# 携帯電話による遠隔ネットワーク監視システム

若居和直　小池英樹

電気通信大学大学院情報システム学研究科

多くのシステム管理者はポケットベルやノートPCを常時携帯し，遠隔からのシステム監視を行っている．ポケットベルは携帯に便利だが簡単な警告を受信することしかできない．ノートPCは詳細な調査が可能だが，重く，かつ通信の確立に手間がかかる．

本論文はiモード端末を用いたシステム監視システムを提案する．本システムは受動的監視システムと能動的監視システムからなる．受動的監視システムは，システムの状態があらかじめ設定した条件になると，電子メールと電話によって警告を行う．能動的監視システムは,iモードの画像表示機能を用いて，netstat, last, w, top等のUNIXシステムコマンドの出力を画像とテキストを用いて視覚的に表示する．

# A Remote Network Monitoring System using Mobile Phone

KAZUNAO WAKAI and HIDEKI KOIKE

Graduate School of Information Systems
University of Electro-Communications

Many system administrators always carry pagers or note PCs to monitor the remote system. Although the pager is easy to carry, it only receives simple messages. The note PC enables the administrators to investigate the system in detail. It is, however, heavy and takes much time to establish communication.

This paper described a remote network monitoring system using mobile phone (i-mode phone). The system composed of two sub systems: passive monitoring system and active monitoring system. The passive monitoring system monitors the system, and send alarms via email and voice when a particular value of the system satisfies a pre-defined condition. The active monitoring system allows administrators to see ouputs of some UNIX system commands (e.g. netstat, last, top) with color pictures and text.

## 1. はじめに

近年，インターネットの普及によりネットワークの重要度が増大し，ネットワークの監視の必要性はましている．そのため，システム管理者がどこにいようとも不正侵入等の明確な異状時には管理者を呼び出し，必要な情報を提示するシステムが必要となっている．

このようなシステムとして現在はポケットベルやノートパソコンを携帯端末として持ち歩くことが多い．ポケットベルはどこでも受信できるため，受動的なシステム監視ができ，手軽である．しかし，単純な文字しか伝達できないため，何がおきているかという詳細が把握できない．PDA等の携帯端末を用いれば能動的な監視ができ，詳細な情報を確認することができる．しかし，電話等への接続が不可欠であり，その分手間と時間がかかり，調査開始までに遅れが生じる．また，ノートパソコンを用いようとした場合，常時携帯する必要があるが，その大きさなどにより実際に常時携帯している人はごく少ない．

一方，最近は携帯電話が著しく普及している．電話としての機能以外にも，簡単な電子メールとWorld Wide Web (WWW)のブラウズ機能を持つものも多い．どこでも受信可能な電話と電子メールにより，ポケットベルよりも詳細な情報のわかる受動的なシステム監視ができる．WWWのブラウズ機能により，システムの詳細情報を調査，能動的なシステム監視ができる．小型軽量のためノートパソコンより常時携帯が容易であり，電話等への接続の手間もない．

そこで，本研究ではNTT DoCoMoのiモードを用いた，サーバの遠隔監視と警告のためのシステムを開発，運用した．

## 2. システムの構成

本システムは受動的監視システムと能動的監視システムを統合したシステムである．ポケットベルやノートパソコンをそれぞれ単体で用いた監視と違い，本システムでは二種類の監視を単体で行なえるため，受動的監視システムは能動的監視システムを用いて詳細を調べる事を前提とした設計を行なった．

図1のように，受動的監視システムはシステムを監視し，異状と判断すると電話や電子メールを用いてユーザ

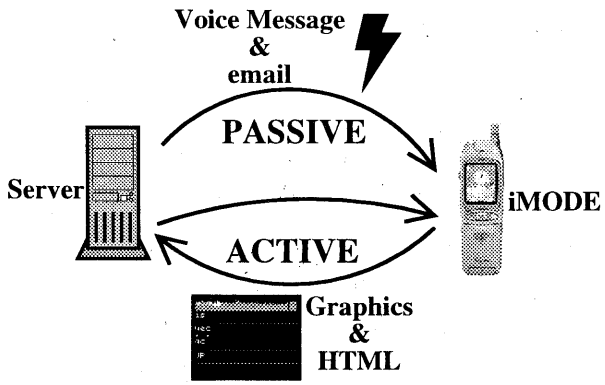


図1　受動的システムと能動的システム

に警告を送る.

能動的監視システムは, ユーザ (管理者) が情報を見て, 状況を把握するためのシステムである. 受動的監視システムにより送られる電子メールに記述された情報を基に, 携帯電話の WWW 閲覧機能を用いて, システムの状態を調査する.

### 2.1　受動的監視システム

受動的なシステム監視は一定時間毎にシステムを監視し, コマンドにより得られるデータの値が, あらかじめ条件として設定した数値を越えると, 異状と判断する. そしてユーザに電話をかけて警告を行ない, 同時に電子メールで異状と判断した条件の情報を送信する. これらを併用するのは, 二つの手段を同時に用いることで, 確実性を高めるためである. 電話が通じない場合, 一定時間毎に継続して電話での呼び出しを行う.

監視のためのデータは, システムに備わっているコマンドを中心に, システムのログ,IDS(Intrudition Detection System) のログ等を利用する. システムに備わっているコマンドを用いる事により, 新たな知識を用いる事無く, ユーザが使い慣れた手順で探索できる. また, 既存のコマンドを利用することにより, 機種依存, 移植性の問題を軽減する.

#### 2.1.1　システム一覧

本システムで使用している監視コマンドの一覧を表 2.1.1に示す. (*) がついている項目は現在は未実装のシステムである.

表1　コマンド / システム一覧

| | |
|---|---|
| netstat | ネットワーク接続状態 |
| last | ログイン / ログアウト状況 |
| w | ログイン中のユーザ / コマンド |
| df | ディスクの使用状況 |
| top | システム / プロセスの状態 |
| syslog | システムのログ |
| ps | 全プロセスの状態 (*) |
| live camera | ホスト周囲の状況 (*) |
| snort | ネットワーク侵入検知 (*) |

コマンドの実行に得られたデータを, フィルタプログラムを通して, 機種依存しない共通化された形でホスト毎, コマンド毎に保存する. 警告, 能動的監視システムにおける閲覧もこのホスト, コマンド単位で行われる.

以下に, 通知を行う際の具体例を述べる. システムの負荷が高い場合,top コマンドを用いると負荷の値がわかる. 値が条件として設定した数字より大きいと, システムは異状とみなし, 警告を生成する. 図 2のように, 全てのコマンドが警告のチェックを終えてから, まとめて一つの警告としてユーザに電話と電子メールで通知するため, 一度に複数の異状が発生しても連続で電話が鳴ることはない.

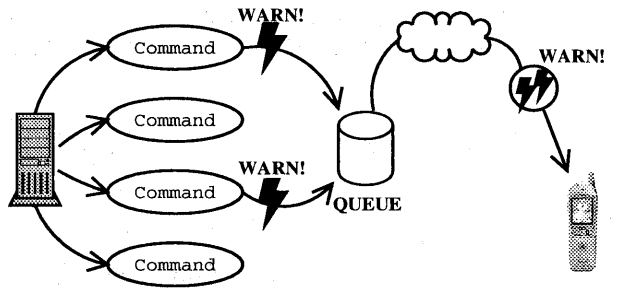


図2　警告配送の仕組み

### 2.2　能動的監視システム

本システムの最大の特徴は,i モードの画像表示機能を用いた能動的監視システムである.

能動的監視システムでは,HTML を用いて, サーバの状態を要約した視覚化画像と, 詳細のための文字による詳細情報を提供する.

これらのデータを一定時間毎に生成して, 視覚化画像と文字情報を用いて情報提示を行う.

#### 2.2.1　視　覚　化

携帯電話を用いて, 視覚化された情報を提示するための最大の問題点はその画面サイズが小さい事である. また,i モードの規格では画像サイズは最大 94x71 ドットであり, ドットが見える程度の粗い画像しか表示できない. そこで, 情報をいかに圧縮して, 最低限の情報のみを表示するかが重要になる. そのため, 時間毎の変位の強調と特徴量の抽出を行った.

まず, 図 3のように, 時間毎の変位を見るために, 横軸として時間をとった. 時間を横軸として見て, その値が急激に変化しているならば, その急激な変化にはなにか理由があるはずである. 時系列として見ることで, その時点の情報のみでは見のがす異状を発見することが出来る. さらに, 棒グラフとして縦軸の値の絶対量を示しつつ, 折線グラフのように微妙な変位をより強調するために, 縦軸の値毎に色を変化させた.

画像自体の大きさも, 図 4のように, 一旦データ自体にあわせたサイズで作製してから, 最終的に画面サイズに縮小することにより, 情報の損失を極力防いだ. この際, 縮小前の画像の一定範囲が, 縮小先の 1 ドットに圧縮される. そのまま縮小すると縮小先でデータの重複が発生するため, データの特徴量を抽出し, 重複範囲内で最も代

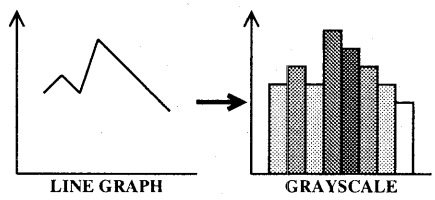


図3　色変化による値の強調

表的な値を採用した.

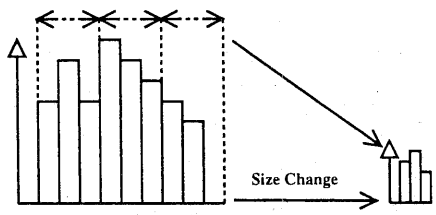


図4　代表値の抽出

#### 2.2.2　文字情報

視覚化画像では詳細な情報は提示できないため, 文字情報を用いてより詳細な情報を表示した. しかし,i モードの規格では, 一画面内に表示できる文字数が最大 18x8 文字であり, 画像と合わせて最大 5KB までのデータ量しか扱えない制約のため, 一度に表示できる情報量は限られる. そのため, 図 5のように, 一つの情報を分割して数ページの HTML に分け, 階層的に表示した.

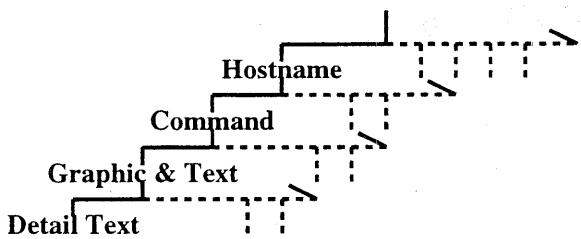


図5　HTML の階層構造

## 3.　監視システムの詳細

各監視システムについて, データの取得方法, 警告と判断する基準, 視覚化の手法, 詳細データについて示す.

### 3.1　netstat

netstat コマンドを利用して, 監視対象のサーバに対して行なわれているネットワークの接続状態を監視する.

データは, 監視対象のサーバと接続先双方の IP アドレスとポート番号, 接続の状態である.

あらかじめ各ドメイン毎に許容できる時間あたりの接続数を設定して, これを接続数が越えた場合, 又は, ドメイン毎に許容できるポート番号を設定して, これ以外のポート番号での接続があった場合に警告を行う.

視覚化手法として, 図 6のように, 縦軸をドメイン毎に分割して, 外部からの接続を発見しやすいようにした. IP アドレスからドメインが取得できないものは, 最下層に表示した.

詳細情報として, 視覚化画像と共に, 接続先毎にまとめた接続ポートの一覧を文字情報として表示し, それぞれの接続先ホストに対して, 接続状態やキューの状態を別ページで表示した.

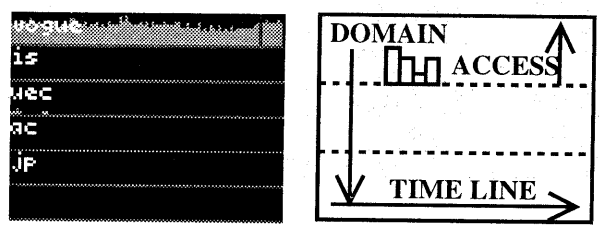


図6　NETSTAT

### 3.2　last

last コマンドを利用して, 監視対象のサーバにおけるユーザのログイン及びログアウトの時間, 接続元を監視する.

データは, ログインしたユーザの名前, どこから接続したか, ログイン時刻, ログアウト時刻, それにシステムが再起動または停止した時刻である.

あらかじめ想定されるユーザと接続元の一覧を設定しておき, それ以外のユーザが接続した場合, ユーザに警告を行う.

視覚化手法として, 図 7のように,netstat と同様に縦軸をドメイン毎に分割, そのドメイン毎にログインしているユーザ数を縦軸としてあてた.

詳細情報として, 視覚化画像と共に最近ログインしたユーザの一覧とそれぞれのログイン時刻, ログアウトしていればその時刻, 接続元を表示する.

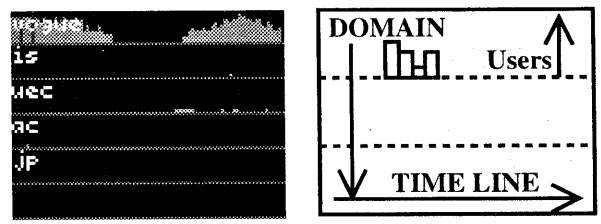


図7　LAST

### 3.3　w

w コマンドを利用して, 監視対象のサーバにおけるログイン中のユーザや使用中のコマンドを監視する.

データは, 使用中の端末, 接続元, ログイン時間, 使用中のコマンドである.

last と同様, あらかじめ想定されるユーザと接続元の一覧を設定しておき, それ以外のユーザが接続した場合, ユーザに警告を行う. また, ログイン時間が極端に長い

ユーザについても警告を行う.

視覚化は, 図8のように, 縦軸に同時にログインしているユーザ数を当てることにより, 時間ごとのユーザ数の変移を強調する.

詳細情報として, 視覚化画像と共に上記全てのデータを文字情報として表示する.

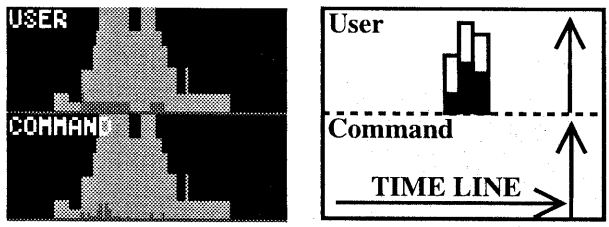


図8 W

### 3.4 df

df コマンドを利用して, 監視対象のサーバにおけるファイルシステムのディスク容量の使用状況を監視する.

データは, ファイルシステム,1K 単位での全容量, 使用容量, 使用可能容量, マウント位置である.

あらかじめファイルシステム毎に限界となる使用割合を設定し, 使用容量が設定値を越えていると警告を行う. また, 設定されていないファイルシステムとマウントの組みがあると警告を行う.

視覚化は, 図9のように縦軸にファイルシステムとマウント位置の組を当てることにより, 時間ごとの使用容量の変移を強調. 組で表現しているので, ファイルシステムが同じでも, マウント位置が違うと別に表示する. オートマウント等, ファイルシステムがマウントされていないときは, ベースを青色で表示する.

詳細情報として, 視覚化画像と共に上記全てのデータを文字情報として表示する.

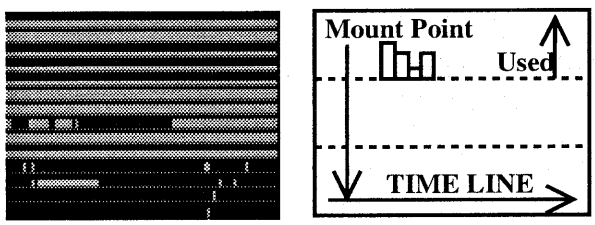


図9 DF

### 3.5 top

top コマンドを利用して, 監視対象のサーバにおけるシステムの状態と CPU の使用状況を監視する.

データは, 表3.5のようにシステムのデータとプロセス毎のデータの二種類にわけられる.

視覚化は, 図10のように, 縦軸をシステム負荷, プロセス数, メモリ量, スワップ量に分割し, システム全体の時間ごとの変移を強調する.

表2 top で得られるデータ

| システム | プロセス |
|---|---|
| load average | PID |
| Process | USER |
| Sleep Process | PRIORITY |
| Memory | NICE |
| Free Memory | SIZE |
| Swap | RSS |
| Free Swap | STATUS |
| uptime | CPU 使用率 |
| | TIME |
| | COMMAND |

あらかじめ閾値を設定しておき, システム負荷, プロセス数, 使用可能メモリ, 使用可能スワップが設定値を上まわった場合, 上まわった項目に対し警告を行う.

詳細情報として, 視覚化画像と共にシステムの情報 (システムの負荷, 起動時間, プロセス数 / スリープ中のプロセス数, メモリ量 / 使用可能なメモリ量, スワップ量 / 使用可能なスワップ量) とプロセス毎のユーザと CPU 使用率, コマンドを表示する.

また, それぞれのプロセスに対して, 全データを表示した詳細画面を表示する.

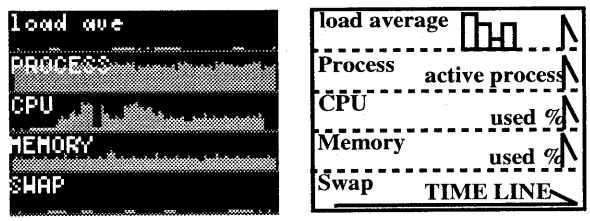


図10 TOP

### 3.6 syslog

syslog で生成されるログを利用して, 監視対象のサーバにおけるログの状況を調べる.

この機能は見えログ[4] の機能の一部を実装したものであり, 図11のように, 上段にシステムのログの量, 下段にシステムの時間辺りのログの長さを視覚化画像として示し, ログの異常な増大等の挙動を発見しやすくした.

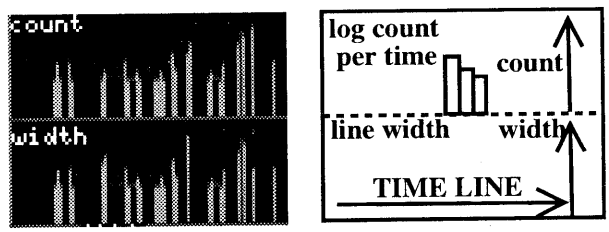


図11 SYSLOG

### 3.7 live camera

サーバに備えられたライブカメラを用いて, 実世界におけるサーバの周辺を監視する.

図12のように, 画像として, 一定時間おきに取られたライブカメラの映像を, 縮小して表示する.

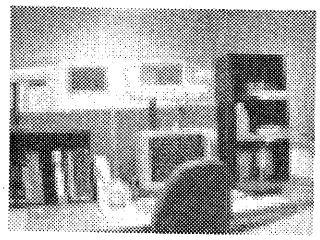

図12 Live Camera

## 4. 実 行 例

現在, プロトタイプのシステムを実際に作製, 運用している. 以下に, その実行例を示す.

```
Subject: iNet WARNNING

——

2000/05/12 17:16
[NETSTAT]
Access from other hosts
vanhalen.other.net
Port 23/3299
Queue 0/0
TIME_WAIT
```

図13 NETSTAT からの警告メール

まず, 未知の外部のホストから TELNET によるアクセスがあったとする. これは NETSTAT の警告条件に該当するので, ユーザに対し, 電話での発呼と, 図13のようなメールが送られる.

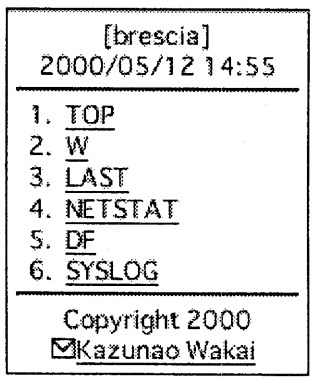


図14 System List

この警告を受け取ったユーザが, 携帯端末の WWW 閲覧機能を用いてアクセスすると, 図14の画面となる. これは, 監視対象のサーバにて現在稼働しているシステムの一覧である. 今回は,netstat が警告を送ってきたので,NETSTAT を選択する.

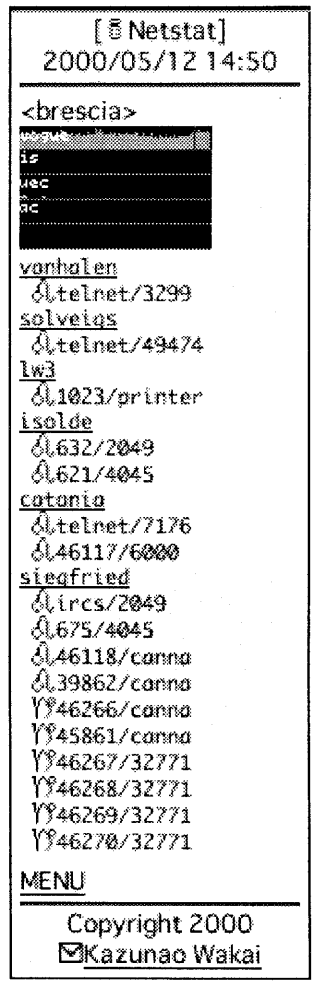


図15 NETSTAT SYSTEM

図15は,NETSTAT のシステムである. 上部にデータの採取時刻と監視対象のサーバ名, 状態を要約した視覚化画像を表示し, その下にアクセスしてきたホスト名 (あるいは IP アドレス) の一覧を表示する.

各ホスト名の下に並んでいるのは, 記号で示された接続状態と, 監視対象サーバと接続しているホストのポート番号である. ポート番号がシステムで定義されたサービス名に該当する場合は, 数字ではなく名前で表示する.

ホスト名はリンクになっており, クリックすると詳細を表示する. 今回は, 警告では vanhalen というホスト名が示されているので,vanhalen のリンクを辿る.

ホスト名のリンクを辿ると,図16となる. これは,NETSTAT のホスト毎の詳細情報である. 先程の情報に加えて,(IP アドレスでない場合は) 完全なホスト名, 送信 / 受信キューの状態, 接続状態を表示する. この画面より,vanhalen が TELNET プロトコルで接続してきていたが, その接続は既に閉じられようとしている事が確認できる.

次に, ログインが成功しているならば,LAST のログに残っているはずなので,LAST で誰が接続してきたのかを調査してみる事にする.

図17は, 最近ログインしたアカウントの一覧である.

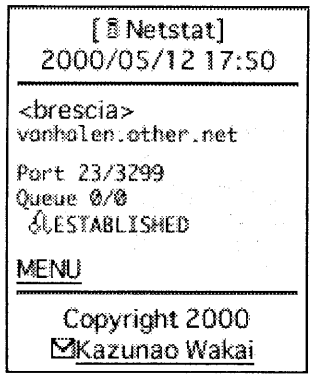


図16 NETSTATの詳細情報

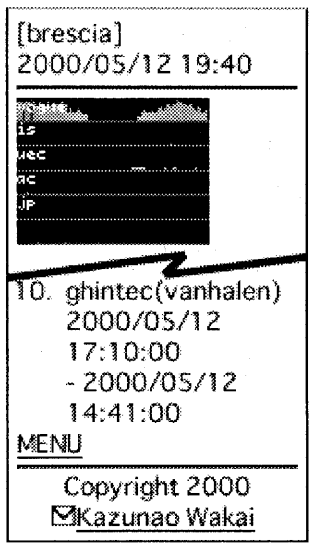


図17 LAST SYSTEM

ログイン時刻と, ログアウトしているならばその時刻, アクセス元のホスト名が表示される, この画面より,ghintecというアカウントでログインしてきた事がわかる.

もし,NETSTATで見て接続が閉じられておらず, ログイン中ならば,WやTOP等他のシステムを用いることで, さらに詳細な情報を得る事ができる.

## 5. 考　　察

携帯電話を持ちあるくだけで, 気になる時に即座にチェックできるので, 受動的監視に頼らずとも, ある程度の異状は能動的監視だけで発見することができた. ただし, 普段より常に監視するわけにはいかないため, そのような時に受動的監視が役に立つ.

携帯電話単体で受動的監視と能動的監視が両立できる事により, 従来よりのポケベルあるいはノートパソコン単体での運用と比較して, シームレスかつ手軽にシステムの状態を把握できた. また, 視覚化画像により要約を示す事で, 一目で状態が把握でき, 時系列による変位もわかるようになった.

ただし, 現段階ではまだいくつかの問題がある. 受動的監視は異状を検知するだけであり, その状況を異常と判断するのはあくまで人間である. そのために, 能動的監視システムを構築したのだが, 今回構築したシステムは未実装のシステムが多く, そのために情報を相互参照して, 有効に活用する事が難しかった. 実際にマシンの前で行う作業とほぼ同じ情報量をどこでも得られる事を目的の一つとしていたが, いくつかのシステムが足りない事により, 得られない情報ができてしまった. だが, 情報を採取するシステムを無闇に増やせばよいということでもないであろう. 最低限有効な情報を得られるにはどの情報を活用して, このシステムに組みこんでゆけばよいのか, これからの課題である.

## 6. ま と め

iモードを使用した携帯電話によるネットワーク監視システムを提案し, プロトタイプを構築, 試験的に運用中である.

このシステムを使用する事で, どのような場所からでも, システムの状態を把握できるようになった. 受動的監視システムと能動的監視システムを組みあわせる事で, 定期的にチェックしなくとも, システムの異状の早期発見, 調査が実現できる. 今後の課題としては, 1) 最低限必要なシステム情報の選択. 2) より効果的な, 電話を用いた警告手法の確立. 3) 現在ホスト毎, コマンド毎に分割されているデータを統合して視覚化, 提示する手法. 4) より正確な異状の検知. 5) 異状時の, ユーザとのインタラクションの改善 6)IDSやSMNP等との連携があげられる.

## 参 考 文 献

1) Martin Roesch, "Snort - Lightweight Intrusion Detection for Networks", USENIX USA '99 Conference(1999).
2) Stephen G. Eick, and Paul J. Lucas., Displaying Trace Files, Software Practice and Experience, Vol. 26, No. 4, pp.399 – 409, April(1996)
3) 吉田功, 桑原晶史 etal, "モバイルコンピューティングの電力現場業務への適用", 電子情報通信学会, TECHNICAL REPORT OF IEICE, IN97-179, p131,(1998-02),
4) 福田晴元, 小野論, 高橋直久, "インターネットQoSビジュアライザの設計と実現", 電子情報通信学会論文誌 B-I, Vol.J80-B-I No.6 pp.438-446, June(1997)
5) 高田哲司, 小池英樹, "ログファイルの視覚化による不正侵入検知手法の提案", 情報処理学会, コンピュータセキュリティシンポジウム '98 論文集, p.153-158(1998).
6) 高田哲司, 小池英樹, "見えログ: 情報視覚化を用いたログ情報調査支援システム", 日本ソフトウェア科学会, インターネットコンファレンス '99 論文集, pp. 146, Dec(1999)