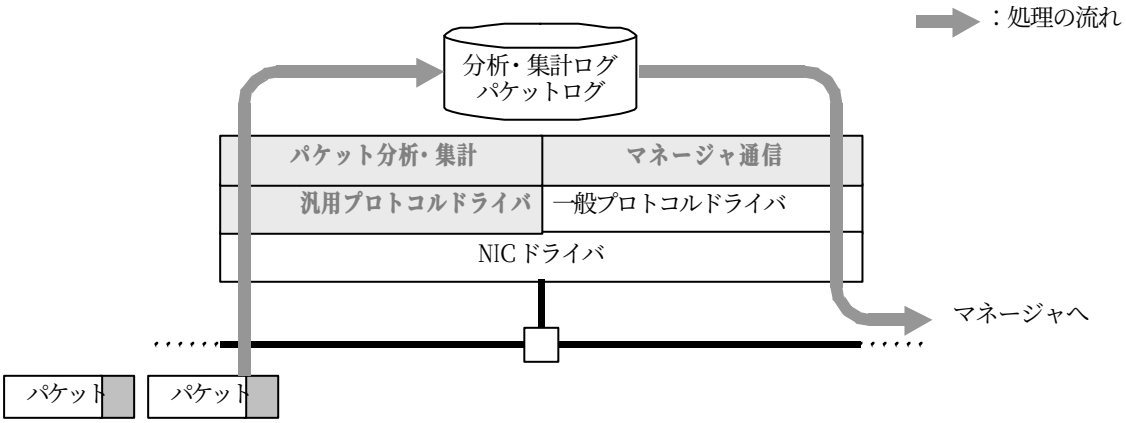


図６　システム構成（エージェント機能）

[5] エージェント－マネージャ連携の監視方式及び通信プロトコルの選定方法について現在特許申請中.（公開番号：特開 2000-194625）

５．システムの評価

４章で述べた解決策を盛り込んだプロトタイプを開発し，実際に社内ネットワークを監視することにより，システムの評価を行った．各解決策の評価方法について以下に述べる．

・汎用プロトコルドライバの評価
　パケットのキャプチャ及び分析の専用ハードウェアである，Sniffer[6]と同時にキャプチャを行い，キャプチャしたパケットの個数及びデータサイズを比較することで，汎用プロトコルドライバ及び，それを用いたパケットキャプチャ機能の評価とする．一見単純な評価方法ではあるが，確実な評価方法である．
・パケット詳細分析機能の評価
　プロトタイプでキャプチャしたパケットの分析結果と，Snifferでキャプチャしたパケットの分析結果を突き合わせて，その機能の評価とする．
・通信プロトコルを適宜切換えるリモート監視及び情報収集機能の評価
　エージェントの一次加工結果つまり収集した情報を，SNMP以外のプロトコルでマネージャに送信し，マネージャ側で受信及び二次加工できるかを検証することにより，リモート機能の評価とする．プロトタイプでは従来のSNMPによる送受信とTCP/IPによる送受信の二種類を用意した．また，マネージャの二次加工として，各エージェントからの受信データの統計的な分析とその表示を行った．

５．１　汎用プロトコルドライバの評価

表1にプロトタイプによるキャプチャ結果と，Snifferによるキャプチャ結果を示す．更に表2にプロトタイプを動作させた端末のマシンスペックを示す．これをみると明らかなように，専用ハードウェアと遜色ないキャプチャ性能を示していることがわかる．なお，プロトタイプを動作させた端末では，コーディングやドキュメント作成といった通常業務も同時に行っていたが，端末そのもののパフォーマンス低下は感じられなかったことも付言しておく．この結果から，２章(１)が実現できたことを確認した．

表１　Snifferとのキャプチャ性能の比較結果

キャプチャ開始時刻	キャプチャ時　間	キャプチャできたパケット数	
		プロトタイプ	Sniffer
09:50	5 分	3235	3235
10:20	1 分	3345	3345
10:50	3 分	8468	8468
10:55	1 分	1919	1919
11:00	1 分	934	934
14:22	1 分	2392	2392

表２　評価に用いた端末のマシンスペック

スペック	
CPU	PentiumPro 200 MHz
メモリ	64 MB
OS	Microsoft Windows98

[6] 米国 Network Associates 社製のパケットキャプチャ及びパケット分析専用ハードウェア．国内では株式会社東陽テクニカ他が販売している．

５．２　パケット詳細分析機能の評価

図７に，あるパケットの分析ログを示す．このパケットはブラウザがWebサイトに接続している状態をキャプチャした時のパケットである．なお，今回の検証実験は社内ネットワークを実際に監視したため，MACアドレスとIPアドレスは伏字とさせていただく．この分析結果より，社内プロキシサーバのポートにパケットを送信していることが確認され，パケットのプロトコル解析が適切に行われていることが確認された．この例以外でも，Snifferの分析結果との照らし合わせにより，パケット分析が正確に行われていることを確認した．

```
==== レコード番号：1152 / 1341 == ドライバシーケンス：49445 ====
  受信時刻：1999/8/28  20:48:55 [120]
  フレーム形式：イーサフレーム V1.2
  ETYPE：0800 ["Internet IP (Ipv4) "]
  Macアドレス：To (xx-xx-xx-xx-xx-xx)  From (xx-xx-xx-xx-xx-xx)
  データ長：382
== IP情報 <<ﾌﾟﾛﾄｺﾙ:: Transmission Control">>==
  Version=4  IHL=5  Length=368
  Ident=0x1ecc  Flag=8  Offset=0
  Time2Live=128  Protocol=6  Checksum=0x86c5
  IP Address
    Source=xx.xx.xx.xx (xx.xx.xx.xx)
    Destination=xx.xx.xx.xx (xx.xx.xx.xx)

 === TCP情報 ===
  Source Port=3719 ()
  Destination Port=8080 ( Proxy port")
  Sequence Number=25479790
  Acknowledgment Number=352395709
  Offset=5  CodeBit=18 (...-ACK-PSH-...-...-...)
  Window=14392 (0x2238)  Checksum=0x39d3  UrgentPointer=0 (0x0000)
  Option=0x47455420

    0000 : 68 74 74 70 3a 2f 2f 77   77 77 2e 61 73 61 68 69
    0010 : 2e 63 6f 6d 2f 69 6d 61   67 65 73 2f 6e 65 77 73
    0020 : 5f 75 70 64 61 74 65 5f   74 69 74 6c 65 5f 4c 2e
    0030 : 67 69 66 20 48 54 54 50   2f 31 2e 30 0d 0a 41 63
    0040 : 63 65 70 74 3a 20
```

図７　パケット分析ログ

また，図８に社内の特定セグメントの午後５時20分から午後６時50分までのアプリケーション別トラフィックの分析結果を棒グラフで表示している画面を示す．ちょうどこの時間帯に，大量ファイルのサーバマシンからのダウンロードを行っていたため，トラフィックが上昇している．また，棒グラフの最下層はHTTPパケットのトラフィックを示している．この時間帯は休憩時間でもあるため，社員のWeb閲覧に伴ってHTTPトラフィックが上昇していたことがわかる．このように，アプリケーション別でトラフィック分析を行うことにより，ネットワークのふるまいを詳細に分析することが可能となる．この結果から，２章(２)は達成できたといえる．

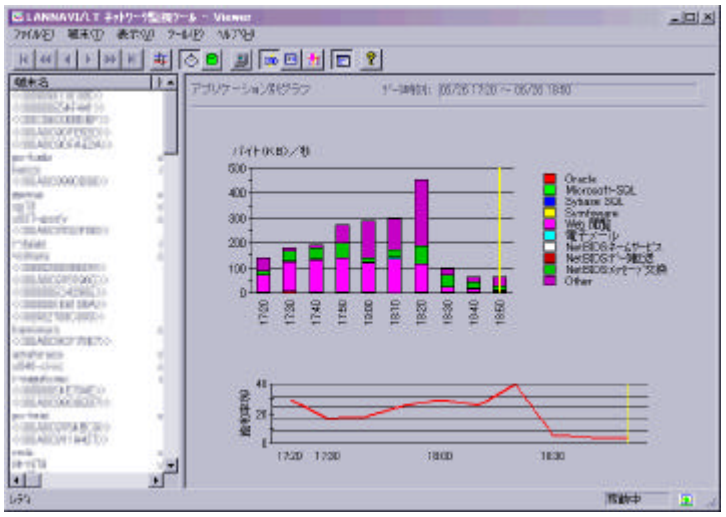


図８　アプリケーション別のトラフィック表示

５．３　通信プロトコルを適宜切換えるリモート監視及び情報収集機能の評価

図９にリモート監視中のマネージャ画面を示す．画面上部にエージェント一覧，下部に各エージェントが監視しているセグメントのサマリー情報を表示している．ここで，エージェント一覧では２台のエージェントが動作していることを示しており，エージェントpc_shiraとはコネクションが確立され，処理結果の送受信が行われている．エージェントlannaviとはコネクションの確立待機中であることが見てとれる．

図９　リモート監視中のマネージャ画面

今回のプロトタイプはSNMPの代わりにTCP/IPを用いて処理結果の伝達を行い，それが正確に処理されていることを確認した．この代替プロトコルを多数用意し，エージェント－

マネージャ間に介在するネットワークアーキテクチャに応じてプロトコルを適宜切換えることで，SNMPを用いなくともリモート機能が容易に実現できることを確認した．更に収集した情報を汎用プロトコルでカプセル化するということは，どんな情報でも伝達できるということである．例えば，キャプチャしたパケットの中身といった詳細情報も，必要なときにマネージャに送信することができる．したがって，2章(３)は達成できたといえよう．

５．４　システム全体の評価

前節までの検証により,パケットキャプチャ機能,アプリケーションレベルまでのパケット分析機能，プロトコル切換えによるリモート機能がソフトウェアのみで実現できることが確認された．ソフトウェアのみでシステムを構築することにより，安価に監視及び情報収集システムが実現できると考えられる．リモート機能を除いたスタンドアロン動作のシステム[7]を先行して発売するが，下表３に示すように，Snifferに比べかなり安価に提供できるようになっている．また，今回検証に用いたパソコンは今日市場に出回っているパソコンに比べると性能的にかなり劣るが取りこぼしは発生しなかった．したがって，CPUビジーの状態にならないような使用頻度の低いパソコンにエージェント機能をインストールすることで，専用のパソコンを設置せずに監視及び情報収集が可能であると考える．ただし，パソコンの性能や負荷状態によるキャプチャ性能の変化について明確な検証を行っていないので，今後の課題としたい．

表３　価格比較(単位　千円)

LANNAVI/LT (ソフトウェア)	Sniffer PT65L-EN 10/100 (ハードウェア)	Sniffer PT26SE-400 10/100 (専用NotePC+ソフトウェア)
50	4，760	2，660

エージェント機能の導入から起動までの手順は，汎用ドライバのパソコンへのインストールと，収集間隔やマネージャの動作しているコンピュータ名といった簡単な動作パラメータの設定だけであり，SNMPの設定のような面倒な操作や専門知識を必要としない．

更にソフトウェアのもつ柔軟性を最大限に生かすことにより，Snifferのようなネットワーク分析ツールとSNMPを必要としないリモート機能の融合が実現可能であることが確認できた．これらの手法を元に，通常はリモート監視システムとして動作し，情報収集を行いたいときには遠隔操作できるネットワーク分析ツールにもなる総合的なネットワーク監視システムの実現が期待できる．

[7] 販売名「LANNAVI™／LT」.

５．５　今後の課題

今後の課題として，現在普及しつつある100BASE[8]のネットワークへの対応があげられる．今回の検証に用いたネットワークは10BASEであったため，取りこぼしがなく良好なキャプチャ性能を発揮することができた．しかし，100BASEのネットワークでどれだけのキャプチャ性能が示せるか，すべてのパケットをキャプチャするのにどれだけの性能がパソコンに要求されるのかを検証する必要がある．

また，今回の研究開発はソフトウェアのみでネットワークの監視及び情報収集を可能とするための方法について検討し，その方法の有効性を検証したに過ぎない．リモート機能を含めた製品版を開発するにあたり，エージェント－マネージャ間のプロトコルの切換えを自動的に行う機能や，収集した情報の多角的な分析，統計的な分析といった現状分析機能をマネージャに付加する必要がある．

更に専門知識を必要としなくなったかという点において，今回の研究開発ではまだまだ不十分である．上で述べた現状分析機能や障害発生時の対応といった本来の機能で，要求される専門知識をいかに減らせるかが，今後の大きな課題となる．

６．将来展望

本研究開発により，汎用プロトコルドライバ，パケット詳細分析機能そして容易なリモート機能が実現可能であることを検証した．今後，これらの技術を応用することにより，サービスビジネスへの適用や関連技術分野の研究への発展が期待される．本章では将来展望について具体的な一例を述べる．

６．１　サービスビジネスへの適用 － ネットワークのリモート監視・診断サービス

現在，当社のネットワークビジネスとして，ネットワーク診断サービスを行っているが，このサービスに本システムが適用できる．図10に示すように情報収集用のエージェント機能を顧客のイントラネットの各セグメントに配置することにより，現場に出向くことなく，必要なときに，リモートで顧客のネットワークの情報収集及び現状分析が可能となる．更に高価な専用ハードウェアを用意する必要がなく，一度に多くの顧客へのサービスが可能となる．

[8] ネットワークの規格．100BASEは理論的に１秒間に最大100Mビット伝送することができるが，実際にはパケット同士の衝突が発生するため30Mビットほどとなる．

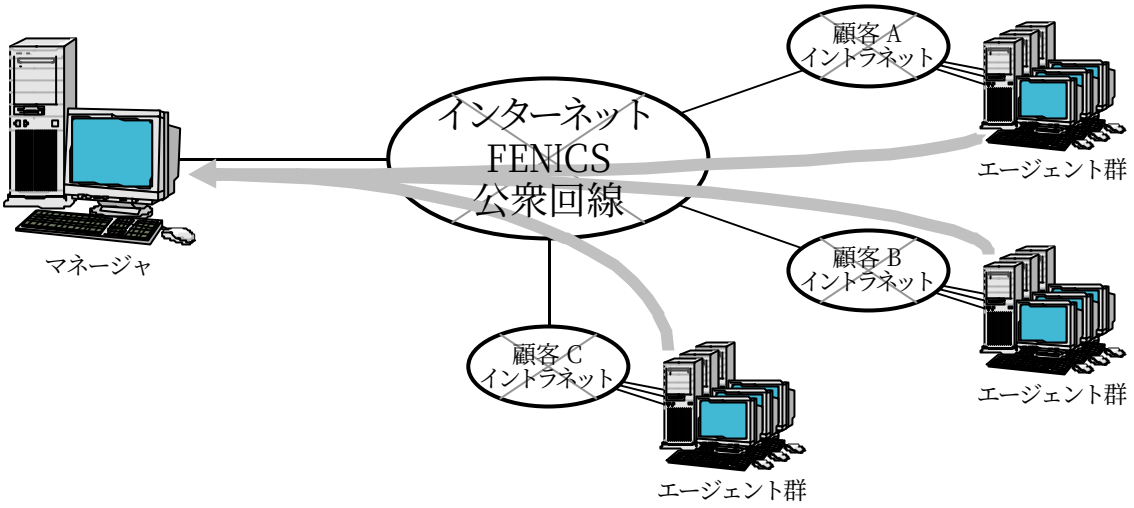


図10　リモート監視・診断サービス

6．2　関連技術の研究開発

6．2．1　ASP における稼働状況監視ツールの開発

近年多くの企業がASP[9]事業に乗り出している．このASP事業を執り行う上で，サービスの質を維持するにあたり重要となるのがSLA[10]である．明確なSLAの指標基準をユーザに示し，SLAを常に満たすように的確な監視を行うことは競合他社との差別化にも繋がるからである．SLAの指標項目のなかでも代表的かつ重要なレスポンスタイム，システムアベイラビリティそしてネットワークエラー発生率の監視ツールの開発に，今回の技術が応用できるのではないかと考える．更にこの監視ツールを用いたSLA監視サービスをビジネス化することも期待できる．

6．2．2　ソフトウェアによるインテリジェントルータへの応用

Microsoft Windows NTにはルーティング機能が標準搭載されており，コンピュータにNICを複数枚装着することにより，ルータとして機能させることができる．しかし，ルーティング対象がIPだけであり，またそのルーティングアルゴリズムも単純なものしかないため，全く使用されていないのが現状である．ここで汎用プロトコルドライバとパケット解析機能を用いたパケットのフルキャプチャにより，過去のトラフィック履歴や現在のトラフィックより理想的なルーティング及びフィルタリングを行うなど，コンピュータならではのインテリジェントなルータ機能が実現できる[11]．

---

[9] Application Service Provider．インターネットを用いて，Web ブラウザ上で動作するアプリケーションを顧客に貸し出す事業者．

[10] Service Level Agreement．顧客に対し，通信サービスの品質を保証する制度．

[11] ルーティング及びフィルタリング方式について現在特許申請中．（出願番号：特願 2000-34223）

6．2．3　非SNMP対応機器監視システムの開発

SNMPに対応したネットワーク機器は，そのSNMP機能により稼働状況の監視が行えるが，そうでない機器は稼働状況の把握は困難である．しかし，ネットワーク機器は制御用パケットやデータパケットの送受信を行っているので，これらのパケットをキャプチャし，集計解析することで非SNMP対応機器についてもその稼働状況の監視が可能となる．例えばネットワークプリンタの稼動状況監視ツールが挙げられる．

7．おわりに

今後ますますの発展が予想されるネットワーク分野における本研究開発は，基礎技術の確立とその検証という意味で有意性の高いテーマであったといえる．IT技術に支えられているネットワークサービスの維持活動は重要なテーマであり，今後はサービスそのものの維持だけではなく品質の維持を求められることが予想される．このような社会的ニーズに対して，本研究開発の成果が活かされていくことを期待する．

謝辞

本研究開発及び本論文の執筆において多大な御協力を頂きました当社科学技術システム部岡崎課長並びに白石SEに心から感謝します．また各部署においてたくさんの方々の御協力を頂きました．心からお礼申し上げます．